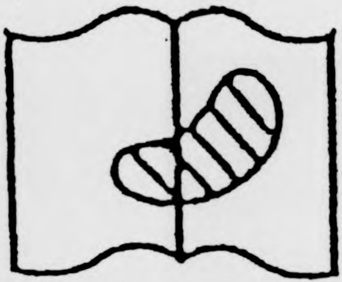
Retrieving information about a group from its character table

Sandro Mattarei

Thesis submitted for the degree of Doctor of Philosophy
of the University of Warwick

Mathematics Institute
University of Warwick
Coventry
CV4 7AL

July 1992



Contents

Acknowledgements

I would like to thank my research supervisor Dr T. O. Hawkes for his constant support.

I acknowledge the financial support of CNR (Consiglio Nazionale delle Ricerche, Italy).

Declaration

The work contained in this thesis is original except where otherwise indicated.

Summary

This thesis concerns character tables of finite soluble groups. In particular, our main objective is that of showing that the derived length of a soluble group G is not determined by the character table of G. In fact, in Chapters 5 and 6 we shall construct pairs (G, H) of groups which have identical character tables but different derived lengths, namely 2 and 3. A more general result will be proved in Chapter 7, namely that for any natural number $n \geq 2$, there exist pairs (G, H) of groups with identical character tables, and derived lengths n and $n+1$ respectively. Two by-products of our investigation are a method for comparing character tables in special situations (in Chapter 4), and a description of the character tables of wreath products (in Chapter 7).

Chapter 1

Introduction

Representation theory, and in particular character theory, have proved to be powerful tools for the study of finite groups. Furthermore, character theory provides a practical way of gathering a lot of information about a group G in a very condensed form, by means of a matrix with complex entries, called the *character table* of G. This is especially true for simple groups. In fact, character tables are perhaps the main information provided by the *Atlas of finite simple groups* [4], which is an indispensable reference for the classification of the finite simple groups. Each finite simple group is uniquely identified by its character table, and some sporadic simple groups were known through their character tables even before their existence was proved.

The character table of a finite group G is the matrix T (which turns out to be square), whose (i,j)th entry is $\chi_i(g_j)$, where $\chi_1, \ldots, \chi_k$ are the irreducible characters of G (over the complex field), and $g_1, \ldots, g_k$ are a set of representatives for the conjugacy classes $\mathcal{K}_1, \ldots, \mathcal{K}_k$ of G (with $g_j \in \mathcal{K}_j$). Since characters are class functions, the character table T is not affected by the choice of different representatives $g_j' \in \mathcal{K}_j$, and thus the columns of T will also be indexed by the conjugacy classes of G. It also follows from this that the knowledge of the character table T of G amounts to the knowledge of all irreducible characters of G, as functions from G into $\mathbb{C}$, once one knows the correspondence between rows of T and irreducible characters of G, and the correspondence between columns of T and conjugacy classes of G. These correspondences will not be considered part of the object *character table*, nor will any other information about G and its characters, like orders of the elements, or Frobenius-Schur indicators. An additional piece of information, namely the so-called power-maps, will be considered occasionally, but this will be explicitly stated as *character table with powermaps*.

Unlike simple groups, soluble groups are not uniquely identified by their character tables. The easiest example is given by the two non-abelian groups of order eight, namely the dihedral group D_8 and the quaternion group Q_8; in fact, their common character table is the following matrix T.

$$T = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{vmatrix}$$

We may notice that the first row of T corresponds to the trivial character of G, and the first column corresponds to the identity class of G. Apart from this, which we shall adopt as a convention, there is no natural rule for ordering the conjugacy classes of G and its irreducible characters (though practical rules are used in [4], for the sake of convenience). Consequently, the character table T of a group G is defined up to permutations of its rows and of its columns. Hence, we shall say that the character tables T_1 and T_2 of two groups are identical if it is possible to obtain T_2 from T_1 by permuting rows and columns of T_1. Later we shall give a more handy definition of having identical character tables, namely Definition 2.7.1.

We shall see in Chapter 4 that D_8 and Q_8 form just a special case of a more general situation in which two groups have identical character tables.

Although a group G is not uniquely determined by its character table T, a lot of properties of G can be read off from T. We shall give a brief review of some of these properties, after noticing that each property can usually be obtained from T in several ways.

A first class of properties employs the so-called *second orthogonality relation*, part of which is the formula

$$|\mathbf{C}_G(g_j)| = \sum_{i=1}^{k} |\chi_i(g_j)|^2,$$

which allows one to compute the order of the centralizer of an element of the class K_j by means of the corresponding column of T. In particular, for the identity class $\mathcal{K}_1$, the above formula becomes

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2,$$

and thus yields the order of G. As a consequence, the length of each conjugacy class $\mathcal{K}_j$ of G can be computed, because $|\mathcal{K}_j| = |G : \mathbf{C}_G(g_j)|$. Also, the columns of T which correspond to central elements of G can be determined, and thus the order of the centre of G can be computed. It follows that it can be decided whether G is abelian (though a simpler method for this is checking that all characters of G have degree 1). If this is the case, then G is determined by T up to isomorphism. More generally, $\mathbf{Z}(G)$ is always determined by T up to isomorphism.

The second class of properties which we are going to examine employs the fact that the kernels of the irreducible characters can be read off from the character table (meaning that it can be decided which classes of G are contained in the kernel of a given irreducible character); in fact, it is easy to see that

$$\ker \chi = \{g \in G \mid \chi(g) = \chi(1)\},$$

if $\chi \in \mathrm{Irr}(G)$. Now, kernels of characters are normal subgroups of G, and conversely, each normal subgroup N of G is the kernel of some character of G, for instance the character afforded by the regular representation of G/N, viewed as a representation of G. Since the kernel of a reducible character is the intersection of the kernels of its irreducible constituents, it follows that all normal subgroups of G can be found from T, as intersections of kernels of irreducible characters. Moreover, since each normal subgroup N of G is found as a union of conjugacy classes of G, its order can be computed, and inclusion relations with other normal subgroups can be determined.

To summarize, from T we read the lattice of normal subgroups of G, each with its order attached. But we can do more: for each normal subgroup N, the character table of the factor group G/N can be extracted from T, simply by deleting those rows of T which correspond to irreducible characters χ such that $N \nleq \ker \chi$, and then replacing each set of identical columns with a single one. Let us remark that a similar procedure for obtaining the character table of the normal subgroup N does not exist. For instance, D_8 has exactly three normal subgroups of order 4, which are indistinguishable by looking at the character table of D_8; yet they do not have identical character tables, because one of them is cyclic, and the other two are elementary abelian.

The knowledge of the lattice of normal subgroups of G, together with the character tables of the corresponding factor groups, allows one to decide about the nilpotency, supersolubility, or solubility of G. In fact, G is nilpotent, respectively supersoluble, or soluble, if and only if there is a normal series

$$1 = N_0 < N_1 < \cdots < N_s = G,$$

such that all factors N_i/N_{i-1} are central, respectively cyclic of prime order, or p-groups; all of these conditions can be checked on the character table T of G.

The terms of the upper central series of G can be inductively located in T, by taking centres and factor groups in turns; in particular, if G is nilpotent, its nilpotency class is determined by T.

The lower central series of G can also be found, for instance by inspecting all central series descending from G and finding the fastest descending one. However, another method is available, which yields even more. In fact, it follows by induction from [13, Problem 3.10(a)] that the character table of G allows one to decide which conjugacy classes of G contain elements of the form $g = [x_1, \dots, x_i]$ with $x_1, \dots, x_i \in G$; these conjugacy classes generate $\gamma_i(G)$, the ith term of the lower central series, though their (set-theoretical) union may be properly contained in $\gamma_i(G)$.

Inspection of the lattice of normal subgroups of G (with orders) shows which normal subgroups N are nilpotent: they are exactly those which contain normal subgroups of G of order $|N|_p$ for all prime divisors p of $|N|$ (here, as usual, $|N|_p$ denotes the biggest power of p which divides the order of N). As a consequence, the Fitting subgroup of G can be found (as the biggest nilpotent normal subgroup of G); hence, if G is soluble, the Fitting series of G can be determined inductively, and the Fitting length can be computed.

What about the derived series of G (and in particular the derived length of G, if G is soluble)? The derived subgroup G' can certainly be read off from T, as the smallest normal subgroup N of G such that G/N is abelian, or equivalently as the intersection of the kernels of all linear characters of G. The problem of finding the second derived subgroup G'' amounts to being able to tell whether G' is abelian from the character table of G. The following more general question appeared as Problem 10 in R. Brauer's report on representations of finite groups, in [19, page 141]:

Given the character table of a group G and the set of conjugacy

> *classes of G which make up a normal subgroup N of G, can it be decided whether or not N is abelian?*

As Brauer then remarked, a positive answer to this question would allow one to identify the terms of the derived series of G by looking at its character table, and in particular to compute the derived length of G, for G soluble.

Unfortunately, the answer to Brauer's Problem 10 is negative, as announced by A. I. Saksonov in [20]. A computational approach to this problem has been used recently by K. Dockx and P. Igodt in [7], which led to the same conclusion and produced additional examples. However, neither Saksonov, nor Dockx and Igodt, answered Brauer's question about the derived length.

One of the main results in this thesis is the construction of groups G and H with identical character tables and derived lengths 2 and 3 respectively, which proves that the derived length of a soluble group cannot be read off from its character table. This will be done in Chapter 5.

The discovery of the above mentioned examples was a consequence of the close study of the structure of a minimal example of groups with identical character tables and different derived lengths. This study is also part of this thesis, and will be carried out in Chapter 3.

Chapter 6 is devoted to the construction of another example of groups with identical character tables and derived lengths 2 and 3. The groups of this example are p-groups, unlike those of Chapter 5, which are not nilpotent. The existence of this chapter is justified by the fact that the discussion of a minimal example in Chapter 3 is carried out under the assumption that the groups in question are not nilpotent.

A tool for the comparison of character tables will be developed in Chapter 4. Being suited to our examples of Chapters 5 and 6, it concerns a rather special configuration, that of Camina groups. However, since Camina groups have been studied extensively, and seem to arise in many different situations, the results of this chapter may prove useful elsewhere.

Early and shorter versions of Chapters 4 and 5 will appear together as an article (namely [17]), in the Journal of the London Mathematical Society.

The final chapter of this thesis, namely Chapter 7, concerns character tables of wreath products. We shall prove that the character table of a wreath product $G \wr A$ is completely determined by the permutation group A and the character table of G. An almost immediate consequence of this fact is the construction of pairs (G, H) of groups with identical character tables and derived lengths n and $n+1$, for any given integer $n \geq 2$.

Some more or less standard results from group theory and representation theory, which we shall need, are collected in Chapter 2.

Chapter 2

Technical results

2.1 Commutators

We shall use the standard notation of [10] for commutators. In particular, if A and B are subsets of a group G, we set

$$[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle.$$

However, it will be useful to have a notation also for the set of commutators $[a, b]$ with $a \in A$ and $b \in B$. Thus, we shall occasionally use the following non-standard notation:

$$\lfloor A, B \rfloor = \{[a, b] \mid a \in A,\ b \in B\}.$$

If $G_1, \dots, G_n$ are subsets of G, we set

$$[G_1, \dots, G_n] = \langle [g_1, \dots, g_n] \mid g_i \in G_i \rangle,$$

where $[g_1, \dots, g_n]$ is defined recursively by the formula

$$[g_1, \dots, g_n] = [[g_1, \dots, g_{n-1}], g_n].$$

We observe that

$$[G_1, \dots, G_n] \le [\dots [[G_1, G_2,], G_3], \dots, G_n],$$

though equality does not hold in general.

We shall need the following well-known lemma about coprime actions.

Lemma 2.1.1 *Let A be a Q-group, with $(|A|, |Q|) = 1$. Then*

$$[[A, Q], Q] = [A, Q],$$

and

$$A = [A, Q]\mathbf{C}_A(Q).$$

Furthermore, if A is abelian, then

$$A = [A, Q] \times \mathbf{C}_A(Q).$$

Proof Our first statement is [10, Kapitel III, Hilfssatz 13.3 b)], from whose proof our second statement follows. Our third statement is [10, Kapitel III, Satz 13.4 b)]. □

2.2 Linear and bilinear maps arising from commutation

Lemma 2.2.1 *Suppose that H_1, H_2, H_3, K_1, K_2, K_3 are subgroups of a group G. Suppose that $K_i \lhd H_i$ and that H_i/K_i is abelian ($i = 1, 2, 3$). Suppose also that $[H_1, H_2] \leq H_3$ and that $[H_1, K_2]$, $[K_1, H_2]$, $[H_1, H_2, H_1]$ and $[H_1, H_2, H_2]$ are all contained in K_3. Then there exists a $\mathbb{Z}$-bilinear map $\gamma : H_1/K_1 \times H_2/K_2 \to H_3/K_3$ such that*

$$(xK_1, yK_2)^\gamma = [x, y]K_3 \text{ for all } x \in H_1 \text{ and for all } y \in H_2.$$

Furthermore, if $H_1 = H_2$ and $K_1 = K_2$, then the map γ is skew-symmetric, in other words $(xK_1, xK_2)^\gamma = K_3$ for all $x \in H_1$.

Proof This lemma is a slightly more general form of [11, Chapter VIII, Lemma 6.1] and can be proved in the same way. The last statement of the lemma is obvious. □

If H_i/K_i has exponent p for $i = 1, 2, 3$, where p is a prime, then each H_i/K_i can be regarded as a vector space over the field $\mathbf{F}_p$, and the map γ is obviously $\mathbf{F}_p$-bilinear.

A different formulation of Lemma 2.2.1 is that (with the given hypotheses) the map

$$\varphi_y : H_1/K_1 \to H_3/K_3$$

such that $(xK_1)^{\varphi_y} = [x, y]K_3$ is a well-defined group homomorphism for all $y \in H_2$, and the map

$$\gamma : H_2/K_2 \to \mathrm{Hom}(H_1/K_1, H_3/K_3)$$

such that $(yK_2)^\gamma = \varphi_y$ is also a well-defined group homomorphism. More generally we have the following result.

Lemma 2.2.2 *Assume the hypotheses of Lemma 2.2.1. In addition, suppose that Q is a group of operators for G and that H_i and K_i are Q-subgroups of G, whence in particular H_i/K_i becomes a $\mathbf{Z}Q$-module ($i = 1, 2, 3$). Suppose also that Q centralizes H_2/K_2. Then the map*

$$\varphi_y : H_1/K_1 \to H_3/K_3$$

such that $(xK_1)^{\varphi_y} = [x, y]K_3$ for all $x \in H_1$ is well defined and a $\mathbf{Z}Q$-module homomorphism for all $y \in H_2$, and the map

$$\gamma : H_2/K_2 \to Hom_{\mathbf{Z}Q}(H_1/K_1, H_3/K_3)$$

such that $(yK_2)^\gamma = \varphi_y$ for all $y \in H_2$ is well defined and a group homomorphism.

Proof The fact that φ_y is a group homomorphism for all $y \in H_2$ follows easily from Lemma 2.2.1. In order to show that the maps φ_y are actually $\mathbf{Z}Q$-homomorphisms it is sufficient to notice that for all $x \in H_1$, $y \in H_2$ and $\xi \in Q$ we have

$$\begin{aligned}((xK_1)^{\varphi_y})^\xi &= [x, y]^\xi K_3 = [x^\xi, y^\xi]K_3 \\ &= (x^\xi K_1, y^\xi K_2)^\gamma = (x^\xi K_1, yK_2)^\gamma = (x^\xi K_1)^{\varphi_y}.\end{aligned}$$

This proves that $\varphi_y \in \mathrm{Hom}_{\mathbf{Z}Q}(H_1/K_1, H_3/K_3)$. It is an easy consequence of Lemma 2.2.1 that γ is a group homomorphism. □

Later on, namely in Section 3.4, we shall see how to handle also the case in which Q does not centralize H_2/K_2. For the moment, let us suppose that we are interested in obtaining a single homomorphism $\varphi_w : H_1/K_1 \to H_3/K_3$ (defined as in Lemma 2.2.2) for a fixed $w \in H_2$. We may apply Lemma 2.2.2 with $H_2 = \langle w \rangle$ and $K_2 = 1$, but since now we do not care anymore about the linearity of φ_w with respect to w we may find the hypotheses of Lemma 2.2.2 too restrictive (for instance we may wish to replace $[H_1, \langle w \rangle] \leq H_3$ with the weaker assumption $[H_1, w] \leq H_1$). In the following lemma we shall also drop the assumption that the factor groups H_1/K_1 and H_3/K_3 are abelian (notice that the subgroups H_3 and K_3 will be renumbered).

Lemma 2.2.3 *Suppose that H_1, H_2, K_1, K_2 are subgroups of a group G, with $K_i \lhd H_i$ $(i = 1, 2)$. Let us fix an element w of G and suppose that $[H_1, w] \leq H_2$ and that $[K_1, w]$ and $[H_1, w, H_1]$ are contained in K_2. Then the map*

$$\varphi_w : H_1/K_1 \to H_2/K_2$$

such that $(xK_1)^{\varphi_w} = [x, w]K_2$ for all $x \in H_1$ is well defined and a group homomorphism. Furthermore, if Q is a group of operators for G which centralizes w and if H_1, H_2, K_1, K_2 are Q-subgroups of G, then the map φ_w is a Q-homomorphism.

Proof Since $[H_1, w] \leq H_2$, we have $[x, w] \in H_2$ for all $x \in H_1$. The following commutator identity holds for all $x, y \in G$:

$$[xy, w] = [x, w]^y [y, w] = [x, w]\,[x, w, y]\,[y, w].$$

If $x \in H_1$ and $y \in K_1$, then we have $[x, w, y] \in K_2$ because $[H_1, w, K_1] \leq K_2$, and $[y, w] \in K_2$ because $[K_1, w] \leq K_2$; hence $[xy, w]K_2 = [x, w]K_2$, and this shows that the map φ_w is well defined. For $x, y \in H_1$ we have $[x, w, y] \in K_2$ since $[H_1, w, H_1] \leq K_2$, and this proves that φ_w is a group homomorphism. Now suppose that the group Q acts on G by automorphisms normalizing H_1, H_2, K_1, K_2 and centralizing w. In particular Q acts on H_1/K_1 and H_2/K_2. Then, for all $x \in H_1$ and $\xi \in Q$, we have

$$\begin{aligned} ((xK_1)^{\varphi_w})^{\xi} &= [x, w]^{\xi} K_2 = [x^{\xi}, w^{\xi}]K_2 \\ &= [x^{\xi}, w]K_2 = (x^{\xi} K_1)^{\varphi_w}. \end{aligned}$$

Thus φ_w is a Q-homomorphism. □

The special case of Lemma 2.2.3 in which $K_1 = K_2 = 1$ will be most useful; in this case, the hypothesis $[K_1, w] \leq K_2$ of Lemma 2.2.3 is trivially satisfied, and thus only the hypotheses $[H_1, w] \leq H_2$ and $[H_1, w, H_1] = 1$ survive. If we also drop the hypothesis $[H_1, w, H_1] = 1$, then the map φ_w is not a group homomorphism in general, but it satisfies the rule

$$(xy)^{\varphi_w} = (x^{\varphi_w})^y y^{\varphi_w} \quad \text{for all } x, y \in H_1.$$

It is clearly possible to obtain a group homomorphism from φ_w by restricting its domain; in fact, the restriction of φ_w to any subgroup $\tilde{H}_1$ of H_1 is a group homomorphism exactly when $[\tilde{H}_1, w, \tilde{H}_1] = 1$. Though there may not be in general a unique subgroup $\tilde{H}_1$ of G which is maximal among those which satisfy this property, a sensible choice of $\tilde{H}_1$ will be given in Lemma 2.2.4.

To proceed systematically, let us first remark that while the image of φ_w is not in general a subgroup of H_2, the inverse image of the trivial subgroup under φ_w is $\mathbf{C}_{H_1}(w)$, and thus it is a subgroup of H_1, although not necessarily normal. (Let us also notice that $\mathbf{C}_{H_1}(w)$ satisfies one of the properties of the kernel of a homomorphism, namely

$$x^{\varphi_w} = y^{\varphi_w} \iff xy^{-1} \in \mathbf{C}_{H_1}(w),$$

though φ_w is not a homomorphism.)

More generally, if $\tilde{H}_2$ is a subgroup of H_2 such that $[H_1, \tilde{H}_2] = 1$, and if $\tilde{H}_1$ denotes the inverse image of $\tilde{H}_2$ under φ_w, then $\tilde{H}_1$ is a subgroup of H_1, and the restriction of φ_w to $\tilde{H}_1$ is a group homomorphism. Both assertions are straightforward consequences of the commutator formula

$$[xy, w] = [x, w]\,[x, w, y]\,[y, w].$$

In fact, for $x, y \in \tilde{H}_1$ we have that

$$[x, w, y] \in [\tilde{H}_1, w, \tilde{H}_1] \leq [\tilde{H}_2, H_1] = 1;$$

therefore $\tilde{H}_1$ is a subgroup of G and the restriction of φ_w to $\tilde{H}_1$ is a group homomorphism.

If, in addition, Q is a group of operators for G which centralizes w and normalizes $\tilde{H}_2$, then $\tilde{H}_1$ is clearly a Q-subgroup of G, and the restriction of φ_w to $\tilde{H}_1$ is a Q-homomorphism. What we have just proved is stated in the following lemma.

Lemma 2.2.4 *Let H_1, H_2 be Q-subgroups of the Q-group G (with Q possibly the trivial group), and let w be an element of G which is centralized by Q and such that $[H_1, w] \leq H_2$. Let us put $\bar{H}_2 = \mathbf{C}_{H_2}(H_1)$, and*

$$\bar{H}_1 = \{h \in H_1 \mid [h, w] \in \bar{H}_2\}.$$

Then $\bar{H}_1$ is a Q-subgroup of H_1, the map

$$\begin{array}{rccc} \varphi_w : & \bar{H}_1 & \rightarrow & \bar{H}_2 \\ & x & \mapsto & [x, w] \end{array}$$

is a Q-homomorphism, and the kernel of φ_w is $\mathbf{C}_{\bar{H}_1}(w) = \mathbf{C}_{H_1}(w)$.

2.3 Irreducible modules for abelian groups

The following theorem describes all irreducible modules for a finite abelian group over a finite field. With an abuse of language, by a *faithful* $\mathbf{F}G$*-module* we shall always mean an $\mathbf{F}G$-module which is faithful for G (that is to say, no non-identity element of G acts trivially on it), but not necessarily for the group algebra $\mathbf{F}G$.

Theorem 2.3.1 *Let $\mathbf{F}_{p^f}$ be the finite field of order p^f, let A be an abelian group and let V be a faithful irreducible $\mathbf{F}_{p^f}A$-module of dimension n over $\mathbf{F}_{p^f}$. Then:*

(i) A is cyclic of order prime to p;

(ii) n is the smallest positive integer such that $|A|$ divides $(p^{nf} - 1)$ (we also say that n is the multiplicative order of p^f modulo $|A|$); thus $\mathbf{F}_{p^{nf}}$ is the smallest extension field of $\mathbf{F}_{p^f}$ which contains a primitive $|A|$-th root of unity ε, in particular we have $\mathbf{F}_{p^f}(\varepsilon) = \mathbf{F}_{p^{nf}}$;

(iii) if a_0 is a generator of A, then there exists a primitive $|A|$-th root of unity ε in $\mathbf{F}_{p^{nf}}$ such that V is isomorphic to the $\mathbf{F}_{p^f}A$-module V_ε whose underlying vector space over $\mathbf{F}_{p^f}$ is the field $\mathbf{F}_{p^{nf}}$ and where the action of A on V_ε is given by

$$x a_0^i = \varepsilon^i x \quad \text{for all } x \in \mathbf{F}_{p^{nf}} \quad \text{and for all } i = 0, \ldots, |A| - 1.$$

(iv) *the ring* $\mathrm{End}_{\mathbb{F}_{p^f}A}(V)$ *is a field isomorphic to* $\mathbb{F}_{p^{nf}}$, *and consists of the maps*

$$\begin{aligned} \varphi_y : V &\to V \\ v &\mapsto vy, \end{aligned}$$

for $y \in \mathbb{F}_{p^f}A$.

Proof Statements (*i*), (*ii*), and (*iii*) of the theorem follow from [10, Kapitel II, Satz 3.10] and its proof. Let us observe that [10, Kapitel II, Satz 3.10] only states that the actions of A on V and on V_ε are permutation isomorphic, but it is clear from its proof that V and V_ε are actually isomorphic as $\mathbb{F}_{p^f}A$-modules.

In order to prove assertion (*iv*) of the theorem, we may take $V = V_\varepsilon$, according to statement (*iii*). Then each of the maps $\varphi_y : V_\varepsilon \to V_\varepsilon$ is the multiplication by some fixed element of $\mathbb{F}_{p^{nf}}$, and thus it is clearly an endomorphism of V_ε as an $\mathbb{F}_{p^f}A$-module. Hence the set of the maps φ_y for $y \in \mathbb{F}_{p^f}A$ is a field isomorphic to $\mathbb{F}_{p^{nf}}$, and is a subring of $\mathrm{End}_{\mathbb{F}_{p^f}A}(V_\varepsilon)$. According to Maschke's Theorem, $\mathrm{End}_{\mathbb{F}_{p^f}A}(V_\varepsilon)$ is a division ring; therefore, V_ε is a vector space over $\mathrm{End}_{\mathbb{F}_{p^f}A}(V_\varepsilon)$. From the fact that V_ε has order p^{nf} it follows now that V_ε has dimension 1 over $\mathrm{End}_{\mathbb{F}_{p^f}A}(V_\varepsilon)$, and that

$$\mathrm{End}_{\mathbb{F}_{p^f}A}(V_\varepsilon) = \{\varphi_y \mid y \in \mathbb{F}_{p^f}A\}.$$

The proof is complete. □

We observe that the choice of the primitive $|A|$-th root of unity ε in statement (*iii*) is not arbitrary. In fact, different choices of ε may give rise to non-isomorphic $\mathbb{F}_{p^f}A$-module structures on $\mathbb{F}_{p^{nf}}$. More precisely, we shall see that V_ε and $V_{\varepsilon'}$ are isomorphic if and only if ε and ε', which are primitive $|A|$th roots of unity in $\mathbb{F}_{p^{nf}}$, are Galois conjugate over $\mathbb{F}_{p^f}$.

Let $m(x) \in \mathbb{F}_{p^f}[x]$ be the minimal polynomial of the $\mathbb{F}_{p^f}$-linear transformation induced by a_0 on V (via the module action). According to Theorem 2.3.1, our $m(x)$ is also the minimal polynomial of the $\mathbb{F}_{p^f}$-linear transformation of $\mathbb{F}_{p^{nf}}$ given by multiplication by ε. It follows that $m(x)$ is the minimal polynomial of ε over $\mathbb{F}_{p^f}$, in particular ε is an eigenvalue of a_0 on V.

Furthermore, the eigenvalues of a_0 on V are exactly the Galois conjugates

$$\varepsilon, \varepsilon^{p^f}, \varepsilon^{p^{2f}}, \ldots, \varepsilon^{p^{(n-1)f}}.$$

In fact, since ε is a root of $m(x)$, and because the coefficients of $m(x)$ belong to the field $\mathbf{F}_{p^f}$, we have

$$m(\varepsilon^{p^{if}}) = m(\varepsilon)^{p^{if}} = 0 \quad \text{for all } i = 0, \ldots, n-1;$$

hence $\varepsilon, \varepsilon^{p^f}, \varepsilon^{p^{2f}}, \ldots, \varepsilon^{p^{(n-1)f}}$ are roots of $m(x)$. They are pairwise distinct as $\mathbf{F}_{p^f}(\varepsilon) = \mathbf{F}_{p^{nf}}$ has dimension n over $\mathbf{F}_{p^f}$. Since the degree of $m(x)$ does not exceed the dimension n of V, they are exactly all the roots of $m(x)$, that is to say, all the eigenvalues of a_0 on V.

Now let us extend the ground field $\mathbf{F}_{p^f}$ of V to $\mathbf{E} = \mathbf{F}_{p^{nf}}$. The tensor product $V^{\mathbf{E}} = V \otimes_{\mathbf{F}_{p^f}} \mathbf{E}$ is a vector space over $\mathbf{E}$ and becomes an $\mathbf{E}A$-module in a natural way (see [10, Kapitel V, Hilfsatz 11.1 and Hilfsatz 11.3]). The $\mathbf{E}$-linear transformation induced by a_0 on $V^{\mathbf{E}}$ can be put into diagonal form, because it has all its eigenvalues in $\mathbf{E}$ and they are all distinct. Hence there exist an $\mathbf{E}$-basis $v_0, \ldots, v_{n-1}$ of $V^{\mathbf{E}}$ such that

$$v_i a_0 = \varepsilon^{p^{if}} v_i \quad \text{for all } i = 0, \ldots, n-1.$$

We have seen that an irreducible faithful module for a cyclic group over a finite field $\mathbf{F}_{p^f}$ determines a Galois conjugacy class of roots of unity over $\mathbf{F}_{p^f}$. The following result is stronger.

Theorem 2.3.2 *Let $A = \langle a_0 \rangle$ be a cyclic group and let $\mathbf{E}$ be a splitting field for the polynomial $x^{|A|} - 1$ over $\mathbf{F}_{p^f}$. The isomorphism classes of irreducible $\mathbf{F}_{p^f}A$-modules are in a bijective correspondence with the orbits of $|A|$th roots of unity in $\mathbf{E}$ under the Galois group of $\mathbf{E}$ over $\mathbf{F}_{p^f}$. This correspondence associates to each irreducible $\mathbf{F}_{p^f}A$-module V the set of the eigenvalues of a_0 on V.*

Proof Let us first prove the theorem under the assumption that $|A|$ is not divisible by p.

Let $\mathcal{R}$ be the set of the $|A|$th roots of unity in $\mathbf{E}$. Since $\mathbf{E}$ is a splitting field for $x^{|A|} - 1$, and since p does not divide $|A|$, the field $\mathbf{E}$ contains $|A|$ distinct $|A|$th roots of unity, and therefore $|\mathcal{R}| = |A|$. If $\varepsilon \in \mathcal{R}$, the extension field $\mathbf{F}_{p^f}(\varepsilon)$ can be regarded as a vector space over $\mathbf{F}_{p^f}$ and becomes an $\mathbf{F}_{p^f}A$-module if one defines

$$v a_0^i = \varepsilon^i v \quad \text{for all } v \in \mathbf{F}_{p^f}(\varepsilon) \text{ and for all } i = 1, \ldots, |A|.$$

This $\mathbf{F}_{p^f}A$-module, which we shall denote by V_ε, is irreducible, because any $\mathbf{F}_{p^f}A$-submodule of V_ε is an ideal of the field $\mathbf{F}_{p^f}(\varepsilon)$, and hence is either 0 or V_ε.

If V is any irreducible $\mathbf{F}_{p^f}A$-module, then V can be regarded as a faithful irreducible module for $A = A/K$ over $\mathbf{F}_{p^f}$, where

$$K = \{a \in A \mid va = v \ \text{ for all } v \in V\}$$

is the kernel of the representation of A on V. It follows from statement (*iii*) of Theorem 2.3.1 that there exists a primitive $|A|$th root of unity ε (in particular ε is an $|A|$th root of unity and we may assume that $\varepsilon \in \mathcal{R}$) such that V is isomorphic to V_ε as an $\mathbf{F}_{p^f}A$-module, and hence as an $\mathbf{F}_{p^f}A$-module.

Thus the set of modules V_ε for $\varepsilon \in \mathcal{R}$ contains a complete set of representatives for the isomorphism classes of irreducible $\mathbf{F}_{p^f}A$-modules. As we have seen above, the eigenvalues of a_0 on V_ε are exactly all the distinct Galois conjugates of ε. In particular if V_ε and $V_{\varepsilon'}$ are isomorphic (for $\varepsilon, \varepsilon' \in \mathcal{R}$), then ε and ε' are Galois conjugate, in other words they belong to the same orbit of the Galois group of $\mathbf{E}$ over $\mathbf{F}_{p^f}$ on $\mathcal{R}$.

Conversely, let us assume that ε and ε' are Galois conjugate. Then since the Galois group of $\mathbf{E}$ over $\mathbf{F}_{p^f}$ is generated by the automorphism $c \mapsto c^{p^f}$, we have $\varepsilon' = \varepsilon^{p^{if}}$ for some integer i. In particular V_ε and $V_{\varepsilon'}$ have the same underlying vector space over $\mathbf{F}_{p^f}$, namely the field $\mathbf{F}_{p^f}(\varepsilon) = \mathbf{F}_{p^f}(\varepsilon')$. The map $\theta : V_\varepsilon \to V_{\varepsilon'}$ such that $v^\theta = v^{p^{if}}$ is then an isomorphism of $\mathbf{F}_{p^f}A$-modules, because it is an isomorphism of vector spaces over $\mathbf{F}_{p^f}$ and it satisfies

$$(va_0)^\theta = (v\varepsilon)^{p^{if}} = v^{p^{if}}\varepsilon^{p^{if}} = v^\theta a_0$$

for all $v \in V_\varepsilon$. Hence V_ε and $V_{\varepsilon'}$ are isomorphic if and only if ε and ε' are Galois conjugate.

Thus the theorem is proved under the additional assumption that $|A|$ is not divisible by p. Now let us drop this assumption, and let p^r be the highest power of p which divides $|A|$. Let us put $A = A/P$, where $P = \langle a_0^{|A|/p^r} \rangle$ is the Sylow p-subgroup of A.

According to [10, Kapitel V, Satz 5.17] P is contained in the kernel of every irreducible representation of A over $\mathbf{F}_{p^f}$; hence each irreducible $\mathbf{F}_{p^f}A$-module V can be regarded as an irreducible $\mathbf{F}_{p^f}A$-module. On the other hand, since

$$x^{|A|} - 1 = x^{|A|p^r} - 1 = (x^{|A|} - 1)^{p^r},$$

the splitting field $\mathbb{E}$ for $x^{|A|} - 1$ over $\mathbf{F}_{p^f}$ is also a splitting field for $x^{|A|} - 1$ and the set $\mathcal{R}$ of $|A|$th roots of unity in $\mathbb{E}$ coincides with the set of $|A|$th roots of unity in $\mathbb{E}$.

Since p does not divide $|A|$, the theorem is true for the group A, as we have proved above. Thus, in view of these observations, its conclusion holds for the group A too. $\square$

We observe here that Theorem 2.3.2 in disguise says that the isomorphism classes of irreducible $\mathbf{F}_{p^f}A$-modules are in a bijective correspondence with the Galois conjugacy classes over $\mathbf{F}_{p^f}$ of irreducible $\mathbb{E}$-characters of A; thus Theorem 2.3.2 may also be deduced from [13, Theorem 9.21] together with [13, Corollary 9.7].

An important consequence of Theorem 2.3.2 is that the isomorphism class of an irreducible $\mathbf{F}_{p^f}A$-module V (for a cyclic group $A = \langle a_0 \rangle$) is uniquely determined by the isomorphism class of the (not necessarily irreducible) $\mathbb{E}A$-module $V^{\mathbb{E}}$. In fact, we saw that $V^{\mathbb{E}}$ has an $\mathbb{E}$-basis whose elements are eigenvectors for a_0 and, according to Theorem 2.3.1, the corresponding eigenvalues form an orbit under the Galois group of $\mathbb{E}$ over $\mathbf{F}_{p^f}$ and determine the $\mathbf{F}_{p^f}A$-module V up to isomorphism. We shall need the following more general result.

Corollary 2.3.3 *Let W be a semisimple module for the cyclic group A over $\mathbf{F}_{p^f}$ and let $\mathbb{E}$ be a splitting field for the polynomial $x^{|A|} - 1$ over $\mathbf{F}_{p^f}$. Then the isomorphism class of W as an $\mathbf{F}_{p^f}A$-module is uniquely determined by the isomorphism class of $W^{\mathbb{E}}$ as an $\mathbb{E}A$-module.*

Proof Since W is semisimple, we have $W = \bigoplus_{i=1}^{t} V_i$, where the V_i are irreducible $\mathbf{F}_{p^f}A$-modules. It is easy to see that $W^{\mathbb{E}} \cong \bigoplus_{i=1}^{t} V_i^{\mathbb{E}}$. Since we saw that $V_i^{\mathbb{E}}$ determines V_i uniquely up to isomorphism, the conclusion follows. $\square$

Let us notice that Corollary 2.3.3 remains true if we replace the cyclic group A with an arbitrary finite group. This is again a consequence of [13, Theorem 9.21 and Corollary 9.7].

2.4 Homogeneous modules

An $\mathbf{F}Q$-module V (where $\mathbf{F}$ is a field and Q is a group) is said to be *homogeneous* if it is semisimple and all its $\mathbf{F}Q$-composition factors are isomorphic.

If V is a semisimple $\mathbf{F}Q$-module (for instance V is always semisimple when the characteristic of $\mathbf{F}$ is 0 or a prime not dividing the order of Q, according to Maschke's Theorem), then by definition V is a direct sum of irreducible $\mathbf{F}Q$-submodules. A submodule of V which is the sum of all irreducible submodules isomorphic to a fixed irreducible $\mathbf{F}Q$-module is called a *homogeneous component* of V. It is easy to see that each homogeneous component of V is invariant under $\mathbf{F}Q$-endomorphisms of V, and that V is the direct sum of its homogeneous components (see for instance [13, Lemma (1.13)]).

Lemma 2.4.1 *Let $\mathbf{F}$ be a field, Q an abelian group and S a semisimple $\mathbf{F}Q$-module. Then the following assertions are equivalent:*

(i) every cyclic $\mathbf{F}Q$-submodule of S is irreducible;

(ii) S is the union of its irreducible $\mathbf{F}Q$-submodules;

(iii) S is $\mathbf{F}Q$-homogeneous.

Proof ((i)$\Rightarrow$ (ii)) If each element of S generates an irreducible submodule of S, then S is clearly a union of irreducible submodules.

((ii)$\Rightarrow$ (iii)) Since S is semisimple, S is the direct sum of its $\mathbf{F}Q$-homogeneous components and every irreducible $\mathbf{F}Q$-submodule of S is contained in some $\mathbf{F}Q$-homogeneous component of S. Hence S has only one $\mathbf{F}Q$-homogeneous component, or in other words, S is $\mathbf{F}Q$-homogeneous.

