Metacyclic Groups of Odd Order

Hyo-Seob Sim

May 1992

A thesis submitted for the degree of Doctor of Philosophy
of The Australian National University

Declaration

The work in this thesis is my own, except where otherwise stated.

Hyo-Seob Sim

Hyo-Seob Sim

Acknowledgements

I am deeply indebted to my supervisors Dr L. G. Kovács and Dr M. F. Newman, who have never stopped encouraging me to improve my ideas further by sharing their ideas and insight with me. I thank them for all their general guidance and inspiration throughout the course of this work. I also thank my advisor Dr R. A. Bryce for his help and comments about various aspects of this thesis.

During the writing of this thesis, I have also been helped by many other people in the Mathematics Research Section at the Australian National University. I wish especially thank Werner Nickel, Alice Niemeyer, Dr E. A. O'Brien, Dr Mark Short, Michael Smith and Dr R. B. Zhang, for all their warm help and valuable comments concerning this work. I am grateful to Professor M. Y. Xu for helpful discussions during his visit. I must also thank Mrs Philippa Harvey, whose generous help made my life in Canberra very pleasant.

My thanks also go to my teachers in the Department of Mathematics and the Department of Mathematics Education at the Pusan National University. They all have guided me and encouraged me. In particular, Professor A. C. Kim, who persistently shepherded my academic life, has provided continual assistance in various ways.

For providing my scholarship throughout the course of this work, I thank the Australian National University. I also thank the Australian Government for subsidizing my study in Australia.

Finally, I would like to thank my wife, both of our families and all my friends for their love and support.

Abstract

The work in this thesis was largely motivated by the aim of producing computer libraries of finite soluble primitive permutation groups with metacyclic point stabilizers. A classical result of Galois reduces the problem to that of determining all metacyclic irreducible linear groups over finite prime fields. The central topic of this thesis is a description of a theoretical approach to the problem for groups of odd order.

The first part of the thesis is devoted to the determination of the abstract isomorphism types of metacyclic groups of odd order. We propose (four-generator) presentations for such groups and obtain a practical solution of the isomorphism problem for these presentations. We then proceed to investigate faithful irreducible representations of metacyclic groups of odd order. We discuss a natural correspondence between faithful irreducible representations of such a group and irreducible representations of the centre of the Fitting subgroup with core-free kernel. This produces, in principle, a solution of the linear isomorphism problem for metacyclic irreducible linear groups of odd order. We also attempt by a direct approach to determine, up to linear isomorphism, metacyclic primitive linear groups of arbitrary order over finite fields.

It is expected that the results we obtained will provide a theoretical basis for a practical algorithm to list representatives of the linear isomorphism types of odd order metacyclic irreducible linear groups over finite fields.

Contents

Chapter 1

Introduction

1.1 Motivation and contents of the thesis

Groups given by finite presentations in terms of 'generators' and 'defining relations' are often investigated by computing their 'small' finite quotients [see, for example, Holt and Rees (1991).] To facilitate this, it is useful to have available lists, perhaps in the form of computer libraries, of 'small' finite groups. One such library was prepared by Holt and Plesken (1989); it contains almost all perfect groups of order less than 10^6. Another, due to Short (1990), gives all soluble primitive permutation groups of degree less than 2^8. The work reported in this thesis was largely motivated by the long-term aim of producing libraries of another accessible kind of group, namely finite soluble primitive permutation groups with metacyclic point stabilizers. More ambitiously, instead of making lists of such groups up to a certain size once and for all, one would like to have an algorithm for generating such lists up to limits set interactively according to the applications envisaged and the resourses available.

Permutation isomorphism types of finite soluble primitive permutation groups with metacyclic point stabilizers are in one-to-one correspondence with linear isomorphism types of finite metacyclic irreducible linear groups over finite prime fields. Before practical algorithms of the kind indicated above can be contem-

plated, we need to improve our understanding of these linear groups. In this thesis we explore this problem at a theoretical level, with a view to turning to algorithmic issues at a later stage.

Chapter 2 presents some necessary general background; along with Section 1.3, it establishes most of the terminology and notation used in the thesis. Chapter 3 and Chapter 4 form the main body of the thesis. They are concerned with the theory of presentations and representation theory of metacyclic groups of odd order. The results developed in these two chapters form a theoretical description of our motivating problem.

In Chapter 3 we consider isomorphism types of finite metacyclic groups. The traditional setting for any discussion of (finite) metacyclic groups is provided by *metacyclic presentations.* Namely, each finite metacyclic group has presentations of the form

$$\langle\, a, b \mid a^m = b^s,\ b^n = 1,\ a^{-1}ba = b^r \,\rangle$$

(with positive integers m, n, r, s), and each group defined by such a presentation is finite and metacyclic. There are two problems with this approach. One is that the order of the group so defined is not necessarily mn. This is a special case of a problem for all polycyclic presentations. We call a metacyclic presentation of the above kind *consistent* if the order of the group defined is mn. In terms of the parameters, this is the case if and only if $n \mid r^m - 1$ and $n \mid s(r-1)$. There is an algorithm which, given a polycyclic presentation, produces a consistent polycyclic presentation. This algorithm applied to a metacyclic presentation produces a consistent metacyclic presentation. The other problem is to decide whether two such presentations define isomorphic groups or not. The outstanding issue is to have an efficient algorithm for making this decision.

The first step towards the solution of this isomorphism problem is traditional: one tries to choose a class of 'special presentations' in which each isomorphism type of metacyclic groups has precisely one representative. The second step is to supplement the first step by an efficient algorithm for computing the special

presentation of a metacyclic group. Given any two metacyclic presentations, one can use the algorithm to compute a special presentation for each in turn: the two metacyclic presentations define isomorphic groups if and only if the two special presentations are identical. This is the form in which solutions of the isomorphism problem are envisaged.

We propose presentations of a certain form for metacyclic groups of odd order, which are called *standard presentations* in this thesis. Note that the standard presentations are not metacyclic presentations in the above sense. We also provide a practical solution of the isomorphism problem for presentations of this special kind [see Theorem 3.5.4]. This investigation enables us to list representatives of the isomorphism types of metacyclic groups of odd order in terms of standard presentations. The second step for metacyclic groups of odd order now amounts to having an algorithm which produces a standard metacyclic presentation from an arbitrary consistent metacyclic presentation for odd order. There is no question that such algorithms exist; the issue is to find one that is reasonably efficient. We hope that our discussion have clarified theoretical matters in sufficient detail. On the other hand, the second step is not needed for tasks like counting the number of isomorphism types of metacyclic groups of any given order or generating computer libraries of the kind envisaged above. In view of our motivation, we do not pursue that second step in this thesis.

Apart from basic generalities, the literature usually deals with groups of prime-power order. The isomorphism types of metacyclic p-groups have been determined by several authors. The odd prime-power order case is relatively easy; it will suit us to give a concise treatment of it in detail [see Section 3.1]. (For 2-groups, the situation is rather more complicated, but the problem has been solved by several authors; see, for example, Newman and Xu (1990).)

Once we have studied the theory of abstract metacyclic groups of odd order in sufficient detail, we proceed to investigate faithful irreducible representations of such groups. Chapter 4 is devoted to this subject. Most of the work in this

chapter is done without restriction to the characteristic of the ground field, but difficulties relating to Schur indices intrude in some parts and to avoid these we then restrict attention to fields of nonzero characteristic. This restriction does no harm, given that our aim is to deal with metacyclic irreducible linear groups over finite fields. These linear groups are then the images of the representations so studied. The remaining problem is to decide when two such images are linearly isomorphic, that is, conjugate in the relevant general linear group. Of course conjugacy is not a question until abstract isomorphism is assured but equivalence of representations is denied, and then we are dealing with the conjugacy of images of the various faithful irreducible representations of one group, one representation from each equivalence class.

Two listing problems are envisaged in Chapter 4. One is to list the equivalence types of faithful irreducible representations of a given metacyclic group of odd order, and the other is to list the conjugacy classes of metacyclic irreducible subgroups of the general linear groups. The correspondence theorem established in Section 4.4 reduces the first problem to a corresponding problem for an abelian characteristic subgroup, namely the centre of the Fitting subgroup. This yields, in principle, a solution of the conjugacy problem.

In Chapter 5 an attempt is made to determine, up to conjugacy, all metacyclic primitive subgroups of $GL(n, p^k)$. There exists a metacyclic subgroup (namely, the normalizer of a cyclic irreducible subgroup of order $p^{kn}-1$ of $GL(n, p^k)$) which contains a conjugate of each metacyclic primitive subgroup of $GL(n, p^k)$. The problem may be solved by discussing the $GL(n, p^k)$-conjugacy of the subgroups of this subgroup. We give an explicit solution for odd prime-power degree. This supplements the result of Chapter 4 of Short (1990).

We conclude the thesis with some comments on possible future developments for algorithmic problems.

1.2 An introduction to metacyclic groups

A *metacyclic group* is a group G which has a cyclic normal subgroup K such that G/K is also cyclic. We shall usually deal with finite metacyclic groups in this thesis; to avoid repeated use of the adjective 'finite', by a metacyclic group we shall mean a finite metacyclic group. Subgroups and quotient groups of metacyclic groups are also metacyclic. Some special classes of metacyclic groups can be found in Beyl (1972) and Chapter 1 of Coxeter and Moser (1957).

We note that there is different terminology in the literature. Some authors often replace the term by *bycyclic*, which is also used for groups which are products of two cyclic subgroups (not necessarily normal). Other authors use the term 'metacyclic' in a different sense, namely for groups with both the commutator subgroup and the commutator quotient group cyclic; see, for example, Zassenhaus (1958, p. 174) or Hall (1959, p. 146).

Metacyclic groups are usually presented on two generators with three defining relations. In fact, each metacyclic group has presentations of the form

$$\langle\, x, y \mid x^m = y^s,\ y^n = 1,\ x^{-1}yx = y^r \,\rangle$$

with the numerical conditions

$$0 < m, n, \quad r^m \equiv 1 \bmod n, \quad s(r-1) \equiv 0 \bmod n.$$

Conversely, any group defined by such a presentation is a metacyclic group of order mn. This characterization is well known and found several times in the literature; for example, as Theorem 7.21 in Zassenhaus (1958, p. 129).

Basmaji (1969) attempted to give a partial answer for the isomorphism problem for these presentations. Most of the literature of metacyclic groups concerns the classification of metacyclic groups of prime power order, or more simply metacyclic p-groups. Various classifications for metacyclic p-groups may be found in Lindenberg (1970a, 1970b, 1971), Beyl (1972), King (1973), Newman and Xu (1988, 1990), and Rédei (1989).

In his series of papers, Lindenberg gave a classification for metacyclic p-groups by analysing the subgroup lattices in great detail. He divided those groups into four classes: split-modular, nonsplit-modular, split-nonmodular and nonsplit-nonmodular groups. (In the last case, his claim concerning the number of such groups was wrong. He counted some groups twice when $n > 4$ [see Lindenberg (1971)]. The corrected number is $(n^2-6n+12)/4$ if $n \equiv 0 \bmod 2$, or $(n^2-6n+13)/4$ otherwise.) The treatment in Beyl (1972) is based on cohomology methods. He obtained a classification theorem for metacyclic p-groups by studying 'weak congruence classes of metacyclic maximal kernel extensions'. King (1973) derived his result mainly by manipulation of the usual metacyclic presentations and by group theoretic considerations. Newman and Xu (1990) pointed out that King's result contained some mistakes, which can easily be corrected. Very recently Newman and Xu (1988, 1990) have developed a new approach to metacyclic p-groups suggested by the p-group generation algorithm [see Newman (1977) and O'Brien (1990) for details of the p-group generation algorithm]. They give a complete determination of metacyclic p-groups. Rédei (1989) also gives a list of presentations for metacyclic p-groups in his book. Rédei's result and the corrected results of Lindenberg and King coincide with the Newman-Xu result.

The understanding of the structure of subgroup lattices may be useful for the study of metacyclic groups (our approach in this thesis is independent of the study of subgroup lattices). A group is *modular* if it has a modular subgroup lattice. Such groups were determined by Iwasawa [see Suzuki (1956)]. Characterizations of modular metacyclic p-groups are shown in Gerhards (1970), Lindenberg (1971) and King (1973); the non-Hamiltonian modular metacyclic groups are exactly the class of 'ordinary' metacyclic groups in King (1973). A lattice-isomorphism of the subgroup lattice of a group G onto that of a group H is called a *projectivity* of G onto H. Projectivities of modular groups were studied in Baer (1944) and Jones (1945). Every non-Hamiltonian modular finite p-group has a projectivity induced by a 'crossed isomorphism' onto an abelian group. This result make it

possible to determine the subgroup lattices of non-Hamiltonian modular finite p-groups. The structure of subgroup lattices of nonmodular metacyclic p-groups was also studied in Lindenberg (1971).

1.3 Terminology and notation

In this section we set up some general conventions and notation, which will be used frequently in this thesis. Some basic terminology is also defined.

Throughout this thesis actions of groups and most algebraic maps such as automorphisms, homomorphisms and isomorphisms are usually written as right operators. If g and h are elements of a group, the conjugate $h^{-1}gh$ is denoted by g^h.

Let m and n be positive integers and p a prime number. Let $\pi(m)$ denote the set of all prime divisors of m; let $m(p)$ denote the largest integer i such that p^i divides m. Define

$$|m \bmod n| := \min\{i \in \mathbb{Z} : i > 0,\ m^i \equiv 1 \bmod n\},$$

the multiplicative order of m modulo n: it is not defined unless $\gcd(m,n) = 1$.

The identity element of a multiplicative group is denoted by 1 and the same notation is also used for the trivial subgroup consisting of the identity element.

Let G be a finite group. $\pi(G)$ denotes the set of all prime divisors of the order of G. The centre of G is denoted by $Z(G)$. The Frattini subgroup of G is denoted by $\Phi(G)$. If G is a finite p-group, then $\Omega_1(G)$ denotes the subgroup generated by all elements of order p. The *socle* of G is the subgroup generated by all minimal normal subgroups of G.

The subgroup generated by all the nilpotent normal subgroups of G is called the *Fitting subgroup* of G. The Fitting subgroup of G is denoted by $\mathrm{Fit}\, G$. If π is a set of primes, the product of all the normal π-subgroups of G is denoted by $\mathrm{O}_\pi(G)$. The Fitting subgroup is the direct product of the $\mathrm{O}_p(G)$ for all prime divisors p of the order of G.

The largest normal subgroup of G that is contained in a subgroup X is called the *core* of X in G and is denoted by $\mathrm{core}_G X$. We often say that X is *core-free* to indicate that $\mathrm{core}_G X = 1$.

Let H, N be groups and $\phi : H \longrightarrow \mathrm{Aut}\, N$ a homomorphism. Then the homomorphism defines a semidirect product of H and N; we denote that semidirect product by $H \ltimes_\phi N$, or simply by $H \ltimes N$. We usually regard H and N as subgroups of $H \ltimes N$ via the natural identifications.

Let G be a group, H a subgroup of G and K a normal subgroup of H. Let N be a group of automorphisms of G which normalize (that is, stabilize setwise) both H and K. Every automorphism in N defines an automorphism of H/K in a natural way; the set of all such automorphisms obtained from the automorphisms of N will be denoted by $\mathsf{N}{\downarrow}_{H/K}$. For example, if C is a normal subgroup of a group P then $\mathsf{N}_{\mathrm{Aut}P}(C){\downarrow}_{P/C}$ is the group of automorphisms of P/C obtained from all automorphisms of P which normalize C.

Most general concepts of the group representation theory which are used in this thesis may be found in Curtis and Reiner (1962) or Huppert (1967) and Huppert and Blackburn (1982). Some notation and terminology for the group representation theory is shown in Section 2.3.

The notation and terminology not defined in this thesis is standard and can be found in almost all standard books on related areas. A list of notation is included at the end of the thesis.

Chapter 2

General background

In this chapter we present some general facts that will be useful in this thesis. No originality is claimed for any of the results here. Some basic concepts and notation are also defined.

2.1 Some basic facts

We first state the following basic facts without proof.

Lemma 2.1.1 *Let p be an odd prime, let m, n be nonnegative integers and let r be an integer.*

(i) *If $r \equiv 1 \bmod p$, then $|r \bmod p^n| = p^n/(p^n, r-1)$.*

(ii) *If $r^{p^m} \equiv 1 \bmod p^n$, then $1 + r + \cdots + r^{p^m-1} \equiv p^m \bmod p^n$.*

Lemma 2.1.2 *Suppose that a and m are integers with greatest common divisor d. Then the congruence $ax \equiv 0 \mod m$ has precisely the following solutions:*

$$x = tm/d, \ t \in \mathbf{Z}.$$

Lemma 2.1.3 [Dedekind's Law] *Let A, B and C be any subgroups of a group such that $A \leq B$. Then $A(B \cap C) = B \cap AC$.*

We will also need the following lemma; a stronger version of it can be found in Rose (1978, p. 193).

Lemma 2.1.4 *If C is a cyclic subgroup of a finite abelian group A such that $|C| = \exp A$, then C is a direct factor of A.*

The following slightly different version of the result by Remak (1930) will be needed. (Remak attributed some of this result to Klein and Fricke. The result is also found in several books; see, for example, Suzuki (1982, pp. 140–141).)

Theorem 2.1.5 *Let the group G be the internal direct product of its subgroups H and K. Suppose that*

$$H_2 \trianglelefteq H_1 \leq H, \quad K_2 \trianglelefteq K_1 \leq K, \quad H_1/H_2 \cong K_1/K_2.$$

Let θ be an isomorphism of H_1/H_2 onto K_1/K_2. Set

$$L := \{hk : (hH_2)\theta = kK_2, h \in H_1, k \in K_1\}.$$

Then L is a subgroup of order $|H_1K_2|$ such that

$$H \cap L = H_2, \ K \cap L = K_2 \text{ and } H_1L = H_1K_1 = LK_1.$$

(This group L is called the *diagonal* defined by θ.) *The map*

$$(H_1, H_2, K_1, K_2, \theta) \mapsto L$$

defines a bijection between the set of all such 5-tuples $(H_1, H_2, K_1, K_2, \theta)$ and the set of all subgroups of G.

We now describe some properties of semidirect products.

Lemma 2.1.6 *Let P and Q be finite groups and $\phi, \psi : P \longrightarrow \operatorname{Aut} Q$ homomorphisms. If γ is an isomorphism of $P \ltimes_\phi Q$ onto $P \ltimes_\psi Q$ which normalizes P and Q, then for all $x \in P$, $y \in Q$,*

$$(y(x\phi))\gamma = (y\gamma)((x\gamma)\psi).$$

Proof Since the two semidirect products have the same set of elements, strictly speaking our notation should distinguish between two group operations on that set. Fortunately our argument is so brief that the reader will understand our meaning without that. For example, when we write $(x\gamma)(y^x\gamma)$ the reader will note that $x\gamma$ and $y^x\gamma$ are viewed as elements of the codomain of γ so their product is to be performed in $P \ltimes_\psi Q$, while y^x is in the domain of γ so this conjugate of y by x must have been formed in $P \ltimes_\phi Q$.

Then

$$(xy^x)\gamma = (x\gamma)(y^x\gamma) = (x\gamma)((y(x\phi))\gamma).$$

On the other hand,

$$(xy^x)\gamma = (yx)\gamma = (y\gamma)(x\gamma) = (x\gamma)(y\gamma)^{x\gamma} = (x\gamma)((y\gamma)((x\gamma)\psi)).$$

It follows that $(y(x\phi))\gamma = (y\gamma)((x\gamma)\psi)$. □

Theorem 2.1.7 *Let P and Q be finite groups with* $\gcd(|P|, |Q|) = 1$. *Suppose ϕ and ψ are homomorphisms of P into* $\operatorname{Aut} Q$. *Then $P \ltimes_\phi Q \cong P \ltimes_\psi Q$ if and only if there exist $\alpha \in \operatorname{Aut} P$, $\beta \in \operatorname{Aut} Q$ such that $(y(x\phi))\beta = (y\beta)((x\alpha)\psi)$ for every $x \in P$, $y \in Q$.*

Proof Let γ be an isomorphism between $P \ltimes_\phi Q$ and $P \ltimes_\psi Q$. The coprimality of $|P|$ and $|Q|$ implies that Q is characteristic, so γ normalizes Q. We may assume that γ normalizes P also by replacing γ with its composite with an inner automorphism. Let α and β be the restrictions of γ on P and Q, respectively. Then $\alpha \in \operatorname{Aut} P$ and $\beta \in \operatorname{Aut} Q$. The relation $(y(x\phi))\beta = (y\beta)((x\alpha)\psi)$ follows from Lemma 2.1.6.

Suppose that α and β are automorphisms which relate to ϕ and ψ in the given way. Define a map γ of $P \ltimes_\phi Q$ to $P \ltimes_\psi Q$ as $(xy)\gamma = (x\alpha)(y\beta)$. It is straight-forward to show that the map γ is an isomorphism between the two groups. □

2.2 Metacyclic groups

Let G be a metacyclic group and K a cyclic normal subgroup with cyclic quotient. Then G has a cyclic subgroup S such that $G = SK$. Such a factorization $G = SK$ is called a *metacyclic factorization.* In particular, if $S \cap K = 1$, the metacyclic factorization is called *split.* A metacyclic group is *split* if it has a split metacyclic factorization.

Metacyclic groups are, of course, soluble; in fact supersoluble. Therefore, every metacyclic group has the following well known property of supersoluble groups.

Lemma 2.2.1 *Let G be a metacyclic group and $p_1 < p_2 < \cdots < p_r$ the increasing sequence of all prime divisors of the order of G. Set $\pi_i = \{p_i, ..., p_r\}$. Then a Hall π_i-subgroup of G is normal. In particular, the Sylow subgroup corresponding to the largest prime divisor is normal.*

We now collect some properties of metacyclic groups, which will be used later. Some of them are well known and others seem to be folklore.

Lemma 2.2.2 *Let G be a metacyclic group with a metacyclic factorization $G = SK$. Let $S = \langle x \rangle$, $K = \langle y \rangle$ and $A := \mathrm{C}_G(K)$. Let r be an integer such that $y^x = y^r$. Define $s := |r \bmod |K||$ and $t := |K|/(|K|, r-1)$. Then*

(i) $G' = \langle y^{r-1} \rangle$;

(ii) $Z(G) = \mathrm{C}_S(K)\mathrm{C}_K(S) = \langle x^s, y^t \rangle$;

(iii) $G/A \cong S/\mathrm{C}_S(K) \cong \mathsf{C}(s)$;

(iv) $A/Z(G) \cong K/\mathrm{C}_K(S) \cong G' \cong \mathsf{C}(t)$.

Proof For (i), see Curtis and Reiner (1962, 47.10); for (ii), see Beyl and Tappe (1982, Lemma IV.2.13). From $A = \mathrm{C}_S(K)K$, we observe that $G/A = S/\mathrm{C}_S(K)$. It is also obvious that $|S/\mathrm{C}_S(K)| = s$. It follows from $Z(G) = \mathrm{C}_S(K)\mathrm{C}_K(S)$

that $A/Z(G) \cong K/\mathrm{C}_K(S) \cong \mathsf{C}(t)$. It is routine to show that the map $b \mapsto b^{r-1}$ defines a homomorphism of K onto G' with kernel $\mathrm{C}_K(S)$. □

Corollary 2.2.3 *Let P be a metacyclic p-group for odd p and let $P = SK$ be a metacyclic factorization. Define $A := \mathrm{C}_P(K)$. Then*

$$A/Z(P) \cong P' \cong P/A.$$

Proof Since S is a finite p-group, $r^{p^i} \equiv 1 \bmod p$ for some nonnegative integer i. Fermat's Little Theorem yields $r \equiv 1 \bmod p$. By Lemma 2.1.1, we have $s = t$, so the result follows from (iii) and (iv) of the above lemma. □

Lemma 2.2.4 [Suzuki (1986, Theorem 4.3.14)] *Let P be a metacyclic p-group for odd p. Then*

(i) *P is regular;*

(ii) *$(xy^{-1})^{p^m} = 1 \iff x^{p^m} = y^{p^m}$, for every x, y in P and every nonnegative integer m.*

Lemma 2.2.5 *Let P be a noncyclic metacyclic p-group. Then*

(i) $P/\Phi(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$;

(ii) $\Omega_1(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$ *if p is odd.*

Proof The first result is obvious. Since P is regular, $\Omega_1(P)$ is a metacyclic p-group of exponent p. As p is odd, if $\Omega_1(P)$ is cyclic then P is cyclic [see Huppert (1967, Satz III.8.2)]. Thus the second result follows. □

Lemma 2.2.6 *Let P be a noncyclic metacyclic p-group and K a subgroup.*

(i) *If p is odd, K is cyclic if and only if K does not contain $\Omega_1(P)$.*

(ii) *K is normal and P/K is cyclic if and only if K contains P' and K is not contained in $\Phi(P)$.*

Proof (i) By Lemma 2.2.5, $\Omega_1(P)$ is isomorphic to $\mathsf{C}(p) \times \mathsf{C}(p)$. Suppose K is not cyclic. Then the subgroup $\Omega_1(K)$ is also isomorphic to $\mathsf{C}(p) \times \mathsf{C}(p)$ and hence

$$\mathsf{C}(p) \times \mathsf{C}(p) \cong \Omega_1(K) \leq \Omega_1(P) \cong \mathsf{C}(p) \times \mathsf{C}(p);$$

that is $\Omega_1(K) = \Omega_1(P)$. Therefore K contains $\Omega_1(P)$. Conversely, if K is cyclic then obviously K does not contain $\Omega_1(P)$.

(ii) *"only if"* Since K is normal and P/K is cyclic, obviously K contains P'. If K is contained in $\Phi(P)$, then $P/\Phi(P)$, a homomorphic image of the cyclic group P/K, is cyclic; so is P, a contradiction. Thus K is not contained in $\Phi(P)$.

"if" Since K contains P', the group K is normal in P. Since K is not contained in $\Phi(P)$, the Frattini subgroup $\Phi(P)$ is properly contained in $\Phi(P)K$. It follows from $P/\Phi(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$ that $P/\Phi(P)K$ is cyclic. Since $\Phi(P/K)$ contains $\Phi(P)K/K$ [see Robinson (1982, 5.2.13(iii))], $(P/K)/\Phi(P/K)$ is cyclic; so is P/K. □

2.3 Some representation theory

We first recall some notation and terminology from representation theory which are very often used in this thesis. The presentation, which is largely based on the treatments of Huppert and Blackburn (1982) and Feit (1982), will be given mostly in terms of modules.

