Minimal parabolic subgroups in the symmetric groups

by

Sandra Covello

A Thesis submitted to the University of Birmingham
for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
The University of Birmingham
Birmingham
United Kingdom

May 31, 2000

Acknowledgements

The author would like to express her most sincere appreciation to her supervisor Chris Parker, who has guided her step by step throughout the preparation of this work with enthusiasm and dedication. Working alongside him has given her many insights into her project as well as into research methods in group theory.

Special thanks go, for their warm hospitality, to all the people at the Department of Mathematics of Kansas State University, Manhattan, Kansas, USA, where the author held a position as teaching assistant during Fall 1998.

She would also like to thank Patrizia Longobardi and Ulderico Dardano at the Dipartimento di Matematica ed Applicazioni R. Caccioppoli, Università degli Studi di Napoli Federico II, Naples, Italy, for suggesting and supporting her Ph.D. application at the University of Birmingham.

Further thanks go to the Istituto Nazionale di Alta Matematica F. Severi, Rome, Italy, and to the Consiglio Nazionale delle Ricerche, Italy, for their financial support.

Abstract

The purpose of this dissertation is to start the investigation of minimal parabolic subgroups and minimal parabolic systems of the symmetric group $\mathrm{Sym}(n)$ with respect to the normalizer of a Sylow p-subgroup.

A first crucial step is to classify all symmetric groups which are themselves minimal parabolic subgroups. This enables us to reduce our study to some critical cases. More specifically, it is possible to assume that a minimal parabolic subgroup is imprimitive and this forces some restrictions on the degree n of the symmetric group, giving also information about the solubility of the minimal parabolic subgroup.

We then focus our attention on one of these main cases, namely, the case when n is a power of the prime p associated with the minimal parabolic subgroups. If $n = p^r$ and $r = 1$ or 2, then all minimal parabolic subgroups and systems of $\mathrm{Sym}(n)$ are known. For $r > 2$, we characterize, in terms of certain modules, all minimal parabolic subgroups and systems for the subgroup H of $\mathrm{Sym}(n)$ which is isomorphic to the wreath product of r copies of $\mathrm{Hol}(\mathbb{Z}_p)$. If $p \geq 3$, those contained in H are all the soluble minimal parabolic subgroups of $\mathrm{Sym}(p^r)$. Thus, using the list of critical cases, we can conclude that for any symmetric group all the minimal parabolic subgroups that are soluble are known, except when $n = p^{r+1} + p^r$, with $r \geq 1$, and $p = 3$.

Finally, as an application of the results proved in the $\mathrm{Sym}(p^r)$ case, we present some MAGMA programs that generate the minimal parabolic subgroups of H.

Contents

List of Figures

List of Tables

Notation

Introduction

Suppose that G is a finite group and p is a prime dividing the order of G. Let T be a Sylow p-subgroup of G and B the normalizer of T in G. A subgroup P of G properly containing B is said to be a **minimal parabolic subgroup** of G with respect to B if B is contained in a unique maximal subgroup of P.

Every group G is generated by its minimal parabolic subgroups. In particular, a collection $\mathcal{S}$ of minimal parabolic subgroups of G with respect to B is called a **minimal parabolic system** of G if $G = \langle \mathcal{S} \rangle$ and no proper subset of $\mathcal{S}$ generates G. The **rank** of $\mathcal{S}$ is the number of subgroups belonging to $\mathcal{S}$.

Our aim is to study the structure of minimal parabolic subgroups and minimal parabolic systems in the symmetric group of degree n and in some of its subgroups, for any integer n and any prime p dividing the order of the group.

The concept of a minimal parabolic subgroup arises from the study of group geometries and, as well as in this field (see [3], [25]), it has important applications in representation theory (see [13], [32], [33], [35]) and to the problem of group recognition (see [18], [19], [31]).

The connection between minimal parabolic subgroups and group geometries is best illustrated in the case of groups of Lie type in their defining characteristic. Parabolic subgroups are defined in terms of $(B, N)-$pairs ([6]) and are used to construct a geometrical structure, called a building ([38]), associated with the group. In particular, the chambers of the building are the conjugates of B and adjacency between chambers is defined using the parabolic subgroups. This approach to group geometries is then used in representation theory, in particular by Ronan and Smith (see [27], [28], [29]), and in group recognition.

In the following example we shall describe all minimal parabolic subgroups and systems of $\mathrm{GL}_5(q)$ with respect to the normalizer of a Sylow p-subgroup, where q is a power of p.

Example 1: $\mathbf{GL}_5(q)$

Let $G = \mathrm{GL}_5(F)$, where F is a finite field of q elements, $q = p^r$ and p is a prime. In writing matrices, we shall use the convention that a missing entry stands for a zero entry.

A Sylow p-subgroup T of G is given by the set of all matrices of the form

$$\begin{pmatrix} 1 & & & & \\ a_{21} & 1 & & & \\ a_{31} & a_{32} & 1 & & \\ a_{41} & a_{42} & a_{43} & 1 & \\ a_{51} & a_{52} & a_{53} & a_{54} & 1 \end{pmatrix},$$

where $a_{ij} \in F$, for all i, j. In particular, $|T| = q^{10}$.

The normalizer B of T in G is the set of all nonsingular matrices of the form

$$\begin{pmatrix} a_{11} & & & & \\ a_{21} & a_{22} & & & \\ a_{31} & a_{32} & a_{33} & & \\ a_{41} & a_{42} & a_{43} & a_{44} & \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix},$$

with $a_{ij} \in F$, for all i, j. Hence $|B| = q^{10}(q-1)^5$.

Now let P_1 be the subgroup of G consisting of all nonsingular matrices of the form

$$\begin{pmatrix} a_{11} & a_{12} & & & \\ a_{21} & a_{22} & & & \\ a_{31} & a_{32} & a_{33} & & \\ a_{41} & a_{42} & a_{43} & a_{44} & \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix},$$

with $a_{ij} \in F$, for all i, j. Then $P_1 = HK$, where H is the subgroup of T consisting of the matrices of the form

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ a_{31} & a_{32} & 1 & & \\ a_{41} & a_{42} & a_{43} & 1 & \\ a_{51} & a_{52} & a_{53} & a_{54} & 1 \end{pmatrix}$$

and K is the subgroup of G whose elements are matrices of the form

$$\begin{pmatrix} a_{11} & a_{12} & & & \\ a_{21} & a_{22} & & & \\ & & a_{33} & & \\ & & & a_{44} & \\ & & & & a_{55} \end{pmatrix}.$$

Hence P_1 is a group of shape $q^9(q-1)^3\mathrm{GL}_2(F)$. In particular, P_1 contains a normal subgroup $L \leqslant B$ of order $q^9(q-1)^3$ and, since B/L is a maximal subgroup of $P_1/L \cong \mathrm{GL}_2(F)$, we can conclude that P_1 is a minimal parabolic subgroup of G with respect to B.

Similarly, we can show that, for $k = 2, 3, 4$, the subgroups

$$P_k = \{(a_{ij}) \mid a_{ij} = 0, \text{ for all } (i,j) \text{ with } i < j \text{ and } (i,j) \neq (k, k+1)\}$$

are minimal parabolic subgroups of G with respect to B. Moreover these are the only minimal parabolic subgroups of G with respect to B and, for all $i = 1, \ldots, 4$, $G \neq \langle P_k \mid k \neq i \rangle$. Therefore G has a unique minimal parabolic system $\mathcal{S}$ and $\mathcal{S} = \{P_1, P_2, P_3, P_4\}$. ■

The definition of minimal parabolic subgroups in terms of the normalizer of a Sylow p-subgroup is given in the works of Ronan and Smith ([26]) and Ronan and Stroth ([30]), in which they study minimal parabolic geometries for the 26 sporadic finite simple groups. As an example we shall look at the Monster group.

Example 2: the Monster M

Let $G = M$ be the Monster group and $p = 7$. We borrow our notation from the ATLAS ([7]). The order of a Sylow p-subgroup T of G is 7^6 and the normalizer B of T in G has shape $7^2.7.7^2 : 7 : 6^2$.

Consider now the subgroups

$$P_1 \cong 7^{1+4} : (3 \times (2^{\cdot}\mathrm{Sym}(7)))$$
$$P_2 \cong 7^2.7.7^2 : \mathrm{GL}_2(7).$$

Clearly, B is a maximal subgroup of both P_1 and P_2 and so P_1 and P_2 are minimal parabolic subgroups of G with respect to B. Moreover, by the ATLAS ([7]), P_1 and P_2 are maximal subgroups of G and, by considering the orders, they are the only maximal subgroups of G containing B. Hence we can conclude that P_1 and P_2 are the only minimal parabolic subgroups of G with respect to B and that G has a unique minimal parabolic system $\mathcal{S}$ and $\mathcal{S} = \{P_1, P_2\}$. ∎

The idea of studying minimal parabolic subgroups in the symmetric groups was first suggested by Stroth in [34] and recently Lempken, Parker and Rowley ([21]) determined all the minimal parabolic subgroups and systems for the symmetric and alternating groups, with respect to the prime $p = 2$. This case is relatively easy to study and an example illustrating their result is presented next.

Example 3: Sym(11)

Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n = 11$. Suppose that $p = 2$ and let T be a Sylow p-subgroup of G. Then $|T| = 2^8$ and $N_G(T) = T$. Consider the p-adic decomposition of n, $n = 8+2+1 = 2^3+2+2^0$ and write $\Omega = \Omega_1 \cup \Omega_2 \cup \Omega_3$, with $|\Omega_1| = 8$, $|\Omega_2| = 2$ and $|\Omega_3| = 1$. Then $T = T_1 \times T_2 \cong (C_2 \wr C_2 \wr C_2) \times C_2$, with T_i Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$, for $i = 1, 2$, and C_2 cyclic group of order 2. Also the Ω_i's are the orbits of T on Ω. In particular, T has one fixed point on Ω.

By [21, Theorem 1.1], the minimal parabolic subgroups of G with respect to T are the following:

$$
\begin{aligned}
P(1+2) &\cong C_2 \wr \mathrm{Sym}(5) \\
P(1+3) &\cong \mathrm{Sym}(9) \times T_2 \\
P(2+3) &\cong \mathrm{Sym}(3) \times T_1 \\
P(1;1) &\cong (\mathrm{Sym}(4) \wr C_2) \times T_2 \\
P(1;2) &\cong (C_2 \wr \mathrm{Sym}(4)) \times T_2
\end{aligned}
$$

and, by [21, Theorem 1.3 (ii)], G has three distinct minimal parabolic systems with respect to T, each of rank 2 and they are:

$$\{P(1+2), P(1+3)\}$$

$$\{P(1+2), P(2+3)\}$$

$$\{P(1+3), P(2+3)\}.$$

■

Hence our aim is to extend the results obtained by Lempken, Parker and Rowley for the symmetric groups to any prime p.

However, in the general case there are some immediate complications that are not present in the $p = 2$ case.

First, for $p \neq 2$, a Sylow p-subgroup of the symmetric group is not equal to its normalizer and so much more work needs to be done to understand the structure of the normalizer.

Moreover, as $p - 1 \neq 1$, the prime divisors of $p - 1$ play a certain role in the investigation of the overgroups of the normalizer, and thus of the minimal parabolic subgroups. For instance, in the case of $\mathrm{Sym}(p^2)$, there is an isomorphism between the lattice of subgroups of a cyclic group of order $p - 1$ and the lattice of certain overgroups of the normalizer and a similar correspondence holds also for the case $\mathrm{Sym}(p^r)$, with $r > 2$.

Throughout all groups considered, and in particular all sets on which a permutation group acts, will be finite.

The work is organized as follows.

The first three chapters are devoted to introduce the preliminaries required. Basic facts of general group theory are presented and some fundamental results on minimal parabolic subgroups are proved. The theory of permutation groups is introduced, with special attention drawn to minimal normal subgroups of 2-transitive groups.

Chapters 4 and 5 are concerned with the structure of a Sylow p-subgroup T of the symmetric group and of its normalizer B. Particular emphasis is given to the case when the degree of the symmetric group is a power of p, for which a detailed description of the generators of T and B is provided and some of the notation which will be used in the later chapters is set.

Chapter 6 starts the investigation of minimal parabolic subgroups and plays a fundamental role for a further study on the topic.

Some specific cases are analyzed (see Theorems 6.1.2, 6.3.1, 6.4.1, 6.5.2) and, in particular, the following theorem, which demonstrates a further difference from the untypical case $p = 2$, is proved (see Theorem 6.2.2):

Theorem A. *Let p be a prime and $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p+1$. Suppose that $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then*

(i) *if $p = 2, 3$, there is a unique minimal parabolic subgroup of G with respect to B and it is G itself; in particular, the unique minimal parabolic system of G is given by $\{G\}$;*

(ii) *if $p \neq 2, 3$, there are only two minimal parabolic subgroups P_1 and P_2 of G with respect to B; P_1 is isomorphic to $\mathrm{Sym}(p)$ embedded as a point stabilizer and P_2 is isomorphic to $\mathrm{PGL}(2,p)$ acting on one dimensional subspaces. In particular, there is a unique minimal parabolic system $\mathcal{S}$ of G and it is $\{P_1, P_2\}$.*

The study undertaken also leads to the classification of all symmetric groups which are themselves minimal parabolic subgroups, that is, those for which B is contained in a unique maximal subgroup of G (see Theorem 6.6.1).

Theorem B. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. Suppose that $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Then G is a minimal parabolic subgroup with respect to B if and only if one of the following occurs:*

(i) *$n = p$ and $p \neq 2, 3$;*

(ii) *$n = p + 1$ and $p = 2, 3$;*

(iii) *$n = kp$, with $1 < k \leq p$;*

(iv) *$n = k_1 p^{\alpha_1} + k_0$, with $1 \leq k_0, k_1 < p$, $\alpha_1 \geq 1$ and $(k_0, k_1, \alpha_1) \neq (1,1,1)$.*

Theorem B has very important consequences on the study of minimal parabolic subgroups. All minimal parabolic subgroups which are primitive are known and, for those that are imprimitive, some restrictions on the degree n are derived, leaving us with a list of critical cases to investigate (see Theorem 6.7.4). Furthermore, for most of these cases, a minimal parabolic subgroup is nonsoluble and, when n is a power of p, say $n = p^r$, for some r, and $p \geq 3$, all soluble minimal parabolic subgroups are contained in the wreath product of r copies of $\mathrm{Hol}(\mathbb{Z}_p)$.

The rest of the dissertation is devoted to the study of the case $\mathrm{Sym}(p^r)$, which is one of those listed in Theorem 6.7.4. So set $G = \mathrm{Sym}(p^r)$, with p prime and $r \in \mathbb{N}$, $T \in \mathrm{Syl}_p(G)$ and

$B = N_G(T)$. We shall also denote by H the wreath product of r copies of $\mathrm{Hol}(\mathbb{Z}_p)$. Recall that, by Theorem 5.2.4, $\mathrm{Hol}(\mathbb{Z}_p)$ is isomorphic to the normalizer of a Sylow p-subgroup of the symmetric group $\mathrm{Sym}(p)$, which is, by Theorem 6.1.2, a maximal subgroup of $\mathrm{Sym}(p)$.

We start our investigation with the case $\mathrm{Sym}(p^2)$, which is described in Chapter 7. The results achieved are summarized in the next theorem. For more details about the subgroups mentioned in Theorem C, the reader can refer to Theorems 7.3.2 and 7.3.5.

Theorem C. *All minimal parabolic subgroups of G with respect to B are known:*

(i) *the minimal parabolic subgroups which are contained in H are in one-to-one correspondence with the prime-power order subgroups of a cyclic group of order $p-1$ and so there are $\sum_{q\in\pi(p-1)}\alpha_q$ of them, where $\pi(p-1)$ denotes the set of prime divisors of $p-1$ and, for $q \in \pi(p-1)$, q^{α_q} is the highest power of q dividing $p-1$;*

(ii) *a minimal parabolic subgroup which is not contained in H is either G or one of two others.*

In particular, G has $3+\sum_{q\in\pi(p-1)}\alpha_q$ minimal parabolic subgroups with respect to B. Furthermore G has a unique minimal parabolic system $\mathcal{S}$ and $\mathcal{S} = \{G\}$.

Theorem C provides us with the base for an induction argument to be carried out on r. Furthermore, the role played in the $\mathrm{Sym}(p^2)$ case by the subgroups of H containing B, which are proved to be in one-to-one correspondence with the subgroups of a cyclic group of order $p-1$, suggests, for the general case, the study of minimal parabolic subgroups which are contained in H. However, when moving from the case $\mathrm{Sym}(p^2)$ to the case $\mathrm{Sym}(p^r)$, with $r > 2$, the situation becomes much more complicated and the generalization of Theorem C (i) that we get (see Theorems 10.2.2 and 10.2.3) is not the most immediate one. In particular, we need to move out of the context of permutation groups to find new more powerful tools and this is done in Chapters 8 and 9.

In Chapter 8 we study some modules which are invariant under the action of the normalizer of a Sylow p-subgroup. The results proved are summarized in the following:

Theorem D. *Let B_i be the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$, with $i \in \mathbb{N}$. For a prime $q \neq p$, denote by V_i the natural permutation module over $\mathrm{GF}(q)$ corresponding to*

B_i. Then $V_i = V_{0,i} \oplus \cdots \oplus V_{i,i}$, where, for $j = 0, \ldots, i$, $V_{j,i}$ is an absolutely irreducible $\mathrm{GF}(q)B_i$*-module,* $\dim(V_{0,i}) = 1$ *and* $\dim(V_{j,i}) = p^{j-1}(p-1)$.

Chapter 9 illustrates some facts about invariant subgroups of the direct sum of some copies of a homocyclic q-group whose Frattini quotient is absolutely irreducible. The main result, whose proof is modelled on a well-known result for $\mathrm{GF}(q)K$-modules ([14, Thm. 5.5, pg 79]), is the following:

Theorem E. *Let A be a homocyclic q-group of exponent q^α. Let $K \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)K$-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j K-isomorphic to A, for all $j = 1, \ldots, t$. Then all K-subgroups of D which are K-isomorphic to a nontrivial quotient of A can be characterized in terms of some sequences of integers modulo q^α. In particular, for $t = 1$, there are α distinct such subgroups and, for $t > 1$, the number of distinct K-subgroups of D which are K-isomorphic to a nontrivial quotient of A is given by*

$$\frac{q^t - 1}{q - 1} \frac{q^{(t-1)\alpha} - 1}{q^{t-1} - 1}.$$

Details of the above mentioned characterization can be found in Theorem 9.2.4.

In Chapter 10 we classify all minimal parabolic subgroups of G with respect to B which are contained in H and all minimal parabolic systems of H. In particular, the results proved here generalize those from Chapter 7.

The minimal parabolic subgroups of H fall into families, each corresponding to a prime divisor q of $p-1$ and to a module $V_{i,i}$, with $i = 1, \ldots, r-1$. For each choice of q and i, the elements belonging to the corresponding family are in one-to-one correspondence with certain invariant subgroups of the direct product $D_{q,i}$ of $r - i$ copies of a homocyclic q-group $A(q,i)$ whose Frattini quotient is isomorphic to the module $V_{i,i}$. More specifically, every minimal parabolic subgroup P has the form $BR_{q,i}$, where $R_{q,i}$ is a B_i-invariant subgroup of $D_{q,i}$ isomorphic to a nontrivial quotient of $A(q,i)$, with B_i the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$, and so $R_{q,i}$ is completely described by Theorem E. Notice that the subgroups $R_{q,i}$ do not necessarily embed in one of the factors of $D_{q,i}$, but can involve several direct factors. The characterization of the minimal parabolic systems of H then follows as an application of some results from Chapter 9.

For more specific details, the reader should refer to Chapter 10. Here we draw some conclusions about the number of minimal parabolic subgroups and systems of H. We remark that all minimal parabolic systems have the same rank.

Theorem F. *All minimal parabolic subgroups and systems of H with respect to B are known. In particular, there are*

$$\sum_{q\in\pi(p-1)} \alpha_q + \sum_{t=2}^{r-1}\left(\sum_{q\in\pi(p-1)} \frac{q^t-1}{q-1}\,\frac{q^{(t-1)\alpha_q}-1}{q^{t-1}-1}\right)$$

minimal parabolic subgroups, where, for $q \in \pi(p-1)$, q^{α_q} denotes the highest power of q dividing $p-1$, and

$$\prod_{q\in\pi(p-1)}\left(\frac{q^{(r^3/3-r^2+2r/3)(2\alpha_q-1)/2}}{(q-1)^{r(r-1)/2}}\prod_{s=1}^{r-1}\left(\frac{q^s-1}{s}\right)^{r-s}\right)$$

minimal parabolic systems, each of which has rank $|\pi(p-1)|r(r-1)/2$.

Since any group is generated by its minimal parabolic subgroups, Theorem F gives information also about the subgroups of H that contain B. In particular, the lattice of subgroups of H containing B is known (see Figure 1 in Example 6).

Furthermore, since, for $p \geq 3$, all soluble minimal parabolic subgroups of $\mathrm{Sym}(p^r)$ are contained in H (Lemma 6.7.6), from the list of critical cases given in Chapter 6 (see Corollary 6.7.5) and from the work of Lempken, Parker and Rowley for $p = 2$ ([21]), we get

Corollary G. *Let $G = \mathrm{Sym}(n)$ and p be a prime. All the soluble minimal parabolic subgroups of G with respect to the normalizer of a Sylow p-subgroup are known, except when $n = p^{r+1} + p^r$, with $r \geq 1$, and $p = 3$.*

Finally, the characterization of the minimal parabolic subgroups of H given in Chapter 10, together with Theorem E, provides us with a practical method to build all these subgroups and Chapter 11 presents some MAGMA programs that implement this method.

We make a final remark on the use of the Classification of Finite Simple Groups. Throughout the whole work we have attempted to keep the use of the classification to a minimum. However, in proving the maximality of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p)$ in the full symmetric group, and hence whenever we refer to this result, we use the list of minimal normal subgroups of a 2-transitive group, given by Peter Cameron ([4]) using the Classification of Finite Simple Groups.

We conclude this introduction with some examples related to the main results achieved.

Example 4: Sym($p+1$)

Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p+1$ and $p \neq 2, 3$ a prime. Suppose that T is a Sylow p-subgroup of G and B is the normalizer of T in G. Then $T \cong \mathbb{Z}_p$ is also a Sylow p-subgroup of $\mathrm{Sym}(p)$ and B is equal to the normalizer in $\mathrm{Sym}(p)$ of T. Hence, $B \cong \mathrm{Hol}(T)$ is a maximal subgroup of $\mathrm{Sym}(p)$ (see Theorems 5.2.4 and 6.1.2). Therefore, if H is a subgroup of G containing B and H is isomorphic to $\mathrm{Sym}(p)$, then H is a minimal parabolic subgroup of G with respect to B. Now let K be a subgroup of G containing B and isomorphic to $\mathrm{PGL}_2(p)$. Then B is a maximal subgroup of K and so K is a minimal parabolic subgroup of G with respect to B. Moreover, it is possible to show (see Theorem 6.2.2) that any other minimal parabolic subgroup L of G with respect to B is conjugate to either H or K. Hence, since H, K and L all contain the normalizer of a Sylow p-subgroup, L is either H or K.

Thus there are only two minimal parabolic subgroups with respect to B and they are

$$P_1 \cong \mathrm{Sym}(p)$$
$$P_2 \cong \mathrm{PGL}_2(p)$$

Moreover, G has a unique minimal parabolic system $\mathcal{S}$ and $\mathcal{S} = \{P_1, P_2\}$. ■

Example 5: Sym(7^2)

Let $G = \mathrm{Sym}(p^2)$, with $p = 7$. A Sylow p-subgroup T of G can be generated by the elements

$x_1 = (1\ 2\ 3\ 4\ 5\ 6\ 7)$,

$x_2 = (1\ 8\ 15\ 22\ 29\ 36\ 43)(2\ 9\ 16\ 23\ 30\ 37\ 44)(3\ 10\ 17\ 24\ 31\ 38\ 45)(4\ 11\ 18\ 25\ 32\ 39\ 46)$
$(5\ 12\ 19\ 26\ 33\ 40\ 47)(6\ 13\ 20\ 27\ 34\ 41\ 48)(7\ 14\ 21\ 28\ 35\ 42\ 49)$

and, by Corollary 5.2.6, the normalizer B of T in G can be written as $B = T \rtimes \langle h_1, h_2 \rangle \cong 7^7 : 6 : 7 : 6$, where

$$h_1 = (2\ 4\ 3\ 7\ 5\ 6)(9\ 11\ 10\ 14\ 12\ 13)(16\ 18\ 17\ 21\ 19\ 20)(23\ 25\ 24\ 28\ 26\ 27)$$
$$(30\ 32\ 31\ 35\ 33\ 34)(37\ 39\ 38\ 42\ 40\ 41)(44\ 46\ 45\ 49\ 47\ 48),$$
$$h_2 = (8\ 22\ 15\ 43\ 29\ 36)(9\ 23\ 16\ 44\ 30\ 37)(10\ 24\ 17\ 45\ 31\ 38)(11\ 25\ 18\ 46\ 32\ 39)$$
$$(12\ 26\ 19\ 47\ 33\ 40)(13\ 27\ 20\ 48\ 34\ 41)(14\ 28\ 21\ 49\ 35\ 42).$$

Then, by Theorems 7.3.2 and 7.3.5, G has five minimal parabolic subgroups with respect to B, including G itself. Using the notation from the ATLAS ([7]), the proper minimal parabolic subgroups of G can be described as

$$P_1 \cong \mathrm{Alt}(7)^7 : 2 : 7 : 6$$
$$P_2 \cong 7^7 : 2^7 : 3 : 7 : 6$$
$$P_3 \cong 7^7 : 3^7 : 2 : 7 : 6$$
$$P_4 \cong 7^7 : 6 : \mathrm{Sym}(7),$$

where P_2 and P_3 are contained in the wreath product of two copies of $\mathrm{Hol}(\mathbb{Z}_7) \cong 7 : 6$. Furthermore, each of them can be written as $P_i = \langle B, z_i \rangle$, with

$$z_1 = (3\ 4\ 5\ 6\ 7),$$
$$z_2 = (2\ 7)(3\ 6)(4\ 5)(9\ 14)(10\ 13)(11\ 12),$$
$$z_3 = (2\ 3\ 5)(4\ 7\ 6)(9\ 12\ 10)(11\ 13\ 14),$$
$$z_4 = (1\ 8)(2\ 9)(3\ 10)(4\ 11)(5\ 12)(6\ 13)(7\ 14).$$

Finally, G has a unique minimal parabolic system, which is $\{G\}$, since G itself is a minimal parabolic subgroup. ■

Example 6: Sym(3^3)

Let $G = \mathrm{Sym}(p^3)$, with $p = 3$. Let T be a Sylow p-subgroup of G and let

$$x_1 = (1\ 2\ 3),$$
$$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9),$$
$$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$$

be its generators. The normalizer B of T in G can be described as $B = T \rtimes \langle h_1, h_2, h_3 \rangle$, with

$$h_1 = (2\ 3)(5\ 6)(8\ 9)(11\ 12)(14\ 15)(17\ 18)(20\ 21)(23\ 24)(26\ 27),$$
$$h_2 = (4\ 7)(5\ 8)(6\ 9)(13\ 16)(14\ 17)(15\ 18)(22\ 25)(23\ 26)(24\ 27),$$
$$h_3 = (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27).$$

Denote by H a subgroup of G containing T and isomorphic to the wreath product of three copies of $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Then Theorem 10.2.3 implies that there are four minimal parabolic subgroups of H with respect to B and they are

$$P_1 = \langle B, (2\ 3)(5\ 6)(8\ 9)(11\ 12)(14\ 15)(17\ 18) \rangle$$
$$P_2 = \langle B, (2\ 3)(5\ 6) \rangle$$
$$P_3 = \langle B, (4\ 7)(5\ 8)(6\ 9)(13\ 16)(14\ 17)(15\ 18) \rangle$$
$$P_4 = \langle B, (2\ 3)(4\ 7)(5\ 9)(6\ 8)(11\ 12)(13\ 16)(14\ 18)(15\ 17) \rangle.$$

Furthermore, by Corollary 10.3.8, H has three minimal parabolic systems each of rank 3 and they are

$$\{P_1, P_2, P_3\},\ \{P_1, P_2, P_4\},\ \{P_2, P_3, P_4\}.$$

Figure 1, on the next page, shows the lattice of subgroups of H that contain B. Every subgroup is expressed in terms of the minimal parabolic subgroups that generates it. In particular, for $i, j = 1, \ldots, 4$, P_{ij} denotes the subgroup generated by P_i and P_j. Furthermore minimal parabolic subgroups of the same colour belong to the same family, that is, correspond to the same prime divisor q of $p - 1$ and to the same module $V_{i,i}$, with $i = 1, 2$, in the way described in Chapter 10.