((iii)$\Rightarrow$ (i)) Since S is semisimple, S can be written as an internal direct sum $S = V_1 \oplus \cdots \oplus V_k$ of irreducible $\mathbf{F}Q$-submodules $V_1, \ldots, V_k$, which are all isomorphic because S is $\mathbf{F}Q$-homogeneous. We may therefore assume that $S = V \oplus \cdots \oplus V$, the external direct sum of k isomorphic copies of an irreducible $\mathbf{F}Q$-module V.

Let $(v_1, \ldots, v_k)$ be a non-zero element of S. We may assume $v_1 \neq 0$. Since V is irreducible we have $v_1\mathbf{F}Q = V$, in particular for each $i = 2, \ldots, k$ there exists an element a_i of $\mathbf{F}Q$ such that $v_1 a_i = v_i$.

Now the map

$$\begin{aligned} \varphi : V &\rightarrow S \\ v &\mapsto (v, va_2, \ldots, va_k) \end{aligned}$$

is clearly $\mathbf{F}$-linear. Furthermore, the map φ is an $\mathbf{F}Q$-homomorphism, because Q is abelian.

Since V is irreducible and φ is not the zero homomorphism, φ is a monomorphism. Thus its image $(v_1, \ldots, v_k)\mathbf{F}Q$, namely the cyclic $\mathbf{F}Q$-submodule of S generated by $(v_1, \ldots, v_k)$, is isomorphic to V, in particular it is an irreducible $\mathbf{F}Q$-module. □

The notion of homogeneous component generalizes to a situation in which the modules are not semisimple, namely that of abelian groups (or in other words, $\mathbf{Z}$-modules) with operator groups of coprime order. To proceed systematically, let us first recall some well-known facts.

Theorem 2.4.2 *Let A be an abelian p-group, and let Q be a p'-group of automorphisms of A. Suppose that A is indecomposable as a Q-group. Then A is homocyclic (in other words, A is the direct product of cyclic groups of the same order), and the only Q-subgroups of A are*

$$\Omega_i(A) = \{a \in A \mid a^{p^i} = 1\},$$

for $i = 0, 1, \ldots, e$, where p^e is the exponent of A. Furthermore, all Q-composition factors of A are Q-isomorphic.

Proof See [11, Chapter VIII, Theorem 5.9 and Theorem 5.10]. The fact that all Q-composition factors of A are Q-isomorphic is a consequence of the fact that the map

$$\begin{array}{ccc} A & \to & A \\ a & \mapsto & a^p \end{array}$$

is a Q-endomorphism of A. □

Now let A be an abelian p group with a p'-group of automorphisms Q. If V is a fixed irreducible $\mathbf{F}_pQ$-module, let B be the product of all indecomposable Q-subgroups of A which have some Q-composition factor isomorphic to V (as a Q-group, or equivalently as an $\mathbf{F}_pQ$-module). It is an easy consequence of Theorem 2.4.2 that all Q-composition factors of B are Q-isomorphic to V. We shall thus call B a *Q-homogeneous component* of A. The name is justified by the easy facts that Q-homogeneous components of A are invariant under Q-endomorphisms of A, and that A is the direct product of its Q-homogeneous components. (We observe that the statement of Lemma 2.1.1 which refers to A abelian is a special case of this, $\mathbf{C}_Q(A)$ being the Q-homogeneous component of A which corresponds to the trivial module.)

2.5 Induction and tensor induction

While the reader is certainly familiar with induction of modules and characters, he may be not so with tensor induction. This technique is particularly useful for the description of the representations of wreath products. In order to show the similarity between ordinary induction and tensor induction we shall give a brief exposition of both techniques in succession. Expositions of tensor induction can also be found in [5, §13] and [14, Section 4].

Let H be a subgroup of the group G, let $\mathbf{F}$ be a field and W a right $\mathbf{F}H$-module. Since the group algebra $\mathbf{F}G$ is an $(\mathbf{F}H, \mathbf{F}G)$-bimodule, the tensor product $W \otimes_{\mathbf{F}H} \mathbf{F}G$ becomes a right $\mathbf{F}G$-module according to [10, Kapitel V, Satz 9.8], which is called the induced module and is denoted by W^G.

Let T be a right transversal for H in G. Then $\mathbf{F}H = \bigoplus_{t \in T}(\mathbf{F}H)t$ is a decomposition of $\mathbf{F}G$ as a left $\mathbf{F}H$-module (which shows that $\mathbf{F}G$ is a free left $\mathbf{F}H$-module). Hence we have the decomposition

$$W^G = W \otimes_{\mathbf{F}H} \mathbf{F}G = \bigoplus_{t \in T}(W \otimes t)$$

of W^G as a vector space over $\mathbf{F}$, where $W \otimes t = \{w \otimes t \mid w \in W\}$. Each $W \otimes t$ is an $\mathbf{F}H^t$-submodule of W^G. In fact, for $h \in H$ we have

$$(w \otimes t)h^t = w \otimes ht = wh \otimes t.$$

Now G acts on the set of right cosets of H in G by right multiplication, hence it acts on T. Let us denote this action by $(t, g) \mapsto t \cdot g$. In other words, $t \cdot g$ (for $t \in T$ and $g \in G$) is the unique element of T such that $tg \in H(t \cdot g)$, or equivalently $tg(t \cdot g)^{-1} \in H$.

We therefore have

$$(w \otimes t)g = wtg(t \cdot g)^{-1} \otimes (t \cdot g) \in W \otimes (t \cdot g),$$

where we observe that in order to compute $wtg(t \cdot g)^{-1}$ it is sufficient to know W as an $\mathbf{F}H$-module, because $tg(t \cdot g)^{-1} \in H$. More generally, any element of $W^{\uparrow G}$ has the form $\sum_{t\in T}(w_t \otimes t)$ for some $w_t \in W$, and we have

$$\left(\sum_{t\in T}(w_t \otimes t)\right) g = \sum_{t\in T}(x_t \otimes t),$$

where $x_t = w_{t\cdot g^{-1}}((t\cdot g^{-1})gt^{-1})$.

There is an alternative definition of $W^{\uparrow G}$ which builds it as the direct sum of $\mathbb{F}$-spaces $W \otimes t$, each isomorphic to W via the map $w \mapsto w \otimes t$, and makes it into an $\mathbb{F}G$-module according to the formula above. Although our original definition of $W^{\uparrow G}$ is to be preferred as it does not involve any choice of a transversal T, the formula above will serve as a model for the definition of the tensor induced module $W^{\otimes G}$.

As we have seen, $W^{\uparrow G}$ is the direct sum of the $\mathbb{F}$-subspaces $W \otimes t$ for $t \in T$, and each $W \otimes t$ is an $\mathbb{F}H^t$-submodule of $W^{\uparrow G}$. Let us define the $\mathbb{F}$-space

$$W^{\otimes G} = \bigotimes_{t\in T}(W \otimes t),$$

namely $W^{\otimes G}$ is the tensor product over $\mathbb{F}$ of the $\mathbb{F}$-spaces $W \otimes t$, where we are assuming some fixed but arbitrary total order on T.

The $\mathbb{F}H^t$-module structure of each $W \otimes t$ can now be used to give $W^{\otimes G}$ an $\mathbb{F}G$-module structure, much in the same way as for $W^{\uparrow G}$. We define an action of $g \in G$ on the pure tensors $\bigotimes_{t\in T}(w_t \otimes t)$ (for some $w_t \in W$), as follows:

$$\left(\bigotimes_{t\in T}(w_t \otimes t)\right) g = \bigotimes_{t\in T}(x_t \otimes t),$$

where $x_t = w_{t\cdot g^{-1}}((t\cdot g^{-1})gt^{-1})$. We observe that this formula can be obtained from that which gives the action of g on $W^{\uparrow G}$ by replacing $\sum_{t\in T}$ with $\bigotimes_{t\in T}$. Consequently, the action of g on the pure tensors of $W^{\otimes G}$ can be described in terms of the action of g on $W^{\uparrow G}$ as follows:

$$\left(\bigotimes_{t\in T}(w_t \otimes t)\right) g = \bigotimes_{t\in T}\left(\left(\sum_{s\in T}(w_s \otimes s)\right) g\right)^{\pi_t},$$

where the maps $\pi_t : W^{\uparrow G} \to W \otimes t$ are the projections on the summands of $W^{\uparrow G} = \bigoplus_{t\in T}(W \otimes t)$.

Since the action of g on the pure tensors is linear in each $w_t \otimes t$, it extends to a unique and well-defined action of g on $W^{\otimes G}$. It is easy to check that

$$\left(\left(\bigotimes_{t\in T}(w_t \otimes t)\right) g_1\right) g_2 = \bigotimes_{t\in T}(w_t \otimes t) g_1 g_2;$$

hence $W^{\otimes G}$ becomes an $\mathbb{F}G$-module. We observe that

$$\dim W^G = |G:H| \dim W,$$

and that

$$\dim W^{\otimes G} = (\dim W)^{|G:H|}.$$

It is not difficult to show that the isomorphism class of $W^{\otimes G}$ depends only on the isomorphism class of W, and not on the transversal T, or on the particular ordering given to it.

Now let ψ be the character of H afforded by W and let ψ^G and $\psi^{\otimes G}$ be the characters of G afforded by W^G and $W^{\otimes G}$ respectively. We shall compute explicit expressions for ψ^G and $\psi^{\otimes G}$ in terms of ψ.

Lemma 2.5.1 *Let $g \in G$ and let ψ° denote the function from the group G to the field $\mathbb{F}$ which coincides with ψ on the subgroup H and takes the value zero on $G \setminus H$. Then we have*

$$\psi^G(g) = \sum_{t \in T} \psi^\circ(tgt^{-1}).$$

Proof Let $w_1, \dots, w_s$ be a basis of W. Then a basis of W^G is given by the elements $w_i \otimes t$ for $i = 1, \dots s$ and for $t \in T$. Let us write

$$w_i h = \sum_{j=1}^{s} a_{ij}(h) w_j$$

for $h \in H$, with $a_{ij}(h) \in \mathbb{F}$. In particular, we have $\psi(h) = \sum_{i=1}^{s} a_{ii}(h)$. On the other hand, we have

$$(w_i \otimes t)g = w_i(tg(t \cdot g)^{-1}) \otimes (t \cdot g) = \sum_{j=1}^{s} a_{ij}(tg(t \cdot g)^{-1}) w_j \otimes (t \cdot g).$$

Now we have $w_i \otimes t = w_j \otimes (t \cdot g)$ exactly when $i = j$ and $t = t \cdot g$, or equivalently when $i = j$ and $tgt^{-1} \in H$. It follows that

$$\psi^G(g) = \sum_{t \in T'} \sum_{i=1}^{s} a_{ii}(tgt^{-1}) = \sum_{t \in T} \psi^\circ(tgt^{-1}),$$

where T' is the set of the elements t of T such that $tgt^{-1} \in H$. The proof is complete. $\square$

We observe that since ψ is a class function, when $\mathbb{F}$ has characteristic zero we can also write

$$\psi^G(g) = \frac{1}{|H|} \sum_{x \in G} \psi^\circ(xgx^{-1}).$$

If we choose a set of representatives $x_1, \ldots, x_m$ for the conjugacy classes of H contained in g^G (that is to say, $g^G \cap H = x_1^H \dot{\cup} \cdots \dot{\cup} x_m^H$), we obtain

$$\psi^G(g) = \frac{|G:H|}{|g^G|} \sum_{i=1}^{m} |x_i^H| \psi(x_i).$$

The following useful formula follows:

$$\psi^G(g) = |\mathbf{C}_G(g)| \sum_{i=1}^{m} \frac{\psi(x_i)}{|\mathbf{C}_H(x_i)|}.$$

This can also be expressed by saying that $\psi^G(g)$ equals $|G:H|$ times the mean value of ψ° over g^G.

Now let us pass to the computation of the tensor induced character $\psi^{\otimes G}$.

Lemma 2.5.2 *Let $g \in G$ and let T_0 be a set of representatives for the orbits of $\langle g \rangle$ in its action on T via $\cdot$. For $t \in T$, let $n(t)$ denote the size of the $\langle g \rangle$-orbit which contains t. Then we have*

$$\psi^{\otimes G}(g) = \prod_{t \in T_0} \psi(tg^{n(t)}t^{-1}).$$

Proof Let $\Omega_1, \ldots, \Omega_r$ be the orbits of $\langle g \rangle$ on T, let us choose a set

$$T_0 = \{t_1, \ldots, t_r\}$$

of representatives for them (with $t_i \in \Omega_i$), and let us put $n(i) = |\Omega_i|$. Hence $\langle g \rangle / \langle g^{n(i)} \rangle$ acts regularly on Ω_i and we have

$$\Omega_i = \{t_i \cdot g, \ldots, t_i \cdot g^{n(i)} = t_i\}.$$

Since the isomorphism class of $W^{\otimes G}$ is independent of the ordering given to T, we are allowed to order T as follows:

$$T = \{t_1 \cdot g, \ldots, t_1 \cdot g^{n(1)}, \ldots, t_r \cdot g, \ldots, t_r \cdot g^{n(r)}\}.$$

Now $W^{\otimes G}$ regarded as an $\mathbf{F}\langle g\rangle$-module is isomorphic to the tensor product module $\bigotimes_{i=1}^{r} W_i$, where W_i is the $\mathbf{F}\langle g\rangle$-module

$$W_i = \bigotimes_{j=1}^{n(i)} (W \otimes (t_i \cdot g^j)).$$

If ψ_i denotes the character of $\langle g\rangle$ afforded by W_i, we have

$$\psi^{\otimes G}(g) = \prod_{i=1}^{r} \psi_i(g),$$

according to [13, Theorem 4.1].

Let us fix an index $i = 1, \ldots, r$. We shall prove that $\psi_i(g) = \psi(t_i g^{n(i)} t_i^{-1})$. Let $w_1, \ldots, w_s$ be an $\mathbf{F}$-basis of W, then an $\mathbf{F}$-basis of W_i is given by the tensors

$$\bigotimes_{j=1}^{n(i)} (w_{k_j} \otimes (t_i \cdot g^j)),$$

for $(k_1, \ldots, k_{n(i)}) \in \{1, \ldots, s\}^{n(i)}$. The action of g on any element of this basis of $W^{\otimes G}$ is given by the formula

$$\left(\bigotimes_{j=1}^{n(i)} (w_{k_j} \otimes (t_i \cdot g^j))\right) g = \bigotimes_{j=1}^{n(i)} (x_j \otimes (t_i \cdot g^j)),$$

where $x_j = w_{k_{j-1}}((t_i \cdot g^{j-1})g(t_i \cdot g^j)^{-1})$, and the index j is read mod $n(i)$ (in particular, $w_{k_0} = w_{k_{n(i)}}$). Let $A_j = (a_{jkl})_{k,l=1,\ldots,s}$ be the matrix of the action of $((t_i \cdot g^{j-1})g(t_i \cdot g^j)^{-1})$ on W with respect to the basis $w_1, \ldots, w_s$; in other words

$$w_k((t_i \cdot g^{j-1})g(t_i \cdot g^j)^{-1}) = \sum_{l=1}^{s} a_{jkl} w_l.$$

Now the coefficient of the basis element $\bigotimes_{j=1}^{n(i)}(w_{k_j} \otimes (t_i \cdot g^j))$ in the expression of $\bigotimes_{j=1}^{n(i)}(x_j \otimes (t_i \cdot g^j))$ as a linear combination of the elements of the given basis of W_i is

$$\prod_{j=1}^{n(i)} a_{jk_{j-1}k_j}.$$

Hence we have

$$\psi_i(g) = \sum \prod_{j=1}^{n(i)} a_{j,k_{j-1},k_j} = \mathrm{tr}(A_1 A_2 \cdots A_{n(i)}),$$

where the sum is taken over $(k_1, \ldots, k_{n(i)}) \in \{1, \ldots, s\}^{n(i)}$. The matrix $A_1 A_2 \cdots A_{n(i)}$ is the matrix of the action of

$$\prod_{j=1}^{n(i)} ((t_i \cdot g^{j-1}) g (t_i \cdot g^j)^{-1}) = t_i g^{n(i)} t_i^{-1}$$

on W, with respect to the basis $w_1, \ldots, w_s$. Therefore we have

$$\psi_i(g) = \psi(t_i g^{n(i)} t_i^{-1}),$$

as claimed. It follows that

$$\psi^{\uparrow G} = \prod_{i=1}^{r} \psi(t_i g^{n(i)} t_i^{-1}),$$

which concludes the proof. □

2.6 Basic commutators

In Chapter 6 we shall need the notion of basic commutators.

Definition 2.6.1 *[8, p. 178] Let F be a free group of rank n, generated by $x_1, \ldots, x_n$. The basic commutators on $x_1, \ldots, x_n$ are the elements of the ordered infinite set $\{c_i\}_{i \in \mathbb{N}}$, defined inductively as follows:*

(i) *$c_i = x_i$, for $i \leq n$, are the basic commutators of weight 1, and are ordered by the rule $c_1 < c_2 < \cdots < c_n$;*

(ii) *if basic commutators of weight less than l have been defined and ordered, then the commutator $[u, v]$ is a basic commutator exactly when*

  (a) *u and v are basic commutators, and the sum of their weights is l,*

  (b) *$u > v$,*

(c) if $u = [w, t]$, then $v \geq t$;

furthermore, commutators of weight l follow all those of lower weight, and if $[u_1, v_1]$ and $[u_2, v_2]$ have weight l, then we have

$$[u_1, v_1] < [u_2, v_2]$$

if either $v_1 < v_2$ or $v_1 = v_2$ and $u_1 < u_2$.

We state without proof the following theorem (see [8, Theorem 11.2.4] for a proof).

Theorem 2.6.2 *If F is a free group with free generators $x_1, \ldots, x_n$, and if $l \geq 1$, then an arbitrary element f of F has a unique representation*

$$f \equiv c_1^{e_1} c_2^{e_2} \cdots c_t^{e_t} \bmod \gamma_{l+1}(F),$$

where $c_1, \ldots, c_t$ are the ordered basic commutators of weight less than or equal to n, and $e_1, \ldots, e_t$ are integers. In particular, for all $l \geq 1$, the factor group $\gamma_l(F)/\gamma_{l+1}(F)$ is a free abelian group (this is also in [11, Chapter VIII, Theorem 11.15]), and the basic commutators of weight l form (a set of representatives of) a basis for $\gamma_l(F)/\gamma_{l+1}(F)$ over $\mathbf{Z}$.

The analysis of the descending central series of a free group F in terms of basic commutators, provided by Theorem 2.6.2, will be used in Chapters 5 and 6 for the construction of certain groups of exponent p, where p is a prime. Thus we shall be mainly interested in the structure of the descending central series of the factor group $F = F/F^p$ (of course this is a hard problem in general, directly related to the famous Burnside's problem, see [10, Kapitel III, Bemerkungen 6.7]).

The factors $\gamma_l(F)/\gamma_{l+1}(F)$ of the descending central series of F are finite elementary abelian p-groups; hence, they can be regarded as vector spaces over $\mathbf{F}_p$ (while the factors $\gamma_l(F)/\gamma_{l+1}(F)$ can be regarded as free $\mathbf{Z}$-modules). It is easy to see that the basic commutators of weight l generate $\gamma_l(F)/\gamma_{l+1}(F)$. Unfortunately, what would be the analogue for F of the last statement of Theorem 2.6.2 does not hold in general: the basic commutators of weight l in F do not constitute a basis of $\gamma_l(F)/\gamma_{l+1}(F)$ over $\mathbf{F}_p$ in general. For instance, when $p = 2$ we have $F' \leq F^2$ (see [10, Kapitel III, Satz 3.14]); consequently, F is an elementary abelian 2-group, and thus all commutators of weight $l > 1$ are trivial.

However, the last statement of Theorem 2.6.2 passes on to F (with the word $\mathbf{Z}$-basis replaced by $\mathbf{F}_p$-basis) for $l < p$. Let us state this fact as a theorem.

Theorem 2.6.3 *Let F be a free group with free generators $x_1, \ldots, x_n$, let p be a prime, and let $F = F/F^p$. Then, for all $l \geq 1$, the factor group $\gamma_l(F)/\gamma_{l+1}(F)$ is a finite elementary abelian p-group, and it is generated by the basic commutators of weight l. Furthermore, if $l < p$, the basic commutators of weight l form a basis of $\gamma_l(F)/\gamma_{l+1}(F)$ over $\mathbf{F}_p$.*

Theorem 2.6.3 is an easy consequence of a well-known result (see for instance [21, Lemmas 1.11 and 1.12]), which gives $\mathbf{F}_p$-bases, in terms of basic commutators and their powers, for the factors of the p-lower central series $\kappa_l(F)$ of F (which is defined in [11, Chapter VIII, Definition 1.10] as

$$\kappa_l(G) = \prod_{ip^k \geq l} \gamma_i(G)^{p^k},$$

for an arbitrary group G, and with respect to a fixed prime p): $\kappa_l(F)/\kappa_{l+1}(F)$ is an elementary abelian p-group, and (a set of representatives of) a basis for it over $\mathbf{F}_p$ is given by the set of all elements of F of the form c^{p^k}, where p^k divides l, and c is some basic commutator of weight l/p^k (in particular, the basic commutators of weight l form a basis of $\kappa_l(F)/\kappa_{l+1}(F)$ over $\mathbf{F}_p$ for l not a multiple of p). Now since $\kappa_l(F) = F^p\gamma_l(F)$ for $l \leq p$, we have $\kappa_l(F) = \gamma_l(F)$ for $l \leq p$, and Theorem 2.6.3 follows.

However, we shall give here a more self-contained proof of Theorem 2.6.3, after recalling without proof the following lemma.

Lemma 2.6.4 *If x, y are elements of a group G, and p is a prime, then*

$$(xy)^p \equiv x^p y^p \bmod \gamma_2(G)^p \gamma_p(G)$$

(that is to say, the map

$$\begin{array}{rcl} G & \to & G/\gamma_2(G)^p\gamma_p(G) \\ x & \mapsto & x^p\gamma_2(G)^p\gamma_p(G) \end{array}$$

is a group homomorphism).

Proof This is a special case of [11, Chapter VIII, Lemma 1.1]. □

Proof of Theorem 2.6.3 We have $\gamma_l(F) = \gamma_l(F)F^p/F^p$ for $l \geq 1$, and thus

$$\begin{aligned}\gamma_l(F)/\gamma_{l+1}(F) &= \gamma_l(F)F^p/\gamma_{l+1}(F)F^p \\ &\cong \gamma_l(F)/\gamma_l(F) \cap \gamma_{l+1}(F)F^p = \gamma_l(F)/(\gamma_l(F) \cap F^p)\gamma_{l+1}(F).\end{aligned}$$

Hence $\gamma_l(F)/\gamma_{l+1}(F)$ is isomorphic to a factor group of the free abelian group $\gamma_l(F)/\gamma_{l+1}(F)$. It follows from Theorem 2.6.2 that the basic commutators of weight l on $x_1, \ldots, x_n$ (as elements of F) generate $\gamma_l(F)/\gamma_{l+1}(F)$. Consequently, and because F has exponent p, the factor group $\gamma_l(F)/\gamma_{l+1}(F)$ is a finite elementary abelian p-group, and its dimension over $\mathbb{F}_p$ is at most the rank of the free abelian group $\gamma_l(F)/\gamma_{l+1}(F)$.

Now the basic commutators of weight l on $x_1, \ldots, x_n$ clearly form an $\mathbb{F}_p$-basis of $\gamma_l(F)/\gamma_l(F)^p\gamma_{l+1}(F)$. Consequently, the conclusion of the theorem will follow if we can prove that

$$(\gamma_l(F) \cap F^p)\gamma_{l+1}(F) = \gamma_l(F)^p\gamma_{l+1}(F)$$

for $l < p$. Since the inclusion $\geq$ is clearly true for all l, we only have to prove that, for $l < p$,

$$\gamma_l(F) \cap F^p \leq \gamma_l(F)^p\gamma_{l+1}(F).$$

We shall prove the following equivalent statement, which lends itself to an inductive argument:

$$\gamma_l(F) \cap \gamma_{l-k}(F)^p \leq \gamma_l(F)^p\gamma_{l+1}(F) \quad \text{for all } k = 0, \ldots, l.$$

This is certainly true for $k = 0$. Now let $0 < k < l$, and let assume that

$$\gamma_l(F) \cap \gamma_{l-k+1}(F)^p \leq \gamma_l(F)^p\gamma_{l+1}(F)$$

has already been proved. Let g be an element of $\gamma_l(F) \cap \gamma_{l-k}(F)^p$; then g can be written as a product

$$g = \prod_{j=1}^{r} y_j^p,$$

with $y_1, \ldots, y_r \in \gamma_{l-k}(F)$. According to Lemma 2.6.4, we have that

$$g = \prod_{j=1}^{r} y_j^p \equiv \left(\prod_{j=1}^{r} y_j\right)^p \bmod \gamma_2(G)^p\gamma_p(G),$$

where we have put $G = \gamma_{l-k}(F)$. In particular, the above congruence holds

$$\mathrm{mod}\, \gamma_{l-k+1}(F)^p \gamma_p(F),$$

because according to [10, Kapitel III, Hauptsatz 2.11 b)] we have that

$$\gamma_2(\gamma_{l-k}(F)) \leq \gamma_{2(l-k)}(F) \leq \gamma_{l-k+1}(F),$$

and clearly $\gamma_p(\gamma_{l-k}(F)) \leq \gamma_p(F)$.

Now we shall prove that $\prod_{j=1}^{r} y_j \in \gamma_{l-k+1}(F)$. According to Theorem 2.6.2, we can write

$$\prod_{j=1}^{r} y_j \equiv \prod_{i=s}^{t} c_i^{e_i} \bmod \gamma_{l-k+1}(F),$$

where $c_s, \ldots, c_t$ are the basic commutators of weight $l-k$, and $e_s, \ldots, e_t$ are integers. As before, Lemma 2.6.4 yields that

$$\left(\prod_{i=s}^{t} c_i^{e_i}\right)^p \equiv \prod_{i=s}^{t} c_i^{pe_i} \bmod \gamma_2(G)^p \gamma_p(G),$$

where $G = \gamma_{l-k}(F)$; in particular this holds $\mathrm{mod}\, \gamma_{l-k+1}(F)$ (let us notice that here we are not using the fact that $l < p$, because

$$\gamma_p(\gamma_{l-k}(F)) \leq \gamma_{p(l-k)}(F) \leq \gamma_{l-k+1}(F),$$

by a repeated application of [10, Kapitel III, Hauptsatz 2.11 b)]). Now we obtain that

$$g \equiv \left(\prod_{j=1}^{r} y_j\right)^p \equiv \prod_{i=s}^{t} c_i^{pe_i} \bmod \gamma_{l-k+1}(F).$$

On the other hand, $g \in \gamma_l(F) \leq \gamma_{l-k+1}(F)$. According to Theorem 2.6.2, $c_1, \ldots, c_t$ are $\mathbf{Z}$-linearly independent in $\gamma_{l-k}(F)/\gamma_{l-k+1}(F)$; consequently, we have $e_s = \cdots = e_t = 0$, and thus

$$\prod_{j=1}^{r} y_j \in \gamma_{l-k+1}(F),$$

as claimed. Since we found earlier that

$$g \equiv \left(\prod_{j=1}^{r} y_j\right)^p \bmod \gamma_{l-k+1}(F)^p \gamma_p(F),$$

it follows that $g \in \gamma_{l-k+1}(F)^p\gamma_p(F)$. Now our hypothesis that $l < p$ comes into play, and yields that $\gamma_p(F) \leq \gamma_{l+1}(F)$. Consequently,

$$g \in \gamma_l(F) \cap \gamma_{l-k+1}(F)^p\gamma_{l+1}(F) = (\gamma_l(F) \cap \gamma_{l-k+1}(F)^p)\gamma_{l+1}(F).$$

By inductive hypothesis, we finally obtain that

$$g \in \gamma_l(F)^p\gamma_{l+1}(F).$$

This concludes the proof. □

2.7 Character table isomorphisms

As promised in Chapter 1, here is a more handy definition of 'having identical character tables'.

Definition 2.7.1 *Let G_1, G_2 be finite groups. We will say that G_1 and G_2 have identical character tables if there exist bijections*

$$\alpha : G_1 \to G_2$$

and

$$\beta : \mathrm{Irr}(G_1) \to \mathrm{Irr}(G_2),$$

such that

$$\chi^\beta(g^\alpha) = \chi(g) \quad \textit{for all } g \in G_1 \quad \textit{and for all } \chi \in \mathrm{Irr}(G_1).$$

We shall also say that (α, β) is a character table isomorphism *from G to H.*

Since the irreducible characters of G_i (for $i = 1, 2$) form a basis of the space of class functions on G_i, with values in the field of the complex numbers, if such α, β exist, α must send any conjugacy class of G_1 onto a conjugacy class of G_2. It is also clear that α sends the identity class of G_1 to the identity class of G_2, and that β sends the trivial character of G_1 to the trivial character of G_2.

Chapter 3

Looking for a counterexample

3.1 Introduction

The work of this thesis began as an attempt to prove that the character table of a soluble group G determines the derived length of G. Our exposition will follow this approach, and thus this chapter begins with the following conjecture, which will eventually turn out to be false.

Conjecture 3.1.1 *Let G and H be groups with identical character tables and assume that G is metabelian. Then H is metabelian.*

We shall disprove this conjecture by exhibiting a counterexample. But what could such a counterexample look like? Let us choose a counterexample (G, H) to Conjecture 3.1.1 with $|G|$ minimal and let (α, β) be a character table isomorphism from G to H. Then H'' is the unique minimal normal subgroup of H. In fact, if this were not true, H would have some non-trivial normal subgroup K with $H'' \not\leq K$. But then the factor groups $G/\bar{K}$, where $\bar{K} = K^{\alpha^{-1}}$, and H/K would have identical character tables, and $(H/K)'' = H''K/K \neq 1$; hence $(G/\bar{K}, H/K)$ would be a counterexample to our conjecture with $|G/\bar{K}| < |G|$, a contradiction. Thus H'' is the unique minimal normal subgroup of H. Since G and H have isomorphic lattices of normal subgroups, the subgroup $(H'')^{\alpha^{-1}}$, which we will henceforth call N, is the unique minimal normal subgroup of G.

Hence N and H'' are elementary abelian p-groups for some prime p, and of course they are isomorphic as they have the same order (because α is a bijection). Throughout this chapter we shall assume that G and H are not p-groups. More precisely, we shall consider the following hypotheses.

Hypotheses 3.1.2 *Let G and H be groups with identical character tables via the bijections (α, β). Let us assume that G and H are not nilpotent, that G is metabelian and that H'' is the unique minimal normal subgroup of H. Thus $N = (H'')^{\alpha^{-1}}$ is the unique minimal normal subgroup of G, and in particular N and H'' are elementary abelian p-groups for some prime p.*

Under these hypotheses we shall obtain in the next section a nice description of a minimal counterexample (G, H). Subsequently, in Chapter 6, we shall also construct a counterexample (G, H) with G and H nilpotent.

3.2 Structure of a minimal counterexample

Lemma 3.2.1 *Assume Hypotheses 3.1.2. Then*

(i) G' and H' are p-groups;

(ii) G' has a complement $W \times Q$ in G and H' has a complement $W \times Q$ in H, where W, W are (abelian) p-groups and Q, Q are cyclic p'-groups;

(iii) Q acts regularly on G' and Q acts regularly on H';

(iv) Q acts faithfully and irreducibly on N by conjugation and Q acts faithfully and irreducibly on H'' by conjugation;

(v) $\mathbf{C}_W(G') = 1$ and $\mathbf{C}_W(H') = 1$.

Proof Since the Fitting subgroup $\mathbf{F}(G)$ of G is nilpotent, each Sylow subgroup of $\mathbf{F}(G)$ is normal in $\mathbf{F}(G)$ and hence in G. But G has a unique minimal normal subgroup N, which is a p-group; hence $\mathbf{F}(G)$ is a p-group.

We have $G' \leq \mathbf{F}(G)$. Let P be a Sylow p-subgroup of G. Then from $G' \leq \mathbf{F}(G) \leq P$ it follows that $P \lhd G$ and hence $\mathbf{F}(G) = P$. Let us put $P = P^\alpha$. Because α is a bijection, P is a Sylow p-subgroup of H and of course $H' \leq P \lhd H$. Thus both G and H have a normal Sylow p-subgroup, which contains the derived subgroup, and assertion (*i*) is proved.

Let Q and Q be complements for P in G and for P in H respectively; these exist according to the Theorem of Schur-Zassenhaus. Clearly Q and Q are abelian. They are also non-trivial, because we assumed that G and H are not nilpotent. Since G and H are soluble groups, we have $\mathbf{C}_G(\mathbf{F}(G)) \leq \mathbf{F}(G)$ and $\mathbf{C}_H(\mathbf{F}(H)) \leq \mathbf{F}(H)$ (see [10, Kapitel III, Satz 4.2]); in particular it follows that $\mathbf{C}_Q(P) = 1$ and $\mathbf{C}_Q(P) = 1$.

Now we shall prove that Q acts regularly on G'. Let K be a non-trivial subgroup of Q. Then, according to Lemma 2.1.1, we have $G' = [G', K] \times \mathbf{C}_{G'}(K)$. Since $[G', K] = [G', G'K]$ and $\mathbf{C}_{G'}(K) = \mathbf{C}_{G'}(G'K)$ are normal subgroups of G, and since G has the unique minimal normal subgroup N, either $[G', K']$ or $\mathbf{C}_{G'}(K)$ is trivial. Assume for a contradiction that $[G', K]$ is trivial. Then we have $[P, K, K] = 1$, whence $[P, K] = 1$ according to Lemma 2.1.1. This contradicts the fact that $\mathbf{C}_Q(P) = 1$; we conclude that $\mathbf{C}_{G'}(K) = 1$ and $[G', K] = G'$. Thus Q acts regularly on G'.

Now let us prove that Q acts regularly on H'. We cannot apply the same argument as for G, because H' is not abelian. But since $(|P|, |Q|) = 1$, asserting that Q acts regularly on G' is equivalent to saying that all nontrivial conjugacy classes of G contained in G' have length a multiple of $|Q|$. From the fact that the bijection α sends each conjugacy class of G contained in G' onto a conjugacy class of H contained in H', we deduce that all nontrivial conjugacy classes of H contained in H' have length a multiple of $|Q| = |Q|$. This fact in turn is equivalent to saying that Q acts regularly on H'. Thus assertion (*iii*) is proved. Furthermore, we have that $H' = [H', Q]\mathbf{C}_{H'}(Q)$, according to Lemma 2.1.1 again. Since $\mathbf{C}_{H'}(Q) = 1$, it follows that $[H', Q] = H'$.

Now let us put $W = \mathbf{C}_P(Q)$ and $W = \mathbf{C}_P(Q)$. We have $P = [P, Q]\mathbf{C}_P(Q)$. Since $G' = [G', Q] \leq [P, Q] \leq G'$, we have $[P, Q] = G'$, and thus $P = G'W$. From $G' \cap W = G' \cap \mathbf{C}_P(Q) = \mathbf{C}_{G'}(Q) = 1$ it follows that W is a complement for G' in P. Now W is centralized by Q; consequently, $WQ = W \times Q$ is a complement for G' in G. We obtain similarly that W is a complement for H' in P and thus $WQ = W \times Q$ is a complement for H' in H.

Now let us show that Q and Q are cyclic groups. The minimal normal subgroup N of G, like any chief factor of G, can be regarded as an irreducible $\mathbb{F}_pG$-module. By restriction N can be also regarded as an $\mathbb{F}_pQ$-module, and N is still irreducible as an $\mathbb{F}_pQ$-module. In fact any $\mathbb{F}_pQ$-submodule of N is an $\mathbb{F}_pG$-submodule, because $G = PQ$ and $N \leq \mathbf{Z}(P)$. Furthermore, N is a faithful $\mathbb{F}_pQ$-module, because Q acts regularly on G', and in particular on N. According to Theorem 2.3.1 then Q is cyclic of order dividing $|N| - 1$.

Similarly, we can deduce that Q is cyclic (this also follows directly from the fact that Q and Q are both isomorphic to $G/P \cong H/P$), and that Q acts faithfully and irreducibly on H''. Thus assertions (ii) and (iv) are proved.

It remains to prove assertion (v). If the element w of W centralized G', then w would be central in G, because WQ is an abelian complement for G' in G. Hence $\langle w \rangle$ would be a normal subgroup of G not containing the unique minimal normal subgroup N. Therefore $w = 1$. Thus we have $\mathbf{C}_W(G') = 1$. Similarly one proves that $\mathbf{C}_W(H') = 1$. The proof of the lemma is now complete. $\square$

Let us notice that $W \times Q \cong G/G'$ and $W \times Q \cong H/H'$. From the fact that G and H have identical character tables we deduce that G/G' is isomorphic to H/H'. It follows that $W \cong W$ and $Q \cong Q$.

We also observe, as we already said in the proof of Lemma 3.2.1, that Q and Q are non-trivial, otherwise G and H would be p-groups, contrary to Hypotheses 3.1.2. The groups W and W are not trivial either; if they were, then G would have a normal abelian Sylow p-subgroup (namely G') and H would not (because H' is not abelian). This would contradict the fact that G and H have the same character degrees; in fact [13, Corollary 12.34] asserts that a group has a normal abelian Sylow p-subgroup if and only if all its irreducible characters have degree not divisible by p.

3.3 Chief factors

We continue our analysis of groups G and H satisfying Hypotheses 3.1.2. In the next three lemmas we shall be concerned with certain chief factors of G and H regarded as irreducible G-groups and respectively H-groups by conjugation.

Let M_1/M_2 be a chief factor of G; hence M_1 and M_2 are normal subgroups of G with $M_2 \leq M_1$ and there exists no normal subgroup M of G with $M_2 < M < M_1$. Then M_1/M_2 becomes an irreducible G-group by conjugation. Since the Fitting subgroup $\mathbf{F}(G)$ of G centralizes all chief factors of G (see [10, Kapitel III, Satz 4.3]), in particular $\mathbf{F}(G)$ is contained in the kernel of the action of G on M_1/M_2. Since Q is a complement for $\mathbf{F}(G)$ in G, the G-group M_1/M_2 remains irreducible when it is regarded as a Q-group by restriction. Thus all chief factors of G are Q-composition factors of G (but not vice versa, because if M_1/M_2 is a Q-composition factor of G the Q-subgroups M_1, M_2 of G are not necessarily normal in G). Furthermore, two chief factors of G are

G-isomorphic exactly when they are Q-isomorphic. Similar assertions hold for chief factors of H regarded as H-groups and as Q-groups.