Let F be a field, G a finite group and H a subgroup of G. By an $\mathsf{F}G$-module we always mean a right $\mathsf{F}G$-module of finite dimension. We define the *kernel* of an $\mathsf{F}G$-module V as the subgroup $\ker V := \{g \in G : vg = v \text{ for all } v \in V\}$. We shall use the notation $[V]$ for the isomorphism types of V. We shall denote by $V{\downarrow_H}$ the $\mathsf{F}H$-module obtained by the restriction of the operators on V to $\mathsf{F}H$. For an $\mathsf{F}H$-module W, we shall denote by $W{\uparrow^G}$ the induced $\mathsf{F}G$-module $W \otimes_{\mathsf{F}H} \mathsf{F}G$. For every extension field E of F, we shall denote by W^{E} the $\mathsf{E}G$-module $W \otimes_{\mathsf{F}} \mathsf{E}$.

An $\mathsf{F}G$-module U is called a *direct summand* of an $\mathsf{F}G$-module V if there exists an $\mathsf{F}G$-module U' such that $V \cong U \oplus U'$. An irreducible $\mathsf{F}G$-module U isomorphic to a factor of a composition series for an $\mathsf{F}G$-module V is called an *irreducible constituent* of V. If U is isomorphic to an irreducible submodule of V, then we call it a *bottom constituent*; each irreducible homomorphic image of V is called a *top constituent* of V. We say that an irreducible F-representation ρ of G is a *top/bottom constituent* of an F-representation σ of G if an $\mathsf{F}G$-module which affords σ has a composition series whose top/bottom constituent affords ρ. In general, ρ is an *irreducible constituent* of σ if some composition factor of that module affords ρ.

Let W be an $\mathsf{F}H$-module. For a ring automorphism α of $\mathsf{F}G$ such that $\mathsf{F}\alpha = \mathsf{F}$ and $G\alpha = G$, we define an $(\mathsf{F}H)\alpha$-module W^α with the underlying set $W \times \{\alpha\}$ as follows. Define the vector space structure of W^α by the rule

$$(w_1, \alpha) + (w_2, \alpha) = (w_1 + w_2, \alpha), \ w_1, w_2 \in W$$

and

$$(\lambda\alpha)(w, \alpha) = (\lambda w, \alpha), \quad \lambda \in \mathsf{F}, w \in W.$$

We then define the action of $H\alpha$ via

$$(w, \alpha)(h\alpha) = (wh, \alpha), \quad w \in W, h \in H.$$

It is routine to check that W^α is an $(\mathsf{F}H)\alpha$-module.

We now consider some special cases of the above construction. Let α be an automorphism of G and let α^* be the F-automorphism of $\mathsf{F}G$ induced from α. Then of course F and G admit α^*. Suppose that H is a characteristic subgroup of G. We define W^α as the $\mathsf{F}H$-module W^{α^*}. In terms of representations, we may rephrase this as follows. Let ρ be a representation of H over F. Then the composite map $(\alpha{\downarrow_H})\rho$ is a new representation of H over F. Since we prefer to keep all actions on the right, we have defined W^α so that if W affords ρ then W^α affords $(\alpha^{-1}{\downarrow_H})\rho$.

When $H = G$, this construction of a new representation by composition with an automorphism yields a natural left action of $\operatorname{Aut} G$ on the set of F-representations of G. Two F-representations ρ_1 and ρ_2 of G are equivalent if and only if $\alpha\rho_1$ and $\alpha\rho_2$ are equivalent, so $\operatorname{Aut} G$ also acts naturally on the set of equivalence types of F-representations of G.

Suppose that H is a normal subgroup of G. Let g be an element of G and let g^* be an inner automorphism defined by

$$x \mapsto g^{-1}xg, \quad x \in G.$$

We then define W^g as the $\mathsf{F}H$-module W^{g^*} and call it a *G-conjugate* (namely, the g-conjugate) of W. In this natural way, G acts on the set of all isomorphism classes of irreducible $\mathsf{F}H$-modules. The G-orbit of each $[W]$ is called the *G-conjugacy class of* $[W]$.

The subgroup $T(W) := \{g \in G : W^g \cong W\}$ is called the *inertia group of* W. If W is an irreducible $\mathsf{F}H$-module such that $T(W) = H$, then $W\uparrow^G$ is an irreducible $\mathsf{F}G$-module.

Let E be a Galois extension of F with the Galois group $\operatorname{Gal}(\mathsf{E}|\mathsf{F})$. Let U be any $\mathsf{E}H$-module. Let $\alpha \in \operatorname{Gal}(\mathsf{E}|\mathsf{F})$ and let α^* be the automorphism of $\mathsf{E}G$ defined by

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G}(a_g\alpha)g, \ a_g \in \mathsf{E}.$$

We define U^α as the $\mathsf{E}H$-module U^{α^*} and call it a *Galois-conjugate* of U. Let $\{u_1, ..., u_n\}$ be an E-basis of U. Then $\{(u_1, \alpha), ..., (u_n, \alpha)\}$ is an E-basis of U^α. If

$$u_i h = \sum_{j=1}^{n} a_{ij}(h)u_j \ (i = 1, 2, ..., n),$$

where $h \in H$, $a_{ij}(h) \in \mathsf{E}$, then

$$(u_i, \alpha)h = \sum_{j=1}^{n}(a_{ij}(h)\alpha)(u_j, \alpha).$$

In this sense the matrix representation of H on U^α is 'conjugate' under α to the matrix representation of H on U.

We now state the following results without proof, which are immediate from the definitions.

Lemma 2.3.1 *Let $\alpha \in \operatorname{Aut} G$ and let $\beta \in \operatorname{Gal}(\mathsf{E}|\mathsf{F})$. Let U be an $\mathsf{E}H$-module and let W be an $\mathsf{F}H$-module. Then*

(i) $(W^\alpha)\uparrow^G \cong (W\uparrow^G)^\alpha$,

(ii) $(W^\alpha)^{\mathsf{E}} \cong (W^{\mathsf{E}})^\alpha$,

(iii) $(W^{\mathsf{E}})\uparrow^G \cong (W\uparrow^G)^{\mathsf{E}}$,

(iv) $(U^\beta)\uparrow^G \cong (U\uparrow^G)^\beta$,

(v) $(U^\alpha)^\beta \cong (U^\beta)^\alpha$.

The following result also seems to be part of the folklore. Recall that the equivalence class of a representation ρ is denoted by $[\rho]$.

Theorem 2.3.2 *Let F be a field and let G be a finite group. Let ρ_1 and ρ_2 be faithful irreducible F-representations of G of degree n. Then $G\rho_1$ is conjugate to $G\rho_2$ in $GL(n,\mathsf{F})$ if and only if $[\rho_1]$ and $[\rho_2]$ belong to the same orbit of the natural action of $\operatorname{Aut} G$ on the set of equivalence classes of faithful irreducible F-representations of G.*

2.4 Existence of faithful irreducible representations

The problem of characterizing those groups which have faithful irreducible representations, was initially considered in Burnside (1911, Note F); subsequently it has been treated in several papers, for example Weisner (1939), Kochendörffer (1948), and Gaschütz (1954). The common idea involves the abelian part of the socle, that is, the product of all abelian minimal normal subgroups.

Let G be a finite group and let U be a finite $\mathbf{Z}G$-module (or simply a G-module). Let F be a field that contains all $(\exp U)$th roots of unity and whose characteristic does not divide the order of U as a finite abelian group. Set

$$U^* := \mathrm{Hom}(U, \mathsf{F}^\times)$$

where $\mathsf{F}^\times$ is the multiplicative group of nonzero elements in F. Then U^* is also a G-module by means of the following natural construction:

(i) if $\alpha, \beta \in U^*$ then define $\alpha + \beta$ by $u(\alpha + \beta) = (u\alpha)(u\beta)$ for every u in U;

(ii) if $g \in G$ and $\alpha \in U^*$ then define αg as the map such that $u \mapsto (ug^{-1})\alpha$ for every u in U.

The G-module U^* is called the *dual* of U. In fact, U^* consists of all irreducible F-representations of U as an abelian group, and hence $|U^*| = |U|$. As a G-module, U^{**} is naturally isomorphic to U. For every subgroup V of U, define $V^\perp := \{\alpha \in U^* : v\alpha = 1 \text{ for all } v \text{ in } V\}$. If V is a submodule of the G-module U, then $V^\perp$ is also a submodule of U^*. Moreover, $V^\perp$ is a submodule of U^* such that $U^*/V^\perp \cong V^*$. Indeed, the usual relations between subspaces, quotient spaces and duality of a vector space also carry over to this case.

The prototype for such a G-module in this thesis is an abelian normal subgroup A of G, regarded as a G-module with respect to conjugation action. In this case, the action of G on A^* will be written in the form of α^g for $\alpha \in A^*$ and $g \in G$.

We prove the following lemma.

Lemma 2.4.1 *Let α be an element in U^*. Then*

$$\mathrm{core}_G \ker \alpha = 1 \iff \alpha \textit{ generates } U^* \textit{ as a } G\textit{-module.}$$

Proof

$$\begin{aligned}
\mathrm{core}_G \ker \alpha = 1 &\iff \ker \alpha \text{ does not contain nonzero } G\text{-submodules of } U \\
&\iff \langle \alpha \rangle^\perp \text{ does not contain nonzero } G\text{-submodules of } U^{**} \\
&\iff \langle \alpha \rangle \text{ is not contained in a proper } G\text{-submodule of } U^* \\
&\iff \langle \alpha \rangle \text{ generates } U^* \text{ as a } G\text{-module.} \qquad \square
\end{aligned}$$

Let U be a finite semisimple $\mathbb{Z}G$-module. Then U is a direct sum of simple $\mathbb{Z}G$-modules and also U, as an abelian group, is the direct sum of the Sylow subgroups U_p. Each simple submodule of U_p may be regarded as an $\mathbb{F}_pG$-module and so U_p is a direct sum of irreducible $\mathbb{F}_pG$-modules.

By Theorem VII.4.13a in Huppert and Blackburn (1982), the multiplicity of each irreducible $\mathbb{F}_pG$-module V as a direct summand in the largest semisimple quotient of the regular module over the prime field $\mathbb{F}_p$, is the dimension of V over the finite field $\mathrm{End}_{\mathbb{F}_pG}V$. Denote the dimension by $\mathrm{Dim}V$ and call it the *absolute dimension* of V. Each U_p is generated by a single element as a G-module if and only if each U_p is a homomorphic image of the regular module $\mathbb{F}_pG$. Therefore, U_p is generated by a single element if and only if for every simple G-module V, the multiplicity of V in U_p is at most $\mathrm{Dim}V$. Moreover, if u_p generates U_p then $\Sigma_p u_p$ also generates $\bigoplus_p U_p$, while if u generates $\bigoplus_p U_p$ and $u = \Sigma_p u_p, u_p \in U_p$, then u_p generates U_p. We then have the following fact.

Lemma 2.4.2 *A finite semisimple $\mathbb{Z}G$-module U is generated by a single element if and only if for every simple $\mathbb{Z}G$-submodule V, the multiplicity of V as a direct summand in U is at most the absolute dimension* $\mathrm{Dim}V$.

The following result is a consequence of the above lemma.

Lemma 2.4.3 *A semisimple $\mathbb{Z}G$-module U is generated by a single element if and only if the dual U^* is generated by a single element.*

Proof

$$
\begin{aligned}
& U \text{ is generated by a single element} \\
\iff\ & \forall \text{ simple } V, \text{ (multiplicity of } V \text{ in } U) \leq \mathrm{Dim}V \\
\iff\ & \forall \text{ simple } V^*, \text{ (multiplicity of } V^* \text{ in } U) \leq \mathrm{Dim}V^* \\
\iff\ & \forall \text{ simple } V, \text{ (multiplicity of } V \text{ in } U^*) \leq \mathrm{Dim}V^* \\
\iff\ & \forall \text{ simple } V, \text{ (multiplicity of } V \text{ in } U^*) \leq \mathrm{Dim}V \\
\iff\ & U^* \text{ is generated by a single element.}
\end{aligned}
$$

□

The following result is an elucidation of the main theorem in Gaschütz (1954).

Theorem 2.4.4 *Let G be a finite group and A the abelian part of the socle S of G. Then G has a faithful irreducible representation over a field F if and only if the characteristic of F does not divide the order of A and A is generated by a single element as a $\mathbb{Z}G$-module with respect to the conjugation action.*

Proof It is easy to see from Theorem VII.1.16d and Theorem VII.1.18b in Huppert and Blackburn (1982) that the existence of faithful irreducible modules is unaffected by extensions of the underlying field. Thus we may assume that the field F is algebraically closed.

Suppose the characteristic of F does not divide the order of A and A is generated by a single element as a $\mathbb{Z}G$-module. By Lemma 2.4.3, A^* is also generated by a single element; let us denote it by α. It follows from Lemma 2.4.1 that $\mathrm{core}_G \ker\alpha = 1$.

Let B be the nonabelian part of the socle S of G. Then B is the product of nonabelian minimal normal subgroups of G. Since each nonabelian minimal normal subgroup is a direct product of nonabelian simple groups, $B = \prod_i B_i$ for some nonabelian simple groups B_i. Let β_i be a nontrivial irreducible F-representation of B_i for each i. Let β be the outer tensor product $\#_i \beta_i$ of the β_i; it is irreducible. Then β is a faithful F-representation of B because there are no minimal normal subgroups of B except the B_i. Then the outer tensor product $\alpha\#\beta$ is an irreducible representation of the socle S with kernel $\ker\alpha$.

Let γ be a top or bottom constituent of the induced representation $(\alpha\#\beta)\uparrow^G$. Then the Nakayama Reciprocity yields $S \cap \ker\gamma \leq \ker\alpha$ and hence we have $S \cap \ker\gamma \leq \mathrm{core}_G \ker\alpha = 1$. So $\ker\gamma$ contains no nontrivial minimal normal subgroup of G. Thus $\ker\gamma = 1$ and hence the irreducible representation γ is a faithful irreducible representation of G, as required.

Conversely, if γ is a faithful irreducible F-representation and α is an irreducible constituent of $\gamma\downarrow_A$, then $\gamma\downarrow_A$ is a direct sum of G-conjugates of α. So $\mathrm{core}_G \ker\alpha = 1$. Then by Lemma 2.4.1, the representation α generates A^* as a $\mathbb{Z}G$-module and thus A is generated by a single element by Lemma 2.4.3. $\square$

2.5 Some linear groups

Let V be an n-dimensional vector space over a field F. The group of all invertible linear transformations of V will be denoted by $GL(V)$. Each choice of a basis for V defines an isomorphism from $GL(V)$ to the group of all invertible n by n matrices over F; we denote this matrix group by $GL(n,\mathsf{F})$. If F is a finite field with p^k elements, we also use the notation $GL(n,p^k)$ for $GL(n,\mathsf{F})$. A subgroup of $GL(V)$ is called a *linear group* of degree n over F, or an F-linear group of degree n; we shall often fail to specify the underlying field or the degree when it is not necessary to do so. Let G and H be linear groups acting on the vector spaces V and W, respectively. Then we say that G and H are *linearly isomorphic* if there exist a vector space isomorphism α between V and W and a group isomorphism β between G and H such that $(vg)\alpha = (v\alpha)(g\beta)$ for all v in V and for all g in G. In any linear isomorphism between subgroups of $GL(V)$, we have $\alpha \in GL(V)$ and β is the conjugation by α.

Given a linear group G acting on V, the images of G under the isomorphisms $GL(V) \longrightarrow GL(n,\mathsf{F})$ corresponding to the various bases of V form a single conjugacy class of subgroups in $GL(n,\mathsf{F})$. Two linear groups of degree n are linearly isomorphic if and only if the conjugacy classes of subgroups of $GL(n,\mathsf{F})$ which correspond to them in this sense are the same. Conversely, $GL(n,\mathsf{F})$ may be identified with $GL(\mathsf{F}^n)$ where F^n is the Cartesian power with its usual vector space structure, and the identification is done along the isomorphism corresponding to the standard basis of that vector space. In this way we obtain a bijection between the set of linear isomorphism types of F-linear groups of degree n and the set of conjugacy classes of subgroups of $GL(n,\mathsf{F})$. This distinction between linear groups and matrix groups is rarely of any importance. For example, in referring to a general linear group we may mean either a $GL(V)$ or a $GL(n,\mathsf{F})$.

A linear group G in $GL(V)$ is called *irreducible* if V has no subspace which is setwise invariant under the action of G; equivalently, if the inclusion map from G is an irreducible representation of degree n over F.

An irreducible linear group G in $GL(V)$ is called *imprimitive* if V has a decomposition

$$V = V_1 \oplus \cdots \oplus V_r \quad (r > 1)$$

into a direct sum of nonzero subspaces which are permuted transitively by the action of G; equivalently, V is induced from a submodule of a proper subgroup of G. If an irreducible linear group G is not imprimitive, we call G *primitive.* If G is primitive then V_N is homogeneous (that is, a direct sum of pairwise isomorphic irreducible modules) for every normal subgroup N. We now collect some well known results.

Theorem 2.5.1 [Suprunenko (1963, Lemma I.7)] *Every abelian normal subgroup of a primitive linear group is cyclic.*

Regarded as a subgroup of $GL(n, p^k)$, the general linear group $GL(1, p^{kn})$ of degree 1 is an irreducible linear group of degree n. In fact, every cyclic irreducible subgroup of order $p^{kn}-1$ in $GL(n, p^k)$ is conjugate to $GL(1, p^{kn})$. The normalizers of these kinds of cyclic subgroups are determined by the following theorem.

Theorem 2.5.2 [Huppert (1967, Satz II.7.3a)] *Let Y be a cyclic irreducible subgroup of order $p^{kn}-1$ of the general linear group $GL(n, p^k)$. Let C be an irreducible subgroup of Y. Then the centralizer of C in $GL(n, p^k)$ is Y, and the normalizer of C in $GL(n, p^k)$ is the semidirect product of the cyclic group Y and a cyclic group X of order n. The action of one generator of X on Y is p^kth powering.*

Chapter 3

Metacyclic groups of odd order

The aim of this chapter is to determine the isomorphism types of metacyclic groups of odd order. The determination is not only a subject of independent interest but it also serves as a step towards enumerating metacyclic irreducible linear groups.

The first two sections are devoted to investigating some properties of metacyclic p-groups which are needed for our purpose. Section 3.3 discusses metacyclic factorizations of metacyclic groups of odd order. Section 3.4 establishes presentations of a certain form for metacyclic groups of odd order. An explicit solution of the isomorphism problem for the presentations proposed will be obtained in Section 3.5. We shall close this chapter with an application to metacyclic $\{p, q\}$-groups.

3.1 Metacyclic p-groups

We shall explore some properties of metacyclic p-groups, which will be crucial for our general discussion of metacyclic groups of odd order. The emphasis in this section (and in the next one) is on metacyclic p-groups for odd p. However, an attempt to avoid the restriction will be made if the restriction does not simplify the discussion. As a consequence of our discussion, we also have a canonical form of presentation for metacyclic p-groups for odd p.

Lemma 3.1.1 *Let P be a metacyclic p-group, p odd. If K and P/K are cyclic, then there exists a cyclic subgroup S of P such that $P = SK$ and $|S| = \exp P$.*

Proof Let $P = S_0K$ be a metacyclic factorization. Since P is regular, we observe that $\exp P = \max(|S_0|, |K|)$ from Lemma 2.2.4. Therefore, if $|K| \neq \exp P$ then $|S_0| = \exp P$. So we may assume that $|K| = \exp P$ and $|S_0| < |K|$. We may also assume that P is not cyclic. Define $S = \langle ab^{-1} \rangle$ where a, b are generators of S_0, K, respectively. Let $|K| = p^{k+1}$. Since $|S_0| < |K|$, we have $a^{p^k} = 1 \neq b^{p^k}$. The regularity of P then implies that $(ab^{-1})^{p^k} \neq 1$. It follows that $|S| = \exp P$. We know $SK = P$ since a, b are contained in SK. □

Lemma 3.1.2 *Let $P = SK$ be a metacyclic factorization of a metacyclic p-group P for any prime p. Let C be a proper subgroup of P containing K. Then every supplement of C in P is a supplement of K.*

Proof The result is obvious if P is cyclic, so we assume that P is noncyclic. By Lemma 2.2.6(ii), K is not contained in $\Phi(P)$, and $C\Phi(P)$ is a proper subgroup of P. It follows from Lemma 2.2.5(i) that $K\Phi(P) = C\Phi(P)$. Thus if X is a supplement to C in P then $XK\Phi(P) = XC\Phi(P) = P$, so $XK = P$; the result follows. □

Let P be a metacyclic p-group for odd p. For a subgroup C of P, consider the set

$$\{K : K \leq C,\ K \trianglelefteq P,\ K \text{ and } P/K \text{ cyclic }\}.$$

The subgroups of minimal order in this set will be called *C-minimal kernels.* A metacyclic factorization $P = SK$ is called *C-standard* if $|S| = \exp P$ and K is a C-minimal kernel. From Lemma 3.1.1, we observe that P has a C-standard metacyclic factorization, provided the set displayed above is nonempty.

Note that 'C-standard' in a difference sense can be defined correspondingly; that is, $P = SK$ is 'C-standard' if and only if $|S| = \exp P$ and K is a subgroup of *maximal* order in the above set.

Lemma 3.1.3 *Let $P = SK$ be a metacyclic factorization. Define $\alpha, \beta, \gamma, \delta$ by*

$$p^\alpha = |S : S\cap K|,\ p^\beta = |K : S\cap K|,\ p^\gamma = |K : P'|,\ p^\delta = |S\cap K|.$$

Then P has the presentation

$$\langle\, x, y \mid x^{p^\alpha} = y^{p^\beta},\ \ y^{p^{\beta+\delta}} = 1,\ \ y^x = y^{1+p^\gamma}\,\rangle.$$

Moreover, if $P = SK$ is C-standard for a subgroup C with index p^κ, then

(i) $\alpha \geq \beta \geq \gamma - \delta \geq 0$;

(ii) *if* $\gamma = 0$ *then* $\beta = 0$;

(iii) *if* $\beta < \gamma$ *then* $\alpha - \beta < \kappa$.

Remark The proofs of this lemma and Lemma 3.1.1 indicate that one can easily transform a given metacyclic presentation of a metacyclic p-group P with a C-standard metacyclic factorization to a presentation with the above conditions.

Proof The proof of the first claim is obvious when P is abelian, so we assume $\gamma < \beta+\delta$. Since $S/\mathrm{C}_S(K) \cong P'$ by Lemma 2.2.2 and Corollary 2.2.3, S acts on K as an automorphism group of order $p^{\beta+\delta-\gamma}$. Since $\mathrm{Aut}K$ is cyclic, it has only one subgroup of this order. On the other hand, $b \mapsto b^{1+p^\gamma}$ defines an automorphism of order $p^{\beta+\delta-\gamma}$. Therefore we can choose x in S so that $b^x = b^{1+p^\gamma}$ for all $b \in K$; then $\langle x\rangle = S$, and y can be chosen so that $x^{p^\alpha} = y^{p^\beta}$; then $\langle y\rangle = K$. Thus we have

$$x^{p^\alpha} = y^{p^\beta},\ \ y^{p^{\beta+\delta}} = 1,\ \ y^x = y^{1+p^\gamma}.$$

So P is a homomorphic image of the group presented by

$$\langle\, x, y \mid x^{p^\alpha} = y^{p^\beta},\ y^{p^{\beta+\delta}} = 1,\ y^x = y^{1+p^\gamma}\,\rangle.$$

On the other hand, the presentation gives a group of order at most $p^{\alpha+\beta+\delta}$, so P is isomorphic to the group so defined.

Suppose $P = SK$ is C-standard. It follows from $|S| = \exp P$ that $\alpha \geq \beta$. Since $P' \leq K$, we also have $\beta \geq \gamma - \delta$. Since $y^{p^\beta} = (y^{p^\beta})^x = y^{p^\beta(1+p^\gamma)}$, we

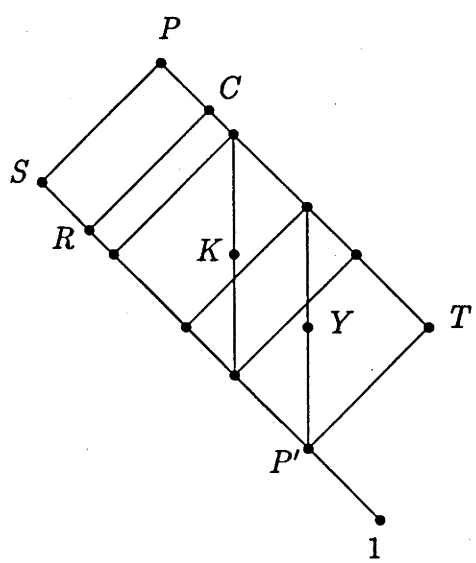
have $p^{\beta+\gamma} \equiv 0 \bmod p^{\beta+\delta}$, so $\gamma \geq \delta$; this completes the proof of (i). To prove (ii), assume $\beta \geq 1$. Then P is not cyclic. The Frattini subgroup $\Phi(P)$ contains the commutator subgroup P', but by Lemma 2.2.6(ii) it does not contain K, so we have that P' is a proper subgroup of K and hence $\gamma \geq 1$.

To prove (iii), suppose that $\alpha - \beta \geq \kappa$ when $\beta < \gamma$. The proof will be done by producing a contradiction. Set $R := S \cap C$; the condition $\beta < \gamma$ implies that P' is contained in S, thus also in R. The condition $\alpha - \beta \geq \kappa$ implies that $|R/P'| \geq |K/P'|$. Since $RK = C$ and C/P' is finite abelian, we have $\exp(C/P') = |R/P'|$. By Lemma 2.1.4, there exists a subgroup T such that $TR = C$ and $T \cap R = P'$. Both T/P' and R/P' are cyclic and $|T| < |K|$.

Suppose T is not cyclic. Let ϕ be an isomorphism from T/P' to some subgroup, S_ϕ say, of R/P': in fact, $|T/P'| < |R/P'|$, so there exists always such an isomorphism. In this case, define

$$Y = \{ts : (tP')\phi = sP',\ s \in S_\phi, t \in T\}.$$

(A relevant figure is shown below.)



Then from Theorem 2.1.5, Y is a subgroup such that $R \cap Y = T \cap Y = P'$. Since $P'\Omega_1(P) \leq T$ [see Lemma 2.2.6(i)], this implies that Y does not contain $\Omega_1(P)$ and hence Y is cyclic. In fact Y is normal in P because $Y \geq P'$. By

Theorem 2.1.5 again, $|Y| = |T|$, hence $|Y| < |K|$. It also follows that $P = SY$ and hence Y is a cyclic normal subgroup of P such that P/Y is cyclic. It is obvious that $Y \leq C$.

If T is cyclic, define $Y := T$. Then $|Y| < |K|$ also holds in this case. So in any case, there exists a cyclic normal subgroup Y such that P/Y is cyclic, $Y \leq C$ and $|Y| < |K|$. This contradicts the C-minimality of K. Consequently, if $\beta < \gamma$ then $\alpha - \beta < \kappa$, which completes the proof of (iii). □

Now we are ready to prove a classification theorem of metacyclic p-groups.