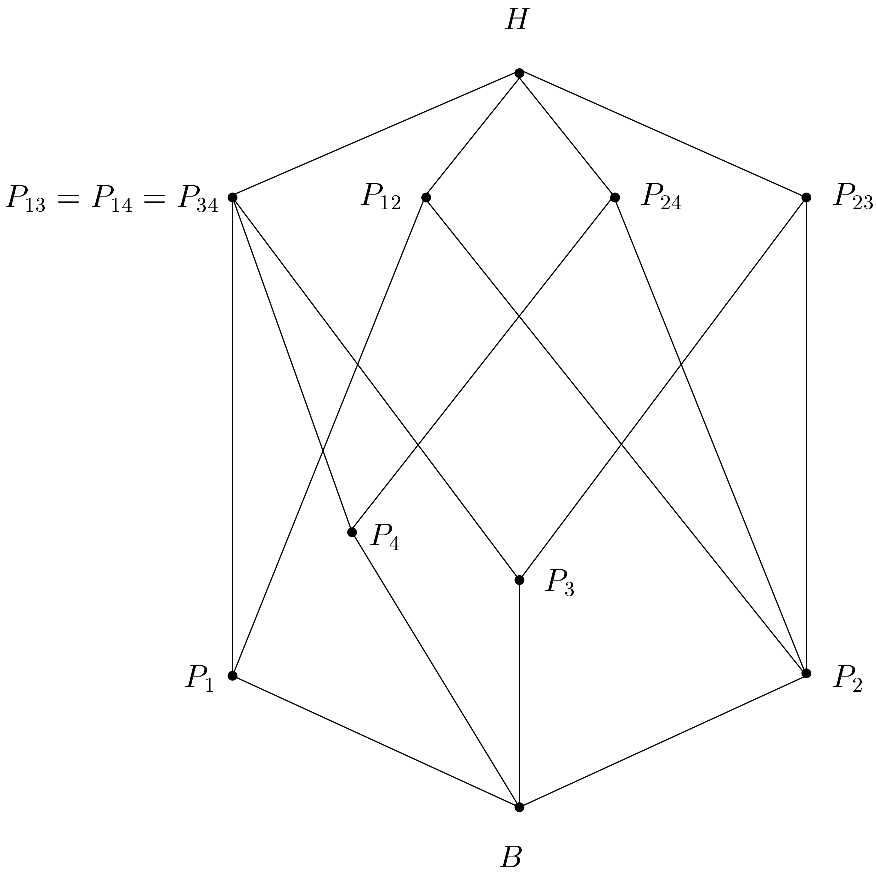

Figure 1: The lattice of subgroups of H containing B

$\blacksquare$

Chapter 1

Preliminaries

In this first chapter, we give a brief description of some concepts and results of general group theory we shall use later. We also introduce the concept of minimal parabolic subgroup and minimal parabolic system ([21]) which is what the present work will be concerned with. We start with Sylow's Theorems ([42]), which are the premise for everything which follows. Recall that all groups considered are finite.

1.1 Sylow's Theorems

Definition 1.1.1. *Let p be a prime and G be a group. If $|G| = p^\alpha m$, with $(p, m) = 1$, then a* **Sylow p-subgroup** *S of G is a subgroup of G of order p^α.*

The set of all Sylow p-subgroups of a group G will be denoted by

$$\mathrm{Syl}_p(G).$$

Theorem 1.1.2 (Sylow's First Theorem). *Let $|G| = p^\alpha m$, with $(p, m) = 1$ and p prime. Then G has a Sylow p-subgroup.*

Theorem 1.1.3 (Sylow's Second Theorem). *Any p-subgroup of G is contained in a Sylow p-subgroup and all Sylow p-subgroups are conjugate in G.*

Theorem 1.1.4 (Sylow's Third Theorem). *The number n_p of Sylow p-subgroups satisfies the following conditions:*

(i) $n_p = |G : N_G(S)|$;

(ii) $n_p \equiv 1 \pmod{p}$; *and*

(iii) $n_p | m$.

The next result provides a very powerful tool when working with Sylow subgroups.

Proposition 1.1.5 (The Frattini argument). *Let G be a group. If $K \trianglelefteq G$ and S is a Sylow p-subgroup of K, then $G = N_G(S)K$.*

Proof. Let $g \in G$. Then $S^g \leqslant K$, since $K \trianglelefteq G$, and so both S and S^g are Sylow p-subgroups of K. Then $S^g = S^k$, for some $k \in K$, and $gk^{-1} \in N_G(S)$, which implies that $g \in N_G(S)K$. □

The following are some useful facts related to Sylow subgroups.

Proposition 1.1.6. *Let S be a Sylow p-subgroup of a group G. If $N_G(S) \leqslant H \leqslant G$, then $H = N_G(H)$. In particular, if $H \trianglelefteq G$, then $H = G$.*

Proof. Set $N = N_G(H)$. Then, by the Frattini argument, we have that $N = HN_N(S) = HN_G(S) = H$, since $N_G(S) \leqslant H$. □

Proposition 1.1.7. *Let G be a group and $S \in \mathrm{Syl}_p(G)$. Let H and K be subgroups of G both containing $N_G(S)$. If $H^g = K$, for some $g \in G$, then $H = K$.*

Proof. Since $S \leqslant H$, we have that $S^g \leqslant H^g = K$. Then S and S^g are both Sylow p-subgroups of K and so there exists $k \in K$ such that $S^{gk} = S$. Hence $gk \in N_G(S) \leqslant K$ and so $g \in K$. Thus $H = H^{gg^{-1}} = K^{g^{-1}} = K$. □

Proposition 1.1.8. *Let G be a group and $S \in \mathrm{Syl}_p(G)$. Suppose that $S \trianglelefteq H \leqslant G$ and $K \leqslant G$. If K normalizes H, then K normalizes S.*

Proof. Let $k \in K$. Since K normalizes H, we have that $S^k \leqslant H$. Thus S^k is a Sylow p-subgroup of H. But, as $S \trianglelefteq H$, H has a unique Sylow p-subgroup. Hence $S^k = S$ and K normalizes S. □

Proposition 1.1.9. *Let G be a group and $S \in \mathrm{Syl}_p(G)$. Set $N = N_G(S)$ and suppose that $G = \langle N, H \rangle$, with $H \leqslant G$. Then $G = N[N, H]$.*

Proof. We shall first show that $N[N,H] \trianglelefteq G$. Propositions [24, 5.1.6 (i)] and [24, 5.1.6 (ii)] tell us that $N^H = \langle N, [N,H] \rangle$ and that $[N,H] \trianglelefteq \langle N, H \rangle$, from which it follows that $N[N,H]$ is a subgroup of G and is normalized by H. Hence $N[N,H] \trianglelefteq \langle N,H \rangle = G$. Then Proposition 1.1.6 implies that $G = N[N,H]$. $\square$

We now want to investigate Sylow subgroups of direct products and their normalizers.

Proposition 1.1.10. *Let G be a group and suppose that $G = A \times B$. Let $S \in \mathrm{Syl}_p(G)$. Then $S = (S \cap A) \times (S \cap B)$ and*

$$N_G(S) = (N_G(S) \cap A) \times (N_G(S) \cap B),$$

with $N_G(S) \cap A = N_A(S \cap A)$ and $N_G(S) \cap B = N_B(S \cap B)$.

Proof. Since A and B are normal subgroups of G, we have that $S \cap A \in \mathrm{Syl}_p(A)$ and $S \cap B \in \mathrm{Syl}_p(B)$ and, by considering the orders, it follows that $S = (S \cap A) \times (S \cap B)$.
But the converse is also true, that is, if $S_A \in \mathrm{Syl}_p(A)$ and $S_B \in \mathrm{Syl}_p(B)$, then $S_A \times S_B \in \mathrm{Syl}_p(G)$. Thus, by Sylow's Third Theorem,

$$|G : N_G(S)| = |A : N_A(S \cap A)||B : N_B(S \cap B)|$$

and so $|N_G(S)| = |N_A(S \cap A)||N_B(S \cap B)|$.
Moreover, as $[A,B] = 1$, $N_A(S \cap A)$ centralizes $S \cap B$ and so $N_A(S \cap A) \leqslant N_G(S) \cap A$. Similarly, $N_B(S \cap B) \leqslant N_G(S) \cap B$. Therefore $N_A(S \cap A) \times N_B(S \cap B) \leqslant N_G(S)$ and, by orders, it follows that $N_G(S) = N_A(S \cap A) \times N_B(S \cap B)$.
Finally, $N_G(S) \cap A$ centralizes $S \cap B$ and normalizes S. Thus, since $S = (S \cap A) \times (S \cap B)$, we must conclude that $N_G(S) \cap A \leqslant N_A(S \cap A)$ and so $N_G(S) \cap A = N_A(S \cap A)$. Similarly, we have that $N_G(S) \cap B = N_B(S \cap B)$, which completes the proof. $\square$

Proposition 1.1.11. *Let G be a group and suppose that $G = A \times B$. Let $S \in \mathrm{Syl}_p(G)$ and let L be a subgroup of G containing $N_G(S)$. Then*

$$L = (L \cap A) \times (L \cap B),$$

with $L \cap A = (N_G(S) \cap A)^L$ and $L \cap B = (N_G(S) \cap B)^L$.

Proof. By Proposition 1.1.10, $N_G(S) = (N_G(S) \cap A) \times (N_G(S) \cap B)$ and, since $N_G(S) \leqslant L$, we have that $N_G(S) = N_L(S)$. Thus $(N_G(S) \cap A)^L \times (N_G(S) \cap B)^L$ is a normal subgroup of L containing $N_L(S)$ and from Proposition 1.1.6 it follows that $L = (N_G(S) \cap A)^L \times (N_G(S) \cap B)^L$. Furthermore $N_G(S) \cap A = N_A(S \cap A) = N_{L\cap A}(S \cap A)$ and so $(N_G(S) \cap A)^L$ is a normal subgroup of $L \cap A$ containing $N_{L\cap A}(S \cap A)$. Therefore, by Proposition 1.1.6, we have that $(N_G(S) \cap A)^L = L \cap A$. Similarly, $(N_G(S) \cap B)^L = L \cap B$ and so $L = (L \cap A) \times (L \cap B)$. □

Corollary 1.1.12. *Let G be a group and suppose that $G = A_1 \times \cdots \times A_n$. Let $S \in \mathrm{Syl}_p(G)$ and let L be a subgroup of G containing $N_G(S)$. Then the following hold:*

(i) $S = (S \cap A_1) \times \cdots \times (S \cap A_n)$*;*

(ii) $N_G(S) = (N_G(S) \cap A_1) \times \cdots \times (N_G(S) \cap A_n)$*;*

(iii) $L = (L \cap A_1) \times \cdots \times (L \cap A_n)$*.*

Last we look at the normalizer of a Sylow p-subgroup of a quotient of G.

Proposition 1.1.13. *Let G be a group, $K \trianglelefteq G$ and $S \in \mathrm{Syl}_p(G)$. Then $N_G(SK) = N_G(S)K$.*

Proof. As $K \trianglelefteq G$, $N_G(S)$ normalizes both S and K and thus SK. So $N_G(S)K \leqslant N_G(SK)$. Conversely, let $N = N_G(SK)$. Then, since $SK \trianglelefteq N$ and $S \in \mathrm{Syl}_p(SK)$, by the Frattini argument, we have that $N = N_N(S)SK = N_N(S)K \leqslant N_G(S)K$ and we get also the other inclusion. □

Proposition 1.1.14. *Let G be a group, $H \leqslant G$ and $K \trianglelefteq G$. Then*

$$N_{G/K}(HK/K) = N_G(HK)/K.$$

Proof. We have that $gK \in N_G(HK)/K$ if and only if $g \in N_G(HK)$, that is, $g^{-1}hg \in HK$, for all $h \in HK$. But this last condition is equivalent to saying that $(g^{-1}hg)K \in HK/K$, for all $h \in HK$, that is, $(g^{-1}K)(hK)(gK) \in HK/K$, for all $hK \in HK/K$, and this happens if and only if $gK \in N_{G/K}(HK/K)$. □

Corollary 1.1.15. *Let G be a group, $K \trianglelefteq G$ and $S \in \mathrm{Syl}_p(G)$. Then*

$$N_{G/K}(SK/K) = N_G(SK)/K = N_G(S)K/K.$$

1.2 The subgroups $O_p(G)$ and $O_{p,q}(G)$

Definition 1.2.1. *Let G be a group and p be a prime. Define the subgroup $O_p(G)$ to be the largest normal subgroup of G whose order is a power of p.*

Notice that the subgroup $O_p(G)$ is well defined. For, if G is a finite group and $A, B \trianglelefteq G$, with $|A|$ and $|B|$ powers of p, then $\langle A, B\rangle = AB \trianglelefteq G$ and $|AB|$ is a power of p, since $|AB| = |A||B|/|A \cap B|$.
Clearly, $O_p(G)$ is a characteristic subgroup of G. Furthermore $O_p(G)$ can be characterized in terms of the Sylow p-subgroups of G.

Proposition 1.2.2. *Let G be a group and p be a prime. Then $O_p(G)$ is equal to the intersection of all the Sylow p-subgroups of G.*

Proof. Let K denote the intersection of all Sylow p-subgroups of G. Then K is a p-group and $K \trianglelefteq G$, since Sylow p-subgroups are all conjugate. Hence $K \leqslant O_p(G)$.
Conversely, by definition, $O_p(G)$ is a p-group and so there exists $S \in \mathrm{Syl}_p(G)$ such that $O_p(G) \leqslant S$. But $O_p(G)$ is also normal in G. Therefore $O_p(G) \leqslant S^g$, for all $g \in G$, and, since Sylow p-subgroups are all conjugate, we have that $O_p(G) \leqslant K$. $\square$

Definition 1.2.3. *Let G be a group and let p and q be primes. Define the subgroup $O_{p,q}(G)$ to be the preimage in G of the group $O_q(G/O_p(G))$, that is,*

$$O_{p,q}(G)/O_p(G) = O_q(G/O_p(G)).$$

1.3 The Frattini and p-Frattini subgroups

Definition 1.3.1. *Let G be a group. The* **Frattini subgroup** *of G, denoted by $\Phi(G)$, is defined to be the intersection of all the maximal subgroups of G.*

Notice that the Frattini subgroup is a characteristic subgroup.
One of the most remarkable properties of the Frattini subgroup is the following:

Proposition 1.3.2. *Let G be a group and $X \subseteq G$. If $G = \langle X, \Phi(G)\rangle$, then $G = \langle X\rangle$.*

Proof. Let $X \subseteq G$ and suppose that $G \neq \langle X \rangle$. Then there exists a maximal subgroup M of G such that $\langle X \rangle \leqslant M$. But, by definition, $\Phi(G) \leqslant M$ and so $G = \langle X, \Phi(G) \rangle \leqslant M < G$. Therefore we must have that $G = \langle X \rangle$. $\square$

Definition 1.3.3. *Let G be a group and let p be a prime. Define the* p**-Frattini subgroup** *$\Phi_p(G)$ of G as the preimage of the Frattini subgroup of $G/O_p(G)$, that is,*

$$\Phi_p(G)/O_p(G) = \Phi(G/O_p(G)).$$

So $\Phi_p(G)$ is the intersection of all maximal subgroups of G which contain $O_p(G)$.
The next result extends the idea of Proposition 1.3.2 to the subgroup $\Phi_p(G)$.

Proposition 1.3.4. *Let G be a group and let p be a prime. Let $X \subseteq G$ and suppose that $G = \langle X, \Phi_p(G) \rangle$. Then $G = \langle X, O_p(G) \rangle$.*

Proof. Let $X \subseteq G$ and suppose that $G = \langle X, \Phi_p(G) \rangle$. Then

$$G/O_p(G) = \langle X, \Phi_p(G) \rangle / O_p(G) = \langle X, O_p(G) \rangle / O_p(G) \Phi(G/O_p(G))$$

and so, by Proposition 1.3.2, $G/O_p(G) = \langle X, O_p(G) \rangle / O_p(G)$, that is, $G = \langle X, O_p(G) \rangle$. $\square$

The Frattini subgroup of a group of prime power order can be characterized as follows:

Proposition 1.3.5. *Let G be a p-group, with p prime. Then $\Phi(G)$ is the smallest normal subgroup H of G such that G/H is elementary abelian.*

Proof. Let M be a maximal subgroup of G. Then, since G is nilpotent, $M \trianglelefteq G$ by [24, 5.2.4]. Furthermore $G/M \cong \mathbb{Z}_p$. In particular, $[G, G] \leqslant M$ and so $G/\Phi(G)$ is abelian. Now let $x \in G$. Then $x^p M = (xM)^p = M$ and so $x^p \in M$. Hence $x^p \in \Phi(G)$, that is, $(x\Phi(G))^p = \Phi(G)$, and so $G/\Phi(G)$ is elementary abelian.
Conversely, let $H \trianglelefteq G$ such that G/H is elementary abelian. Set $\bar{G} = G/H$. Then $\bar{G} = \bar{G}_1 \times \cdots \times \bar{G}_n$, with $\bar{G}_i \cong \mathbb{Z}_p$, for $i = 1, \ldots, n$. Set $H_i = \langle G_j \mid j \neq i \rangle$. Then

$$|G : H_i| = |\bar{G} : \prod_{j \neq i} \bar{G}_j| = p.$$

Therefore H_i is a maximal subgroup of G. But $H = \bigcap_{i=1}^n H_i$, that is, H is the intersection of some maximal subgroups of G. Hence $\Phi(G) \leqslant H$ and the proof is complete. $\square$

Proposition 1.3.5 implies, in particular, that, if G is p-group, then $G/\Phi(G)$ can be regarded as a GF(p)-module.

Proposition 1.3.6. *Let G be a p-group, with p prime. If G is abelian, then $\Phi(G) = G^p$, where $G^p = \langle g^p \mid g \in G\rangle$.*

Proof. Let $g \in G$. Since $G/\Phi(G)$ is an elementary abelian p-group, we have that $(g\Phi(G))^p = g^p\Phi(G) = \Phi(G)$. Hence $g^p \in \Phi(G)$ and $G^p \leqslant \Phi(G)$.
Conversely, take the quotient G/G^p. Since G is abelian, so is G/G^p. Also $(gG^p)^p = g^pG^p = G^p$, for all $g \in G$, and so G/G^p is an elementary abelian p-group. Therefore, by Proposition 1.3.5 it follows that $\Phi(G) \leqslant G^p$ and so the result is proved. □

Proposition 1.3.7. *Let G be a homocyclic p-group of exponent p^t, for some prime p. Then $\Phi(G)$ is equal to the set $\{g \in G \mid \mathrm{o}(g) \leq p^{t-1}\}$.*

Proof. Set $X = \{g \in G \mid \mathrm{o}(g) \leq p^{t-1}\}$. We shall prove that $X = G^p$.
Let $g \in G$. Then $(g^p)^{p^{t-1}} = g^{p^t} = 1$, since G has exponent p^t. Hence $g^p \in X$ and $G^p \subseteq X$.
Conversely, let $g \in X$. By assumption, G is homocyclic of exponent p^t, so $G = \langle g_1\rangle \times \cdots \times \langle g_n\rangle$, with $\mathrm{o}(g_i) = p^t$, for all $i = 1, \ldots, n$. Then $g = g_1^{\alpha_1} \ldots g_n^{\alpha_n}$, where, for $i = 1, \ldots, n$, $1 \leq \alpha_i \leq p^t$. But, since $\mathrm{o}(g) \leq p^{t-1}$, we must have that p divides α_i, for all $i = 1, \ldots, n$. Therefore

$$g = g_1^{p\beta_1} \ldots g_n^{p\beta_n} = (g_1^{\beta_1} \ldots g_n^{\beta_n})^p$$

and so $g \in G^p$. □

Definition 1.3.8. *Let G be an abelian p-group of exponent p^t, for some prime p. The* **Frattini series** *of G is the series*

$$1 = \Phi^t(G) \trianglelefteq \Phi^{t-1}(G) \trianglelefteq \ldots \trianglelefteq \Phi^1(G) \trianglelefteq \Phi^0(G) = G,$$

where $\Phi^0(G) = G$ and, for $k = 1, \ldots, t$, $\Phi^k(G) = \Phi(\Phi^{k-1}(G))$.

Notice that, for $k = 1, \ldots, t$, $\Phi^k(G) = G^{p^k}$, by Proposition 1.3.6. Also, if G is homocyclic, then Proposition 1.3.7 implies that $\Phi^k(G) = \{g \in G \mid \mathrm{o}(g) \leq p^{t-k}\}$.
The Frattini series can be defined more generally for any group G. If G is finite, then the series always reaches the trivial subgroup, since $\Phi(G) < G$ and so at each step we get a smaller subgroup. However we do not know how many terms there are. On the contrary, if G is infinite, then the Frattini series of G does not necessarily terminate.