Lemma 3.3.1 *Assume Hypotheses 3.1.2. Then all chief factors of G below G' are G-isomorphic.*

Proof Let us regard the abelian normal subgroup G' of G as a Q-group (actually a $\mathbf{Z}Q$-module) by conjugation. In view of the remark which precedes the lemma it suffices to show that all composition factors of G' are isomorphic as Q-groups.

As we said in Section 2.4, there exists a unique decomposition of G' (written additively) into the direct sum of its Q-homogeneous components $B_1, \dots, B_m$. Now W centralizes Q: consequently, each element of W induces by conjugation an automorphism of G' as a Q-group. According to what we said in Section 2.4, it follows that each B_i is normalized by W, and being of course normal in G' because G' is abelian, each B_i is a normal subgroup of G.

Since each non-trivial B_i contains the unique minimal normal subgroup N of G, there is a unique non-trivial B_i; consequently, G' is Q-homogeneous, that is to say, all Q-composition factors of G' are Q-isomorphic. □

We shall also prove that when Hypotheses 3.1.2 hold, all chief factors of H below H' are H-isomorphic. We cannot use the same arguments as for G because H' is not abelian. Hence we shall split the proof in two parts: first we shall show that all chief factors of H lying between H' and H'' are H-isomorphic and then that they are H-isomorphic to H''.

In order to prove the first part we shall employ the fact that G and H have identical character tables, and hence in particular isomorphic lattices of normal subgroups.

Lemma 3.3.2 *Assume Hypotheses 3.1.2. Then all chief factors of H between H' and H'' are H-isomorphic.*

Proof The statement of the lemma is clearly equivalent to the following assertion: all chief factors of H/H'' below H'/H'' are H-isomorphic. Since Q is a complement in H for the Fitting subgroup of H, which centralizes all chief factors of H, the proof will be complete once we show that the Q-group

H'/H'' is Q-homogeneous. We shall infer this from the fact that G'/N is Q-homogeneous, by using the fact that G/N and H/H'' have identical character tables. In fact, the character table isomorphism (α, β) from G to H induces a character table isomorphism $(\bar{\alpha}, \beta)$ from G/N to H/H'' in a natural way.

Let S be the product of all minimal normal subgroups of G/N contained in G'/N (in other words, S is the socle of G'/N as a $\mathbb{Z}G$-module). Since the map α induces an isomorphism between the lattices of normal subgroups of G/N and H/H'', and sends G'/N onto H'/H'', the image S of S under α is the product of all minimal normal subgroups of H/H'' contained in H'/H''. The groups S and S are elementary abelian p-groups, and thus can be regarded as an $\mathbb{F}_pG$-module and an $\mathbb{F}_pH$-module respectively. The $\mathbb{F}_pG$-submodules of S (that is to say, the normal subgroups of G/N contained in S) are in a bijective correspondence, induced by the map α, with the $\mathbb{F}_pH$-submodules of S. We also observe that the Fitting subgroups of G and H centralize S and S respectively; it follows that the set of $\mathbb{F}_pG$-submodules of S coincides with the set of $\mathbb{F}_pQ$-submodules of S. Of course, a similar assertion holds for H. As a consequence, the map $\bar{\alpha}$ induces a bijection from the set of $\mathbb{F}_pQ$-submodules of S onto the set of $\mathbb{F}_pQ$-submodules of S.

We know that the semisimple $\mathbb{F}_pQ$-module S is homogeneous; according to Lemma 2.4.1, this is equivalent to the fact that S is the (set-theoretic) union of its irreducible $\mathbb{F}_pQ$-submodules. This property of S can clearly be passed on to S via the bijection $\bar{\alpha}$, namely we get that S is the union of its irreducible $\mathbb{F}_pQ$-submodules. Then Lemma 2.4.1 again yields that S is $\mathbb{F}_pQ$-homogeneous.

From this fact we deduce that H'/H'' is Q-homogeneous, as follows. The abelian Q-group H'/H'' can be decomposed into the direct product of its Q-homogeneous components (see Section 2.4). If M is a non-trivial Q-homogeneous component of H'/H'', then M is normalized by W. In fact, every element of W commutes with the elements of Q, and therefore induces a Q-automorphism of H'/H'' by conjugation; on the other hand, M is left invariant by every Q-endomorphism of H'/H'', and thus is normalized by W. It follows that M is a non-trivial normal subgroup of H'/H''. In particular, M intersects S non-trivially. Because we have proved that S is Q-homogeneous, it follows that H'/H'' has only one Q-homogeneous component. In other words, H'/H'' is Q-homogeneous, and the proof is complete. $\square$

It remains to show that some chief factor of H between H' and H'' is

H-isomorphic to H''. As we have already remarked in several places, since Q complements the Fitting subgroup P of H in H, it is sufficient to find a Q-isomorphism from a chief factor of H between H' and H'' onto H''. The tool which will produce such an isomorphism is Lemma 2.2.4.

Let us fix an element w of $W = \mathbf{C}_P(Q)$. The map from H' to itself which sends x to $[x, w]$ is not a group homomorphism, and thus its image $\lfloor H', w \rfloor$ is not necessarily a subgroup of H'. However, according to Lemma 2.2.4 and the discussion which precedes it, the inverse image of H'' under this map, namely

$$M_w = \{x \in H' \mid [x, w] \in H''\},$$

is a subgroup of H', and the restriction

$$\begin{aligned} \varphi_w : M_w &\rightarrow H'' \\ x &\mapsto [x, w] \end{aligned}$$

of our map is a WQ-homomorphism with kernel $\mathbf{C}_{H'}(w)$. From the fact that $H'' \leq \mathbf{Z}(P)$ it follows that the subgroups M_w and $\mathbf{C}_{H'}(\bar{w})$ of H' contain H''; therefore, they are normal in H', because H'/H'' is abelian. The fact that they are normalized by WQ finally implies that they are normal subgroups of H.

Let us suppose for a moment that our WQ-homomorphism φ_w is surjective. Then φ_w induces a WQ-isomorphism from $M_w/\mathbf{C}_{H'}(w)$, which therefore is a chief factor of H, onto H''. Thus the assertion that some chief factor of H between H' and H'' is WQ-isomorphic to H'' is proved, provided we can show that $H'' \subseteq \lfloor H', w \rfloor$, or equivalently that $H'' \subseteq \lfloor w, H' \rfloor$, for some $w \in W$.

We shall infer this fact from a corresponding fact for G by means of the character table isomorphism (α, β). Indeed, we shall prove the following lemma.

Lemma 3.3.3 *Assume Hypotheses 3.1.2. Then $wN \subseteq w^G$ for all $w \in W \setminus 1$, and $wH'' \subseteq w^H$ for all $w \in W \setminus 1$.*

Proof Let us fix $w \in W = \mathbf{C}_{G'}(Q)$ and let us consider the map

$$\varphi_w : G' \rightarrow G'$$

defined by $x^{\varphi_w} = [x, w]$. According to Lemma 2.2.3 (with H_1, H_2, K_1, K_2, w, Q replaced by G', G', 1, 1, w, WQ respectively), the map φ_w is a WQ-homomorphism. Thus the situation here is much better than it was for H. In fact, the image $(G')^{\varphi_w} = [G', w]$ of φ_w is a WQ-subgroup of G'; hence it is a normal subgroup of G, because G' is abelian and $G = G'WQ$.

Now let us assume that $w \neq 1$. Then w does not centralize G', because we know from Lemma 3.2.1 that W acts faithfully on G' by conjugation. Hence φ_w is not the trivial homomorphism. In particular, its image $[G', w] = [G', w]$ is a non-trivial normal subgroup of G, and therefore it contains the unique minimal normal subgroup N. This is clearly equivalent to $N \subseteq [w, G']$, and eventually to $wN \subseteq w^G$. This clearly implies the first assertion of the lemma.

In order to pass on this piece of information to H we shall first express it in character-theoretical language. According to Lemma 4.2.1, the statement

$$wN \subseteq w^G \quad \text{for all } w \in W \setminus 1$$

is equivalent to

$$\chi(w) = 0 \quad \text{for all } \chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N) \quad \text{and for all } w \in W \setminus 1.$$

We must be cautious here in applying the character table isomorphism (α, β), because W^α does not necessarily coincide with W, indeed, W^α is not necessarily a subgroup of H. But we observe that since characters are class functions, the statement

$$\chi(g) = 0 \quad \text{for all } \chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$$

actually holds for all $g \in G$ which are conjugate to some $w \in W \setminus 1$.

Now we claim that the set of elements $g \in G$ which are conjugate to some element of W coincides with the set of elements $g \in P$ such that $|Q|$ divides $|\mathbf{C}_G(g)|$ (and a similar assertion holds for H). In fact, if $g \in G$ is conjugate to $w \in W$, then $|\mathbf{C}_G(g)| = |\mathbf{C}_G(w)|$, and $|Q|$ divides $|\mathbf{C}_G(w)|$ because $Q \leq \mathbf{C}_G(w)$. On the other hand, suppose that $|Q|$ divides the order of the centralizer in G of an element g of G. According to the Theorem of Schur-Zassenhaus, there exists a complement Q_0 for $P \cap \mathbf{C}_G(g)$ in $\mathbf{C}_G(g)$. Since $|G|_{p'} = |Q|$ divides $|\mathbf{C}_G(g)|$, we have $|Q_0| = |Q|$; therefore Q_0 is a complement for P in G. The conjugacy part of the Theorem of Schur-Zassenhaus yields now that $Q = Q_0^x$ for some $x \in G$. Since obviously $g \in \mathbf{C}_P(Q_0)$, it follows that $g^x \in \mathbf{C}_P(Q_0^x) = \mathbf{C}_P(Q) = W$, and therefore g is conjugate to some element of W. Our claim is proved. The analogous claim for H can be proved similarly.

Thus we have

$$\chi(g) = 0 \quad \text{for all } \chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N),$$

for all $g \in P\setminus 1$ such that $|Q|$ divides $|\mathbf{C}_G(g)|$. Let us apply the character table automorphism (α, β) to this statement. After noticing that $P^\alpha = P$, and that $|\mathbf{C}_H(g^\alpha)| = |\mathbf{C}_G(g)|$ for all $g \in G$ (according to the second orthogonality relation), we obtain

$$\chi(h) = 0 \quad \text{for all } \chi \in \mathrm{Irr}(H) \setminus \mathrm{Irr}(H/H''),$$

for all $h \in P\setminus 1$ such that $|Q|$ divides $|\mathbf{C}_H(h)|$. Since in particular $|Q|$ divides $|\mathbf{C}_H(w)|$ for all $w \in W$, an application of Lemma 4.2.1 yields

$$wH'' \subseteq w^H \quad \text{for all } w \in W \setminus 1,$$

which concludes the proof. $\square$

Now the second assertion of Lemma 3.3.3 together with the fact that $W \neq 1$ (see the note after Lemma 3.2.1) implies that there exists some $w \in W \setminus 1$ such that $H'' \subseteq [H, w]$. Since $H = WQH'$ and $[WQ, w] = 1$, we have $[H, w] = [H', w]$. It follows that the WQ-homomorphism

$$\begin{aligned} \varphi_w : M_w &\rightarrow H'' \\ x &\mapsto [x, w], \end{aligned}$$

which we defined in the discussion preceding Lemma 3.3.3, is an epimorphism, and thus induces an H-isomorphism of some chief factor of H between H' and H'' onto H''. Thus we have the following lemma.

Lemma 3.3.4 *Assume Hypotheses 3.1.2. Then all chief factors of H below H' are H-isomorphic.*

Proof The assertion follows from the preceding discussion together with Lemma 3.3.2. $\square$

Let us remark again that since Q is a complement for the Fitting subgroup $\mathbf{F}(G)$ in G, any chief factor of G is irreducible as a Q-group and is therefore a composition factor of G as a Q-group (similarly for H). Hence Lemma 3.3.1 and Lemma 3.3.4 imply that all Q-composition factors of G' are Q-isomorphic and respectively that all Q-composition factors of H' are Q-isomorphic.

3.4 More about the action of Q on H'

In the previous section we have proved in particular that all Q-composition factors of H' are Q-isomorphic. On the other hand, the actions of Q on H'/H'' and on H'' are not independent: in fact the action of Q on $H'/\mathbf{Z}(H')$ determines uniquely the action of Q on H'' via the operation of forming commutators. In this section we shall play these two facts against each other in order to draw further consequences about the action of Q on H'. This will require the machinery developed in Sections 2.2 and 2.3, but the simpler reasoning of the next proposition will give the reader a taste of the method.

First let us recall a basic fact about automorphisms of cyclic p-groups: if C is a cyclic group of order p^e (p a prime), and $\bar\psi$ is an automorphism of p'-order of $C/\Phi(C)$, then there is a unique automorphism ψ of p'-order of C which induces $\bar\psi$. In fact, $\bar\psi$ has the form

$$c^{\bar\psi} = c^a \bmod \Phi(C) \quad \text{for all } c \in C,$$

for some integer a (which is unique if we require $0 < a < p$). The map $\tilde\psi : C \to C$ defined by

$$c^{\tilde\psi} = c^a \quad \text{for all } c \in C,$$

is an automorphism of C, because p does not divide a. However, $\tilde\psi$ might have order divisible by p. According to [10, Kapitel I, Satz 4.6 and Satz 13.19], the group of automorphisms of C is abelian (cyclic if $p \neq 2$) of order $(p-1)p^{e-1}$, hence if f is any integer greater than or equal to $e-1$, then the automorphism $\psi = \tilde\psi^{p^f}$ of C has p'-order. We clearly have

$$c^{\psi} = c^b \quad \text{for all } c \in C,$$

where $b = a^{p^f}$. Since $b \equiv a \pmod{p}$, the automorphism of $C/\Phi(C)$ induced by ψ is $\bar\psi$. The uniqueness of ψ follows from the fact that C and $C/\Phi(C)$ have the same number of automorphisms of p'-order, namely $p-1$.

Proposition 3.4.1 *Assume Hypotheses 3.1.2. Then H'' is not cyclic.*

Proof Let us assume for a contradiction that H'' is cyclic, whence it has order p. Let us choose a generator η of Q and let a be the unique integer with $1 \leq a < p$ such that

$$z^\eta = z^a \quad \text{for all } z \in H''.$$

The abelian factor group H'/H'' has a decomposition into a direct product of Q-indecomposable groups. Let C be one of them. According to Theorem 2.4.2, the group C is homocyclic and $C/\Phi(C)$ is an irreducible Q-group; hence $C/\Phi(C)$ is a Q-composition factor of H'/H''. Since all Q composition factors of H'/H'' are Q-isomorphic to H'' by Lemma 3.3.4, we have that $C/\Phi(C)$ is cyclic of order p. Consequently, C is cyclic. Because $C/\Phi(C)$ is Q-isomorphic to H'', we have

$$c^\eta \equiv c^a \bmod \Phi(C) \quad \text{for all } c \in C.$$

If p^e is the exponent of H'/H'', then $|C|$ divides p^e. Since η acts on C as an automorphism of order prime to p, the remark which precedes this proposition yields

$$c^\eta = c^b \quad \text{for all } c \in C,$$

where $b = a^{p^{e-1}}$. Now this holds for all Q-indecomposable groups C of which H'/H'' is the direct product, and therefore we have

$$x^\eta = x^b \bmod H'' \quad \text{for all } x \in H'.$$

We also have

$$z^\eta = z^b \quad \text{for all } z \in H'',$$

because $b \equiv a \pmod{p}$.

Now let us choose $x, y \in H'$ such that $[x, y] \neq 1$, whence $\langle [x, y] \rangle = H''$. Remembering that $H'' \leq \mathbf{Z}(H')$, we compute

$$[x, y]^\eta = [x^\eta, y^\eta] = [x^b, y^b] = [x, y]^{b^2}.$$

On the other hand, since $[x, y] \in H''$ we have

$$[x, y]^\eta = [x, y]^b.$$

Since $[x, y]$ has order p, it follows that $b^2 \equiv b \pmod{p}$; it follows that $b \equiv 1 \pmod{p}$, because b is not divisible by p. But this implies that

$$z^\eta = z^b = z \quad \text{for all } z \in H'',$$

or in other words, that η centralizes H''. This contradicts the fact that Q acts faithfully on H'', by Lemma 3.2.1. Hence our assumption is wrong, and thus H'' cannot be cyclic. □

The key idea of the proof of Proposition 3.4.1, namely that the action of Q on H' must be compatible with commutation, will now be generalized to the case in which H'' is not assumed to be cyclic. However, this will not lead to any contradiction in general.

Let us assume Hypotheses 3.1.2, and let us fix a chief series of H going from 1 to H' thus:

$$1 < H'' = K_1 < K_2 < \cdots < K_t = H'.$$

Let r be the smallest index i such that $K_i \not\leq \mathbf{Z}(H')$ (since H' is not abelian such an index exists), and then let s be the smallest index j such that $[K_r, K_j] \neq 1$. Then we clearly have $1 < r \leq s \leq t$.

Since $[K_r, K_s] \leq H'' \leq \mathbf{Z}(H')$ and $[K_r, K_{s-1}] = [K_{r-1}, K_s] = 1$, according to Lemma 2.2.1 the map

$$\gamma : K_r/K_{r-1} \times K_s/K_{s-1} \rightarrow H''$$

such that

$$(xK_{r-1}, yK_{s-1})^\gamma = [x, y] \quad \text{for all } x \in K_r \quad \text{and for all } y \in K_s,$$

is $\mathbf{Z}$-bilinear. Moreover, if $r = s$, the map γ is skew-symmetric.

Since K_r/K_{r-1}, K_s/K_{s-1} and H'' have exponent p, they can be regarded as vector spaces over $\mathbf{F}_p$, and the map γ is $\mathbf{F}_p$-bilinear. We shall put $V_1 = K_r/K_{r-1}$, $V_2 = K_s/K_{s-1}$ and $V = H''$.

Let $V_1 \otimes V_2$ denote the tensor product of V_1 and V_2 over $\mathbf{F}_p$. According to the universal property of tensor products, there exists a unique $\mathbf{F}_p$-linear map $\tilde{\gamma} : V_1 \otimes V_2 \rightarrow V$ such that

$$(v_1 \otimes v_2)^{\tilde{\gamma}} = (v_1, v_2)^\gamma \quad \text{for all } v_1 \in V_1 \quad \text{and for all } v_2 \in V_2.$$

Now V_1, V_2 and V are irreducible $\mathbf{F}_p Q$-modules by conjugation, and according to Lemma 3.3.4, they are all isomorphic.

The tensor product $V_1 \otimes V_2$ becomes an $\mathbf{F}_p Q$-module in a standard way (see for instance [13, Chapter 4], [10, Kapitel V, Definition 10.4], or [5, Definition (10.15)]). In short, the action of a generator η of Q on $V_1 \otimes V_2$ is defined on the pure tensors $v_1 \otimes v_2$ (for $v_i \in V_i$) by the formula

$$(v_1 \otimes v_2)\eta = v_1\eta \otimes v_2\eta$$

and extended $\mathbf{F}_p$-linearly to $V_1 \otimes V_2$. (Although the module action in this case is given by conjugation, instead of the exponential notation v_1^η we shall use the more common notation $v_1\eta$.)

Since $[x^\eta, y^\eta] = [x, y]^\eta$ for all $x \in K_r$ and $y \in K_s$, we have

$$((v_1 \otimes v_2)\eta)^\gamma = ((v_1 \otimes v_2)^\gamma)\eta$$

for all pure tensors $v_1 \otimes v_2$; hence it follows by linearity that

$$(w\eta)^\gamma = (w^\gamma)\eta \quad \text{for all } w \in V_1 \otimes V_2.$$

Thus $\gamma : V_1 \otimes V_2 \to V$ is an $\mathbf{F}_p Q$-module homomorphism. It cannot be the zero homomorphism, because $[K_r, K_s] \neq 1$. But V is an irreducible $\mathbf{F}_p Q$-module, and therefore γ is an epimorphism. Hence the tensor square $\mathbf{F}_p Q$-module $V \otimes V$ (which is isomorphic to $V_1 \otimes V_2$) has some factor module isomorphic to V. This is impossible when V has dimension 1 over $\mathbf{F}_p$ (unless V is the trivial module, which it is not in our case, according to Lemma 3.2.1). In fact, if V has dimension 1, then $V \otimes V$ also has dimension 1; in particular $V \otimes V$ is irreducible, but it cannot be isomorphic to V, unless V is the trivial module. For, let v be a generator of V; hence $v \otimes v$ generates $V \otimes V$. We have $v\eta = av$ for some $a \in \mathbf{F}_p^\times$ (which is clearly independent of the choice of v), and thus

$$(v \otimes v)\eta = v\eta \otimes v\eta = av \otimes av = a^2(v \otimes v).$$

It is clear then that V and $V \otimes V$ are not isomorphic unless $a = a^2$, that is to say $a = 1$ (because $a \neq 0$), which means that V is the trivial module. Thus we obtain a different formulation of the proof of Proposition 3.4.1.

In the next section we shall examine when $V \otimes V$ has a factor module isomorphic to V, for small values of the dimension of V over $\mathbf{F}_p$. But before doing that, we observe that in the special case in which $r = s$ we have $V_1 = V_2$, and the bilinear map γ is skew-symmetric, which means

$$(v, v)^\gamma = 0 \quad \text{for all } v \in V_1.$$

The subspace

$$W = \langle v \otimes v \in V_1 \otimes V_1 \mid v \in V_1 \rangle$$

of $V_1 \otimes V_1$, which is clearly an $\mathbf{F}_p Q$-submodule of $V_1 \otimes V_1$, is therefore contained in the kernel of the $\mathbf{F}_p Q$-module epimorphism γ.

The factor space $V_1 \otimes V_1 / W$ is by definition the exterior square $V_1 \wedge V_1$, which thus becomes an $\mathbf{F}_p Q$-module (with the notation of [11, Chapter VII, Definition 8.16] and according to [11, Chapter VII, Lemma 8.17], we have $V_1 \wedge V_1 = V_1 \otimes V_1 / \mathbf{S}(V_1) \cong \mathbf{A}(V_1)$; see also [5, §12A]).

Hence we obtain an $\mathbf{F}_p Q$-module epimorphism $\bar{\gamma} : V_1 \wedge V_1 \to V$, such that

$$(v_1 \wedge v_2)^{\bar{\gamma}} = (v_1, v_2)^\gamma \quad \text{for all } v_1, v_2 \in V_1,$$

where by definition

$$v_1 \wedge v_2 = (v_1 \otimes v_2) + W \in V_1 \wedge V_1.$$

Therefore, when $r = s$, the $\mathbf{F}_p Q$-module V is isomorphic to a factor module of $V \wedge V$.

We shall henceforth distinguish between the case in which $r < s$ (which only gives rise to a map $\gamma : V_1 \otimes V_2 \to V$) and the case in which $r = s$ (which in addition gives rise to a map $\bar{\gamma} : V_1 \wedge V_1 \to V$) by referring to them as *the binary case* and *the unary case*.

3.5 The smallest cases which can occur

In this section we shall investigate for which values of p and $|Q|$ the modules $V \otimes V$ and $V \wedge V$ have a composition factor isomorphic to V, where V is a faithful irreducible module for the cyclic p'-group Q over $\mathbf{F}_p$.

Let $\mathbb{E}$ be a splitting field for the polynomial $x^{|Q|} - 1$ over $\mathbf{F}_p$; hence $\mathbb{E}$ is the smallest extension field of $\mathbf{F}_p$ which contains a primitive $|Q|$th root of unity, or, in other words, the smallest extension field of $\mathbf{F}_p$ whose multiplicative group $\mathbb{E}^\times$ contains a subgroup of order $|Q|$ (which is necessarily cyclic). Hence $\mathbf{E}$ is clearly isomorphic to $\mathbf{F}_{p^n}$, where n is the multiplicative order of p (mod $|Q|$), that is to say, n is the smallest positive integer such that $|Q|$ divides $p^n - 1$. According to Theorem 2.3.1, the integer n equals the dimension of V over $\mathbf{F}_p$.

Since $|Q|$ is not divisible by p, the $\mathbf{F}_p$-algebra $\mathbf{F}_pQ$ is semisimple, according to Maschke's Theorem. In particular, $V \otimes V$ and $V \wedge V$ are semisimple $\mathbf{F}_pQ$-modules. According to Corollary 2.3.3, the composition factors of $V \otimes V$ and $V \wedge V$ as $\mathbf{F}_pQ$-modules are completely determined by the composition factors of $(V \otimes V)^{\mathbf{E}}$ and $(V \wedge V)^{\mathbf{E}}$ as $\mathbf{E}Q$-modules. It is easy to see that

$$(V \otimes V)^{\mathbf{E}} \cong V^{\mathbf{E}} \otimes V^{\mathbf{E}} \quad \text{and} \quad (V \wedge V)^{\mathbf{E}} \cong V^{\mathbf{E}} \wedge V^{\mathbf{E}}.$$

Let ε be a primitive $|Q|$th root of unity in $\mathbf{E}$. The discussion which follows Theorem 2.3.1 yields that $\varepsilon, \varepsilon^p, \ldots, \varepsilon^{p^{n-1}}$ are all the distinct eigenvalues of η (a generator of Q) on $V^{\mathbf{E}}$. Moreover, $V^{\mathbf{E}}$ has a basis $v_0, \ldots, v_{n-1}$ over $\mathbf{E}$ such that

$$v_i\eta = \varepsilon^{p^i} v_i, \quad \text{for all } i = 0, \ldots, n-1.$$

Thus bases for $V^{\mathbf{E}} \otimes V^{\mathbf{E}}$ and $V^{\mathbf{E}} \wedge V^{\mathbf{E}}$ over $\mathbf{E}$ are given by

$$v_i \otimes v_j, \text{ for } i, j = 0, \ldots, n-1,$$

and respectively

$$v_i \wedge v_j, \text{ for } 0 \leq i < j < n.$$

These bases are made of eigenvectors for η; in fact

$$(v_i \otimes v_j)\eta = v_i\eta \otimes v_j\eta = \varepsilon^{p^i + p^j}(v_i \otimes v_j)$$

and

$$(v_i \wedge v_j)\eta = v_i\eta \wedge v_j\eta = \varepsilon^{p^i + p^j}(v_i \wedge v_j).$$

The eigenvalues for η on $V^{\mathbf{E}} \otimes V^{\mathbf{E}}$ and $V^{\mathbf{E}} \wedge V^{\mathbf{E}}$ (considered with multiplicities) can be grouped into Galois conjugacy classes, which in turn determine the isomorphism classes of the composition factors of $V^{\mathbf{E}} \otimes V^{\mathbf{E}}$ and respectively of $V^{\mathbf{E}} \wedge V^{\mathbf{E}}$ as $\mathbf{F}_pQ$-modules, according to Theorem 2.3.2.

Sets of representatives of the distinct Galois conjugacy classes of the eigenvalues of η on $V^{\mathbf{E}} \otimes V^{\mathbf{E}}$ and $V^{\mathbf{E}} \wedge V^{\mathbf{E}}$ are contained in the set

$$\{\varepsilon^{p^i+1} \mid 0 \leq i \leq n/2\}$$

and respectively in the set

$$\{\varepsilon^{p^i+1} \mid 0 < i \leq n/2\}.$$

In fact, the eigenvalue $\varepsilon^{p^i+p^j}$ is Galois conjugate to $\varepsilon^{p^{j-i}+1} = (\varepsilon^{p^i+p^j})^{p^{n-i}}$ and to $\varepsilon^{p^{n+i-j}+1} = (\varepsilon^{p^i+p^j})^{p^{n-j}}$; on the other hand, if $0 \leq i \leq j < n$, then we have either $0 \leq j - i \leq n/2$ or $0 \leq n + i - j \leq n/2$.

Hence $V \otimes V$ has a composition factor (hence a direct summand, because $V \otimes V$ is semisimple) isomorphic to V exactly when ε^{p^j} appears as an element of the set $\{\varepsilon^{p^i+1} \mid 0 \leq i \leq n/2\}$ for some $j = 0, \ldots, n-1$. A similar assertion holds for $V \wedge V$. We shall state both assertions in the following lemma.

Lemma 3.5.1 *Let V be a faithful irreducible module for a cyclic group Q over $\mathbf{F}_p$ (in particular p does not divide $|Q|$) and let n be the dimension of V over $\mathbf{F}_p$. Then:*

(i) *the tensor square $\mathbf{F}_pQ$-module $V \otimes V$ has a direct summand isomorphic to V if and only if*

$$p^i + 1 \equiv p^j \bmod |Q|$$

for some i, j with $0 \leq i \leq n/2$ and $0 \leq j < n$ (or, equivalently, for some non-negative integers i, j);

(ii) *the exterior square $\mathbf{F}_pQ$-module $V \wedge V$ has a direct summand isomorphic to V if and only if*

$$p^i + 1 \equiv p^j \bmod |Q|$$

for some i, j with $0 < i \leq n/2$ and $0 < j < n$ (or, equivalently, for some non-negative integers i, j, with i not a multiple of n).

We observe here that we may also restrict our attention to $|Q|$ odd in Lemma 3.5.1. In fact, if $|Q|$ is even, then p is odd, and hence the congruence $p^i + 1 \equiv p^j \pmod{|Q|}$, has clearly no solution. It follows in particular that if (G, H) is a pair of groups which satisfy Hypotheses 3.1.2, then the cyclic complement Q for the normal Sylow p-subgroup of H has odd order. However, this is also a consequence of the general fact that a non-abelian group cannot have a fixed-point-free automorphism of order 2, according to [10, Kapitel V, Satz 8.18] (while any non-identity element of Q induces a fixed-point-free automorphism of the non-abelian group H' by conjugation).

We shall see in Chapter 5 that all the cases described in Lemma 3.5.1 actually arise from the analysis of counterexamples to Conjecture 3.1.1. In other words, for any faithful irreducible module V for a non-trivial cyclic group Q over $\mathbf{F}_p$ such that $V \otimes V$ (respectively $V \wedge V$) has a composition factor isomorphic to V, there exists a pair of groups (G, H) satisfying Hypotheses 3.1.2 and such that

- Q is a complement for the normal Sylow p-subgroup of H,
- H'' is isomorphic to V when it is regarded as an $\mathbf{F}_pQ$-module by conjugation,
- the map γ (respectively γ) arising from some chief series of H, as described in the last section, is an $\mathbf{F}_pQ$-module epimorphism of $V \otimes V$ (respectively of $V \wedge V$) onto V.

Now let us take a different point of view. We shall explicitly construct pairs (G, H) of groups satisfying Hypotheses 3.1.2 in Chapter 5: we would like them to be as small as possible. Therefore it makes sense to fix a small value n of the dimension of V and then determine for which primes p and cyclic p'-groups Q some (actually, according to Lemma 3.5.1, any) faithful irreducible module V for Q over $\mathbf{F}_p$ appears as a composition factor of $V \otimes V$, or even of $V \wedge V$. We shall see in some detail what happens for $n = 1, 2, 3, 4$ and show in particular that while case (i) of Lemma 3.5.1 can already happen for $n = 2$, case (ii) does not occur unless $n \geq 4$.

Case $n = 1$. We have already seen that in this case $V \otimes V$ (which is irreducible, because it has dimension 1 over $\mathbf{F}_p$) cannot be isomorphic to V as an $\mathbf{F}_pQ$-module.

Case $n = 2$. Since in this case $V \wedge V$ has dimension 1, it is irreducible and certainly not isomorphic to V, which has dimension 2.

On the other hand, $V \otimes V$ has dimension 4 over $\mathbf{F}_p$. According to Lemma 3.5.1 then $V \otimes V$ has a composition factor isomorphic to V if and only if $p^i + 1 \equiv p^j \pmod{|Q|}$ for some $i = 0, 1$ and $j = 0, 1$. The cases $(i, j) = (0, 0), (1, 0), (1, 1)$ are easily ruled out, remembering that p does not divide $|Q|$. Hence we are left with $p^0 + 1 = p \pmod{|Q|}$. If this is the case, from $|Q| \mid (p - 2)$ it follows that $(|Q|, p - 1) = 1$. Now $\mathbf{F}_{p^2}$ contains a primitive $|Q|$th root of unity according to Theorem 2.3.1; consequently, $|Q|$ divides

$|\mathbb{F}_{p^2}^\times| = p^2 - 1 = (p-1)(p+1)$. Therefore $|Q|$ divides both $p+1$ and $p-2$, and hence $|Q| = 3$.

Thus there exists a two-dimensional faithful irreducible module V for a cyclic group Q over $\mathbb{F}_p$ such that V is isomorphic to a composition factor of $V \otimes V$, if and only if $|Q| = 3$ and $p \equiv -1 \pmod 3$.

Case $n = 3$. It is certainly possible that V is isomorphic to a composition factor of $V \otimes V$. For instance, when $|Q| = 7$ and $p \equiv 4 \pmod 7$ we have that p has multiplicative order 3 $(\mathrm{mod}\ |Q|)$ and that $p^0 + 1 \equiv p^2 \pmod{|Q|}$. However, we shall not go into further details here. We shall only prove that $V \wedge V$ cannot have any composition factor isomorphic to V. In fact, if this were true we would have, according to Lemma 3.5.1, that $p+1 \equiv p^j \bmod |Q|$ for some $j = 0, 1, 2$. Since the cases $j = 0, 1$ are easily ruled out, we would have that $|Q|$ divides $p^2 - p - 1$. On the other hand, because $\mathbb{F}_{p^3}$ must contain a primitive $|Q|$th root of unity, $|Q|$ should divide $p^3 - 1$. It would follow that $|Q|$ divides $(p^3 - 1) - (p+1)(p^2 - p - 1) = 2p$, and this contradicts the fact that $|Q|$ is odd and prime to p.

Case $n = 4$. We shall prove that if V has dimension 4 it can happen that V is a composition factor of $V \wedge V$ (and hence of $V \otimes V$ too). According to Lemma 3.5.1 we need to determine for which values of p and $|Q|$ it is possible to have $p^i + 1 \equiv p^j \pmod{|Q|}$ for some $i = 1, 2$ and $j = 0, 1, 2, 3$.

It is not difficult to rule out the cases with $i = 2$, either by working with the congruences or by simply noticing that the eigenvalues ε^{p^2+1} and ε^{p^3+p} of a generator η of Q on $V \wedge V$ form a Galois conjugacy class of length two over $\mathbb{F}_p$, which thus corresponds to a composition factor of $V \wedge V$ of dimension two, in particular not isomorphic to V, which has dimension $n = 4$. Hence we are left with $i = 1$.

Now the cases $(i, j) = (1, 0), (1, 1)$ are clearly impossible; hence we have either $(i, j) = (1, 2)$ or $(i, j) = (1, 3)$. In the first case, we have that $p + 1 \equiv p^2$ $(\mathrm{mod}\ |Q|)$, in other words $|Q|$ divides $p^2 - p - 1$. Keeping in mind that $|Q|$ also divides $p^4 - 1 = |\mathbb{F}_{p^4}^\times|$, we obtain that $|Q|$ divides

$$(p^4 - 1) - (p^2 - p - 1)(p^2 + 1) = p(p^2 + 1)$$

and therefore that $|Q|$ divides $p^2 + 1$. Hence $|Q|$ also divides

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

Now from $p^2 \equiv -1 \pmod{|Q|}$ and $p \equiv -2 \pmod{|Q|}$ we obtain that $5 \equiv 0 \pmod{|Q|}$. It follows that $|Q| = 5$ and $p \equiv 3 \pmod{|Q|}$. In a similar way one can find that in the case $(i, j) = (1, 3)$ it must be $|Q| = 5$ and $p \equiv 2 \pmod{|Q|}$.

Conversely, if $|Q| = 5$ and $p \equiv 3 \pmod{|Q|}$ or $p \equiv 2 \pmod{|Q|}$, then p has multiplicative order 4 $\pmod{|Q|}$ and $p + 1 \equiv p^2 \pmod{|Q|}$, or respectively $p + 1 \equiv p^3 \pmod{|Q|}$.

We conclude that there exists a faithful irreducible module V of dimension 4 over $\mathbf{F}_p$ for a cyclic group Q, such that V is isomorphic to a composition factor of $V \wedge V$, exactly when $|Q| = 5$ and $p \equiv 2$ or $3 \pmod 5$.

Chapter 4

Comparing character tables

4.1 Our philosophy

We said in Chapter 1 that two groups can have identical character tables without being isomorphic. But how can one compare character tables in practice? In this chapter we shall develop a method which allows one to do this, in special situations. We shall employ some basic Clifford theory. This is the part of character theory which analyzes the relations between the characters of a group G and the characters of a normal subgroup N of G. For our present purposes, the two most fundamental results of Clifford theory will suffice, namely Clifford's Theorem (see [13, Theorem 6.2]), and the Clifford Correspondence ([13, Theorem 6.11]).

Let us start from the side of group theory by recalling the well-known analysis of a group G in terms of a normal subgroup N of G and the factor group G/N. Given two groups N and H, there are in general many ways of constructing a group G which has N as a normal subgroup and such that $G/N \cong H$. This is the so-called extension problem for groups, and its answer is given by the following well-known theorem.

Theorem 4.1.1 *Let H and N be groups, let*

$$h \mapsto \varphi(h)$$

be a map from H into $\mathrm{Aut}(N)$, *and let*

$$(h_1, h_2) \mapsto f(h_1, h_2)$$

be a map from $H \times H$ into N, a so-called factor system. Let us assume that φ and f satisfy the following conditions, for all $n \in N$ and for all $h_i, h \in H$:

(1) $f(h_1, h_2h_3)f(h_2, h_3) = f(h_1h_2, h_3)f(h_1, h_2)^{\varphi(h_3)}$,

(2) $n^{\varphi(h_1)\varphi(h_2)} = (n^{\varphi(h_1h_2)})^{f(h_1,h_2)}$,

(3) $f(h, 1) = f(1, h) = 1$.

Let us define a multiplication on the cartesian product

$$G = \{(h, n) \mid h \in H,\ n \in N\},$$

through the formula

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, f(h_1, h_2)n_1^{\varphi(h_2)}n_2).$$

Then G becomes a group with this multiplication. The set

$$\bar{N} = \{(1, n) \mid n \in N\}$$

is a normal subgroup of G isomorphic to N, and the factor group $G/\bar{N}$ is isomorphic to H. The group G is called the extension of H by N with respect to the automorphisms $\varphi(h)$ and the factor set $f(\ ,\ )$.

Proof See [10, Kapitel I, Satz 14.2], or [8, Theorem 15.1.1]. □

Let us summarize Theorem 4.1.1 by saying that in order to construct the group G from the normal subgroup N and the factor group G/N, we need the following ingredients:

(i) the group $H = G/N$,

(ii) the group N, together with a map $\varphi : H \to \mathrm{Aut}(N)$,

(iii) a factor set $f : H \times H \to N$;

moreover, conditions (1), (2), and (3) of Theorem 4.1.1 have to be satisfied.