Theorem 3.1.4 *For odd p, every metacyclic p-group P has a presentation of the form*

$$P = \langle\, a, b \mid a^{p^\alpha} = b^{p^\beta},\ b^{p^{\beta+\delta}} = 1,\ b^a = b^{1+p^\gamma} \,\rangle$$

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $\alpha \geq \beta \geq \gamma \geq \delta$ and either $\gamma \geq 1$ or $\beta = \gamma = \delta = 0$. Conversely, each such presentation defines a metacyclic p-group of order $p^{\alpha+\beta+\delta}$, different values of the parameters $\alpha, \beta, \gamma, \delta$ (with the above condition) giving nonisomorphic groups.

Remark The group P is cyclic if and only if $\beta = \gamma = \delta = 0$. (For the cyclic case, this presentation is of course highly redundant but having a uniform treatment of cyclic and noncyclic groups here will be essential later when we deal with metacyclic groups whose orders are not prime powers.) The above result for noncyclic metacyclic p-groups can be translated from the result of Newman and Xu (1988) and vice versa; P is split if and only if $\alpha = \beta$, or $\beta = \gamma$, or $\delta = 0$.

Proof Choose a metacyclic factorization $P = SK$ so that S is of order $\exp P$ and K is of least possible order; Lemma 3.1.1 guarantees that this can be done. Lemma 3.1.3 with $C = P$ and $\kappa = 0$ yields the first sentence. Further, we observe $P/P' \cong \mathsf{C}(p^\alpha) \times \mathsf{C}(p^\gamma)$ and $\exp P = p^{\alpha+\delta}$, while $|P| = p^{\alpha+\beta+\delta}$. It follows that α, β, γ and δ are invariants of P, so the second sentence follows. □

We here derive a certain property which will turn out to be of great importance for our goal in the general case.

Lemma 3.1.5 *Let $P = SK$ be a metacyclic factorization of a metacyclic p-group P for any prime p. Suppose C is a subgroup of P containing K. Then*

(i) *if P is abelian, then* $\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C} = \mathrm{Aut}(P/C)$;

(ii) *in any case,* $\mathsf{N}_{\mathrm{Aut}P}(C) = [\mathsf{N}_{\mathrm{Aut}P}(S) \cap \mathsf{N}_{\mathrm{Aut}P}(C)]\mathsf{C}_{\mathrm{Aut}P}(P/C)$.

Proof Since P/C is cyclic, each automorphism of it is of the form $x \mapsto x^s$ for some integer s with $\gcd(p, s) = 1$. If P is abelian, $x \mapsto x^s$ also defines an automorphism of P, which normalizes every subgroup, and hence

$$\mathrm{Aut}(P/C) = \mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C} = [\mathsf{N}_{\mathrm{Aut}P}(S) \cap \mathsf{N}_{\mathrm{Aut}P}(C)]\downarrow_{P/C}.$$

The first result has now been proved; when P is abelian, the second claim also follows from the above observation.

Next we assume that P is not abelian. The result is obvious when $C = P$, so we assume that C is a proper subgroup of P. Since the other direction of inclusion is obvious, it remains only to demonstrate that

$$\mathsf{N}_{\mathrm{Aut}P}(C) \leq [\mathsf{N}_{\mathrm{Aut}P}(S) \cap \mathsf{N}_{\mathrm{Aut}P}(C)]\mathsf{C}_{\mathrm{Aut}P}(P/C).$$

Suppose σ is an automorphism in $\mathsf{N}_{\mathrm{Aut}P}(C)$. Then $S^\sigma K^\sigma$ is another metacyclic factorization of P with $K^\sigma \leq C$. So $S^\sigma K = P$ by Lemma 3.1.2. Let x be a fixed generator of S. Then there exists an integer m such that $b^x = b^m$ for all b in K. We can also choose a generator y for K so that $x^{|S:S\cap K|} = y^{|K:S\cap K|}$. Then P has a presentation on these generators x, y with the defining relations

$$x^{|S:S\cap K|} = y^{|K:S\cap K|},\ y^{|K|} = 1,\ y^x = y^m.$$

Let $\bar{x}$ be the element in S^σ such that $x = \bar{x}b$ for some b in K. Then $xC = \bar{x}C$. Since $\langle\bar{x}\rangle$ is a supplement of K, Dedekind's Law then yields that $\bar{x}$ generates S^σ. We can choose a generator $\bar{y}$ of K so that $\bar{x}^{|S^\sigma:S^\sigma\cap K|} = \bar{y}^{|K:S^\sigma\cap K|}$. Because $|S\cap K| = |S^\sigma\cap K|$, we have $\bar{x}^{|S:S\cap K|} = \bar{y}^{|K:S\cap K|}$. It is obvious that $\bar{y}^{\bar{x}} = \bar{y}^m$. So we have a presentation for P obtained from the previous one

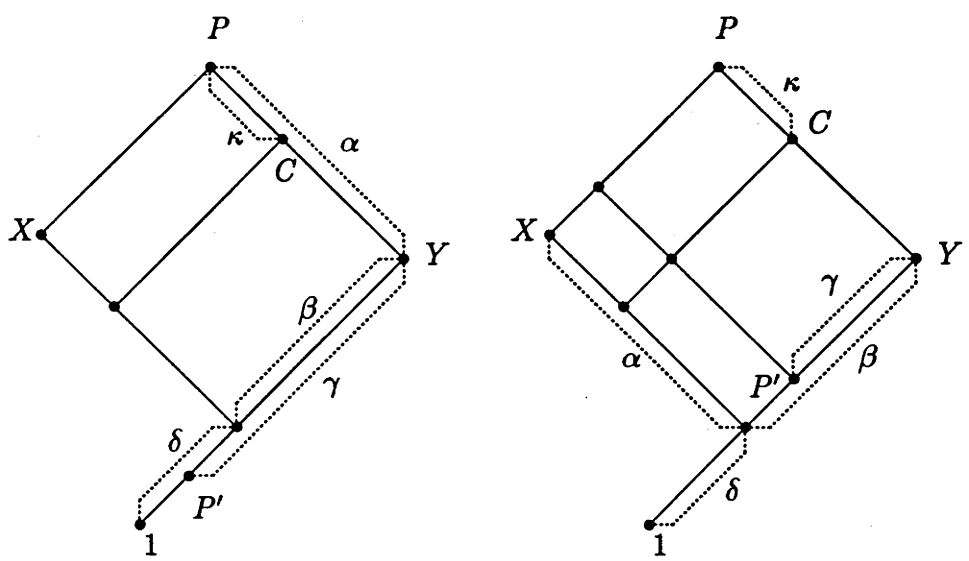
simply by replacing x with $\bar{x}$ and y with $\bar{y}$. The map $\bar{x} \mapsto x$, $\bar{y} \mapsto y$ yields an automorphism of P: call it τ. Then $S^{\sigma\tau} = S$. We know that C and C^τ are subgroups of the same order containing K; since P/K is cyclic, $C/K = C^\tau/K$, so $C = C^\tau$. Thus $\sigma\tau \in \mathsf{N}_{\mathrm{Aut}P}(S) \cap \mathsf{N}_{\mathrm{Aut}P}(C)$. On the other hand, $\tau \in \mathsf{C}_{\mathrm{Aut}P}(P/C)$ since $x\tau^{-1}C = \bar{x}C = xC$. Therefore $\sigma = (\sigma\tau)\tau^{-1} \in [\mathsf{N}_{\mathrm{Aut}P}(S) \cap \mathsf{N}_{\mathrm{Aut}P}(C)]\mathsf{C}_{\mathrm{Aut}P}(P/C)$. □

3.2 Some groups of automorphisms

Throughout this section, let P be a given metacyclic p-group for odd p and let $P = XY$ be a fixed C-standard metacyclic factorization of P for a subgroup C of P. Define $\alpha, \beta, \gamma, \delta$ and κ by

$$p^\alpha = |X : X \cap Y|,\ p^\beta = |Y : X \cap Y|,\ p^\gamma = |Y : P'|,\ p^\delta = |X \cap Y|,\ p^\kappa = |P : C|.$$

In what follows, the reader may find the following figures helpful.



$\beta \leq \gamma$ $\qquad$ $\beta > \gamma$

This section will be devoted to the determination of $\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}$; it is sufficient to know the order since the group is the unique subgroup of that order of the cyclic group $\mathrm{Aut}(P/C)$. We shall find this group needed in our study of the isomorphism problem for our special presentations of metacyclic groups of

odd order. All results in this section are also true, without additional work, for 'maximal' choices of Y.

If $\kappa = 0$ (equivalently, $C = P$), then the order is 1 since $\mathrm{Aut}(P/C) = 1$. If P is abelian (equivalently, $\beta + \delta = \gamma$), then from Lemma 3.1.5(i) we know that $\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C} = \mathrm{Aut}(P/C)$, so the order is $(p-1)p^{\kappa-1}$ provided $\kappa > 0$. So we may assume that $\kappa > 0$ and P is not abelian (or equivalently $\beta + \delta > \gamma$). We proceed with some notation:

$$\mathcal{K} := \{K : P = XK \text{ is a } C\text{-standard metacyclic factorization}\}.$$

For every K in $\mathcal{K}$, define

$$A(K) := \{a \in X : b^a = b^{1+p^\gamma} \text{ for all } b \in K\}.$$

Then $A(K)$ is a coset of $\mathsf{C}_X(P)$ in X and each subgroup generated by an element of $A(K)$ is a supplement of $\mathsf{C}_P(K)$ in P, hence by Lemma 3.1.2 also a supplement of K in P. It follows from Dedekind's Law that each element of $A(K)$ generates X. We now define some notation as follows:

$$\begin{aligned}
&A := \textstyle\bigcup_{K\in\mathcal{K}} A(K)\\
&\mathcal{L} := \{K \in \mathcal{K} : A(K) = A(Y)\}\\
&N := \mathsf{N}_{\mathrm{Aut}P}(X) \cap \mathsf{N}_{\mathrm{Aut}P}(C)\\
&U := X/\mathsf{C}_X(P), \quad V := X/(X\cap C)\\
&W := \begin{cases} \mathsf{C}_X(P)/(X\cap C) \text{ if } \mathsf{C}_X(P) \geq X \cap C\\ (X\cap C)/\mathsf{C}_X(P) \text{ if } \mathsf{C}_X(P) < X \cap C. \end{cases}
\end{aligned}$$

Consider the natural action of N on the set A. For all $a \in A(K)$ and for all $\rho \in N$, we know $a\rho \in A(K\rho) \subseteq A$. Therefore N acts on A in a natural way. We shall then show that the action is transitive. Let $x \in A(Y)$ and choose y in Y so that $x^{p^\alpha} = y^{p^\beta}$; then x, y are generators of X and Y, respectively, which satisfy the defining relations in Lemma 3.1.3. Let K be a member of $\mathcal{K}$. Since K is a cyclic group of order $|Y|$, we have $X \cap K = X \cap Y$. Thus for a given a in $A(K)$, we can select b in K so that $a^{p^\alpha} = b^{p^\beta}$; then a and b are generators of X and

K, respectively, which also satisfy the defining relations. Thus the map $x \mapsto a$, $y \mapsto b$ defines an automorphism ϱ in $\mathrm{Aut}P$ that normalizes X and maps Y to K. Then $C\varrho = (X \cap C)\varrho Y\varrho = (X \cap C)K = C$, that is, ϱ normalizes C, and so we are done.

The natural action of N on A induces a transitive action on the set of $\{A(K) : K \in \mathcal{K}\}$. When $\mathrm{C}_X(P) \geq X \cap C$, the action also induces a transitive action on the set of those cosets of $X \cap C$ which are included in A. Since each a in A generates X, an automorphism ρ in N stabilizes $A(K)$ if and only if $\rho{\downarrow_U} = 1$, so $N{\downarrow_U}$ acts regularly on $\{A(K) : K \in \mathcal{K}\}$. Similarly when $\mathrm{C}_X(P) \geq X \cap C$, the group $N{\downarrow_V}$ acts regularly on the set of parts in the partition of A into cosets of $X \cap C$.

Now we are in the position to determine the order of $\mathrm{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}}$. First we know from Lemma 3.1.5(ii) that $\mathrm{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}} = N{\downarrow_{P/C}}$. The natural isomorphism of $X/(X \cap C)$ onto P/C induces an isomorphism $N{\downarrow_V}$ onto $N{\downarrow_{P/C}}$. This implies that $\mathrm{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}} \cong N{\downarrow_V}$. In order to determine the order of $\mathrm{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}}$, we only need to investigate that of $N{\downarrow_V}$.

To determine the order of $N{\downarrow_V}$, we first suppose $\mathrm{C}_X(P) \geq X \cap C$. Then each $A(K)$ is partitioned into exactly $|W|$ different cosets of $X \cap C$. We have already observed that $N{\downarrow_V}$ acts regularly on the set of parts in the partition of A into cosets of $X \cap C$. This yields $|N{\downarrow_V}| = (|\mathcal{K}|/|\mathcal{L}|)|W|$.

We next consider the other case, when $\mathrm{C}_X(P) < X \cap C$ holds. In this case there exists a homomorphism of $N{\downarrow_U}$ onto $N{\downarrow_V}$, which is induced by the natural homomorphism of U onto V; the kernel is $\mathrm{C}_{N{\downarrow_U}}(V)$, of course. We observe that $\mathrm{C}_{N{\downarrow_U}}(V) = N{\downarrow_U} \cap \mathrm{C}_{\mathrm{Aut}U}(V)$ and $|\mathrm{C}_{\mathrm{Aut}U}(V)| = |\mathrm{C}_{\mathrm{Aut}U}(U/W)| = |W|$ unless $W = U$, for the map $\sigma \mapsto u^{-1}(u\sigma)$ defines a bijection between the two cyclic groups where $\sigma \in \mathrm{C}_{\mathrm{Aut}U}(U/W)$ and u is a fixed generator of U. So we see that

$$|\mathrm{C}_{N{\downarrow_U}}(V)| = \gcd(|N{\downarrow_U}|, |W|).$$

Since $N{\downarrow_U}$ acts regularly on that set $\{A(K) : K \in \mathcal{K}\}$, it follows that

$$|N{\downarrow_U}| = |\mathcal{K}|/|\mathcal{L}|$$

and hence $|N{\downarrow_V}| = |N{\downarrow_U}|/|\mathrm{C}_{N{\downarrow_U}}(V)| = (|\mathcal{K}|/|\mathcal{L}|)/\gcd(|\mathcal{K}|/|\mathcal{L}|, |W|)$.

Note that $|X : X \cap C| = p^{\kappa}$ and $|X : \mathrm{C}_X(P)| = p^{\beta-\gamma+\delta}$. We now summarize the above conclusions of this argument as follows.

Theorem 3.2.1 *If $\kappa > 0$ and $\beta + \delta > \gamma$, then*

$$|\mathsf{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}}| = \begin{cases} m/\gcd(m, p^{\beta-\gamma+\delta-\kappa}) & \text{if } \beta-\kappa > \gamma-\delta, \\ mp^{\kappa-\beta+\gamma-\delta} & \text{otherwise} \end{cases}$$

where $m = |\mathcal{K}|/|\mathcal{L}|$.

The remainder of this section will be devoted to the explicit determination of the order of $\mathsf{N}_{\mathrm{Aut}P}(C){\downarrow_{P/C}}$. It will be done by calculating $|\mathcal{K}|$ and $|\mathcal{L}|$.

Assume that P is not abelian. Let x be a fixed element in $A(Y)$ and let y be a fixed element of Y such that $x^{p^{\alpha}} = y^{p^{\beta}}$. We then know that x and y are generators of X and Y, respectively. Define $D := XP' \cap Y$ and $E := XP' \cap C$. Then $D = (X \cap Y)P'$, $EY = C$ and $E \cap Y = D$ by Dedekind's Law. Thus $Y/D \cong \mathsf{C}(\min(p^{\beta}, p^{\gamma}))$ and $E/D \cong \mathsf{C}(p^{\alpha-\kappa})$. We shall next deduce that $K \in \mathcal{K}$ if and only if K is a cyclic subgroup of C containing D and K/D is a direct complement of E/D in C/D. Suppose $P = XK$ is a C-standard metacyclic factorization. Then K is a cyclic group of order $|Y|$, so $X \cap K = X \cap Y$. Thus $D = (X \cap Y)P' = (X \cap K)P' = XP' \cap K = E \cap K$. Applying Dedekind's Law again, we also have $EK = (XP' \cap C)K = C$. So K/D is a direct complement of E/D in C/D. Conversely let K be a cyclic subgroup containing D such that K/D is a direct complement of E/D in C/D. Then $K \geq P'$ and hence K is normal in P. Since $E \leq XK$, we have $XK = XKE = XC = P$. It follows from $E \cap K = D = E \cap Y$ that $C/K \cong C/Y$, that is $|K| = |Y|$. So $K \in \mathcal{K}$ and the deduction is now complete. The conclusion may also be put as follows. Set

$$\mathcal{K}^* = \{K : K/D \text{ is a direct complement of } E/D \text{ in } C/D\};$$

then $\mathcal{K} = \{K \in \mathcal{K}^* : K \text{ is cyclic}\}$.

There exists a one-to-one correspondence between $\mathcal{K}^*$ and $\mathrm{Hom}(Y/D, E/D)$ [see Robinson (1982, 11.1.2) or Bechtell (1991, Corollary 2.4)]. The correspondence is in fact given by

$$\phi \longmapsto \{ba : (bD)\phi = aD,\ b \in Y\}$$

for any homomorphism ϕ in $\mathrm{Hom}(Y/D, E/D)$. The group corresponding to ϕ in $\mathrm{Hom}(Y/D, E/D)$ will be denoted by K_ϕ. In fact, K_ϕ is the diagonal defined by the isomorphism induced by ϕ [see Theorem 2.1.5]. Since Y/D and E/D are cyclic, $|\mathrm{Hom}(Y/D, E/D)| = \min(|Y/D|, |E/D|)$. As $|Y/D| = \min(p^\beta, p^\gamma)$ while $|E/D| = p^{\alpha-\kappa}$, the order is equal to $\min(p^{\alpha-\kappa}, p^\beta, p^\gamma)$. We set

$$\alpha^* := \max(\kappa,\ \alpha-\beta,\ \alpha-\gamma).$$

Let ϕ be a homomorphism in $\mathrm{Hom}(Y/D, E/D)$. Then ϕ is defined by the map $yD \mapsto x^{sp^{\alpha^*}}D$ for some unique integer s such that $0 \le s < p^{\alpha-\alpha^*}$. We may abbreviate K_ϕ to K_s; thus $\mathcal{K}^* = \{K_s : 0 \le s < p^{\alpha-\alpha^*}\}$. The remaining issue is to decide how many of the K_s are cyclic.

Let D^* be the unique subgroup of Y of index $p^{\alpha-\alpha^*}$. Then

$$D^* = X \cap Y \iff \alpha - \alpha^* = \beta \iff \alpha - \kappa \ge \beta \le \gamma.$$

Our discussion now divides into the following two cases, which depend whether $D^* = X \cap Y$ or not.

Case I: $\alpha - \kappa \ge \beta \le \gamma$ (equivalently, $D^* = X \cap Y$).
In this case, $D^* = D = X \cap Y$ and $\Omega^+ := D\Omega_1(P)$ is a diagonal defined by an isomorphism ψ of $\Omega_1(Y/D)$ onto $\Omega_1(E/D)$ [see Theorem 2.1.5]. (The case is pictured below.)

It follows that K_ϕ is cyclic if and only if K_ϕ does not contain Ω^+ if and only if $\phi{\downarrow}_{\Omega_1(Y/D)}$ is not equal to ψ. If

$$\phi_0 \in \{\phi \in \mathrm{Hom}[\mathsf{C}(p^\beta), \mathsf{C}(p^\beta)] :\ \phi{\downarrow}_{\mathsf{C}(p)} = \psi\},$$

then

$$\begin{aligned} & \{\phi \in \mathrm{Hom}[\mathsf{C}(p^\beta), \mathsf{C}(p^\beta)] : \ \phi{\downarrow}_{\mathsf{C}(p)} = \psi\} \\ = \ & \{\phi_0 + \phi : \ \phi \in \mathrm{Hom}[\mathsf{C}(p^\beta), \mathsf{C}(p^\beta)], \ \ker\phi \geq \mathsf{C}(p)\}, \end{aligned}$$

and hence there is a one-to-one correspondence between

$$\{\phi \in \mathrm{Hom}[\mathsf{C}(p^\beta), \mathsf{C}(p^\beta)] : \ \phi{\downarrow}_{\mathsf{C}(p)} = \psi\} \text{ and } \mathrm{Hom}[\mathsf{C}(p^\beta)/\mathsf{C}(p), \mathsf{C}(p^\beta)].$$

Therefore,

$$|\mathcal{K}| = |\mathrm{Hom}[\mathsf{C}(p^\beta), \mathsf{C}(p^\beta)]| - |\mathrm{Hom}[\mathsf{C}(p^{\beta-1}), \mathsf{C}(p^\beta)]|.$$

Consequently, $|\mathcal{K}| = (p-1)p^{\beta-1}$ if $\alpha - \kappa \geq \beta \leq \gamma$.

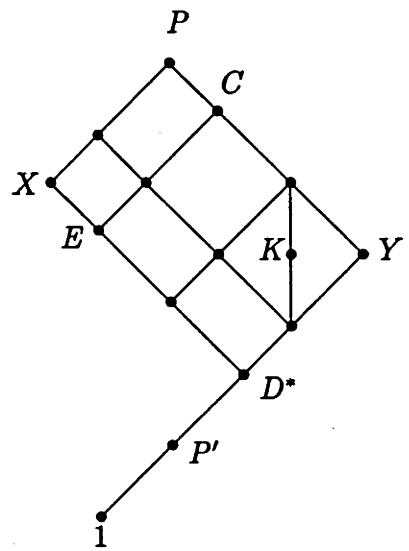


Figure for Case I.

Case II: either $\alpha - \kappa < \beta$ or $\beta > \gamma$ (equivalently, $D^* > X \cap Y$).

In this case, $X \cap Y$ is a proper subgroup of D^*. Since $X^* := XD^*$ is not cyclic, X^* contains $\Omega_1(P)$. On the other hand, $X^* \cap K = (X \cap K)D^* = D^*$ for every $K \in \mathcal{K}^*$, so K does not contains $\Omega_1(P)$. It follows that K is cyclic for all $K \in \mathcal{K}^*$. Hence

$$\mathcal{K}^* = \mathcal{K}.$$

Therefore $|\mathcal{K}| = p^{\alpha - \alpha^*}$.

The following figure illustrates the case.

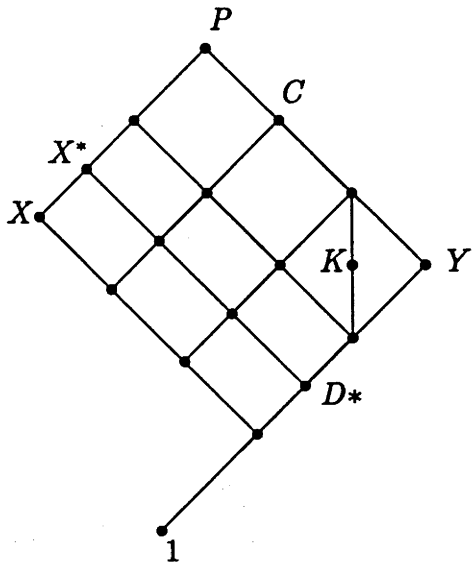


Figure for Case II.

The following result has now been completely established.

Lemma 3.2.2 *If $\beta + \delta > \gamma$ then*

$$|\mathcal{K}| = \begin{cases} (p-1)p^{\beta-1} & \text{if } \alpha - \kappa \geq \beta \leq \gamma \\ \min(p^{\alpha-\kappa},\ p^{\gamma}) & \text{otherwise.} \end{cases}$$

We prove the following lemmas.

Lemma 3.2.3 *If $\beta + \delta > \gamma$ then*

(i) *if $\alpha - \kappa \geq \beta \leq \gamma$ then*

$$\mathcal{K} = \{\langle x^{sp^{\alpha-\beta}} y\rangle : 0 \leq s < p^{\beta}, (s+1, p) = 1\};$$

(ii) *otherwise,*

$$\mathcal{K} = \{\langle x^{sp^{\alpha^*}} y\rangle : 0 \leq s < p^{\alpha-\alpha^*}\}$$

where $\alpha^* = \max(\kappa, \alpha-\beta, \alpha-\gamma)$.

Proof From the definition of the parameters and Lemma 2.2.4, we first observe that

$$(x^{sp^{\alpha^*}} y)^{p^{\beta+\delta-1}} = 1 \iff x^{sp^{\alpha^*+\beta+\delta-1}} = y^{-p^{\beta+\delta-1}} \iff \begin{cases} \delta > 0, \\ 1+sp^{\alpha^*+\beta-\alpha} \equiv 0 \bmod p. \end{cases}$$

It is obvious that $x^{sp^{\alpha^*}}y \in K_s$. So K_s is cyclic if s is not a solution of $1 + sp^{\alpha^*+\beta-\alpha} \equiv 0 \bmod p$; in this case, $K_s = \langle x^{sp^{\alpha^*}}y\rangle$.

If $\alpha - \kappa \geq \beta \leq \gamma$ then $\delta > 0$ since $\beta + \delta > \gamma$; in this case, $\alpha^* = \alpha - \beta$ and hence the solutions are $s \equiv -1 \bmod p$. In the other case, $\alpha^* > \alpha - \beta$. So there is no solution of $1 + sp^{\alpha^*+\beta-\alpha} \equiv 0 \bmod p$ unless $\alpha - \kappa \geq \beta \leq \gamma$. By Lemma 3.2.2, there are precisely $|\mathcal{K}|$ choices of s which are not solutions of the congruence and this completes the proof. □

Lemma 3.2.4 *If $\beta + \delta > \gamma$ then*

$$A(Y) = A(K_s) \iff sp^{\gamma-\delta} \equiv 0 \mod p^{\alpha-\alpha^*}$$

where $\alpha^* = \max(\kappa, \alpha-\beta, \alpha-\gamma)$.