Proposition 1.3.9. *Let G be a homocyclic p-group of exponent p^t, for some prime p. Let $H \leqslant \mathrm{Aut}(G)$ and K be a H-invariant subgroup of G of exponent p^{t-k}, for some fixed $k = 0, \ldots, t-1$. Then, for all $r = 0, \ldots, t-k-1$,*

$$K/(K \cap \Phi^{k+1}(G)) \cong K^{p^r}/(K^{p^r} \cap \Phi^{k+1+r}(G)),$$

as $\mathrm{GF}(p)H$*-modules.*

Proof. For $e = 0, \ldots, t$, set $F_e = \Phi^e(G)$. By Proposition 1.3.6, we have that $F_e = (F_{e-1})^p$, for all $e = 1, \ldots, t$. Therefore it is enough to prove the result for $r = 1$. Notice also that, since K has exponent p^{t-k}, we have that $K \leqslant F_k$ and $K \nleqslant F_{k+1}$.
So assume that $r = 1$ and define the map

$$\begin{aligned} \psi\colon K/(K \cap F_{k+1}) &\longrightarrow K^p/(K^p \cap F_{k+2}) \\ x(K \cap F_{k+1}) &\longmapsto x^p(K^p \cap F_{k+2}). \end{aligned}$$

First ψ is well defined. In fact let $x_1(K \cap F_{k+1}) = x_2(K \cap F_{k+1})$, with $x_1, x_2 \in K$. Then $x_1 = x_2 y$, for some $y \in K \cap F_{k+1}$, and $x_1^p(K^p \cap F_{k+2}) = x_2^p y^p (K^p \cap F_{k+2}) = x_2^p(K^p \cap F_{k+2})$, since K is abelian and, for $y \in K \cap F_{k+1}$, we have $y^p \in K^p \cap F_{k+2}$. Hence $\psi(x_1(K \cap F_{k+1})) = \psi(x_2(K \cap F_{k+1}))$.
Next we show that ψ is a group homomorphism. Let $x_1, x_2 \in K$. Then, since K is abelian, we have that $(x_1x_2)^p(K^p \cap F_{k+2}) = x_1^p x_2^p (K^p \cap F_{k+2}) = x_1^p(K^p \cap F_{k+2}) x_2^p (K^p \cap F_{k+2})$ and so $\psi(x_1^p(K^p \cap F_{k+2})x_2^p(K^p \cap F_{k+2})) = \psi(x_1^p(K^p \cap F_{k+2}))\psi(x_2^p(K^p \cap F_{k+2}))$.
Furthermore ψ is one-to-one. In fact let $x(K \cap F_{k+1}) \in \ker \psi$. Then $x^p \in K^p \cap F_{k+2}$. In particular, $x^p \in F_{k+2}$, which implies that $x^{p^{t-k-1}} = (x^p)^{p^{t-k-2}} = 1$. But, by Proposition 1.3.7, $F_{k+1} = \{g \in G \mid \mathrm{o}(g) \leq p^{t-k-1}\}$. So $x \in F_{k+1}$ and $x(K \cap F_{k+1}) = K \cap F_{k+1}$.
From the definition of K^p and from K being abelian it follows that ψ is onto. But clearly ψ is invariant under the action of H, since $H \leqslant \mathrm{Aut}(G)$, and is invariant under scalar multiplication, since, for $\lambda \in \mathrm{GF}(p)$ and $x \in K$, λx is defined to be x^λ. Therefore ψ is a module isomorphism between the $\mathrm{GF}(p)H$-modules $K/(K \cap F_{k+1})$ and $K^p/(K^p \cap F_{k+2})$. $\square$

Corollary 1.3.10. *Let G be a homocyclic p-group of exponent p^t, for some prime p. Suppose that $H \leqslant \mathrm{Aut}(G)$. Then the factors of the Frattini series of G are all isomorphic as* $\mathrm{GF}(p)H$*-modules. In particular, if $G/\Phi(G)$ is an irreducible* $\mathrm{GF}(p)H$*-module, then the Frattini series of G is a G-composition series.*

Proof. Set $K = G$. Then $K^{p^r} = G^{p^r} = \Phi^r(G)$, for all $r = 0, \dots, t$, and the result follows from Proposition 1.3.9. □

Proposition 1.3.11. *Let G be a homocyclic p-group of exponent p^t, for some prime p. Let $H \leqslant \mathrm{Aut}(G)$ and assume that $G/\Phi(G)$ is an irreducible $\mathrm{GF}(p)H$-module. Then any H-subgroup K of G is equal to $\Phi^k(G)$, for some $k = 0, \dots, t$. In particular, K is H-isomorphic to a quotient of G, namely $G/\Phi^{t-k}(G)$.*

Proof. Let K be a H-subgroup of G and suppose that K has exponent p^{t-k}, for some $k = 0, \dots, t$. Then $K \leqslant \Phi^k(G)$ and $K \nleqslant \Phi^{k+1}(G)$. Therefore $K\Phi^{k+1}(G)/\Phi^{k+1}(G)$ is a nontrivial H-subgroup of $\Phi^k(G)/\Phi^{k+1}(G)$ and, since, by Corollary 1.3.10, $\Phi^k(G)/\Phi^{k+1}(G)$ is irreducible, we must have $K\Phi^{k+1}(G) = \Phi^k(G)$. But $\Phi^{k+1}(G) = \Phi(\Phi^k(G))$ and so, by Proposition 1.3.2, we get that $K = \Phi^k(G) = G^{p^k}$. In particular, K is H-isomorphic to the quotient $G/\Phi^{t-k}(G)$ via the map

$$\tau_k \colon g \in G \longmapsto g^{p^k} \in G.$$

□

1.4 Minimal parabolic subgroups and systems

Definition 1.4.1. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing the order of G. Then a subgroup P of G which properly contains B is called a* **minimal parabolic subgroup** *of G with respect to B if B is contained in a unique maximal subgroup of P.*

We shall denote by $\mathcal{M}(G, B)$ the collection of all minimal parabolic subgroups of G with respect to B.

Lemma 1.4.2. *Let G be a group, p a prime dividing the order of G and B the normalizer in G of a Sylow p-subgroup. Suppose that P is a minimal parabolic subgroup of G with respect to B and let U be the unique maximal subgroup of P containing B. Then, for all $z \in P \setminus U$, $P = \langle B, z \rangle$.*

Proof. Choose $z \in P \setminus U$. Then $B < \langle B, z \rangle \leqslant P$ and $\langle B, z \rangle \nleqslant U$. Thus, U being the unique maximal subgroup of P containing B, $\langle B, z \rangle$ must be equal to P. □

Proposition 1.4.3. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing $|G|$. Then G is generated by its minimal parabolic subgroups with respect to B.*

Proof. Let $M = \langle P \mid P \in \mathcal{M}(G,B)\rangle$. By way of a contradiction suppose that $G \neq M$ and that G is a minimal counterexample. This implies, in particular, that G is not a minimal parabolic subgroup with respect to B. Then there exist H and K distinct maximal subgroups of G containing B. Since H and K are proper subgroups of G, from the choice of G it follows that $H = \langle P \mid P \in \mathcal{M}(H,B)\rangle$ and $K = \langle P \mid P \in \mathcal{M}(K,B)\rangle$. Thus $H, K \leqslant M$ which implies that $G = \langle H, K\rangle \leqslant M$, contradicting our assumption. $\square$

Proposition 1.4.3 justifies the following definition.

Definition 1.4.4. *Let $P_1, \ldots, P_m \in \mathcal{M}(G,B)$. Then $\mathcal{S} = \{P_1, \ldots, P_m\}$ is called a* **minimal parabolic system** *of G of rank m if $G = \langle \mathcal{S}\rangle$ and no proper subset of $\mathcal{S}$ generates G.*

Theorem 1.4.5. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing the order of G. If G is a minimal parabolic subgroup with respect to B, then there is a unique minimal parabolic system $\mathcal{S}$ of G and $\mathcal{S} = \{G\}$.*

Proof. Let U be the unique maximal subgroup of G containing the normalizer B. Then every proper subgroup of G containing B is contained in U. In particular, all minimal parabolic subgroups different from G are contained in U and so they cannot generate G. Hence every collection of minimal parabolic subgroups which generates G must contain G itself, which implies that $\{G\}$ is the unique minimal parabolic system for G. $\square$

Lemma 1.4.6. ([21]) *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing the order of G. If $P \in \mathcal{M}(G,B)$ and $K \trianglelefteq P$, then either*

(i) *$KB = P$; or*

(ii) *$T \cap K \trianglelefteq P$.*

In particular, if $N_K(T \cap K) = B \cap K$, then either $K \leqslant B$ or $KB = P$.

Proof. Set $T_K = T \cap K$. Then $T_K \in \mathrm{Syl}_p(K)$ and, by the Frattini argument, we have that $P = KN_P(T_K)$. Now $T_K \trianglelefteq B$, so $B \leqslant N_P(T_K)$. Thus, as $P \in \mathcal{M}(G,B)$, either $N_P(T_K) = P$, that is, $T_K \trianglelefteq P$ and case (ii) holds, or $N_P(T_K) \leqslant U$, where U is the unique maximal subgroup

of P containing B. So assume that $N_P(T_K) \leqslant U$. Since $P \neq U$, this implies that $K \nleqslant U$ and, in particular, $KB \nleqslant U$. But $B \leqslant KB$. Hence $KB = P$ and (i) holds.
Assume now that $N_K(T_K) = B \cap K$. If $KB \neq P$, then, by the first part of the lemma, we must have that $T_K \trianglelefteq P$ and, in particular, $T_K \trianglelefteq K$. Hence $K = N_K(T_K) = B \cap K$ and $K \leqslant B$. □

Next we shall look at the image in a quotient of G of a minimal parabolic subgroup of G with respect to B.

Lemma 1.4.7. *Let G be a group, $K \trianglelefteq G$ and $T \in \mathrm{Syl}_p(G)$. Set $B = N_G(T)$ and suppose that $P \in \mathcal{M}(G,B)$. Then either $PK/K = BK/K$, which is the normalizer in G/K of a Sylow p-subgroup, or PK/K is a minimal parabolic subgroup of G/K with respect to BK/K.*

Proof. First notice that, by Corollary 1.1.15, BK/K is equal to the normalizer in G/K of a Sylow p-subgroup of G/K, namely TK/K, and, as $B \leqslant P$, we have that $BK/K \leqslant PK/K \leqslant G/K$. Now suppose that $BK/K \neq PK/K$ and, in order to find a contradiction, suppose that PK/K is not a minimal parabolic subgroup of G/K with respect to BK/K. Since $PK/K \cong P/(P \cap K)$, this is equivalent to saying that $P/(P \cap K)$ is not a minimal parabolic subgroup with respect to $B(P \cap K)/(P \cap K)$. So there exist P_1 and P_2, distinct maximal subgroups of P properly containing $B(P \cap K)$ and therefore properly containing B, which contradicts the fact that P is a minimal parabolic subgroup with respect to B. □

Proposition 1.4.8. *Let G be a group, $K \trianglelefteq G$ and $T \in \mathrm{Syl}_p(G)$. Set $B = N_G(T)$. Let $P \in \mathcal{M}(G,B)$ and suppose that PK/K is a minimal parabolic subgroup of G/K with respect to BK/K. Then the unique maximal subgroup of PK/K containing the normalizer BK/K is UK/K, with U unique maximal subgroup of G containing B. In particular, $P \cap K = U \cap K$.*

Proof. Let $K \trianglelefteq G$ and let $P \in \mathcal{M}(G,B)$. Set $L = P \cap K \trianglelefteq P$ and denote by U the unique maximal subgroup of P containing B. Then $P/L \cong PK/K$ is a minimal parabolic subgroup with respect to $BL/L \cong B/B \cap L = B/B \cap K \cong BK/K$. We shall prove that the unique maximal subgroup of P/L containing BL/L is U/L.
Let P_1/L be the unique maximal subgroup of P/L containing BL/L. Then P_1 is a maximal subgroup of P containing BL and thus B. Therefore $P_1 = U$, that is, $P_1/L = U/L$, and,

in particular, $L = P \cap K \leqslant U$, which implies that $P \cap K = L = U \cap K$. Hence $UK/K \cong U/U \cap K = U/L$ is the unique maximal subgroup of PK/K containing BK/K. $\square$

Proposition 1.4.9. *Let G be a group, $K \trianglelefteq G$ and $T \in \mathrm{Syl}_p(G)$. Set $B = N_G(T)$ and suppose that $P \in \mathcal{M}(G, B)$. Then PK/K is a minimal parabolic subgroup of G/K with respect to BK/K if and only if $P \cap K = U \cap K$, with U unique maximal subgroup of G containing B. In particular, if $P \cap K = B \cap K$, then $PK/K \in \mathcal{M}(G/K, BK/K)$.*

Proof. Let $P \in \mathcal{M}(G, B)$ and denote by U the unique maximal subgroup of P containing B. Let $K \trianglelefteq G$ and suppose that $PK/K \in \mathcal{M}(G/K, BK/K)$. Then, by Proposition 1.4.8, $P \cap K = U \cap K$. Conversely, suppose that $P \cap K = U \cap K$ and assume that PK/K is not a minimal parabolic subgroup of G/K with respect to BK/K. Then, by Lemma 1.4.7, we have that $PK/K = BK/K$, which implies, since $B \leqslant U < P$, that $PK/K = UK/K$. Therefore $P/P \cap K \cong U/U \cap K$ and so, as $P \cap K = U \cap K$, we have that $P/P \cap K = U/P \cap K$, that is, $P = U$, which is a contradiction. $\square$

We shall conclude this section by presenting some factorizations of minimal parabolic subgroups.

Lemma 1.4.10. ([21]) *Let G be a group and suppose that $G = X \times Y$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Suppose that P is a subgroup of G containing B. Then $P \in \mathcal{M}(G, B)$ if and only if $P = (B \cap X) \times (P \cap Y)$, with $P \cap Y \in \mathcal{M}(Y, B \cap Y)$, or $P = (P \cap X) \times (B \cap Y)$, with $P \cap X \in \mathcal{M}(X, B \cap X)$.*

Proof. Suppose that $P \in \mathcal{M}(G, B)$ and denote by U the unique maximal subgroup of P containing B. By Proposition 1.1.11 we have that $P = (P \cap X) \times (P \cap Y)$, with $P \cap X = (B \cap X)^P$ and $P \cap Y = (B \cap Y)^P$. If $B \cap X < P \cap X$ and $B \cap Y < P \cap Y$, that is, if P normalizes neither $B \cap X$ nor $B \cap Y$, then U contains the subgroups $(P \cap X) \times (B \cap Y)$ and $(B \cap X) \times (P \cap Y)$ and thus U contains $P = (P \cap X) \times (P \cap Y)$, which is a contradiction. Hence either $B \cap X = P \cap X$ and so $P = (B \cap X) \times (P \cap Y)$, or $B \cap Y = P \cap Y$ and $P = (P \cap X) \times (B \cap Y)$.

Suppose that $P = (B \cap X) \times (P \cap Y)$. We want to show that $P \cap Y \in \mathcal{M}(Y, B \cap Y)$. First recall, from Proposition 1.1.10, that $T \cap Y \in \mathrm{Syl}_p(Y)$ and that $B \cap Y = N_Y(T \cap Y)$. So $P \cap Y$ is a subgroup of Y containing the normalizer of a Sylow p-subgroup. Furthermore

every maximal subgroup M_Y of $P \cap Y$ containing $B \cap Y$ determines a maximal subgroup of P containing B, namely the subgroup $(B \cap X) \times M_Y$. Hence, since $P \in \mathcal{M}(G, B)$, there is a unique maximal subgroup of $P \cap Y$ containing $B \cap Y$ and $P \cap Y \in \mathcal{M}(Y, B \cap Y)$.
Conversely, let $P_Y \in \mathcal{M}(Y, B \cap Y)$ and set $P = (B \cap X) \times P_Y$. Then $B = (B \cap X) \times (B \cap Y) \leqslant P$. Moreover, if M is a maximal subgroup of P containing B, then, by Dedekind's Modular Law, $M = M \cap P = (B \cap X) \times (M \cap P_Y)$, with $M \cap P_Y$ maximal subgroup of P_Y containing $B \cap Y$. Therefore $P_Y \in \mathcal{M}(Y, B \cap Y)$ implies that $P \in \mathcal{M}(G, B)$. □

Corollary 1.4.11. ([21]) *Let G be a group and suppose that $G = X_1 \times \cdots \times X_n$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Let P be a subgroup of G containing B. Then $P \in \mathcal{M}(G, B)$ if and only if $P = (P \cap X_j) \times \prod_{i \neq j} (B \cap X_i)$, for some $j = 1, \ldots, n$, with $P \cap X_j \in \mathcal{M}(X_j, B \cap X_j)$.*

Proposition 1.4.12. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let $P \in \mathcal{M}(G, B)$ and suppose that $P = BR$, with $B \cap R = 1$. Then $R \neq \langle R_1, R_2 \rangle$, for any R_1, R_2 proper B-invariant subgroups of R, that is, R has a unique maximal B-invariant subgroup. In particular, if $R \trianglelefteq P$, then the unique maximal B-invariant subgroup of R is $R \cap U$, where U is the unique maximal subgroup of P containing B.*

Proof. Let R_1 and R_2 be proper B-invariant subgroups of R and suppose that $R = \langle R_1, R_2 \rangle$. Consider the subgroup BR_1. From $B \cap R = 1$, it follows that $B \cap R_1 = 1$. Therefore $|BR_1| = |B||R_1|$ and so $BR_1 \neq P$, for otherwise we would have $R_1 = R$. Similarly, we get that $BR_2 \neq P$. Hence $BR_1, BR_2 \leqslant U$, where U is the unique maximal subgroup of P containing B. But this yields the contradiction $P = BR = \langle BR_1, BR_2 \rangle \leqslant U$. Therefore we must have $R \neq \langle R_1, R_2 \rangle$ and R has a unique maximal B-invariant subgroup.
Now suppose that $R \trianglelefteq P$. Set $R_0 = R \cap U$, with U unique maximal subgroup of P containing B. Then R_0 is B-invariant. Let M be a B-invariant subgroup of R properly containing R_0. Then $M \nleqslant U$, for otherwise $M \leqslant R \cap U = R_0$. Therefore $BM = P$ and so $R = R \cap P = R \cap (BM) = (R \cap B)M = M$. Hence $R = M$ and R_0 is the unique maximal B-invariant subgroup of R. □

Proposition 1.4.13. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let $P \in \mathcal{M}(G, B)$ and suppose that $P = BR$, with $B \cap R = 1$. Let R_0 be a proper B-invariant normal subgroup of R. If $S \trianglelefteq B$ such that $S \leqslant T$ and $[R, S] \leqslant R_0$, then $S \trianglelefteq P$; in particular, $[R, S] = 1$.*

Proof. Since $T \leqslant B$ and $B \cap R = 1$, we have that R is a p'-group. Also R is normalized by S, since $[R, S] \leqslant R_0 \leqslant R$. Hence from [1, 18.7] it follows that

$$C_R(S)R_0/R_0 = C_{R/R_0}(S).$$

But, because $[R, S] \leqslant R_0$, the latter is equal to R/R_0, which implies that $R = C_R(S)R_0$. Now let U denote the unique maximal subgroup of P containing B. Then, because R_0 is a proper B-invariant subgroup of R, we have that $R_0 \leqslant U$. Therefore $C_R(S) \nleqslant U$, for otherwise $C_R(S)R_0 = R \leqslant U$ implying $P \leqslant U$. Then $\langle B, x\rangle = P$, for all $x \in C_R(S)$ such that $x \notin U$, and so $S \trianglelefteq P$. In particular, this implies that $[R, S] \leqslant R \cap S$. But R is a p'-group and $S \leqslant T$, so $R \cap S = 1$. Hence $[R, S] = 1$. $\square$

Proposition 1.4.14. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing the order of G. Let $P \in \mathcal{M}(G, B)$ and suppose that $P = BR$, where R is B-invariant and $R/O_p(R)$ is nilpotent. Then $P = BO_{p,q}(R)$, for some uniquely determined prime $q \in \pi(R) \setminus \{p\}$.*

Proof. By hypothesis $R/O_p(R)$ is nilpotent and so

$$R/O_p(R) = \prod_{t \in \pi(R/O_p(R))} O_t(R/O_p(R)) = \prod_{t \in \pi(R/O_p(R))} (O_{p,t}(R)/O_p(R)).$$

Therefore

$$R = \prod_{t \in \pi(R/O_p(R))} O_{p,t}(R).$$

Let U be the unique maximal subgroup of P containing B. Since $P = BR$, we have that $R \nleqslant U$. Hence there exists $q \in \pi(R)$, $q \neq p$, such that $O_{p,q}(R) \nleqslant U$. Then $P = BO_{p,q}(R)$. Moreover $|P : B| = |O_{p,q}(R) : B \cap O_{p,q}(R)|$ is a q-power, which implies, in particular, that q is uniquely determined. $\square$

Proposition 1.4.15. *Let G be a group, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime dividing the order of G. Let $P \leqslant G$ such that $B < P$. Suppose that $P = BR$, with $R \trianglelefteq P$, and that $R/\Phi_p(R)$ has no nontrivial proper B-invariant subgroup. Then $P \in \mathcal{M}(G, B)$ and $B\Phi_p(R)$ is the unique maximal subgroup of P containing B.*

Proof. First notice that $\Phi_p(R)$ is a characteristic subgroup of R and so $\Phi_p(R) \trianglelefteq P$.
Set $U = B\Phi_p(R)$. We shall prove that U is the unique maximal subgroup of P containing B.
First, U is a proper subgroup of P. For, if $U = P$, then, by Proposition 1.3.4, $R = R \cap P = R \cap B\Phi_p(R) = (R \cap B)\Phi_p(R) = (R \cap B)O_p(R) = R \cap B$, since $O_p(R) \leqslant R \cap B$, and we would have that $P = B$.
Now let $M \leqslant P$ such that $B \leqslant M$. By Dedekind's Modular Law, we have that

$$M = M \cap P = M \cap (BR) = B(M \cap R).$$

Consider the subgroup $(M \cap R)\Phi_p(R)$. This is a B-invariant subgroup of R containing $\Phi_p(R)$. Therefore, since $R/\Phi_p(R)$ has no nontrivial proper B-invariant subgroup, it is either $\Phi_p(R) = (M \cap R)\Phi_p(R)$ or $R = (M \cap R)\Phi_p(R)$.
If $\Phi_p(R) = (M \cap R)\Phi_p(R)$, then $M \cap R \leqslant \Phi_p(R)$ and $M \leqslant U$. If $R = (M \cap R)\Phi_p(R)$, then, by Proposition 1.3.4, $R = (M \cap R)O_p(R) = M \cap R$ and so $M = P$. Hence, either $M \leqslant U$ or $M = P$, which says that U is the unique maximal subgroup of P containing B. $\square$

Chapter 2

Finite permutation groups

We introduce finite permutation groups and their basic properties, for which the main reference will be ([41]). Some related concepts are also illustrated, like the holomorph of a group, which is proved to be the normalizer of a regular permutation group, and wreath products ([15]), which will be used later to describe the structure of the Sylow p-subgroups of the symmetric group and of the stabilizer of a block system.

2.1 Introduction

Let Ω be a finite set and suppose that $|\Omega| = n$. We shall denote by

$$\mathrm{Sym}(\Omega) \quad \text{or} \quad \mathrm{Sym}(n)$$

the **symmetric group** on Ω and by

$$\mathrm{Alt}(\Omega) \quad \text{or} \quad \mathrm{Alt}(n)$$

the **alternating group** on Ω. Recall that $\mathrm{Alt}(n)$ is a normal subgroup of $\mathrm{Sym}(n)$ of index 2. Furthermore, by [23], for $n \geq 5$, every element of $\mathrm{Alt}(n)$ is a commutator of elements in $\mathrm{Sym}(n)$ and so, in particular, $\mathrm{Alt}(n)$ is equal to the commutator subgroup of $\mathrm{Sym}(n)$.
The subgroups of $\mathrm{Sym}(\Omega)$ will be called **permutation groups** on Ω.
The **degree** of a permutation group $G \neq 1$ is the number of points moved by G and is denoted by $\deg G$. The **degree** of a permutation $g \neq 1$ is the degree of the cyclic group $\langle g \rangle$ generated by g.

Finally, for $\Delta \subseteq \Omega$ and $K \subseteq \mathrm{Sym}(\Omega)$, we denote by Δ^K the set

$$\{\delta^k \mid \delta \in \Delta, k \in K\}.$$

Definition 2.1.1. *Let G be a permutation group on Ω. A subset Δ of Ω is a* **fixed block** *of G or is* **fixed** *by G if $\Delta^G = \Delta$.*

If Δ is a fixed block of G, then the restriction g^Δ of an element $g \in G$ to Δ is a permutation on Δ and the set

$$G^\Delta = \{g^\Delta \mid g \in G\}$$

is a permutation group on Δ, called the **constituent** of G on Δ. Also the mapping $\phi\colon g \to g^\Delta$ is a homomorphism of G onto G^Δ. If ϕ is an isomorphism, then G^Δ is called **faithful**. Clearly, the intersection and the union of two fixed blocks of G are again fixed by G and, for every set $\Delta \subseteq \Omega$, Δ^G is the smallest fixed block of G containing Δ. Also every permutation group G has the trivial fixed blocks $\emptyset$ and Ω.

Definition 2.1.2. *A permutation group G on Ω is called* **transitive** *if its only fixed blocks are $\emptyset$ and Ω. Otherwise G is called* **intransitive**.

Definition 2.1.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ and let $\emptyset \neq \Delta \subseteq \Omega$. Then Δ is called an* **orbit** *of G on Ω if Δ is a minimal fixed block of G. The order of Δ is called the* **length** *of the orbit.*

The orbit of G containing the point $\alpha \in \Omega$ is denoted by α^G and is equal to $\{\alpha^g \mid g \in G\}$. Notice that, if Δ is an orbit of G on Ω, then the constituent G^Δ is transitive on Ω. In particular, G is transitive on each of its orbits.

Proposition 2.1.4. *If Δ is an orbit of G and $\pi \in \mathrm{Sym}(\Omega)$, then Δ^π is an orbit of $\pi^{-1}G\pi$.*

Finally notice that the orbits of G on Ω arise also as equivalence classes of the relation $\sim$ defined by $\alpha \sim \beta$ if and only if there exists $g \in G$ such that $\alpha^g = \beta$, for all $\alpha, \beta \in \Omega$. This implies, in particular, that they form a partition of Ω.