Let us say that our ingredient (*iii*) is usually the most difficult to handle, and can be dealt with by using cohomological methods.

Let us remark that in the special case in which N is abelian, and more generally when $f(h_1, h_2) \in \mathbf{Z}(N)$ for all $h_1, h_2 \in H$, the map

$$h \mapsto \varphi(h)$$

is a group homomorphism from H into $\mathrm{Aut}(N)$; thus when N is abelian, it becomes a $\mathbb{Z}H$-module. When N is arbitrary, the map φ is not a group homomorphism; however, the composite map

$$\varphi\pi : H \to \mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Inn}(N)$$

is a homomorphism, where $\pi : \mathrm{Aut}(N) \to \mathrm{Aut}(N)/\mathrm{Inn}(N)$ is the natural epimorphism. As a consequence, φ induces an action of H on the set of conjugacy classes of N. The knowledge of the orbits of this action allows one to determine the conjugacy classes of G which are contained in N. More information is needed in general in order to determine the remaining conjugacy classes of G, namely some information about the factor set f is necessary.

Let us turn our attention to the character tables now. Let us order the conjugacy classes of G in such a way that those which are contained in the normal subgroup N precede those which are contained in $G \setminus N$. Similarly, for the irreducible characters of G, let us first list those whose kernel contains N, which we shall identify with the characters of G/N, and then the remaining ones. The character table T of G can be divided into four submatrices accordingly, thus:

$$\begin{array}{rc} & \begin{array}{cc} N & G\setminus N \end{array} \\ \begin{array}{r} \mathrm{Irr}(G/N) \\ \mathrm{Irr}(G)\setminus\mathrm{Irr}(G/N) \end{array} & \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \end{array}$$

Let us examine which of the submatrices A, B, C, D of T is influenced by each of our ingredients (i), (ii), and (iii).

Ingredient (i), namely the factor group $H = G/N$, gives information about A and B. In fact, the submatrix of T made up of the submatrices A and B coincides with the character table $\bar{T}$ of the factor group G/N, except that some columns of $\bar{T}$ are repeated in A or B (in particular all the columns of A are equal). Therefore (i) determines the number of rows of A and B, and all the entries, up to repeating some columns.

Now let us see how the normal subgroup N together with the map $\varphi : H \to \mathrm{Aut}(N)$, which constitute our ingredient (ii), give information about A and C. The matrices A and C display the restrictions of the irreducible characters of G to the normal subgroup N. According to Clifford's Theorem, if χ is an irreducible character of G, then its restriction χ_N is a multiple of the sum over a G-orbit of irreducible characters of N. We are assuming that the group N is known; consequently, its character table is uniquely determined.

We have already said that the map φ determines an action of $H = G/N$ on the set of conjugacy classes of N; to be explicit, if $h \in H$ and $\mathcal{K}$ is a conjugacy class of N, then $\mathcal{K}^h$ is the conjugacy class of N given by

$$\mathcal{K}^h = \{n^{\varphi(h)} \mid n \in \mathcal{K}\}.$$

The map φ also determines an action of H on $\mathrm{Irr}(N)$ via

$$\theta^h(n) = \theta(n^{\varphi(h)^{-1}}) \text{ for all } n \in N,$$

where $h \in H$ and $\theta \in \mathrm{Irr}(N)$. In other words, the map φ induces two actions of H, one on the set of columns and one on the set of rows of the character table of N. Therefore, assuming that we are able to write the character table of N, we can replace each set of rows of the table which correspond to a G-orbit of $\mathrm{Irr}(N)$ with a single row, namely their sum; finally, we can delete multiple columns. Let us call $\tilde{T}$ the matrix which we obtain. Then, first of all, A and C have the same number of columns as $\tilde{T}$. Secondly, possibly after permuting the columns of $\tilde{T}$, each row of A or C is a multiple of some row of $\tilde{T}$ by a positive integer; on the other hand, each row of $\tilde{T}$ has some multiple which appears as a row of either A or C. In other words, the submatrix of T made up of A and C has the same number of columns as $\tilde{T}$, and can be obtained from $\tilde{T}$ by repetition of some rows and then multiplication of some rows by some positive integers.

The little asymmetry in the ways in which we obtained A, B from T and A, C from $\tilde{T}$ would disappear if we considered the table of central characters ω_χ of G, instead of the ordinary character table of G; here the central character ω_χ associated with the irreducible character χ of G is the map from G into $\mathbb{C}$ defined by the formula

$$\omega_\chi(g) = \frac{\chi(g)}{\chi(1)} \text{ for all } g \in G$$

(the name *central character* is due to the fact that ω_χ can be extended $\mathbb{C}$-linearly to a character of the centre $\mathbf{Z}(\mathbb{C}G)$ of the group algebra $\mathbb{C}G$, in other words, to a $\mathbb{C}$-algebra homomorphism from $\mathbf{Z}(\mathbb{C}G)$ into $\mathbb{C}$).

We have seen that the submatrix A of T is completely determined by our ingredients (i) and (ii), while B and C are only partly determined (B is determined up to repeating columns, and C up to repeating rows and multiplying them by positive integers). The remaining submatrix of T, namely D, usually requires some knowledge of our ingredient (iii).

We shall get rid of the problem of computing D by assuming that D is the zero matrix. As we shall see, this assumption will also eliminate the residual indeterminacy in the matrices B and C; in fact there will not be any repeated column in B, nor any repeated row in C, and the first orthogonality relation will determine which multiple of each row of $\tilde{T}$ (not corresponding to the trivial character of N) appears as a row of C. Thus our ingredients (i) and (ii), together with the assumption $D = 0$, will determine the character table of G uniquely (though they do not determine G up to isomorphism). We shall see in Section 4.2 how the condition $D = 0$ can be expressed by two equivalent statements: one of them concerns conjugacy classes of G and G/N, while the other one concerns irreducible characters of G and N.

We observe now that in order to describe the submatrices A, B, and C of T we did not use all of the information contained in our ingredients (i) and (ii). In fact, in our discussion we never used the group structure of H and N, but only their character tables, together with the orbits of H on the set of conjugacy classes and the set of irreducible characters of N. It turns out that our ingredients (i) and (ii) can be safely replaced with the following weaker ingredients:

(I) the character table of $H = G/N$,

(II) the character table of N, together with the knowledge of the G-orbits of $\mathrm{Irr}(N)$.

With Theorem 4.3.1 we shall give a formal proof that (I) and (II), together with the condition $D = 0$, determine the character table T of G uniquely. We only observe here that in (II) we do not require the knowledge of the orbits of G on the set of conjugacy classes of N. This is due to the following general fact, which we mention without proof: if the character table of a normal subgroup N of G is given, together with the orbits of the action of G on $\mathrm{Irr}(N)$ (whithout any further information about this action), then the orbits of G on the set of conjugacy classes of N can be uniquely determined; conversely, the character table of N and the orbits of G on the set of conjugacy classes of N determine the orbits of G on $\mathrm{Irr}(N)$.

We conclude this section by noting that ingredient (II) can be further weakened (though it is sufficient as it stands for our purposes), because, instead of the character table of N we rather used the table $\tilde{T}$, which displays the values of the sums over the G-orbits of $\mathrm{Irr}(N)$. We shall come back to this remark in Section 4.4.

4.2 Vanishing of character values

The matter of this section is the vanishing of the submatrix D of the character table T of G, as described above. The following two lemmas show how the vanishing of a column (respectively row) of D is equivalent to a conditon on the conjugacy class (respectively irreducible character) of G which corresponds to that column (respectively row). Since these results cannot be easily found in the literature in this form, we shall give their proofs in full.

Lemma 4.2.1 *Let N be a normal subgroup of the group G, let $g \in G$ and let $\pi : G \to G/N$ be the natural epimorphism. Then any two of the following conditions are equivalent:*

(a) $\chi(g) = 0$ *for all* $\chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$;

(b) $|\mathbf{C}_G(g)| = |\mathbf{C}_{G/N}(g^\pi)|$;

(c) $g^G = g^G \cdot N$;

(d) $gN \subseteq g^G$;

(e) $N \subseteq [g, G]$.

Proof $((a) \iff (b))$ By using the second orthogonality relation we get

$$|\mathbf{C}_{G/N}(g^\pi)| = \sum_{\chi \in \mathrm{Irr}(G/N)} |\chi(g)|^2 \leq \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 = |\mathbf{C}_G(g)|,$$

with equality if and only if $\chi(g) = 0$ for all $\chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$.

$((b) \iff (c))$ Since $(g^\pi)^{(x^\pi)} = (g^x)^\pi$ for all $g, x \in G$, we have

$$((g^\pi)^{(x^\pi)})^{\pi^{-1}} = g^x \cdot N \quad \text{and} \quad ((g^\pi)^{G/N})^{\pi^{-1}} = g^G \cdot N.$$

Therefore

$$g^G \subseteq g^G \cdot N = ((g^\pi)^{G/N})^{\pi^{-1}}.$$

It follows that $|g^G| \leq |N| \cdot |(g^\pi)^{G/N})|$, which is equivalent to

$$|\mathbf{C}_G(g)| \geq |\mathbf{C}_{G/N}(g^\pi)|.$$

We have equality here if and only if $g^G = g^G \cdot N$.

$((c) \iff (d) \iff (e))$ This is easy. □

If N is a normal subgroup of the group G and $\theta \in \mathrm{Irr}(N)$, let us write

$$\mathrm{Irr}(G,\theta) = \{\chi \in \mathrm{Irr}(G) | [\chi_N, \theta] > 0\},$$

where the brackets $[\ ,\ ]$ denote the scalar product of characters. Since $[\chi_N, \theta] = [\chi, \theta^G]$ by Frobenius Reciprocity, $\mathrm{Irr}(G,\theta)$ is the set of all irreducible constituents of θ^G.

Lemma 4.2.2 *Let $N \lhd G$, let $\theta \in \mathrm{Irr}(N)$ and $\chi \in \mathrm{Irr}(G,\theta)$. Let $e = [\chi_N, \theta]$ and let t be the number of distinct G-conjugates of θ. Then the following conditions are equivalent:*

(a) $\mathrm{Irr}(G,\theta) = \{\chi\}$;

(b) $\chi(g) = 0$ *for all* $g \in G \setminus N$;

(c) $e^2 t = |G : N|$.

Proof Let $\theta = \theta_1, \ldots, \theta_t$ be all the distinct G-conjugates of θ; then according to Clifford's Theorem we have

$$\chi_N = e \sum_{i=1}^{t} \theta_i, \quad \text{where } e = [\chi_N, \theta] = [\chi, \theta^G].$$

Thus χ is an irreducible constituent of θ^G with multiplicity e. It follows that $\mathrm{Irr}(G,\theta) = \{\chi\}$ if and only if $\theta^G = e\chi$, or equivalently $\theta^G(1) = e\chi(1)$. But

$$\theta^G(1) = |G : N|\theta(1) \quad \text{and} \quad \chi(1) = et\theta(1),$$

and so $\mathrm{Irr}(G,\theta) = \{\chi\}$ is equivalent to $|G : N| = e^2 t$. According to [13, Lemma (2.29)] we have

$$e^2 t = [\chi_N, \chi_N] \leq |G : N|[\chi, \chi] = |G : N|,$$

and equality holds if and only if $\chi(g) = 0$ for all $g \in G \setminus N$. This concludes the proof. $\square$

It follows from Lemma 4.2.1 that the obvious character-theoretic expression of the condition $D = 0$, namely

$$\chi(g) = 0 \text{ for all } g \in G \setminus N \text{ and for all } \chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N),$$

has a purely group-theoretic equivalent, namely

$$|\mathbf{C}_G(g)| = |\mathbf{C}_{G/N}(gN)| \quad \text{for all } g \in G \setminus N.$$

This condition on G, with respect to a normal subgroup N, has been given a name.

Definition 4.2.3 *Let N be a proper non-trivial normal subgroup of the group G. The pair (G, N) is called a* Camina pair *if the following condition holds:*

$$|\mathbf{C}_G(g)| = |\mathbf{C}_{G/N}(gN)| \quad \textit{for all } g \in G \setminus N.$$

Camina pairs have been introduced in [2] as a generalization of Frobenius groups; in fact it is easy to see that (G, N) is a Camina pair if G is a Frobenius group and N is its Frobenius kernel. Further examples of Camina pairs are given by (G, G'), where G is an extraspecial p-group. We refer to [2], [3] and [16] for series of results on Camina pairs.

We observe that, according to Lemma 4.2.1, Camina pairs are also characterized by the following property: the inverse image of each non-trivial conjugacy class $(gN)^{G/N}$ of the factor group G/N, under the natural epimorphism $\pi : G \to G/N$, is a conjugacy class of G, namely g^G. (Let us note that in general the inverse image under π of a conjugacy class of G/N is a union of conjugacy classes of G.)

Finally, let us mention a remarkable property of Camina pairs: if (G, N) is a Camina pair, then every chief series of G must pass through N; in other words, each normal subgroup of G, either contains N, or is contained in N.

4.3 A tool for comparing character tables

The following theorem provides a rigorous formulation of the result which we sketched in Section 4.1.

Theorem 4.3.1 *Let $N_1 \lhd G_1$, $N_2 \lhd G_2$, and suppose that the following conditions hold:*

(i) G_1/N_1 and G_2/N_2 have identical character tables;

(ii) *N_1 and N_2 have identical character tables, via the bijections*

$$\alpha : N_1 \to N_2$$

and

$$\beta : \mathrm{Irr}(N_1) \to \mathrm{Irr}(N_2),$$

and, moreover, β takes each G_1-orbit of $\mathrm{Irr}(N_1)$ *onto some G_2-orbit of* $\mathrm{Irr}(N_2)$*;*

(iii) *(G_1, N_1) and (G_2, N_2) are Camina pairs.*

Then G_1 and G_2 have identical character tables.

Proof By hypothesis (i), there exist bijections

$$\bar{\alpha} : G_1/N_1 \to G_2/N_2$$

and

$$\bar{\beta} : \mathrm{Irr}(G_1/N_1) \to \mathrm{Irr}(G_2/N_2),$$

such that

$$\chi^{\bar{\beta}}(x^{\bar{\alpha}}) = \chi(x) \;\text{ for all } x \in G_1/N_1 \;\text{ and for all } \chi \in \mathrm{Irr}(G_1/N_1).$$

Let $\pi_i : G_i \to G_i/N_i$, for $i = 1, 2$, be the natural epimorphisms. Let $\alpha : G_1 \setminus N_1 \to G_2 \setminus N_2$ be any bijection making the following diagram commute:

$$\begin{tikzcd} G_1 \setminus N_1 \arrow[r, "\alpha"] \arrow[d, "\pi_1"] & G_2 \setminus N_2 \arrow[d, "\pi_2"] \\ (G_1/N_1) \setminus \{1\} \arrow[r, "\bar{\alpha}"] & (G_2/N_2) \setminus \{1\} \end{tikzcd}$$

Let us extend α to a bijection $\alpha : G_1 \to G_2$ by

$$n^{\alpha} = n^{\alpha} \;\text{ for all } n \in N_1.$$

Then the extended α also satisfies $\alpha\pi_2 = \pi_1\bar{\alpha}$.

If $\chi \in \mathrm{Irr}(G_i) \setminus \mathrm{Irr}(G_i/N_i)$ (for $i = 1$ or 2), then hypothesis (iii) together with Lemma 4.2.1 guarantee that

$$\chi(g) = 0 \;\text{ for all } g \in G_i \setminus N_i.$$

Furthermore, if θ is an irreducible constituent of the restriction χ_{N_1}, then

$$\mathrm{Irr}(G_1, \theta) = \{\chi\},$$

according to Lemma 4.2.2.

Let us define a map:

$$\beta : \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1) \to \mathrm{Irr}(G_2) \setminus \mathrm{Irr}(G_2/N_2),$$

as follows. If $\chi \in \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1)$, let θ be an irreducible constituent of χ_{N_1}, so that $\mathrm{Irr}(G_1, \theta) = \{\chi\}$ and θ is not the trivial character of N_1. It follows that θ^β is not the trivial character of N_2, and hence $\mathrm{Irr}(G_2, \theta^\beta)$ is a subset of $\mathrm{Irr}(G_2) \setminus \mathrm{Irr}(G_2/N_2)$. Therefore $\mathrm{Irr}(G_2, \theta^{\bar\beta}) = \{\bar\chi\}$, for some $\bar\chi \in \mathrm{Irr}(G_2) \setminus \mathrm{Irr}(G_2/N_2)$ (namely $\bar\chi$ is the unique irreducible constituent of the induced character $(\theta^{\bar\beta})^{G_2}$). Then define $\chi^\beta = \bar\chi$.

This definition does not depend on the only choice we made, namely the choice of an irreducible constituent θ of χ_{N_1}, because β takes G_1-conjugate characters of N_1 to G_2-conjugate characters of N_2, according to hypothesis (ii).

By Clifford's Theorem and Lemma 4.2.2, the map which sends any $\chi \in \mathrm{Irr}(G_i) \setminus \mathrm{Irr}(G_i/N_i)$ (for $i = 1$ or 2) to the set of the irreducible constituents of χ_{N_i} is a bijection from $\mathrm{Irr}(G_i) \setminus \mathrm{Irr}(G_i/N_i)$ onto the set of G_i-orbits of $\mathrm{Irr}(N_i) \setminus \{1_{N_i}\}$. Since β is a bijection, it is clear that the map β is also a bijection.

Let us extend β to a bijection $\beta : \mathrm{Irr}(G_1) \to \mathrm{Irr}(G_2)$ by defining

$$\chi^\beta = \chi^{\bar\beta} \quad \text{for all } \chi \in \mathrm{Irr}(G_1/N_1).$$

It will follow that G_1 and G_2 have identical character tables, once we show that

$$\chi^\beta(g^\alpha) = \chi(g) \quad \text{for all } g \in G_1 \quad \text{and for all } \chi \in \mathrm{Irr}(G_1).$$

We will prove this by distinguishing three cases.

Case 1: $\chi \in \mathrm{Irr}(G_1/N_1), \quad g \in G_1$.

We have

$$\chi^\beta(g^\alpha) = \chi^{\bar\beta}(g^{\alpha\pi_2}) = \chi^\beta(g^{\pi_1\bar\alpha}) = \chi(g^{\pi_1}) = \chi(g).$$

Case 2: $\chi \in \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1)$, $g \in N_1$.

Let θ be an irreducible constituent of χ_{N_1} and let $\theta = \theta_1, \cdots, \theta_t$ be all the distinct G_1-conjugates of θ. Then

$$\chi_{N_1} = e \sum_{j=1}^{t} \theta_j,$$

and the positive integer e is determined by $e^2 t = |G_1 : N_1|$, according to Lemma 4.2.2. The G_2-conjugates of θ^{β} are $\theta^{\beta} = \theta_1^{\beta}, \cdots, \theta_t^{\beta}$, by hypothesis (ii); hence

$$(\chi^{\beta})_{N_2} = \hat{e} \sum_{j=1}^{t} \theta_j^{\beta},$$

and $\hat{e}^2 t = |G_2 : N_2|$, by Lemma 4.2.2 again. But the groups G_1/N_1 and G_2/N_2 have identical character table, in particular they have the same order. This forces e and $\hat{e}$ to be the same number, therefore

$$(\chi^{\beta})_{N_2} = e \sum_{j=1}^{t} \theta_j^{\beta}.$$

But then we have

$$\chi^{\beta}(g^{\alpha}) = e \sum_{j=1}^{t} \theta_j^{\beta}(g^{\hat{\alpha}}) = e \sum_{j=1}^{t} \theta_j(g) = \chi(g).$$

Case 3: $\chi \in \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1)$, $g \in G_1 \setminus N_1$.

Since χ and χ^{β} vanish on $G_1 \setminus N_1$ and $G_2 \setminus N_2$ respectively, we have

$$\chi^{\beta}(g^{\alpha}) = 0 = \chi(g).$$

This completes the proof. □

The previous theorem will actually be used in presence of much stronger hypotheses, namely those of the next corollary.

If N is an abelian normal subgroup of the group G, we can regard N as a $\mathbf{Z}G$-module, with G acting on N by conjugation. Since N is contained in the kernel of this action, N can also be regarded as a $\mathbf{Z}(G/N)$-module. If H is a group and $\gamma : H \to G/N$ is a group homomorphism, then N becomes an $\mathbf{Z}H$-module in the usual way.

Corollary 4.3.2 *Let N_i be an abelian normal subgroup of G_i, for $i = 1, 2$, and suppose that the following conditions hold:*

(i) *there exists a group isomorphism*

$$\hat{\alpha} : G_1/N_1 \longrightarrow G_2/N_2;$$

(ii) *there exists a $\mathbf{Z}(G_1/N_1)$-module isomorphism*

$$\alpha : N_1 \longrightarrow N_2,$$

where the $\mathbf{Z}(G_2/N_2)$-module N_2 is regarded as a $\mathbf{Z}(G_1/N_1)$-module via the isomorphism $\hat{\alpha}$;

(iii) *(G_1, N_1) and (G_2, N_2) are Camina pairs.*

Then G_1 and G_2 have identical character tables.

Proof Suppose that the hypotheses of the corollary hold. Then hypotheses (*i*) and (*iii*) of Theorem 4.3.1 are clearly satisfied. Let us define a map $\beta : \mathrm{Irr}(N_1) \longrightarrow \mathrm{Irr}(N_2)$ by means of the formula

$$\theta^{\beta}(n) = \theta(n^{\alpha^{-1}}) \text{ for all } n \in N_2 \text{ and for all } \theta \in \mathrm{Irr}(N_1).$$

Then N_1 and N_2 have identical character tables, via the bijections α and β.

Let $\theta \in \mathrm{Irr}(N_1)$ and $g \in G_1$; then, for all $n \in N_1$, we have

$$(\theta^g)^{\beta}(n) = \theta^g(n^{\hat{\alpha}^{-1}}) = \theta((n^{\hat{\alpha}^{-1}})^{g^{-1}}) = \theta((n^{g^{-1}})^{\hat{\alpha}^{-1}}) = \theta^{\beta}(n^{g^{-1}}) = (\theta^{\beta})^{g}(n).$$

Hence

$$(\theta^g)^{\beta} = (\theta^{\beta})^{g} \text{ for all } \theta \in \mathrm{Irr}(N_1) \text{ and for all } g \in G_1.$$

It follows that β takes each G_1-orbit of $\mathrm{Irr}(N_1)$ onto some G_2-orbit of $\mathrm{Irr}(N_2)$. Thus hypothesis (*ii*) of Theorem 4.3.1 is also satisfied, and the desired conclusion follows. □

Perhaps the simplest situation in which Corollary 4.3.2 applies is when G_1 and G_2 are extraspecial p-groups of the same order, and N_1, N_2 are their centres; in fact (G_i, N_i) is obviously a Camina pair in this case (for $i = 1, 2$). More generally, $(G, \mathbf{Z}(G))$ is easily seen to be a Camina pair if G is a semi-extraspecial p-group, according to the following definition, which was introduced in [1].

Definition 4.3.3 *A non-trivial p-group G is called semi-extraspecial if G/N is extraspecial for each maximal subgroup N of $\mathbf{Z}(G)$.*

A semi-extraspecial p-group G is obviously a special p-group, and

$$|G : \mathbf{Z}(G)| = p^{2n}$$

for some positive integer n. It turns out then that $|\mathbf{Z}(G)| \leq p^n$ (see [1]). For example, Suzuki 2-groups of type B, C, D (see [9] or [11, Chapter VIII, §7]) are semi-extraspecial and satisfy $|G : \mathbf{Z}(G)| = |\mathbf{Z}(G)|^2$. According to Corollary 4.3.2, the character table of a semi-extraspecial p-group G is completely determined by the two numbers $|G : \mathbf{Z}(G)|$ and $|\mathbf{Z}(G)|$. Consequently, semi-extraspecial p-groups provide plenty of examples of non-isomorphic groups which have the same character table.

4.4 A generalization

In this section we shall generalize Theorem 4.3.1 in two different directions.

Our first generalization concernes a weakening of the condition that the pairs of groups (G_1, N_1) and (G_2, N_2) are Camina pairs, that is to say, hypothesis (*iii*) of Theorem 4.3.1. The condition that a group G forms a Camina pair, together with some normal subgroup N, is indeed quite a strong requirement on G, as it appears for instance from the results of [3] and [16]. The more general condition which we propose is better illustrated by using the language of Section 4.1.

Let us consider two proper non-trivial normal subgroups N and M of a group G, with $N \leq M$. The character table T of G assumes the following form, after possibly rearranging the conjugacy classes and the irreducible characters of G:

$$\begin{array}{r|c|c|c|}
 & N & M \setminus N & G \setminus M \\
\mathrm{Irr}(G/M) & A_{11} & A_{12} & A_{13} \\
\mathrm{Irr}(G/N) \setminus \mathrm{Irr}(G/M) & A_{21} & A_{22} & A_{23} \\
\mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N) & A_{31} & A_{32} & A_{33}
\end{array}$$

We shall assume that A_{33} is the zero matrix (this clearly specializes to (G, N) being a Camina pair, when $N = M$). An (informal) argument similar to that used in Section 4.1 suggests that it should be possible to obtain T

starting from the character table of the factor group G/N, and the character table of the normal subgroup M, together with the knowledge of the orbits of G on the set of conjugacy classes of M. It also appear that there must be some kind of compatibility between the character tables of G/N and M, where these two pieces of information overlap, namely on the normal section M/N of G. These heuristic considerations lead to the following theorem, which generalizes Theorem 4.3.1.

Theorem 4.4.1 *Let $N_i \lhd G_i$ and $M_i \lhd G_i$ for $i = 1, 2$, with $N_i \leq M_i$, and suppose that the following conditions hold:*

(i) G_1/N_1 and G_2/N_2 have identical character tables, via the bijections

$$\alpha : G_1/N_1 \to G_2/N_2$$

and

$$\beta : \mathrm{Irr}(G_1/N_1) \to \mathrm{Irr}(G_2/N_2);$$

(ii) M_1 and M_2 have identical character tables, via the bijections

$$\tilde{\alpha} : M_1 \to M_2$$

and

$$\tilde{\beta} : \mathrm{Irr}(M_1) \to \mathrm{Irr}(M_2),$$

and, moreover, $\tilde{\beta}$ takes each G_1-orbit of $\mathrm{Irr}(M_1)$ onto a G_2-orbit of $\mathrm{Irr}(M_2)$;

(iii) $g^{G_i} = g^{G_i} \cdot N_i$ for all $g \in G_i \setminus M_i$, for $i = 1, 2$;

(iv) $(M_1/N_1)^{\alpha} = M_2/N_2$, and the diagram

$$\begin{tikzcd} M_1 \arrow[r, "\tilde{\alpha}"] \arrow[d, "\pi_1"] & M_2 \arrow[d, "\pi_2"] \\ M_1/N_1 \arrow[r, "\alpha"] & M_2/N_2 \end{tikzcd}$$

is commutative, where $\pi_i : M_i \to M_i/N_i$ are the natural epimorphisms (for $i = 1, 2$).

Then G_1 and G_2 have identical character tables.

Proof A full proof can be given along the lines of the proof of Theorem 4.3.1, but we shall not give it here. Let us only notice that we need hypothesis (iv) here, in order to be able to extend the bijection $\bar{\alpha}$ to a bijection $\alpha : G_1 \to G_2$ which satisfies $\alpha\pi_2 = \pi_1\alpha$. □

Now we propose a second generalization of Theorem 4.3.1, which weakens hypothesis (ii). Informally, as we anticipated at the end of Section 4.1, hypothesis (ii) of Theorem 4.3.1 can be replaced by the weaker requirement that the matrices T_1 and T_2 are equal, where the matrix T_i is obtained from the character table of N_i as we did in Section 4.1, and thus T_i displays the values of the sums of irreducible characters of N_i over G_i-orbits, as functions of the conjugacy classes of G_i contained in N_i. This weaker condition will be made precise in the following theorem.

Theorem 4.4.2 *Let $N_1 \lhd G_1$ and $N_2 \lhd G_2$. For $i = 1, 2$, let $\mathcal{I}_i$ denote the set of the (possibly reducible) characters ψ of N_i such that*

$$\psi = \sum_{j=1}^{t} \theta_j$$

for some G_i-orbit $\theta_1, \dots, \theta_t$ of $\mathrm{Irr}(N_i)$ (where $\theta_1, \dots, \theta_t$ are pairwise distinct). Suppose that the following conditions hold:

(i) *G_1/N_1 and G_2/N_2 have identical character tables;*

(ii) *there exist bijections*

$$\bar{\alpha} : N_1 \to N_2$$

and

$$\beta' : \mathcal{I}_1 \to \mathcal{I}_2$$

such that

$$\psi^{\beta'}(n^{\bar{\alpha}}) = \psi(n) \text{ for all } n \in N_1 \text{ and for all } \psi \in \mathcal{I}_1;$$

(iii) *(G_1, N_1) and (G_2, N_2) are Camina pairs.*

Then G_1 and G_2 have identical character tables.

Proof This theorem can be proved essentially in the same way as Theorem 4.3.1. The main difference is when one defines χ^{β} for $\chi \in \mathrm{Irr}(G_1)\setminus\mathrm{Irr}(G_1/N_1)$. We shall briefly sketch this part of the proof.

Let $\chi \in \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1)$. Let us choose an irreducible constituent θ of χ_{N_1}; then we have $\mathrm{Irr}(G_1, \theta) = \{\chi\}$. Now, if we put $e = [\chi_{N_1}, \theta]$, then we have $\chi_{N_1} = e\psi$ for a unique $\psi \in \mathcal{I}_1$, namely the sum of all G_1-conjugates of θ. Let $\tilde{\theta}$ be an irreducible constituent of $\psi^{\tilde{\beta}'}$; then we have $\mathrm{Irr}(G_2, \tilde{\theta}) = \{\tilde{\chi}\}$ for some $\tilde{\chi} \in \mathrm{Irr}(G_2) \setminus \mathrm{Irr}(G_2/N_2)$. Finally, let us define $\chi^{\beta} = \tilde{\chi}$.

Another remark that should be made is that the number t of G_1-conjugates of θ equals the number $\tilde{t}$ of G_2-conjugates of $\tilde{\theta}$; in fact, we have

$$t = [\psi, \psi] = \frac{1}{|G_1|} \sum_{g \in G_1} |\psi(g)|^2 = \frac{1}{|G_2|} \sum_{g \in G_2} |\psi^{\tilde{\beta}'}(g^{\tilde{\alpha}})|^2 = [\psi^{\tilde{\beta}'}, \psi^{\tilde{\beta}'}] = \tilde{t}.$$

For the rest of the proof, the reader is referred to the proof of Theorem 4.3.1. □

Clearly, hypothesis (*ii*) of Theorem 4.3.1 implies hypothesis (*ii*) of Theorem 4.4.2. However, we do not know of any example of groups G_1 and G_2, with normal subgroups N_1 and respectively N_2, which satisfy the hypotheses of Theorem 4.4.2 without satisfying the hypotheses of Theorem 4.3.1.

Chapter 5

Counterexamples

5.1 Introduction

In this chapter we shall construct pairs of groups (G, H) with identical character tables and derived length 2 and 3 respectively, which thus will be counterexamples to our Conjecture 3.1.1. Since our philosophy is that of trying to build our examples as small as possible we shall assume that G and H satisfy Hypotheses 3.1.2. With these hypotheses, a fairly detailed description of the structure of G and H is given in Chapter 3, in particular by Lemmas 3.2.1, 3.3.1 and 3.3.4. Thus, using for a moment a common notation for G and H, each of the groups G and H is a semidirect product of the form

$$[D](W \times Q),$$

where

- D (which stands for 'derived subgroup') is a p-group containing the unique minimal normal subgroup N of G (respectively H),
- D/N is abelian,
- W is an abelian p-group,
- Q is a non-trivial cyclic p'-group,
- Q acts faithfully and irreducibly on N by conjugation,
- W acts faithfully on D by conjugation,

- all Q-composition factors of D are Q-isomorphic.

Furthermore, if we fix a chief series of H going from 1 to $D = H'$, according to our analysis carried out in Section 3.4, commutation in H' gives rise to an $\mathbf{F}Q$-module epimorphism

$$\bar{\bar{\gamma}} : V \wedge V \to V$$

in the unary case (that is to say, when $r = s$, where r and s are as defined in Section 3.4), or

$$\gamma : V \otimes V \to V$$

in the binary case (when $r < s$), where V denotes the elementary abelian p-group H'' regarded as a faithful irreducible $\mathbf{F}_p Q$-module by conjugation.

We shall not attempt to describe all pairs of groups (G, H) which satisfy Hypotheses 3.1.2. However, at least for $p \neq 2$, we shall construct examples (G, H) which satisfy Hypotheses 3.1.2, and which give rise to any prescribed $\mathbf{F}_p Q$-epimorphism $\bar{\bar{\gamma}} : V \wedge V \to V$ or $\gamma : V \otimes V \to V$. In our examples, the subgroup D will have the smallest possible Q-length, namely 2 in the unary case, and 3 in the binary case. In all cases the factor group D/N will be elementary abelian.

Now a word should be spent on W. We shall assume that $[D, W] \leq N$. In particular $(DW)' \leq N$ (we shall have equality for H), and since $N \leq \mathbf{Z}(DW)$ because N is a minimal normal subgroup of G (respectively H), the subgroup DW will be nilpotent of class at most 2 (actually, exactly 2). According to Lemma 2.2.2 (with $H_1/K_1 = D/N$, $H_2/K_2 = W$ and $H_3/K_3 = N$), the map

$$\begin{aligned} \varphi_w : D/N &\to N \\ x &\mapsto [x, w] \end{aligned}$$

is a Q-homomorphism for all $w \in W$, and the map

$$\begin{aligned} \hat{\gamma} : W &\to \mathrm{Hom}_Q(D/N, N) \\ w &\mapsto \varphi_w \end{aligned}$$

is a group homomorphism. Actually $\hat{\gamma}$ is a monomorphism, because W acts faithfully on D. We shall employ Corollary 4.3.2 to prove that the groups G and H of our examples have identical character tables. In order to satisfy hypothesis (iii) of that corollary we shall require that the map $\hat{\gamma}$ above is surjective, and hence that it is a group isomorphism.

5.2 General construction

In the present section we shall develop the part of the construction which is common to the groups G and H of all the examples which we are going to build in this chapter and we shall prove that the resulting groups G and H have identical character tables.

Let us fix a prime p and make the following assumptions (for $i = 1, 2$):

(1) D_i is a p-group with an elementary abelian subgroup N_i such that $\Phi(D_i) \le N_i \le \mathbf{Z}(D_i)$;

(2) Q_i is a non-trivial cyclic p'-group of automorphisms of D_i which normalizes N_i and acts faithfully and irreducibly on N_i; hence N_i becomes a faithful irreducible module for Q_i over $\mathbb{F}_p$;

(3) all Q_i-composition factors of D_i are Q_i-isomorphic;

(4) there is a group isomorphism $\sigma : Q_1 \to Q_2$;

(5) N_2 regarded as an $\mathbb{F}_pQ_1$-module via σ is isomorphic to the $\mathbb{F}_pQ_1$-module N_1;

(6) D_1 and D_2 have the same order (in particular the Q_1-length of D_1 equals the Q_2-length of D_2).

Starting from these ingredients, we shall define a certain group W_i of automorphisms of D_i. Let us regard the elementary abelian p-group D_i/N_i as an $\mathbb{F}_pQ_i$-module by conjugation. According to Maschke's Theorem, the module D_i/N_i is semisimple, because p does not divide $|Q_i|$. If V denotes N_i regarded as an $\mathbb{F}_pQ_i$-module, then by assumption V is irreducible and all composition factors of D_i/N_i as an $\mathbb{F}_pQ_i$-module are isomorphic to V. Hence D_i/N_i is isomorphic to $\bigoplus_{j=1}^{l} V_j$, where $V_1, \ldots, V_l$ are copies of V, and the number l is the same for $i = 1, 2$, because the Q_1-length of D_1/N_1 equals the Q_2-length of D_2/N_2.

Now we have the $\mathbb{F}_pQ_i$-module isomorphism

$$\mathrm{Hom}_{\mathbb{F}_pQ_i}\left(\bigoplus_{j=1}^{l} V_j, V\right) \cong \bigoplus_{j=1}^{l} \mathrm{Hom}_{\mathbb{F}_pQ_i}(V_j, V)$$

(which holds more generally if $V_1, \dots, V_l$, and V are arbitrary $\mathbf{F}_pQ_i$-modules). According to Theorem 2.3.1, the ring $\mathrm{End}_{\mathbf{F}_pQ_i}(V)$ is a field of p^n elements, where $|V| = p^n$. Since $V_j \cong V$, we have

$$|\,\mathrm{Hom}_{\mathbf{F}_pQ_i}(V_j, V)| = |V| \quad \text{for all } j = 1, \dots, l.$$

It follows that

$$|\,\mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i)| = |D_i : N_i|.$$

Later on we shall also need the following fact, which is easy to prove: for any element xN_i of D_i/N_i with $x \notin N_i$ there exists some

$$\varphi \in \mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i)$$

such that $(xN_i)^\varphi \neq 1$.