Proof Let

$$B := (1+p^\gamma)^{sp^{\alpha^*}}, \quad B(p^\gamma) := B^{p^\gamma-1} + \cdots + B + 1.$$

Since $\alpha^* + 2\gamma \geq \beta + \delta$, by Lemma 2.1.1 $B^{p^\gamma} \equiv 1 \mod p^{\beta+\delta}$, and hence $B(p^\gamma) \equiv p^\gamma \mod p^{\beta+\delta}$. Then we observe

$$\begin{aligned} A(Y) = A(K_s) &\iff (x^{sp^{\alpha^*}}y)^x = (x^{sp^{\alpha^*}}y)^{1+p^\gamma} \\ &\iff x^{sp^{\alpha^*}}y^{1+p^\gamma} = x^{(1+p^\gamma)sp^{\alpha^*}}y^{B^{p^\gamma}+B(p^\gamma)} \\ &\iff x^{sp^{\alpha^*+\gamma}} = 1 \\ &\iff sp^{\alpha^*+\gamma} \equiv 0 \bmod p^{\alpha+\delta} \\ &\iff sp^{\gamma-\delta} \equiv 0 \bmod p^{\alpha-\alpha^*}. \end{aligned}$$

□

Applying Lemma 2.1.2 and Lemma 3.2.3 and the above lemma, we have an immediate consequence.

Lemma 3.2.5 *If $\beta + \delta > \gamma$ then*

$$|\mathcal{L}| = \min(p^{\gamma-\delta}, p^{\alpha-\kappa}).$$

We now conclude this section by summarizing the determination of the order of $\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}$. When $\kappa = 0$ the order is obviously 1. Recall that the order is $(p-1)p^{\kappa-1}$ when $\kappa > 0$ and $\beta + \delta = \gamma$. We prove the following result.

Corollary 3.2.6 *Let ω be the second term of the sequence obtained by arranging $\alpha - \kappa$, $\beta - \kappa$, γ, $\gamma - \delta$ in nonincreasing order. If $\kappa > 0$ then*

$$|\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}| = \begin{cases} (p-1)p^{\kappa-1} & \text{if } \beta \leq \omega \\ p^{\kappa-\beta+\omega} & \text{otherwise.} \end{cases}$$

Proof We first show that

$$(\text{either } \beta + \delta = \gamma \text{ or } \alpha - \kappa \geq \beta \leq \gamma) \iff \beta \leq \omega.$$

If $\alpha - \kappa \geq \beta \leq \gamma$, then $\omega \geq \beta$. Since $\omega \geq \gamma - \delta$, we also have $\omega \geq \beta$ whenever $\beta + \delta = \gamma$. To show the converse statement, suppose $\beta \leq \omega$. Then either $\omega = \alpha - \kappa$, or $\omega = \gamma$, or $\omega = \gamma - \delta$. If $\omega = \alpha - \kappa$, then $\beta \leq \omega = \alpha - \kappa \leq \gamma$. If $\omega = \gamma$, then $\beta \leq \omega = \gamma \leq \alpha - \kappa$. Since $\gamma - \delta \leq \beta$, if $\omega = \gamma - \delta$, then $\beta \leq \omega = \gamma - \delta \leq \beta$, so $\beta + \delta = \gamma$. Consequently, if $\beta \leq \omega$ then either $\beta + \delta = \gamma$ or $\alpha - \kappa \geq \beta \leq \gamma$.

Now we divide the proof into two cases:

(i) $\beta \leq \omega$: In this case either $\beta + \delta = \gamma$ or $\alpha - \kappa \geq \beta \leq \gamma$. When $\beta + \delta = \gamma$, the result follows from Lemma 3.1.5(i). We assume $\beta + \delta > \gamma$. Then $|\mathcal{K}| = (p-1)p^{\beta-1}$ by Lemma 3.2.2. Since $\alpha - \kappa \geq \beta > \gamma - \delta$, we have $|\mathcal{K}|/|\mathcal{L}| = (p-1)p^{\beta-\gamma+\delta-1}$ using Lemma 3.2.5, Using the formulae of Theorem 3.2.1, we easily obtain $|\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}| = (p-1)p^{\kappa-1}$.

(ii) $\beta > \omega$: In this case $\beta + \delta > \gamma$ and either $\alpha - \kappa < \beta$ or $\beta > \gamma$. Thus $|\mathcal{K}| = \min(p^{\alpha-\kappa}, p^{\gamma})$, $|\mathcal{L}| = \min(p^{\alpha-\kappa}, p^{\gamma-\delta})$. We divide this case into six subcases:

(1) $\alpha - \kappa \geq \beta - \kappa \geq \gamma \geq \gamma - \delta$, so $\omega = \beta - \kappa$,

(2) $\alpha - \kappa \geq \gamma \geq \beta - \kappa > \gamma - \delta$, so $\omega = \gamma$,

(3) $\alpha - \kappa \geq \gamma \geq \gamma - \delta \geq \beta - \kappa$, so $\omega = \gamma$,

(4) $\gamma \geq \gamma - \delta \geq \alpha - \kappa \geq \beta - \kappa$, so $\omega = \gamma - \delta$,

(5) $\gamma \geq \alpha - \kappa \geq \gamma - \delta \geq \beta - \kappa$, so $\omega = \alpha - \kappa$,

(6) $\gamma \geq \alpha - \kappa \geq \beta - \kappa > \gamma - \delta$, so $\omega = \alpha - \kappa$.

In each subcase, routine calculations yield $|\mathrm{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}| = p^{\kappa-\beta+\omega}$. □

3.3 Metacyclic factorizations

In this section, we describe some properties of metacyclic groups to obtain a canonical form of metacyclic factorizations. We start with a basic lemma; we omit the easy proof.

Lemma 3.3.1 *Let $G = H \ltimes N$ be a finite group with $(|H|, |N|) = 1$. If $H = XY$ and $N = UV$ are metacyclic factorizations such that $X \leq \mathrm{N}_H(V)$, $Y \leq \mathrm{C}_H(N)$ and $U \leq \mathrm{C}_N(H)$, then $G = (XU)(YV)$ is a metacyclic factorization of G.*

It will be used repeatedly and without reference that if $G = SK$ is a metacyclic factorization then every subgroup of K is normal in G (for K is cyclic and in a cyclic group every subgroup is characteristic). We now have some basic results on metacyclic factorizations. The following lemma is a generalized version of Lemma 3.1.1 for nilpotent metacyclic groups of odd order; we omit the obvious proof.

Lemma 3.3.2 *Let H be a nilpotent metacyclic group of odd order. If Y is a cyclic normal subgroup of H such that H/Y is also cyclic, then there exists a cyclic supplement X of Y in H such that $|X| = \exp H$.*

We prove the following fundamental result.

Lemma 3.3.3 *Let q be a prime, G a metacyclic group with a Sylow q-subgroup Q and H a q'-subgroup of G. Let $G = SK$ be a metacyclic factorization such that $H = (S \cap H)(K \cap H)$ and $Q = (S \cap Q)(K \cap Q)$. If H normalizes Q, then either*

$$[H,\ Q] = 1$$

or

$$K \cap H \leq \mathrm{C}_H(Q), \quad S \cap Q = \mathrm{C}_Q(H), \quad K \cap Q = [H,\ Q], \quad (S \cap Q) \cap (K \cap Q) = 1.$$

Proof Let $X = S \cap H$, $Y = K \cap H$, $U = S \cap Q$ and $V = K \cap Q$. It follows from the hypothesis that $H = XY$ and $Q = UV$ are metacyclic factorizations of H and Q, respectively. Since Y is a normal q'-subgroup of G which normalizes Q, we have $Y \leq \mathrm{C}_H(Q)$. Therefore, $U \leq \mathrm{C}_Q(H)$ and $[H, Q] = [X, V]$. Suppose $[H, Q]$ is nontrivial. Then the q'-group X acts nontrivially on the cyclic and therefore directly indecomposable q-group V. On the other hand, $V = \mathrm{C}_V(X) \times [X, V]$ [see Gorenstein (1968, Theorem 5.2.3)]; so $\mathrm{C}_V(X) = 1$ and $V = [H, Q]$. We then have $V \cap \mathrm{C}_Q(H) = 1$, so $U \cap V = 1$. Since $Q = UV$ and $U \leq \mathrm{C}_Q(H)$, Dedekind's Law yields that $U = \mathrm{C}_Q(H)$. □

Let G be a group with a metacyclic factorization $G = SK$. For any set π of prime numbers, we denote the Hall π-subgroup of a cyclic group C by C_π. Then we have the following lemma.

Lemma 3.3.4 *To each set π of prime divisors of the order of G, the subgroup $H = S_\pi K_\pi$ is the unique Hall π-subgroup of G such that $S_\pi = S \cap H$ and $K_\pi = K \cap H$, so $H = (S \cap H)(K \cap H)$.*

Proof Since K_π is normal in G, it follows that $G = S_\pi K_\pi S_{\pi'} K_{\pi'}$. Since $S_\pi K_\pi \cap S_{\pi'} K_{\pi'} = 1$, we have $|G| = |S_\pi K_\pi||S_{\pi'} K_{\pi'}|$. Therefore $H = S_\pi K_\pi$ is a Hall π-subgroup of G. Dedekind's Law yields that $S \cap H = S_\pi$ and $K \cap H = K_\pi$; thus the proof is now complete. □

Throughout the remainder of this section, we keep the following notation.

Notation 3.3.5

(i) *G denotes a metacyclic group with a metacyclic factorization $G = SK$.*

(ii) *π denotes the set $\{p \in \pi(G) : G$ has a normal Hall p'-subgroup$\}$.*

(iii) *H denotes the Hall π-subgroup $S_\pi K_\pi$.*

(iv) *N denotes the intersection of all Hall p'-subgroups for $p \in \pi$.*

Then N is the normal Hall π'-subgroup of G [see Robinson (1982, 9.2.1) or Suzuki (1986, (4.5.8))]. Since $S_{\pi'}K_{\pi'}$ is a Hall π'-subgroup of G, we have $N = S_{\pi'}K_{\pi'}$, so $N = (S \cap N)(K \cap N)$. We also know that $H \cong G/N$ is nilpotent. Of course $H = (S \cap H)(K \cap H)$. We have a semidirect decomposition $G = HN$ with Hall subgroups as semidirect factors.

Definition 3.3.6 The decomposition $G = HN$ is called the *standard Hall-decomposition* for the metacyclic factorization $G = SK$.

Keeping the above notation fixed, we also define some notation. For any q in π', define $\hat{q} := \{p \in \pi' : p < q\}$; for any subset ϖ of π', define $N_\varpi := S_\varpi K_\varpi$. Then we have the following.

Lemma 3.3.7 *Keeping the above notation, we have*

(i) $K_{\pi'} = G' \cap N$;

(ii) $S_{\pi'} = \prod_{q \in \pi'} \mathrm{C}_{N_q}(HN_{\hat{q}}) \leq \mathrm{C}_N(H)$;

(iii) $S_{\pi'} \cap K_{\pi'} = 1$.

Proof If G is nilpotent, then $\pi(N)$ is empty, so the results are vacuous. Assume that G is nonnilpotent. Then N is nontrivial. Let q be in $\pi(N)$. Then $S \cap N_q = S_q$ and $K \cap N_q = K_q$. Since K_π is a normal π-subgroup of G, it is contained in $\mathrm{O}_\pi(G)$, that is, in $\mathrm{C}_H(N)$. Thus H normalizes N_q and so does $HN_{\hat{q}}$. Since $[HN_{\hat{q}}, N_q]$ is nontrivial, we have, from Lemma 3.3.3,

$$K_q = [HN_{\hat{q}}, N_q], \; S_q = \mathrm{C}_{N_q}(HN_{\hat{q}}) \leq \mathrm{C}_N(H)$$

and $S_q \cap K_q = 1$ for all $q \in \pi(N)$. Thus (ii) and (iii) follow immediately. It remains to show that $K_{\pi'} = G' \cap N$. It is obvious that $K_q = [HN_{\hat{q}}, N_q]$ for every $q \in \pi(N)$ implies that $K_{\pi'} \leq G'$, so $K_{\pi'} \leq G' \cap N$. Since $G' \leq K$, we also have $G' \cap N \leq K \cap N = K_{\pi'}$. Thus $K_{\pi'} = G' \cap N$. □

We have an immediate consequence of the above lemma by observing that the conjugacy class of H and N are determined by G.

Theorem 3.3.8 *Let G be a group with a metacyclic factorization $G = SK$. Let $G = HN$ be the standard Hall-decomposition for this metacyclic factorization. Then $N = (S \cap N)(K \cap N)$ is a split metacyclic factorization with $S \cap N \leq \mathrm{C}_N(H)$. No matter how we choose a metacyclic factorization $G = SK$, the subgroup $K \cap N$ is independent of the choice of the factorization and the conjugacy class of $S \cap N$ is also independent of the choice of the factorization.*

Definition 3.3.9 Let G be a metacyclic group. A metacyclic factorization $G = SK$ is called *standard* if $|S| \geq |X|$ and $|K| \leq |Y|$ for every metacyclic factorization $G = XY$. If $G = SK$ is a standard metacyclic factorization with the standard Hall-decomposition $G = HN$, then the factorization $G = (S \cap H)(K \cap H)(S \cap N)(K \cap N)$ is called a *standard factorization* of G.

Let $G = SK$ be a given metacyclic factorization with the standard Hall-decomposition $G = HN$ of odd order. Let $\mathcal{K}$ denote the set of all cyclic normal subgroups Y such that H/Y is cyclic and $Y \leq \mathrm{O}_\pi(G)$. Then $K \cap H$ belongs to the set $\mathcal{K}$, so the set is nonempty. Choose Y in $\mathcal{K}$ so that Y is of least order in the set. Then, from Lemma 3.3.2, there exists a cyclic subgroup X such that $H = XY$ and $|X| = \exp H$. Define $S^* := X(S \cap N)$ and $K^* := Y(K \cap N)$. Then $|S^*|$ is maximal and $|K^*|$ is minimal. By Lemma 3.3.1, $G = S^*K^*$ is a metacyclic factorization and so it is a standard metacyclic factorization of G. Moreover $S^* \cap H = X$ and $K^* \cap H = Y$; $S^* \cap N = S \cap N$ and $K^* \cap N = K \cap N$.

This observation proves the existence of standard metacyclic factorization.

Lemma 3.3.10 *Every metacyclic group of odd order has a standard metacyclic factorization.*

The following result also follows from the above observation.

Lemma 3.3.11 *A metacyclic factorization $G = SK$ of a metacyclic group G of odd order is standard if and only if for every p in π, $H_p = S_pK_p$ is an $\mathrm{O}_p(G)$-standard metacyclic factorization (as defined in Section 3.1).*

3.4 Presenting metacyclic groups of odd order

In this section, we propose presentations of certain form for metacyclic groups of odd order. It will be proved that most parameters involved in the proposed presentations are determined as some invariants of the isomorphism types of groups so defined. We first define 8-tuples of positive integers which will serve as parameters of such presentations. We use the notation $|m \bmod n|$, $\pi(m)$ and $m(p)$ as defined in Section 1.3.

Let Ω be the set of all 8-tuples $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ of positive integers such that for $\mu := \mathrm{lcm}\{q-1 : q \in \pi(\zeta)\}$ (when $\zeta = 1$, $\mu := 1$) and $\kappa := |\theta \bmod \zeta|$, the following conditions hold:

$$\delta \mid \gamma,\ \gamma \mid \beta\delta,\ \beta \mid \alpha,$$

$$\pi(\beta) \subseteq \pi(\gamma),$$

$$\pi(\varepsilon) \subseteq \pi(\zeta),$$

$$\pi(\alpha\delta) \cap \pi(\zeta) = \varnothing,$$

$$\eta^{\varepsilon} \equiv 1 \bmod \zeta,$$

$$\theta^{\alpha} \equiv 1 \bmod \zeta,$$

$$\theta^{\mu} \equiv 1 \bmod \zeta,$$

$$\gcd(\theta\eta - 1, \zeta) = 1,$$

$$\forall p \in \pi(\alpha\delta),\ \ \beta(p) < \gamma(p) \Rightarrow \alpha(p) - \beta(p) < \kappa(p).$$

We shall establish some notation.

Notation 3.4.1 *Given two positive integers m and n, the number $(m|n)$ denotes the smallest nonnegative solution of the simultaneous congruence system*

$$x \equiv p^{m(p)} \bmod p^{n(p)},\ \ p \in \pi(n).$$

Note that if m divides n then $m = \gcd((m|n), n)$.

Let $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ be a fixed element in Ω such that $\alpha, \beta, \gamma, \delta, \varepsilon$ and ζ are odd numbers. We define a presentation with the generating set

$$\{x, y, u, v\}$$

and the following defining relations:

$$\begin{aligned}
&x^{\alpha} = y^{\beta}, \\
&y^{x} = y^{1+(\gamma|\beta\delta)}, \quad y^{\beta\delta} = 1, \\
&u^{x} = u, \qquad u^{y} = u, \quad u^{\varepsilon} = 1, \\
&v^{x} = v^{\theta}, \qquad v^{y} = v, \quad v^{u} = v^{\eta}, \quad v^{\zeta} = 1.
\end{aligned}$$

We denote the presentation by $\wp(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ and call such a presentation a *standard presentation.* Keeping the other parameters fixed, we sometimes abbreviate it to $\wp(\eta, \theta)$, or $\wp(\theta)$, or $\wp(\eta)$, or $\wp$.

Remark 3.4.2 A consistent metacyclic presentation for the group defined by a standard presentation may be given as follows:

$$\langle a, b \mid a^{\alpha\varepsilon} = b^{\beta\zeta},\ b^{\beta\delta\zeta} = 1,\ b^{a} = b^{n} \rangle$$

where n is the smallest nonnegative integer such that

$$\begin{cases} n \equiv 1+(\gamma|\beta\delta) \bmod \beta\delta \\ n \equiv \eta\theta \bmod \zeta. \end{cases}$$

Then we have following theorem.

Theorem 3.4.3 *Every metacyclic group of odd order has a standard presentation and each standard presentation defines a metacyclic group of odd order. The parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and the multiplicative order κ of θ modulo ζ are uniquely determined by the isomorphism type of the group so presented.*

Note that η, θ are not invariants in general. We divide the proof of the theorem into several lemmas.

Lemma 3.4.4 *Let G be a metacyclic group of odd order and $G = XYUV$ a standard factorization. Then G has a standard presentation $\wp(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ where*

$$\alpha = |X : X \cap Y|,\ \beta = |Y : X \cap Y|,\ \gamma = |Y : (XY)'|,\ \delta = |X \cap Y|,\ \varepsilon = |U|, \zeta = |V|.$$

Proof Set $H := XY$, $N := UV$, $S := XU$ and $K := YV$. Remember that $G = HN$ is the standard Hall-decomposition for the metacyclic factorization $G = SK$. Define π, ϖ to be the set of all prime divisors of orders of H and N, respectively. Then $\pi = \pi(\alpha\delta)$, because $|X| = \exp H$. If $K_q = 1$ for some q in ϖ, then $S_{q'}K_{q'}$ is a normal Hall q'-subgroup, so q is contained in π but this is not the case. Thus for every q in ϖ, we have $K_q \neq 1$ and hence $\varpi = \pi(\zeta)$. So

$$\pi(\varepsilon) \subseteq \pi(\zeta).$$

Since π and ϖ are disjoint,

$$\pi(\alpha\delta) \cap \pi(\zeta) = \varnothing.$$

By Lemma 3.1.3 and Lemma 3.3.11,

$$\delta \mid \gamma,\ \gamma \mid \beta\delta,\ \beta \mid \alpha$$

and

$$\pi(\beta) \subseteq \pi(\gamma).$$

By Lemma 3.1.3, for every $p \in \pi$, the Sylow p-subgroup of H has the following presentation:

$$\langle\, x_p, y_p \mid x_p^{p^{\alpha(p)}} = y_p^{p^{\beta(p)}},\ y_p^{p^{\beta(p)+\delta(p)}} = 1,\ y_p^{x_p} = y_p^{1+p^{\gamma(p)}} \,\rangle.$$

Let $x := \prod_{p\in\pi} x_p$ and $y := (\prod_{p\in\pi} y_p^{\alpha_{p'}})^s$ where $\alpha_{p'}$ is the p'-component of α and $s = (\beta|\beta\delta)/\beta$. A routine verification shows that

$$x^\alpha = y^\beta,\ y^{\beta\delta} = 1,\ y^x = y^{1+(\gamma|\beta\delta)}.$$

Let θ be a positive integer such that

$$v^x = v^\theta,$$

and set

$$\kappa := |\theta \bmod \zeta|.$$

Then $\kappa = |H : \mathrm{O}_\pi(G)|$. It is obvious that $\kappa \mid \alpha$, $\kappa \mid \mu$, here μ as defined in the beginning of this section. So we have

$$\theta^\alpha \equiv 1 \bmod \zeta, \quad \theta^\mu \equiv 1 \bmod \zeta.$$

Since the metacyclic factorization $\langle x_p \rangle \langle y_p \rangle$ of each Sylow p-subgroup of H is $\mathrm{O}_p(G)$-standard, it is obvious from Lemma 3.1.3(iii) that

$$\text{if } \beta(p) < \gamma(p) \text{ then } \alpha(p) - \beta(p) < \kappa(p).$$

Choose generators u, v of U, V, respectively. Of course,

$$u^\varepsilon = 1, \ v^\zeta = 1.$$

Next let η be a positive integer such that

$$v^u = v^\eta.$$

Then

$$\eta^\varepsilon \equiv 1 \bmod \zeta.$$

If G is nilpotent, then $N = 1$, or equivalently $\zeta = 1$. If G is not nilpotent, let q be a prime in ϖ. Since $G = HN$ is the standard Hall-decomposition, the Hall q'-subgroups are not normal. Thus $S_{q'}$ acts nontrivially on K_q and so does on $\Omega_1(K_q)$ [see Suzuki (1986, Corollary, p. 74)]. Thus S acts nontrivially on $\Omega_1(K_q)$. It follows that $\gcd(\theta\eta - 1, q) = 1$. So in either case

$$\gcd(\theta\eta - 1, \zeta) = 1.$$

We have observed that the parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta$ and θ satisfy the conditions for the parameters of standard presentations. So it gives rise to a standard

presentation $\wp(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,\eta,\theta)$. The generating set $\langle x,y,u,v\rangle$ of G satisfies the defining set of relations of $\wp$. Thus G is a homomorphic image of a group defined by the standard presentation $\wp$. The presentation $\wp$ defines a metacyclic group of order at most $\alpha\beta\delta\varepsilon\zeta$, so $\wp$ is a standard presentation of G. □

Let $G := \langle x,y,u,v\rangle$ be a fixed group defined by the standard presentation $\wp(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,\eta,\theta)$. Throughout the remainder of this section, κ denotes the multiplicative order $|\theta \bmod \zeta|$ and we keep the following notation fixed

$$\begin{aligned} H &:= \langle x,y\rangle, & N &:= \langle u,v\rangle;\\ X &:= \langle x\rangle, & Y &:= \langle y\rangle;\\ U &:= \langle u\rangle, & V &:= \langle v\rangle;\\ S &:= XU, & K &:= YV;\\ \pi &:= \pi(H), & \varpi &:= \pi(N). \end{aligned}$$

Lemma 3.4.5

(i) *H is a nilpotent metacyclic subgroup with the presentation*

$$\langle\, x,y \mid x^\alpha = y^\beta,\ y^{\beta\delta} = 1,\ y^x = y^{1+(\gamma|\beta\delta)}\,\rangle$$

and $|H| = \alpha\beta\delta,\ \ |H/H'| = \alpha\gamma,\ \ \exp H = \alpha\delta$.

(ii) *N is a metacyclic normal subgroup of order $\varepsilon\zeta$ with the presentation*

$$\langle\, u,v \mid u^\varepsilon = 1,\ v^\zeta = 1,\ v^u = v^\eta\,\rangle.$$

(iii) *$G = SK$ is a metacyclic factorization with the standard Hall-decomposition $G = HN$.*

(iv) $\mathrm{O}_\pi(G) = \langle x^\kappa, y\rangle$ *and hence* $|H : \mathrm{O}_\pi(G)| = \kappa$.

Proof Let

$$\bar{H} := \langle\, a,b \mid a^\alpha = b^\beta,\ b^{\beta\delta} = 1,\ b^a = b^{1+(\gamma|\beta\delta)}\,\rangle$$

and

$$\bar{N} := \langle\, c,d \mid c^\varepsilon = 1,\ d^\zeta = 1,\ d^c = d^\eta\,\rangle.$$

Obviously $|\bar{H}| \leq \alpha\beta\delta$. For each prime divisor p of $\alpha\delta$, there is a homomorphism from $\bar{H}$ onto the group defined by

$$\langle\, a_p, b_p \mid a_p^{p^{\alpha(p)}} = b_p^{p^{\beta(p)}},\ b_p^{p^{\beta(p)+\delta(p)}} = 1,\ b_p^{a_p} = b_p^{1+p^{\gamma(p)}}\,\rangle.$$

We know from Theorem 3.1.4 that the latter group has order $p^{\alpha(p)+\beta(p)+\delta(p)}$; the intersection of the kernels of these homomorphisms has index $\alpha\beta\delta$. This proves that $|\bar{H}| = \alpha\beta\delta$ and $\bar{H}$ is the direct product of the p-groups defined by the presentations displayed above. In particular, these p-groups are the Sylow subgroups of $\bar{H}$. So $\bar{H}$ is nilpotent. By the cyclic extension theory, $\bar{N}$ is a metacyclic group of order $\varepsilon\zeta$. The group $\langle a^\kappa, b\rangle$ is a normal subgroup of index κ in the group $\bar{H}$ so defined, while $\bar{N}$ has an automorphism of order κ such that $c \mapsto c,\ d \mapsto d^\theta$. Consequently,

$$c^a = c,\ d^a = d^\theta,\ c^b = c,\ d^b = d$$

define a nontrivial action of $\bar{H}$ on $\bar{N}$ with kernel $H^* = \langle a^\kappa, b\rangle$, and we may form a semidirect product $\bar{G} = \bar{H} \ltimes \bar{N}$ accordingly. The set $\{a, b, c, d\}$ of elements in $\bar{G}$ generates $\bar{G}$, and the elements satisfy all the relations of G. So $\bar{G}$ is a homomorphic image of G. On the other hand, the subgroup H of G is a homomorphic image of $\bar{H}$ and the subgroup N of G is a homomorphic image of $\bar{N}$ and $N \trianglelefteq G$, so $G = HN$. Hence

$$|\bar{G}| \leq |G| \leq |H||N| \leq |\bar{H}||\bar{N}| = |\bar{G}|.$$

It follows that $H \cong \bar{H}$, $N \cong \bar{N}$ and $G \cong \bar{G}$. From Lemma 3.3.1, we know that $G = SK$ is a metacyclic factorization. Consequently, G is a metacyclic group of order $\alpha\beta\delta\varepsilon\zeta$.