Definition 2.1.5. *Let $G \leqslant \mathrm{Sym}(\Omega)$ and $\Delta \subseteq \Omega$. The set*

$$G_\Delta = \{g \in G \mid \delta^g = \delta, \text{ for all } \delta \in \Delta\}$$

of elements of G which fix each point of Δ forms a subgroup of G, called the **pointwise stabilizer** *of Δ in G. If $\Delta = \{\alpha\}$, then $G_\Delta = G_\alpha$ is called the* **point stabilizer** *of α in G and is denoted also by $\mathrm{Stab}_G(\alpha)$.*

Proposition 2.1.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ and $\Delta \subseteq \Omega$. For all $g \in G$, $g^{-1}G_\Delta g = G_{\Delta^g}$. In particular, if Δ is fixed by G, then $G_\Delta \trianglelefteq G$ and $G/G_\Delta \cong G^\Delta$. Also, if $\alpha^G = \beta^G$, then G_α and G_β are conjugate in G.*

Proposition 2.1.7. *Let G be a permutation group on Ω. If $K \leqslant G$ is transitive on Ω, then $G = G_\alpha K$, for all $\alpha \in \Omega$.*

Proof. Let $\alpha \in \Omega$ and $g \in G$. Since K is transitive on Ω, there exists $k \in K$ such that $\alpha^g = \alpha^k$. Then $gk^{-1} \in G_\alpha$, that is, $g \in G_\alpha K$, which gives the result. $\square$

Orbit-Stabilizer Theorem. *Let G be a permutation group on Ω and $\alpha \in \Omega$. Then the following holds:*

$$|G| = |G_\alpha||\alpha^G|.$$

Proof. Let $\alpha^h, \alpha^k \in \alpha^G$. Then $\alpha^h = \alpha^k$ if and only if $hk^{-1} \in G_\alpha$, that is, $G_\alpha h = G_\alpha k$. Hence the number of distinct points of α^G is equal to the number of distinct right cosets of G_α, that is, $|\alpha^G| = |G : G_\alpha| = |G|/|G_\alpha|$. $\square$

Definition 2.1.8. *A permutation group G on Ω is called* **semiregular** *if $G_\alpha = 1$, for all $\alpha \in \Omega$. G is* **regular** *if it is semiregular and transitive.*

Proposition 2.1.9. *Let $G \leqslant \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. If G is transitive or semiregular, then $\deg G = n = |\Omega|$.*

Proof. In both cases, for all $\alpha \in \Omega$, $G_\alpha \neq G$, that is, for all $\alpha \in \Omega$, there exists $g \in G$ such that $\alpha^g \neq \alpha$. $\square$

Proposition 2.1.10. *The order of a semiregular group G is a divisor of its degree. A transitive group is regular if and only if its order and degree are equal.*

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a semiregular group. Then, by the Orbit-Stabilizer Theorem, $|G| = |\alpha^G|$, for all $\alpha \in \Omega$. But the set of orbits of G on Ω form a partition of Ω. Hence $|G|$ divides $|\Omega|$. Now, suppose that G is regular. Then Proposition 2.1.9 implies that

$$|G| = |\alpha^G| = |\Omega| = \deg G.$$

Conversely, let G be transitive and suppose that $|G| = \deg G$. Then

$$|G_\alpha||\Omega| = |G| = \deg G = |\Omega|.$$

Hence $G_\alpha = 1$, for all $\alpha \in \Omega$, and G is regular. □

2.2 Centralizer of a permutation group

Proposition 2.2.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ and let Δ be the set of points fixed by G. Then the centralizer C of G in $\mathrm{Sym}(\Omega)$ contains the symmetric group $\mathrm{Sym}(\Delta)$ and so is transitive on Δ. In particular, this holds for the normalizer of G in $\mathrm{Sym}(\Omega)$.*

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ and let Δ be the set of all points fixed by G. Then every permutation on the set Δ is disjoint with every element of G. But disjoint cycles commute, so $\mathrm{Sym}(\Delta)$ is contained in the centralizer of G in $\mathrm{Sym}(\Omega)$. □

Proposition 2.2.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$. If the centralizer C of G in $\mathrm{Sym}(\Omega)$ is transitive, then G is semiregular.*

Proof. Let $\alpha, \beta \in \Omega$. By hypothesis, there exists $c \in C = C_{\mathrm{Sym}(\Omega)}(G)$ such that $\alpha^c = \beta$. Then $G_\alpha = c^{-1}G_\alpha c = G_{\alpha^c} = G_\beta$, which implies that G_α fixes every point of Ω and so $G_\alpha = 1$, for all $\alpha \in \Omega$. □

Proposition 2.2.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$. If G is transitive on Ω, then the centralizer C of G in $\mathrm{Sym}(\Omega)$ is semiregular.*

Proof. Let C be the centralizer of G in $\mathrm{Sym}(\Omega)$ and H be the centralizer of C in $\mathrm{Sym}(\Omega)$. Then $G \leqslant H$, so H is transitive and, by Proposition 2.2.2, C is semiregular. □

Under the hypothesis of Proposition 2.2.3 it can also be shown that $|C|$ equals the number of fixed points of G_α, for any $\alpha \in \Omega$ (see [10, Thm. 4.2A]).

Proposition 2.2.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$. If G is transitive on Ω and abelian, then G is regular. In particular, G is its own centralizer in* $\mathrm{Sym}(\Omega)$.

Proof. Set $C = C_{\mathrm{Sym}(\Omega)}(G)$. As G is abelian, $G \leqslant C$ and so, since G is transitive, C is transitive. Then, by Proposition 2.2.2, G is semiregular and hence regular.
But, by Proposition 2.2.3, also C is regular. Thus, by Proposition 2.1.10, $|C| = |\Omega| = |G|$ and, since $G \leqslant C$, it follows that $G = C$. □

2.3 Normalizer of a cyclic group of order p

Suppose that p is a prime. We describe a procedure to build, given a p-cycle x, a $(p-1)$-cycle y which normalizes $\langle x \rangle$. We start with a definition.

Definition 2.3.1. *Let Ω be a set and $c \in \mathrm{Sym}(\Omega)$ be a cycle. Let $\alpha, \beta \in \Omega \setminus \mathrm{Fix}(c)$. The* **distance** $\mathrm{d}_c(\alpha, \beta)$ *between α and β with respect to c is the number of points in c between α and β, that is, the number t such that c^t takes α to β.*

For instance, if $c = (c_1 \dots c_r)$, then the distance between c_h and c_k with respect to c is given by $\mathrm{d}_c(c_h, c_k) = k - h$.
Let $a \in \{2, \dots, p-1\}$ and suppose that $a^{p-1} \equiv 1 \pmod p$ and $a^r \not\equiv 1 \pmod p$, for all $r < p - 1$, that is, a is a primitive element in the field $\mathbb{F}_p$ of order p.
Let x be a p-cycle and suppose that Ω is the set of points moved by x. Write

$$x = (i_0 \; i_1 \dots i_{p-1}).$$

Consider the permutation y_a defined as follows

$$y_a = \begin{pmatrix} i_0 & i_1 & \dots & i_k & \dots & i_{p-1} \\ i_0 & i_a & \dots & i_{ak} & \dots & i_{a(p-1)} \end{pmatrix} = (i_1 \; i_a \; i_{a^2} \dots i_{a^{p-2}}),$$

where all the subscripts are taken modulo p. Of course, y_a acts on $\Omega \setminus \{i_0\}$ and, because of the choice of a, y_a is a $(p-1)$-cycle. Moreover,

$$x^{y_a} = (i_0 \; i_a \dots i_{ak} \dots i_{a(p-1)}) = x^a,$$

because the distance between any two consecutive points i_{aj} and $i_{a(j+1)}$ of x^{y_a} with respect to x is a. Hence, y_a normalizes $\langle x \rangle$.
So $y = y_a$, for some $a \in \{2, \dots, p-1\}$ such that the order of a in $\mathbb{Z}_p$ is $p - 1$.

2.4 Permutation representations of a group

Let G be any group. Then G can be regarded as a permutation group on its underlying set in the two following ways. Let $g \in G$ and consider the permutations

$$g\rho\colon x \in G \longmapsto xg \in G$$
$$g\lambda\colon x \in G \longmapsto g^{-1}x \in G$$

of G regarded as a set. Then the mappings

$$\rho\colon g \in G \longmapsto g\rho \in \mathrm{Sym}(G)$$
$$\lambda\colon g \in G \longmapsto g\lambda \in \mathrm{Sym}(G)$$

are isomorphisms between G and the regular permutation groups

$$G\rho = \{g\rho \mid g \in G\}$$
$$G\lambda = \{g\lambda \mid g \in G\},$$

which are subgroups of $\mathrm{Sym}(G)$. In particular, as a permutation group, G is regular on itself. ρ and λ are called, respectively, **right regular** and **left regular representations** of G. Also $G\lambda \cap G\rho = Z\lambda = Z\rho$, where Z is the centre of G.

Lemma 2.4.1. *Let ρ and λ be, respectively, the right regular and the left regular representations of a group G. Then $C_{\mathrm{Sym}(G)}(G\lambda) = G\rho$ and $C_{\mathrm{Sym}(G)}(G\rho) = G\lambda$.*

Proof. We shall prove only the first equation, from which the second will follow by symmetry. Clearly, $(g\rho)(h\lambda) = (h\lambda)(g\rho)$, for all $h, g \in G$, since both maps send x to $h^{-1}xg$. This shows that $[G\rho, G\lambda] = 1$ and, in particular, $G\rho \leqslant C_{\mathrm{Sym}(G)}(G\lambda)$. But, since $G\lambda$ is regular, by Proposition 2.2.3, $C_{\mathrm{Sym}(G)}(G\lambda)$ is semiregular and so, by Proposition 2.1.10, $|C_{\mathrm{Sym}(G)}(G\lambda)|$ divides $|G| = |G\rho|$. Hence $|G\rho| = |C_{\mathrm{Sym}(G)}(G\lambda)|$ and so $G\rho = C_{\mathrm{Sym}(G)}(G\lambda)$. $\square$

More generally, if G is a group and H is a subgroup of G, then G can be regarded as a permutation group on the set of right cosets of H in G as shown below.

Denote by Ω the set of right cosets of H in G and define $\rho_H\colon G \to \mathrm{Sym}(\Omega)$ by

$$\rho_H : g \longmapsto \begin{pmatrix} Hk \\ Hkg \end{pmatrix}.$$

Then the map $Hk \mapsto Hkg$ is a permutation on Ω and ρ_H is a homomorphism from G to $\mathrm{Sym}(\Omega)$. Also $G\rho_H$ is a transitive permutation group on Ω.
The reader will easily recognize that the right regular representation ρ of G is precisely the ρ_H, for $H = 1$.

Proposition 2.4.2. *Let G be a group and let H be a subgroup of G. Then the kernel of the action ρ_H of G on the set of right cosets of H in G is given by*

$$\ker \rho_H = \bigcap_{k \in G} H^k.$$

In particular, $\ker \rho_H$ *is the largest normal subgroup of G contained in H.*

Proof. Let $g \in G$. Then $g \in \ker \rho_H$ if and only if, for all $k \in G$, $Hk = Hkg$, that is, $kgk^{-1} \in H$, namely, $g \in k^{-1}Hk$. Hence $\ker \rho_H = \bigcap_{k \in G} H^k$. □

2.5 The holomorph of a group

Let G be a group and let λ and ρ be the left and the right regular representations of G. Then $G\lambda$ and $G\rho$ are subgroups of $\mathrm{Sym}(G)$, as is $\mathrm{Aut}(G)$. Also, for all $x \in G$, we have that $x(g\lambda)(g\rho) = g^{-1}xg$ and so $(g\lambda)(g\rho)$ is the inner automorphism induced by g. Thus

$$\langle G\rho, \mathrm{Aut}(G)\rangle = \langle G\lambda, \mathrm{Aut}(G)\rangle.$$

This subgroup is called the **holomorph** of G ([24]) and is denoted by

$$\mathrm{Hol}(G).$$

Now, since, for all $\phi \in \mathrm{Aut}(G)$ and $x \in G$,

$$x(\phi^{-1}(g\rho)\phi) = ((x\phi^{-1})g)\phi = ((x\phi^{-1})\phi)(g\phi) = x(g\phi) = x((g\phi)\rho),$$

we get that $G\rho \trianglelefteq \mathrm{Hol}(G) = \mathrm{Aut}(G)G\rho$. Moreover, since ρ is regular and every automorphism has at least one fixed point, we have that $G\rho \cap \mathrm{Aut}(G) = 1$. Thus

$$\mathrm{Hol}(G) = G\rho \rtimes \mathrm{Aut}(G).$$

Similarly,

$$\mathrm{Hol}(G) = G\lambda \rtimes \mathrm{Aut}(G).$$

Finally, as $G\rho \cong G \cong G\lambda$, we can also write

$$\mathrm{Hol}(G) \cong G \rtimes \mathrm{Aut}(G).$$

Proposition 2.5.1. *Let H be a regular permutation group on a set Ω. Then the normalizer of H in $\mathrm{Sym}(\Omega)$ is isomorphic to $\mathrm{Hol}(H)$.*

Proof. Set $N = N_{\mathrm{Sym}(\Omega)}(H)$ and $C = C_{\mathrm{Sym}(\Omega)}(H)$. Consider the action

$$\rho\colon N \longrightarrow \mathrm{Aut}(H)$$

of N on H by conjugation. Then $\ker \rho = C$ and so N/C is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Moreover, since H is regular, by Lemma 2.4.1 we have that H is isomorphic to C and so $N/H \cong N/C$.
Now let $K = \mathrm{Hol}(H) \cong H \rtimes \mathrm{Aut}(H)$. Since $H \trianglelefteq K$ and, as H is regular, $|H| = |\Omega|$, K is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$ contained in N. Hence

$$\mathrm{Aut}(H) \cong K/H \lesssim N/H \lesssim \mathrm{Aut}(H)$$

and $K/H \cong N/H$, which implies $K \cong N$. $\square$

2.6 Wreath products

Definition 2.6.1. *Let K be a group and H be a permutation group on a set Ω. Consider the set*

$$\{(\alpha, h) \mid h \in H,\ \alpha\colon \Omega \to K\}.$$

Define a multiplication on this set by

$$(\alpha_1, h_1)(\alpha_2, h_2) = (\beta, h_1 h_2),$$

where β is a map from Ω to K defined by $\beta(i) = \alpha_1(i)\alpha_2(i^{h_1})$, for all $i \in \Omega$. Then

(i) *the multiplication so defined is associative;*

(ii) *the element $(\tau, 1_H)$, with $\tau(i) = 1_K$, for all $i \in \Omega$, is the identity element; and*

(iii) *the element (β, h^{-1}), with $\beta(i) = \alpha(i^{h^{-1}})^{-1}$, for all $i \in \Omega$, is the inverse of (α, h).*

The group so constructed is called the **wreath product** *of K by H and is denoted by*

$$K \wr H.$$

Theorem 2.6.2. *Let H be a permutation group on a set Ω, with $|\Omega| = n$, and let K be any group. Suppose that G is the wreath product of K by H. Then*

(i) *for all $i = 1, \ldots, n$, the subgroup*

$$B_i = \{(\alpha, 1_H) \mid \alpha(j) = 1_K, \text{ for all } j \neq i\}$$

is isomorphic to K;

(ii) $B = B_1 \times \cdots \times B_n$ *is a normal subgroup of G;*

(iii) *the group*

$$H^* = \{(\tau, h) \mid h \in H, \ \tau(i) = 1_K, \text{ for all } i \in \Omega\},$$

isomorphic to H, is a complement to B in G;

(iv) *the action of an element $h^* = (\tau, h) \in H^*$ on the direct factors B_i is given by $B_i^{h^*} = B_{i^h}$. In particular, $C_{H^*}(B_i) = \mathrm{Stab}_H(i)$; and*

(v) $|G| = |K|^n|H|$.

Proof. Let $\Omega = \{1, \ldots, n\}$. Set $B = \{(\alpha, 1_H) \mid \alpha\colon \Omega \to K\}$ and, for $i = 1, \ldots, n$,

$$B_i = \{(\alpha, 1_H) \mid \alpha(j) = 1_K, \text{ for all } j \neq i\}.$$

Clearly, $B_i \cong K$ and so (i) holds. Also $B = B_1 \times \cdots \times B_n$. Consider now the map

$$\phi\colon (\alpha, h) \longmapsto h.$$

ϕ is an epimorphism from G to H with kernel B. So $B \trianglelefteq G$ and (ii) holds. Moreover, since

$$(\alpha, h) = (\alpha, 1_H)(\tau, h),$$

with $\tau(i) = 1_K$, for all $i \in \Omega$, the group

$$H^* = \{(\tau, h) \mid h \in H, \ \tau(i) = 1_K, \text{ for all } i \in \Omega\}$$

is a complement to B in G, which gives us (iii). Now let $h^* = (\tau, h) \in H^*$ and $(\alpha, 1_H) \in B_i$. Then

$$h^{*^{-1}}(\alpha, 1_H)h^* = (\beta, 1_H),$$

with $\beta(j) = \alpha(j^{h^{-1}})$. So $(\beta, 1_H) \in B_{i^h}$ and $B_i^{h^*} = B_{i^h}$. So (iv) holds. Finally, part (v) follows from Definition 2.6.1. □

The subgroup B defined in the statement of Theorem 2.6.2 is called the **base group** of the wreath product of K by H. Note that B is uniquely determined by K and by the degree n of H. Also note that $B = K \wr T$, where T is the trivial permutation group on Ω.

Corollary 2.6.3. *The wreath product $K \wr H$ of K by H is the semidirect product of B by H^*, with B the direct product of n copies of K and $H^* \cong H$ acting on B permuting the direct factors by conjugation in the same way as H permutes the elements of Ω.*

Theorem 2.6.4. *Let H be a permutation group on a set Ω, with $|\Omega| = n$, and let K be any group. Let B denote the base group of the wreath product $K \wr H$. Then $B = B_1^L$, for any subgroup L of H which is transitive on Ω, where B_1 is defined as in the statement of Theorem 2.6.2.*

Proof. Let $L \leqslant H$ be a transitive permutation group on the set Ω. By construction, $B = B_1 \times \cdots \times B_n$, where $B_i \cong K$, for all $i = 1, \ldots, n$, and L acts on the direct factors B_i by $B_i^x = B_{i^x}$, for all $x \in L$. Therefore

$$B_1^L = \langle B_1^x \mid x \in L \rangle = \langle B_{1^x} \mid x \in L \rangle$$

and, since L is transitive on $\Omega = \{1, \ldots, n\}$, we have that $B_1^L = \langle B_1, \ldots, B_n \rangle = B$. □

Corollary 2.6.5. *Let $H, L \leqslant \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, and let K be any group. Suppose that H and L are transitive on Ω. Then $B_1^H = B_1^L$, as subgroups of $K \wr \langle H, L \rangle$, where B_1 is defined as in the statement of Theorem 2.6.2.*

Proof. Let B denote the base group of the wreath product $K \wr \langle H, L \rangle$. Then, since H is transitive on Ω, Theorem 2.6.4 implies that $B = B_1^H$. Similarly, since L is transitive on Ω, we get that $B = B_1^L$. Hence $B_1^H = B_1^L$. □

Theorem 2.6.6. *Let K be a group acting on a set Γ and H be a permutation group on a set Ω. Then the wreath product $K \wr H$ acts on the set $\Gamma \times \Omega$ by*

$$(i,j)(\alpha,h) = (i^{\alpha(j)}, j^h),$$

for all $(i,j) \in \Gamma \times \Omega$. Moreover, if K is faithful on Γ, then $K \wr H$ is faithful on $\Gamma \times \Omega$ and, if both K and H are transitive on Γ and Ω, respectively, then $K \wr H$ is transitive on $\Gamma \times \Omega$.

Proof. Let $(i,j) \in \Gamma \times \Omega$ and $(\alpha_1,h_1),(\alpha_2,h_2) \in K \wr H$. Then we have that

$$\begin{aligned}((i,j)(\alpha_1,h_1))(\alpha_2,h_2) &= (i^{\alpha_1(j)}, j^{h_1})(\alpha_2,h_2)\\ &= (i^{\alpha_1(j)\alpha_2(j^{h_1})}, j^{h_1h_2}) = (i,j)((\alpha_1,h_1)(\alpha_2,h_2))\end{aligned}$$

and so we have defined an action of $K \wr H$ on the set $\Gamma \times \Omega$.
Now suppose that K is faithful on Γ. Then

$$(i,j)(\alpha,h) = (i^{\alpha(j)}, j^h) = (i,j),$$

for all $(i,j) \in \Gamma \times \Omega$, implies that $h = 1$ and $\alpha(j) = 1$, for all $j \in \Omega$, and so $K \wr H$ is faithful on $\Gamma \times \Omega$.
Finally, let K and H be transitive on Γ and Ω, respectively, and let $(i,j),(i',j') \in \Gamma \times \Omega$. By the transitivity of H on Ω, there exists $h \in H$ such that $j^h = j'$ and, by the transitivity of K on Γ, there exists $k \in K$ such that $i^k = i'$. Then

$$(i,j)(\alpha,h) = (i',j'),$$

where $\alpha\colon \Omega \to K$ is a mapping which takes j to k. Therefore $K \wr H$ is transitive on $\Gamma \times \Omega$. $\square$

For our purposes the most important consequence of Theorem 2.6.6 is that, if $K \leqslant \mathrm{Sym}(\Gamma)$ and $H \leqslant \mathrm{Sym}(\Omega)$, then the wreath product $K \wr H$ is a subgroup of $\mathrm{Sym}(\Gamma \times \Omega)$.

Theorem 2.6.7. *Let K, H and L be permutation groups on the sets Γ, Ω and Δ, respectively. Then, identifying the sets $(\Gamma \times \Omega) \times \Delta$ and $\Gamma \times (\Omega \times \Delta)$ via the map*

$$((i,j),s) \longmapsto (i,(j,s)),$$

the permutation groups $(K \wr H) \wr L$ and $K \wr (H \wr L)$ are isomorphic.

Proof. Let $x = (\alpha, l) \in (K \wr H) \wr L$, with $\alpha(s) = (\alpha_s, h_s) \in K \wr H$, for all $s \in \Delta$. Then

$$((i,j),s)x = ((i,j)^{\alpha(s)}, s^l) = ((i^{\alpha_s(j)}, j^{h_s}), s^l).$$

Consider now the element $y = (\beta, (\gamma, l)) \in K \wr (H \wr L)$, with $\gamma(s) = h_s$ and $\beta((j,s)) = \alpha_s(j)$, for all $j \in \Omega$ and $s \in \Delta$. Then

$$(i,(j,s))y = (i^{\beta((j,s))}, (j,s)^{(\gamma,l)}) = (i^{\alpha_s(j)}, (j^{\gamma(s)}, s^l)) = (i^{\alpha_s(j)}, (j^{h_s}, s^l)).$$

□

Lemma 2.6.8. *Suppose that R is a transitive permutation group of degree n. Let $H = L \wr R$ and $G = K \wr R$, with L maximal subgroup of K, and let p be a prime dividing $|K|$. If L contains the normalizer of a Sylow p-subgroup of K, then H is a maximal subgroup of G.*

Proof. Let $H = L \wr R$ and $G = K \wr R$, with L maximal subgroup of K. Let $\bar{L} = L_1 \times \cdots \times L_n$, with $L_i \cong L$, and $\bar{K} = K_1 \times \cdots \times K_n$, with $K_i \cong K$, be the base groups of H and G, respectively. Then $H = \bar{L} \rtimes R$ and $G = \bar{K} \rtimes R$ and, in particular, H can be regarded as a subgroup of G. Also notice that, by Corollary 1.1.12, $\bar{L}$ contains the normalizer of a Sylow p-subgroup of $\bar{K}$. Now let M be a subgroup of G properly containing H. By Dedekind's Modular Law, we have that

$$M = M \cap G = M \cap (\bar{K} \rtimes R) = (M \cap \bar{K}) \rtimes R,$$

with $\bar{L} \leqslant M \cap \bar{K} \leqslant \bar{K}$. Therefore $M \cap \bar{K}$ is a subgroup of $\bar{K}$ containing the normalizer of a Sylow p-subgroup of $\bar{K}$. Then, by Corollary 1.1.12,

$$M \cap \bar{K} = M_1 \times \cdots \times M_n,$$

with $M_i = M \cap K_i$ and $L_i \leqslant M_i \leqslant K_i$, for all $i = 1, \ldots, n$. Since $M \neq H$, from the factorization of M it follows that $M \cap \bar{K} \neq \bar{L}$ and so there exists $j \in \{1, \ldots, n\}$ such that $M_j \neq L_j$. As L_j is a maximal subgroup of K_j, it follows that $M_j = K_j$ and, R being transitive on $\{M_1, \ldots, M_n\}$, this implies that $M_i = K_i$, for all $i = 1, \ldots, n$. Hence $M \cap \bar{K} = \bar{K}$ and $M = \bar{K} \rtimes R = G$. □

Lemma 2.6.9. *Let K be a group and H be a group operating on K. Suppose that M is a maximal subgroup of H such that $|H : M| > |K|$. Then any complement to K in KH which contains M is equal to H.*

Proof. Let L be a complement to K in KH and assume that $M \leqslant L$. Firstly, since any two complements are isomorphic, we have that $L \cong H$ and so, in particular, $|L| = |H|$. Moreover

$$|L||H|/|L \cap H| = |LH| \leq |KH| = |K||H|.$$

Now $M \leqslant L \cap H \leqslant H$. Then, by the maximality of M in H, either $L \cap H = M$ or $L \cap H = H$. If $L \cap H = M$, then from the above relation it follows that

$$|L : L \cap H| = |H : M| \leq |K|,$$

which is a contradiction. Hence $L \cap H = H$, which implies $L = H$. $\square$

Chapter 3

Primitive, imprimitive and multiply transitive permutation groups

3.1 Introduction

Definition 3.1.1. *Let G be a permutation group on a set Ω and $\Gamma \subseteq \Omega$. Γ is called a* **block** *of G if, for all $g \in G$, Γ^g either is equal to Γ or has no point in common with Γ, that is, $\Gamma^g \cap \Gamma \in \{\Gamma, \emptyset\}$. The* **length** *of the block Γ is $|\Gamma|$.*

The whole set Ω, the empty set $\emptyset$ and the singletons $\{\alpha\}$, for $\alpha \in \Omega$, are blocks of G, for all $G \leqslant \mathrm{Sym}(\Omega)$. We call these **trivial blocks**. Also every orbit of G on Ω is a block of G. We plainly have that, if $H \leqslant G \leqslant \mathrm{Sym}(\Omega)$, then every block of G is a block of H.

Proposition 3.1.2. *The intersection of two blocks of G is a block of G.*

Proof. Let Γ and Δ be blocks of G and let $g \in G$. Suppose that $(\Gamma \cap \Delta)^g \cap (\Gamma \cap \Delta) \neq \emptyset$. Then, $\Gamma^g \cap \Gamma$ and $\Delta^g \cap \Delta$ are nonempty. Therefore, $\Gamma^g = \Gamma$ and $\Delta^g = \Delta$, which implies that $(\Gamma \cap \Delta)^g = \Gamma^g \cap \Delta^g = \Gamma \cap \Delta$. ☐

Proposition 3.1.3. *Let $H \leqslant G \leqslant \mathrm{Sym}(\Omega)$. If Γ is a block of H, then Γ^g is a block of $g^{-1}Hg$, for all $g \in G$. In particular, if Γ is a block of G, then Γ^g is a block of G, for all $g \in G$.*

Proof. Let $h \in H$ and $g \in G$ and suppose that $(\Gamma^g)^{g^{-1}hg} \cap \Gamma^g \neq \emptyset$. Applying g^{-1}, it follows that $\Gamma^h \cap \Gamma \neq \emptyset$, which implies, as Γ is a block of H, that $\Gamma^h = \Gamma$. Then, applying g, we get that $(\Gamma^g)^{g^{-1}hg} = \Gamma^{hg} = \Gamma^g$ and Γ^g is a block of $g^{-1}Hg$. $\square$

We shall call the blocks Γ and Γ^g **conjugate**. By definition, conjugate blocks are either equal or disjoint. For a block Γ of G the set of all blocks conjugate to Γ is called a **complete block system** of G. All blocks of a complete block system have the same length. Also, if G is transitive on Ω, then the blocks belonging to a complete block system of G partition Ω.