Now we shall associate to each $\varphi \in \mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i)$ an automorphism w_φ of D_i. Let $\varphi : D_i/N_i \to N_i$ be an $\mathbf{F}_pQ_i$-homomorphism. Since N_i is a central subgroup of D_i, the map

$$\begin{array}{rcl} w_\varphi : D_i & \to & D_i \\ x & \mapsto & x(xN_i)^\varphi \end{array}$$

is a group automorphism of D_i and it clearly commutes with the action of Q_i. Let W_i be the set of all automorphisms of D_i which arise in this way, in other words

$$W_i = \{w_\varphi \mid \varphi \in \mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i)\}.$$

Then W_i is a subgroup of $\mathrm{Aut}_{\mathbf{F}_pQ_i}(D_i)$. In fact, the map

$$\begin{array}{rcl} \delta : \mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i) & \to & \mathrm{Aut}_{Q_i}(D_i) \\ \varphi & \mapsto & w_\varphi \end{array}$$

is a group homomorphism, because

$$x^{w_{\varphi_1+\varphi_2}} = x(xN_i)^{\varphi_1+\varphi_2} = x(xN_i)^{\varphi_1}(xN_i)^{\varphi_2} = (x^{w_{\varphi_1}})^{w_{\varphi_2}}$$

for all $x \in D_i$, and W_i is its image. Clearly δ is a monomorphism, namely w_φ is the identity automorphism of D_i exactly when φ is the zero homomorphism. It follows in particular that the order of W_i equals the order of $\mathrm{Hom}_{\mathbf{F}_pQ_i}(D_i/N_i, N_i)$, which we computed earlier; hence

$$|W_i| = |D_i : N_i|.$$

We observe that the group W_i is an elementary abelian p-group, because $\mathrm{Hom}_{\mathbb{F}_pQ_i}(D_i/N_i, N_i)$ is a vector space over $\mathbb{F}_p$. Let us also notice that if φ_w, for $w \in W_i$, denotes the $\mathbb{F}_pQ$-module homomorphism

$$\begin{aligned}\varphi_w : D_i/N_i &\rightarrow N_i\\ xN_i &\mapsto [x,w],\end{aligned}$$

then the group homomorphism

$$\begin{aligned}\gamma : W_i &\rightarrow \mathrm{Hom}_{\mathbb{F}_pQ_i}(D_i/N_i, N_i)\\ w &\mapsto \varphi_w,\end{aligned}$$

is an isomorphism, in accordance with the requirement which we made at the end of Section 5.1, and is the inverse of the isomorphism

$$\delta : \mathrm{Hom}_{\mathbb{F}_pQ_i}(D_i/N_i, N_i) \rightarrow W_i$$

defined above.

The subgroups W_i and Q_i of $\mathrm{Aut}(D_i)$ satisfy $W_i \cap Q_i = [W_i, Q_i] = 1$, hence W_iQ_i is a subgroup of $\mathrm{Aut}(D_i)$, and is the internal direct product of W_i and Q_i. Hence W_iQ_i is canonically isomorphic to the external direct product $W_i \times Q_i$, which thus acts on D_i. Let us define groups G_1 and G_2 as the semidirect products

$$G_i = [D_i](W_i \times Q_i).$$

We observe that N_i is a minimal normal subgroup of G_i, because Q_i acts irreducibly on N_i. It would not be difficult to prove that N_i is the unique minimal normal subgroup of G_i. However, according to the last observation of Section 4.2, this will also follow from the fact that (G_i, N_i) is a Camina pair, which is proved in the following lemma.

Lemma 5.2.1 *Let G_1 and G_2 as above. Then*

(i) $G_1' = D_1$ *and* $G_2' = D_2$*;*

(ii) G_1 *and* G_2 *have identical character tables;*

(iii) (G_1, N_1) *and* (G_2, N_2) *are Camina pairs.*

Proof (i) Since $[D_i, Q_i] \leq D_i$ and $[D_i, Q_i] \lhd \langle D_i, Q_i \rangle = D_iQ_i$, the group $[D_i, Q_i]$ is a normal subgroup of D_i and is also normalized by Q_i (in other words, $[D_i, Q_i]$ is a normal Q_i-subgroup of D_i). Furthermore, Q_i centralizes the factor group $D_i/[D_i, Q_i]$. Since by hypothesis all Q_i-composition factors of D_i are Q_i-isomorphic and Q_i does not centralize N_i, we have $[D_i, Q_i] = D_i$. In particular, it follows that $G_i' = D_i$, because G_i/D_i is clearly abelian.

(ii) We shall apply Corollary 4.3.2 to the groups G_i and the normal subgroups N_i. Let us check then that the hypotheses of Corollary 4.3.2 are satisfied.

First of all, let us show that $G_1/N_1 \cong G_2/N_2$. We assumed that D_i is a Q_i-group all whose Q_i-composition factors are Q_i-isomorphic, for $i = 1, 2$. Let us regard the Q_2-group D_2 as a Q_1-group via the isomorphism $\sigma : Q_1 \rightarrow Q_2$. It follows that all Q_1-composition factors of D_2 are Q_1-isomorphic. Since we also assumed that N_2, viewed as an $\mathbb{F}_pQ_1$-module, is isomorphic to N_1, we get that each Q_1-composition factor of D_1 is Q_1-isomorphic to each Q_1-composition factor of D_2. Now the Q_1-factor groups D_1/N_1 and D_2/N_2 are elementary abelian p-groups; hence they can be regarded as $\mathbb{F}_pQ_1$-modules, and they are semisimple according to Maschke's theorem, because p does not divide $|Q_1|$. Also, they have the same Q_1-length, let us say l. Hence, if V denotes N_1 regarded as an $\mathbb{F}_pQ_1$-module, then each of D_1/N_1 and D_2/N_2 is isomorphic as an $\mathbb{F}_pQ_1$-module to the direct sum of l copies of V, in particular D_1/N_1 and D_2/N_2 are isomorphic as $\mathbb{F}_pQ_1$-modules. Let us fix an $\mathbb{F}_pQ_1$-isomorphism $\tau : D_1/N_1 \rightarrow D_2/N_2$. In other words, let τ be a group isomorphism which satisfies

$$((xN_1)^{\xi})^{\tau} = ((xN_1)^{\tau})^{\xi^{\sigma}} \quad \text{for all } x \in D_1 \quad \text{and for all } \xi \in Q_1.$$

Now, the groups W_1 and W_2 are elementary abelian p-groups of the same order; in fact,

$$|W_1| = |D_1/N_1| = |D_2/N_2| = |W_2|.$$

Let us fix a group isomorphism

$$\rho : W_1 \rightarrow W_2.$$

Since W_i centralizes Q_i and D_i/N_i by construction, we have

$$G_i/N_i = (D_iW_iQ_i)/N_i \cong (D_iQ_i/N_i) \times W_i.$$

Let

$$\bar{\alpha} : G_1/N_1 \to G_2/N_2$$

be the map such that $(xw\xi N_1)^{\bar{\alpha}} = (xN_1)^{\tau} w^{\rho} \xi^{\sigma}$ for all $x \in D_1$, for all $w \in W_1$ and for all $\xi \in Q_1$. It is clear that $\bar{\alpha}$ is a bijection; moreover, $\bar{\alpha}$ is a group isomorphism. In fact, we have

$$\begin{aligned}
((xw\xi N_1)(\bar{x}\bar{w}\bar{\xi} N_1))^{\bar{\alpha}} &= ((x\bar{x}^{\xi^{-1}})(w\bar{w})(\xi\bar{\xi})N_1)^{\bar{\alpha}} \\
&= (x\bar{x}^{\xi^{-1}} N_1)^{\tau}(w\bar{w})^{\rho}(\xi\bar{\xi})^{\sigma} \\
&= (xN_1)^{\tau}((\bar{x}N_1)^{\tau})^{(\xi^{\sigma})^{-1}} w^{\rho}\bar{w}^{\rho}\xi^{\sigma}\bar{\xi}^{\sigma} \\
&= ((xN_1)^{\tau} w^{\rho}\xi^{\sigma})((\bar{x}N_1)^{\tau}\bar{w}^{\rho}\bar{\xi}^{\sigma}) \\
&= (xw\xi N_1)^{\bar{\alpha}}(\bar{x}\bar{w}\bar{\xi} N_1)^{\bar{\alpha}}.
\end{aligned}$$

Thus hypothesis (i) of Corollary 4.3.2 has been verified.

Let us regard N_i as an $\mathbf{F}_p Q_i$-module by conjugation. We can also regard N_2 as an $\mathbf{F}_p Q_1$-module via the isomorphism $\sigma : Q_1 \to Q_2$. We assumed that N_1 and N_2 are isomorphic as $\mathbf{F}_p Q_1$-modules. Let

$$\tilde{\alpha} : N_1 \to N_2$$

be an $\mathbf{F}_p Q_1$-module isomorphism. Now N_1 can be regarded as an $\mathbf{F}_p(G_1/N_1)$-module by conjugation, while N_2 can be regarded as an $\mathbf{F}_p(G_2/N_2)$-module by conjugation and also as an $\mathbf{F}_p(G_1/N_1)$-module via the isomorphism $\bar{\alpha} : G_1/N_1 \to G_2/N_2$ which we defined earlier. Because $N_i \leq \mathbf{Z}(D_i W_i)$, the $\mathbf{F}_p(G_1/N_1)$-modules N_1 and N_2 can also be viewed as $\mathbf{F}_p(G_1/D_1 W_1)$-modules. Since the isomorphism $\bar{\alpha}$ extends the isomorphism $\sigma : Q_1 \to Q_2$, and Q_i (for $i = 1, 2$) is a complement for $D_i W_i$ in G_i, it is clear that the $\mathbf{F}_p Q_1$-module isomorphism $\tilde{\alpha} : N_1 \to N_2$ is actually an $\mathbf{F}_p(G_1/D_1 W_1)$-module isomorphism and thus an $\mathbf{F}_p(G_1/N_1)$-module isomorphism. This is exactly what is required by hypothesis (ii) of Corollary 4.3.2.

It remains to chech that hypothesis (iii) of Corollary 4.3.2 is satisfied, namely that (G_1, N_1) and (G_2, N_2) are Camina pairs, or in other words, that

$$g_i^{G} = g_i^{G} \cdot N_i \quad \text{for all } g \in G_i \setminus N_i, \text{ for } i = 1, 2.$$

According to Lemma 4.2.1, this is equivalent to

$$N_i \subseteq [g, G_i] \quad \text{for all } g \in G_i \setminus N_i.$$

We will distinguish three cases.

Case 1: $g \in N_i W_i \setminus N_i$.

Let us write $g = x w_\varphi$, with $x \in N_i$ and $w_\varphi \in W$. Since $w_\varphi \neq 1$, the $\mathbb{F}_p Q_i$-module homomorphism $\varphi : D_i/N_i \to N_i$ is not the zero homomorphism; therefore φ is surjective, because N_i is an irreducible $\mathbb{F}_p Q_i$-module. Thus we have

$$[D_i, g] = [D_i, w_\varphi] = (D_i/N_i)^\varphi = N_i.$$

In particular $N_i = [g, D_i] \subseteq [g, G_i]$.

Case 2: $g \in D_i W_i \setminus N_i W_i$.

Let us write $g = xw$, with $x \in D_i \setminus N_i$ and $w \in W_i$. Then

$$[g, W_i] = [x, W_i] = \{(xN_i)^\varphi \mid \varphi \in \mathrm{Hom}_{\mathbb{F}_p Q_i}(D_i/N_i, N_i)\}$$

is clearly a subgroup of N_i normalized by Q_i, in other words an $\mathbb{F}_p Q_i$-submodule of the irreducible $\mathbb{F}_p Q_i$-module N_i. As we remarked earlier, since $xN_i \neq N_i$, there exists some $\varphi \in \mathrm{Hom}_{\mathbb{F}_p Q_i}(D_i/N_i, N_i)$ such that $(xN_i)^\varphi \neq 1$. Hence $[g, W_i]$ is not the trivial $\mathbb{F}_p Q_i$-submodule of N_i and thus we have $[g, W_i] = N_i$. In particular $N_i \subseteq [g, G_i]$.

Case 3: $g \in G_i \setminus D_i W_i$.

Let us write $g = xw\xi$, with $x \in D_i$, $w \in W_i$ and $\xi \in Q_i$ with $\xi \neq 1$. Then $[N_i, g] = [N_i, \xi]$ is an $\mathbb{F}_p Q_i$-submodule of N_i; in fact, it is the image of the $\mathbb{F}_p Q_i$-module homomorphism

$$\begin{array}{ccc} N_i & \to & N_i \\ x & \mapsto & [x, \xi]. \end{array}$$

Since Q_i acts faithfully on N_i and $\xi \neq 1$, we have $[N_i, g] \neq 1$ and thus $[N_i, g] = N_i$. In particular, $N_i = [g, N_i] \subseteq [g, G_i]$.

Hence we have proved that

$$g_i^G = g_i^G \cdot N_i \quad \text{for all } g \in G_i \setminus N_i,$$

and thus hypothesis (*iii*) of Corollary 4.3.2 has also been verified. Its conclusion that G_1 and G_2 have identical character tables now follows.

(iii) The fact that (G_1, N_1) and (G_2, N_2) are Camina pairs has been proved above. $\square$

5.3 The unary case

This section and Section 5.5 are devoted to the construction of pairs (G, H) of groups, according to the pattern described in the previous section (with $G_1 = G$ and $G_2 = H$). The derived subgroups D_1 (abelian) and D_2 (metabelian) will have Q_1-length and respectively Q_2-length 2 in this section and 3 in Section 5.5.

As we said earlier, any $\mathbf{F}_p Q$-module epimorphism

$$\bar{\bar{\gamma}} : V \wedge V \to V$$

or

$$\gamma : V \otimes V \to V,$$

where V is a faithful irreducible $\mathbf{F}_p Q$-module, can arise from concrete examples (G, H) satisfying Hypotheses 3.1.2, by means of the procedure described in Section 3.4. However, for the sake of simplicity we shall prove this fact only for $p \neq 2$ and limit ourselves to giving some representative examples for $p = 2$ (in Sections 5.4 and 5.6).

Hence let us assume that p is an odd prime, and let us make the following assumptions:

- Q is a (non-trivial) cyclic group of p'-order;
- V is a faithful irreducible $\mathbf{F}_p Q$-module;
- $\gamma : V \wedge V \to V$ is a fixed $\mathbf{F}_p Q$-module epimorphism.

We observe that the dimension n of V over $\mathbf{F}_p$ is uniquely determined by p and $|Q|$ according to Lemma 2.3.1.

Let $A = V \oplus V$ be the direct sum of two copies of V. The $\mathbf{F}_p Q$-factor module $A/(0 \oplus V)$ and the $\mathbf{F}_p Q$-submodule $0 \oplus V$ are both isomorphic to V, in particular

$$\mathrm{Hom}_{\mathbf{F}_p Q}(A/(0 \oplus V), 0 \oplus V) \cong \mathbf{F}_{p^n},$$

as vector spaces over $\mathbf{F}_p$, where n is the dimension of V over $\mathbf{F}_p$. For any

$$\varphi \in \mathrm{Hom}_{\mathbf{F}_p Q}(A/(0 \oplus V), 0 \oplus V),$$

the map w_φ defined by

$$a^{w_\varphi} = a + (a + (0 \oplus V))^\varphi \quad \text{for all } a \in A,$$

is an automorphism of A as an $\mathbf{F}_pQ$-module. Then

$$W = \{w_\varphi \mid \varphi \in \mathrm{Hom}_{\mathbf{F}_pQ}(A/(0 \oplus V), 0 \oplus V)\}$$

is a subgroup of $\mathrm{Aut}_{\mathbf{F}_pQ}(A)$. The order of W equals the order of V, namely p^n. In fact, if we put $D_1 = A$, $N_1 = 0 \oplus V$, $Q_1 = Q$ and use a multiplicative notation for D_1, then D_1 satisfies conditions $(1), \ldots, (6)$ of Section 5.2; hence W is exactly the subgroup W_1 of $\mathrm{Aut}_{Q_1}(D_1)$ which is defined there and has order $|D_1 : N_1| = p^n$. Let us define

$$G_1 = [D_1](W_1 \times Q_1)$$

as in Section 5.2. The group G_1 will also be called G here and we shall therefore write

$$G = [A](W \times Q).$$

According to Lemma 5.2.1, we have $G' = A$ and thus $G'' = 1$, that is to say, G is metabelian.

Let us pass to the construction of the group H. Let $\dot{F}$ be a free group of rank n. Then

$$F = \dot{F}/\gamma_3(\dot{F})\dot{F}^p$$

is a free nilpotent group of class two and exponent p (that is to say, F is a free object in the variety of nilpotent groups of class 2 and exponent p, see [18]). If p were the prime 2, then the group F would be abelian, but since we assumed $p \neq 2$, we have $F' \neq 1$. More precisely, F' is elementary abelian of order $p^{n(n-1)/2}$. In fact, according to Lemma 2.6.3, if

$$F = \langle x_1, \ldots, x_n \rangle,$$

then a basis of F' over $\mathbf{F}_p$ is given by the set of basic commutators of weight 2 on $x_1, \ldots x_n$, namely

$$\{[x_j, x_k] \mid 1 \leq k < j \leq n\}.$$

The factor group F/F' is a free abelian group of exponent p and rank n, in other words it is elementary abelian of order p^n. Let us fix an $\mathbf{F}_p$-linear isomorphism

$$\tau : V \to F/F'$$

and let us make F/F' into an $\mathbb{F}_pQ$-module isomorphic to V via τ, namely let us define an action of Q on F/F' according to the formula

$$(xF')^{\xi} = ((xF')^{\tau^{-1}}\xi)^{\tau} \quad \text{for all } x \in F \quad \text{and for all } \xi \in Q,$$

and extend it $\mathbb{F}_p$-linearly to an action of $\mathbb{F}_pQ$ on F/F'. Thus F/F' becomes an $\mathbb{F}_pQ$-module and τ an $\mathbb{F}_pQ$-module isomorphism.

Let us fix a generator ξ of Q. The automorphism of F/F' induced by ξ can be lifted to an automorphism $\bar{\xi}$ of F, because F is a relatively free group (see [18]). Since F is a finite group, the automorphism $\bar{\xi}$ has finite order; this is certainly a multiple of $|Q|$, which is the order of ξ. We may assume that the order of $\bar{\xi}$ is not a multiple of p, otherwise we can replace $\bar{\xi}$ with a suitable power $\bar{\xi}^{p^t}$ (t integer), which induces on F/F' the same automorphism as ξ does. Now $\bar{\xi}^{|Q|}$ is an automorphism of p'-order of the p-group F, which induces the identity automorphism on $F/\Phi(F) = F/F'$. According to [10, Kapitel III, Satz 3.18] then $\bar{\xi}^{|Q|}$ is the identity automorphism of F, and thus $\bar{\xi}$ has order $|Q|$. Therefore F can be regarded as a Q-group. In particular F' can be viewed as a (semisimple) $\mathbb{F}_pQ$-module.

According to Lemma 2.2.1 (with $H_1/K_1 = H_2/K_2 = F/F'$ and $H_3/K_3 = F'$), commutation in F gives rise to an $\mathbb{F}_p$-bilinear map

$$\begin{aligned} \delta : (F/F') \times (F/F') &\to F' \\ (xF', yF') &\mapsto [x, y]. \end{aligned}$$

Since δ is skew-symmetric and F' is a Q-subgroup of the Q-group F, we obtain in turn an $\mathbb{F}_pQ$-module homomorphism

$$\begin{aligned} \delta : (F/F') \wedge (F/F') &\to F' \\ (xF') \wedge (yF') &\mapsto [x, y]. \end{aligned}$$

Because we assumed that p is odd, δ is an isomorphism. In fact, the set

$$\{(x_jF') \wedge (x_kF') \mid 1 \leq k < j \leq n\}$$

is a basis of $(F/F') \wedge (F/F')$ over $\mathbb{F}_p$, and δ sends it bijectively onto the set of basic commutators of weight 2 on $x_1, \dots, x_n$, which is an $\mathbb{F}_p$-basis of F', as we saw earlier. The $\mathbb{F}_pQ$-module isomorphism

$$\tau : V \to F/F'$$

induces an $\mathbf{F}_pQ$-module isomorphism

$$\tau \wedge \tau : V \wedge V \to (F/F') \wedge (F/F')$$

in an obvious way. We get the following commutative diagram of $\mathbf{F}_pQ$-module homomorphisms:

$$\begin{tikzcd}
(F/F') \wedge (F/F') \arrow[r, "\bar{\delta}"] & F' \arrow[d, "\bar{\bar{\delta}}^{-1}(\tau\wedge\tau)^{-1}\bar{\bar{\gamma}}"] \\
V \wedge V \arrow[u, "\tau\wedge\tau"] \arrow[r, "\bar{\gamma}"] & V
\end{tikzcd}$$

Now let us put

$$K = \ker\,(\bar{\bar{\delta}}^{-1}(\tau \wedge \tau)^{-1}\bar{\bar{\gamma}}) = (\ker\ \bar{\bar{\gamma}})^{(\tau\wedge\tau)\bar{\delta}}.$$

The factor group F'/K is then an $\mathbf{F}_pQ$-module, and the $\mathbf{F}_pQ$-module epimorphism

$$\bar{\bar{\delta}}^{-1}(\tau \wedge \tau)^{-1}\gamma : F' \to V$$

induces an $\mathbf{F}_pQ$-module isomorphism

$$\nu : F'/K \to V$$

such that $\bar{\bar{\delta}}^{-1}(\tau \wedge \tau)^{-1}\bar{\bar{\gamma}} = \pi\nu$, where $\pi : F' \to F'/K$ is the natural epimorphism. Since K is also a central subgroup of F, we can form the factor group $X = F/K$, which is a p-group of class 2, exponent p and order p^{2n}.

Let $\bar{\bar{\xi}}$ denote the automorphism of X (like ξ and $\bar{\xi}$, having order $|Q|$) induced by the automorphism ξ of F and let Q be the subgroup of $\mathrm{Aut}(X)$ generated by $\bar{\bar{\xi}}$. Let $\sigma : Q \to Q$ be the group isomorphism such that $\bar{\xi}^{\sigma} = \bar{\bar{\xi}}$. Then the Q-group X becomes a Q-group via σ^{-1}, it has Q-length 2 and its Q-composition factors $X/X' = F/F'$ and $X' = F'/K$, regarded as $\mathbf{F}_pQ$-modules via σ, are both isomorphic to V. We clearly have $\Phi(X) = X'$, and also $\mathbf{Z}(X) = X'$, because $\mathbf{Z}(X)$ is a proper Q-subgroup of X which contains the derived subgroup X', and X/X' is an irreducible $\mathbf{F}_pQ$-module.

For each

$$\varphi \in \mathrm{Hom}_{\mathbf{F}_pQ}(X/X', X'),$$

the map w_φ defined by

$$x^{w_\varphi} = x(xX')^{\varphi} \text{ for all } x \in X,$$

is an automorphism of X commuting with ξ. The set

$$W = \{w_\varphi \mid \varphi \in \mathrm{Hom}_{\mathbf{F}_p Q}(X/X', X')\}$$

is a subgroup of $\mathrm{Aut}_Q(X)$, and the order of W equals the order of X/X', namely p^n. In fact, if we put $D_2 = X$, $N_2 = X'$ and $Q_2 = Q$, then D_2 satisfies conditions (1), ..., (6) of Section 5.2, and W is exactly the subgroup W_2 of $\mathrm{Aut}_{Q_2}(D_2)$ which is defined there.

Let us define

$$G_2 = [D_2](W_2 \times Q_2)$$

as in Section 5.2. The group G_2 will also be called H here and we shall therefore write

$$H = [X](W \times Q).$$

Since all assumptions of the previous section are satisfied, Lemma 5.2.1 applies and yields that G and H have identical character tables, and that $H' = X$, whence $H'' = X'$ and $H''' = 1$. Thus G and H have identical character tables and G is metabelian, as we saw earlier, while H has derived length 3.

We observe that the group $X = H'$ has a unique Q-composition series, namely

$$1 < X' < X,$$

which is also part of a chief series of H going from 1 to X. According to the analysis of commutation in X which we carried out in Section 3.4, the $\mathbf{F}_p Q$-module epimorphism associated with our chief series is the following:

$$\begin{aligned} \delta\pi : (X/X') \wedge (X/X') &\rightarrow X' \\ (xX') \wedge (yX') &\mapsto [x, y]. \end{aligned}$$

Now, the $\mathbf{F}_p Q$-module epimorphism $\delta\pi$ coincides with our prescribed $\mathbf{F}_p Q$-module epimorphism $\gamma : V \wedge V \rightarrow V$, after identifying X/X' and X' with V by means of suitable $\mathbf{F}_p Q$-module isomorphisms. In fact, one can easily check that the following diagram is commutative:

$$\begin{tikzcd} (X/X') \wedge (X/X') \arrow[r, "\delta\pi"] & X' \arrow[d, "\nu"] \\ V \wedge V \arrow[u, "\tau \wedge \tau"] \arrow[r, "\gamma"] & V. \end{tikzcd}$$

As we promised, under the assumption $p \neq 2$, we have constructed pairs of groups (G, H) which satisfy Hypotheses 3.1.2 and which give rise, through the method of Section 3.4, to any arbitrarily given $\mathbf{F}_p Q$-module epimorphism $\gamma : V \wedge V \to V$.

Let us remark that the normal Sylow p-subgroups of G and H, namely $P = AW$ and $P = XW$, have identical character tables, as one could easily show by applying Corollary 4.3.2. Of course P and P are both metabelian, because they are nilpotent groups of class two, but we want to stress here that they are not isomorphic. Let us prove this fact.

Let $\mathcal{A}_P$ (and respectively $\mathcal{A}_P$) denote the set of the abelian subgroups of P (resp. P) of order p^{2n} and containing P' (resp. P'). Once we prove that the sets $\mathcal{A}_P$ and $\mathcal{A}_P$ have different cardinality, it will follow that P and P are not isomorphic.

First, let K be a non trivial subgroup of Q, and let S be a subgroup of P of order p^{2n} which contains P' and is normalized by K. According to Lemma 2.1.1 we have

$$S = [S, K]\mathbf{C}_S(K),$$

with $[S, K] \leq G' = A$ and $\mathbf{C}_S(K) \leq \mathbf{C}_P(K) = W$ (this last assertion follows easily from statements (ii) and (iii) of Lemma 3.2.1). Let us assume that S is different from A and $P'W$, that is to say, $[S, K] > P'$ and $\mathbf{C}_S(K) \neq 1$. Let w be a non-identity element of $\mathbf{C}_S(K)$, and hence in particular of W; then the map

$$\begin{array}{ccc} A & \to & P' \\ a & \mapsto & [a, w] \end{array}$$

is by construction a group epimorphism with kernel P', and hence its restriction to the subgroup $[S, K]$ of A is not the zero homomorphism. As a consequence, S is not abelian. It follows that A (which is G') and $P'W$ are the only abelian subgroups of P of order p^{2n} which contain P' and are normalized by some non-trivial subgroup K of Q. Since Q acts on $\mathcal{A}_P$ and every non-trivial subgroup K of Q fixes only the elements A and $P'W$ of $\mathcal{A}_P$, it follows that all orbits of Q on $\mathcal{A}_P \setminus \{A, P'W\}$ have length $|Q|$; therefore we have

$$|\mathcal{A}_P| \equiv 2 \bmod |Q|.$$

Similarly one proves that $P'W = X'W$ is the only abelian subgroup of P of order p^{2n} which contains $P' = X'$ and is normalized by some non-trivial subgroup of Q (because in this case $H' = X$ is not abelian). Here Q acts on $\mathcal{A}_P$, and every non-trivial subgroup of Q fixes only the element $P'W$ of $\mathcal{A}_P$. It follows that

$$|\mathcal{A}_P| \equiv 1 \bmod |Q|.$$

Since $|Q| = |Q|$, we conclude that P and P are not isomorphic.

Finally let us compute the smallest possible order of G (and hence of H) for a pair of groups (G, H) constructed by the above method. As we saw in Section 3.5, V cannot appear as a composition factor of $V \wedge V$ unless the dimension of V over $\mathbf{F}_p$ is at least 4. Moreover, there exists a faithful irreducible module V of dimension 4 over $\mathbf{F}_p$ for a (non-trivial) cyclic p'-group Q, such that V is isomorphic to a composition factor of $V \wedge V$, if and only if Q has order 5 and $p \equiv 2$ or $3 \bmod 5$. Since in the present section we assumed that p is odd, we see that the smallest possible value for $|G|$ occurs when $p = 3$ and $|Q| = 5$, in which case we have

$$|G| = 3^{12} \cdot 5.$$

5.4 Matrix representations for the unary case

All groups G and H which we have constructed have natural faithful representations as groups of matrices over $\mathbf{F}_{p^n}$; in other words, G and H are isomorphic to certain subgroups of $GL_r(p^n)$ for some r. Whereas G is isomorphic to a subgroup of $GL_3(p^n)$, we need bigger matrices for representing H. The smallest possible size depends on the choice of the particular $\mathbf{F}_pQ$-module epimorphism $\gamma : V \wedge V \to V$. We shall not discuss such matrix representations in general. However, for each choice of an odd prime p and of a faithful irreducible module V for a cyclic p'-group Q over $\mathbf{F}_p$, such that V is a composition factor of $V \wedge V$, we shall choose a particular $\mathbf{F}_pQ$-module epimorphism $\bar{\gamma} : V \wedge V \to V$ and give an explicit representation of the resulting group H as a subgroup of $GL_4(p^n)$.

We recall that if V is a faithful irreducible module for a cyclic group Q over $\mathbf{F}_p$, then V is isomorphic to the module V_ε defined in Theorem 2.3.1, for a suitable primitive $|Q|$th root of unity ε in $\mathbf{F}_{p^n}$, where n is the dimension of V over $\mathbf{F}_p$. Furthermore, according to Lemma 3.5.1, the fact that V is a composition factor of $V \wedge V$ (or of $V \otimes V$) depends only on the prime p and the order q of Q. As a consequence, we do not lose in generality if we take, as the basic ingredients of our construction, an odd prime p and a positive integer q satisfying the conditions stated below.

Let us fix an odd prime p and a positive integer q, such that

$$p^i + 1 \equiv p^j \bmod q$$

for some integers i, j, with i not divisible by n, where n is the multiplicative order of $p \bmod q$. It follows from the observation which precedes Lemma 3.5.1 that we may always assume that

$$0 < i \leq n/2 \qquad \text{and} \qquad 0 \leq j < n.$$

Even with this assumption, the pair (i, j) is in general not unique. For instance, if q is also a prime and p has multiplicative order $q - 1 \bmod q$ (examples are given by $(p, q) = (3, 5), (5, 7), (7, 11)$), then

$$\{p, p^2, \ldots, p^{q-2}\} \equiv \{2, 3, \ldots, q-1\} \bmod q;$$

consequently, if $q \geq 5$ there exists at least one pair (i, j) of integers such that

$$p^i + 1 \equiv p^j \bmod q,$$

and with

$$0 < i \leq (q-1)/2 \qquad \text{and} \qquad 0 \leq j < q - 1;$$

if $q \geq 7$, there exist at least two such pairs.

Let $Q = \langle \xi \rangle$ be a cyclic group of order q, and let ε be a primitive qth root of unity in $\mathbb{F}_{p^n}$. According to Theorem 2.3.1, the module V_ε is a faithful irreducible module for Q over $\mathbb{F}_p$, where the underlying vector space of V_ε is the field $\mathbb{F}_{p^n}$, and the action of Q on V_ε is given by

$$v\xi = \varepsilon v \quad \text{for all } v \in V_\varepsilon.$$

We shall also consider the $\mathbb{F}_pQ$-module $V_{\varepsilon^{p^j}}$ defined similarly, which is isomorphic to V_ε via the $\mathbb{F}_pQ$-module isomorphism

$$\begin{aligned} V_\varepsilon &\to V_{\varepsilon^{p^j}} \\ v &\mapsto v^{p^j}. \end{aligned}$$

Because of our assumptions on p and q, and according to Lemma 3.5.1, the $\mathbb{F}_pQ$-module $V_\varepsilon \wedge V_\varepsilon$ has a composition factor isomorphic to V_ε, and hence to $V_{\varepsilon^{p^j}}$. Actually, we can explicitly define an $\mathbf{F}_pQ$-epimorphism from $V_\varepsilon \wedge V_\varepsilon$ onto $V_{\varepsilon^{p^j}}$, as follows. Let $\bar\gamma$ be the map

$$\bar\gamma : V_\varepsilon \wedge V_\varepsilon \to V_{\varepsilon^{p^j}}$$

such that

$$(x \wedge y)^{\bar\gamma} = xy^{p^i} - x^{p^i}y \quad \text{for all } x, y \in V_\varepsilon.$$

Because the expression $xy^{p^i} - x^{p^i}y$ is $\mathbf{F}_p$-bilinear and skew-symmetric in (x, y), the map $\bar\gamma$ is well defined and $\mathbf{F}_p$-linear. We have

$$\begin{aligned}
((x \wedge y)\xi)^{\bar\gamma} &= ((\varepsilon x) \wedge (\varepsilon y))^{\bar\gamma} \\
&= \varepsilon^{1+p^i}(xy^{p^i} - x^{p^i}y) \\
&= \varepsilon^{1+p^i}(x \wedge y)^{\bar\gamma} \\
&= \varepsilon^{p^j}(x \wedge y)^{\bar\gamma} \\
&= (x \wedge y)^{\bar\gamma}\xi,
\end{aligned}$$

and hence it follows by $\mathbf{F}_p$-linearity that $\bar\gamma$ is an $\mathbf{F}_pQ$-module homomorphism.

Furthermore, $\bar\gamma$ is surjective. In fact, a non-zero element of $V_\varepsilon \wedge V_\varepsilon$ of the form $x \wedge y$ (which of course is not a generic element of $V_\varepsilon \wedge V_\varepsilon$) belongs to the kernel of $\bar\gamma$ exactly when

$$(xy^{-1})^{p^i} = xy^{-1};$$

on the other hand, the field automorphism of $\mathbf{F}_{p^n}$ given by $x \mapsto x^{p^i}$ is not the identity automorphism, because i is not a multiple of n. It follows that the kernel of $\bar\gamma$ is not the whole of $V_\varepsilon \wedge V_\varepsilon$. Hence $\bar\gamma$ is not the zero homomorphism, and thus it is an $\mathbf{F}_pQ$-module epimorphism, because $V_{\varepsilon^{p^j}}$ is irreducible. (It should be said that not all $\mathbf{F}_pQ$-module epimorphisms from $V \wedge V$ onto V can be put into this particularly simple form by suitably identifying V with V_ε and $V_{\varepsilon^{p^j}}$.)

With this particular choice of the $\mathbf{F}_pQ$-module epimorphism $\bar\gamma$, let us define the group $X = F/K$ as we did in Section 5.3. The set X_3 whose elements are the matrices

$$\begin{vmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{vmatrix}$$

with $a, b \in \mathbb{F}_{p^n}$ is clearly a subgroup of $GL_3(p^n)$ (because the map $a \mapsto a^{p^i}$ is a field automorphism of $\mathbb{F}_{p^n}$, and in particular it is $\mathbb{F}_p$-linear). Furthermore, X_3 is isomorphic to X. In fact, it is not difficult to define an epimorphism from F onto X with kernel K, after noticing that

$$\begin{bmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & & aa^{p^i} - a^{p^i}a \\ & 1 & \\ & & 1 \end{bmatrix}.$$

It is also clear that the diagonal matrix

$$\xi_3 = \begin{bmatrix} 1 & & \\ & \varepsilon & \\ & & \varepsilon^{1+p^i} \end{bmatrix}$$

normalizes X_3, and induces by conjugation an automorphism of X_3 which corresponds to the automorphism ξ of X defined in Section 5.3 (for a suitable choice of the isomorphism from X to X_3). Thus the normal subgroup XQ of H is isomorphic to a subgroup of $GL_3(p^n)$.

Let us note in passing that X_3 would be abelian if i were a multiple of n, which it is not in our case.

Now we are ready to embed the whole of H into $GL_4(p^n)$. First of all, we observe that the set X_4 of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b \\ & 1 & & a^{p^i} \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

with $a, b \in \mathbb{F}_{p^n}$ is a subgroup of $GL_4(p^n)$ isomorphic to X_3 (and hence to X); in fact, the map

$$\begin{bmatrix} 1 & a & b \\ & 1 & a^{p^i} \\ & & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & a & a^{p^j} & b \\ & 1 & & a^{p^i} \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

is an isomorphism from X_3 onto X_4. The diagonal matrix

$$\bar{\xi}_4 = \begin{bmatrix} 1 & & & \\ & \varepsilon & & \\ & & \varepsilon^{p^j} & \\ & & & \varepsilon^{p^j} \end{bmatrix}$$

normalizes X_4 (remember here that $\varepsilon^{1+p^j} = \varepsilon^{p^j}$). The automorphism of X_4 induced by ξ_4 by conjugation corresponds to the automorphism of X_3 induced by ξ_3 by conjugation (with respect to the given isomorphism from X_3 onto X_4) and thus to the automorphism ξ of X (with respect to a suitable isomorphism from X onto X_4).

Now the subgroup W_4 of $GL_4(p^n)$ consisting of the matrices

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & c \\ & & & 1 \end{bmatrix}$$

with $c \in \mathbf{F}_{p^n}$ is elementary abelian of order p^n, centralizes ξ_4, and normalizes X_4; in fact,

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & c \\ & & & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & a & a^{p^j} & b \\ & 1 & & a^{p^j} \\ & & 1 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & c \\ & & & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & a & a^{p^j} & b + a^{p^j}c \\ & 1 & & a^{p^j} \\ & & 1 & \\ & & & 1 \end{bmatrix}.$$

Now it is clear that $H = [X](W \times Q)$ is isomorphic to the subgroup $H_4 = X_4 W_4 \langle \xi_4 \rangle$ of $GL_4(p^n)$, namely the group of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b \\ & \varepsilon^l & & a^{p^j} \\ & & \varepsilon^{lp^j} & c \\ & & & \varepsilon^{lp^j} \end{bmatrix}$$

with $a, b, c \in \mathbb{F}_{p^n}$ and $l = 1, \dots, |Q|$. Thus we have constructed a faithful matrix representation of H.

It is much easier to give a matrix representation of the group G. In fact, it is straightforward to check that G is isomorphic to the subgroup G_3 of $GL_3(p^n)$ which consists of the matrices

$$\begin{bmatrix} 1 & a & b \\ & \varepsilon^l & c \\ & & \varepsilon^l \end{bmatrix}$$

with $a, b, c \in \mathbb{F}_{p^n}$ and $l = 1, \dots, |Q|$; in particular, the normal Sylow p-subgroup AW of G is isomorphic to a Sylow p-subgroup of $GL_3(p^n)$.

Let us also notice that G is isomorphic to the subgroup G_4 of $GL_4(p^n)$ which consists of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b \\ & \varepsilon^l & & \\ & & \varepsilon^{lp^j} & c \\ & & & \varepsilon^{lp^j} \end{bmatrix}$$

with $a, b, c \in \mathbb{F}_{p^n}$ and $l = 1, \dots, |Q|$. In fact, an isomorphism from G_3 onto G_4 is given by the map

$$\begin{bmatrix} 1 & a & b \\ & \varepsilon^l & c \\ & & \varepsilon^l \end{bmatrix} \mapsto \begin{bmatrix} 1 & a & a^{p^j} & b^{p^j} \\ & \varepsilon^l & & \\ & & \varepsilon^{lp^j} & c^{p^j} \\ & & & \varepsilon^{lp^j} \end{bmatrix}.$$

Since G_4 and H_4 normalize each other, G_4H_4 is a subgroup of $GL_4(p^n)$. Clearly G_4H_4 consists of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b \\ & \varepsilon^l & & d \\ & & \varepsilon^{lp^j} & c \\ & & & \varepsilon^{lp^j} \end{bmatrix}$$

with $a, b, c, d \in \mathbb{F}_{p^n}$ and $l = 1, \dots, |Q|$. The groups G_4 and H_4 are normal subgroups of G_4H_4 of index p^n. In particular, we have shown that our groups

G and H can be simultaneously embedded as normal subgroups into a group of order $p^n|G|$.