Suppose there exists a prime q in ϖ such that a Hall q'-subgroup is normal in G. Then $S_{q'}K_{q'}$ is normal in G, so $[S_{q'}, K_q] = 1$. On the other hand, the condition $\gcd(\theta\eta - 1, \zeta) = 1$ implies that $\gcd(\theta\eta - 1, q) = 1$, so $\gcd(\theta\eta^{q^\epsilon} - 1, q) = 1$ since $\eta^{q^\epsilon} \equiv \eta \bmod q$ by Fermat's Little Theorem. This amounts to saying that $S_{q'}$ acts nontrivially on K_q, contradicting $[S_{q'}, K_q] = 1$. Thus there are no q in

ϖ such that a Hall q'-subgroup is normal in G. So we have

$$\pi = \{p \in \pi(G) : G \text{ has a normal Hall } p'\text{-subgroup}\}.$$

Thus $G = HN$ is the standard Hall-decomposition for $G = SK$. Finally, we easily observe that

$$|H/H'| = \alpha\gamma, \ \exp H = \alpha\delta, \ \mathrm{O}_\pi(G) = H^*.$$

The proof is now complete. □

Lemma 3.4.6 *The parameters α, β, γ, δ, ε, ζ and κ are invariants of G.*

Proof Since N is the intersection of all normal Sylow complements, we know that $|N|$ is an invariant of G, and hence $|H| = \alpha\beta\delta$ is also an invariant. By the above lemma, β and κ are invariants.

For every $p \in \pi$, we define $e_p := \exp(H_p/H_p')$, $f_p := |H_p|/\exp \mathrm{O}_p(G)$ and $g_p := p^{\beta(p)+\kappa(p)}$, where H_p is the Sylow p-subgroup of H. Then obviously e_p, f_p are invariants for every $p \in \pi$. The g_p are also invariants since $p^{\beta(p)}$ and $p^{\kappa(p)}$ are invariants. Moreover, we observe that $e_p = \max(p^{\alpha(p)}, p^{\alpha(p)+\gamma(p)-\beta(p)})$ and $f_p = \min(p^{\alpha(p)}, p^{\beta(p)+\kappa(p)})$. Let π^* be the set $\{p \in \pi : f_p = g_p\}$. Then π^* and $\pi - \pi^*$ are determined by the isomorphism type of G. If $f_p = g_p$ then $\alpha(p) \geq \beta(p) + \kappa(p)$; hence $\beta(p) \geq \gamma(p)$, so $e_p = p^{\alpha(p)}$. If $f_p < g_p$ then $\alpha(p) < \beta(p) + \kappa(p)$ and hence $f_p = p^{\alpha(p)}$. Therefore, $\alpha = \prod_{p\in\pi^*} e_p \prod_{p\in\pi-\pi^*} f_p$ is an invariant. Since $\exp H = \alpha\delta$ and $|H/H'| = \alpha\gamma$ are invariants, and so are γ and δ.

Since $U = S \cap N$ and $V = K \cap N$, we know from Theorem 3.3.8 that $|U| = \varepsilon$ and $|V| = \zeta$ are also invariants of G. □

Now the three lemmas above provide a proof of Theorem 3.4.3. Keeping the above notation, we also have a consequence of the above lemmas.

Corollary 3.4.7 *$G = XYUV$ is a standard factorization.*

Proof Let $G = X_0Y_0U_0V_0$ be a standard factorization. Since $|X| = |X_0|$, by Theorem 3.3.8, we only need to show that $|Y| = |Y_0|$. By Lemma 3.4.4, G has a standard presentation $\wp(\alpha_0, \beta_0, \gamma_0, \delta_0, \varepsilon_0, \zeta_0, \eta_0, \theta_0)$ with $|Y_0| = \beta_0\delta_0$. By Lemma 3.4.6, we have $\beta = \beta_0$ and $\delta = \delta_0$. Thus $|Y| = \beta\delta = \beta_0\delta_0 = |Y_0|$, as required. □

3.5 Isomorphism Problem

The aim of this section is to solve the isomorphism problem for groups G defined by standard presentations $\wp(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$. We have already seen that the parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and the multiplicative order κ of θ modulo ζ are invariants of G. So we keep these parameters fixed throughout this section. We only need to determine which values of η and θ give isomorphic metacyclic groups for the given parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and κ. Where necessary, we write $G(\eta)$ or $G(\theta)$ or $G(\eta, \theta)$ instead of G to indicate that the groups depend on η or θ or both η and θ. Note that the relevant range of (η, θ) is the set

$$\{\, (\eta, \theta) : (\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta) \in \Omega,\ |\theta \bmod \zeta| = \kappa \,\}$$

for the fixed positive integers $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and κ. Note that κ satisfies

$$\kappa(p) \leq \alpha(p),\ \kappa(p) \leq \mu(p)$$

whenever $p \in \pi$, and

$$\text{if } \beta(p) < \gamma(p) \text{ then } \alpha(p) - \beta(p) < \kappa(p).$$

We here have some examples which illustrate our problem.

Example Define

$$G_1 := \langle\, a, b, d \mid a^9 = b^3, b^9 = 1, b^a = b^4, d^7 = 1, d^a = d^2, d^b = d \,\rangle,$$

$$G_2 := \langle\, a, b, d \mid a^9 = b^3, b^9 = 1, b^a = b^4, d^7 = 1, d^a = d^4, d^b = d \,\rangle,$$

$$G_3 := \langle\, a, b, d \mid a^3 = b^3, b^9 = 1, b^a = b^4, d^7 = 1, d^a = d^2, d^b = d \,\rangle,$$

$$G_4 := \langle a, b, d \mid a^3 = b^3, b^9 = 1, b^a = b^4, d^7 = 1, d^a = d^4, d^b = d \rangle.$$

The groups G_1 and G_2 are isomorphic because the map $a \mapsto a^2$, $b \mapsto a^3b$, $c \mapsto c$, $d \mapsto d$ defines an isomorphism of G_1 and G_2. We shall see that G_3 and G_4 are not isomorphic.

Now we return to general situation with the following lemma.

Lemma 3.5.1

$$G(\eta_1, \theta_1) \cong G(\eta_2, \theta_2) \iff G(\eta_1, \theta_1) \cong G(\eta_1, \theta_2),\ G(\eta_1, \theta_2) \cong G(\eta_2, \theta_2).$$

Proof Suppose $G(\eta_1, \theta_1) \cong G(\eta_2, \theta_2)$. Then there exists a metacyclic group G which has standard presentations $\wp(\eta_1, \theta_1)$ and $\wp(\eta_2, \theta_2)$. For $i = 1, 2$, let $\{x_i, y_i, u_i, v_i\}$ be a generating set of G which satisfies the defining relations of $\wp(\eta_i, \theta_i)$. Then $\langle u_1, v_1 \rangle = \langle u_2, v_2 \rangle$; we denote this common subgroup by N. We may assume that $\langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle$ by replacing the generators by the relevant conjugates if necessary; H denotes this common subgroup. By Corollary 3.4.7, $G = \langle x_i \rangle \langle y_i \rangle \langle u_i \rangle \langle v_i \rangle$ is a standard factorization and hence $[H, u_i] = 1$ and $[y_i, N] = 1$ for each $i = 1, 2$. It follows from Theorem 3.3.8 that $\langle v_1 \rangle = \langle v_2 \rangle$. So $v_1 = v_2^n$ for some integer n. We observe that

$$v_1^{x_2} = (v_2^n)^{x_2} = (v_2^n)^{\theta_2} = v_1^{\theta_2}.$$

Thus the generating set $\{x_2, y_2, u_1, v_1\}$ satisfies $\wp(\eta_1, \theta_2)$, so $G(\eta_1, \theta_1) \cong G(\eta_1, \theta_2)$ and $G(\eta_1, \theta_2) \cong G(\eta_2, \theta_2)$. The other direction of the statement is obvious; the proof is now complete. □

By the above result, we only need to investigate the isomorphism problem for fixed η and that for fixed θ, respectively. We first consider the problem for fixed θ. It will turn out that this case is much easier than the other.

Lemma 3.5.2

$$G(\eta_1) \cong G(\eta_2) \iff \exists s \in \mathbf{Z} : \eta_1 \equiv \eta_2^s \bmod \zeta,\ (s, \varepsilon) = 1.$$

Proof Let $XYUV$ be a standard factorization corresponding to a standard presentation $\wp(\eta)$. Let x, y, u, v be the corresponding generators to the standard presentation. Write $\bar{\eta}$ for the homomorphism of U into $\operatorname{Aut} V$ defined by $u\bar{\eta}: v \mapsto v^{\eta}$. Suppose $G(\eta_1) \cong G(\eta_2)$. Let G be a metacyclic group which has the standard presentations $\wp(\eta_1)$ and $\wp(\eta_2)$. For each $i = 1, 2$, choose a standard factorization $G = X_iY_iU_iV_i$ which yields the standard presentation $\wp(\eta_i)$. Remember that $V_1 = V_2$ and U_1 is conjugate to U_2. Since $\operatorname{Aut} V_1$ is abelian, it follows from Lemma 2.1.6 that $U_1\bar{\eta}_1 = U_2\bar{\eta}_2$. So there is an integer s such that $\eta_1 \equiv \eta_2^s \bmod \zeta$ and $(s, \varepsilon) = 1$. The proof of the converse is obvious: in fact, $\wp(\eta_1)$ is obtained from $\wp(\eta_2)$ by simply changing the generator u to u^s. □

We now investigate the isomorphism problem for fixed η.

Let $H = \langle x, y \rangle$ be the group given by the defining relations

$$x^{\alpha} = y^{\beta},\ y^{\beta\delta} = 1,\ y^{x} = y^{1+(\gamma|\beta\delta)}$$

and let $H^* := \langle x^{\kappa}, y \rangle$. Let $N = \langle u, v \rangle$ be the group given by the defining relations

$$u^{\varepsilon} = 1,\ v^{\zeta} = 1,\ v^{u} = v^{\eta}.$$

Note that H and N are independent of θ. Write $\bar{\theta} : H \longrightarrow \operatorname{Aut} N$ for the action of H on N defined by $x\bar{\theta} : u \mapsto u,\ v \mapsto v^{\theta}$ and $y\bar{\theta} = 1$. We may view $G(\theta)$ as $H \ltimes_{\bar{\theta}} N$. Then obviously H^* is the common kernel of the actions by $\bar{\theta}$ for all possible alternatives θ.

Suppose that $H \ltimes_{\bar{\theta}_1} N \cong H \ltimes_{\bar{\theta}_2} N$. Set $G_i := H \ltimes_{\bar{\theta}_i} N$ for $i = 1, 2$. Suppose τ is an isomorphism of G_1 onto G_2. These two groups have the same set of elements; H and N and all their subgroups are subgroups in both G_1 and G_2. Since $\mathrm{O}_{\varpi}(G_1) = N = \mathrm{O}_{\varpi}(G_2)$ and $G_1' \cap N = \langle v \rangle = G_2' \cap N$, we must have $N\tau = N$ and $\langle v \rangle\tau = \langle v \rangle$. Since $\mathrm{O}_{\pi}(G_1) = H^* = \mathrm{O}_{\pi}(G_2)$, the isomorphism τ also maps H^* to H^*. Replacing τ by its composite with an inner automorphism if necessary, we can arrange τ also maps H to H. So we may assume that τ normalizes H. In that case τ induces an automorphism on H/H^*; since H/H^*

is generated by xH^*, we have

$$(x\tau)H^* = x^t H^*$$

for some integer t, which may be chosen so that $0 < t < \kappa$ and is then determined by τ. It follows from Lemma 2.1.6 that

$$v(x\bar{\theta}_1)\tau = (v\tau)(x\tau\bar{\theta}_2).$$

Then we have

$$\begin{aligned} v^{\theta_1} &= v(x\bar{\theta}_1) \\ &= [v(x\bar{\theta}_1)\tau]\tau^{-1} \\ &= [(v\tau)(x\tau\bar{\theta}_2)]\tau^{-1} \\ &= [(v\tau)(x^t\bar{\theta}_2)]\tau^{-1} \text{ (because } x\tau \equiv x^t \bmod \ker\bar{\theta}_2) \\ &= [(v\tau)^{\theta_2^t}]\tau^{-1} \text{ (because } v\tau \in \langle v\rangle) \\ &= (v\tau\tau^{-1})^{\theta_2^t}. \end{aligned}$$

This shows that

$$\theta_1 \equiv \theta_2^t \bmod \zeta.$$

Of course here we had $\tau\downarrow_H \in \mathsf{N}_{\mathrm{Aut}\,H}(H^*)$ and $(x\tau)H^* = x^t H^*$.

Conversely, suppose that $\rho \in \mathsf{N}_{\mathrm{Aut}(H)}(H^*)$ with $(x\rho)H^* = x^t H^*$ for some integer t such that $\theta_1 \equiv \theta_2^t \bmod \zeta$. Consider the permutation $\tau : (h, n) \mapsto (h\rho, n)$ of the common set of elements $H \times N$ of $H \ltimes_{\bar{\theta}_1} N$ and $H \ltimes_{\bar{\theta}_2} N$. This τ stabilizes $H \times 1$ and $1 \times N$, and its restrictions to these subgroups are automorphisms. In order to prove that τ is an isomorphism from $H \ltimes_{\bar{\theta}_1} N$ to $H \ltimes_{\bar{\theta}_2} N$, from Theorem 2.1.7, it remains to verify that $(n(h\bar{\theta}_1))\tau = (n\tau)(h\tau\bar{\theta}_2)$ holds as h, n range through the generating sets of H, N, respectively. With $h = y$, it holds because y and $y\rho$ lie in the common kernel H^* of $\bar{\theta}_1$ and $\bar{\theta}_2$. With $n = u$, the assertion holds because u is a fixed point of the common image of $\bar{\theta}_1$ and $\bar{\theta}_2$. In the remaining case $h = x$, $n = v$, and

$$(v(x\bar{\theta}_1))\tau = (v^{\theta_1})\tau = v^{\theta_1}$$

while

$$\begin{aligned}(v\tau)(x\tau\bar{\theta}_2) &= v(x\rho\bar{\theta}_2)\\ &= v(x^t\bar{\theta}_2)\\ &= v^{\theta_2^t}\\ &= v^{\theta_1}.\end{aligned}$$

We have thus proved the following.

Lemma 3.5.3

$$H \ltimes_{\bar{\theta}_1} N \cong H \ltimes_{\bar{\theta}_2} N \iff \exists \rho \in \mathsf{N}_{\mathrm{Aut}\,H}(H^*) : \theta_1 \equiv \theta_2^t \bmod \zeta$$

for some integer t satisfying $(x\rho)H^* = x^tH^*$.

Note that the map $(xH^* \mapsto x^tH^*) \mapsto t$, $0 < t < \kappa$, determins the natural isomorphism between $\mathrm{Aut}\,(H/H^*)$ and the multiplicative group of units of reduced residues modulo κ. Let Φ be the isomorphic copy of the group $\mathsf{N}_{\mathrm{Aut}\,H}(H^*)\downarrow_{H/H^*}$ in the multiplicative group of the units of reduced residues [smallest nonnegative representatives of residue classes] modulo κ. Then we conclude the following result.

Theorem 3.5.4 *The standard presentations $\wp(\eta,\theta)$ and $\wp(\eta',\theta')$ define isomorphic groups if and only if* (i) *there exists a positive integer s such that $\eta^s \equiv \eta' \bmod \zeta$ and $(s,\varepsilon) = 1$ and* (ii) *there exists an integer t in Φ such that $\theta' \equiv \theta^t \bmod \zeta$.*

Now we shall give an explicit description of Φ, which enables us to list all isomorphism types of the metacyclic groups of odd order. For each positive integer t and for each prime p, let $t[p]$ be the remainder obtained on dividing t by $p^{\kappa(p)}$: that is, the unique integer such that

$$0 \le t[p] < p^{\kappa(p)},\ t \equiv t[p] \bmod p^{\kappa(p)}.$$

Since H is nilpotent, it is the direct product $\prod_{p\in\pi} H_p$; as the H_p are characteristic in H, we also have $\mathrm{Aut}\,H = \prod_{p\in\pi}\mathrm{Aut}\,H_p$ by identifying them; moreover,

$$\mathsf{N}_{\mathrm{Aut}\,H}(H^*) = \prod_{p\in\pi}\mathsf{N}_{\mathrm{Aut}\,H_p}(H_p^*)$$

and

$$\mathsf{N}_{\mathrm{Aut}\,H}(H^*)\downarrow_{H/H^*} = \prod_{p\in\pi} \mathsf{N}_{\mathrm{Aut}\,H_p}(H_p^*)\downarrow_{H_P/H_p^*}.$$

In terms of reduced residues modulo κ and modulo the $p^{\kappa(p)}$, this amounts to the following. If $\rho \in \mathsf{N}_{\mathrm{Aut}\,H}(H^*)$ and $(x\rho)H^* = x^tH^*$ with $0 < t < \kappa$, then $t[p]$ corresponds to the component of $\rho\downarrow_{H/H^*}$ in the direct factor indexed by p in the direct decomposition displayed above, in the same sense as t corresponds to $\rho\downarrow_{H/H^*}$. Conversely, according to the Chinese Remainder Theorem, t can be recovered from the $t[p]$.

For any p in π, we define $\omega(p)$ to be the second term of the sequence obtained by arranging $\alpha(p)-\kappa(p)$, $\beta(p)-\kappa(p)$, $\gamma(p)$, $\gamma(p)-\delta(p)$ in nonincreasing order. In Section 3.2 we calculated $|\mathsf{N}_{\mathrm{Aut}\,H_p}(H_p^*)|$. Since the relevant set, $\Phi(p)$ say, of reduced residues is the unique subgroup of that order in the cyclic group of units of reduces residues modulo $p^{\kappa(p)}$, we may identify $\Phi(p)$ as follows.

Theorem 3.5.5 *If $\kappa(p) = 0$ then $\Phi(p) = 1$. Suppose $\kappa(p) > 0$. if $\beta(p) \le \omega(p)$ then $\Phi(p) = \{t \in \mathbf{Z} : \ 0 < t < p^{\kappa(p)}, \ \gcd(t,p) = 1\}$, while if $\beta(p) > \omega(p)$ then $\Phi(p) = \{t \in \mathbf{Z} : \ 0 < t < p^{\kappa(p)}, \ \ t \equiv 1 \bmod p^{\beta(p)-\omega(p)}\}$. Moreover, $\Phi = \{t \in \mathbf{Z} : 0 < t < \kappa,$ for any $p \in \pi$, $t[p] \in \Phi(p)\}$.*

3.6 Metacyclic $\{p,q\}$-groups

Applying the result developed so far, we shall determine the metacyclic groups whose order have only two prime divisors. For the sake of simplicity, we only consider nonnilpotent metacyclic groups of this kind. In this case the situation is relatively simple so that we can here explicitly list a set of complete and irredundant representatives of the isomorphism types of those groups in terms of standard presentations. Throughout this section, let p, q be two odd prime numbers such that p divides $q-1$, and let μ be the largest integer such that p^μ divides $q-1$.

Let Γ be the set of all 5-tuples $(\alpha, \beta, \gamma, \delta, \kappa)$ of nonnegative integers satisfying the following conditions:

(i) $\alpha \geq \beta \geq \gamma - \delta \geq 0$;

(ii) either $\gamma \geq 1$ or $\beta = 0$;

(iii) $1 \leq \kappa \leq \min(\alpha, \mu)$;

(iv) either $\beta \geq \gamma$ or $\alpha - \beta < \kappa$.

Let Δ be the set of all triples $(\varepsilon, \zeta, \eta)$ of nonnegative integers satisfying

$$\varepsilon + \eta \geq \zeta \geq \eta > 0.$$

Let $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \kappa, \eta$ be given nonnegative integers such that

$$(\alpha, \beta, \gamma, \delta, \kappa) \in \Gamma \text{ and } (\varepsilon, \zeta, \eta) \in \Delta$$

and let θ be a primitive p^κth root of unity modulo q^ζ. Then we define a presentation with the generating set consisting of x, y, u, v and the following defining relations:

$$\begin{aligned}
&x^{p^\alpha} = y^{p^\beta}, \\
&y^x = y^{1+p^\gamma}, \quad y^{p^{\beta+\delta}} = 1, \\
&u^x = u, \qquad u^y = u, \qquad u^{q^\varepsilon} = 1, \\
&v^x = v^\theta, \qquad v^y = v, \qquad v^u = v^{1+q^\eta}, \qquad v^{q^\zeta} = 1.
\end{aligned}$$

We here denote the presentation by $\langle \alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta \rangle$. Then the presentation is a standard presentation of a nonnilpotent metacyclic group of order $p^{\alpha+\beta+\delta} q^{\varepsilon+\zeta}$ and every nonnilpotent metacyclic $\{p, q\}$-group has a presentation of this form. We have also shown that the parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and the multiplicative order κ of θ modulo q^ζ are determined by the isomorphism type of the group so presented. We observe that η is also an invariant of that group. In fact, the normal Sylow q-subgroup of a group defined by the presentation has a presentation

$$\langle u, v : u^{q^\varepsilon} = 1,\ v^{q^\zeta} = 1,\ v^u = v^{1+q^\eta} \rangle.$$

We observe easily that $Q/Q' \cong C(q^\varepsilon) \times C(q^\eta)$. Since ε is an invariant, η is also invariant.

It follows that $\langle \alpha, ..., \theta \rangle \cong \langle \alpha', ..., \theta' \rangle$ if and only if $\alpha = \alpha', ..., \eta = \eta'$ while θ and θ' are in the same orbit of Φ. The listing of representatives of the isomorphism types of metacyclic $\{p, q\}$-groups with invariants $\alpha, ..., \eta$ has therefore been reduced to listing representatives of the orbits of Φ on the set of elements θ of multiplicative order p^κ in the group of units of reduced residues modulo p^ζ. Since these θ are permuted regularly by the group of units of reduced residues modulo p^κ, this amounts to listing representatives of the cosets of Φ (as defined in Theorem 3.5.4) in that group. There is a chain of subgroups from Φ to that group, the index of one term in the next being $p, ..., p, p-1$. Choosing an obvious transversal for each term in the nest and then forming the product of these transversals, we obtain the desired transversal of Φ. An explicit list of such representatives may be determined as follows. Let $\omega = \omega(\alpha, \beta, \gamma, \delta, \kappa)$ to be the second term of the sequence obtained by arranging

$$\alpha - \kappa, \ \beta - \kappa, \ \gamma, \ \gamma - \delta$$

in nonincreasing order. When $\beta \leq \omega$, define $\Lambda = \Lambda(\alpha, \beta, \gamma, \delta, \kappa) := \{1\}$; otherwise define

$$\Lambda := \{ i \prod_{j=1}^{\beta-\omega-1} (1 + s_j p^j) : i, j, s_j \in \mathbb{Z}, \ 1 \leq i \leq p-1, \ 0 \leq s_j \leq p-1 \}.$$

Then $\Lambda(\alpha, \beta, \gamma, \delta, \kappa)$ is a transversal of the subgroup Φ in the multiplicative group of the units of reduced residues modulo p^k.

Let θ_κ denote the smallest positive p^κth root of unity modulo q^ζ. We have proved the following.

Theorem 3.6.1 *The presentations*

$$\langle \alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta_\kappa^s \rangle$$

with $(\alpha, \beta, \gamma, \delta, \kappa) \in \Gamma$, $(\varepsilon, \zeta, \eta) \in \Delta$ *and* $s \in \Lambda(\alpha, \beta, \gamma, \delta, \kappa)$ *form a complete and irredundant set of representatives of the isomorphism types of nonnilpotent metacyclic* $\{p, q\}$*-groups.*

Chapter 4

Faithful irreducible representations of metacyclic groups

Most of this chapter is devoted to the study of faithful irreducible representations of metacyclic groups. The aim is to explore how the study for a given metacyclic group may be reduced to the analogous study for some subgroups. A correspondence between such representations of a metacyclic group of odd order and irreducible representations of the centre of the Fitting subgroup will be established. This provides a complete reduction of the problem of determining faithful irreducible representations of a metacyclic group of odd order to a similar problem for that abelian characteristic subgroup. We will also find that this yields, at least in principle, a solution to the conjugacy problem for isomorphic metacyclic subgroups of the general linear groups.

4.1 The representation theory of cyclic groups

The representation theory of finite cyclic groups for arbitrary fields seems to be part of the folklore; we present some of the main results from the theory without proof.

Theorem 4.1.1 *Let G be a cyclic group of order n, and let F be a field. Then the set of all isomorphism types of irreducible $\mathsf{F}G$-modules is bijective with the set of all monic irreducible polynomials in $\mathsf{F}[x]$ that divide $x^n - 1$. Given a generator g of G, one may define such a bijection by associating with each irreducible $\mathsf{F}G$-module the minimal polynomial of g on that module.*

Theorem 4.1.2 *If G is a cyclic group of order n and F is a field whose characteristic does not divide n, then the isomorphism types of the faithful irreducible $\mathsf{F}G$-modules correspond to the irreducible divisors of the nth cyclotomic polynomial in $\mathsf{F}[x]$; these all have the same degree, d say. If F is a finite field, then d is the smallest positive integer such that n divides $|\mathsf{F}|^d - 1$. The endomorphism rings of the faithful irreducible modules also have dimension d over F.*

Theorem 4.1.3 *In any general linear group, there is at most one conjugacy class of cyclic irreducible subgroups of any given finite order.*

4.2 Faithful irreducible representations

In this section, we shall investigate some principal results on faithful irreducible representations of metacyclic groups.

Clifford's Theorem states that if N is a normal subgroup of a finite group G and V is an irreducible $\mathsf{F}G$-module for a field F, then the restriction $V{\downarrow_N}$ is a completely reducible $\mathsf{F}N$-module and its irreducible submodules form a class of G-conjugate $\mathsf{F}N$-modules. Let W be an irreducible submodule of $V{\downarrow_N}$ and T the inertia group of W, that is, $T = \{t \in G : W^t \cong W\}$. Note that T is determined by V up to conjugacy; in other words, the G-conjugacy class of T does not depend on the particular choice of W. If U is the sum of all submodules of $V{\downarrow_N}$ isomorphic to W, then U is an irreducible $\mathsf{F}T$-module such that $U{\uparrow^G} \cong V$ and $U{\downarrow_N} \cong W^{\oplus m}$, the direct sum of m copies of W for some positive integer m.

We shall develop a strengthened form of Clifford's Theorem in our case. We first fix some notation. Let G be a metacyclic group and K a fixed cyclic normal subgroup such that G/K is cyclic. Define $A := \mathrm{C}_G(K)$. We first need the following two lemmas.

Lemma 4.2.1 *The group A is a normal abelian subgroup of G with $\mathrm{C}_G(A) = A$. In particular A is maximal among the abelian subgroups of G.*

We omit the easy proof of the above lemma.

Lemma 4.2.2 *If L is a subgroup of A such that A/L is cyclic and $\mathrm{core}_G\, L = 1$, then*

(i) $\mathrm{C}_G(A/L) = A$;

(ii) $|A/L| = \exp A$.