Proposition 3.1.4. *The length of a block of a transitive permutation group G divides the degree of G.*

Proof. Let Γ be a block of G, with $G \leqslant \mathrm{Sym}(\Omega)$. Since G is transitive, Ω is the union of all blocks of the complete block system determined by Γ. But conjugate blocks have the same length and so $|\Gamma|$ must divide $|\Omega|$, which, by Proposition 2.1.9, is equal to $\deg G$. $\square$

Proposition 3.1.5. *Let $G = \mathrm{Sym}(\Omega)$, $H \leqslant G$ and set $N = N_G(H)$. If $\mathcal{B} = \{\Omega_1, \ldots, \Omega_n\}$ is a complete block system of H, then, for all $x \in N$, $\mathcal{B}^x = \{\Omega_1^x, \ldots, \Omega_n^x\}$ is also a complete block system of H.*

Proof. Let $\mathcal{B} = \{\Omega_1, \ldots, \Omega_n\}$ be a complete block system of H. Let $x \in N = N_G(H)$ and consider the set $\mathcal{B}^x = \{\Omega_1^x, \ldots, \Omega_n^x\}$. By Proposition 3.1.3, Ω_i^x is a block of $x^{-1}Hx = H$, for all $i = 1, \ldots, n$. So $\mathcal{B}^x$ is a set of blocks of H. Furthermore, since $\mathcal{B}$ is a complete block system of H and $N = N_G(H)$, we have that for $h \in H$

$$\Omega_i^{xh} = \Omega_i^{h^{x^{-1}}x} = \Omega_i^{h'x} = \Omega_j^x,$$

for some $j = 1, \ldots, n$. Therefore the elements of $\mathcal{B}^x$ are permuted by conjugation by the elements of H and so $\mathcal{B}^x$ is a complete block system of H. $\square$

3.2 Primitive and imprimitive groups

Definition 3.2.1. *Let G be a transitive permutation group. Then G is* **imprimitive** *if G has at least one nontrivial block; otherwise G is called* **primitive**.

Theorem 3.2.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group which contains an intransitive normal subgroup $K \neq 1$. Then G is imprimitive and the orbits of K on Ω form a complete block system of G.*

Proof. Let Γ be an orbit of K on Ω and let $g \in G$. Then, by Proposition 2.1.4, Γ^g is an orbit of $g^{-1}Kg = K$. Thus G acts on the set of orbits of K and, as orbits are either equal or disjoint, Γ is a block of G. Also, as $K \neq 1$, its orbits contain more than one point and, because of the intransitivity of K, they are proper subsets of Ω. So G is imprimitive.
Moreover, because G is transitive on Ω, the orbits of K are all conjugate in G and so the set of orbits of K is a complete block system of G. $\square$

Corollary 3.2.3. *Every nontrivial normal subgroup of a primitive group is transitive.*

Theorem 3.2.4. *Let $\alpha \in \Omega$ and G be a transitive permutation group on Ω. Then G is imprimitive if and only if there is a subgroup Z which lies properly between G_α and G.*

Proof. Let G be imprimitive and Γ be a nontrivial block of G. Let Z be the set of all elements $z \in G$ such that $\Gamma^z = \Gamma$. Clearly, Z is a subgroup of G and is not equal to G, since G is transitive on Ω and $\Gamma \subset \Omega$. Now let $\alpha \in \Gamma$. As Γ is a block of G, if $\alpha^g = \alpha$, then $\Gamma^g = \Gamma$. Therefore, $G_\alpha \leqslant Z$. Moreover, as $|\Gamma| > 1$, there exists $\beta \in \Gamma$, $\beta \neq \alpha$, and, since G is transitive on Ω, $\beta = \alpha^h$, for some $h \in G$. Then $\beta \in \Gamma \cap \Gamma^h$ and so $h \in Z$, but $h \notin G_\alpha$. Thus G_α is properly contained in Z.
Conversely, let Z be a subgroup of G such that $G_\alpha < Z < G$, and set $\Gamma = \alpha^Z$. Let $\beta \in \Gamma \cap \Gamma^g$, with $g \in G$. Then $\beta = \alpha^z = \alpha^{z'g}$, with $z, z' \in Z$. Therefore, $z'gz^{-1} \in G_\alpha < Z$, which implies that $g \in Z$. Thus $\Gamma^g = (\alpha^Z)^g = \Gamma$ and Γ is a block of G. Also, since $G_\alpha < Z$, Γ has more than one element. But, by the previous argument, $\Gamma = \Gamma^g$ implies $g \in Z$. So, since $Z < G$, there exists $g \in G$ such that $\Gamma \neq \Gamma^g$. Thus $\Gamma \neq \Omega$ and Γ is a nontrivial block of G. $\square$

Corollary 3.2.5. *The lattice of subgroups between G_α and G is isomorphic to the lattice of blocks of G which contain α.*

As a consequence of Theorem 3.2.4 we get the following important result:

Theorem 3.2.6. *Let $\alpha \in \Omega$, $|\Omega| > 1$. A transitive permutation group G on Ω is primitive if and only if G_α is a maximal subgroup of G.*

Proposition 3.2.7. *A transitive permutation group G of prime degree is primitive.*

Proof. By Proposition 3.1.4, the length of a block of a transitive permutation group divides its degree and so G has only trivial blocks. $\square$

Transitive permutation groups of prime degree which are soluble can be characterized in terms of Sylow subgroups thanks to a result due to Galois.

Theorem 3.2.8. ([15, pg. 163]) *Let G be a transitive permutation group of prime degree p. Then G is soluble if and only if G has a unique Sylow p-subgroup.*

Our final two theorems provide a method for recognizing symmetric and alternating groups.

Theorem 3.2.9. ([41, 13.3]) *A primitive permutation group which contains a transposition is a symmetric group.*

Theorem 3.2.10. ([41, 13.9]) *Let p be a prime and G a primitive permutation group of degree $n = p + k$, with $k \geq 3$. If G contains an element of degree and order p, then G is either* $\mathrm{Alt}(n)$ *or* $\mathrm{Sym}(n)$.

3.3 Multiply transitive groups

The concept of a transitive group can be generalized as follows.

Definition 3.3.1. *Let G be a permutation group on Ω, with $|\Omega| = n$, and let k be an integer such that $1 \leq k \leq n$. Then G is called k-**transitive** on Ω if, for every two k-tuples $(\alpha_1, \ldots, \alpha_k)$, $(\beta_1, \ldots, \beta_k)$ of distinct elements of Ω, there exists $g \in G$ such that $\alpha_i^g = \beta_i$, for all $i = 1, \ldots, k$.*

From the definition it immediately follows that every $(k+1)$-transitive group is also k-transitive and a group containing a k-transitive subgroup is itself k-transitive.

Theorem 3.3.2. *Let G be a transitive permutation group on Ω and $\alpha \in \Omega$. Then G is $(k+1)$-transitive on Ω if and only if G_α is k-transitive on $\Omega \setminus \{\alpha\}$.*

In particular, we can consider 2-transitive groups for which we have the following important result:

Theorem 3.3.3. *Every 2-transitive group G is primitive.*

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ and let $\Delta \subseteq \Omega$, with $|\Delta| > 1$, be a block of G. Let $\alpha, \beta \in \Delta$, $\alpha \neq \beta$. Because G is 2-transitive on Ω, for any $\gamma \in \Omega$, there exists $g \in G$ such that

$$(\alpha, \beta)^g = (\alpha^g, \beta^g) = (\alpha, \gamma).$$

Then $\alpha \in \Delta \cap \Delta^g$, which implies, as Δ is a block of G, that $\Delta = \Delta^g$ and so $\gamma = \beta^g$ is also in Δ. Hence $\Delta = \Omega$. $\square$

Definition 3.3.4. *Let G be a permutation group on Ω, with $|\Omega| = n$, and let k be an integer such that $1 \leq k \leq n$. Then G is said to be* **sharply k-transitive** *on Ω if, for every two k-tuples $(\alpha_1, \dots, \alpha_k)$, $(\beta_1, \dots, \beta_k)$ of distinct elements of Ω, there exists a unique $g \in G$ such that $\alpha_i^g = \beta_i$, for all $i = 1, \dots, k$.*

Clearly, this is the same as saying that G is k-transitive and the stabilizer in G of any k points of Ω is trivial. Thus a sharply 1-transitive permutation group is a regular group.

Proposition 3.3.5. *A k-transitive permutation group G of degree n is sharply k-transitive if and only if the order of G is equal to $n(n-1)\dots(n-k+1)$.*

Proof. Suppose that G is k-transitive on a set Ω of order n and let $\alpha_1, \dots, \alpha_k \in \Omega$. By the Orbit–Stabilizer Theorem and because of the k-transitivity of G on Ω, we have that

$$\begin{aligned} |G : G_{\alpha_1 \dots \alpha_k}| &= |G : G_{\alpha_1}||G_{\alpha_1} : G_{\alpha_1 \alpha_2}| \dots |G_{\alpha_1 \dots \alpha_{k-1}} : G_{\alpha_1 \dots \alpha_k}| \\ &= n(n-1)\dots(n-k+1). \end{aligned}$$

Hence $|G| = n(n-1)\dots(n-k+1)$ if and only if $G_{\alpha_1 \dots \alpha_k} = 1$, that is, G is sharply k-transitive. $\square$

We conclude this section with the statement of a much deeper result due to Zassenhaus, whose proof can be found in [17, Thm. 2.6, pg. 176].

Theorem 3.3.6. ([43]) *If G is sharply 3-transitive of degree $p^f + 1$, with $p > 2$ prime, then either $G \cong \mathrm{PGL}(2, p^f)$ or $f = 2m$ is even and $G \cong M(p^{2m})$.*

For a description of the subgroup $M(p^{2m})$ the reader should refer to [17, 1.3c, pg. 162].

3.4 Minimal normal subgroups of a 2-transitive group

Proposition 3.4.1. *Let H be a group. Then a minimal normal subgroup of H is a direct product of isomorphic simple groups.*

Proof. Let N be a minimal normal subgroup of H. If N has no proper minimal normal subgroup, then N is simple and we get the result. So suppose that N has at least one minimal normal subgroup K and, using induction on $|H|$, assume that K is a direct product of isomorphic simple groups. Since N is a minimal normal subgroup of H, K is not normal in H. Hence there exists an element $h \in H$ such that $K^h \neq K$ and K^h is also a minimal normal subgroup of N. Moreover, K and K^h commute, so the subgroup $\langle K^h \mid h \in H\rangle$ of N is a direct product of some conjugates of K in H and is normal in H. But, as N is a minimal normal subgroup of H, this implies that $N = \langle K^h \mid h \in H\rangle$, which is, applying the inductive hypothesis to each K^h, with $h \in H$, a direct product of isomorphic simple groups. $\square$

More generally, it can be proved [1, 8.2] that every characteristically simple finite group is a direct product of isomorphic simple groups.

Corollary 3.4.2. *Let H be a group and N be a minimal normal subgroup of H. If N is abelian, then N is elementary abelian and $|N| = p^d$, for some prime p.*

Theorem 3.4.3. ([4]) *A primitive permutation group G has either one or two minimal normal subgroups. If G has two minimal normal subgroups, then they are isomorphic, regular and centralize each other. If G has a unique minimal normal subgroup N, then there are two possibilities for N: either N is abelian and regular, that is, N is elementary abelian and $|N| = p^d = \deg G$, and $N = C_G(N)$; or $C_G(N) = 1$ and G is isomorphic to a subgroup of $\mathrm{Aut}(N)$.*

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group on a set Ω of degree n. Let N be a minimal normal subgroup of G. Then, by Corollary 3.2.3, N is transitive on Ω. Consider now the centralizer $C_G(N)$ of N in G. As $N \trianglelefteq G$, we also have $C_G(N) \trianglelefteq G$. Therefore, if $C_G(N) \neq 1$, again by Corollary 3.2.3, $C_G(N)$ is transitive on Ω. Then, by Propositions 2.2.2 and 2.2.3, both N and $C_G(N)$ are semiregular and thus regular. In particular, by Lemma 2.4.1, $N \cong C_G(N)$, since they are right and left regular representations of the same group N.

Now $C_G(N)$ is also a minimal normal subgroup of G. In fact, let $1 \neq K \leqslant C_G(N)$, $K \trianglelefteq G$. By Corollary 3.2.3, K is transitive on Ω and so, by the Orbit-Stabilizer Theorem, $|K| \geq |\Omega|$. But, as $C_G(N)$ is regular on Ω, by Proposition 2.1.10, we have that $|C_G(N)| = |\Omega|$, which implies that $K = C_G(N)$ and so $C_G(N)$ is a minimal normal subgroup of G.

Moreover, N and $C_G(N)$ are the only minimal normal subgroups of G. For, if K is a minimal normal subgroup of G different from N, then $[K, N] \leqslant K \cap N \trianglelefteq G$ and $K \cap N \leqslant K$. By the minimality of K, either $K \cap N = K$, that is, $K \leqslant N$ or $K \cap N = 1$. But, if $K \leqslant N$, by the minimality of N, we get $K = N$, which is a contradiction. So $K \cap N = 1$ and K centralizes N. Thus, by the minimality of $C_G(N)$, it follows that $K = C_G(N)$.

Now, if N is abelian, by Proposition 2.2.4, $N = C_G(N)$ and G has a unique minimal normal subgroup. Also, by Corollary 3.4.2, N is elementary abelian of order p^d, for some prime p, and, since it is regular, $p^d = n$. If N is not abelian, then N and $C_G(N)$ are distinct and G has two minimal normal subgroups which are isomorphic and regular.

On the other hand, if $C_G(N) = 1$, then N is the unique minimal normal subgroup of G. For, if K is a minimal normal subgroup of G different from N, as we saw before, K centralizes N and so $K = 1$, which is a contradiction. In particular, by considering the action of G on N by conjugation, we have that G is isomorphic to a subgroup of $\mathrm{Aut}(N)$. $\square$

Proposition 3.4.4. *Let G be a primitive permutation group on Ω, with $|\Omega| > 2$, and N be a minimal normal subgroup of G. Then $N \leqslant \mathrm{Alt}(\Omega)$.*

Proof. Suppose that $N \nleqslant \mathrm{Alt}(\Omega)$. Then $N \cap \mathrm{Alt}(\Omega) \neq N$ and $N \cap \mathrm{Alt}(\Omega) \trianglelefteq G$. As N is a minimal normal subgroup of G, this implies that $N \cap \mathrm{Alt}(\Omega) = 1$. Thus

$$1 \neq N \cong N/(N \cap \mathrm{Alt}(\Omega)) \cong N\mathrm{Alt}(\Omega)/\mathrm{Alt}(\Omega) \leqslant \mathrm{Sym}(\Omega)/\mathrm{Alt}(\Omega) \cong \mathbb{Z}_2,$$

and so $N \cong \mathbb{Z}_2$, that is, $|N| = 2$. But, by Corollary 3.2.3, N is transitive on Ω and so, by the Orbit-Stabilizer Theorem, $|N| \geq |\Omega| > 2$ and we get a contradiction. Hence we must conclude that $N \leqslant \mathrm{Alt}(\Omega)$. $\square$

Theorem 3.4.5. *Let G be a 2-transitive permutation group on Ω and let $N \trianglelefteq G$. If N is regular, then N is elementary abelian.*

Proof. Let $\alpha \in \Omega$ and $x_1, x_2 \in N \setminus \{1\}$. Since N is regular, $N \cap G_\alpha = 1$ and, in particular, $\alpha^{x_1}, \alpha^{x_2} \in \Omega \setminus \{\alpha\}$. Then, since G_α is transitive on $\Omega \setminus \{\alpha\}$, there exists $g \in G_\alpha$ such that $\alpha^{x_1} = (\alpha^{x_2})^g$. So $x_1 g^{-1} x_2^{-1} \in G_\alpha$, which implies, as $N \trianglelefteq G$, that $x_1^{g^{-1}} x_2^{-1} = g x_1 g^{-1} x_2^{-1} \in G_\alpha \cap N = 1$. Thus $x_1^{g^{-1}} = x_2$ and G_α acts transitively on $N \setminus \{1\}$.

Now let p be a prime dividing the order of N. Then, by Cauchy's Theorem ([24, 1.6.17]), there exists $x \in N$ of order p and, by the transitivity of G_α on $N \setminus \{1\}$, it follows that every nontrivial element of N has order p, that is, N has exponent p.
Finally look at the centre of N. Since N is a p-group, $Z(N)$ is nontrivial. Also $Z(N) \trianglelefteq G$. Then, for $x \in Z(N)$, we have that $x^g \in Z(N)$, for all $g \in G$, and the transitivity of G_α on $N \setminus \{1\}$ implies that $N = Z(N)$. Hence N is abelian and so elementary abelian. $\square$

Corollary 3.4.6. *A 2-transitive permutation group has a unique minimal normal subgroup N and N is either elementary abelian or simple.*

Proof. Let G be a 2-transitive permutation group and N be a minimal normal subgroup of G. Then G is primitive and, by Theorem 3.4.3, either N is regular or N is simple. If N is regular, then Theorem 3.4.5 implies that N is elementary abelian. Hence, by Theorem 3.4.3, we can conclude that G has a unique minimal normal subgroup and this is either elementary abelian or simple. $\square$

When the unique minimal normal subgroup N is simple, then, by a result due to Burnside ([41, Exercise 12.4]), N is primitive.
Table 3.1 gives a list of all nonabelian simple groups N which can occur as minimal normal subgroups of a 2-transitive permutation group of degree n. This list was obtained by Peter Cameron in [4] using the classification of finite simple groups. The number k is the maximum degree of transitivity of a group G whose unique minimal normal subgroup equals N.

3.5 Partitions and block systems

Proposition 3.5.1. *Let Ω be a set and $G = \mathrm{Sym}(\Omega)$. Let $\mathcal{B} = \{\Omega_1, \ldots, \Omega_m\}$ be a partition of Ω into m subsets of the same cardinality. Then the stabilizer L of $\mathcal{B}$ in G is isomorphic to*

$$\mathrm{Sym}(\Omega_1) \wr \mathrm{Sym}(\mathcal{B}).$$

In particular, L is imprimitive and $\mathcal{B}$ is a complete block system of L.

Proof. Let L denote the stabilizer in G of $\mathcal{B}$. Then, clearly, L contains the subgroup

$$(\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_m)) \rtimes \mathrm{Sym}(\mathcal{B}) \cong \mathrm{Sym}(\Omega_1) \wr \mathrm{Sym}(\mathcal{B})$$

N	n	k	Remarks
$\mathrm{Alt}(n), n \geq 5$	n	n	Two representations if $n = 6$
$\mathrm{PSL}(d, q)$, $d \geq 2$	$(q^d - 1)/(q - 1)$	3 if $d = 2$,	$(d, q) \neq (2, 2), (2, 3)$
		2 if $d > 2$	Two representations if $d > 2$
$\mathrm{PSU}(3, q)$	$q^3 + 1$	2	$q > 2$
${}^2B_2(q)$ (Suzuki)	$q^2 + 1$	2	$q = 2^{2a+1} > 2$
${}^2G_2(q)$ (Ree)	$q^3 + 1$	2	$q = 3^{2a+1} > 3$
$\mathrm{PSp}(2d, 2)$	$2^{2d-1} + 2^{d-1}$	2	$d > 2$
$\mathrm{PSp}(2d, 2)$	$2^{2d-1} - 2^{d-1}$	2	$d > 2$
PSL(2,11)	11	2	Two representations
PSL(2,8)	28	2	
Alt(7)	15	2	Two representations
M_{11} (Mathieu)	11	4	
M_{11} (Mathieu)	12	3	
M_{12} (Mathieu)	12	5	Two representations
M_{22} (Mathieu)	22	3	
M_{23} (Mathieu)	23	4	
M_{24} (Mathieu)	24	5	
HS (Higman–Sims)	176	2	Two representations
Co_3 (Conway)	276	2	

Table 3.1: Nonabelian simple minimal normal subgroups of a 2-transitive group

of G. Moreover L acts on $\mathcal{B}$ and so there exists a homomorphism $\phi\colon L \to \mathrm{Sym}(\mathcal{B})$, whose kernel is the set of all $x \in L$ such that $\Omega_i^x = \Omega_i$, for all $i = 1, \ldots, m$, that is,

$$\ker \phi = \mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_m).$$

Hence $|L| \leq |\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_m)||\mathrm{Sym}(\mathcal{B})|$, which implies the result. In particular, since $\mathcal{B}$ is a partition of Ω, the subsets Ω_i are blocks of L and, since $\mathrm{Sym}(\mathcal{B})$ is transitive on $\mathcal{B}$, they are all conjugate in L. Thus $\mathcal{B}$ is a complete block system of L. $\square$

Corollary 3.5.2. *Let Ω be a set and $G = \mathrm{Sym}(\Omega)$. Let $H \leqslant G$ be imprimitive and Γ*

be a block of H. Then the stabilizer in G of the complete block system $\mathcal{B}_\Gamma = \{\Gamma^g \mid g \in H\}$ is isomorphic to $\mathrm{Sym}(\Gamma) \wr \mathrm{Sym}(\mathcal{B}_\Gamma)$. In particular, H is isomorphic to a subgroup of $\mathrm{Sym}(\Gamma) \wr \mathrm{Sym}(\mathcal{B}_\Gamma)$.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an imprimitive group and let $\mathcal{B} = \{\Omega_1, \ldots, \Omega_m\}$ be a complete block system of G. Then G acts on $\mathcal{B}$ and we can consider the homomorphism

$$\phi\colon G \longrightarrow \mathrm{Sym}(\mathcal{B}),$$

whose kernel is given by

$$G \cap (\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_m)).$$

We shall refer to $\ker\phi$ as the **base group of G with respect to $\mathcal{B}$**. Notice that, though by Corollary 3.5.2 G is a subgroup of $(\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_m)) \rtimes \mathrm{Sym}(\mathcal{B})$, G does not necessarily decompose as a wreath product.

Theorem 3.5.3. *Let $G \cong K \wr H$, with $K \leqslant \mathrm{Sym}(k)$, $H \leqslant \mathrm{Sym}(m)$. If K is transitive and H is primitive on the respective sets, then every nontrivial block of G corresponds to a block of K. In particular, the length of every nontrivial block of G divides k.*

Proof. By assumption, G is an imprimitive permutation group acting on a set Ω of cardinality km and G has a complete block system $\mathcal{B} = \{\Omega_1, \ldots, \Omega_m\}$ of m block of length k. Also, G can be written as

$$G = (K_1 \times \cdots \times K_m) \rtimes \bar{H},$$

with $K \cong K_i \leqslant \mathrm{Sym}(\Omega_i)$, for all $i = 1, \ldots, m$, and $H \cong \bar{H} \leqslant \mathrm{Sym}(\mathcal{B})$.
Let Γ be a nontrivial block of G and suppose that $\Gamma \cap \Omega_1 \neq \emptyset$. For $\alpha \in \Gamma \cap \Omega_1$, the stabilizer G_α of α in G is given by

$$G_\alpha = \mathrm{Stab}_{K_1}(\alpha) \times ((K_2 \times \cdots \times K_m) \rtimes \mathrm{Stab}_{\bar{H}}(\Omega_1)).$$

For $g \in G_\alpha$, $\alpha^g = \alpha$ and so, since Γ is a block of G, we get that $\Gamma^g = \Gamma$ and Γ is preserved by G_α. Moreover, for $i \neq 1$, G_α is transitive on Ω_i, since $K_i \leqslant G_\alpha$ and, by assumption, K_i is transitive on Ω_i.
Suppose that $\Gamma \not\subseteq \Omega_1$. Assume that $\Gamma \cap \Omega_2 \neq \emptyset$ and let $\beta \in \Gamma \cap \Omega_2$. Then, as G_α is transitive

on Ω_2 and Γ is preserved by G_α, it follows that $\Gamma \supseteq \Omega_2$. The same argument applied with G_β in place of G_α implies that $\Gamma \supseteq \Omega_1$. Thus $\Gamma \supseteq \Omega_1 \cup \Omega_2$ and Γ must be the union of some Ω_i's. Therefore Γ is a block of $\bar{H}$ on $\mathcal{B}$. But $\bar{H}$ is primitive on $\mathcal{B}$ and so, since $\Omega_1 \subset \Gamma$, we must have that $\Gamma = \Omega$, which is a contradiction.

Hence we must have that $\Gamma \subseteq \Omega_1$, which implies, as Γ is a block of $K_1 \times \cdots \times K_m$, that Γ is a block of K_1 and, in particular, because of the transitivity of K_1 on Ω_1, the length of Γ divides k. □

3.6 Maximal subgroups of the symmetric group

Theorem 3.6.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n > 2$. Then, for all $r \geq 1$ such that $n \neq 2r$, the group*

$$L = \mathrm{Sym}(n-r) \times \mathrm{Sym}(r)$$

is a maximal subgroup of G.

Proof. Let $r \geq 1$ be an integer such that $2r < n$. Consider a partition of Ω into two subsets Ω_1 and Ω_2 such that $|\Omega_1| = n - r$ and $|\Omega_2| = r$ and set $L = \mathrm{Sym}(\Omega_1) \times \mathrm{Sym}(\Omega_2)$. Then L is not transitive on Ω and Ω_1 and Ω_2 are the orbits of L on Ω.

Now let M be a subgroup of G properly containing L. Then M is transitive on Ω. Let $\alpha \in \Omega$. The orbits of M_α on Ω are the union of the orbits of L_α on Ω. Also, as M is transitive on Ω, all stabilizers in M are conjugate and so, by Proposition 2.1.4, for all $\alpha \in \Omega$, the M_α's produce on Ω the same kind of decomposition into orbits. But, if $\alpha \in \Omega_1$, then the orbits of L_α on Ω have length

$$1, \;\; n-r-1 \quad \text{and} \quad r,$$

whereas, if $\alpha \in \Omega_2$, then the orbits of L_α on Ω have length

$$n-r, \;\; 1 \quad \text{and} \quad r-1.$$

This implies, as $n \neq 2r$, that M_α cannot have three orbits on Ω. So M_α has on Ω two orbits which are $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$. Therefore M_α is transitive on $\Omega \setminus \{\alpha\}$ and so M is 2-transitive on Ω. Hence M is primitive and, since M contains transpositions, by Theorem 3.2.9, we get that $M = G$. □

Theorem 3.6.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n > 1$. Then, for all integers k and m such that $n = km$, the group*

$$L = \mathrm{Sym}(k) \wr \mathrm{Sym}(m)$$

is a maximal subgroup of G.