As a final remark, we observe that the construction of all groups of matrices of this section works as well if we drop our assumption that the prime p is odd. The resulting groups G_4 and H_4 do have identical character tables and derived length 2 and 3 respectively, even if $p = 2$. The only differences for $p = 2$ are that they do not correspond to any of the groups defined in Section 5.3, and that the normal Sylow 2-subgroups of G_4 and H_4 have exponent $4 = p^2$ instead of p. However, the construction of Section 5.3 could be easily modified in order to include the case $p = 2$. If we allow $p = 2$, then the smallest possible order for G_4 and H_4 drops down to $2^{12} \cdot 5$.

5.5 The binary case

Let p be an odd prime, and let us make the following assumptions:

- Q is a non-trivial cyclic group of p' order;
- V is a faithful irreducible $\mathbb{F}_pQ$-module;
- $\gamma : V \otimes V \to V$ is a fixed $\mathbb{F}_pQ$-module epimorphism.

Let $A = V \oplus V \oplus V$ be the direct sum of three copies of V. We have

$$\mathrm{Hom}_{\mathbb{F}_pQ}(A/(0 \oplus 0 \oplus V), 0 \oplus 0 \oplus V) \cong \mathbb{F}_{p^n} \oplus \mathbb{F}_{p^n},$$

as vector spaces over $\mathbb{F}_p$, where n is the dimension of V over $\mathbb{F}_p$. For any

$$\varphi \in \mathrm{Hom}_{\mathbb{F}_pQ}(A/(0 \oplus 0 \oplus V), 0 \oplus 0 \oplus V),$$

the map w_φ defined by

$$a^{w_\varphi} = a + (a + (0 \oplus 0 \oplus V))^\varphi \quad \text{for all } a \in A,$$

is an automorphism of A as an $\mathbb{F}_pQ$-module. The group

$$W = \{w_\varphi \mid \varphi \in \mathrm{Hom}_{\mathbb{F}_pQ}(A/(0 \oplus 0 \oplus V), 0 \oplus 0 \oplus V)\}$$

is a subgroup of $\mathrm{Aut}_{\mathbb{F}_pQ}(A)$, of order $|V \oplus V| = p^{2n}$. With the notation of Section 5.2, we may take $D_1 = A$, $N_1 = 0 \oplus 0 \oplus V$, $Q_1 = Q$, and thus obtain $W_1 = W$. Let us construct the semidirect product

$$G_1 = [D_1](W_1 \times Q_1)$$

as in Section 5.2. The group G_1 will also be called G here and we shall therefore write

$$G = [A](W \times Q).$$

According to Lemma 5.2.1, we have $G' = A$; therefore $G'' = 1$, and thus G is metabelian.

Let us pass to the construction of the group H. Let

$$\bar{F} = \langle x_1, \dots, x_n, y_1, \dots, y_n \rangle$$

be a free group of rank $2n$. Then $\bar{F}/\gamma_3(\bar{F})\bar{F}^p$ is a free nilpotent group of class two and exponent p. Its derived subgroup is elementary abelian of order $p^{n(2n-1)}$ and, according to Lemma 2.6.3, it has a basis over $\mathbb{F}_p$ given by the set of basic commutators of weight 2 on $x_1, \dots, x_n, y_1, \dots, y_n$, namely

$$\{[x_j, x_k],\ [y_j, y_k] \mid 1 \leq k < j \leq n\} \cup \{[y_j, x_k] \mid j, k = 1, \dots, n\}.$$

Let us put $R = \langle [x_j, x_k],\ [y_j, y_k] \mid 1 \leq k < j \leq n \rangle$ and define

$$F = \bar{F}/\gamma_3(\bar{F})\bar{F}^p R.$$

Then F' is clearly elementary abelian of order p^{n^2} and a basis of F' over $\mathbb{F}_p$ is given by the set

$$\{[y_j, x_k] \mid j, k = 1, \dots, n\}.$$

The factor group F/F' is a free abelian group of exponent p and rank $2n$; in other words, it is elementary abelian of order p^{2n}. Let us fix an $\mathbb{F}_p$-linear isomorphism

$$\tau : V \oplus V \to F/F'$$

such that τ maps

$$V \oplus 0 \quad \text{onto} \quad \langle x_1, \dots, x_n \rangle F'/F',$$

$$\text{and} \quad 0 \oplus V \quad \text{onto} \quad \langle y_1, \dots, y_n \rangle F'/F'.$$

Let us make F/F' into an $\mathbb{F}_p Q$-module isomorphic to $V \oplus V$ via τ, namely let us define an action of Q on F/F' according to the formula

$$(xF')^\xi = ((xF')^{\tau^{-1}}\xi)^\tau \quad \text{for all } x \in F \text{ and for all } \xi \in Q,$$

and extend it $\mathbb{F}_p$-linearly to an action of $\mathbb{F}_pQ$ on F/F'. Thus F/F' becomes an $\mathbb{F}_pQ$-module and τ an $\mathbb{F}_pQ$-module isomorphism. Furthermore, F/F' is the direct sum of the $\mathbb{F}_pQ$-submodules $\langle x_1, \ldots, x_n\rangle F'/F'$ and $\langle y_1, \ldots, x_n\rangle F'/F'$.

Let us fix a generator ξ of Q. We shall show that the automorphism of F/F' induced by ξ can be lifted to an automorphism $\hat{\xi}$ of F. First of all, the automorphism induced by ξ on $F/F' = \hat{F}/\hat{F}'\hat{F}^p$ can be lifted to an automorphism $\hat{\xi}$ of the free group $\hat{F}$, and we may assume that the subgroups $\hat{F}_1 = \langle x_1, \ldots, x_n\rangle$ and $\hat{F}_2 = \langle y_1, \ldots, y_n\rangle$ of $\hat{F}$ are left invariant by $\hat{\xi}$. In particular, the subgroups

$$\hat{F}_1' = \langle [x_j, x_k], \gamma_3(\hat{F}_1) \mid 1 \leq k < j \leq n\rangle$$

and

$$\hat{F}_2' = \langle [y_j, y_k], \gamma_3(\hat{F}_2) \mid 1 \leq k < j \leq n\rangle$$

are left invariant by $\hat{\xi}$, or in other words, $(\hat{F}_1')^{\hat{\xi}} = \hat{F}_1'$ and $(\hat{F}_2')^{\hat{\xi}} = \hat{F}_2'$. Since $\gamma_3(\hat{F})$ and $\hat{F}^p$ are characteristic subgroups of $\hat{F}$, we also have that $\gamma_3(\hat{F})^{\hat{\xi}} = \gamma_3(\hat{F})$ and $(\hat{F}^p)^{\hat{\xi}} = \hat{F}^p$. As a consequence, the automorphism $\hat{\xi}$ of $\hat{F}$ induces an automorphism of $F = \hat{F}/\gamma_3(\hat{F})\hat{F}^p\hat{F}_1'\hat{F}_2'$, which we shall also call $\hat{\xi}$. We may assume that $\hat{\xi}$ has order $|Q|$ (otherwise we may replace $\hat{\xi}$ with a suitable power $\hat{\xi}^{p^{m'}}$), and thus we can regard F as a Q-group. In particular, F' can be regarded as a (semisimple) $\mathbb{F}_pQ$-module.

Now let us put

$$E = \langle F', x_1, \ldots, x_n\rangle$$

and let us apply Lemma 2.2.1 to the following subgroups of F:

$$K_3 = 1, \quad H_3 = K_1 = F', \quad H_1 = K_2 = E, \quad H_2 = F.$$

Thus we obtain an $\mathbb{F}_p$-bilinear map

$$\begin{aligned} \delta : (E/F') \times (F/E) &\to F' \\ (xF', yE) &\mapsto [x, y]. \end{aligned}$$

Since E is a Q-subgroup of F, the factor groups E/F', F/E can also be regarded as $\mathbb{F}_pQ$-modules. Thus we obtain an $\mathbb{F}_pQ$-module homomorphism

$$\begin{aligned} \delta : (E/F') \otimes (F/E) &\to F' \\ (xF') \otimes (yE) &\mapsto [x, y]. \end{aligned}$$

Actually, δ is an isomorphism. In fact, the set

$$\{(x_jF') \otimes (y_kE) \mid j, k = 1, \dots, n\}$$

is a basis of $(E/F') \otimes (F/E)$ over $\mathbb{F}_p$, and we have

$$((x_jF') \otimes (y_kE))^\delta = [x_j, y_k] = [y_k, x_j]^{-1};$$

on the other hand, the elements $[y_k, x_j]$ of F' are distinct for $j, k = 1, \dots, n$ and form a basis of F' over $\mathbb{F}_p$, as we saw earlier. Thus δ is an $\mathbb{F}_pQ$-module isomorphism, and hence F' is isomorphic to $V \otimes V$ as an $\mathbb{F}_pQ$-module.

Now the $\mathbb{F}_pQ$-module isomorphism

$$\tau : V \oplus V \to F/F'$$

induces two $\mathbb{F}_pQ$-module isomorphisms from V onto E/F' and F/E respectively, namely

$$\begin{aligned} \tau_1 : V &\to E/F' \\ v &\mapsto (v, 0)^\tau, \end{aligned}$$

and

$$\begin{aligned} \tau_2 : V &\to F/E \\ v &\mapsto (0, v)^\tau E. \end{aligned}$$

An $\mathbb{F}_pQ$-module isomorphism

$$\tau_1 \otimes \tau_2 : V \otimes V \to (E/F') \otimes (F/E)$$

is induced in an obvious way, and we have the following commutative diagram of $\mathbb{F}_pQ$-module homomorphisms:

$$\begin{tikzcd} (E/F') \otimes (F/E) \arrow[r, "\delta"] & F' \arrow[d, "\delta^{-1}(\tau_1\otimes\tau_2)^{-1}\gamma"] \\ V \otimes V \arrow[u, "\tau_1\otimes\tau_2"] \arrow[r, "\gamma"] & V \end{tikzcd}$$

Let us put

$$K = \ker\,(\delta^{-1}(\tau_1 \otimes \tau_2)^{-1}\gamma) = (\ker\,\gamma)^{(\tau_1\otimes\tau_2)\delta}.$$

The factor group F'/K is then an $\mathbb{F}_pQ$-module and the $\mathbb{F}_pQ$-module epimorphism

$$\delta^{-1}(\tau_1 \otimes \tau_2)^{-1}\gamma : F' \to V$$

induces an $\mathbb{F}_pQ$-module isomorphism

$$\nu : F'/K \to V$$

such that $\delta^{-1}(\tau_1 \otimes \tau_2)^{-1}\gamma = \pi\nu$, where $\pi : F' \to F'/K$ is the natural epimorphism. Since K is also a central subgroup of F, we can form the factor group $X = F/K$, which is a p-group of class 2, exponent p and order p^{3n}. Let us put $L = E/K$. Then L is an elementary abelian normal subgroup of X and has order p^{2n}.

Let ξ denote the automorphism of X (like ξ and $\bar{\xi}$, having order $|Q|$) induced by the automorphism ξ of F and let Q be the subgroup of $\mathrm{Aut}(X)$ generated by ξ. Let $\sigma : Q \to Q$ be the group isomorphism such that $\xi^\sigma = \xi$. Then the Q-group X becomes a Q-group of Q-length 3 via σ^{-1}. The series

$$1 < X' < L < X$$

is a Q-composition series of X and the Q-composition factors of X, regarded as $\mathbb{F}_pQ$-modules via σ, are all isomorphic to V. Furthermore, the factor group X/X' is elementary abelian, and regarded as an $\mathbb{F}_pQ$-module it is isomorphic to $V \oplus V$. In particular, X' is the Frattini subgroup of X.

Furthermore, we have that $\mathbf{Z}(X) = X'$. In fact, $\mathbf{Z}(X)$ is a Q-subgroup of X, and it contains X'. Let us suppose for a moment that $X' < \mathbf{Z}(X)$. It follows that $\mathbf{Z}(X)$ has Q-length 2, because $\mathbf{Z}(X)$ cannot be the whole of X, which is not abelian. If $\mathbf{Z}(X)$ contained L, then from the fact that $[L, X] = 1$, it would follow that $[E, F] \leq K$; this would contradict the fact that the map δ defined above is an isomorphism. We deduce that $\mathbf{Z}(X) \neq L$, and thus that $\mathbf{Z}(X)L = X$, because X/X' has Q-length 2. It follows that $X' = L' = 1$, which contradicts the fact that X is not abelian. As a consequence, our assumption is wrong, and therefore we get that $\mathbf{Z}(X) = X'$.

For each

$$\varphi \in \mathrm{Hom}_{\mathbb{F}_pQ}(X/X', X'),$$

the map w_φ defined by

$$x^{w_\varphi} = x(xX')^\varphi \quad \text{for all } x \in X,$$

is an automorphism of X commuting with ξ. The set

$$W = \{w_\varphi \mid \varphi \in \mathrm{Hom}_{\mathbf{F}_pQ}(X/X', X')\}$$

is a subgroup of $\mathrm{Aut}_Q(X)$, and the order of W equals the order of X/X', namely p^{2n}. In fact, if we put $D_2 = X$, $N_2 = X'$ and $Q_2 = Q$, then D_2 satisfies conditions (1), ..., (6) of Section 5.2, and W is exactly the subgroup W_2 of $\mathrm{Aut}_{Q_2}(D_2)$ which is defined there.

Let us define

$$G_2 = [D_2](W_2 \times Q_2)$$

as in Section 5.2. The group G_2 will also be called H here and we will therefore write

$$H = [X](W \times Q).$$

Since all assumptions of Section 5.2 are satisfied, Lemma 5.2.1 applies and yields that G and H have identical character tables, and that $H' = X$, whence $H'' = X'$ and $H''' = 1$. Thus G and H have identical character tables and G is metabelian, as we said earlier, while H has derived length 3.

Let us consider the following Q-composition series of X, which is also part of a chief series of H going from 1 to X:

$$1 < X' < L < X.$$

According to the analysis of commutation in X which we carried out in Section 3.4, the $\mathbf{F}_pQ$-module epimorphism associated with our chief series is the following:

$$\begin{aligned} \delta\pi : (L/X') \otimes (X/L) &\rightarrow X' \\ (xX') \otimes (yL) &\mapsto [x, y], \end{aligned}$$

where the factor groups L/X' and X/L have been identified with E/F' and F/E respectively. If we regard the $\mathbf{F}_pQ$-modules L/X', X/L and X' as $\mathbf{F}_pQ$-modules via σ, then the $\mathbf{F}_pQ$-module epimorphism $\delta\pi$ is also an $\mathbf{F}_pQ$-module epimorphism. As such, $\delta\pi$ coincides with our prescribed $\mathbf{F}_pQ$-module epimorphism $\gamma : V \otimes V \rightarrow V$, after identifying L/X', X/L and X' with V by means of suitable $\mathbf{F}_pQ$-module isomorphisms. In other words, the following diagram is commutative:

$$
\begin{tikzcd}
(L/X') \otimes (X/L) \arrow[rr, "\delta_\otimes"] & & X' \arrow[d, "\nu"] \\
V \otimes V \arrow[u, "\eta \otimes \eta"] \arrow[rr, "\gamma"] & & V.
\end{tikzcd}
$$

As we promised, in analogy with what we did in Section 5.3 for the map γ, under the assumption $p \neq 2$ we have constructed pairs of groups (G, H) which satisfy Hypotheses 3.1.2 and which give rise,through the method of Section 5.2, to any arbitrarily given $\mathbf{F}_p Q$-module epimorphism $\gamma : V \otimes V \to V$.

It is perhaps worth remarking that

$$1 < X' < L < X$$

is not in this case the unique Q-composition series of X, nor the unique chief series of H passing through 1 and H. If we choose a different Q-composition series

$$1 < X' < \tilde{L} < X,$$

it may happen that $\tilde{L}$ is not abelian. In that case, our analysis of commutation in X would produce a non-trivial skew-symmetric $\mathbf{F}_p$-bilinear map

$$\delta' : (\tilde{L}/X') \times (\tilde{L}/X') \to X',$$

and thus we would fall again into the unary case, for which we have already built examples in Section 5.3. However, the situation described above cannot happen if our $\mathbf{F}_p Q$-module V is a composition factor of $V \otimes V$, but not of $V \wedge V$ (for example, if V has dimension 2 or 3 over $\mathbf{F}_p$); this shows that the binary case gives rise to examples which are genuinely different from those of the unary case.

Now, we observe that the normal Sylow p-subgroups of G and H, namely $P = AW$ and $P = XW$, have identical character tables but are not isomorphic. We omit the proof of this fact, which consists of a counting argument similar to that which we used in the proof of the corresponding fact of Section 5.3. We only observe that the argument here is slightly more complicated, because A/P' is not a chief factor of G; therefore, in addition to the set $\mathcal{A}_P$ of abelian subgroups of P which have order p^{3n} and contain P', one needs to consider also the set $\mathcal{B}_P$ of unordered pairs $\{B, C\}$ of elements of $\mathcal{A}_P$ such that $BC = P$ (and similar sets $\mathcal{A}_{\bar{P}}$ and $\mathcal{B}_{\bar{P}}$ concerning $\bar{P}$).

We conclude this section by computing the smallest possible order of G and H for a pair (G, H) of groups constructed as above. It follows easily from the case-study which concludes Section 3.5 that if p is an odd prime, Q is a non-trivial cyclic p'-group, and V is faithful irreducible module for Q over $\mathbb{F}_p$ such that $V \otimes V$ has a composition factor isomorphic to V, then the smallest possible order of V is attained when V has dimension 2 over $\mathbb{F}_p$, the group Q has order 3, and the prime p is 5. In that case, V has 25 elements, and the order of G is as small as possible, namely

$$|G| = 5^{10} \cdot 3;$$

however, this is bigger that $3^{12} \cdot 5$, that is the order of the smallest groups G and H which we constructed in Section 5.3.

5.6 Matrix representations for the binary case

In this section we shall construct explicit matrix representations for some of the groups of Section 5.5. We shall represent faithfully G as a subgroup of $GL_4(p^n)$, and H as a subgroup of $GL_5(p^n)$.

Let us fix an odd prime p and a positive integer q such that

$$p^i + 1 \equiv p^j \bmod |Q|$$

for some integers i, j (and we may always assume that

$$0 \leq i \leq n/2 \qquad \text{and} \qquad 0 \leq j < n).$$

Let $Q = \langle \xi \rangle$ be a cyclic group of order q, and let ε be a primitive q-th root of unity in $\mathbb{F}_{p^n}$. Let V_ε be a cyclic group of order q, and let ε be a primitive qth root of unity in $\mathbb{F}_{p^n}$. Let V_ε be the faithful irreducible module for Q over $\mathbb{F}_p$ which is defined in Theorem 2.3.1. We shall also consider the $\mathbb{F}_pQ$-modules $V_{\varepsilon^{p^i}}$ and $V_{\varepsilon^{p^j}}$ defined similarly, which are both isomorphic to V_ε. Because of our assumptions on p and q, the module V_ε appears as a composition factor of the tensor square module $V_\varepsilon \otimes V_\varepsilon$. We shall explicitly define an $\mathbb{F}_pQ$-epimorphism from $V_\varepsilon \otimes V_{\varepsilon^{p^i}}$ onto $V_{\varepsilon^{p^j}}$.

For all pure tensors $x \otimes y$ of $V_\varepsilon \otimes V_{\varepsilon^{p^i}}$, let us define

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

Since the expression xy is $\mathbf{F}_p$-bilinear in (x, y), it follows that γ extends to an $\mathbf{F}_p$-linear map

$$\gamma : V_\varepsilon \otimes V_{\varepsilon^{p^i}} \to V_{\varepsilon^{p^j}}.$$

Furthermore, the map γ is an $\mathbf{F}_p Q$-module homomorphism, because we have

$$\begin{aligned}
((x \otimes y)\xi)^\gamma &= ((\varepsilon x) \otimes (\varepsilon^{p^i} y))^\gamma \\
&= \varepsilon^{1+p^i} xy \\
&= \varepsilon^{1+p^i} (x \otimes y)^\gamma \\
&= \varepsilon^{p^j} (x \otimes y)^\gamma \\
&= (x \otimes y)^\gamma \xi.
\end{aligned}$$

It is clear that γ is not the zero homomorphism. Thus γ is an $\mathbf{F}_p Q$-module epimorphism, because $V_{\varepsilon^{p^j}}$ is an irreducible $\mathbf{F}_p Q$-module. (It should be said that not all $\mathbf{F}_p Q$-module epimorphisms from $V \otimes V$ onto V can be put into this particularly simple form by suitably identifying V with V_ε, $V_{\varepsilon^{p^i}}$ and $V_{\varepsilon^{p^j}}$.)

With this particular choice of the $\mathbf{F}_p Q$-epimorphism γ, let us define the group $X = F/K$ as we did in Section 5.5. Let X_3 be the set of the matrices

$$\begin{bmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{bmatrix},$$

with $a, b, c \in \mathbf{F}_{p^n}$; hence X_3 is a Sylow p-subgroup of $GL_3(p^n)$. Moreover, X_3 is isomorphic to X, and it is not too difficult to construct an epimorphism from F onto X, with kernel K. It is also clear that the diagonal matrix

$$\xi_3 = \begin{bmatrix} 1 & & \\ & \varepsilon & \\ & & \varepsilon^{1+p^i} \end{bmatrix}$$

normalizes X_3, and induces by conjugation an automorphism of X_3 which corresponds to the automorphism ξ of X defined in Section 5.5 (for a suitable choice of the isomorphism $X \to X_3$). Thus the normal subgroup XQ of H is isomorphic to a subgroup of $GL_3(p^n)$.

Now we are ready to embed the whole of H into $GL_5(p^n)$. First of all, we observe that the set X_5 of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b^{p^j} & c \\ & 1 & & & b \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$$

with $a, b, c \in \mathbb{F}_{p^n}$ is a subgroup of $GL_5(p^n)$ isomorphic to X_3 (and hence to X). In fact, an explicit isomorphism from X_3 onto X_5 is given by the map

$$\begin{bmatrix} 1 & a & c \\ & 1 & b^{p^i} \\ & & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & a & a^{p^j} & b^{p^j} & c \\ & 1 & & & b^{p^i} \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}.$$

The diagonal matrix

$$\xi_5 = \begin{bmatrix} 1 & & & & \\ & \varepsilon & & & \\ & & \varepsilon^{p^j} & & \\ & & & \varepsilon^{p^j} & \\ & & & & \varepsilon^{p^j} \end{bmatrix}$$

normalizes X_5. The automorphism of X_5 induced by ξ_5 by conjugation corresponds to the automorphism of X_3 induced by ξ_3 by conjugation (with respect to the given isomorphism from X_3 onto X_5) and thus to the automorphism ξ of X (with respect to a suitable isomorphism from X onto X_5).

Now the subgroup W_5 of $GL_5(p^n)$ consisting of the matrices

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & d \\ & & & 1 & e \\ & & & & 1 \end{bmatrix}$$

with $d, e \in \mathbb{F}_{p^n}$ is elementary abelian of order p^{2n}, centralizes ξ_5, and normalizes X_5. It is quite clear now that $H = [X](W \times Q)$ is isomorphic to the subgroup $H_5 = X_5W_5(\xi_5)$ of $GL_5(p^n)$, namely the group of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b^{p^j} & c \\ & \varepsilon^l & & & b^{p^i} \\ & & \varepsilon^{lp^j} & & d \\ & & & \varepsilon^{lp^j} & e \\ & & & & \varepsilon^{lp^j} \end{bmatrix},$$

with $a, b, c, d, e \in \mathbb{F}_{p^n}$ and $l = 1, \ldots, |Q|$. Thus we have constructed a faithful matrix representation of H.

It is much easier to give a matrix representation of the group G. In fact, it is easy to see that G is isomorphic to the subgroup G_4 of $GL_4(p^n)$ which consists of the matrices

$$\begin{bmatrix} 1 & a & b & c \\ & \varepsilon^l & & d \\ & & \varepsilon^l & e \\ & & & \varepsilon^l \end{bmatrix},$$

with $a, b, c \in \mathbb{F}_{p^n}$ and $l = 1, \ldots, |Q|$.

Let us also notice that G is isomorphic to the subgroup G_5 of $GL_5(p^n)$ which consists of the matrices

$$\begin{bmatrix} 1 & a & a^{p^j} & b & c \\ & \varepsilon^l & & & \\ & & \varepsilon^{lp^j} & & d \\ & & & \varepsilon^{lp^j} & e \\ & & & & \varepsilon^{lp^j} \end{bmatrix}$$

with $a, b, c \in \mathbb{F}_{p^n}$ and $l = 1, \ldots, |Q|$. In fact an isomorphism from G_3 onto G_5 is given by the map

$$\begin{bmatrix} 1 & a & b & c \\ & \varepsilon^l & & d \\ & & \varepsilon^l & e \\ & & & \varepsilon^l \end{bmatrix} \mapsto \begin{bmatrix} 1 & a & a^{p^j} & b^{p^j} & c^{p^j} \\ & \varepsilon^l & & & \\ & & \varepsilon^{lp^j} & & d^{p^j} \\ & & & \varepsilon^{lp^j} & e^{p^j} \\ & & & & \varepsilon^{lp^j} \end{bmatrix}.$$

Since G_5 and H_5 normalize each other, G_5H_5 is a subgroup of $GL_5(p^n)$.

Clearly G_5H_5 consists of the matrices

$$\begin{vmatrix} 1 & a & a^{p^j} & b & c \\ & \varepsilon^{l} & & & f \\ & & \varepsilon^{lp^j} & & d \\ & & & \varepsilon^{lp^j} & e \\ & & & & \varepsilon^{lp^j} \end{vmatrix},$$

with $a, b, c, d, e, f \in \mathbb{F}_{p^n}$ and $l = 1, \ldots, |Q|$. The groups G_5 and H_5 are normal subgroups of G_5H_5 of index p^n. In particular, we have obtained that our groups G and H can be simultaneously embedded as normal subgroups into a group of order $p^n|G|$.

We finally observe that our assumption that the prime p is odd is unnecessary for the construction of our groups of matrices (like it was in Section 5.4). Of course, when $p = 2$, the normal Sylow 2-subgroups of G and H will have exponent $4 = p^2$ instead of p. If we allow $p = 2$, then the smallest possible order for G_5 and H_5 becomes $2^{10} \cdot 3$, which is smaller than the minimal order of the matrix groups G_4 and H_4 of Section 5.4. Indeed, this is the smallest example of a pair of groups satisfying Hypotheses 3.1.2 which we were able to construct.

5.7 Power-maps

In this last section we shall show that for most of the pairs of groups (G, H) which we have constructed in this chapter, G and H have not only identical character tables, but also identical character tables with power-maps.

If $\mathcal{K}$ is a conjugacy class of G and m is an integer, then there is a conjugacy class $\mathcal{K}^{[m]}$ of G which consists of the mth powers of the elements of $\mathcal{K}$. The maps $\mathcal{K} \mapsto \mathcal{K}^{[m]}$ from the set of the conjugacy classes of G into itself are usually called *power-maps*. When the power-maps are added to the character table of a group G (in some way which we shall not formalize here), the resulting object gives considerably more information about G than the character table alone does. In particular, the power-maps determine the order of the elements of any given conjugacy class, and thus sometimes allow one to distinguish between groups which have identical character tables, like for instance D_8 and Q_8 (or, more generally, the two non-isomorphic extraspecial p-groups of a given order). We should say, though, that the prime factors of the orders of the elements are determined by the character table alone, as shown in [13, Theorem (8.21)].

If two groups G and H have identical character tables, via some bijections α and β, the additional condition that G and H also have identical power-maps can be expressed by requiring that

$$(\mathcal{K}^{\alpha})^{[m]} = (\mathcal{K}^{[m]})^{\alpha}$$

for all conjugacy classes $\mathcal{K}$ of G and for all integers m. We shall give instead the following equivalent definition.

Definition 5.7.1 *Let G_1 and G_2 be finite groups. We shall say that G_1 and G_2 have identical character tables with power-maps if there exist bijections*

$$\alpha : G_1 \to G_2$$

and

$$\beta : \mathrm{Irr}(G_1) \to \mathrm{Irr}(G_2),$$

such that for all integers m we have

$$\chi^{\beta}((g^{\alpha})^{m}) = \chi(g^{m}) \quad \textit{for all } g \in G_1 \quad \textit{and for all } \chi \in \mathrm{Irr}(G_1).$$

We observe that when m is composite, the mth power-map $\mathcal{K} \mapsto \mathcal{K}^{[m]}$ of a group G is completely determined by the set of the pth power-maps with p ranging over the prime divisors of m. Furthermore, we can restrict our attention to the primes p which divide the order of G. In fact, the mth power-maps for $(m, |G|) = 1$ (which, incidentally, are the only power-maps which are bijective) are uniquely determined by the character table of G, as the following well-known lemma shows.

Lemma 5.7.2 *Let G_1 and G_2 have identical character tables via the bijections*

$$\alpha : G_1 \to G_2,$$

$$\beta : \mathrm{Irr}(G_1) \to \mathrm{Irr}(G_2),$$

and let m be an integer with $(m, |G|) = 1$. Then we have

$$\chi^{\beta}((g^{\alpha})^{m}) = \chi(g^{m}) \quad \textit{for all } g \in G_1 \quad \textit{and for all } \chi \in \mathrm{Irr}(G_1).$$

Proof Let $n = |G_1|$, and let $\mathbb{E}$ be the splitting field for the polynomial $x^n - 1$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $\mathbb{E} = \mathbb{Q}[\varepsilon]$, where ε is a primitive nth root of 1 in $\mathbb{C}$. From the fact that $(m, |G|) = 1$ it follows that ε^m is also a primitive nth root of 1. Now let $\mathcal{G}$ be the Galois group of $\mathbb{E}$ over $\mathbb{Q}$. Since the cyclotomic polynomials over $\mathbb{Q}$ are irreducible (see for instance [15, Theorem 4.17]), the primitive nth roots of 1 in $\mathbb{C}$ are transitively permuted by $\mathcal{G}$. Hence there exists $\sigma \in \mathcal{G}$ such that $\varepsilon^\sigma = \varepsilon^m$.

Now let $\chi \in \mathrm{Irr}(G_1)$ and $g \in G_1$. If $\mathfrak{X}$ is a complex representation of G_1 affording the character χ, then, according to [13, Lemma (2.15)], $\mathfrak{X}(g)$ is similar to a diagonal matrix

$$\mathrm{diag}(\varepsilon^{i_1}, \dots, \varepsilon^{i_f}),$$

where $f = \chi(1)$ and $i_1, \dots, i_f$ are integers. In particular,

$$\chi(g) = \sum_{j=1}^{f} \varepsilon^{i_j}.$$

It follows that $\mathfrak{X}(g^m) = \mathfrak{X}(g)^m$ is similar to $\mathrm{diag}(\varepsilon^{i_1 m}, \dots, \varepsilon^{i_f m})$, and hence

$$\chi(g^m) = \sum_{j=1}^{f} \varepsilon^{i_j m} = \sum_{j=1}^{f} (\varepsilon^\sigma)^{i_j} = \left(\sum_{j=1}^{f} \varepsilon^{i_j}\right)^\sigma = \chi(g)^\sigma.$$

In a similar way we obtain that

$$\chi^\beta((g^\alpha)^m) = \chi^\beta(g^\alpha)^\sigma.$$

Since $\chi^\beta(g^\alpha) = \chi(g)$, the conclusion now follows. □

A straightforward consequence of Lemma 5.7.2 is the following: if two p-groups of exponent p have identical character tables, then they have identical character tables with power-maps. This fact was employed by Dade in [6], where he gave the first examples of non-isomorphic groups having identical character tables with power-maps, as an answer to a question of Brauer [19, Problem 4]. Let us notice in passing that Dade's proof that his p-groups have identical character tables was a special case of our Theorem 4.3.1.

Now, our Corollary 4.3.2 can be easily adapted in order to handle character tables with power-maps. Let us see only a special case.

Theorem 5.7.3 *Let N_i be an abelian normal subgroup of G_i, for $i = 1, 2$. Let us suppose that following condition holds, in addition to hypotheses (i), (ii), (iii) of Corollary 4.3.2:*

(iv) $\langle g \rangle \cap N_i = 1$ *for all* $g \in G_i \setminus N_i$, *for* $i = 1, 2$.

Then G_1 and G_2 have identical character tables with power-maps.

Proof Let us construct the maps α and β according to the proof of Corollary 4.3.2. Then we have

$$\chi^{\beta}(g^{\alpha}) = \chi(g) \text{ for all } g \in G_1 \text{ and for all } \chi \in \mathrm{Irr}(G_1).$$

Let us fix an integer m. Although it is not necessarily true that $(g^{\alpha})^m = (g^m)^{\alpha}$ for all $g \in G_1$ (which would conclude the proof), we do have that

$$(g^{\hat{\alpha}})^m = (g^m)^{\hat{\alpha}} \text{ for all } g \in N_1,$$

and that

$$((gN_1)^{\bar{\alpha}})^m = (g^m N_1)^{\bar{\alpha}} \text{ for all } g \in G_1,$$

because $\hat{\alpha}$ and $\bar{\alpha}$ are group isomorphisms.

As a first consequence, the assertion

$$\chi^{\beta}((g^{\alpha})^m) = \chi(g^m) \text{ for all } \chi \in \mathrm{Irr}(G_1),$$

is certainly true for $g \in N_1$. Furthermore, it is also true for those $g \in G_1 \setminus N_1$ such that $g^m \in G_1 \setminus N_1$. In fact, this implies that $(g^{\alpha})^m \in G_2 \setminus N_2$, because α is a group isomorphism; hence

$$\chi^{\beta}((g^{\alpha})^m) = 0 = \chi(g^m) \text{ for all } \chi \in \mathrm{Irr}(G_1) \setminus \mathrm{Irr}(G_1/N_1).$$

On the other hand, if $\chi \in \mathrm{Irr}(G_1/N_1)$ we have

$$\begin{aligned}
\chi^{\beta}((g^{\alpha})^m) &= \chi^{\bar{\beta}}((g^{\alpha})^m N_2) \\
&= \chi^{\bar{\beta}}((((gN_1)^{\bar{\alpha}})^m) \\
&= \chi^{\bar{\beta}}((g^m N_1)^{\bar{\alpha}}) \\
&= \chi(g^m N_1) \\
&= \chi(g^m).
\end{aligned}$$

Now we are left with the case of an element g of $G_1 \setminus N_1$ such that $g^m \in N_1$. In this case we have $(g^\alpha)^m \in N_2$, again because α is a group isomorphism. According to hypothesis (iv), we have $g^m = 1$ and $(g^\alpha)^m = 1$. Consequently, we have

$$\chi^\beta((g^\alpha)^m) = \chi^\beta(1) = \chi(1) = \chi(g^m).$$

This concludes the proof. □

Now let us assume the hypotheses $(1), \ldots, (6)$ of Section 5.2, and let us assume in addition that the groups D_1 and D_2 have exponent p; in particular, the prime p must be odd. Let us define the groups

$$G_i = [D_i](W_i \otimes Q_i),$$

for $i = 1, 2$, as we did in Section 5.2. Then the normal Sylow p-subgroup $D_i W_i$ of G_i has exponent p (for $i = 1, 2$); in fact, since $D_i W_i$ has class two and both of D_i and W_i have exponent p, we have

$$(xw)^p = x^p w^p [w, x]^{\binom{p}{2}} = 1$$

for all $x \in D_i$ and $w \in W_i$, according to [10, Kapitel III, Hilfssatz 1.3 b)].

As we proved in Lemma 5.2.1, G_1 and G_2 have identical character tables. Now Theorem 5.7.3 allows us to prove that G_1 and G_2 have identical character tables with power-maps. Indeed, let us define isomorphisms

$$\alpha : G_1/N_1 \to G_2/N_2$$

and

$$\hat{\alpha} : N_1 \to N_2$$

as in the proof of Lemma 5.2.1; as we proved there, hypotheses (i), (ii), and (iii) of Lemma 4.3.2 (and thus of Theorem 5.7.3) are satisfied. Hence it remains to check hypothesis (iv) of Theorem 5.7.3, namely that

$$\langle g \rangle \cap N_i = 1 \quad \text{for all } g \in G_i \setminus N_i, \text{ for } i = 1, 2.$$

This is clearly true for $g \in D_i W_i \setminus N_i$, because $D_i W_i$ has exponent p.

Let $g \in G_i \setminus D_i W_i$. Then the order of g is not a power of p, and we can choose a prime divisor q of the order $|g|$ of g, distinct from p. Hence $h = g^{|g|/q}$ has order q; consequently, h belongs to some Sylow q-subgroup of G_i. On the other hand, Q_i contains a Sylow q-subgroup of G_i. It follows that h is conjugate to some (non-identity) element of Q_i.

Now, every element of Q_i different from the identity element acts fixed-point-freely on D_i by conjugation. Consequently, h acts fixed-pont-freely on D_i by conjugation; in other words,

$$\mathbf{C}_G(h) \cap D_i = 1.$$

Because $\langle g \rangle \leq \mathbf{C}_G(h)$ and $N_i \leq D_i$, we have that

$$\langle g \rangle \cap N_i = 1.$$

Thus hypothesis (iv) of Theorem 5.7.3 is also satisfied.

We conclude that the groups G_1 and G_2 have identical character tables with power-maps, as claimed. In particular, for all the examples (G, H) which we constructed in Sections 5.3 and 5.5, which satisfy the assumption $p \neq 2$, we obtain that G and H have identical character tables with power-maps.

Chapter 6

Nilpotent counterexamples

In Chapter 4 we had a fairly deep insight into the structure of a minimal counterexample (G, H) to Conjecture 3.1.1. In fact, the results of Chapter 4 strongly suggest that the basic pattern for the construction of G and H is essentially that of our examples of Chapter 5. However, behind our investigations of Chapter 4 there was a fundamental assumption, namely that G and H were not nilpotent (Hypotheses 3.1.2).

In this chapter we shall turn our attention to p-groups. Although our knowledge about nilpotent counterexamples to Conjecture 3.1.1 is very limited, we shall be able to construct such a counterexample.