Proof (i) Since each subgroup of K is characteristic in K and so normal in G, it follows from $\mathrm{core}_G\, L = 1$ that $L \cap K = 1$. Let N be the normalizer of L. Since N/A acts faithfully on K and $KL/L \cong K/(K \cap L) \cong K$ are N-isomorphisms, the action of N/A on KL/L is faithful. As $KL \leq A$, it follows that $\mathrm{C}_G(A/L) \leq A$. The other direction of inequality is obvious, so the result follows.

(ii) L contains the subgroup $A^{|A/L|}$, consisting of all $|A/L|$th powers of elements of A. The subgroup $A^{|A/L|}$ is normal in G and L is core-free and thus $A^{|A/L|} = 1$. Since A/L is cyclic, there exists a cyclic subgroup of order $|A/L|$. It follows that $|A/L| = \exp A$. □

We then have an immediate consequence of Lemma 4.2.2(i).

Corollary 4.2.3 *Let W be an irreducible $\mathsf{F}A$-module with $\mathrm{core}_G \ker W = 1$. If F is a splitting field for A, then the inertia group of W is A itself.*

Now we have the main theorem of this section.

Theorem 4.2.4 *Let* F *be a field and* G *a metacyclic group with a normal subgroup* A *chosen as before. Let* V *be a faithful irreducible* $\mathsf{F}G$*-module, let* W *be an irreducible submodule of* $V{\downarrow_A}$*, and let* T *be the inertia subgroup of* W*. Then*

(i) $\mathrm{core}_G \ker W = 1$;

(ii) *if* F *has nonzero characteristic, then there exists an* $\mathsf{F}T$*-module* U *such that* $U{\uparrow^G} \cong V$ *and* $U{\downarrow_A} \cong W$;

(iii) *if* F *is finite, then the image of* T *in* $GL(U)$ *normalizes an irreducible cyclic subgroup of order* $|U|-1$ *in* $GL(U)$ *(namely the group of nonzero elements of the linear span of the image of* A*).*

Proof By Clifford's Theorem, there exists an $\mathsf{F}T$-module U such that $U{\uparrow^G} \cong V$ and $U{\downarrow_A} \cong W^{\oplus m}$, the direct sum of m copies of W for some positive integer m. Set $L := \ker U$, then $\mathrm{core}_G L = 1$ since V is faithful and $\ker V = \mathrm{core}_G \ker U$. Each subgroup of K is characteristic in K and hence normal in G; we have $K \cap L = 1$. Thus $[K, L] = 1$, and hence $L \leq A$, $L = \ker W$ and A/L is cyclic. Therefore $\mathrm{C}_G(A/L) = A$ by Lemma 4.2.2(i). Incidentally, we have proved (i).

Since W is irreducible, $\mathrm{End}_{\mathsf{F}A} W$ is a division ring; the linear F-span of the image of A in $\mathrm{End}_{\mathsf{F}} W$ is a commutative F-algebra in the division ring. So it is semisimple. It follows from Wedderburn's Structure Theorem that the F-span of the image of A is a field: call it E. Then E is a splitting field for A. Since W is irreducible, $\dim_{\mathsf{E}} W = 1$, so $\dim_{\mathsf{F}} W = \dim_{\mathsf{F}} \mathsf{E} =: d$, say. (In fact, $\mathsf{E} = \mathrm{End}_{\mathsf{F}A} W$.) By Theorem (9.21) and Corollary (10.2h) in Isaacs (1976), $W \otimes_{\mathsf{F}} \mathsf{E} \cong W_1 \oplus \cdots \oplus W_d$ where the W_i are different $\mathrm{Gal}\,(\mathsf{E}|\mathsf{F})$-conjugates of a one-dimensional $\mathsf{E}A$-module. For any $t \in T$, $W^t \cong W$ means that W_i^t is also isomorphic to an irreducible direct summand of $W \otimes_{\mathsf{F}} \mathsf{E}$, so $W_i^t \cong W_j$ for some integer j such that $1 \leq j \leq d$. Since $W_i^{t_1 t_2} \cong (W_i^{t_1})^{t_2}$ for all $i = 1, ..., d$ and t_1, t_2 in T, the inertia subgroup T acts on the set $\{1, ..., d\}$. The stabilizer of each point i is A: for the stabilizer obviously contains A; the other inequality follows from $\mathrm{C}_T(A/L) = A$, $\ker W_i = \ker \mathrm{W} = L$ and $\dim_{\mathsf{E}} W_i = 1$ for all i. Thus T

permutes the set $\{1, ..., d\}$ in orbits of length $|T{:}A|$, the number of orbits being $d/|T{:}A|$.

Suppose the characteristic of F is not zero. By Theorem VII.1.15 in Huppert and Blackburn (1982),

$$U \otimes_{\mathsf{F}} \mathsf{E} \cong U_1 \oplus \cdots \oplus U_k$$

where the U_j are pairwise nonisomorphic irreducible $\mathsf{E}T$-modules. Thus

$$\begin{aligned} \oplus_{j=1}^{k} U_j{\downarrow}_A &\cong (U \otimes_{\mathsf{F}} \mathsf{E}){\downarrow}_A \\ &\cong U{\downarrow}_A \otimes_{\mathsf{F}} \mathsf{E} \\ &\cong W^{\oplus m} \otimes_{\mathsf{F}} \mathsf{E} \\ &\cong (W \otimes_{\mathsf{F}} \mathsf{E})^{\oplus m} \\ &\cong \oplus_{i=1}^{d} W_i^{\oplus m}. \end{aligned}$$

Let X be an irreducible $\mathsf{E}A$-submodule of U_j, and R a complete set of representatives of the cosets of T modulo A. Then there exists i_0 such that $X \cong W_{i_0}$. The sum of the Xr with $r \in R$ is an $\mathsf{E}T$-submodule of the irreducible $\mathsf{E}T$-module U_j, so that sum is U_j, and the Xr are pairwise nonisomorphic $\mathsf{E}A$-modules since $Xr \cong W_{i_0}^r$. So their sum is a direct sum; thus $\dim_{\mathsf{E}} U_j = |T : A| = \dim_{\mathsf{E}} W_{i_0}{\uparrow}^T$. By the Nakayama Reciprocity,

$$0 \neq \dim_{\mathsf{E}} \mathrm{Hom}_{\mathsf{E}A}(W_{i_0}, U_j{\downarrow}_A) = \dim_{\mathsf{E}} \mathrm{Hom}_{\mathsf{E}T}(W_{i_0}{\uparrow}^T, U_j),$$

and a nonzero homomorphism of $W_{i_0}{\uparrow}^T$ into the irreducible module U_j, of the same dimension as $W_{i_0}{\uparrow}^T$, must be an isomorphism, so $U_j \cong W_{i_0}{\uparrow}^T$. We observe that W_{i_0} occurs in $(U \otimes_{\mathsf{F}} \mathsf{E}){\downarrow}_A$ with multiplicity m, but in $U_j{\downarrow}_A$ only with multiplicity 1. So if $m > 1$ then W_{i_0} would also occurs in some other $U_l{\downarrow}_A$. Then $U_l \cong W_{i_0}{\uparrow}^T \cong U_j$ would follow, contradicting that $U \otimes_{\mathsf{F}} \mathsf{E}$ is multiplicity free. This proves that $m = 1$, and hence (ii) holds.

Suppose now that F is finite. We have seen that $\dim_{\mathsf{F}} U = \dim_{\mathsf{F}} W = \dim_{\mathsf{F}} \mathsf{E}$, so $|U| = |\mathsf{E}|$. The image of T in $\mathrm{End}_{\mathsf{F}} U$ normalizes the F-span E of the image of A, and hence it normalizes the cyclic irreducible subgroup $\mathsf{E}^{\times}$ of order $|U|-1$ in $GL(U)$. $\square$

Remark If the characteristic of the field is 0, the multiplicity of W in $U{\downarrow}_A$ need not be 1. In this case we can show that the multiplicity is equal to the Schur index of an irreducible submodule of $U \otimes_{\mathsf{F}} \mathsf{F}^*$ for an algebraic closure F^* of F, but we omit the details because we are really interested in finite fields in view of our motivation.

We now consider a necessary and sufficient condition for the existence of faithful irreducible representations of a metacyclic group G in terms of the abelian normal subgroup A. We prove the following result.

Theorem 4.2.5 *G has a faithful irreducible representation over a field F if and only if the characteristic of F does not divide $\exp A$ and there exists a subgroup L of A such that A/L is cyclic and $\mathrm{core}_G\, L = 1$.*

The proof requires the following lemma.

Lemma 4.2.6 *Let F be a field whose characteristic does not divide the order of A. Let W be an irreducible $\mathsf{F}A$-module with core-free kernel. Then every irreducible submodule of the induced module $W{\uparrow}^G$ is faithful. Conversely, each faithful irreducible $\mathsf{F}G$-module is a submodule of such a $W{\uparrow}^G$.*

Proof Let V be an irreducible submodule of $W{\uparrow}^G$. Since $(W{\uparrow}^G){\downarrow}_A \cong \bigoplus W^g$ where the direct sum is taken over all g in a transversal of A in G, we have $V{\downarrow}_A \cong \bigoplus_{\text{some}\, g} W^g$. So $A \cap \ker V \leq (\ker W)^{g_0}$ for some g_0 in G. Because $A \cap \ker V$ is normal in G, this implies that $A \cap \ker V \leq \ker W$. So $A \cap \ker V \leq \mathrm{core}_G \ker W = 1$. Since $[A, \ker V] = 1$, we have $\ker V \leq \mathrm{C}_G(A) = A$. Therefore $\ker V = 1$.

Given a faithful irreducible $\mathsf{F}G$-module V, let W be an irreducible constituent of the $\mathsf{F}A$-module $V{\downarrow}_A$. Since $V{\downarrow}_A$ is a sum of G-conjugates of W, we have $\mathrm{core}_G \ker W = 1$. By the Nakayama Reciprocity,

$$0 \neq \mathrm{Hom}_{\mathsf{F}A}(V{\downarrow}_A, W) \cong \mathrm{Hom}_{\mathsf{F}G}(V, W{\uparrow}^G),$$

so $W{\uparrow}^G$ has a submodule isomorphic to V. □

With Lemma 4.2.2(ii), Theorem 4.2.4(i) proves the 'only if' part of Theorem 4.2.5; on the other hand, Lemma 4.2.6 proves the 'if' part. Thus the proof of Theorem 4.2.5 is complete.

In Section 2.4, we have characterized the finite groups having faithful irreducible representations in general; applying the general result of Theorem 2.4.4, we may have an alternative condition for the existence of faithful irreducible representations of metacyclic groups.

Theorem 4.2.7 *A metacyclic group has a faithful irreducible representation over a field* F *if and only if the centre of the group is cyclic and the characteristic of* F *does not divide the order of the Fitting subgroup.*

Proof Since one direction of the result is well known [see Huppert and Blackburn (1982, Theorem VII.13.4, Theorem VIII.3.2)], by Theorem 2.4.4 it remains to prove that if the centre of a metacyclic group G is cyclic and the condition for the field is satisfied, then the socle U of G is generated by a single element.

Suppose that the centre Z of G is cyclic and the condition for the underlying field is satisfied. Let $G = SK$ be a metacyclic factorization with a cyclic normal subgroup K. Suppose there are two different minimal normal subgroups M_1, M_2 of G which are G-isomorphic. Since K is cyclic, the subgroup $M_1 \times M_2$ is not contained in K. Without loss of generality, we assume that M_2 is not contained in K; then

$$M_1 \cong_G M_2 \cong_G M_2K/K \leq G/K.$$

So G acts trivially on $M_1 \times M_2$, that is $M_1 \times M_2 \leq Z$, a contradiction to the assumption that Z is cyclic. Consequently, no two distinct minimal normal subgroups are G-isomorphic.

Let M be a minimal normal subgroup in G. Since no distinct minimal normal subgroups are G-isomorphic, the multiplicity of M as a direct summand of U is 1. It follows from Lemma 2.4.2 that U is generated by a single element and hence the proof is complete. □

4.3 Degrees of faithful irreducible representations

In this section, we consider the degrees of faithful irreducible representations of metacyclic groups. We shall prove that the degrees are all the same for a given metacyclic group over a given field when that field has prime characteristic. Given this result, the problem of determining the linear isomorphism types of metacyclic irreducible linear groups which fall into a single abstract isomorphism type is equivalent to that of determining the conjugacy classes of those subgroups in the general linear group of the relevant degree.

Let G be a metacyclic group and A a subgroup in G chosen as before. Let F be a field; suppose that G has at least one faithful irreducible F-representation. The image of an irreducible F-representation of A with core-free kernel is cyclic; by Lemma 4.2.2, its order is $\exp A$; hence by Theorem 4.1.2, the degrees of all such representations are the same: call this common degree d. It follows from Theorem 4.2.4 that if the characteristic of F is prime then the degree of a faithful irreducible F-representation of G is $|G{:}T|d$, where T is the inertia group defined in that theorem. Our aim in this section is to show that this T is the same for all faithful irreducible F-representations of G, so these representations have a common degree.

Let E be a field whose characteristic does not divide $\exp A$ and which contains all $(\exp A)$th roots of unity. Regarding A as a G-module with respect to G-conjugation action, the dual $A^* := \mathrm{Hom}(A, \mathsf{E}^\times)$ is also a G-module with respect to the natural G-conjugation action:

$$\lambda^g : a \mapsto (gag^{-1})\lambda, \ a \in A$$

for every $\lambda \in A^*$ and $g \in G$. In Section 2.4, we have already observed some usual properties of duals. In particular, every irreducible E-representation of A with core-free kernel generates A^* as a G-module.

Since G has at least one faithful irreducible representations over a field F, of course, the characteristic of F does not divide the order of A. We prove the following lemma.

Lemma 4.3.1 *Let* F *be any field (of any characteristic). All irreducible* $\mathsf{F}A$*-modules* W *with* $\mathrm{core}_G \ker W = 1$ *have the same inertia group.*

Proof Let E be the field obtained by adjoining to F an element of multiplicative order $\exp A$. Let α be an irreducible F-representation of A. From Theorem (9.21) and Corollary (10.2h) in Isaacs (1976), α^{E} is the sum of the distinct $\mathrm{Gal}\,(\mathsf{E}|\mathsf{F})$-conjugates of some element λ of A^*. It follows that for any element g of G,

$$[\alpha^g] = [\alpha] \iff \lambda^g \text{ is a } \mathrm{Gal}\,(\mathsf{E}|\mathsf{F})\text{-conjugate of } \lambda,$$

because $[\alpha^g] = [\alpha] \iff [(\alpha^{\mathsf{E}})^g] = [\alpha^{\mathsf{E}}]$ [see Huppert and Blackburn (1982, Theorem VII.1.22) and Lemma 2.3.1]. All Galois-conjugates of λ have the same kernel as λ, so that is also the kernel of α^{E} and hence also of α; thus if α has core-free kernel, so does λ. From Lemma 2.4.1, we know that if λ has core-free kernel then λ generates A^* as a G-module. Since $G/\mathrm{C}_G(A^*)$ is abelian, conjugation by g is a G-module automorphism of A^*, so if g acts on a G-module generator λ as some element η of $\mathrm{Gal}\,(\mathsf{E}|\mathsf{F})$, then g acts like η on all of A^*. The conclusion is that if $\mathrm{core}_G \ker \alpha = 1$ and $[\alpha^g] = [\alpha]$, then $[\beta^g] = [\beta]$ for all irreducible F-representations β of G. □

We have already observed that the degree of a faithful irreducible representation is determined by $|G{:}T|d$ when the underlying field has nonzero characteristic. So we here have an immediate consequence of the above lemma.

Corollary 4.3.2 *The degrees of the faithful irreducible representations of a metacyclic group over a field of nonzero characteristic are all the same, and the common degree is given by* $|G{:}T|d$ *where* d *is the degree of an irreducible representation of* A *with core-free kernel and* T *the inertia group of the representation of* A.

Finally we consider the problem of recognizing the inertia group T for a finite field F.

Remark 4.3.3 *Let F be a finite field and let W be an irreducible $\mathsf{F}A$-module with the kernel L. Set $N := \mathsf{N}_G(L)$; let $\bar{N}$ be the natural image of N in $\mathrm{Aut}(A/L)$. The inertia group of W is the unique subgroup T with*

$$|T : A| = |\bar{N} \cap \langle \alpha_0 \rangle|$$

where α_0 is the automorphism of A/L defined by $aL \mapsto a^{|\mathsf{F}|}L$.

Proof The automorphism group $\mathrm{Aut}(A/L)$ acts transitively on the isomorphism types of irreducible representations of A with kernel L. The result will immediately follow if we show that $\langle \alpha_0 \rangle$ is the stabilizer of the isomorphism type of W. Let $d := \dim W$ and $m := |\mathrm{Aut}(A/L)|$. Then d is the smallest positive integer such that $|\mathsf{F}|^d \equiv 1 \bmod |A/L|$. From the representation theory of cyclic groups, we know that there are precisely m/d isomorphism types of faithful irreducible $\mathsf{F}(A/L)$-modules. It follows that the stabilizer in $\mathrm{Aut}(A/L)$ of the isomorphism type of W is a subgroup of index m/d in $\mathrm{Aut}(A/L)$ (equivalently, of order d).

The statement $W \cong W^\alpha$ says that the element α in $\mathrm{Aut}(A/L)$ lies in this subgroup of order d. On the other hand, the group $\langle \alpha_0 \rangle$ acts trivially on W. Since the group has order d, the group $\langle \alpha_0 \rangle$ is the stabilizer of the isomorphism type of W. Thus the assertion is now clear. □

4.4 Correspondence Theorem

In this section we shall establish a natural correspondence between the faithful irreducible representations of a metacyclic group of odd order and the irreducible representations with core-free kernel of the centre of the Fitting subgroup. This reduces the problem of determining the faithful irreducible representations of a metacyclic group of odd order to a corresponding problem for that abelian characteristic subgroup.

We start with some information about the general context. Let F be a field, G a finite group and N a normal subgroup. We shall use the notation $W \in \mathrm{Irr}_{\mathsf{F}} N$ to indicate that W is an irreducible $\mathsf{F}N$-module. We define

$$[\mathrm{Irr}^*_{\mathsf{F}} N] := \{[W] \mid W \in \mathrm{Irr}_{\mathsf{F}} N,\ \mathrm{core}_G \ker W = 1\},$$

the set of all isomorphism types of irreducible $\mathsf{F}N$-modules with core-free kernel. In particular, $[\mathrm{Irr}^*_{\mathsf{F}} G]$ is the set of all isomorphism types of faithful irreducible $\mathsf{F}G$-modules. Let H be a group that acts on a set Ω, the action being understood from the context. We denote by Ω/H the set of orbits of this action. If $H = G$, the envisaged action is usually conjugation; $[\mathrm{Irr}^*_{\mathsf{F}} N]/G$ means the set of all G-conjugacy classes of the isomorphism types of irreducible $\mathsf{F}N$-modules with core-free kernel. In particular, as G acts trivially on the set of the isomorphism types of irreducible $\mathsf{F}G$-modules, $[\mathrm{Irr}^*_{\mathsf{F}} G]/G = [\mathrm{Irr}^*_{\mathsf{F}} G]$.

Let V be an irreducible $\mathsf{F}G$-module and let W be an irreducible $\mathsf{F}N$-module. By Clifford's Theorem and the Nakayama Reciprocity, V is isomorphic to a submodule of $W{\uparrow}^G$ if and only if W is a direct summand of the $\mathsf{F}N$-module $V{\downarrow}_N$. Suppose that the equivalent conditions hold. Then $\mathrm{core}_G \ker W = N \cap \ker V$. If N contains all minimal normal subgroups of G, then we easily observe that

$$\mathrm{core}_G \ker W = 1 \iff \ker V = 1.$$

There exists a surjective map from the set of the isomorphism types of irreducible $\mathsf{F}G$-modules onto that of the G-conjugacy classes of isomorphism types of irreducible $\mathsf{F}N$-modules. By the above observation, this maps $[\mathrm{Irr}^*_{\mathsf{F}} G]$ onto $[\mathrm{Irr}^*_{\mathsf{F}} N]/G$, provided N contains the socle of G; we call the surjective restriction $[\mathrm{Irr}^*_{\mathsf{F}} G] \longrightarrow [\mathrm{Irr}^*_{\mathsf{F}} N]/G$ the *Clifford map.* This map is far from being bijective in general.

We need the following basic fact.

Lemma 4.4.1 [see Rose (1978, Lemma 7.65, Theorem 7.67)] *If G is a finite soluble group, then $Z(\mathrm{Fit}\, G)$, the centre of the Fitting subgroup of G, contains the socle of G.*

The correspondence theorem may be stated as follows.

Theorem 4.4.2 *Let G be a metacyclic group of odd order. If $N \geq Z(\mathrm{Fit}\, G)$ and if $W \in \mathrm{Irr}_{\mathsf{F}} N$ with $\mathrm{core}_G \ker W = 1$, then*

$$W\uparrow^G \cong V \oplus \cdots \oplus V$$

for some $V \in \mathrm{Irr}_{\mathsf{F}} G$ with $\ker V = 1$. Hence in this case the Clifford map between $[\mathrm{Irr}^*_{\mathsf{F}} G]$ and $[\mathrm{Irr}^*_{\mathsf{F}} N]/G$ is bijective.

Throughout the proof of the theorem, let $A := \mathrm{C}_G(K)$ for a fixed cyclic normal subgroup K of G such that G/K is cyclic. Since the story for abelian groups is obvious, we may deal with only nonabelian metacyclic groups. So we assume that $G > A$. We also assume that G has at least one faithful irreducible representation over F. (This assumption does not do harm because if it is not the case, the claim of the theorem is vacuously true.) Then the characteristic of F does not divide the order of $\mathrm{Fit}\, G$; hence every $\mathsf{F}A$-module is completely reducible. We assume $N = Z(\mathrm{Fit}\, G)$. In fact, there is no loss of generality in assuming this [if $N \geq Z(\mathrm{Fit}\, G)$ and $W \in \mathrm{Irr}_{\mathsf{F}} N$ and if U is a submodule of $W\downarrow_{Z(\mathrm{Fit}\, G)}$, then W is isomorphic to a submodule of $U\uparrow^N$, so $W\uparrow^G$ is isomorphic to a submodule of $U\uparrow^G$; thus if the theorem is proved under the assumption, then the theorem will be proved in general].

We need the following lemma for the proof of the theorem.

Lemma 4.4.3

(i) $Z(\mathrm{Fit}\, G) \leq A$,

(ii) $|\mathrm{Fit}\, G : A| = |A : Z(\mathrm{Fit}\, G)|$.

Proof The observation $Z(\mathrm{Fit}\, G) \leq \mathrm{C}_G(\mathrm{Fit}\, G) \leq \mathrm{C}_G(K) = A$ proves the first result. The second result follows from Corollary 2.2.3, since we only need to know that the claim is true for every metacyclic group of odd-prime power order. □

Note that the first result is true for every metacyclic group. However, the second result is not true for metacyclic groups of even order in general: the metacyclic 2-group $\langle x, y \mid x^2 = 1,\ y^8 = 1,\ y^x = y^{-1} \rangle$ is one of the counter-examples.

For the proof of the theorem, we first start with a restriction on the field and then we shall consider the general case later. For the first consideration, we assume that the field F is big enough so that F is a splitting field for both of A and N. In this special case, the inertia groups of all irreducible representations of A with core-free kernel are equal to A, as observed in Corollary 4.2.3.

Let W be an irreducible $\mathsf{F}N$-module with $\operatorname{core}_G \ker W = 1$. Let U be an irreducible submodule of the induced $\mathsf{F}A$-module $W{\uparrow}^A$. Then W is isomorphic to a direct summand of the restricted $\mathsf{F}N$-module $U{\downarrow}_N$ by the Nakayama Reciprocity, so $N \cap \operatorname{core}_G \ker U \leq \operatorname{core}_G \ker W = 1$. Since N contains every minimal normal subgroup of G, we have

$$\operatorname{core}_G \ker U = 1.$$

By Corollary 4.2.3, the inertia subgroup of U is A itself, so if R is a transversal of A in $\operatorname{Fit} G$, then the U^g with $g \in R$ are pairwise nonisomorphic. Since the Fitting subgroup acts trivially on N, we have $(W{\uparrow}^A)^g \cong (W^g){\uparrow}^A \cong W{\uparrow}^A$ for every g in $\operatorname{Fit} G$, so each of the U^g with $g \in R$ is also a direct summand of $W{\uparrow}^A$. As these U^g are pairwise nonisomorphic, their direct sum $\bigoplus_{g \in R} U^g$ is also a direct summand of $W{\uparrow}^A$. Since this sum has dimension $|\operatorname{Fit} G : A|$ while $W{\uparrow}^A$ has dimension $|A : N|$, it follows from Lemma 4.4.3 that $W{\uparrow}^A \cong \bigoplus_{g \in R} U^g$. Write V for $U{\uparrow}^G$. Then V is a faithful irreducible $\mathsf{F}G$-module. It is obvious that

$$W{\uparrow}^G \cong V \oplus \cdots \oplus V,$$

as required. We have proved the theorem under the restriction on the field. We shall show that this restriction is not necessary.

Let E be the extension field obtained by adjoining to F an element of multiplicative order $\exp A$. Then of course the field E is a Galois extension of F and a splitting field for both of A and N. Let Γ denote the Galois group $\operatorname{Gal}(\mathsf{E}|\mathsf{F})$.

For our purpose we need to recall the behaviour of irreducible modules under extension of the ground field [see Huppert and Blackburn (1982, Theorem VII.1.8, Theorem VII.1.18)]. For each irreducible $\mathsf{F}G$-module V, the isomorphism types of the irreducible constituents of the $\mathsf{E}G$-module $V^{\mathsf{E}} := V \otimes_{\mathsf{F}} \mathsf{E}$ form a (single, complete) Γ-orbit. On the other hand, every irreducible $\mathsf{E}G$-module X determines exactly one isomorphism type of irreducible $\mathsf{F}G$-modules V such that X is isomorphic to an irreducible constituent of V^{E}. It follows that two irreducible $\mathsf{F}G$-modules V_1 and V_2 are isomorphic if some irreducible constituent of the $\mathsf{E}G$-modules V_1^{E} is Γ-conjugate to some irreducible constituent of the $\mathsf{E}G$-module V_2^{E}. We shall also need that if V is an $\mathsf{F}G$-module such that V^{E} is completely reducible, then V itself is completely reducible.