Proof. First, by Proposition 3.5.1, L is the stabilizer in G of a block system of m blocks of length k and L is imprimitive.

Now let $M \leqslant G$ such that $L < M$. If M is primitive, then, as M contains transpositions, by Theorem 3.2.9, $M = G$. So assume that M is imprimitive. Then, as $M \neq L$, M has a nontrivial block system of blocks of length different from k and so L has a nontrivial block of length different from k, since $L \leqslant M$, against Theorem 3.5.3. Thus L is a maximal subgroup of G. □

Chapter 4

Sylow p-subgroups of the symmetric group

The order and the structure of Sylow p-subgroups of the symmetric group have been known for many years and many references can be found about the topic. Among the others we recall Dixon [10] and Huppert [15], who both refer to the same paper by Kaloujnine [20] from 1948. Further references are a paper by Findlay [12] from 1904 and a paper by Weir [39] from 1955. Here we present our own proofs.

4.1 The order of a Sylow p-subgroup

Definition 4.1.1. *Let $k \in \mathbb{N}$ and p be a prime. The* **weight of k with respect to p** *is the highest natural number r such that p^r divides k, that is, $r \in \mathbb{N}$ such that p^r divides k and p^{r+1} does not divide k.*

The weight of k with respect to p will be denoted by

$$w_p(k).$$

Clearly, $p|k$ if, and only if, $w_p(k) > 0$.
Let $k \in \mathbb{N}$ and p be a prime. By definition, the weight of $k!$ with respect to p is that natural number α such that p^α is the order of a Sylow p-subgroup of $\mathrm{Sym}(k)$.

Now take a factorization of k

$$k = k_1 \cdot k_2 \cdot \ldots \cdot k_l.$$

Since p is a prime, the weight of k with respect to p is given by the sum of the weights with respect to p of all the elements of the factorization, so

$$w_p(k) = \sum_{i=1}^{l} w_p(k_i).$$

In particular, since

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (k-1) \cdot k$$

is a factorization of $k!$, the weight of $k!$ with respect to p is given by the sum of the weights with respect to p of all integers h such that $1 \leq h \leq k$, that is,

$$w_p(k!) = \sum_{1 \leq h \leq k} w_p(h).$$

Since $w_p(h) > 0$ if, and only if, $p|h$, it follows that the weight of $k!$ with respect to p is given by the sum of the weights with respect to p of all p-multiples h such that $1 \leq h \leq k$, that is, in the natural factorization of $k!$ the factors giving a contribution to the order of a Sylow p-subgroup are the p-multiples.

Lemma 4.1.2. *Suppose that p is a prime and $n \in \mathbb{N}$. Then the order of a Sylow p-subgroup of* $\mathrm{Sym}(p^n)$ *is*

$$p^{p^{n-1}+p^{n-2}+\cdots+p+1} = p^{\frac{p^n-1}{p-1}}.$$

Proof. Let $S \in \mathrm{Syl}_p(\mathrm{Sym}(p^n))$. We have to determine the weight of $(p^n)!$ with respect to p. We do this by determining the number of integers less or equal to p^n with given weight and then summing these numbers to obtain the weight of $(p^n)!$. As we have just seen, it is enough to consider p-multiples less or equal to p^n. The biggest p-multiple dividing $(p^n)!$ is $p^n = (p^{n-1})p$. So there exist p^{n-1} multiples of p dividing $(p^n)!$. Each of them has weight at least 1, since it is a p-multiple, so they give p^{n-1} as total weight. Every p of them there exists one of weight at least 2, so there are p^{n-2} multiples of p which have weight at least 2, which give p^{n-2} as contribution. In general, for each p consecutive p-multiples of weight at least j

$$(hp+1)p^j, \quad (hp+2)p^j, \ldots$$
$$\ldots, (hp+p-1)p^j, \quad (hp+p)p^j = [(h+1)p]p^j = (h+1)p^{j+1},$$

there is a multiple of weight at least $j + 1$. And so on until we reach $(p^{n-1})p$, which is the only one of weight n. Therefore, $|S| = p^{\alpha}$, with

$$\alpha = p^{n-1} + p^{n-2} + \cdots + p + 1 = (p^n - 1)/(p - 1).$$

$\square$

Lemma 4.1.3. *Suppose that p is a prime and k is an integer such that $1 \leq k < p$. Then the order of a Sylow p-subgroup S of* $\mathrm{Sym}(kp^n)$ *is*

$$p^{k(p^{n-1}+p^{n-2}+\cdots+p+1)}.$$

Proof. The result follows by using the same approach as in the proof of Lemma 4.1.2. $\square$

Lemma 4.1.4. *Suppose that p is a prime and n is an integer and let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, be the p-adic decomposition of n. Then a Sylow p-subgroup S of $\mathrm{Sym}(n)$ *has order p^{α}, with*

$$\alpha = k_t(p^{t-1} + \cdots + p + 1) + k_{t-1}(p^{t-2} + \cdots + p + 1) + \cdots + k_2(p + 1) + k_1.$$

Proof. Let

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, be the p-adic decomposition of n and suppose that $k_t \neq 0$. We wish to prove that

$$w_p(n!) = \sum_{j=0}^{t} w_p((k_j p^j)!) = w_p(k_0!) + w_p((k_1 p)!) + \cdots + w_p((k_t p^t)!).$$

Consider the following factorization of $n!$:

$$\begin{aligned} n! =& [(k_t p^t)!][(k_t p^t + 1) \ldots (k_t p^t + k_{t-1} p^{t-1})] \\ & [(k_t p^t + k_{t-1} p^{t-1} + 1) \ldots (k_t p^t + k_{t-1} p^{t-1} + k_{t-2} p^{t-2})] \ldots \\ & \ldots [(k_t p^t + \cdots + k_1 p + 1) \ldots (k_t p^t + \cdots + k_1 p + k_0)], \end{aligned}$$

that is,

$$n! = d_0 \cdot d_1 \cdot \ldots \cdot d_t,$$

with

$$d_i = \prod_{z=1}^{k_i p^i} \left(\sum_{j=i+1}^{t} k_j p^j + z \right), \ i = 0, \dots, t.$$

Then

$$w_p(n!) = \sum_{i=0}^{t} w_p(d_i).$$

But, for all $i = 0, \dots, t$ and for all $z = 1, \dots, k_i p^i$,

$$w_p \left(\sum_{j=i+1}^{t} k_j p^j + z \right) = w_p(z).$$

So, for all $i = 0, \dots, t$, $w_p(d_i) = w_p((k_i p^i)!)$ and we get the result. □

4.2 The structure of a Sylow p-subgroup

Theorem 4.2.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$, where p is a prime and $n \in \mathbb{N}$. Then a Sylow p-subgroup of G is isomorphic to the wreath product of n copies of a cyclic group of order p acting on p points.*

Proof. Let Δ be a set of cardinality p and let C_p denote a cyclic group of order p acting on Δ. Let W be the wreath product of n copies of C_p and set $H = \mathrm{Sym}(\Delta^n)$, with Δ^n cartesian product of n copies of the set Δ. Then $W \leqslant H \cong G$ and it will suffice to show that W is a Sylow p-subgroup of H, that is, that W has the right order. By Theorem 2.6.6, the wreath product of k copies of C_p acts on p^k points. Hence, from Theorem 2.6.2 it follows that

$$|W| = |C_p|^{p^{n-1}} |C_p|^{p^{n-2}} \dots |C_p|^p |C_p| = p^{p^{n-1}+p^{n-2}+\dots+p+1},$$

as required by Lemma 4.1.2. □

Theorem 4.2.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = kp^n$, p prime and $1 \leq k < p$. Then a Sylow p-subgroup of G is given by the direct product of k factors, each isomorphic to a Sylow p-subgroup of $\mathrm{Sym}(\Delta)$, with $|\Delta| = p^n$.*

Proof. Let $\Omega_1, \ldots, \Omega_k$ be a partition of Ω into k subsets of order p^n. For $i = 1, \ldots, k$ let S_i be a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$ and set $S = S_1 \times \cdots \times S_k$. Then, from Lemma 4.1.2, it follows that

$$|S| = |S_1|^k = p^{k(p^{n-1}+p^{n-2}+\cdots+p+1)},$$

and so, by Lemma 4.1.3, $S \in \mathrm{Syl}_p(G)$. $\square$

Theorem 4.2.3. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. Suppose that p is a prime and let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, be the p-adic decomposition of n. Then a Sylow p-subgroup S of G is given by

$$S = S_1 \times \cdots \times S_t,$$

where, for $j = 1, \ldots, t$, S_j is a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$, with $\Omega_j \subseteq \Omega$ and $|\Omega_j| = k_j p^j$. In particular, S has no fixed points on Ω if and only if $k_0 = 0$, that is, $p|n$.

Proof. Let $\Omega_0, \Omega_1, \ldots, \Omega_t$ be a partition of Ω into $t+1$ subsets such that, for $j = 0, \ldots, t$, $|\Omega_j| = k_j p^j$. For $j = 1, \ldots, t$ let S_j be a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$ and set $S = S_1 \times \cdots \times S_t$. Then, $|S| = |S_1||S_2| \ldots |S_t|$, where, by Lemma 4.1.3,

$$|S_j| = p^{k_j(p^{j-1}+p^{j-2}+\cdots+p+1)}.$$

Thus, by Lemma 4.1.4, $S \in \mathrm{Syl}_p(G)$. In particular, it follows that S has k_0 fixed points on Ω and so S has no fixed points on Ω if and only if $p|n$. $\square$

4.3 The transitivity of a Sylow p-subgroup

Theorem 4.3.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$, where p is a prime and $n \in \mathbb{N}$. Then a Sylow p-subgroup of G is transitive on Ω.*

Proof. Let Δ be a set of cardinality p and let C_p denote a cyclic group of order p acting on Δ. By Theorem 4.2.1, a Sylow p-subgroup S of G is isomorphic to the wreath product W of n copies of C_p. But, since C_p is transitive on Δ, Theorem 2.6.6 implies that W is transitive on Δ^n, which is a set of cardinality p^n. Hence, since transitivity is preserved by similarity, we have that S is transitive on Ω. $\square$

Note that, if $|\Omega|$ is not a power of p, then, by Theorems 4.2.2 and 4.2.3, a Sylow p-subgroup S of $\mathrm{Sym}(\Omega)$ is not transitive on Ω. In this case we shall study the orbits of S on Ω.

Theorem 4.3.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = kp^n$, p prime and $1 \leq k < p$. Then a Sylow p-subgroup of G has k orbits on Ω, each of length p^n.*

Proof. According to Theorem 4.2.2, $S = S_1 \times \cdots \times S_k$, where, for $i = 1, \dots, k$, S_i is a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$ and $\Omega_1, \dots, \Omega_k$ is a partition of Ω into k subsets of order p^n. Then, by Theorem 4.3.1, it follows that the orbits of S on Ω are precisely the sets $\Omega_1, \dots, \Omega_k$. $\square$

Theorem 4.3.3. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. Suppose that p is a prime and let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \dots, t$, be the p-adic decomposition of n. Then, for all $j = 0, \dots, t$, a Sylow p-subgroup S of G has k_j orbits on Ω, each of length p^j.

Proof. Let $\Omega_0, \Omega_1, \dots, \Omega_t$ be a partition of Ω into $t+1$ subsets such that, for $j = 0, \dots, t$, $|\Omega_j| = k_j p^j$. Then, by Theorem 4.2.3, $S = S_1 \times \cdots \times S_t$, where, for $j = 1, \dots, t$, S_j is a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$ and, by Theorem 4.3.2, S_j has k_j orbits on Ω_j. Hence S has k_j orbits on Ω, each of length p^j, for all $j = 1, \dots, t$. Furthermore, since $\Omega_0 = \mathrm{Fix}_\Omega(S)$, S has other k_0 orbits, each of length 1, namely the sets $\{\omega\}$, for $\omega \in \Omega_0$. $\square$

4.4 Blocks of a Sylow p-subgroup

Proposition 4.4.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$, and let $S \in \mathrm{Syl}_p(G)$. Then every block of S has length a power of p. Moreover, S has a block of length p^r, for all $r = 1, \dots, n$.*

Proof. By Theorem 4.3.1, S is transitive on Ω and so, by Proposition 3.1.4, the length of every block of S is a power of p. Moreover, by Theorem 4.2.1 and by the associativity of the wreath product, we have that S is isomorphic to a subgroup of $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(p^{n-r})$, for all $r = 1, \dots, n$, where, by Proposition 3.5.1, $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(p^{n-r})$ is the stabilizer of a block system whose blocks have length p^r. Therefore S has blocks of length p^r, for all $r = 1, \dots, n$. $\square$

Proposition 4.4.2. *Let* $G = \mathrm{Sym}(\Omega)$, *with* $|\Omega| = kp^n$, $1 < k < p$, *and let* $S \in \mathrm{Syl}_p(G)$. *Then* S *has blocks of length* p^r, *for all* $r = 1, \ldots, n$.

Proof. By Theorem 4.2.2, $S = S_1 \times \cdots \times S_k$, with $S_i \in \mathrm{Syl}_p(\mathrm{Sym}(\Omega_i))$ and $|\Omega_i| = p^n$, for all $i = 1, \ldots, k$. Now, by Proposition 4.4.1, each S_i has blocks of length p^r, for all $r = 1, \ldots, n$, but, as $S_{|\Omega_i} \cong S_i$, a block of S_i is also a block of S and so we get the result. $\square$

Proposition 4.4.3. *Let* $G = \mathrm{Sym}(\Omega)$, *with* $|\Omega| = n$, *and let* $S \in \mathrm{Syl}_p(G)$. *Let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, *for all* $j = 0, \ldots, t$, *and* $k_t \neq 0$, *be the* p*-adic decomposition of* n. *Then* S *has blocks of length* p^r, *for all* $r = 1, \ldots, t$, *and blocks of length* $k_i p^i$, *for all* $i \in \{j \mid k_j \neq 0\}$.

Proof. By Theorem 4.2.3, $S = S_1 \times \cdots \times S_t$, with $S_j \in \mathrm{Syl}_p(\mathrm{Sym}(\Omega_j))$ and $|\Omega_j| = k_j p^j$, for all $j = 1, \ldots, t$. Clearly, for each $i \in \{j \mid k_j \neq 0\}$, S_i has the trivial block Ω_i of length $k_i p^i$ and, by Proposition 4.4.2, S_t has blocks of length p^r, for all $r = 1, \ldots, t$. But, as $S_{|\Omega_j} \cong S_j$, a block of S_j is also a block of S and so we get the result. $\square$

Chapter 5

The normalizer of a Sylow p-subgroup of the symmetric group

This chapter is devoted to understanding and describing the structure of the normalizer of a Sylow p-subgroup of the symmetric group, the crucial case being when the degree of the symmetric group is a power of p (see [5], [11]). For this case, a detailed construction of the normalizer, based on a description of the Sylow p-subgroup and illustrated by an example, is presented. Some interesting facts about overgroups of the normalizer are also proved.

5.1 A description of the Sylow p-subgroup of $\mathrm{Sym}(p^n)$

Let $G = \mathrm{Sym}(p^n)$, with p prime and $n \in \mathbb{N}$. Let $T \in \mathrm{Syl}_p(G)$. In this section we shall give a description of T in terms of its generators and shall study the complete block systems of T. In doing this we introduce some notation, which will be used later when describing the structure of $N_G(T)$ and when studying some minimal parabolic subgroups of G with respect to $N_G(T)$.

According to Theorem 4.2.1, T is isomorphic to the wreath product $\bar{T}$ of n copies of a cyclic group of order p acting on p points. Set

$$\bar{T} = \langle \bar{x}_1 \rangle \wr \cdots \wr \langle \bar{x}_n \rangle.$$

Then we have that

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

where, for $i = 1, \ldots, n$, x_i is the image in G of the element $\bar{x}_i \in \mathrm{Sym}(p)$. In particular, x_i is the product of p^{i-1} disjoint cycles of length p and so the order of x_i is p and x_i acts on p^i points. We illustrate this with an example.

Example 5.1:
Let $G = \mathrm{Sym}(27)$, so $p = 3$ and $n = 3$. Denote by T a Sylow 3-subgroup of G and by $\bar{T}$ the wreath product of three copies of a cyclic group of order 3. If we set

$$\bar{T} = \langle(1\ 2\ 3)\rangle \wr \langle(1\ 2\ 3)\rangle \wr \langle(1\ 2\ 3)\rangle,$$

then we have that T can be generated by the elements $x_1, x_2, x_3 \in G$ such that

$x_1 = (1\ 2\ 3)$,

$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$,

$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$.

In fact, the effect of the action of x_2 on the set $\{1, \ldots, 9\}$ is that of a 3-cycle permuting transitively the sets $\{1, 2, 3\}$, $\{4, 5, 6\}$ and $\{7, 8, 9\}$. Similarly, x_3 acts on the set $\{1, \ldots, 27\}$ by permuting transitively the sets $\{1, \ldots, 9\}$, $\{10, \ldots, 18\}$ and $\{19, \ldots, 27\}$.
Notice that, given $\bar{T}$, neither T nor its generators are uniquely determined. ■

For $i = 1, \ldots, n-1$ set

$$T_{n-i} = \langle x_{i+1}, \ldots, x_n \rangle.$$

Then $T_{n-i} \cong \langle \bar{x}_{i+1} \rangle \wr \cdots \wr \langle \bar{x}_n \rangle$ and so T_{n-i} is a subgroup of T isomorphic to a Sylow p-subgroup of $\mathrm{Sym}(p^{n-i})$. Furthermore, we have that

$$T = \langle x_1 \rangle^{T_{n-1}} \rtimes \langle x_2 \rangle^{T_{n-2}} \rtimes \cdots \rtimes \langle x_{n-1} \rangle^{T_1} \rtimes \langle x_n \rangle,$$

where $\langle x_i \rangle^{T_{n-i}}$ denotes the normal closure of $\langle x_i \rangle$ in T_{n-i}. Notice that the action of T_{n-i} on $\langle x_i \rangle$ by conjugation corresponds in $\bar{T}$ to the natural action of the permutation group $\langle \bar{x}_{i+1} \rangle \wr \cdots \wr \langle \bar{x}_n \rangle$ on p^{n-i} points as defined in Theorem 2.6.2.
Finally for $i = 1, \ldots, n-1$ set

$$S_i = \langle x_1 \rangle^{T_{n-1}} \rtimes \cdots \rtimes \langle x_i \rangle^{T_{n-i}} = \langle x_1, \ldots, x_i \rangle^{T_{n-i}}.$$

Then S_i is the direct product of p^{n-i} copies of $\langle x_1, \ldots, x_i \rangle$, that is, the direct product of p^{n-i} copies of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$, and $S_i = S_{i-1} \rtimes \langle x_i \rangle^{T_{n-i}}$. Moreover

$$T = S_i \rtimes T_{n-i}$$

and S_i corresponds to the base group of the wreath product

$$\bar{T} = (\langle \bar{x}_1 \rangle \wr \cdots \wr \langle \bar{x}_i \rangle) \wr (\langle \bar{x}_{i+1} \rangle \wr \cdots \wr \langle \bar{x}_n \rangle).$$

Let us see with an example what these subgroups of T look like.

Example 5.2:

Let $G = \mathrm{Sym}(27)$, that is, $p = 3$ and $n = 3$. Let T be a Sylow 3-subgroup of G and write $T = \langle x_1, x_2, x_3 \rangle$, with x_1, x_2, x_3 as in Example 5.1. Then

$$\begin{aligned} T_1 &= \langle x_3 \rangle \cong \langle (1\ 2\ 3) \rangle \leqslant \mathrm{Sym}(3), \\ T_2 &= \langle x_2, x_3 \rangle = \langle x_2 \rangle^{\langle x_3 \rangle} \rtimes \langle x_3 \rangle \cong \langle (1\ 2\ 3) \rangle \wr \langle (1\ 2\ 3) \rangle \leqslant \mathrm{Sym}(3) \wr \mathrm{Sym}(3) \end{aligned}$$

and thus

$$\begin{aligned} S_1 &= \langle x_1 \rangle^{T_2} = \langle x_1 \rangle^{\langle x_2, x_3 \rangle}, \\ S_2 &= \langle x_1 \rangle^{T_2} \rtimes \langle x_2 \rangle^{T_1} = \langle x_1 \rangle^{\langle x_2, x_3 \rangle} \rtimes \langle x_2 \rangle^{\langle x_3 \rangle}, \\ T &= \langle x_1, x_2, x_3 \rangle = \langle x_1 \rangle^{\langle x_2, x_3 \rangle} \rtimes \langle x_2 \rangle^{\langle x_3 \rangle} \rtimes \langle x_3 \rangle, \end{aligned}$$

where

$$\begin{aligned} \langle x_3 \rangle &= \langle (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26) \\ &\qquad (9\ 18\ 27) \rangle, \\ \langle x_2 \rangle^{\langle x_3 \rangle} &= \langle (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9) \rangle \times \langle (10\ 13\ 16)(11\ 14\ 17)(12\ 15\ 18) \rangle \times \\ &\qquad \langle (19\ 22\ 25)(20\ 23\ 26)(21\ 24\ 27) \rangle, \\ \langle x_1 \rangle^{\langle x_2, x_3 \rangle} &= \langle (1\ 2\ 3) \rangle \times \langle (4\ 5\ 6) \rangle \times \langle (7\ 8\ 9) \rangle \times \langle (10\ 11\ 12) \rangle \times \langle (13\ 14\ 15) \rangle \times \langle (16\ 17\ 18) \rangle \times \\ &\qquad \langle (19\ 20\ 21) \rangle \times \langle (22\ 23\ 24) \rangle \times \langle (25\ 26\ 27) \rangle. \end{aligned}$$

■

We now want to study the subgroups $\langle x_i \rangle^{T_{n-i}}$ in more detail. Since T_{n-i} is a transitive permutation group acting on p^{n-i} points and conjugation of x_i by elements of T_{n-i} produces disjoint cycles, we have that $\langle x_i\rangle^{T_{n-i}}$ is the direct product of p^{n-i} cyclic groups of order p each generated by a conjugate of x_i in T_{n-i}. We shall present a way to produce the p^{n-i} conjugates of x_i that generate $\langle x_i\rangle^{T_{n-i}}$, that is, we shall implicitly provide a set X of elements of T_{n-i} such that $\langle x_i\rangle^{T_{n-i}}$ is generated by the conjugates x_i^x, for all $x \in X$. Of course, such a set is not unique.

For $i = 1, \dots, n-1$ and $j = 2, \dots, n$, $j > i$, define

$$F_j(\langle x_i\rangle) = \prod_{e=0}^{p-1} \langle x_i^{x_j^e}\rangle.$$

Clearly, $F_j(\langle x_i\rangle) = \langle x_i\rangle^{\langle x_j\rangle}$ and $F_j(\langle x_i\rangle)$ is an elementary abelian p-group of order p^p. For $h = 2, \dots, n$, $h > j > i$, define

$$(F_h \circ F_j)(\langle x_i\rangle) = F_h(F_j(\langle x_i\rangle)) = \prod_{e=0}^{p-1} F_h(\langle x_i^{x_j^e}\rangle).$$

Then $(F_h \circ F_j)(\langle x_i\rangle) \leqslant \langle x_i\rangle^{\langle x_j, x_h\rangle}$ and $(F_h \circ F_j)(\langle x_i\rangle)$ is the direct product of p^2 cyclic groups of order p each generated by a conjugate of x_i in $\langle x_j, x_h\rangle$. Thus $(F_h \circ F_j)(\langle x_i\rangle) = \langle x_i\rangle^{\langle x_j, x_h\rangle}$. In particular, it follows that

$$\langle x_i\rangle^{T_{n-i}} = \langle x_i\rangle^{\langle x_{i+1}, \dots, x_n\rangle} = (F_n \circ \cdots \circ F_{i+1})(\langle x_i\rangle)$$

and so

$$T = (F_n \circ \cdots \circ F_2)(\langle x_1\rangle) \rtimes \cdots \rtimes F_n(\langle x_{n-1}\rangle) \rtimes \langle x_n\rangle,$$

where the i-th factor $(F_n \circ \cdots \circ F_{i+1})(\langle x_i\rangle)$ of the semidirect product is an elementary abelian p-group of order $p^{p^{n-i}}$.

The next example will clarify how the construction of $\langle x_i\rangle^{T_{n-i}}$ in terms of $F_{i+1}, \dots, F_n$ works.

Example 5.3:

Let $G = \mathrm{Sym}(27)$, that is, $p = 3$ and $n = 3$, and let x_1, x_2, x_3 be as in Example 5.1. So

$x_1 = (1\ 2\ 3)$,

$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$,

$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$.

Recall from Example 5.2 that

$$\begin{aligned}
\langle x_2\rangle^{\langle x_3\rangle} &= \langle (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)\rangle \times \langle (10\ 13\ 16)(11\ 14\ 17)(12\ 15\ 18)\rangle \times \\
&\quad \langle (19\ 22\ 25)(20\ 23\ 26)(21\ 24\ 27)\rangle, \\
\langle x_1\rangle^{\langle x_2,x_3\rangle} &= \langle (1\ 2\ 3)\rangle \times \langle (4\ 5\ 6)\rangle \times \langle (7\ 8\ 9)\rangle \times \langle (10\ 11\ 12)\rangle \times \langle (13\ 14\ 15)\rangle \times \langle (16\ 17\ 18)\rangle \times \\
&\quad \langle (19\ 20\ 21)\rangle \times \langle (22\ 23\ 24)\rangle \times \langle (25\ 26\ 27)\rangle.
\end{aligned}$$

Then it is easy to check that

$$\begin{aligned}
\langle x_2\rangle^{\langle x_3\rangle} &= \langle x_2\rangle \times \langle x_2^{x_3}\rangle \times \langle x_2^{x_3^2}\rangle = F_3(\langle x_2\rangle), \\
\langle x_1\rangle^{\langle x_2,x_3\rangle} &= \langle x_1\rangle \times \langle x_1^{x_2}\rangle \times \langle x_1^{x_2^2}\rangle \times \langle x_1^{x_3}\rangle \times \langle x_1^{x_2x_3}\rangle \times \langle x_1^{x_2^2x_3}\rangle \times \langle x_1^{x_3^2}\rangle \times \langle x_1^{x_2x_3^2}\rangle \times \langle x_1^{x_2^2x_3^2}\rangle \\
&= F_3(F_2(\langle x_1\rangle)) = (F_3\circ F_2)(\langle x_1\rangle).
\end{aligned}$$

■

We shall now describe some complete block systems of T, which arise from the description of T given above. As we shall see, these are the only complete block systems of T.