Let us briefly sketch how this example originates. We aim to construct p-groups G_1 and G_2, such that $G_1'' = 1$ and $G_2'' \neq 1$, and G_1, G_2 have identical character tables. Since the character table of a nilpotent group determines its nilpotency class, G_1 and G_2 must have the same class c; necessarily c is at least 4, because $\gamma_4(G_2) \geq G_2'' \neq 1$. Thus, the smallest example we can hope for will have $|\gamma_4(G_1)| = |\gamma_4(G_2)| = p$ and $G_1'' = 1$, $G_2'' = \gamma_4(G_2)$.

Our basic tool for comparing character tables is Corollary 4.3.2. In order to be able to apply that corollary with $N_i = \gamma_4(G_i)$ for $i = 1, 2$, we shall require that

$$G_1/\gamma_4(G_1) \cong G_2/\gamma_4(G_2).$$

But then we may as well regard G_1 and G_2 as factor groups of the same group G; for example, we may take G to be the direct product of G_1 and G_2 with amalgamated factor groups $G_1/\gamma_4(G_1) \cong G_1/\gamma_4(G_2)$ (see [10, Kapitel I, Satz 9.11]).

In the last analysis, we are looking for a p-group G of class 4, in which

$\gamma_4(G)$ is the direct product of two cyclic groups Z_1, Z_2 of order p with $Z_1 = G''$, and such that $(G/Z_1, \gamma_4(G)/Z_1)$ and $(G/Z_2, \gamma_4(G)/Z_2)$ are both Camina pairs (which is hypothesis (iii) of Corollary 4.3.2). Let us put $G_i = G/Z_i$ and $N_i = \gamma_4(G)/Z_i$, for $i = 1, 2$. According to Lemma 4.2.1, the condition that (G_1, N_1) and (G_2, N_2) are Camina pairs is equivalent to

$$N_i \subseteq \lfloor g, G_i \rfloor \quad \text{for all } g \in G_i \setminus N_i, \text{ for } i = 1, 2.$$

This condition can be easily reformulated in terms of G, as follows:

$$(\lfloor g, G \rfloor \cap \gamma_4(G)) \cdot Z_i = \gamma_4(G) \quad \text{for all } g \in G \setminus \gamma_4(G), \text{ for } i = 1, 2.$$

We only observe that because $\gamma_4(G)$ is a central subgroup of G, the set $\lfloor g, G \rfloor \cap \gamma_4(G)$ is a subgroup of $\gamma_4(G)$ (though it may be strictly contained in $[g, G] \cap \gamma_4(G)$); this fact can easily be proved directly, or it can be viewed as an application of Lemma 2.2.4. It will be useful to keep in mind the above condition during the course of the construction.

Now let us proceed with the details of the construction. Let F be the free group on three generators x, y and z. Let us fix a prime $p \geq 5$, and define

$$F = F/\gamma_5(F)F^p,$$

where F^p denotes the (fully invariant) subgroup of F generated by the pth powers of all elements of F. Then F is a nilpotent group of class 4 and exponent p (actually F is the 3-generator free object in the variety of nilpotent groups of class 4 and exponent p).

We know from Theorem 2.6.3 that the factor groups $\gamma_n(F)/\gamma_{n+1}(F)$ for $n = 1, 2, 3, 4$ are elementary abelian, and that a set of representatives for a basis of $\gamma_n(F)/\gamma_{n+1}(F)$ as a vector space over the field $\mathbb{F}_p$ is given by the set C_n of basic commutators of weight n. Explicitly, we have:

$$C_1 = \{x, y, z\},$$

$$C_2 = \{[y, x], [z, x], [z, y]\},$$

$$C_3 = \{[y, x, x], [z, x, x], [y, x, y], [z, x, y], [z, y, y], [y, x, z], [z, x, z], [z, y, z]\},$$

$$
\begin{aligned}
C_4 \;=\; \{ & [y,x,x,x],[z,x,x,x],[y,x,x,y],[z,x,x,y],[y,x,y,y],\\
& [z,x,y,y],[z,y,y,y],[y,x,x,z],[z,x,x,z],[y,x,y,z],\\
& [z,x,y,z],[z,y,y,z],[y,x,z,z],[z,x,z,z],[z,y,z,z],\\
& [[z,x],[y,x]],[[z,y],[y,x]],[[z,y],[z,x]]\}.
\end{aligned}
$$

In the next lemma we shall define a certain factor group H of F, which is a 'first approximation' of the group G that we are looking for.

We recall that in a group of class 4, like F, we have the identity

$$[h,g,k] = [g,h,k]^{-[h,g]} = [g,h,k]^{-1};$$

furthermore, the Witt's identity

$$[g,h,k^g]\,[k,g,h^k]\,[h,k,g^h] = 1$$

assumes the following form:

$$[g,h,k]\,[[g,h],[k,g]]\,[k,g,h]\,[[k,g],[h,k]]\,[h,k,g]\,[[h,k],[g,h]] = 1.$$

Lemma 6.0.4 *For any prime $p \geq 5$, there exists a group $H = \langle x,y,z\rangle$ of order p^{10}, exponent p and class 4, such that the following conditions are satisfied:*

(i) *the subset C_n of H defined below, for $i = 1,2,3,4$, forms a set of representatives of a basis of $\gamma_n(H)/\gamma_{n+1}(H)$, viewed as a vector space over $\mathbb{F}_p$, the field of p elements:*

$$C_1 = \{x,y,z\},$$

$$C_2 = \{[y,x],[z,x]\},$$

$$C_3 = \{[y,x,x],[z,x,x],[y,x,z]\},$$

$$C_4 = \{[y,x,x,z],[[z,x],[y,x]]\};$$

(ii) *the following relations hold*

$$[z,x,x,y] = [y,x,x,z]\,[[z,x],[y,x]]^{-2},$$

$$[z,x,y] = [y,x,z]\,[[z,x],[y,x]]^{-1};$$

(iii) *in addition, the relation $c = 1$ holds for each basic commutator c not appearing in the diagram in (i) or in the relations in (ii).*

Proof We shall proceed in three steps.

Step 1. Let us define the following subgroup of F:

$$\begin{aligned} R_4 &= \langle C_4 \setminus \{[z,x,x,y],[y,x,x,z],[[z,x],[y,x]]\}, \\ &\qquad [z,x,x,y]^{-1}[y,x,x,z]\,[[z,x],[y,x]]^{-2}\rangle. \end{aligned}$$

Since $R_4 \leq \gamma_4(F) \leq \mathbf{Z}(F)$ (actually, it is not too difficult to prove that $\gamma_4(F) = \mathbf{Z}(F)$), we have that C_1, C_2, C_3, and C_4 are sets of representatives of bases of $\gamma_n(F/R_4)/\gamma_{n+1}(F/R_4)$ for $n = 1,2,3,4$ respectively.

Step 2. Let us define the following subgroup of F:

$$\begin{aligned} R_3 &= \langle R_4, [y,x,y],[z,y,y],[z,x,z],[z,y,z], \\ &\qquad [z,x,y]^{-1}[y,x,z]\,[[z,x],[y,x]]^{-1}\rangle. \end{aligned}$$

Then $R_3/R_4 \leq \mathbf{Z}(F/R_4)$. We shall sketch a proof of this fact.

First of all, the basic commutators $[y,x,y],[z,y,y],[z,x,z],[z,y,z]$ are central in F/R_4. In fact, the commutator of any of these elements with x, y or z (for instance $[[z,y,y],x] = [z,y,y,x]$) is a (not necessarily basic) commutator of weight 4 in the letters x, y, z, in which either y or z appears at least twice; by a repeated application of the Witt's identity, this commutator can be written as a product of basic commutators of weight 4 and their inverses (we recall that since we are working in a group of class 4, all commutators of higher weight are trivial) in which, again, either y or z appears at least twice; such basic commutators all belong to R_4, and what we claimed is proved. Since the computations which we outlined are easy, but tedious, let us see just one example:

$$\begin{aligned} [z,y,y,x] &= [[z,y],[y,x]]\,[z,y,x,y] \\ &= [[z,y],[y,x]]\,[y,x,z,y]^{-1}\,[z,x,y,y] \\ &= [[z,y],[y,x]]\,([y,x,y,z]^{-1}\,[[y,x],[z,y]]^{-1})\,[z,x,y,y] \\ &= [[z,y],[y,x]]^2\,[y,x,y,z]^{-1}\,[z,x,y,y] \in R_4. \end{aligned}$$

Now, we observe that $[[z,x],[y,x]]$ is central in F/R_4; furthermore, the product $[z,x,y]^{-1}[y,x,z]$ is also central in F/R_4, because the elements y and

z centralize both of $[z,x,y]$ and $[y,x,z] \pmod{R_4}$, while we have

$$\begin{aligned}[][z,x,y]^{-1}[y,x,z],x] &= [z,x,y,x]^{-1}[y,x,z,x]\\ &= [z,x,x,y]^{-1}[[z,x],[y,x]]^{-1}[y,x,x,z][[y,x],[z,x]]\\ &= [z,x,x,y]^{-1}[y,x,x,z][[z,x],[y,x]]^{-2} \in R_4.\end{aligned}$$

Hence $[z,x,y]^{-1}[y,x,z][[z,x],[y,x]]^{-1}$ is also central in F/R_4.

We conclude that $R_3/R_4 \le \gamma_3(F/R_4) \cap \mathbf{Z}(F/R_4)$. Since we also have $R_3/R_4 \cap \gamma_4(F/R_4) = 1$, it follows that sets of representatives of bases of $\gamma_n(F/R_3)/\gamma_{n+1}(F/R_3)$ for $n = 1,2,3,4$ are given by $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$ respectively.

Step 3. Let us define the following subgroup of F:

$$R_2 = \langle R_3, [z,y]\rangle.$$

Then $R_2/R_3 \le \mathbf{Z}(F/R_3)$. In fact, $[z,y]$ clearly commutes with y and $z \pmod{R_3}$; it commutes with x too, $\pmod{R_3}$, because the Witt's identity

$$[z,y,x^z][x,z,y^x][y,x,z^y] = 1$$

read $\pmod{R_3}$ becomes

$$[z,y,x][x,z,y][[x,z],[y,x]][y,x,z] \equiv 1 \bmod R_3,$$

and thus we get that

$$\begin{aligned}[][z,y,x] &\equiv [y,x,z]^{-1}[[x,z],[y,x]]^{-1}[x,z,y]^{-1}\\ &= [[z,x],[y,x]][y,x,z]^{-1}[z,x,y]\\ &= ([z,x,y]^{-1}[y,x,z][[z,x],[y,x]]^{-1})^{-1} \equiv 1 \bmod R_3.\end{aligned}$$

Hence $R_2/R_3 \le \gamma_2(F/R_3) \cap \mathbf{Z}(F/R_3)$. This fact, together with the fact that $R_2/R_3 \cap \gamma_3(F/R_3) = 1$, implies that sets of representatives of bases of $\gamma_n(F/R_2)/\gamma_{n+1}(F/R_2)$ for $n = 1,2,3,4$ are given by $\mathcal{C}_1 = \mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$ respectively.

Let us define $H = F/R_2$. Then H has exponent p and clearly satisfies the conditions (i), (ii) and (iii). In particular H has order p^{10} and class 4. This completes the proof of the lemma. □

Lemma 6.0.4 implicitly gives a (rather long) presentation of H in terms of generators (namely x, y and z) and relations. It would be easy to prove that a shorter presentation is

$$\begin{aligned} H &= \langle x, y, z \mid x^p = y^p = z^p = 1, \\ &\qquad [z, y] = [y, x, y] = [z, x, z] = [y, x, x, x] = [z, x, x, x] = 1, \\ &\qquad [g_1, g_2, g_3, g_4, g_5] = 1 \text{ for all } g_1, \dots, g_5 \in H \rangle. \end{aligned}$$

We said earlier that the group H should be a 'first approximation' of the group G that we are trying to construct. In fact, it would be possible to show that

$$\lfloor g, H \rfloor \cap \gamma_4(H) \neq 1 \quad \text{for all } g \in H \setminus \gamma_4(H).$$

However, H does not satisfy the stronger condition which we required, namely

$$(\lfloor g, H \rfloor \cap \gamma_4(H)) \cdot H'' = \gamma_4(H) \quad \text{for all } g \in H \setminus \gamma_4(H),$$

because we have for instance

$$\lfloor [y, x], H \rfloor \cap \gamma_4(H) = \langle [[z, x], [y, x]] \rangle = H''.$$

We shall quickly remedy this problem. The assignments

$$\begin{cases} x^u &= x[z, x, x]^{-1} \\ y^u &= y \\ z^u &= z \end{cases} \qquad \begin{cases} x^v &= x[y, x, x]^{-1} \\ y^v &= y \\ z^v &= z \end{cases}$$

clearly define two mutually commuting automorphisms u, v of the group F.

Actually, they also define automorphisms u, v of its factor group $H = F/R_2$. In fact, u and v fix each element of $\gamma_3(F)$, and of course they fix $[z, y]$. Since $R_2 = (R_2 \cap \gamma_3(F)) \cdot \langle [z, y] \rangle$, it follows that u, v centralize R_2. Hence they lift to automorphisms u, v of $H = F/R_2$.

Since the automorphisms u and v of H have order p (because they also have order p as automorphisms of F) the group $K = \langle u, v \rangle$ is an elementary abelian group of automorphisms of H, of order p^2.

Let us consider the semidirect product $G = [H]K$. It has order p^{12} and class 4. Since we assumed that $p \geq 5$, the p-group G is regular (see for example [10, Kapitel III, Satz 10.2 a)]); therefore G has exponent p, because H and K have exponent p.

The following equalities which hold in G will be useful in computations:

$$\begin{array}{rclrcl} [y,x,u] &=& [z,x,x,y], & [y,x,v] &=& 1, \\ [z,x,u] &=& 1, & [z,x,v] &=& [y,x,x,z]. \end{array}$$

Let us define two central subgroups of G, namely

$$Z_1 = \langle [[z,x],[y,x]] \rangle = G'',$$

$$Z_2 = \langle [y,x,x,z][[z,x],[y,x]]^s \rangle,$$

where s is an integer such that $s \not\equiv 0, -1, -2 \pmod p$ (for instance $s = 1$). The factor groups $G_1 = G/Z_1$ and $G_2 = G/Z_2$ are groups of order p^{11}.

Now we state our final result.

Theorem 6.0.5 *The groups G_1 and G_2 have identical character tables, but G_1 is metabelian, while G_2 has derived length three.*

Proof It is clear that the derived lengths of G_1 and G_2 are 2 and 3 respectively.

In order to prove that G_1 and G_2 have identical character tables, we shall appeal to Corollary 4.3.2, with

$$N_1 = \gamma_4(G_1) = \gamma_4(G)/Z_1,$$

$$N_2 = \gamma_4(G_2) = \gamma_4(G)/Z_2,$$

$$\alpha : G/\gamma_4(G) \to G/\gamma_4(G)$$

the identity map and

$$\bar{\alpha} : N_1 \to N_2$$

any group isomorphism, which is necessarily a $G/\gamma_4(G)$-module isomorphism, the central subgroups N_1 of G_1 and N_2 of G_2 beeing regarded as trivial $G/\gamma_4(G)$-modules by conjugation. Then the conditions (i) and (ii) of the corollary are satisfied.

It remains to verify condition (iii), namely that (G_1, N_1) and (G_2, N_2) are Camina pairs, or equivalently that

$$N_i \subseteq [g, G_i] \quad \text{for all } g \in G_i \setminus N_i, \text{ for } i = 1, 2.$$

We shall distinguish two cases.

Case 1: Either $g \in \gamma_3(G_i) \setminus \gamma_4(G_i)$ or $g \in G_i \setminus \langle \gamma_2(G_i), u, v\rangle$.

Let us regard the elementary abelian groups $V_1 = \gamma_3(G)/\gamma_4(G)$ and $V_2 = G/\langle \gamma_2(G), u, v\rangle$ as vector spaces of dimension 3 over $\mathbb{F}_p$. Then the ordered sets $\{[y,x,x],[z,x,x],[y,x,z]\}$ and $\{x,y,z\}$ are sets of representatives of bases of V_1 and V_2 respectively. Let us fix also the bases $\{[y,x,x,z]\}$ of $\gamma_4(G)/Z_1$ and $\{[[z,x],[y,x]]\}$ of $\gamma_4(G)/Z_2$. We have

$$[\gamma_3(G), G] \subseteq \gamma_4(G),$$

$$[\gamma_3(G), \langle \gamma_2(G), u, v\rangle] = 1$$

$$\text{and} \quad [\gamma_4(G), G] = 1;$$

according to Lemma 2.2.1, commutation in G gives rise in a natural way to a $\mathbb{Z}$-bilinear map (actually $\mathbb{F}_p$-bilinear, because V_1, V_2 are vector spaces over $\mathbb{F}_p$)

$$\gamma : V_1 \times V_2 \to \gamma_4(G).$$

Let $\pi_i : \gamma_4(G) \to \gamma_4(G)/Z_i$ be the natural homomorphisms for $i = 1, 2$. We shall show that the composite maps

$$\gamma\pi_i : V_1 \times V_2 \to \gamma_4(G)/Z_i$$

are non-degenerate.

We compute:

$$[[y,x,x]^a [z,x,x]^b [y,x,z]^c, x^{\bar{a}} y^{\bar{b}} z^{\bar{c}}] = [y,x,x,z]^{a\bar{c}+b\bar{b}+c\bar{a}} [[z,x],[y,x]]^{-2b\bar{b}-c\bar{a}}.$$

Thus the map $\gamma\pi_1$ has matrix

$$\begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}$$

with respect to the given bases of V_1, V_2 and $\gamma_4(G)/Z_1$, and hence $\gamma\pi_1$ is non-degenerate. On the other hand, the map $\gamma\pi_2$ has matrix

$$\begin{bmatrix} & & -s \\ & -2-s & \\ -1-s & & \end{bmatrix}$$

with respect to the given bases of V_1, V_2 and $\gamma_4(G)/Z_2$; hence $\gamma\pi_2$ is non-degenerate, because $s \not\equiv 0, -1, -2 \pmod p$. The non-degeneracy of $\gamma\pi_1$ and $\gamma\pi_2$ means that

$$[g, G_i] \supseteq N_i, \quad \text{for all } g \in \gamma_3(G_i) \setminus \gamma_4(G_i), \text{ for } i = 1, 2.$$

and that

$$[\gamma_3(G_i), g] \supseteq N_i, \quad \text{for all } g \in G_i \setminus \langle \gamma_2(G_i), u, v\rangle, \text{ for } i = 1, 2.$$

It follows in particular that

$$[g, G_i] \supseteq N_i \quad \text{for all } g \in (\gamma_3(G_i) \setminus \gamma_4(G_i)) \cup (G_i \setminus \langle \gamma_2(G_i), u, v\rangle), \text{ for } i = 1, 2.$$

Case 2: $g \in \langle \gamma_2(G_i), u, v\rangle \setminus \gamma_3(G_i)$.

Let us regard the elementary abelian group

$$W = g \in \langle \gamma_2(G), u, v\rangle / \gamma_3(G)$$

as a vector space of dimension 4 over $\mathbf{F}_p$. The ordered set $\{u, v, [y, x], [z, x]\}$ is then a set of representatives of a basis of W.

We have

$$\langle \gamma_2(G), u, v\rangle' \leq \gamma_4(G),$$
$$\text{and} \quad [\langle \gamma_2(G), u, v\rangle, \gamma_3(G)] = 1;$$

according to Lemma 2.2.1, commutation in G gives rise to an $\mathbf{F}_p$-bilinear map

$$\delta : W \times W \to \gamma_4(G).$$

We shall show that the maps

$$\delta\pi_i : W \times W \to \gamma_4(G)/Z_i,$$

for $i = 1, 2$, are non-degenerate.

We compute

$$\begin{aligned}
&[u^a v^b [y, x]^c [z, x]^d, u^\alpha v^\beta [y, x]^\gamma [z, x]^\delta] = \\
&= [y, x, u]^{c\alpha - a\gamma} [z, x, v]^{d\beta - b\delta} [[z, x], [y, x]]^{d\gamma - c\delta} \\
&= [y, x, x, z]^{(c\alpha - a\gamma) + (d\beta - b\delta)} [[z, x], [y, x]]^{(d\gamma - c\delta) - 2(c\alpha - a\gamma)}.
\end{aligned}$$

Thus the map $\delta\pi_1$ has matrix

$$\begin{vmatrix} & & -1 & \\ & & & -1 \\ 1 & & & \\ & 1 & & \end{vmatrix}$$

with respect to the given bases of W and $\gamma_4(g)/Z_1$; it follows that the map $\delta\pi_1$ is non-degenerate. On the other hand, the map $\delta\pi_2$ has matrix

$$\begin{vmatrix} & & s+2 & \\ & & & s \\ -s-2 & & & -1 \\ & -s & 1 & \end{vmatrix}$$

with respect to the given bases of W and $\gamma_4(G)/Z_2$. This matrix has determinant $s^2(s+2)^2 \not\equiv 0 \pmod{p}$, because $s \not\equiv 0, -2 \pmod{p}$. Hence $\delta\pi_2$ is non-degenerate.

The non-degeneracy of $\delta\pi_1$, $\delta\pi_2$ means that

$$[g, \langle\gamma_2(G_i), u, v\rangle] \supseteq N_i \quad \text{for all } g \in \langle\gamma_2(G_i), u, v\rangle \setminus \gamma_3(G_i), \text{ for } i = 1, 2.$$

In particular, it follows that

$$[g, G_i] \supseteq N_i \quad \text{for all } g \in \langle\gamma_2(G_i), u, v\rangle \setminus \gamma_3(G_i), \text{ for } i = 1, 2.$$

We have proved that

$$[g, G_i] \supseteq N_i, \quad \text{for all } g \in G_i \setminus N_i, \text{ for } i = 1, 2;$$

hence all hypotheses of Corollary 4.3.2 have been verified, and its conclusion that G_1 and G_2 have identical character tables now follows. $\square$

Chapter 7

Wreath products

In this last chapter we shall study the character tables of wreath products. The theory of the characters of wreath products has been known for a long time. However, as far as we know, nobody has tried to isolate the exact ingredients on which the character table of a wreath product $G \wr A$ depends. We shall show that such ingredients are the character table of G and the permutation group A: these determine the character table of $G \wr A$ uniquely. What results is a powerful tool for increasing the derived length of a group, while keeping its character table under control. We shall employ it in Section 7.4 to construct pairs (G, H) of groups with identical character tables and derived lengths n and $n + 1$, for any given natural number $n \geq 2$.

It is a pleasure to thank Prof. I. M. Isaacs for the conversations on this subject which we had during his stay at the University of Warwick in June 1991.

7.1 Characters of wreath products

In this section and in the next one we shall collect some facts about irreducible characters, and respectively conjugacy classes of wreath products.

Definition 7.1.1 *Let G be a group and let A be a (not necessarily transitive) permutation group on a finite set Ω. Then the wreath product $\Gamma = G \wr A$ is defined as the semidirect product $[B]A$, where the so-called base-group $B = \prod_{\omega \in \Omega} G_\omega$ is the direct product of $|\Omega| = k$ copies of G and the action of A on*

B is given by

$$(g_1, \ldots, g_k)^a = (g_{1^{a^{-1}}}, \ldots, g_{k^{a^{-1}}})$$

for all $(g_1, \ldots, g_k) \in B$ and for all $a \in A$.

We shall use the notation $(g_1, \ldots, g_k)$, assuming that the set Ω is identified with the set $\{1, \ldots, k\}$.

Let us recall that the irreducible characters of the base group $B = G_1 \times \cdots \times G_k$, or more generally of any direct product $G_1 \times \cdots \times G_k$, where $G_1, \ldots, G_k$ are arbitrary groups, are exactly the characters

$$\theta = \theta_1 \times \cdots \times \theta_k$$

with $\theta_i \in \mathrm{Irr}(G_i)$ for $i = 1, \ldots, k$, where by definition

$$\theta(g_1, \ldots, g_k) = \theta_1(g_1) \cdots \theta_k(g_k) \quad \text{for all } (g_1, \ldots, g_k) \in G_1 \times \cdots \times G_k.$$

Furthermore, each θ_i is uniquely determined by θ, as the unique irreducible constituent of the restriction θ_{G_i}.

The action of A on B induces the following action of A on $\mathrm{Irr}(B)$:

$$(\theta_1 \times \cdots \times \theta_k)^a = \theta_{1^{a^{-1}}} \times \cdots \times \theta_{k^{a^{-1}}}.$$

In fact, we have

$$\begin{aligned}
(\theta_1 \times \cdots \times \theta_k)^a(g_1, \ldots, g_k) &= (\theta_1 \times \cdots \times \theta_k)((g_1, \ldots, g_k)^{a^{-1}}) \\
&= (\theta_1 \times \cdots \times \theta_k)(g_{1^a}, \ldots, g_{k^a}) \\
&= \theta_1(g_{1^a}) \cdots \theta_k(g_{k^a}) \\
&= \theta_{1^{a^{-1}}}(g_1) \cdots \theta_{k^{a^{-1}}}(g_k) \\
&= (\theta_{1^{a^{-1}}} \times \cdots \times \theta_{k^{a^{-1}}})(g_1, \ldots, g_k).
\end{aligned}$$

We shall employ the technique of tensor induction, an account of which was given in Section 2.5. A well-known result on characters of wreath products asserts that any irreducible character θ of the base group B which is invariant in $\Gamma = [B]A$ is extendible to a character of Γ (a generalization of this fact is given in [14, Theorem 5.2]). In lemma 7.1.3 we shall compute explicitly an extension $\eta \in \mathrm{Irr}(\Gamma)$ of θ, but first let us do this in the special case in which A is cyclic and acts regularly on Ω. This special case is easier to prove and illustrates very well how tensor induction comes into play.

Lemma 7.1.2 *Let G be a group and let C be a cyclic group of order k. Let us form the regular wreath product $\Gamma = G \wr C$ (that is to say, with respect to the regular permutation representation of C). Let $\theta = \theta_1 \times \cdots \times \theta_k$ be an irreducible character of the base group B and assume that θ is invariant in Γ. Then θ is extendible to Γ and an extension is given by $\psi^{\otimes\Gamma}$, where ψ is the irreducible character of B defined by*

$$\psi = \theta_1 \times 1_G \times \cdots \times 1_G.$$

Furthermore, if c is any generator of C, we have

$$\psi^{\otimes\Gamma}(c) = \theta_1(1) = \theta(1)^{1/k}.$$

Proof The base group B is a direct product of p copies of G. We may fix a generator c of C and assume that the action of C on B by conjugation is given by

$$(g_1, \ldots, g_k)^c = (g_k, g_1, \ldots, g_{k-1}) \text{ for all } (g_1, \ldots, g_k) \in B.$$

If θ is any irreducible character of B, then θ can be written in a unique way as $\theta_1 \times \cdots \times \theta_k$, where $\theta_1, \ldots, \theta_k$ are irreducible characters of G. The action of C on B induces the following action of C on $\mathrm{Irr}(B)$

$$(\theta_1 \times \cdots \times \theta_k)^c = \theta_k \times \theta_1 \times \cdots \times \theta_{k-1}.$$

Let us assume now that $\theta = \theta_1 \times \cdots \times \theta_k$ is invariant in Γ; hence $\theta^c = \theta$. It follows that $\theta_1 = \theta_2 = \cdots = \theta_k$, and in particular that $\theta_1, \ldots, \theta_k$ have all the same degree, namely $\theta_1(1) = \theta(1)^{1/k}$.

Let us define $\psi = \theta_1 \times 1_G \times \cdots \times 1_G$ and let us show that $(\psi^{\otimes\Gamma})_B = \theta$. For $(g_1, \ldots, g_k) \in B$ we have

$$\begin{aligned}
\psi^{\otimes\Gamma}(g_1, \ldots, g_k) &= \prod_{i=0}^{k-1} \psi(c^i(g_1, \ldots, g_k)c^{-i}) \\
&= \prod_{i=0}^{k-1} \psi(g_{i+1}, \ldots, g_k, g_1, \ldots, g_i) \\
&= \prod_{i=0}^{k-1} \theta_1(g_{i+1}) \\
&= \prod_{i=0}^{k-1} \theta_{i+1}(g_{i+1}) \\
&= \theta(g_1, \ldots, g_k).
\end{aligned}$$

where we have employed the formula for $\psi^{\otimes\Gamma}$ given by Lemma 2.5.2. Hence $\psi^{\otimes\Gamma}$ extends θ.

To prove the last assertion, let c^i be a generator of C. Since $C = \langle c^i \rangle$ acts transitively on the transversal $T = C$ of B in Γ via $\cdot$, we have

$$\psi^{\otimes\Gamma}(c^i) = \psi(c^{ik}) = \psi(1) = \theta_1(1).$$

The proof is complete. $\square$

The general form of Lemma 7.1.2 is the following.

Lemma 7.1.3 *Let G be a group and let A be a permutation group on Ω, with $|\Omega| = k$. Let us form the wreath product $\Gamma = G \wr A$. Let $\theta = \theta_1 \times \cdots \times \theta_k$ be an irreducible character of the base group B, and let us assume that θ is invariant in Γ. Then θ has an extension $\eta \in \mathrm{Irr}(\Gamma)$, and the value of η on the generic element $g = (g_1, \ldots, g_k)a$ of Γ is given by the formula*

$$\eta(g) \;=\; \prod_{i=1}^{l} \theta_{\omega_i}(g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{n(i)-1}}}), \tag{7.1}$$

where $\omega_1, \ldots, \omega_l$ are representatives for the orbits of $\langle a \rangle$ on Ω and $n(i)$ is the length of the $\langle a \rangle$-orbit containing ω_i.

Proof Let us decompose Ω into A-orbits

$$\Omega = \Omega_1 \dot\cup \cdots \dot\cup \Omega_v.$$

We may identify Ω with the set $\{1, \ldots, k\}$ in such a way that

$$\begin{aligned}
\Omega_1 &= \{k_1 = 1, \ldots, k_2 - 1\} \\
\Omega_2 &= \{k_2, \ldots, k_3 - 1\} \\
&\vdots \\
\Omega_v &= \{k_v, \ldots, k\}.
\end{aligned}$$

Then $k_1, \ldots, k_v$ is a set of representatives for the orbits of A on Ω. Let S_i denote the stabilizer of k_i in A, for $i = 1, \ldots, v$.

By assumption θ is invariant in Γ. This is equivalent to

$$(\theta_1 \times \cdots \times \theta_k)^a = \theta_1 \times \cdots \times \theta_k \quad \text{for all } a \in A,$$

that is to say,

$$\theta_{1^{a^{-1}}} \times \cdots \times \theta_{k^{a^{-1}}} = \theta_1 \times \cdots \times \theta_k \quad \text{for all } a \in A.$$

Since the components θ_j are uniquely determined by θ, we have

$$\theta_{j^a} = \theta_j \quad \text{for all } j = 1, \ldots, k \quad \text{and for all } a \in A.$$

Now let us define the following characters of B, for $i = 1, \ldots, v$:

$$\hat{\theta}_i = 1_{G_1} \times \cdots \times 1_{G_{k_i - 1}} \times \theta_{k_i} \times \cdots \times \theta_{k_{i+1}-1} \times 1_{G_{k_{i+1}}} \times \cdots \times 1_{G_k}.$$

Each $\hat{\theta}_i$ is irreducible and is clearly invariant in Γ. We shall find an extension $\eta_i \in \mathrm{Irr}(\Gamma)$ of $\hat{\theta}_i$ for each $i = 1, \ldots, v$. Since $\theta = \hat{\theta}_1 \cdots \hat{\theta}_v$, the character $\eta = \eta_1 \cdots \eta_v$ of Γ will be an extension of θ.

Let us fix an index i. The stabilizer S_i of k_i in A centralizes G_{k_i}; consequently, the subgroup BS_i of Γ decomposes into a direct product

$$BS_i = G_{k_i} \times \left(\left(\prod_{\substack{1 \leq j \leq k \\ j \neq k_i}} G_j \right) S_i \right).$$

Thus there exists a unique extension $\psi_i \in \mathrm{Irr}(BS_i)$ of the irreducible character θ_{k_i} of G_{k_i}, such that

$$\left(\prod_{\substack{1 \leq j \leq k \\ j \neq k_i}} G_j \right) S_i \leq \ker \psi_i.$$

The value of ψ_i on a generic element $g = (g_1, \ldots, g_k)a$ of BS_i is given by

$$\psi_i(g) = \theta_{k_i}(g_{k_i}).$$

Now we claim that the tensor induced character $\eta_i = \psi_i^{\otimes \Gamma}$ is an extension of $\hat{\theta}_i$. In order to prove the claim, let R_i be a set of representatives for the right cosets of S_i in A; hence R_i also represents the right cosets of BS_i in Γ. The action of Γ by right translation on the set of right cosets of BS_i in Γ induces an action of Γ on R_i, namely $r \cdot g$ for $r \in R_i$ and $g \in \Gamma$ is the unique element of R_i such that

$$(BS_i r)g = BS_i(r \cdot g).$$

Let us fix an element $g = (g_1, \ldots, g_k)a$ of Γ. Let R_{i0} be a set of representatives of the orbits of $\langle g \rangle$ on R via $\cdot$, and for $r \in R_{i0}$ let $n(r)$ denote the length of the $\langle g \rangle$-orbit $r^{\langle g \rangle}$. According to Lemma 2.5.2, we have

$$\psi_i^{\otimes \Gamma}(g) = \prod_{r \in R_{i0}} \psi_i(r g^{n(r)} r^{-1}).$$

We compute:

$$\begin{aligned}
g^{n(r)} &= ((g_1, \ldots, g_k)a)^{n(r)} \\
&= (g_1, \ldots, g_k)(g_1, \ldots, g_k)^{a^{-1}} \cdots (g_1, \ldots, g_k)^{a^{-(n(r)-1)}} a^{n(r)} \\
&= (g_1, \ldots, g_k)(g_{1^a}, \ldots, g_{k^a}) \cdots (g_{1^{a^{n(r)-1}}}, \ldots, g_{k^{a^{n(r)-1}}}) a^{n(r)} \\
&= (g_1 g_{1^a} \cdots g_{1^{a^{n(r)-1}}}, \ldots, g_k g_{k^a} \cdots g_{k^{a^{n(r)-1}}}) a^{n(r)}.
\end{aligned}$$

It follows that

$$r g^{n(r)} r^{-1} = (g_{1^r} g_{1^{ra}} \cdots g_{1^{ra^{n(r)-1}}}, \ldots, g_{k^r} g_{k^{ra}} \cdots g_{k^{ra^{n(r)-1}}})(r a^{n(r)} r^{-1}).$$

According to the definition of $n(r)$, we have $r \cdot g^{n(r)} = r$, which means $BS_i r g^{n(r)} = BS_i r$, or in other words $r g^{n(r)} r^{-1} \in BS_i$. Hence

$$r a^{n(r)} r^{-1} \in A \cap BS_i = S_i.$$

Therefore we have

$$\psi_i(r g^{n(r)} r^{-1}) = \theta_{k_i}(g_{k_i^r} g_{k_i^{ra}} \cdots g_{k_i^{ra^{n(r)-1}}})$$

for $r \in R_{i0}$; it follows that

$$\psi_i^{\otimes \Gamma}(g) = \prod_{r \in R_{i0}} \theta_{k_i}(g_{k_i^r} g_{k_i^{ra}} \cdots g_{k_i^{ra^{n(r)-1}}}).$$

We said earlier that $\theta_{j^a} = \theta_j$ for all $j = 1, \ldots, k$ and for all $a \in A$; hence we may also write

$$\psi_i^{\otimes \Gamma}(g) = \prod_{r \in R_{i0}} \theta_{k_i^r}(g_{k_i^r} g_{k_i^{ra}} \cdots g_{k_i^{ra^{n(r)-1}}}). \tag{7.2}$$

We shall see that this result can be formulated differently. Let $g = (g_1, \ldots, g_k)a \in \Gamma$. Then g acts on R_i via $\cdot$ as a does; in fact, we have

$$(BS_i r)g = (BS_i (g_1, \ldots, g_k)^{r^{-1}}) ra = (BS_i r)a,$$

and thus $r \cdot g = r \cdot a$ for all $r \in R_i$. Since R_{i0} is a set of representatives of the orbits of $\langle g \rangle$ on R_i via $\cdot$, it is also a set of representatives of the orbits of $\langle a \rangle$ on R_i via $\cdot$. Now the action of A on R_i via $\cdot$ is similar to the given permutation representation of A on Ω_i, because R_i is a right transversal for the stabilizer S_i of k_i in A. More precisely, the map

$$\begin{array}{ccc} R_i & \to & \Omega_i \\ r & \mapsto & k_i^r \end{array}$$

is a bijection and satisfies

$$k_i^{r \cdot a} = (k_i^r)^a.$$

Therefore, the elements k_i^r for $r \in R_{i0}$ are distinct, they form a set of representatives for the orbits of $\langle a \rangle$ on Ω_i, and $n(r)$ is the length of the $\langle a \rangle$-orbit containing k_i^r. Thus formula 7.2 can be rewritten as follows:

$$\psi_i^{\otimes\Gamma}(g) = \prod_{j=1}^{l_i} \theta_{\omega_{ij}}(g_{\omega_{ij}} g_{\omega_{ij}^a} \cdots g_{\omega_{ij}^{a^{n(i,j)-1}}}), \tag{7.3}$$

where $\omega_{i1}, \ldots, \omega_{il_i}$ are representatives for the orbits of $\langle a \rangle$ on Ω_i, and $n(i,j)$ is the length of the $\langle a \rangle$-orbit which contains ω_{ij}. In the particular case in which $g = (g_1, \ldots, g_k)a \in B$, we have $a = 1$, and hence all orbits of $\langle a \rangle$ on Ω_i have length one. Thus we get

$$\psi_i^{\otimes\Gamma}(g) = \prod_{j=k_i}^{k_{i+1}-1} \theta_j(g_j) = \hat{\theta}_i(g).$$

Hence $\eta_i = \psi_i^{\otimes\Gamma}$ is an extension of $\hat{\theta}_i$, as we claimed.