Given $W \in \mathrm{Irr}_{\mathsf{F}} N$ with $\mathrm{core}_G \ker W = 1$, we want to prove that $W\uparrow^G$ is completely reducible and its irreducible constituents are pairwise isomorphic. We know that $W^{\mathsf{E}} \cong \bigoplus_{i=1}^t W_i$ where the W_i are pairwise Γ-conjugate irreducible $\mathsf{E}N$-modules with $\mathrm{core}_G \ker W_i = 1$. We also know that $W_i\uparrow^G \cong V_i \oplus \cdots \oplus V_i$, for some V_i in $\mathrm{Irr}_{\mathsf{E}} G$ with $\ker V_i = 1$: the V_i are pairwise Γ-conjugate [if $W_i^\gamma \cong W_j$ for some $\gamma \in \Gamma$, then $V_i^\gamma \oplus \cdots \oplus V_i^\gamma \cong (W_i\uparrow^G)^\gamma \cong (W_i^\gamma)\uparrow^G \cong W_j\uparrow^G \cong V_j \oplus \cdots \oplus V_j$, so by the Krull-Schmidt Theorem, $V_i^\gamma \cong V_j$]. Therefore we have

$$(W\uparrow^G)^{\mathsf{E}} \cong \bigoplus_{i=1}^t W_i\uparrow^G \cong \bigoplus_{i=1}^t (V_i \oplus \cdots \oplus V_i).$$

So $(W\uparrow^G)^{\mathsf{E}}$ is completely reducible and its irreducible constituents are pairwise Γ-conjugate and hence $W\uparrow^G$ is also completely reducible. Let U_1 and U_2 be irreducible constituents of $W\uparrow^G$. Then U_1^{E} and U_2^{E} are direct summands of $(W\uparrow^G)^{\mathsf{E}}$, so their irreducible constituents are also irreducible constituents of $(W\uparrow^G)^{\mathsf{E}}$; thus an irreducible constituent of U_1^{E} is Γ-conjugate to an irreducible constituent of U_2^{E}, so $U_1 \cong U_2$. □

Remark One may note that the proof and the theorem hold for every metacyclic group G such that $|\mathrm{Fit}\, G : A| \geq |A : Z(\mathrm{Fit}\, G)|$. These groups include the symmetric group S_3, the dihedral group D_8 and the quaternion group Q_8.

4.5 Conjugacy of metacyclic linear groups

In this section, we apply the correspondence theorem obtained in the previous section to solve the linear isomorphism problem for abstractly isomorphic metacyclic irreducible F-linear groups. For this purpose, we change the point of view from modules to representations, but we will use the same notation established in the previous section.

We have already shown that in a general linear group all isomorphic cyclic irreducible subgroups of a given order are conjugate. For a prime p which is not equal to the characteristic of F, Conlon (1976, 1977) also showed that two nonabelian finite p-subgroups of $GL(p, \mathsf{F})$ are conjugate in $GL(p, \mathsf{F})$ if and only if they are isomorphic as abstract groups. The analogue of this is not true for our case. Consider $GL(3,7)$ and take a generator of a cyclic irreducible subgroup of order $(7^3-1)/2$; write b for it. Then the cyclic group is normalized by an element a of order 3 in $GL(3,7)$. The action of a on b is given by $b^a = b^7$. We can easily show that the two irreducible subgroups $\langle ab^{19}, b^9\rangle$ and $\langle a^2b^{19}, b^9\rangle$ are isomorphic as abstract groups. One may apply the general results in the next chapter to show that the two subgroups are not conjugate in $GL(3,7)$.

We now turn to the general situation. Let G be a metacyclic groups of odd order. The automorphism group $\operatorname{Aut} G$ acts on the set $[\operatorname{Irr}^*_{\mathsf{F}} G]$ in a natural way [see Section 2.3]. A basic result [see Theorem 2.3.2] shows that there is a natural one-to-one correspondence between the set of orbits under this action and that of all linear isomorphism types of irreducible F-linear groups that are abstractly isomorphic to G. Expressed differently: two equivalence types of faithful irreducible F-representations belong to the same $\operatorname{Aut} G$-orbit if and only if the images of the two representations are linearly isomorphic.

Let N be a characteristic subgroup of G which contains $Z(\operatorname{Fit} G)$. The automorphism group $\operatorname{Aut} G$ also acts on $[\operatorname{Irr}^*_{\mathsf{F}} N]$ in a natural manner, inducing the same group of permutations of this set as $(\operatorname{Aut} G)\downarrow_N$ in its natural action. Let ν be an irreducible F-representation of N with $\operatorname{core}_G \ker \nu = 1$.

Then $\nu\uparrow^G = \rho \oplus \cdots \oplus \rho$ by Theorem 4.4.2. Since $[(\nu^\alpha)\uparrow^G] = [(\nu\uparrow^G)^\alpha]$ for every $\alpha \in \operatorname{Aut} G$, the $\operatorname{Aut} G$-orbit of $[\nu]$ determines the $\operatorname{Aut} G$-orbit of $[\rho]$ and vice versa. This gives a bijection between $[\mathrm{Irr}^*_{\mathsf{F}} N]/\operatorname{Aut} G$ and $[\mathrm{Irr}^*_{\mathsf{F}} G]/\operatorname{Aut} G$.

We have proved the following theorem.

Theorem 4.5.1 *Let σ and ρ be faithful irreducible representations of G. Let μ and ν be irreducible constituents of $\sigma\downarrow_{Z(\mathrm{Fit}\, G)}$ and $\rho\downarrow_{Z(\mathrm{Fit}\, G)}$, respectively. Then the F-linear groups $G\sigma$ and $G\rho$ are linearly isomorphic if and only if $[\mu]$ and $[\nu]$ are in the same orbit of the natural action of $(\operatorname{Aut} G)\downarrow_{Z(\mathrm{Fit}\, G)}$ on $[\mathrm{Irr}^*_{\mathsf{F}} Z(\mathrm{Fit}\, G)]$.*

Remark When the field F has nonzero characteristic, the degrees of the faithful irreducible F-representations of a given metacyclic group G are all the same; then each linear isomorphism type of irreducible F-linear groups abstractly isomorphic to G has representatives among the subgroups of one general linear group. So in this case one may replace the term 'linearly isomorphic' with 'conjugate in $GL(n, \mathsf{F})$' where n is the common degree of the faithful irreducible representations of G.

Example Let p be an odd prime which is not equal to the characteristic of F. Then by Lemma 2.2.2(ii), Theorem 3.1.4 and Theorem 4.2.7, every noncyclic metacyclic p-group with at least one faithful irreducible F-representation has a presentation of the form

$$P = \langle\, a, b \mid a^{p^\alpha} = b^{p^\beta},\ b^{p^{\beta+\delta}} = 1,\ b^a = b^{1+p^\gamma} \,\rangle$$

where $\alpha, \beta, \gamma, \delta$ are integers such that $\alpha \geq \beta \geq \gamma = \delta \geq 1$.

Then $P' = \langle b^{p^\gamma} \rangle$ and $Z(P) = \langle a^{p^\beta} \rangle$, so $|P'| = p^\beta$ and $|Z(P)| = p^{\alpha-\beta+\delta}$. Since P is regular, $(a^i b^j)^{p^n} = a^{ip^n} b^{jp^n}$ for all integers i, j, n with $n \geq \beta$.

We consider the automorphisms of P and their restrictions to the centre $Z(P)$. Let K be the subgroup generated by b and let

$$A(K) := \{x \in P : y^x = y^{1+p^\gamma}, y \in K\}.$$

Then $A(K) = a\mathrm{C}_P(K)$. Let N be the set of all automorphisms θ of P such that $K\theta = K$. Then N is a subgroup of $\mathrm{Aut}\, P$. The map

$$a \mapsto x,\ b \mapsto y$$

defines an automorphism in N if and only if $x \in A(K)$, $\langle y \rangle = K$ and $x^{p^\alpha} = y^{p^\beta}$. Define

$$\mathcal{K} := \{K\theta : \theta \in \mathrm{Aut}\, P\}.$$

Then $|\mathrm{Aut}\, P| = |N||\mathcal{K}|$.

Let r, s, t be integers such that

$$0 \le r < p^{\alpha-\beta},\ 1 \le s \le p^{\beta+\delta},\ 1 \le t \le p^{\beta+\delta}.$$

The map

$$a \mapsto a^{1+rp^\beta} b^{s-1},\ b \mapsto b^t$$

defines an automorphism in N if and only if

$$\gcd(p,t) = 1,\ (s-1)p^{\alpha-\beta} \equiv t-1 \bmod p^\delta.$$

In this case, the automorphism so defined is denoted by $\theta_{r,s,t}$. Conversely, let θ be an automorphism in N. Then $a\theta \in a\mathrm{C}_P(K)$. Since $\mathrm{C}_P(K) = \langle a^{p^\beta}, b\rangle$, we have $a\theta = a^{1+rp^\beta} b^{s-1}$ for some integers r, s such that $0 \le r < p^{\alpha-\beta}$ and $1 \le s \le p^{\beta+\delta}$. Obviously $b\theta = b^t$ for some integer t with $1 \le t \le p^{\beta+\delta}$. Therefore, N consists of the automorphisms $\theta_{r,s,t}$ with the above conditions.

Consider the case when $\alpha = \beta \ge \gamma = \delta \ge 1$. In this case we shall show that all irreducible F-linear groups isomorphic to P as abstract groups are linearly isomorphic. By Theorem 4.5.1, it suffices to show that $\mathrm{Aut}\, Z(P) = (\mathrm{Aut}\, P)\downarrow_{Z(P)}$. In this case,

$$N = \{\theta_{0,s,t} : 1 \le s \le p^{\beta+\delta}, 1 \le t \le p^{\beta+\delta},\ \gcd(p,t) = 1,\ s \equiv t \bmod p^\delta\}.$$

Therefore, we have $|N| = (p-1)p^{2\beta+\delta-1}$. On the other hand,

$$\begin{aligned} \theta_{0,s,t}\downarrow_{Z(P)} = 1_{Z(P)} \quad &\Longleftrightarrow \quad (b^{p^\beta})\theta_{0,s,t} = b^{p^\beta} \\ &\Longleftrightarrow \quad b^{tp^\beta} = b^{p^\beta} \\ &\Longleftrightarrow \quad t \equiv 1 \bmod p^\delta. \end{aligned}$$

So we have

$$|N{\downarrow}_{Z(P)}| = (p-1)p^{2\beta+\delta-1}/p^{2\beta} = (p-1)p^{\delta-1} = |\mathrm{Aut}\, Z(P)|,$$

that is, $\mathrm{Aut}\, Z(P) = (\mathrm{Aut}\, P){\downarrow}_{Z(P)}$.

The general phenomenon is not always as good as the above case. We consider the case when $\alpha > \beta > \gamma = \delta \geq 1$. In this case P' properly contains $S \cap K$. Let θ be an automorphism of P. Then $K\theta$ is a cyclic normal subgroup such that $P/(K\theta)$ is cyclic and $|K\theta| = |K|$. Since $K\theta$ contains P', we have $S \cap (K\theta) = S \cap K$, so $P = S(K\theta)$. Therefore $K\theta/P'$ is a direct complement of SP'/P' in P/P'. Conversely, if Y is a direct complement of SP'/P' in P/P', then $P = SY$ is a standard metacyclic factorization [see Chapter 3], so there exist generators x and y of S and Y, respectively, which satisfy the defining relations of P. Then $a \mapsto x$, $b \mapsto y$ defines an automorphism of P and so $Y \in \mathcal{K}$. There are exactly $|\mathrm{Hom}(K/P', SP'/P')|$ different Y. Consequently, $|\mathcal{K}| = p^{\gamma}$. There exist precisely $p^{2\beta+\delta}$ different pairs of integers s and t satisfying

$$1 \leq s \leq p^{\beta+\delta},\ 1 \leq t \leq p^{\beta+\delta},\ \gcd(p,t) = 1 \text{ and } (s-1)p^{\alpha-\beta} \equiv t-1 \bmod p^{\delta}.$$

So $|\mathrm{Aut}\, P| = p^{\alpha+\beta+\gamma+\delta}$. It follows that $\mathrm{Aut}\, P$ is a p-group and hence it is impossible to have $\mathrm{Aut}\, Z(P) = (\mathrm{Aut}\, P){\downarrow}_{Z(P)}$. Thus at least when F is a splitting field for $Z(P)$, we have irreducible F-linear groups that are not linearly isomorphic but isomorphic to P as abstract groups.

Chapter 5

Metacyclic primitive linear groups

In this chapter we shall attempt to enumerate all metacyclic primitive subgroups of the general linear groups over a finite field up to conjugacy (for some related terminology and basic concepts for primitive linear groups, see Section 2.5). The approach we adopt here is completely different from that of the previous chapter. In the previous chapter, we were mostly concerned with representations of metacyclic groups to derive somewhat conceptual results. In this chapter, we deal with subgroups of general linear groups rather directly without reference to representations. This approach will enable us to list a complete and irredundant set of representatives of the linear isomorphism types of metacyclic primitive linear groups of odd prime-power degree over a finite field.

Theorem 5.3.1 in Short (1990) says that every abelian-by-nilpotent primitive linear group over a finite field normalizes a large cyclic irreducible group which is called a 'Singer cycle'. This fact reduces our problem to that of determining, up to linear isomorphism, the metacyclic primitive subgroups of the normalizer of a Singer cycle. The normalizer of a Singer cycle turns out to be a maximal soluble irreducible subgroup of the general linear group. Short determined all primitive subgroups of the normalizer of a Singer cycle of prime degree [see Short (1990,

Chapter 4)]. Our result generalizes Short's result to the case of odd prime-power degree.

5.1 Primitivity of cyclic subgroups

In this section we derive criteria for irreducibility and imprimitivity of a cyclic subgroup of the general linear group $GL(n, \mathsf{F})$ for a finite field F of order p^k. Let V be the natural module for $GL(n, \mathsf{F})$ and let C be a cyclic group in $GL(n, \mathsf{F})$.

We first consider the structure of the F-linear span of C in $\mathrm{End}_{\mathsf{F}}V$ when C is irreducible in $GL(n, \mathsf{F})$. Set $\mathsf{E} := \mathrm{End}_{\mathsf{F}C}V$. Since C is irreducible, E is a finite division ring, that is, a finite field. The F-linear span of C of $\mathrm{End}_{\mathsf{F}}V$ is a subring of the finite field E, so it is also a field.

The following result is now obvious from the fact that V is irreducible for a group if and only if V is irreducible for the F-linear span of it.

Lemma 5.1.1 *A cyclic subgroup C in $GL(n, \mathsf{F})$ is irreducible if and only if the F-linear span of C is a field of order $|\mathsf{F}|^n$.*

The following result is an immediate consequence of the above lemma. Note that every cyclic irreducible subgroup of $GL(n, p^k)$ is a subgroup of a cyclic irreducible subgroup of order $p^{kn}-1$ (namely, the nonzero elements of the F-linear span).

Lemma 5.1.2 *Let C be a subgroup in a cyclic irreducible subgroup of order $p^{kn}-1$. Then C is irreducible if and only if for every prime divisor q of n, the order of C does not divide $p^{kn/q}-1$.*

We then have a criterion for imprimitivity of cyclic irreducible subgroups.

Lemma 5.1.3 *Let C be a cyclic irreducible subgroup of $GL(n, p^k)$. Then C is imprimitive if and only if its order divides $q(p^{kn/q}-1)$ for some prime divisor q of $(|C|, n)$.*

Proof Suppose that C is imprimitive. Then there exists a proper subgroup D and a faithful irreducible module U for D such that $U\uparrow^C = V$. Then $n = |C{:}D|\dim U$ and hence for any prime divisor q of $|C{:}D|$ we have $C^q \geq D$ and $V = (U\uparrow^{C^q})\uparrow^C$. Therefore, $U\uparrow^{C^q}$ must be faithful irreducible for C^q of dimension n/q. So $|C^q|$ divides $p^{kn/q}-1$, that is $|C|$ divides $q(p^{kn/q}-1)$.

Conversely, let q be a prime divisor of n such that $|C|$ divides $q(p^{kn/q}-1)$. Then the dimension of any irreducible $\mathsf{F}C^q$-module is at most n/q. If U is an irreducible submodule of $V\downarrow_{C^q}$, then $V \leq U\uparrow^C$; we have dimU $\geq n/q$. Thus $\dim U = n/q$ and hence $V = U\uparrow^C$ follows, as required. □

5.2 Reduction Theorems

In this section, we investigate some results which enable us to reduce our problem considerably.

Lemma 5.2.1 *Let $G = Q \ltimes R$ be a finite group with $(|Q|, |R|) = 1$. Then every subgroup of G is conjugate to a subgroup of the form MN with $M \leq Q$ and $N \leq R$.*

Proof Let H be any subgroup of G and π the set of the prime divisors of the order of Q. Since

$$H/(H\cap R) \cong HR/R \leq G/R \cong Q,$$

the index of $H \cap R$ in H is relatively prime to the order of $H \cap R$. Therefore, the subgroup $H \cap R$ is the normal Hall π'-subgroup of H. By the Schur-Zassenhaus Theorem, there exists a complement X to $H \cap R$ in H, so that $H = X(H\cap R)$. The π-subgroup X is contained in a G-conjugate of Q, so $X^g \leq Q$ for some g in G. Let $M = X^g$ and $N = (R\cap H)^g$. Then $M \leq Q$, $N \leq R$, and $H^g = MN$. □

We now consider general linear groups. In what follows, let F be a finite field with p^k elements for a prime p.

Let G be a metacyclic primitive subgroup of $GL(n,\mathsf{F})$, K a fixed cyclic normal subgroup of G such that G/K is cyclic, and $A := \mathsf{C}_G(K)$. Let V be the natural module for $GL(n,\mathsf{F})$ and let W be an irreducible submodule of $V{\downarrow}_A$. Then of course V is a faithful irreducible $\mathsf{F}G$-module and the inertia group T of W is equal to G itself since G is primitive. Theorem 4.2.4(ii) with $T = G$ shows that $V{\downarrow}_A = W$. So A is irreducible on V, acting faithfully and hence A is in fact a cyclic group whose F-linear span is a field of order p^{kn}. Of course A is normal in G. It also follows that G normalizes the linear F-span E of A, and thus it normalizes the cyclic irreducible subgroup $\mathsf{E}^\times$ of order $p^{kn}-1$ in $GL(n,\mathsf{F})$.

Thus we have proved an important reduction theorem. This result was also known in a more general form by L.G. Kovács [see Short (1990, Theorem 5.3.1)].

Theorem 5.2.2 *If G is a metacyclic primitive subgroup of the general linear group $GL(n,\mathsf{F})$ over a finite field F, then G normalizes a cyclic irreducible subgroup of order $p^{kn}-1$.*

Let π be the set of all prime divisors of n. Let Y be a fixed cyclic irreducible subgroup of order $p^{kn}-1$ and let Γ be the normalizer of Y. Then $\Gamma = X \ltimes Y$ for some cyclic subgroup X of order n [see Theorem 2.5.2]. The generators x and y of X and Y, respectively, satisfy the following relations:

$$x^n = 1,\ y^{p^{kn}-1} = 1, y^x = y^{p^k}.$$

Note that the subgroup of order p^k-1 in Y is the scalar subgroup of $GL(n,\mathsf{F})$.

Let Q be the semidirect product of X and the Hall π-subgroup of Y, and let R be the normal Hall π'-subgroup of Y. Then Q is a Hall π-subgroup of Γ and R is the cyclic normal Hall π'-subgroup of Γ. The group Γ is also the semidirect product of Q and R. In fact, Γ is determined up to conjugacy by $GL(n,\mathsf{F})$ (see Theorem 4.1.3). In other words, the conjugacy class of Γ in $GL(n,\mathsf{F})$ is independent of the choice of Y, so we may fix the choice of Y.

The following corollary now follows from Lemma 5.2.1 and Theorem 5.2.2.

Corollary 5.2.3 *Every metacyclic primitive subgroup is conjugate to a subgroup of the form MN where $M \leq Q$ and $N \leq R$.*

The above corollary indicates that we only need to consider subgroups of the form MN in Γ to list complete and irredundant representatives of $GL(n, \mathsf{F})$-conjugacy classes of the metacyclic primitive subgroups of $GL(n, \mathsf{F})$.

We shall investigate primitivity of subgroups of Γ, the normalizer of a cyclic irreducible subgroup of order $p^{kn}-1$ in the general linear group $GL(n, \mathsf{F})$ over a finite field F, when n is a power of an odd prime.

Theorem 5.2.4 *Let $G = MN$ be a subgroup of Γ for some M in Q and N in R. If the degree n is a power of an odd prime, then*

G is primitive if and only if N is irreducible.

Proof Let q be the unique prime divisor of n. First we suppose that N is irreducible. Then from Lemma 5.1.2, $|N|$ does not divide $p^{kn/q}-1$ and thus $|N|$ does not divide $q(p^{kn/q}-1)$ since $(q, |N|) = 1$. It follows from Lemma 5.1.3 that N is primitive and therefore so is G.

Conversely, suppose G is primitive. Since every group having a primitive subgroup is again primitive, without loss of generality, we assume that $G = QN$. We only need to show that N is irreducible. For the purpose we divide the problem into two cases.

Case 1. q divides p^k-1 :

In this case $Q \cap Y$ is nontrivial, so the q-group $Q = X \ltimes (Q \cap Y)$ is a noncyclic metacyclic group. Since q is an odd prime, the subgroup $\Omega_1(Q)$ is isomorphic to $\mathsf{C}(q) \times \mathsf{C}(q)$.

Suppose N is reducible. Then $|N|$ divides $p^{kn/q}-1$ and hence $x^{n/q}$ acts trivially on N. It follows from $\Omega_1(Q) \leq \langle x^{n/q}, y \rangle$ that $\Omega_1(Q)$ acts trivially on N. Therefore $\Omega_1(Q) \times N$ is a noncyclic abelian normal subgroup of the metacyclic primitive group G. This violates the result of Theorem 2.5.1, so N is irreducible.

Case 2. q does not divide p^k-1 :

By Fermat's Little Theorem, the prime q does not divide $p^{kn}-1$. Thus $Q = X$, so $G = XN$ is a metacyclic factorization. Define $A := \mathrm{C}_G(N)$. Then $A = \mathrm{C}_X(N)N$. Since G is primitive, Theorem 4.2.4 yields that A is irreducible and so cyclic. It follows from Lemma 5.1.1 that $|A|$ divides $p^{kn}-1$. So the order of $\mathrm{C}_X(N)$ should divide the q'-number $p^{kn}-1$. However $\mathrm{C}_X(N)$ is a q-group and hence $A = N$, which implies that N is irreducible. □

The following theorem shows that the conjugacy problem of primitive metacyclic subgroups of $GL(n, \mathsf{F})$ can be reduced to the Q-conjugacy problem of the subgroups of Q when the degree n is a power of odd prime.

Theorem 5.2.5 *Let $G_i = M_iN_i$, $i = 1, 2$, be metacyclic primitive subgroups such that $M_i \leq Q$ and $N_i \leq R$. If n is a power of an odd prime, then G_1 and G_2 are conjugate in $GL(n, \mathsf{F})$ if and only if M_1 and M_2 are conjugate in Q and $N_1 = N_2$.*

Proof Since the 'if' part of the claim is obvious, it only remains to show the 'only if' part. Suppose that G_1 and G_2 are conjugate by an element g in $GL(n, \mathsf{F})$; then $G_1^g = G_2$. The subgroups N_1 and N_2 are the Hall π'-subgroups of G_1 and G_2, respectively, and then N_1 and N_2 are cyclic subgroups of the same order in the cyclic subgroup R. It follows easily that $N_1 = N_2$; we denote this common subgroup by N.

Since N is the normal Hall π'-subgroup of both G_1 and G_2, it is invariant under the conjugation action of g, that is, $N^g = N$. Then g normalizes N. By the previous theorem, N is irreducible; thus Theorem 2.5.2 yields that g is contained in Γ.

The subgroups M_1^g and M_2 are Hall π-subgroups of M_2N_2. Hence M_1 is conjugate to M_2 in Γ. Therefore M_1R is conjugate to M_2R in $Q \ltimes R$. It follows that M_1 is conjugate to M_2 in Q. □

We finally summarize an immediate consequence of the above observation for the general linear groups of odd prime-power degree.

Corollary 5.2.6 *Let $\mathcal{M}$ be a complete set of representatives of all Q-conjugacy classes of subgroups of Q, and let $\mathcal{N}$ be the set of all irreducible subgroups of R, as determined by Lemma 5.1.2. If the degree n is a power of an odd prime, then the set $\{MN : M \in \mathcal{M},\ N \in \mathcal{N}\}$ is a complete set of representatives of all conjugacy classes of metacyclic primitive subgroups of $GL(n, \mathsf{F})$.*

5.3 Q-conjugacy of subgroups of Q

In this section we shall explore the Q-conjugacy of subgroups of Q. By virtue of the reduction theorems in the previous section, the determination of Q-conjugacy of subgroups of Q completes our task.

We first determine all subgroups of Q. We know that Q is a semidirect product of two cyclic subgroups A and B: in fact, B is the normal Hall π-subgroup of the cyclic irreducible subgroup Y and A is a cyclic subgroup of order n. Let C and D be any subgroups of A and B, respectively.

It is necessary to have some knowledge on the theory of group extensions. For the general background, see Robinson (1982) or Robinson (1981).

A *derivation* from C to B/D is a map $\delta : C \longrightarrow B/D$ such that

$$(gh)\delta = (g\delta)^h(h\delta)$$

for all g, h in C. The set $\mathrm{Der}(C, B/D)$ of all such maps becomes an abelian group with a natural addition defined by

$$g(\delta_1 + \delta_2) = g\delta_1 g\delta_2.$$

To each v in B/D the map defined by

$$g \longmapsto v(g^{-1}v^{-1}g)$$

is a derivation. These *inner derivations* form a subgroup $\mathrm{Ider}(C, B/D)$ in $\mathrm{Der}(C, B/D)$. The corresponding factor group $H^1(C, B/D)$ is in fact the first cohomology group of C with coefficients in B/D.

For every derivation δ in $\mathrm{Der}(C, B/D)$, we define

$$[C, D, \delta] := \{cb : c\delta = bD,\ c \in C\}.$$

Then $[C, D, \delta]$ is a group. In fact, as is well known, the set

$$\{\, [C, D, \delta] : \delta \in \mathrm{Der}(C, B/D) \,\}$$

is the set of all subgroups H such that $HB = CB$ and $H \cap B = D$, and the map $\delta \mapsto [C, D, \delta]$ is a bijection between $\mathrm{Der}(C, B/D)$ and this set.

On the other hand, let H be any subgroup of the group $Q = A \ltimes B$. Set $D = H \cap B$ and $C = A \cap HB$. Since $HB = CB$, there exists a derivation δ in $\mathrm{Der}(C, B/D)$ such that $H = [C, D, \delta]$. Thus we have shown that every subgroup of Q can be realized as above.