Write $G = \mathrm{Sym}(\Omega)$, where Ω is a set of cardinality p^n. Recall that, for $\Gamma \subseteq \Omega$ and for $g \in G$, the set $\Gamma^g = \{\gamma^g \mid g \in G\}$ is called the conjugate of Γ by g.

For $i = 1,\dots,n-1$, denote by Δ_i the set of orbits determined by S_i in its action on Ω. Since S_i is the direct product of p^{n-i} copies of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$, we have that $|\Delta_i| = p^{n-i}$ and every element of Δ_i is an orbit of length p^i. Set $\Omega_i = \Omega \setminus \mathrm{Fix}_\Omega(x_i)$, so $x_i \in \mathrm{Sym}(\Omega_i)$ and $|\Omega_i| = p^i$. Then $\Omega_i \in \Delta_i$ and every element of Δ_i is a conjugate of Ω_i in T_{n-i}. In fact, $\langle x_i\rangle^{T_{n-i}} = (F_n\circ\cdots\circ F_{i+1})(\langle x_i\rangle)$ is the direct product of p^{n-i} cyclic groups of order p, each generated by a conjugate of x_i in T_{n-i} and acting on p^i points. So, if we set

$$(F_n\circ\cdots\circ F_{i+1})(\langle x_i\rangle) = \prod_{j=1}^{p^{n-i}} \langle x_i^{t_j}\rangle,$$

for some fixed $t_j \in T_{n-i}$ determined by $F_{i+1},\dots,F_n$, then we have that

$$\Delta_i = \{\Omega_i^{t_j} \mid j = 1,\dots,p^{n-i}\}.$$

Before proceeding with the proof of some properties of the sets Δ_i we shall construct such sets for the case $G = \mathrm{Sym}(27)$.

Example 5.4:

Consider the situation studied in Examples 5.1, 5.2 and 5.3, with $p = 3$, $n = 3$ and

$x_1 = (1\ 2\ 3)$,

$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$,

$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$.

Then we have that

$$\Omega_1 = \{1, 2, 3\},$$
$$\Omega_2 = \{1, \dots, 9\}$$

and so we get

$$\begin{aligned}
\Delta_1 &= \{\Omega_1, \Omega_1^{x_2}, \Omega_1^{x_2^2}, \Omega_1^{x_3}, \Omega_1^{x_2 x_3}, \Omega_1^{x_2^2 x_3}, \Omega_1^{x_3^2}, \Omega_1^{x_2 x_3^2}, \Omega_1^{x_2^2 x_3^2}\} \\
&= \{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{10,11,12\}, \{13,14,15\}, \{16,17,18\}, \{19,20,21\}, \\
&\quad \{22,23,24\}, \{25,26,27\}\}, \\
\Delta_2 &= \{\Omega_2, \Omega_2^{x_3}, \Omega_2^{x_3^2}\} = \{\{1,\dots,9\}, \{10,\dots,18\}, \{19,\dots,27\}\},
\end{aligned}$$

as it follows also by looking at the orbits of S_1 and S_2 on Ω. ■

Lemma 5.1.1. *Let $i = 2, \dots, n-1$. Then every element of Δ_i is the (disjoint) union of p blocks belonging to Δ_{i-1}.*

Proof. Let $\Gamma \in \Delta_{i-1}$. Since the elements of Δ_{i-1} form a partition of Ω, it will suffice to show that Γ is contained in some element of Δ_i. Let $\Gamma \cap \Omega_i^{t_j} \neq \emptyset$, for some $j = 1, \dots, p^{n-i}$ and suppose that $\Gamma \cap \Omega_i^{t_j} \neq \Gamma$. Then $\Gamma \cap \Omega_i^{t_k} \neq \emptyset$, for some $k = 1, \dots, p^{n-i}$, $k \neq j$, and there exist $\alpha \in \Gamma \cap \Omega_i^{t_j}$ and $\beta \in \Gamma \cap \Omega_i^{t_k}$.

Now S_i is transitive on Γ, since Γ is an orbit of S_{i-1} and $S_{i-1} \leqslant S_i$. Therefore there exists $x \in S_i$ such that $\alpha^x = \beta$. But, since $\Omega_i^{t_j}$ is an orbit of S_i, we have that $(\Omega_i^{t_j})^x = \Omega_i^{t_j}$ and so $\beta \in (\Omega_i^{t_j})^x \cap \Omega_i^{t_k} = \Omega_i^{t_j} \cap \Omega_i^{t_k}$, which is a contradiction, since any two elements of Δ_i are disjoint. Therefore we must have $\Gamma \cap \Omega_i^{t_j} = \Gamma$, that is, $\Gamma \subseteq \Omega_i^{t_j}$. □

Lemma 5.1.2. *For $i = 1, \dots, n-1$, the set Δ_i is a complete block system of T of blocks of length p^i.*

Proof. Let $i = 1, \dots, n-1$ and write $T = S_i \rtimes T_{n-i}$. Then S_i is an intransitive normal subgroup of T and so, by Theorem 3.2.2, Δ_i is a complete block system of T. $\square$

Theorem 5.1.3. *Let $i = 1, \dots, n-1$ and let Γ be a block of T of length p^i. Then $\Gamma \in \Delta_i$. In particular, the set Δ_i is the unique complete block system of T of blocks of length p^i.*

Proof. Let $i = 1, \dots, n-1$ and let Γ be a block of T of length p^i. Suppose that $\Gamma \cap \Omega_i^{t_j} \neq \emptyset$, for some $j = 1, \dots, p^{n-i}$, and that $\Gamma \cap \Omega_i^{t_j} \neq \Omega_i^{t_j}$. Since the elements of Δ_i are orbits of S_i and S_i is the direct product of p^{n-i} copies of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$, there exists a direct factor S_{ij} of S_i such that $\Omega_i^{t_j} = \Omega \setminus \mathrm{Fix}_\Omega(S_{ij})$ and S_{ij} is transitive on $\Omega_i^{t_j}$. Therefore, for $\alpha \in \Omega_i^{t_j} \setminus (\Gamma \cap \Omega_i^{t_j})$ and $\beta \in \Gamma \cap \Omega_i^{t_j}$, there exists $x \in S_{ij}$ such that $\beta^x = \alpha$ and $\omega^x = \omega$, for all $\omega \in \Omega \setminus \Omega_i^{t_j}$. Then $\Gamma \cap \Gamma^x \neq \emptyset$, since

$$\emptyset \neq \Gamma \cap \left(\Omega \setminus \Omega_i^{t_j}\right) \subseteq \Gamma \cap \Gamma^x,$$

and $\Gamma \neq \Gamma^x$, since $\alpha \in \Gamma^x$ and $\alpha \notin \Gamma$, against the assumption that Γ is a block of T. Therefore we must have $\Gamma = \Omega_i^{t_j} \in \Delta_i$. $\square$

Corollary 5.1.4. *Let $G = \mathrm{Sym}(p^n)$ and let $T \in \mathrm{Syl}_p(G)$. Set $B = N_G(T)$. Then, for $i = 1, \dots, n-1$, B is contained in the stabilizer in G of the block system Δ_i. In particular, $B \leqslant N_G(S_i)$, for all $i = 1, \dots, n-1$.*

Proof. By Proposition 3.1.5, Δ_i^x is a complete block system of T, for all $x \in B$. But, by Theorem 5.1.3, Δ_i is the unique complete block system of T of blocks of length p^i. Therefore $\Delta_i^x = \Delta_i$, for all $x \in B$, and B is contained in the stabilizer in G of Δ_i.
In particular, since $\mathrm{Stab}_G(\Delta_i) \cong \mathrm{Sym}(p^i) \wr \mathrm{Sym}(p^{n-i})$, B normalizes the base group K of $\mathrm{Stab}_G(\Delta_i)$, which is equal to the direct product of p^{n-i} copies of $\mathrm{Sym}(p^i)$. Hence B normalizes $T \cap K = S_i$ and so $B \leqslant N_G(S_i)$. $\square$

Lemma 5.1.5. *Let $i = 1, \dots, n-1$. Then $N_G(S_i) = K_i \rtimes \mathrm{Sym}(\Delta_i)$, where K_i is the direct product of p^{n-i} copies of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$.*

Proof. First recall that S_i is the product of p^{n-i} copies of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$ and that Δ_i is the set of orbits of S_i on Ω. Then, since $S_i \trianglelefteq N_G(S_i)$, we have that $N_G(S_i)$ acts on Δ_i and so

$$N_G(S_i) \leqslant \mathrm{Stab}_G(\Delta_i) = G_i \rtimes \mathrm{Sym}(\Delta_i) \cong \mathrm{Sym}(\Omega_i) \wr \mathrm{Sym}(\Delta_i),$$

with G_i direct product of p^{n-i} copies of $\mathrm{Sym}(\Omega_i)$. Also $\mathrm{Sym}(\Delta_i) \leqslant N_G(S_i)$. Therefore

$$N_G(S_i) = (N_G(S_i) \cap G_i) \rtimes \mathrm{Sym}(\Delta_i) = N_{G_i}(S_i) \rtimes \mathrm{Sym}(\Delta_i) = K_i \rtimes \mathrm{Sym}(\Delta_i),$$

where, by Corollary 1.1.12, $K_i = N_{G_i}(S_i)$ is the direct product of p^{n-i} copies of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$. $\square$

Notice that K_i is precisely the base group of $N_G(S_i)$ with respect to Δ_i as defined in Section 3.5. Later we shall refer to K_i just as the base group of $N_G(S_i)$.

Last, using the notation introduced so far, we shall build a subgroup H of G containing T and isomorphic to the wreath product of n copies of $\mathrm{Hol}(\mathbb{Z}_p)$. Not only the normalizer in G of T will be constructed as a subgroup of H (see Section 5.2), but H will also play a central role in the study of minimal parabolic subgroups of $\mathrm{Sym}(p^n)$ (see Chapter 10).

Let $\bar{H}$ denote the wreath product of n copies of $\mathrm{Hol}(\mathbb{Z}_p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$ and suppose that $\bar{T} \leqslant \bar{H}$. Write

$$\bar{H} = \langle \bar{x}_1, \bar{y_1} \rangle \wr \cdots \wr \langle \bar{x}_n, \bar{y_n} \rangle,$$

with $\langle \bar{x}_i, \bar{y_i} \rangle \cong \mathrm{Hol}(\mathbb{Z}_p)$, for all $i = 1, \ldots, n$, that is, $\bar{y_i}$ is a $(p-1)$-cycle normalizing $\langle \bar{x}_i \rangle$. We define a subgroup H of G containing T and isomorphic to $\bar{H}$ by setting

$$H = \langle x_1, y_1, \ldots, x_n, y_n \rangle,$$

where, for $i = 1, \ldots, n$, y_i is the image in G of the element $\bar{y_i} \in \mathrm{Sym}(p)$, that is, $y_i \in \mathrm{Sym}(\Omega)$ and y_i is an element of order $p-1$ normalizing $\langle x_i \rangle$ and acting on the same set of points as $\langle x_i \rangle$. More precisely, since x_i is the product of p^{i-1} disjoint cycles of length p, we have that y_i is the product of p^{i-1} disjoint cycles of length $p-1$ each normalizing the subgroup generated by a factor of x_i. For a method of constructing cycles of length $p-1$ that normalize the subgroup generated by a p-cycle see Section 2.3.

For $i = 1, \ldots, n-1$, set

$$H_{n-i} = \langle x_{i+1}, y_{i+1}, \ldots, x_n, y_n \rangle.$$

Then

$$H = \langle x_1, y_1 \rangle^{H_{n-1}} \rtimes \cdots \rtimes \langle x_{n-1}, y_{n-1} \rangle^{H_1} \rtimes \langle x_n, y_n \rangle,$$

where $\langle x_i, y_i\rangle^{H_{n-i}} = \langle x_i\rangle^{H_{n-i}} \rtimes \langle y_i\rangle^{H_{n-i}}$. Also notice that, by Corollary 2.6.5, $\langle y_i\rangle^{H_{n-i}} = \langle y_i\rangle^{T_{n-i}}$ and so, extending the argument used before for $\langle x_i\rangle^{T_{n-i}}$, we have that

$$\langle y_i\rangle^{H_{n-i}} = (F_n \circ \cdots \circ F_{i+1})(\langle y_i\rangle)$$

and $\langle y_i\rangle^{H_{n-i}}$ is the direct product of p^{n-i} cyclic groups of order $p-1$.

Set $L_i = \langle y_i\rangle^{H_{n-i}}$ and $L_n = \langle y_n\rangle$. Then, for all $j > i$, L_i is normalized by L_j, since $L_j \leqslant H_{n-i}$. Therefore, for any i, j, L_i and L_j permute and

$$H = TL_1L_2 \dots L_{n-1}L_n.$$

For consistency with the previous examples, we shall build the subgroup H for $p = 3 = n$, though, as far as H is concerned, this case is not very appropriate, since $\mathrm{Hol}(\mathbb{Z}_3) \cong \mathrm{Sym}(3)$.

Example 5.5:

Let $G = \mathrm{Sym}(27)$, that is, $p = 3$ and $n = 3$. Let T be a Sylow 3-subgroup of G and write $T = \langle x_1, x_2, x_3\rangle$, with

$x_1 = (1\ 2\ 3)$,

$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$,

$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$.

Consider the elements

$y_1 = (2\ 3)$,

$y_2 = (4\ 7)(5\ 8)(6\ 9)$,

$y_3 = (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27)$.

For $i = 1, 2, 3$, y_i is an element of order 2 normalizing $\langle x_i\rangle$ and acting on the same set of points as x_i. Then $H = \langle x_1, y_1, x_2, y_2, x_3, y_3\rangle$ is a subgroup of G containing T and H is isomorphic to the wreath product

$$\bar{H} = \langle (1\ 2\ 3), (2\ 3)\rangle \wr \langle (1\ 2\ 3), (2\ 3)\rangle \wr \langle (1\ 2\ 3), (2\ 3)\rangle$$

of three copies of $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Moreover

$H_1 = \langle x_3, y_3\rangle \cong \langle (1\ 2\ 3), (2\ 3)\rangle$

$H_2 = \langle x_2, y_2, x_3, y_3\rangle = \langle x_2, y_2\rangle^{\langle x_3\rangle} \rtimes \langle x_3, y_3\rangle \cong \langle (1\ 2\ 3), (2\ 3)\rangle \wr \langle (1\ 2\ 3), (2\ 3)\rangle$

and thus

$$\begin{aligned}
L_1 &= \langle y_1\rangle^{H_2} = \langle y_1\rangle^{\langle x_2,x_3\rangle} = F_3(F_2(\langle y_1\rangle)) = (F_3\circ F_2)(\langle y_1\rangle)\\
&= \langle y_1\rangle \times \langle y_1^{x_2}\rangle \times \langle y_1^{x_2^2}\rangle \times \langle y_1^{x_3}\rangle \times \langle y_1^{x_2x_3}\rangle \times \langle y_1^{x_2^2x_3}\rangle \times \langle y_1^{x_3^2}\rangle \times \langle y_1^{x_2x_3^2}\rangle \times \langle y_1^{x_2^2x_3^2}\rangle\\
&= \langle (2\ 3)\rangle \times \langle (5\ 6)\rangle \times \langle (8\ 9)\rangle \times \langle (11\ 12)\rangle \times \langle (14\ 15)\rangle \times \langle (17\ 18)\rangle \times \langle (20\ 21)\rangle \times\\
&\quad \langle (23\ 24)\rangle \times \langle (26\ 27)\rangle,\\
L_2 &= \langle y_2\rangle^{H_1} = \langle y_2\rangle^{\langle x_3\rangle} = F_3(\langle y_2\rangle) = \langle y_2\rangle \times \langle y_2^{x_3}\rangle \times \langle y_2^{x_3^2}\rangle\\
&= \langle (4\ 7)(5\ 8)(6\ 9)\rangle \times \langle (13\ 16)(14\ 17)(15\ 18)\rangle \times \langle (22\ 25)(23\ 26)(24\ 27)\rangle,\\
L_3 &= \langle y_3\rangle = \langle (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27)\rangle.
\end{aligned}$$

■

5.2 The normalizer in $\mathrm{Sym}(p^n)$

Let $G = \mathrm{Sym}(p^n)$, for some prime p. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Our aim in this section is to describe the structure of the normalizer B. We shall first build a subgroup of B of order $|T|(p-1)^n$ and then prove that the number $|T|(p-1)^n$ is an upper bound for the order of B. We shall use the notation introduced in Section 5.1.

For $a \in G$ and for $j = 1,\dots,n$, define the map f_j from G to itself by setting

$$f_j(a) = \prod_{e=0}^{p-1} a^{x_j^e}.$$

Set $h_n = y_n$ and, for $i = 1,\dots,n-1$,

$$h_i = (f_n \circ \cdots \circ f_{i+1})(y_i).$$

Then h_i is the product of p^{n-i} conjugates of y_i in T_{n-i} and so, since y_i is the product of p^{i-1} disjoint cycles of length $p-1$, h_i is the product of p^{n-1} disjoint cycles of length $p-1$. In particular, the order of h_i is $p-1$. More precisely, as we shall see in the following example, h_i is the product of the p^{n-i} generators of the homocyclic group $L_i = (F_n \circ \cdots \circ F_{i+1})(\langle y_i\rangle)$ and, in particular, $h_i \in L_i$.

Example 5.6:

Let $G = \mathrm{Sym}(27)$, that is, $p = 3$ and $n = 3$. Let T be a Sylow 3-subgroup of G and write

$T = \langle x_1, x_2, x_3 \rangle$, with

$$x_1 = (1\ 2\ 3),$$
$$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9),$$
$$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27).$$

Consider the elements

$$y_1 = (2\ 3),$$
$$y_2 = (4\ 7)(5\ 8)(6\ 9),$$
$$y_3 = (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27).$$

Then we have that

$$h_1 = (2\ 3)(5\ 6)(8\ 9)(11\ 12)(14\ 15)(17\ 18)(20\ 21)(23\ 24)(26\ 27),$$
$$h_2 = (4\ 7)(5\ 8)(6\ 9)(13\ 16)(14\ 17)(15\ 18)(22\ 25)(23\ 26)(24\ 27),$$
$$h_3 = (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27)$$

and each element h_i is the product of the generators of the homocyclic group L_i given in Example 5.5. ■

We now want to show some properties of the elements h_i.

Lemma 5.2.1. *For $i = 1, \dots, n$, we have that*

$$[h_i, H_{n-i}] = 1.$$

Proof. Consider the group $L_i = \langle y_i \rangle^{H_{n-i}}$. In its action by conjugation on $\langle y_i \rangle$, H_{n-i} permutes the generators of L_i and so H_{n-i} centralizes h_i, since h_i is the product of all such elements. □

Theorem 5.2.2. *Set $N = \langle h_1, \dots, h_n \rangle$. Then N is abelian. Furthermore, $N = \langle h_1 \rangle \times \cdots \times \langle h_n \rangle$ and $|N| = (p-1)^n$.*

Proof. Let $i = 1, \dots, n-1$. For $j > i$, $h_j \in L_j \leqslant H_{n-j+1} \leqslant H_{n-i}$ and so, by Lemma 5.2.1, $[h_i, h_j] = 1$. Therefore $[h_i, h_j] = 1$, for all $i, j = 1, \dots, n-1$, and N is abelian. Moreover, since $L_i \cap \langle L_j \mid j \neq i \rangle = 1$, we have that $\langle h_i \rangle \cap \langle h_j \mid j \neq i \rangle = 1$. Therefore $N = \langle h_1 \rangle \times \cdots \times \langle h_n \rangle$ and $|N| = (p-1)^n$. □

Theorem 5.2.3. *Let $G = \mathrm{Sym}(p^n)$ and let $T \in \mathrm{Syl}_p(G)$. Write $T = \langle x_1, \dots, x_n \rangle$ and set $N = \langle h_1, \dots, h_n \rangle$. Then N normalizes T.*

Proof. By definition, $h_n = y_n$ normalizes $\langle x_n \rangle$ and $h_n \in H_1$, which normalizes S_{n-1}. Thus, since $T = S_{n-1} \rtimes \langle x_n \rangle$, we have that h_n normalizes T.

Now let $i = 1, \dots, n-1$ and write $T = S_i \rtimes T_{n-i}$, where $S_i = S_{i-1} \rtimes \langle x_i \rangle^{T_{n-i}}$. Then, since $T_{n-i} \leqslant H_{n-i}$, by Lemma 5.2.1, h_i centralizes T_{n-i}. But, $h_i \in L_i$ and L_i normalizes $\langle x_i \rangle^{T_{n-i}}$, so h_i normalizes $\langle x_i \rangle^{T_{n-i}}$. Finally, h_i normalizes S_{i-1}, since $h_i \in H_{n-i+1}$, which normalizes S_{i-1}, by Corollary 2.6.5. Thus we can conclude that h_i normalizes T, for all $i = 1, \dots, n$. $\square$

Theorem 5.2.4. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p$. Then the normalizer in G of a Sylow p-subgroup T of G is isomorphic to $\mathrm{Hol}(T)$ and has order $p(p-1)$.*

Proof. By Theorem 4.2.1, T is isomorphic to a cyclic group C_p of order p acting on p points. So T is transitive on Ω and $|T| = \deg T$, which implies, by Proposition 2.1.10, that T is regular on Ω. Then from Proposition 2.5.1 it follows that $N_G(T) \cong \mathrm{Hol}(T) \cong T \rtimes \mathrm{Aut}(T)$. Moreover, since $\mathrm{Aut}(T) \cong \mathrm{Aut}(C_p) \cong C_{p-1}$, we get that $|N_G(T)| = p(p-1)$. $\square$

Theorem 5.2.5. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$, and let $T \in \mathrm{Syl}_p(G)$. Then*

$$|N_G(T)| \leq |T|(p-1)^n.$$

Proof. We shall prove the theorem by induction on n. If $n = 1$, then the result follows from Theorem 5.2.4. So assume that $n > 1$ and write $T = S_1 \rtimes T_{n-1}$, where $S_1 = \langle x_1 \rangle^{T_{n-1}}$. Let $\Delta_1 = \{\Omega_1^x \mid x \in T_{n-1}\}$ be the set of orbits determined by S_1 in its action on Ω. Recall that Δ_1 is a complete block system of T of blocks of length p and that $T_{n-1} \leqslant \mathrm{Sym}(\Delta_1)$.

Set $B = N_G(T)$ and denote by B_{n-1} the normalizer of T_{n-1} in $\mathrm{Sym}(\Delta_1)$. By Corollary 2.6.5,

$$S_1 = \langle x_1 \rangle^{T_{n-1}} = \langle x_1 \rangle^{B_{n-1}}$$

and so B_{n-1} normalizes S_1. Hence B_{n-1} normalizes $T = S_1 \rtimes T_{n-1}$ and $B_{n-1} \leqslant B$.

By Corollary 5.1.4 and Theorem 5.2.4, $B \leqslant N_G(S_1) = K_1 \rtimes \mathrm{Sym}(\Delta_1)$, with $K_1 = S_1 \rtimes L_1$ and $L_1 = \langle y_1 \rangle^{T_{n-1}}$, and B acts on Δ_1. Consider the action of B on Δ_1 given by the homomorphism

$$\sigma \colon x \in B \longmapsto xK_1/K_1 \in \mathrm{Sym}(\Delta_1).$$

Then $B/\ker\sigma \cong B\sigma$. Also, since $T \trianglelefteq B$, we have that $T\sigma \trianglelefteq B\sigma$. But

$$T\sigma \cong T/(T \cap \ker\sigma) = T/(T \cap K_1) = T/S_1 \cong T_{n-1}.$$

Therefore $B\sigma \leqslant B_{n-1} \leqslant B$ and so $|B| = |\ker\sigma||B\sigma| \leq |\ker\sigma||B_{n-1}| \leq |B|$. In particular, we have that $B = \ker\sigma \rtimes B_{n-1}$. Now $\ker\sigma = B \cap K_1 = B \cap (S_1 \rtimes L_1) = S_1 \rtimes (B \cap L_1)$, by Dedekind's Modular Law. Hence, if we set $N_1 = B \cap L_1$, by the induction hypothesis, we have that

$$|B| = |S_1||N_1||B_{n-1}| \leq |T||N_1|(p-1)^{n-1}.$$

So to complete the proof we need to show that $|N_1| \leq p-1$.

Now $N_1 = B \cap L_1 = B \cap \langle y_1 \rangle^{T_{n-1}}$ is normalized by T_{n-1}, since both B and $\langle y_1 \rangle^{T_{n-1}}$ are. Hence $[N_1, T_{n-1}] \leqslant N_1 \cap T = 1$ and so N_1 is centralized by T_{n-1}.

Assume that $|N_1| > p-1$ and consider the action of S_1N_1 on the block $\Omega_1 \in \Delta_1$ given by the homomorphism

$$\phi \colon S_1N_1 \longrightarrow \mathrm{Sym}(\Omega_1).$$

Since $S_1 \trianglelefteq S_1N_1$, we have that $\phi(S_1) \trianglelefteq \phi(S_1N_1)$. So $\phi(S_1N_1)$ is a subgroup of the normalizer of $\phi(S_1)$ in $\mathrm{Sym}(\Omega_1)$ and, by Theorem 5.2.4, $|\phi(S_1N_1)| \leq p(p-1)$. Since $|N_1| > p-1$ and $(|N_1|, |S_1|) = 1$, we have that

$$\ker\phi \cap N_1 \neq 1,$$

that is, there exists $x \in N_1$, $x \neq 1$, such that $\omega^x = \omega$, for all $\omega \in \Omega_1$.