Let us define

$$\eta = \eta_1 \cdots \eta_v.$$

Then η extends θ, in fact

$$\eta_B = (\eta_1)_B \cdots (\eta_v)_B = \hat{\theta}_1 \cdots \hat{\theta}_v = \theta.$$

Moreover, the value of η on a generic element $g = (g_1, \ldots, g_k)a$ of Γ is given by the formula

$$\eta(g) = \eta_1(g) \cdots \eta_v(g) = \prod_{i=1}^{v} \prod_{j=1}^{l_i} \theta_{\omega_{ij}}(g_{\omega_{ij}} g_{\omega_{ij}^a} \cdots g_{\omega_{ij}^{a^{n(i,j)-1}}}),$$

where $\omega_{i1}, \ldots, \omega_{il_i}$ are representatives for the orbits of $\langle a \rangle$ on Ω_i, and $n(i, j)$ is the length of the $\langle a \rangle$-orbit containing ω_{ij}.

The above formula can clearly be written as

$$\eta(g) = \prod_{i=1}^{l} \theta_{\omega_i}(g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{n(i)-1}}}),$$

where $\omega_1, \ldots, \omega_l$ are representatives for the orbits of $\langle a \rangle$ on Ω and $n(i)$ is the length of the $\langle a \rangle$-orbit containing ω_i. The proof is complete. □

We observe that the formula for the extension η of θ given in Lemma 7.1.3 does not contain any trace of the orbits of A on Ω, which instead are fundamental in the proof of the lemma. In order to compute $\eta(g)$ for $g = (g_1, \ldots, g_k)a \in \Gamma$, we only need to know the action of $\langle a \rangle$ on B. Since the subgroup $B\langle a \rangle$ of Γ is naturally isomorphic to $G \wr \langle a \rangle$, where $\langle a \rangle$ is regarded as a permutation group on Ω as a subgroup of A, it follows that in order to compute $\eta(g)$ we may as well apply the lemma with $A = \langle a \rangle$. This leads to a sort of 'canonicity' of the extension η of θ, as stated in the next corollary.

Corollary 7.1.4 *Let A be a permutation group on a set Ω and let A_1 be a subgroup of A; hence A_1 is also a permutation group on Ω. Let G be a group and let us form the wreath product $\Gamma = G \wr A$. Let Γ_1 be the subgroup of Γ generated by the base group B of Γ and A_1; hence Γ_1 is naturally isomorphic to $G \wr A_1$. Let $\theta \in \mathrm{Irr}(B)$ be invariant in Γ, and let η, η_1 be the extensions of θ to Γ and Γ_1 respectively, constructed as in Lemma 7.1.3. Then $\eta_{\Gamma_1} = \eta_1$.*

Proof The conclusion follows easily from the discussion which precedes the corollary. □

7.2 Conjugacy classes of wreath products

Now that we have an explicit way of extending invariant characters of the base group of a wreath product $\Gamma = G \wr A$, let us turn our attention to the conjugacy classes of Γ. We shall partition Γ into subsets which are not conjugacy classes, though each of them is contained in some conjugacy class of Γ. The result of Lemma 7.1.2 would suggest to associate a subset

$\mathcal{K}_{a,(\mathcal{L}_1,\dots,\mathcal{L}_l)}$ of Γ to each $a \in A$ and each l-ple $(\mathcal{L}_1, \dots, \mathcal{L}_l)$ of conjugacy classes of G, where l is the number of orbits of $\langle a \rangle$ on Ω, according to the following definition:

$$\begin{aligned} \mathcal{K}_{a,(\mathcal{L}_1,\dots,\mathcal{L}_l)} &= \{(g_1, \dots, g_k)a \in \Gamma \mid \\ &\quad g_{\omega_1} g_{\omega_1^a} \cdots g_{\omega_1^{a^{n(1)-1}}} \in \mathcal{L}_1, \\ &\quad \vdots \\ &\quad g_{\omega_l} g_{\omega_l^a} \cdots g_{\omega_l^{a^{n(l)-1}}} \in \mathcal{L}_l\}, \end{aligned}$$

where $\omega_1, \dots, \omega_l$ are representatives for the orbits of $\langle a \rangle$ on Ω and $n(i)$ is the length of the $\langle a \rangle$-orbit containing ω_i (it can be easily shown that this definition is independent of the choice of representatives $\omega_1, \dots, \omega_l$). In fact, if θ is an irreducible character of the base group B which is invariant in $B\langle a \rangle$, then the extension η of θ given by the formula of Lemma 7.1.2 is clearly constant on $\mathcal{K}_{a,(\mathcal{L}_1,\dots,\mathcal{L}_l)}$.

We shall define the subsets $\mathcal{K}_{a,(\mathcal{L}_1,\dots,\mathcal{L}_l)}$ of Γ using a slightly different notation which will allow us to describe more easily how A permutes them by conjugation.

Let $\mathcal{M}$ denote the set of maps $m : \Omega \to \mathrm{cl}(G)$, where $\mathrm{cl}(G)$ is the set of conjugacy classes of G. The action of A on Ω induces an action of A on $\mathcal{M}$, where m^a for $m \in \mathcal{M}$ and $a \in A$ is the map such that

$$(m^a)(\omega) = m(\omega^{a^{-1}}) \text{ for all } \omega \in \Omega.$$

Let us define $\mathcal{M}_a$ for $a \in A$ as the subset of the elements of $\mathcal{M}$ fixed by a; in other words $\mathcal{M}_a$ is the set of maps $m : \Omega \to \mathrm{cl}(G)$ which are constant on the orbits of $\langle a \rangle$ on Ω. We observe that $(\mathcal{M}_a)^b$ for $a, b \in A$ is the set of the elements of $\mathcal{M}$ fixed by a^b; hence

$$(\mathcal{M}_a)^b = \mathcal{M}_{a^b}.$$

Definition 7.2.1 *Let $a \in A$ and $m \in \mathcal{M}_a$. Let us choose representatives $\omega_1, \dots, \omega_l$ for the orbits of $\langle a \rangle$ on Ω and let $n(i)$ be the length of the $\langle a \rangle$-orbit containing ω_i. Let us define*

$$\begin{aligned} \mathcal{K}_{a,m} &= \{(g_1, \dots, g_k)a \in \Gamma \mid \\ &\quad g_{\omega_1} g_{\omega_1^a} \cdots g_{\omega_1^{a^{n(1)-1}}} \in m(\omega_1), \\ &\quad \vdots \\ &\quad g_{\omega_l} g_{\omega_l^a} \cdots g_{\omega_l^{a^{n(l)-1}}} \in m(\omega_l)\}. \end{aligned}$$

This definition does not depend on the choice of the representatives $\omega_1, \dots, \omega_l$ of the orbits of $\langle a \rangle$ on Ω. In fact, let us replace for example ω_i with a different representative $\tilde{\omega}_i$ of its $\langle a \rangle$-orbit, hence $\tilde{\omega}_i = \omega_i^{a^m}$ for some integer m with $1 \leq m \leq n(i) - 1$. The element

$$\begin{aligned} g_{\tilde{\omega}_i} g_{\tilde{\omega}_i^a} \cdots g_{\tilde{\omega}_i^{a^{n(i)-1}}} &= g_{\omega_i^{a^m}} g_{\omega_i^{a^{m+1}}} \cdots g_{\omega_i^{a^{m+n(i)-1}}} \\ &= (g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{m-1}}})^{-1} (g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{m-1}}}) \\ &\quad (g_{\omega_i^{a^m}} \cdots g_{\omega_i^{a^{n(i)-1}}})(g_{\omega_i^{a^{n(i)}}} \cdots g_{\omega_i^{a^{m+n(i)-1}}}) \\ &= (g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{m-1}}})^{-1} (g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{n(i)-1}}})(g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{m-1}}}) \end{aligned}$$

is conjugate to $g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{n(i)-1}}}$ in G, hence it belongs to the conjugacy class $m(\tilde{\omega}_i) = m(\omega_i)$ exactly when $g_{\omega_i} g_{\omega_i^a} \cdots g_{\omega_i^{a^{n(i)-1}}}$ does. Therefore, the definition of the set $\mathcal{K}_{a,m}$ is independent of the choice of the representatives $\omega_1, \dots, \omega_l$.

It is clear that the sets $\mathcal{K}_{a,m}$ for $a \in A$ and $m \in \mathcal{M}_a$ form a partition of Γ. In its action on Γ by conjugation A permutes the sets $\mathcal{K}_{a,m}$, as the next lemma states.

Lemma 7.2.2 *For $a, b \in A$ and $m \in \mathcal{M}_a$, we have*

$$(\mathcal{K}_{a,m})^b = \mathcal{K}_{a^b, m^b}.$$

Proof First of all, the elements of $\mathcal{K}_{a,m}$ have the form $(g_1, \dots, g_k)a$ for some $g_1, \dots, g_k \in G$. Similarly, the elements of $\mathcal{K}_{a^b, m^b}$ have the form $(g_1, \dots, g_k)a^b$ for some $g_1, \dots, g_k \in G$. Let $\omega_1, \dots, \omega_l$ be representatives for the orbits of $\langle a \rangle$ on Ω, then $\omega_1^b, \dots, \omega_l^b$ are representatives for the orbits of $\langle a^b \rangle$ on Ω and the $\langle a^b \rangle$-orbit containing ω_i^b has the same length $n(i)$ of the $\langle a \rangle$-orbit containing ω_i. We have

$$((g_1, \dots, g_k)a)^b = (g_{1^{b^{-1}}}, \dots, g_{k^{b^{-1}}})a^b = (h_1, \dots, h_k)a^b,$$

where we have put $h_j = g_{j^{b^{-1}}}$ for all $j = 1, \dots, k$. The condition

$$(h_1, \dots, h_k)a^b \in \mathcal{K}_{a^b, m^b} \tag{7.4}$$

is equivalent to

$$h_{\omega_i^b} h_{\omega_i^{b(a^b)}} \cdots h_{\omega_i^{b(a^b)^{n(i)-1}}} \in m^b(\omega_i^b) \quad \text{for all } i = 1, \dots, l.$$

Since

$$\begin{aligned} h_{\omega_i b} h_{\omega_i b(b^{-1}ab)} \cdots h_{\omega_i b(b^{-1}ab)^{n(i)-1}} &= h_{\omega_i b} h_{\omega_i ab} \cdots h_{\omega_i a^{n(i)-1} b} \\ &= g_{\omega_i} g_{\omega_i a} \cdots g_{\omega_i a^{n(i)-1}} \end{aligned}$$

and $m^b(\omega_i^b) = m(\omega_i)$ by definition, condition 7.4 is equivalent to

$$g_{\omega_i} g_{\omega_i a} \cdots g_{\omega_i a^{n(i)-1}} \in m(\omega_i) \text{ for all } i = 1, \dots, l,$$

and hence to

$$(g_1, \dots, g_k)a \in \mathcal{K}_{a,m},$$

that is to say,

$$((g_1, \dots, g_k)a)^b \in (\mathcal{K}_{a,m})^b.$$

The proof is complete. □

In the next lemma we shall compute the cardinality of the sets $\mathcal{K}_{a,m}$.

Lemma 7.2.3 *We have*

$$|\mathcal{K}_{a,m}| = |G|^{k-l} \prod_{i=1}^{l} |m(\omega_i)|,$$

where $\omega_1, \dots, \omega_l$ are representatives for the orbits of A on Ω.

Proof We observe that the equation

$$h_1 h_2 \cdots h_n = \bar{h}$$

in the unknowns $h_1, \dots, h_n \in H$, where $\bar{h}$ is a fixed element of a group H, has exactly $|H|^{n-1}$ solutions $(h_1, \dots, h_n)$. In fact, given arbitrary values in H to $h_1, \dots, h_{n-1}$, there is exactly one value for h_n, namely $h_n = h_{n-1}^{-1} \cdots h_1^{-1} \bar{h}$, such that $h_1 h_2 \cdots h_n = \bar{h}$. Now, from the definition of $\mathcal{K}_{a,m}$ we easily get

$$|\mathcal{K}_{a,m}| = \prod_{i=1}^{l} (|G|^{n(i)-1} |m(\omega_i)|),$$

where $n(i)$ is the length of the $\langle a \rangle$-orbit containing ω_i. Since $\sum_{i=1}^{l} n(i) = k$, the conclusion follows. □

7.3 Character tables of wreath products

Theorem 7.3.1 *Let G_1 and G_2 be groups with identical character tables and let A be a permutation group on Ω. Then the wreath products $\Gamma_1 = G_1 \wr A$ and $\Gamma_2 = G_2 \wr A$ have identical character tables.*

Proof Let G_1 and G_2 have identical character tables via the bijections

$$\begin{aligned} \bar{\alpha} : G_1 &\to G_2, \\ \bar{\beta} : \mathrm{Irr}(G_1) &\to \mathrm{Irr}(G_2). \end{aligned}$$

We shall prove the theorem by defining bijections

$$\begin{aligned} \alpha : \Gamma_1 &\to \Gamma_2, \\ \beta : \mathrm{Irr}(\Gamma_1) &\to \mathrm{Irr}(\Gamma_2), \end{aligned}$$

and then checking that

$$\chi^{\beta}(g^{\alpha}) = \chi(g) \ \text{ for all } \chi \in \mathrm{Irr}(\Gamma_1) \ \text{ and for all } g \in \Gamma_1.$$

Definition of α.

Let us define subset of Γ_1 and Γ_2 according to Definition 7.2.1. Since now we have two wreath products $\Gamma_1 = G_1 \wr A$ and $\Gamma_2 = G_2 \wr A$, we shall keep the notation of Definition 7.2.1 for what concerns the group Γ_1, and add bars for the corresponding objects of Γ_2. In particular, $\mathcal{M}_a$ and $\bar{\mathcal{M}}_a$ for $a \in A$ will denote the set of maps $m : \Omega \to \mathrm{cl}(G_1)$, and respectively $\bar{m} : \Omega \to \mathrm{cl}(G_2)$, which are constant on each orbit of $\langle a \rangle$ on Ω.

For each $m \in \mathcal{M}$ let us define a map $m^{\bar{\alpha}} : \Omega \to \mathrm{cl}(G_2)$, that is to say, an element $m^{\bar{\alpha}}$ of $\bar{\mathcal{M}}$, via the formula

$$m^{\bar{\alpha}}(\omega) = m(\omega)^{\bar{\alpha}} \ \text{ for all } \omega \in \Omega.$$

We observe that the map $\bar{\alpha} : \mathcal{M} \to \bar{\mathcal{M}}$ defined above commutes with the actions of A on $\mathcal{M}$ and $\bar{\mathcal{M}}$, namely

$$(m^{\bar{\alpha}})^a = (m^a)^{\bar{\alpha}} \ \text{ for all } a \in A.$$

In fact, for $\omega \in \Omega$ we have

$$(m^{\bar{\alpha}})^a(\omega) = m^{\bar{\alpha}}(\omega^{a^{-1}}) = m(\omega^{a^{-1}})^{\bar{\alpha}} = m^a(\omega)^{\bar{\alpha}} = (m^a)^{\bar{\alpha}}(\omega).$$

As a consequence, for $a \in A$ we have that $m^a \in \mathcal{M}_a$ exactly when $m \in \mathcal{M}_a$; in other words, for each $a \in A$ we get a bijection

$$\begin{aligned} \mathcal{M}_a &\to \mathcal{M}_a \\ m &\mapsto m^{\hat{\alpha}}. \end{aligned}$$

Now the sets $\mathcal{K}_{a,m}$ for $a \in A$ and $m \in \mathcal{M}_a$ form a partition of Γ_1. Similarly, the sets $\mathcal{K}_{a,m^{\hat{\alpha}}}$ for $a \in A$ and $m \in \mathcal{M}_a$ form a partition of Γ_2. Furthermore, according to Lemma 7.2.3, we have

$$|\mathcal{K}_{a,m}| = |G_1|^{k-l} \prod_{i=1}^{l} |m(\omega_i)|,$$

and

$$|\mathcal{K}_{a,m^{\hat{\alpha}}}| = |G_2|^{k-l} \prod_{i=1}^{l} |m^{\hat{\alpha}}(\omega_i)|,$$

where $\omega_1, \ldots, \omega_l$ are representatives for the orbits of $\langle a \rangle$ on Ω. Since $(\hat{\alpha}, \beta)$ is a character table isomorphism, we have $|G_1| = |G_2|$ and

$$|m(\omega_i)| = |m(\omega_i)^{\alpha}| = |m^{\alpha}(\omega_i)|.$$

It follows that

$$|\mathcal{K}_{a,m}| = |\mathcal{K}_{a,m^{\hat{\alpha}}}| \quad \text{for all } a \in A \quad \text{and for all } m \in \mathcal{M}_a.$$

Thus we can choose a bijection $\alpha : \Gamma_1 \to \Gamma_2$ which sends $\mathcal{K}_{a,m}$ onto $\mathcal{K}_{a,m^{\hat{\alpha}}}$ for all $a \in A$ and for all $m \in \mathcal{M}_a$.

Definition of β.

The bijection $\hat{\beta} : \mathrm{Irr}(G_1) \to \mathrm{Irr}(G_2)$ induces a bijection $\beta : \mathrm{Irr}(B_1) \to \mathrm{Irr}(B_2)$, where θ^{β} for $\theta = \theta_1 \times \cdots \times \theta_k \in \mathrm{Irr}(B_1)$ is defined as

$$\theta^{\beta} = \theta_1^{\hat{\beta}} \times \cdots \times \theta_k^{\hat{\beta}} \in \mathrm{Irr}(B_2).$$

The bijection β commutes with the action of A by 'conjugation' on $\mathrm{Irr}(B_1)$ and $\mathrm{Irr}(B_2)$, namely

$$(\theta^a)^{\beta} = (\theta^{\beta})^a \quad \text{for all } \theta \in \mathrm{Irr}(B_1) \quad \text{and for all } a \in A.$$

In fact, if $\theta = \theta_1 \times \cdots \times \theta_k \in \mathrm{Irr}(B_1)$ we have

$$(\theta^a)^\beta = (\theta_{1^{a^{-1}}} \times \cdots \times \theta_{k^{a^{-1}}})^\beta = \theta^\beta_{1^{a^{-1}}} \times \cdots \times \theta^\beta_{k^{a^{-1}}} = (\theta^\beta)^a.$$

Let us choose representatives $\theta_1, \ldots, \theta_r$ for the orbits of A on $\mathrm{Irr}(B_1)$. Then $\theta_1^\beta, \ldots, \theta_r^\beta$ are representatives for the orbits of A on $\mathrm{Irr}(B_2)$. For $i = 1, \ldots, r$ let T_i denote the inertia group of θ_i in A, that is to say, the stabilizer of θ_i in the action of A on $\mathrm{Irr}(B_1)$. Clearly, T_i is also the inertia group of θ_i^β in A. According to Clifford's Theorem, $\mathrm{Irr}(\Gamma_1)$ and $\mathrm{Irr}(\Gamma_2)$ decompose as follows

$$\begin{aligned}\mathrm{Irr}(\Gamma_1) &= \mathrm{Irr}(\Gamma_1, \theta_1) \dot\cup \cdots \dot\cup \mathrm{Irr}(\Gamma_1, \theta_r),\\ \mathrm{Irr}(\Gamma_2) &= \mathrm{Irr}(\Gamma_2, \theta_1^\beta) \dot\cup \cdots \dot\cup \mathrm{Irr}(\Gamma_2, \theta_r^\beta).\end{aligned}$$

We shall define bijections

$$\beta : \mathrm{Irr}(\Gamma_1, \theta_i) \to \mathrm{Irr}(\Gamma_2, \theta_i^\beta),$$

for $i = 1, \ldots, r$, which will then be put together to give a bijection

$$\beta : \mathrm{Irr}(\Gamma_1) \to \mathrm{Irr}(\Gamma_2).$$

Let us fix an index i. According to the Clifford correspondence (see [13, Theorem (6.11)]), induction of characters gives bijections from $\mathrm{Irr}(B_1 T_i, \theta_i)$ onto $\mathrm{Irr}(\Gamma_1, \theta_i)$ and from $\mathrm{Irr}(B_2 T_i, \theta_i^\beta)$ onto $\mathrm{Irr}(\Gamma_2, \theta_i^\beta)$. The construction of our bijection β_i will thus pass through the sets $\mathrm{Irr}(B_1 T_i, \theta_i)$ and $\mathrm{Irr}(B_2 T_i, \theta_i^\beta)$.

Now since θ_i is invariant in $B_1 T_i$ (which is canonically isomorphic to $G_1 \wr T_i$), Lemma 7.1.2 guarantees that θ_i is extendible to $B_1 T_i$ and provides us with a standard extension of θ_i, let us call it $\eta_i \in \mathrm{Irr}(B_1 T_i)$. Similarly, let us call $\hat\eta_i \in \mathrm{Irr}(B_2 T_i)$ the standard extension of θ_i^β provided by Lemma 7.1.2. According to [13, Corollary (6.17)], the elements of $\mathrm{Irr}(B_1 T_i, \theta_i)$ are exactly the characters $\eta_i \varphi$ for $\varphi \in \mathrm{Irr}(B_1 T_i / B_1)$. Similarly, the elements of $\mathrm{Irr}(B_2 T_i, \theta_i^\beta)$ are the characters $\hat\eta_i \psi$ for $\psi \in \mathrm{Irr}(B_2 T_i / B_2)$.

We have a natural bijective correspondence between $\mathrm{Irr}(B_1 T_i / B_1)$ and $\mathrm{Irr}(B_2 T_i / B_2)$, corresponding to the obvious isomorphism from $B_1 T_i / B_1$ onto $B_2 T_i / B_2$. To put it differently, the restriction map gives bijections

$$\begin{aligned}\mathrm{Irr}(B_j T_i / B_j) &\to \mathrm{Irr}(T_i)\\ \varphi &\mapsto \varphi_{T_i},\end{aligned}$$

for $j = 1, 2$; hence we can form a bijection

$$\begin{array}{rcl} \mathrm{Irr}(B_1T_i/B_1) & \to & \mathrm{Irr}(B_2T_i/B_2) \\ \varphi & \mapsto & \hat{\varphi}, \end{array}$$

where $\hat{\varphi}$ denotes the unique irreducible character of B_2T_i whose kernel contains B_2 and such that $\hat{\varphi}_{T_i} = \varphi_{T_i}$.

Now we are ready to set up a bijection from $\mathrm{Irr}(\Gamma_1, \theta_i)$ onto $\mathrm{Irr}(\Gamma_2, \theta_i^\beta)$. In fact, we have seen that

$$\mathrm{Irr}(\Gamma_1, \theta_i) = \{(\eta_i\varphi)^{\Gamma_1} \mid \varphi \in \mathrm{Irr}(B_1T_i/B_1)\}$$

and

$$\mathrm{Irr}(\Gamma_2, \theta_i^\beta) = \{(\hat{\eta}_i\varphi)^{\Gamma_2} \mid \varphi \in \mathrm{Irr}(B_1T_i/B_1)\}.$$

Let us define the following maps, for $i = 1, \ldots, r$:

$$\begin{array}{rcl} \beta_i : \mathrm{Irr}(\Gamma_1, \theta_i) & \to & \mathrm{Irr}(\Gamma_2, \theta_i^\beta) \\ (\eta_i\varphi)^{\Gamma_1} & \mapsto & (\hat{\eta}_i\hat{\varphi})^{\Gamma_2}. \end{array}$$

The maps β_i are well defined and are bijections. The various maps β_i can then be put together to give a single bijection

$$\beta : \mathrm{Irr}(\Gamma_1) \to \mathrm{Irr}(\Gamma_2).$$

Verification that $\chi^\beta(g^\alpha) = \chi(g)$.

Let us fix a character $\chi \in \mathrm{Irr}(\Gamma_1)$, say $\chi \in \mathrm{Irr}(\Gamma_1, \theta_i)$. Then $\chi = (\eta_i\varphi)^{\Gamma_1}$ for some $\varphi \in \mathrm{Irr}(B_1T_i/B_1)$, where η_i is the standard extension of θ_i to B_1T_i given by Lemma 7.1.2. According to our definition of β, we have $\chi^\beta = (\hat{\eta}_i\hat{\varphi})^{\Gamma_2}$, where $\hat{\eta}_i$ is the standard extension of θ_i to B_2T_i, and $\hat{\varphi}$ is the unique character in $\mathrm{Irr}(B_2T_i/B_2)$ such that $\hat{\varphi}_{T_i} = \varphi_{T_i}$.

We shall first show that

$$(\hat{\eta}_i\hat{\varphi})(g^\alpha) = (\eta_i\varphi)(g) \quad \text{for all } g \in B_1T_i.$$

In order to prove this fact, let us fix $g = (g_1, \ldots, g_k)a \in B_1T_i$. Then there is a unique $m \in \mathcal{M}_a$ such that $g \in K_{a,m}$, and hence we have

$$\begin{array}{rcl} g_{\omega_1} g_{\omega_1 a} \cdots g_{\omega_1 a^{n(1)-1}} & \in & m(\omega_1), \\ & \vdots & \\ g_{\omega_l} g_{\omega_l a} \cdots g_{\omega_l a^{n(l)-1}} & \in & m(\omega_l), \end{array}$$

where $\omega_1, \ldots, \omega_l$ are representatives for the orbits of $\langle a \rangle$ on Ω, and $n(i)$ denotes the length of the $\langle a \rangle$-orbit which contains ω_i. According to our definition of α, we have $g^\alpha \in K_{a,m^\alpha}$, and hence $g^\alpha = (h_1, \ldots, h_k)a$ for some $h_1, \ldots, h_k \in G_2$, such that

$$\begin{aligned} h_{\omega_1} h_{\omega_1 a} \cdots h_{\omega_1 a^{n(1)-1}} &\in m^\alpha(\omega_1), \\ &\vdots \\ h_{\omega_l} h_{\omega_l a} \cdots h_{\omega_l a^{n(l)-1}} &\in m^\alpha(\omega_l). \end{aligned}$$

Let us put $\theta_i = \theta_{i1} \times \cdots \times \theta_{ik}$. According to Lemma 7.1.2, we have

$$\eta_i(g) = \prod_{j=1}^{l} \theta_{i\omega_j}(g_{\omega_j} g_{\omega_j a} \cdots g_{\omega_j a^{n(j)-1}}),$$

and similarly,

$$\hat{\eta}_i(g^\alpha) = \prod_{j=1}^{l} (\theta_{i\omega_j})^{\tilde{\beta}}(h_{\omega_j} h_{\omega_j a} \cdots h_{\omega_j a^{n(j)-1}}).$$

Now for each $j = 1, \ldots, l$ we have

$$g_{\omega_j} g_{\omega_j a} \cdots g_{\omega_j a^{n(j)-1}} \in m(\omega_j),$$

and

$$h_{\omega_j} h_{\omega_j a} \cdots h_{\omega_j a^{n(j)-1}} \in m^{\tilde{\alpha}}(\omega_j) = m(\omega_j)^{\tilde{\alpha}}.$$

From the fact that $(\tilde{\alpha}, \tilde{\beta})$ is a character table isomorphism, it follows that

$$(\theta_{i\omega_j})^{\tilde{\beta}}(h_{\omega_j} h_{\omega_j a} \cdots h_{\omega_j a^{n(j)-1}}) = \theta_{i\omega_j}(g_{\omega_j} g_{\omega_j a} \cdots g_{\omega_j a^{n(j)-1}})$$

for all $j = 1, \ldots, l$. Hence we have $\hat{\eta}_i(g^\alpha) = \eta_i(g)$. Since we also have

$$\hat{\varphi}(g^\alpha) = \hat{\varphi}(a) = \varphi(a) = \varphi(g),$$

it follows that

$$(\hat{\eta}_i \hat{\varphi})(g^\alpha) = (\eta_i \varphi)(g) \text{ for all } g \in B_1 T_i,$$

as claimed.

Finally, we shall show that

$$\chi^\beta(g^\alpha) = \chi(g) \text{ for all } g \in \Gamma_1.$$

Let $(\eta_i\varphi)^\circ$ (respectively $(\hat{\eta}_i\hat{\varphi})^\circ$) denote the function on Γ_1 (respectively Γ_2) which extends $\eta_i\varphi$ (respectively $\hat{\eta}_i\hat{\varphi}$) and vanishes on $\Gamma_1 \setminus B_1T_i$ (respectively $\Gamma_2 \setminus B_2T_i$). We clearly have

$$(\hat{\eta}_i\hat{\varphi})^\circ(g^\alpha) = (\eta_i\varphi)^\circ(g) \text{ for all } g \in \Gamma_1.$$

Let us fix $g \in \Gamma_1$; we compute

$$\begin{aligned}\chi(g) = (\eta_i\varphi)^{\Gamma_1}(g) &= \frac{1}{|B_1T_i|}\sum_{x\in\Gamma_1}(\eta_i\varphi)^\circ(xgx^{-1}) \\ &= \frac{1}{|T_i|}\sum_{b\in A}(\eta_i\varphi)^\circ(bgb^{-1}).\end{aligned}$$

Similarly, we have

$$\begin{aligned}\chi^\beta(g^\alpha) = (\hat{\eta}_i\hat{\varphi})^{\Gamma_2}(g^\alpha) &= \frac{1}{|B_2T_i|}\sum_{x\in\Gamma_2}(\hat{\eta}_i\hat{\varphi})^\circ(xg^\alpha x^{-1}) \\ &= \frac{1}{|T_i|}\sum_{b\in A}(\hat{\eta}_i\hat{\varphi})^\circ(bg^\alpha b^{-1}).\end{aligned}$$

In order to conclude that

$$\chi^\beta(g^\alpha) = \chi(g) \text{ for all } g \in \Gamma_1,$$

it will be enough to show that

$$(\hat{\eta}_i\hat{\varphi})^\circ(bg^\alpha b^{-1}) = (\eta_i\varphi)^\circ(bgb^{-1}).$$

Since we have already proved that

$$(\hat{\eta}_i\hat{\varphi})^\circ((bgb^{-1})^\alpha) = (\eta_i\varphi)^\circ(bgb^{-1}),$$

it remains to show that

$$(\hat{\eta}_i\hat{\varphi})^\circ(bg^\alpha b^{-1}) = (\hat{\eta}_i\hat{\varphi})^\circ((bgb^{-1})^\alpha)$$

Because $(\eta_i\bar{\varphi})^{*}$ is constant on each $\mathcal{K}_{c,m}$, the equality above, and hence the conclusion of the proof, will follow from the fact that $bg^{\alpha}b^{-1}$ and $(bgb^{-1})^{\alpha}$ belong to the same $\mathcal{K}_{c,m}$. To prove this fact, we observe that on one hand, from $g^{\alpha} \in \mathcal{K}_{a,m^{\bar{\alpha}}}$ we get

$$bg^{\alpha}b^{-1} = (g^{\alpha})^{b^{-1}} \in \mathcal{K}_{a^{b^{-1}},(m^{\bar{\alpha}})^{b^{-1}}},$$

according to Lemma 7.2.2. On the other hand, since $g \in \mathcal{K}_{a,m}$, we have

$$bgb^{-1} \in \mathcal{K}_{a^{b^{-1}},m^{b^{-1}}},$$

again according to Lemma 7.2.2; consequently, we obtain

$$(bgb^{-1})^{\alpha} \in \mathcal{K}_{a^{b^{-1}},(m^{b^{-1}})^{\bar{\alpha}}} = \mathcal{K}_{a^{b^{-1}},(m^{\bar{\alpha}})^{b^{-1}}},$$

because $(m^{b^{-1}})^{\alpha} = (m^{\bar{\alpha}})^{b^{-1}}$. This concludes the proof. □

7.4 An application to character tables and derived length

In this last section we shall construct, for any given natural number n with $n \geq 2$, a pair of groups G_1 and G_2 with identical character tables and derived lengths n and $n+1$ respectively. Let us begin with a standard result.

Lemma 7.4.1 *Let G be a soluble group and C be a non-trivial cyclic group. Let us form the regular wreath product $\Gamma = G \wr C$. Then we have*

$$\mathrm{dl}(\Gamma) = \mathrm{dl}(G) + 1.$$

Proof The base group B is the direct product

$$B = G_1 \times \cdots \times G_r$$

of $r = |C|$ isomorphic copies of G. We may fix a generator c of C and assume that c acts on B as follows:

$$(g_1, \ldots, g_r)^c = (g_r, g_1, \ldots, g_{r-1}) \quad \text{for all } (g_1, \ldots, g_r) \in B.$$

We claim that

$$\Gamma' = \{(g_1, \dots, g_r) \in B \mid g_1 \cdots g_r \in G'\}.$$

We observe that $B' = G'_1 \times \cdots \times G'_r$ is a normal subgroup of Γ contained in Γ'; hence $\Gamma'/B' = (\Gamma/B')'$. Since Γ/B' is canonically isomorphic to the regular wreath product $(G/G') \wr C$, it will be enough to prove the claim with the additional assumption that G is abelian.

Let us assume that G is abelian and put

$$M = \{(g_1, \dots, g_r) \in B \mid g_1 \cdots g_r = 1\}.$$

Clearly, M is a subgroup of the abelian group B; furthermore, M is normal in Γ, because it is C-invariant. Let $(h_1, \dots, h_r) \in B$. We have

$$\begin{aligned}[(h_1, \dots, h_r), c^{-1}] &= (h_1^{-1}, \dots, h_r^{-1})(h_1, \dots, h_r)^{c^{-1}} \\ &= (h_1^{-1}, \dots, h_r^{-1})(h_2, \dots, h_r, h_1) \\ &= (h_1^{-1}h_2, \dots, h_{r-1}^{-1}h_r, h_r^{-1}h_1) \in M.\end{aligned}$$

It follows that $\Gamma' = (BC)' = [B, C] \leq M$.

Now let $(g_1, \dots, g_r) \in M$. Let us put $h_1 = 1$ and $h_{i+1} = h_i g_i$ for $i = 1, \dots, r-1$. Then we have

$$\begin{aligned}[(h_1, \dots, h_r), c^{-1}] &= (h_1^{-1}h_2, \dots, h_{r-1}^{-1}h_r, h_r^{-1}h_1) \\ &= (g_1, \dots, g_{r-1}, g_{r-1}^{-1} \cdots g_1^{-1}) \\ &= (g_1, \dots, g_r).\end{aligned}$$

Thus we have $M \leq \Gamma'$. We conclude that $\Gamma' = M$, and our claim is proved.

In order to prove the lemma now it suffices to show that

$$\mathrm{dl}(\Gamma') = \mathrm{dl}(G).$$

Since $\Gamma' \leq B$ we have $\mathrm{dl}(\Gamma') \leq \mathrm{dl}(B) = \mathrm{dl}(G)$. On the other hand, the group homomorphism

$$\begin{aligned}\Gamma' &\to G \\ (g_1, \dots, g_r) &\mapsto g_1\end{aligned}$$

is surjective, because the element $(g, g^{-1}, 1, \dots, 1)$ of B is mapped to the generic element g of G. Hence $\mathrm{dl}(\Gamma') \geq \mathrm{dl}(G)$.

We conclude that $\mathrm{dl}(\Gamma') = \mathrm{dl}(G)$, and the lemma is proved. □

Theorem 7.4.2 *Let n be a natural number with $n \geq 2$. Then there exist groups G_1 and G_2 with identical character tables, such that G_1 has derived length n, while G_2 has derived length $n+1$.*

Proof We shall prove the theorem by induction on n.

For the case $n = 2$, the existence of groups G_1 and G_2 with identical character tables and derived lengths 2 and 3 respectively was proved in Chapters 5 and 6, where two different constructions were used.

Now let us fix $n > 2$ and assume that we have been able to construct groups G_1 and G_2 with identical character tables and derived lengths $n-1$ and n respectively. Let C be a non-trivial cyclic group. Let us form the regular wreath product $\Gamma_i = G_i \wr C$, for $i = 1, 2$. Then Γ_1 and Γ_2 have identical character tables, according to Theorem 7.3.1. On the other hand, the derived lengths of Γ_1 and Γ_2 are n and $n+1$ respectively, according to Lemma 7.4.1. This concludes the proof. $\square$

We observe that there are p-groups G_1 and G_2 which satisfy the conclusions of Theorem 7.4.2 (at least when the prime p is greater than or equal to 5); in fact, we may take the p-groups G_1 and G_2 constructed in Chapter 6 as the basis of the inductive proof of Theorem 7.4.2, and then take a cyclic group of order p as the group C of the induction step.

We conclude this thesis with an open question.

Question 7.4.3 *Is there any pair (G, H) of groups which have identical character tables, and derived lengths two and four respectively?*

Bibliography

[1] B. Beisiegel, *Semi-extraspeziellen p-gruppen*, Math. Z. **156** (1977), 247–254.

[2] A. R. Camina, *Some conditions which almost characterize Frobenius groups*, Israel J. Math. **31** (1978), 153–160.

[3] D. Chillag, I. D. Macdonald and C. M. Scoppola, *Generalized Frobenius groups II*, Israel J. Math. **62** (1988), 269–282.

[4] J. H. Conway, T. R. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[5] C. W. Curtis and I. Reiner, *Methods of Representation Theory I*, Wiley Interscience, New York, 1981.

[6] E. C. Dade, *Answer to a Question of R. Brauer*, J. of Algebra, **1** (1964), 1–4.

[7] K. Dock and P. Igodt, *Character tables and commutativity of normal subgroups*, SIGSAM Bull. of ACM, **25** (1991), 28–31.

[8] M. Hall, *The theory of groups*, Macmillan Company, New York, 1959.

[9] G. Higman, *Suzuki 2-groups*, Illinois J. Math. **7** (1963), 79–96.

[10] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[11] B. Huppert, N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[12] B. Huppert, R. Gow, R. Knörr, O. Manz, R. Staszewski, W. Willems, *Lectures on "Clifford theory and applications", Trento, September 14–18, 1987*, Centro Internazionale per la ricerca matematica, Trento.

[13] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, San Francisco, London, 1976.

[14] I. M. Isaacs, *Character Correspondences in Solvable Groups*, Advances in Mathematics **43** (1982), 284–306.

[15] N. Jacobson, *Basic Algebra I*, W. H. Freeman and company, San Francisco, 1973.

[16] A. Mann and C. M. Scoppola, *On p-groups of Frobenius type*, Arch. Math. **56** (1991), 320–332.

[17] S. Mattarei, *Character tables and metabelian groups*, J. London Math. Soc., to appear.

[18] H. Neumann, *Varieties of Groups*, Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[19] T. Saaty (Editor), *Lectures on Modern Mathematics*, Volume 1, John Wiley & Sons, New York, 1963.

[20] A. I. Saksonov, *An answer to a question of R. Brauer* (Russian), Vesci Akad. Navuk BSSR, Ser. Fiz.-Mat. Navuk (1967), no. 1, pp. 129–130 (Math. Reviews 35 (1968) ♯ 5527).

[21] C. M. Scoppola, *Groups of prime power order as Frobenius-Wielandt complements*, Trans. Amer. Math. Soc. (2) **325** (1991), 855–874.