Set

$$\mathrm{D}(Q) = \dot{\bigcup}\{\, \mathrm{Der}(C, B/D) : C \leq A, D \leq B \,\}$$

and

$$\mathrm{S}(Q) = \{[C, B, \delta] : C \leq A, D \leq B, \delta \in \mathrm{Der}(C, B/D)\}.$$

Then the following result is immediate from the above observation.

Lemma 5.3.1 $\mathrm{S}(Q)$ *is the set of all subgroups of* Q *and* $\delta \mapsto [C, D, \delta]$ *is a bijection from* $\mathrm{D}(Q)$ *to* $\mathrm{S}(Q)$.

We now consider the conjugacy problem of subgroups of Q.

Lemma 5.3.2 *Let* $[C_i, D_i, \delta_i] \in \mathrm{S}(Q), i = 1, 2$. *If* $[C_1, D_1, \delta_1]$ *and* $[C_2, D_2, \delta_2]$ *are conjugate in* Q, *then* $C_1 = C_2$ *and* $D_1 = D_2$.

Proof Define $H_i = [C_i, D_i, \delta_i]$ for $i = 1, 2$. Then

$$H_i \cap B = D_i \text{ and } H_i/D_i \cong C_i.$$

Moreover the D_i are normal in Q. So $H_1^g = H_2,\ g \in Q$ implies that

$$D_1 = D_1^g = H_1^g \cap B = H_2 \cap B = D_2$$

and hence that C_1 and C_2 are isomorphic subgroups of the cyclic group A; thus $C_1 = C_2$. □

The following lemma, which is well known, is useful to determine conjugacy.

Lemma 5.3.3 *Let $[C, D, \delta_i], i = 1, 2$ be subgroups in $\mathrm{S}(Q)$ and set $L := CB$. Then $[C, D, \delta_1]$ is conjugate to $[C, D, \delta_2]$ by an element of B if and only if $\delta_1 - \delta_2$ is an inner derivation from C to B/D; thus there is a bijection between the set of L-conjugacy classes of all subgroups H such that $HB = L, H \cap B = D$ on the one hand, and the quotient group $H^1(C, B/D)$ on the other.*

The above lemma does not reveal a complete solution for the Q-conjugacy problem, but does so for the L-conjugacy problem. To solve the Q-conjugacy problem of Q, we here investigate the natural action of A on $H^1(C, B/D)$.

Let $A = \langle x \rangle$ and for any $\delta \in \mathrm{Der}(C, B/D)$, we define δ^x as the function which maps c to $(c\delta)^x$, for every $c \in C$. Note that $\delta \mapsto \delta^x$ is an automorphism of $\mathrm{Der}(C, B/D)$ with $\delta^x = p^k\delta$. So the map induces a natural action of A on $\mathrm{Der}(C, B/D)$. This shows that $\mathrm{Der}(C, B/D)$ is an A-module. Since $\mathrm{Ider}(C, B/D)$ is a submodule, the quotient $H^1(C, B/D)$ is also an A-module.

We then prove the following theorem.

Theorem 5.3.4 *$[C, D, \delta_1]$ is conjugate to $[C, D, \delta_2]$ by an element in Q if and only if $\delta_1 + \mathrm{Ider}(C, B/D)$ and $\delta_2 + \mathrm{Ider}(C, B/D)$ are in the same orbit of the natural action of A on $H^1(C, B/D)$.*

Proof Let δ be a derivation in $\mathrm{Der}(C, B/D)$. First we will verify that $[C, D, \delta]$ is conjugate to $[C, D, \delta_2]$ by an element of A if and only if δ and δ_2 are in the same A-orbit in $\mathrm{Der}(C, B/D)$. In fact,

$$\begin{aligned}
[C, D, \delta]^a &= \{c^a b^a : c\delta = bD,\ c \in C\} \\
&= \{cb^a) : c\delta^a = b^a D,\ c \in C\} \\
&= [C, D, \delta^a]
\end{aligned}$$

for every $a \in A$. So $[C, D, \delta]^a = [C, D, \delta_2]$ if and only if $\delta^a = \delta_2$; thus the above fact follows.

We also know from Lemma 5.3.3 that $[C, D, \delta_1]$ is conjugate to $[C, D, \delta]$ by an element of B if and only if

$$\delta_1 + \mathrm{Ider}(C, B/D) = \delta + \mathrm{Ider}(C, B/D).$$

The result of the lemma follows from the fact that $[C, D, \delta_1]$ is conjugate to $[C, D, \delta_2]$ by an element of Q if and only if there exists a δ in $\mathrm{Der}(C, B/D)$ such that $[C, D, \delta_1]$ is conjugate to $[C, D, \delta]$ by an element of B and $[C, D, \delta]$ is conjugate to $[C, D, \delta_2]$ by an element of A. □

Since the generator x of A acts on $H^1(C, B/D)$ as the p^k-th powering map, we immediately have the following result.

Corollary 5.3.5 *$[C, D, \delta_1]$ is conjugate to $[C, D, \delta_2]$ by an element in Q if and only if $\delta_1 + \mathrm{Ider}(C, B/D) = p^{kr}\delta_2 + \mathrm{Ider}(C, B/D)$ for some integer r such that $1 \leq r \leq |A/C|$.*

Now we only need to calculate the derivations, the inner derivations and the quotients. Let ϕ be the endomorphism of B/D defined by $bD \mapsto b^f D$ where $f = (p^{k|A|}-1)/(p^{k|A:C|}-1)$. An element of B/D is the image of a generator of C under some derivation $C \longrightarrow B/D$ if and only if that element lies in $\ker\phi$; once we know how a derivation acts on a given generator of C, there is no doubt how it must act on the other elements of C; hence $\mathrm{Der}(C, B/D)$ is A-isomorphic to $\ker\phi$. This isomorphism maps $\mathrm{Ider}(C, B/D)$ onto $[C, B/D]$. Since B/D is cyclic, the subgroups $\ker\phi$ and $[C, B/D]$ are also cyclic. It now follows that $\mathrm{Der}(C, B/D)$, $\mathrm{Ider}(C, B/D)$ and the quotient $H^1(C, B/D)$ are all cyclic. It is now sufficient to know the orders of the groups only. We list the orders here.

Lemma 5.3.6

(i) $|\mathrm{Der}(C, B/D)| = |\ker\phi| = \gcd(|B/D|, \frac{p^{k|A|}-1}{p^{k|A:C|}-1})$;

(ii) $|\mathrm{Ider}(C, B/D)| = \frac{|B/D|}{\gcd(|B/D|, p^{k|A:C|}-1)}$.

5.4 Listing Problem

Let a and b be fixed generators of A and B, respectively, chosen so that $b^a = b^{p^k}$. To list the subgroups C of A is a simple matter: set $C = \langle a^u \rangle$ with u ranging through all positive divisors of $|A|$, noting that $|A/C| = u$. Similarly, the subgroups D of B are the $\langle b^v \rangle$ with $v \mid |B|$, and $|B/D| = v$. Having chosen u and v (that is , C and D) in this manner, we aim to list first all derivations $\delta : C \longrightarrow B/D$. Using Lemma 5.3.6, calculate $m = m(u,v) := |B/D : \ker\phi|$; then $\ker\phi = \langle b^m D \rangle$; to each integer i there is a unique derivation δ with $a^u\delta = b^{mi}D$, and each derivation $\delta : C \longrightarrow B/D$ arises in this way. If $a^u\delta = b^{mi}D$ then the subgroup $[C, D, \delta]$ is $\langle a^u b^{mi}, b^v \rangle$: we shall denote this group here by $G(u,v,i)$, or simply by $G(i)$ when u and v are kept fixed for the time being. The subgroups $G(u,v,i)$ are then precisely the subgroups H with $A \cap HB = \langle a^u \rangle$, $H \cap B = \langle b^v \rangle$.

Using Lemma 5.3.6 as well, calculate $h = h(u,v) := |H^1(C, B/D)|$; from the foregoing we know that $G(u,v,i) = G(u',v',i')$ if and only if $u = u'$, $v = v'$, and $i \equiv i' \bmod v/m$. From Lemma 5.3.1, therefore the $G(u,v,i)$ with $1 \leq i \leq v/m$ are pairwise distinct, and each subgroup of Q is of this form. We also know from Corollary 5.3.5 that $G(u,v,i)$ is conjugate in Q to $G(u,v,j)$ if and only if $ip^{kr} \equiv j \bmod h(u,v)$ for some r with $1 \leq r \leq u$. Using this, we may write a simple algorithm to produce a list $\mathcal{L} = \mathcal{L}(u,v)$ of integers i which provide a complete set of representatives of conjugacy classes of $\{G(i) : i \in \mathbf{Z},\ 1 \leq i \leq h\}$.

Step 1) set $i = 1$ and $\mathcal{L} = \varnothing$

Step 2) compute $ip^k, ip^{k2}, ..., ip^{ku}$

Step 3) if one of these is congruent modulo h to an element of $\mathcal{L}$,

replace i by $i+1$

else replace $\mathcal{L}$ by $\mathcal{L} \cup \{i\}$ and replace i by $i+1$

Step 4) if $i > h$, stop and print $\mathcal{L}$

else go to Step 2.

From Lemma 5.3.1, the set

$$\{\, G(u,v,i) : u \mid |A|,\ v \mid |B|,\ i \in \mathcal{L}(u,v) \,\}$$

is a complete and irredundant set of representatives of the Q-conjugacy classes of the subgroups of Q.

When the degree n is a power of an odd prime q (equivalently, Q is a q-group), we can explicitly list a complete and irredundant set of representatives of Q-conjugacy classes of subgroups of Q. We discuss this for the remainder of this section. If Q is cyclic, the problem is a trivial matter and so we assume Q is not cyclic, or equivalently q divides p^k-1.

For this purpose we have to observe how the conjugacy depends on the parameter i when the other parameters are fixed. We first state an immediate consequence of Corollary 5.3.5.

Lemma 5.4.1 (i) *The length of the A-orbit containing $v + \mathrm{Ider}(C, B/D)$ is $|p^k \bmod d|$, where d is the order of $v + \mathrm{Ider}(C, B/D)$ in $H^1(C, B/D)$.*

(ii) *There are exactly*

$$\sum_{C \le A, D \le B} \ \sum_{d \mid |H^1(C,B/D)|} \frac{\varphi(d)}{|p^k \bmod d|}$$

Q-conjugacy classes of subgroups of Q.

Then we prove the following lemma.

Lemma 5.4.2 *Suppose Q is a q-group for some odd prime q. Then $G(i)$ is conjugate to $G(j)$ if and only if (q-component of i) $=$ (q-component of j) and (q'-component of i) $\equiv$ (q'-component of j) $\bmod \gcd(p^k-1, d)$ where d is the quotient of h by the common q-component of i and j.*

Proof Let $s(i)$ be the q'-component of i and $t(i)$ be the q-component of i. From Corollary 5.3.5, we know that the two groups are conjugate in Q if and only if

$i \equiv p^{kr} j \bmod h$ for some integer r. Therefore if the two groups are conjugate in Q, then $t(i) = t(j)$. Then

$$s(i) - s(j) \equiv (p^{kr}-1)s(j) \bmod d.$$

So

$$s(i) \equiv s(j) \bmod (p^k-1, d).$$

Thus there are at least $\varphi(\gcd(p^k-1, d))$ different Q-conjugacy classes of subgroups with the fixed parameters $G(i)$ with $t(i) = h/d$. But from Lemma 5.4.1, there are precisely $\varphi(d)/|p^k \bmod d|$ different Q-conjugacy classes of such subgroups. It is routine to show that the number is exactly equal to $\varphi(\gcd(p^k-1, d))$. So the lemma is now proved. □

Corollary 5.4.3 *Suppose n is a power of an odd prime q. Let r be the q-component of p^k-1. Define $h = h(u,v) := \min(n/u, nr/v, ru, v)$ and define $m = m(u,v) := \max(1, uv/n)$. Then the set*

$$\{\, \langle a^u b^{mst}, b^v \rangle : 1 \leq s,t,u,v \in \mathbb{Z},\ u \mid n,\ v \mid nr,\ t \mid h,\ s < (p^k-1, h/t),\ (s,q) = 1 \}$$

is a complete and irredundant set of representatives of the Q-conjugacy classes of subgroups of Q.

Chapter 6

Conclusion

- towards an algorithm

Our motivation was to have an algorithm for generating computer libraries of finite soluble primitive permutation groups with metacyclic point stabilizers. A classical result, essentially due to Galois [see Huppert (1967, Theorem II.3.2)], shows that the permutation isomorphism types of finite soluble primitive permutation groups correspond one-to-one to the linear isomorphism types of finite soluble irreducible linear groups over finite prime fields. This result reduces the problem to that of determining the irreducible metacyclic subgroups of the general linear groups over finite prime fields. In this point of view, we are interested in listing representatives of the conjugacy classes of metacyclic irreducible subgroups of the general linear group $GL(n, \mathsf{F})$ over a finite field F. We conclude with some comments on this line.

In Chapter 3 we discussed the abstract isomorphism types of metacyclic groups of odd order. The results are explicit enough to give a practical algorithm to list complete and irredundant sets of representatives of the isomorphism types of all metacyclic groups of odd order. Chapter 4 provides some theoretical basis to determine the linear isomorphism types of the images of the faithful irreducible representations of a given metacyclic group of odd order. Utilizing the

results in the two chapters, it may be possible to design a practical algorithm to list representatives of the conjugacy classes of metacyclic irreducible subgroups of odd order in $GL(n, \mathsf{F})$.

The algorithm would be composed of the following processes.

Produce a complete and irredundant list $\mathcal{L}$ of representatives of the abstract isomorphism types of metacyclic irreducible subgroups of odd order in $GL(n, \mathsf{F})$.

Construct the equivalence classes of irreducible representations of $Z(F)$ with core-free kernel of each metacyclic group G in the list $\mathcal{L}$.

Determine the $(\mathrm{Aut}\, G)\downarrow_{Z(F)}$-orbits of the equivalence classes obtained in the second process for each G on the list $\mathcal{L}$.

Calculate one irreducible constituent of the induced representation $\lambda\uparrow^G$ of one representative λ of each orbit in the third process for each G in the list $\mathcal{L}$.

List the images of the irreducible constituents obtained in the above process.

Theorem 4.5.1 guarantees that the list obtained in the last process is a complete and irredundant list of representatives of the linear isomorphism types of all metacyclic irreducible subgroups $GL(n, \mathsf{F})$.

In order to carry out each process, we need to know how to calculate explicitly the following, for each relevant group G.

The centre $Z(G)$.

The Fitting subgroup F and its centre $Z(F)$.

The core-free subgroups L of $Z(F)$ with cyclic quotient.

The restriction of the automorphism group, $(\mathrm{Aut}\, G)\downarrow_{Z(F)}$.

For the first process, we can explicitly choose an 'initial list' containing exactly one representative from each isomorphism type of metacyclic group of odd order, up to some limit of orders, in terms of our standard presentations discussed in

Chapter 3, or in terms of the corresponding metacyclic presentations indicated in Remark 3.4.2. We may choose the initial list so that it includes only those groups of order at most $n(|\mathsf{F}|^n-1)^2$, which is an upper bound of the orders of those subgroups in $GL(n,\mathsf{F})$. Using the results of Section 4.2 and Section 4.3, we can then choose those groups from the initial list which have faithful irreducible representations of the degree n.

In the second process, to construct equivalence types of irreducible representations of the centre of the Fitting subgroup with core-free kernel, we need to determine all core-free subgroups of $Z(F)$ with cyclic quotient. Then we can make use of the representation theory of finite cyclic groups to determine the equivalence types of relevant irreducible representations of the centre of the Fitting subgroup. For the third process, it is necessary to calculate $(\mathrm{Aut}\, G)\downarrow_{Z(F)}$. General algorithms for computing automorphism groups would not be efficient here, but at this stage, we have not explored how one might take advantage of special features (such as the metacyclic nature of G) in computing $(\mathrm{Aut}\, G)\downarrow_{Z(F)}$. The fourth process, as described, would involve finding an irreducible constituent of an induced representation. Again, using a general program of this kind is unlikely to be an efficient way; one should seek to exploit special features. (For example, if the field is large enough, the problem is very easy because of Corollary 4.2.3, so it may be better to proceed via changing fields.)

The possible steps listed here indicate our state of knowledge at the time of writing; many of the steps have not been explored at all, and we do not know which will be hard and which may be easy.

An alternative approach may be to write metacyclic irreducible subgroups directly by an internal way. In fact every metacyclic irreducible linear group of a given degree n is linearly isomorphic to a subgroup of a certain wreath product of a metacyclic primitive linear group of degree m for some positive divisor m of n and a metacyclic transitive subgroup of a symmetric group of degree n/m, which is embedded in the general linear group in a natural way. For relatively

small degrees, it might be possible to reach the goal by investigating the subgroups in question of such wreath products. Short (1990) succeeded in listing all irreducible soluble subgroups of $GL(n,p)$ with $p^n < 256$ by this approach. As we have shown in Chapter 5, if we are only interested in metacyclic primitive linear groups, this direct approach is the more economical. However, this approach is unlikely to produce a complete list of the linear isomorphism types of all metacyclic irreducible subgroups of $GL(n,p)$ in general, because of the gradually increasing complexity of the groups concerned.

Bibliography

Reinhold Baer (1944), "Crossed isomorphisms", *Amer. J. Math.*, **66**, 341–404.

B.G. Basmaji (1969), "On the isomorphisms of two metacyclic groups", *Proc. Amer. Math. Soc.*, **22**, 175–182.

H. Bechtell (1991), "On semidirect products", *Comm. Algebra*, **19**(4), 1151–1163.

F.R. Beyl (1972), *The classification of metacyclic p-groups, and other applications of homological algebra to group theory*, PhD thesis. Cornell University.

F. Rudolf Beyl and Jürgen Tappe (1982), *Group Extensions, Representations, and the Schur Multiplicator*, Lecture Notes in Math., **958**. Springer-Verlag, Berlin, Heidelberg, New York.

W. Burnside (1911), *Theory of Groups of Finite Order* (2nd edition). Cambridge University Press. Reprinted by Dover 1955, New York.

S.B. Conlon (1976), "p-groups with an abelian maximal subgroup and cyclic center", *J. Austral. Math. Soc. Ser. A*, **22**, 221–233.

S.B. Conlon (1977), "Nonabelian subgroups of prime-power order of classical groups of the same prime degree", R.A. Bryce, J. Cossey and M.F. Newman (Eds.), *Group Theory* (Canberra, 1975), Lecture Notes in Mathematics, **573**, pp. 17–50. Springer-Verlag, Berlin, Heidelberg, New York.

H.S.M. Coxeter and W.O.J. Moser (1980), *Generators and Relations for Discrete Groups* (4th edition), Ergeb. Math. Grenzgeb., **14**. Springer-Verlag, Berlin, Göttingen, Heidelberg.

C.W. Curtis and I. Reiner (1962), *Representation Theory of Finite Groups and Associative Algebras* (2nd edition), Pure and Appl. Math., **11**. Interscience, New York.

Walter Feit (1982), *The Representation Theory of Finite Groups*, North-Holland Mathematical Library, **25**. North-Holland Publishing Co., Amsterdam, New York, Oxford.

Wolfgang Gaschütz (1954), "Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen", *Math. Nachr.*, **12**, 253–255.

Leonhard Gerhards (1970), "Über modulare bizyklische Gruppen", Berichte **29**, Gesellschaft für Mathematik und Datenverarbeitung, Bonn.

Daniel Gorenstein (1968), *Finite Groups.* Harper's Series in Modern Mathematics. Harper & Row, New York, Evanston, London.

Marshall Hall, Jr. (1959), *The Theory of Groups.* Macmillan Co., New York.

Derek F. Holt and W. Plesken (1989), *Perfect Groups.* Clarendon Press, Oxford.

Derek F. Holt and Sarah Rees (1991), "A graphics system for displaying finite quotients of finitely presented groups", *Preprint.*

B. Huppert (1967), *Endliche Gruppen I.* Grundlehren Math. Wiss., **134**. Springer-Verlag, Berlin, Heidelberg, New York.

B. Huppert and N. Blackburn (1982), *Finite Groups II*, Grundlehren Math. Wiss., **242**. Springer-Verlag, Berlin, Heidelberg, New York.

I.M. Isaacs (1976), *Character Theory of Finite Groups*, Pure and Applied Mathematics, **69**. Academic Press, Berlin, Heidelberg, New York.

Alfred W. Jones (1945), "The lattice isomorphisms of certain finite groups", *Duke Math. J.*, **12**, 541–560.

Bruce W. King (1973), "Presentations of metacyclic groups", *Bull. Austral. Math. Soc.*, **8**, 103–131.

Rudolf Kochendörffer (1948), "Über treue irreduzible Darstellungen endlicher Gruppen", *Math. Nachr.*, **1**, 25–39.

Wolfgang Lindenberg (1970a), "Über die Struktur zerfallender bizyklischer p-Gruppen", *J. Reine Angew. Math.*, **241**, 118–146.

Wolfgang Lindenberg (1970b), "Über die Struktur zerfallender nicht-modularer bizyklischer 2-Gruppen", Berichte **29**, Gesellschaft für Mathematik und Datenverarbeitung, Bonn.

Wolfgang Lindenberg (1971), "Struktur und Klassifizierung bizyklischer p-Gruppen", Berichte **40**, Gesellschaft für Mathematik und Datenverarbeitung, Bonn.

M.F. Newman (1977), "Determination of groups of prime-power order", *Group Theory* (Canberra, 1975), Lecture Notes in Math., **573**, pp. 73–84. Springer-Verlag, Berlin, Heidelberg, New York.

M.F. Newman and Mingyao Xu (1988), "Metacyclic groups of prime-power order", *Adv. in Math.* (*Beijing*), **17**, 106–107.

M.F. Newman and Ming-Yao Xu (1990), "Metacyclic groups of prime-power order", *Preprint.*

E.A. O'Brien (1990), "The p-group generation algorithm", *J. Symbolic Comput.*, **9**, 677–698.

László Rédei (1989), *Endliche p-Gruppen.* Akadémiai Kiadó, Budapest.

Robert Remak (1930), "Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte", *J. Reine Angew. Math.*, **163**, 1–44.

Derek J. Robinson (1981), "Applications of cohomology to the theory of groups", C.M. Campbell and E.F. Robertson (Eds.), *Group-St Andrews 1981*, LMS Lecture Note, **71**, pp. 46–80.

Derek J. Robinson (1982), *A Course in the Theory of Groups*, Graduate Texts in Math., **80**. Springer-Verlag, New York, Heidelberg, Berlin.

John S. Rose (1978), *A Course on Group Theory.* Cambridge University Press, London, New York, Melbourne.

Mark Short (1990), *The primitive soluble permutation groups of degree less than* 256, PhD thesis. Australian National University.

D. Suprunenko (1963), *Soluble and Nilpotent Linear Groups*, Translations of Mathematical Monographs, **9**. Amer. Math. Soc., Providence, Rhode Island.

Michio Suzuki (1956), *Structure of a Group and the Structure of its Lattice of Subgroups*, Ergeb. Math. Grenzgeb. **10**. Springer-Verlag, Berlin, Göttingen, Heidelberg.

Michio Suzuki (1982), *Group Theory I*, Grundlehren Math. Wiss., **247**. Springer-Verlag, Berlin, Heidelberg, New York.

Michio Suzuki (1986), *Group Theory II*, Grundlehren Math. Wiss., **248**. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo.

Louis Weisner (1939), "Condition that a finite group be multiply isomorphic with each of its irreducible representations", *Amer. J. Math.*, **61**, 709–712.

Hans J. Zassenhaus (1958), *The Theory of Groups* (2nd edition). Chelsea Publishing Company, New York.

List of notation

Z	set of all integers
$\mathsf{F}^\times$	multiplicative group of nonzero elements of a field F
F_p	prime field of order p
$\lvert X\rvert$	cardinality of X
$a \mid b$	a divides b
$(a\lvert b)$	(see Notation 3.4.1)
$a \equiv b \bmod m$	m divides $a - b$
$\lvert r \bmod m\rvert$	multiplicative order of $r \bmod m$ (see Section 1.3)
(a, b), $\gcd(a, b)$	greatest common divisor of a and b
$n(p)$	largest integer i such that p^i divides n
$\min(x, y, ...)$	minimal element of $x, y, ...$
$\max(x, y, ...)$	maximal element of $x, y, ...$
$\langle X\rangle$	subgroup generated by X
$\mathsf{C}(n)$	cyclic group of order n
$H \leq G$	H is a subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
G/N	quotient of G by N
$\lvert G : N\rvert$	index of N in G
HK	$\{hk : h \in H, k \in K\}$
$H \times K$	cartesian product/direct product of H and K
$\prod_i G_i$	direct product of the G_i
$P \ltimes_\phi Q$	semidirect product of P and Q (see Section 1.3)

$Z(G)$	centre of G
$\Phi(G)$	Frattini subgroup (see Section 1.3)
$\Omega_1(P)$	subgroup of generated by elements of order p of P
$\mathrm{Fit}\, G$	Fitting subgroup (see Section 1.3)
$\exp G$	exponent of G
$\mathrm{core}_G X$	core of X in G (see Section 1.3)
$\mathrm{Aut}\, G$	automorphism group of G
$\mathrm{Gal}(\mathsf{E}\|\mathsf{F})$	Galois group of E over F
$\mathrm{Hom}(X, Y)$	group of homomorphisms of X into Y
$\mathsf{C}_G(H)$	centralizer of H in G
$\mathsf{N}_G(H)$	normalizer of H in G
y^x	$x^{-1}yx$
$[x, y]$	$x^{-1}y^{-1}xy$
$[X, Y]$	subgroup generated by $[x, y]$, $x \in X, y \in Y$
G'	commutator subgroup of G
G^n	$\langle g^n : g \in G \rangle$
$GL(V)$	group of invertible linear transformations of V
$GL(n, \mathsf{F})$	general linear group of degree n over F
x^g	image of x under action of g
$\mathsf{N}_{\mathrm{Aut}P}(C)\downarrow_{P/C}$	(see Section 1.3)
$\dim_{\mathsf{F}} V$	dimension of V over F
$[V]$	isomorphism class of V
$\ker V$	kernel of V (see Section 2.3)
$U \# V$	outer tensor product of U and V
$V^{\oplus m}$	direct sum of m copies of V
$V\uparrow^G$	module induced to G (see Section 2.3)
$V\downarrow_H$	module restricted to H (see Section 2.3)
V^*	dual module of V
$\mathrm{End}_R V$	R-endomorphism ring of V

V^α	conjugate of V by α (see Section 2.3)
$[\rho]$	equivalence class of ρ
$\rho\uparrow^G$	representation induced to G
$\rho\downarrow_H$	representation restricted to H
$W \in \mathrm{Irr}_{\mathbf{F}} N$	(see Section 4.4)
$[\mathrm{Irr}^*_{\mathbf{F}} N]/H$	(see Section 4.4)