Now let $\alpha \in \Omega \setminus \Omega_1$. Then $\alpha \in \Omega_1^z$, for some $z \in T_{n-1}$, since $\Delta_1 = \{\Omega_1^x \mid x \in T_{n-1}\}$ is a block system of T, and so $\alpha = \beta^z$, for some $\beta \in \Omega_1$. Then

$$\alpha^x = \beta^{zx} = \beta^{xz} = \beta^z = \alpha,$$

since T_{n-1} centralizes N_1 and x fixes every element in Ω_1. Therefore x fixes ω, for all $\omega \in \Omega$, and so $x = 1$, which is a contradiction. Thus we conclude that $|N_1| \leq p-1$, which implies that

$$|B| = |S_1||N_1||B_{n-1}| \leq |T|(p-1)^n.$$

$\square$

Corollary 5.2.6. *Let $G = \mathrm{Sym}(p^n)$ and $T \in \mathrm{Syl}_p(G)$. Write $T = \langle x_1, \ldots, x_n \rangle$ and set $B = N_G(T)$. Then $B = T \rtimes N$, with $N = \langle h_1, \ldots, h_n \rangle$, and $|B| = |T|(p-1)^n$. In particular, $B \leqslant H$ and a Hall p'-subgroup of B is abelian.*

Proof. By Theorems 5.2.2 and 5.2.3, we have that $T \rtimes N$ is a subgroup of B of order $|T|(p-1)^n$. Hence Theorem 5.2.5 implies that $B = T \rtimes N$ and $|B| = |T|(p-1)^n$. In particular, $B \leqslant H$ and, by Theorem 5.2.2, a Hall p'-subgroup of B is abelian. □

Corollary 5.2.7. *Let $i = 1, \ldots, n-1$. Then a Hall p'-subgroup of the base group K_i of $N_G(S_i)$ is abelian.*

Proof. By Lemma 5.1.5, the base group K_i of $N_G(S_i)$ is the direct product of p^{n-i} copies of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$ and so the result follows from Corollary 5.2.6. □

Thanks to Corollary 5.2.6 we can now write down explicitly all the generators of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^n)$. As an example, we shall illustrate the case $p = 3 = n$.

Example 5.7:
Let $G = \mathrm{Sym}(27)$, that is, $p = 3$ and $n = 3$. Let T be a Sylow 3-subgroup of G and write $T = \langle x_1, x_2, x_3 \rangle$, with

$x_1 = (1\ 2\ 3)$,

$x_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$,

$x_3 = (1\ 10\ 19)(2\ 11\ 20)(3\ 12\ 21)(4\ 13\ 22)(5\ 14\ 23)(6\ 15\ 24)(7\ 16\ 25)(8\ 17\ 26)(9\ 18\ 27)$.

Then the normalizer B of T in G is the subgroup generated by T together with the elements

$$h_1 = (2\ 3)(5\ 6)(8\ 9)(11\ 12)(14\ 15)(17\ 18)(20\ 21)(23\ 24)(26\ 27),$$

$$h_2 = (4\ 7)(5\ 8)(6\ 9)(13\ 16)(14\ 17)(15\ 18)(22\ 25)(23\ 26)(24\ 27),$$

$$h_3 = (10\ 19)(11\ 20)(12\ 21)(13\ 22)(14\ 23)(15\ 24)(16\ 25)(17\ 26)(18\ 27).$$

■

The construction of a Hall p'-subgroup of B in terms of the functions f_j and the description of S_i in terms of $F_{i+1}, \ldots, F_n$ leads to the following description of a Hall p'-subgroup of the base group of $N_G(S_i)$.

Lemma 5.2.8. *Let $i = 1, \ldots, n-1$ and K_i be the base group of $N_G(S_i)$. Then $K_i \cap L_i = L_i$ and, for all $k = 1, \ldots, i-1$,*

$$K_i \cap L_k = (F_n \circ \cdots \circ F_{i+1})(\langle (f_i \circ \cdots \circ f_{k+1})(y_k) \rangle).$$

In particular, $K_j \cap L_k \leqslant K_i \cap L_k$, for all $k = 1, \ldots, i$ and all $j > i$.

Proof. Let $i = 1, \ldots, n-1$ and let S_{i1} denote a Sylow p-subgroup of $\mathrm{Sym}(\Omega_i)$, namely $S_{i1} = \langle x_1, \ldots, x_i \rangle$. By definition S_i is the direct product of p^{n-i} copies of S_{i1}. Moreover S_i can be expressed as $S_i = (F_n \circ \cdots \circ F_{i+1})(S_{i1})$. Similarly, since, by Lemma 5.1.5, K_i is the direct product of p^{n-i} copies of the normalizer N_{i1} of S_{i1} in $\mathrm{Sym}(\Omega_i)$, we can write $K_i = (F_n \circ \cdots \circ F_{i+1})(N_{i1})$. But, as $|\Omega_i| = p^i$, from Corollary 5.2.6 it follows that $N_{i1} \cap L_k = \langle (f_i \circ \cdots \circ f_{k+1})(y_k) \rangle$ and so we have the result. In particular, for $j > i$, we have that

$$K_j \cap L_k = (F_n \circ \cdots \circ F_{j+1})(\langle (f_j \circ \cdots \circ f_{k+1})(y_k) \rangle),$$

where $(f_j \circ \cdots \circ f_{k+1})(y_k) = (f_j \circ \cdots \circ f_{i+1})((f_i \circ \cdots \circ f_{k+1})(y_k))$ is the product of the generators of the group $(F_j \circ \cdots \circ F_{i+1})(\langle (f_i \circ \cdots \circ f_{k+1})(y_k) \rangle) \leqslant K_i \cap L_k$. Therefore $K_j \cap L_k \leqslant K_i \cap L_k$, for all $k = 1, \ldots, i$. $\square$

We conclude the section with some results concerning the blocks of B and the orbits of a point stabilizer in B.

Theorem 5.2.9. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(S)$. Then B is transitive on Ω and every block of B has length a power of p. Furthermore, for $i = 1, \ldots, n-1$, B has a unique complete block system of blocks of length p^i, namely Δ_i, and, in particular, B has blocks of length p^r, for all $r = 1, \ldots, n$.*

Proof. By Theorem 4.3.1, T is transitive on Ω and then so is B. In particular, by Proposition 3.1.4, every block of B has length a power of p.
Moreover Corollary 5.1.4 implies that B acts on Δ_i, for all $i = 1, \ldots, n-1$, and so Δ_i is a complete block system of B. Also, by Theorem 5.1.3, Δ_i is the unique complete block system of B of blocks of length p^i. $\square$

Theorem 5.2.10. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(S)$. Then, for $\alpha \in \Omega$, $\mathrm{Stab}_B(\alpha)$ has $n+1$ orbits on Ω and they have length*

$$1,\ p-1,\ p^2-p,\ \ldots,\ p^n - p^{n-1}.$$

Proof. Let $n = 1$. By Theorem 5.2.4, $B \cong \mathrm{Hol}(T) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$ and so $\mathrm{Stab}_B(\alpha) \cong \mathbb{Z}_{p-1}$. Hence $\mathrm{Stab}_B(\alpha)$ is transitive on $\Omega \setminus \{\alpha\}$ and has on Ω two orbits, which are $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$ and have lengths 1 and $p-1$, respectively.

We now suppose that $n > 1$ and use induction on n. Let $T = \langle x_1, \dots, x_n \rangle$ and, according to Corollary 5.2.6, write $B = (S_1 \rtimes \langle h_1 \rangle) \rtimes B_{n-1}$, where $B_{n-1} = T_{n-1} \rtimes \langle h_2, \dots, h_n \rangle$ and

$$S_1 = \prod_{j=1}^{p^{n-1}} \langle x_1^{t_j} \rangle,$$

with $t_1 = 1$. Recall that the set $\Delta_1 = \{\Omega_1^{t_j} \mid j = 1, \dots, p^{n-1}\}$ is a complete block system of B of blocks of length p. Let $\alpha \in \Omega$ and suppose that $\alpha \in \Omega_1$. Without loss of generality, we can also assume that $\{\alpha\} = \mathrm{Fix}_{\Omega_1}(y_1) = \mathrm{Fix}_{\Omega_1}(h_1)$. Therefore

$$\mathrm{Stab}_B(\alpha) = (\mathrm{Stab}_{S_1}(\alpha) \rtimes \langle h_1 \rangle) \rtimes \mathrm{Stab}_{B_{n-1}}(\Omega_1) = \left(\prod_{j=2}^{p^{n-1}} \langle x_1^{t_j} \rangle \rtimes \langle h_1 \rangle \right) \rtimes \mathrm{Stab}_{B_{n-1}}(\Omega_1).$$

Regard B_{n-1} as a subgroup of $\mathrm{Sym}(\Delta_1)$. Then $\mathrm{Stab}_{B_{n-1}}(\Omega_1)$ is a point stabilizer in the normalizer of a Sylow p-subgroup. Hence, by the induction hypothesis, $\mathrm{Stab}_{B_{n-1}}(\Omega_1)$ has n orbits on Δ_1 of length

$$1,\ p-1,\ p^2 - p,\ \dots,\ p^{n-1} - p^{n-2}$$

and, without loss of generality, they are

$$\{\Omega_1\},\ \{\Omega_1^{t_2}, \dots, \Omega_1^{t_p}\},\ \{\Omega_1^{t_{p+1}}, \dots, \Omega_1^{t_{p^2}}\},\ \dots,\ \{\Omega_1^{t_{p^{n-2}+1}}, \dots, \Omega_1^{t_{p^{n-1}}}\}.$$

On the other hand, $\mathrm{Stab}_{S_1}(\alpha) \rtimes \langle h_1 \rangle$ has on Ω orbits

$$\{\alpha\},\ \Omega_1 \setminus \{\alpha\},\ \Omega_1^{t_2},\ \dots,\ \Omega_1^{t_{p^{n-1}}}.$$

Therefore the orbits of $\mathrm{Stab}_B(\alpha)$ on Ω are

$$\{\alpha\},\ \Omega_1 \setminus \{\alpha\},\ \Omega_1^{t_2} \cup \dots \cup \Omega_1^{t_p},\ \Omega_1^{t_{p+1}} \cup \dots \cup \Omega_1^{t_{p^2}},\ \dots,\ \Omega_1^{t_{p^{n-2}+1}} \cup \dots \cup \Omega_1^{t_{p^{n-1}}}$$

and so $\mathrm{Stab}_B(\alpha)$ has $n+1$ orbits on Ω and, since $|\Omega_1^{t_j}| = p$, for all $j = 1, \dots, p^{n-1}$, they also have the required length. $\square$

5.3 The normalizer in $\mathrm{Sym}(kp^n)$

Theorem 5.3.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = kp^n$ and $1 \leq k < p$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Then B is isomorphic to the wreath product of $\bar{B}$ by $\mathrm{Sym}(k)$, where $\bar{B}$ is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^n)$. In particular,*

$$|B| = |T|k!(p-1)^{nk}$$

and B is transitive on Ω.

Proof. According to Theorems 4.2.2 and 4.3.2, let $\Omega_1, \dots, \Omega_k$, with $|\Omega_i| = p^n$, for $i = 1, \dots, k$, be the orbits of T on Ω and write $T = T_1 \times \cdots \times T_k$, where $T_i \in \mathrm{Syl}_p(\mathrm{Sym}(\Omega_i))$. Let B_i denote the normalizer in $\mathrm{Sym}(\Omega_i)$ of T_i and set

$$K = (B_1 \times \cdots \times B_k) \rtimes \mathrm{Sym}(\Delta) \cong B_1 \wr \mathrm{Sym}(\Delta),$$

with $\Delta = \{\Omega_1, \dots, \Omega_k\}$. For $i = 1, \dots, k$, B_i normalizes T_i and centralizes T_j, with $j \neq i$. Thus B_i normalizes T and so $T \trianglelefteq B_1 \times \cdots \times B_k$. But $B_1 \times \cdots \times B_k \trianglelefteq K$ and so, by Proposition 1.1.8, we get that $K \leqslant B$.
Now, by Theorem 5.2.9, B_1 is transitive on Ω_1 and, of course, $\mathrm{Sym}(\Delta)$ is transitive on Δ. Thus, by Theorem 2.6.6, $B_1 \wr \mathrm{Sym}(\Delta)$ is transitive on the set $\Omega_1 \times \Delta$ of order kp^n, that is, K is transitive on Ω. In particular, B is transitive on Ω, since $K \leqslant B$. Also $T \trianglelefteq B$ and T is intransitive on Ω. Therefore, by Theorem 3.2.2, Δ is a complete block system of B, which implies that

$$B \leqslant \mathrm{Stab}_G(\Delta) = (\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_k)) \rtimes \mathrm{Sym}(\Delta).$$

Hence, by Dedekind's Modular Law and by Corollary 1.1.12, we get that

$$\begin{aligned} B &= B \cap \mathrm{Stab}_G(\Delta) = (B \cap (\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_k))) \rtimes \mathrm{Sym}(\Delta) \\ &= (B_1 \times \cdots \times B_k) \rtimes \mathrm{Sym}(\Delta) = K, \end{aligned}$$

completing the proof. $\square$

Proposition 5.3.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = kp^n$ and $1 < k < p$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Then B has blocks of length p^r, for all $r = 1, \dots, n$, and every nontrivial block of B has length a power of p.*

Proof. Let $\bar{B}$ be the normalizer in $\mathrm{Sym}(p^n)$ of a Sylow p-subgroup of $\mathrm{Sym}(p^n)$. Then, by Theorem 5.3.1, we know that $B \cong \bar{B} \wr \mathrm{Sym}(k)$, where, by Theorem 5.2.9, $\bar{B}$ has blocks of length p^r, for all $r = 1, \dots, n$, that is, $\bar{B} \leqslant \mathrm{Sym}(p^r) \wr \mathrm{Sym}(p^{n-r})$. Therefore

$$B \cong \bar{B} \wr \mathrm{Sym}(k) \leqslant \mathrm{Sym}(p^r) \wr \mathrm{Sym}(p^{n-r}) \wr \mathrm{Sym}(k) \leqslant \mathrm{Sym}(p^r) \wr \mathrm{Sym}(kp^{n-r})$$

and so B has blocks of length p^r, for all $r = 1, \dots, n$.

Moreover, since $\bar{B}$ is transitive on p^n points and $\mathrm{Sym}(k)$ is primitive on k points, from Theorem 3.5.3 it follows that every nontrivial block of B has length a power of p. $\square$

Theorem 5.3.3. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = kp^n$ and $1 < k < p$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Then, for $\alpha \in \Omega$, $\mathrm{Stab}_B(\alpha)$ has $n + 2$ orbits on Ω and they have length*

$$1, \;\; p-1, \;\; p^2 - p, \;\; \dots, \;\; p^n - p^{n-1}, \;\; (k-1)p^n.$$

Proof. According to Theorem 4.2.2, write $T = T_1 \times \cdots \times T_k$, where $T_i \in \mathrm{Syl}_p(\mathrm{Sym}(\Omega_i))$ and $\Omega_1, \dots, \Omega_k$ are the orbits of T on Ω. By Theorem 5.3.1, we have that

$$B = (B_1 \times \cdots \times B_k) \rtimes \mathrm{Sym}(\Delta),$$

where, for $i = 1, \dots, k$, B_i is the normalizer of T_i in $\mathrm{Sym}(\Omega_i)$ and $\Delta = \{\Omega_1, \dots, \Omega_k\}$. Let $\alpha \in \Omega$ and suppose that $\alpha \in \Omega_1$. Then

$$\mathrm{Stab}_B(\alpha) = \mathrm{Stab}_{B_1}(\alpha) \times ((B_2 \times \cdots \times B_k) \rtimes \mathrm{Sym}(\Delta \setminus \{\Omega_1\}))$$

and it will be enough to determine the orbits of the two direct factors of $\mathrm{Stab}_B(\alpha)$ on the sets Ω_1 and $\Omega_2 \cup \cdots \cup \Omega_k$, respectively, on which they act.

Now, by Theorem 5.2.10, $\mathrm{Stab}_{B_1}(\alpha)$ has $n+1$ orbits on Ω_1, say $\Omega_{1,1} = \{\alpha\}, \Omega_{1,2}, \dots, \Omega_{1,n+1}$, of length $1, p-1, p^2-p, \dots, p^n - p^{n-1}$, respectively. Also Theorem 5.3.1 implies that $(B_2 \times \cdots \times B_k) \rtimes \mathrm{Sym}(\Delta \setminus \{\Omega_1\})$ is isomorphic to the normalizer in $\mathrm{Sym}((k-1)p^n)$ of a Sylow p-subgroup and so it is transitive on the set $\Omega_2 \cup \cdots \cup \Omega_k$ of order $(k-1)p^n$ on which it acts. Hence $\mathrm{Stab}_B(\alpha)$ has $n+2$ orbits on Ω of the required length. $\square$

5.4 The general case

Theorem 5.4.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, and let $T \in \mathrm{Syl}_p(G)$. Let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, be the p-adic decomposition of n. Then the normalizer B of T in G is given by

$$B = B_0 \times \cdots \times B_t,$$

where, for $j = 0, \ldots, t$, B_j is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$, with $\Omega_j \subseteq \Omega$ and $|\Omega_j| = k_j p^j$. In particular,

$$|B| = |T| \prod_{j=0}^{t} k_j!(p-1)^{k_j j}$$

and the sets $\Omega_0, \Omega_1, \ldots, \Omega_t$ are the orbits of B on Ω.

Proof. According to Theorem 4.2.3, let $\Omega_0, \Omega_1, \ldots, \Omega_t$ be a partition of Ω into $t+1$ subsets such that, for $j = 0, \ldots, t$, $|\Omega_j| = k_j p^j$ and write $T = T_1 \times \cdots \times T_t$, with T_j Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$. Also let $B_0 = \mathrm{Sym}(\Omega_0)$ and let B_j denote the normalizer of T_j in $\mathrm{Sym}(\Omega_j)$, for all $j > 0$. Then the sets Ω_j are fixed blocks of T all of different length and so, since $T \trianglelefteq B$, they are also fixed blocks of B. Therefore

$$B \leqslant \mathrm{Sym}(\Omega_0) \times \cdots \times \mathrm{Sym}(\Omega_t)$$

and, by Corollary 1.1.12, $B = (B \cap \mathrm{Sym}(\Omega_0)) \times \cdots \times (B \cap \mathrm{Sym}(\Omega_t)) = B_0 \times \cdots \times B_t$. Furthermore, by Theorem 5.3.1, the sets $\Omega_0, \Omega_1, \ldots, \Omega_t$ are the orbits of B on Ω. $\square$

Notice that, by Theorem 5.4.1, $\mathrm{Sym}(\Omega_0)$ is contained in B and, in particular, in the centralizer of T in G, and so B is transitive on the set of points fixed by T, in accordance with Proposition 2.2.1.

Remark. By Sylow's Theorem the number n_p of Sylow p-subgroups of a group G is given by $|G : N_G(T)|$, where T is any Sylow p-subgroup of G, and $n_p \equiv 1 \pmod{p}$. Hence Theorem 5.4.1 tells us how many Sylow p-subgroup there are in a symmetric group of any degree, and, in particular, it implies that, for an integer n whose p-adic decomposition is $n = k_t p^t + \cdots + k_1 p + k_0$, with $0 \leq k_j < p$, for $j = 0, \ldots, t$, the integer

$$\frac{(k_t p^t + \cdots + k_1 p + k_0)!}{\prod_{j=0}^{t} k_j!(p-1)^{k_j j} p^{k_j (p^{j-1} + \cdots + p + 1)}}$$

is congruent $1 \pmod{p}$. We shall also remark that, though it satisfies the above congruency, the number of Sylow p-subgroups of the symmetric group given by Weisner in [40] is wrong.

This happens because the subgroup given by Weisner as the normalizer contains what is in fact the normalizer of a Sylow p-subgroup.

Proposition 5.4.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, and $k_t \neq 0$, be the p-adic decomposition of n. Then B has blocks of length p^r, for all $r = 1, \ldots, t$, and blocks of length $k_s p^s$, for all $s \in \{j \mid k_j \neq 0\}$.

Proof. According to Theorem 5.4.1, write $B = B_0 \times B_1 \times \cdots \times B_t$, with B_j normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$ and $\Omega_0, \Omega_1, \ldots, \Omega_t$ orbits of B on Ω. Then, for all $s \in \{j \mid k_j \neq 0\}$, Ω_s is also a block of B and has length $k_s p^s$. Moreover, by Proposition 5.3.2, B_t has blocks of length p^r, for all $r = 1, \ldots, t$. But, as $B_{|\Omega_t} \cong B_t$, a block of B_t is also a block of B and so we get the result. ☐

Proposition 5.4.3. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \ldots, t$, be the p-adic decomposition of n and

$$\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_t,$$

with $|\Omega_j| = k_j p^j$, for all $j = 0, \ldots, t$, be the corresponding partition of Ω into B-orbits. If Γ is a nontrivial block of B, then either $\Gamma \subseteq \Omega_i$, for a unique i, or Γ is the union of some Ω_j's. Therefore, either the length of Γ is a power of p or is given by

$$\sum_{j \in J} k_j p^j,$$

with $J \subseteq \{0, \ldots, t\}$ and $|J| \geq 1$.

Proof. Let $\Omega_0, \Omega_1, \ldots, \Omega_t$ be the orbits of B on Ω and write $B = B_0 \times B_1 \times \cdots \times B_t$, with B_j normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$, for all $j = 1, \ldots, t$.

Let Γ be a nontrivial block of B. If Γ intersects nontrivially exactly one Ω_j, say $\Gamma \cap \Omega_i \neq \emptyset$, for a unique i, then, as the Ω_j's form a partition of Ω, $\Gamma \subseteq \Omega_i$. In particular, Γ is a block of B_i and so, by Proposition 5.3.2, we get that the length of Γ is either $k_i p^i$ or, if $i \neq 0$, p^{r_i}, with $r_i = 1, \dots, i$.

Suppose now that Γ intersects nontrivially at least two different Ω_j's. Without loss of generality, assume that $\Gamma \cap \Omega_1 \neq \emptyset$ and $\Gamma \cap \Omega_2 \neq \emptyset$. Let $\alpha \in \Gamma \cap \Omega_1$ and $\beta \in \Gamma \cap \Omega_2$. Consider

$$B_\alpha = \mathrm{Stab}_B(\alpha) = B_0 \times \mathrm{Stab}_{B_1}(\alpha) \times B_2 \times \cdots \times B_t.$$

For all $h \in B_\alpha$, $\alpha = \alpha^h \in \Gamma \cap \Gamma^h$ and so, since Γ is a block of B, we have that Γ is preserved by B_α. Then, since $\beta \in \Gamma \cap \Omega_2$ and Ω_2 is an orbit of B_α, we get that $\Omega_2 \subseteq \Gamma$. Similarly, considering the stabilizer in B of β, which has Ω_1 as orbit, we get that $\Omega_1 \subseteq \Gamma$. In general, $\Gamma \supseteq \Omega_i$, for all i such that $\Gamma \cap \Omega_i \neq \emptyset$. Therefore Γ is the union of some Ω_j's and its length is given by

$$\sum_{j \in J} k_j p^j,$$

with $J \subseteq \{0, \dots, t\}$ and $|J| > 1$. $\square$

Theorem 5.4.4. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let*

$$n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0,$$

with $0 \leq k_j < p$, for all $j = 0, \dots, t$, be the p-adic decomposition of n and

$$\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_{t-1} \cup \Omega_t,$$

with $|\Omega_j| = k_j p^j$, for all $j = 0, \dots, t$, be the corresponding partition of Ω into B-orbits. If $\alpha \in \Omega_i$, then, in its action on Ω, $\mathrm{Stab}_B(\alpha)$ has t orbits, each of length $k_j p^j$, for $j \neq i$, namely the Ω_j's, and $i+2$ orbits which have length 1, $p-1$, $p^2-p, \dots,$ $p^i - p^{i-1}$, $(k_i - 1)p^i$.

Proof. Let $\Omega_0, \Omega_1, \dots, \Omega_t$ be the orbits of B on Ω and write $B = B_0 \times B_1 \times \cdots \times B_t$, with B_j normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$, for all $j = 1, \dots, t$. Suppose that $\alpha \in \Omega_i$, for some $i = 1, \dots, t$. Then

$$\mathrm{Stab}_B(\alpha) = \mathrm{Stab}_{B_i}(\alpha) \times \prod_{j \neq i} B_j$$

and the orbits of $\mathrm{Stab}_B(\alpha)$ are those of its direct factors on the respective sets and this gives, by Theorems 5.3.1 and 5.3.3, the result. $\square$

5.5 Overgroups of the normalizer of a Sylow p-subgroup

We shall conclude the chapter by establishing some results on primitive and imprimitive subgroups of $\mathrm{Sym}(\Omega)$ which contain the normalizer of a Sylow p-subgroup. Recall that intransitive overgroups of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$ are described by Corollary 1.1.12. We start with the primitive case.

Lemma 5.5.1. *Let $G = \mathrm{Sym}(\Omega)$ and let $T \in \mathrm{Syl}_p(G)$. Then the normalizer of T in G is never contained in $\mathrm{Alt}(\Omega)$.*

Proof. Let $H = \mathrm{Alt}(\Omega)$ and set $B = N_G(T)$. If $p = 2$, then $T \nleq \mathrm{Alt}(\Omega)$ and the result is trivial. So assume that $p \neq 2$. Then $T \in \mathrm{Syl}_p(H)$ and, by the Frattini argument, it follows that $G = BH$, which implies that $B \nleq H$. $\square$

Theorem 5.5.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, and $T \in \mathrm{Syl}_p(G)$. Suppose that M is a primitive subgroup of G containing the normalizer in G of T. If $n \geq p + 2$, then $M = G$.*

Proof. Set $B = N_G(T)$ and suppose that M is a primitive subgroup of G containing B.
Let $n > p+2$. Since M is transitive on Ω, by Proposition 2.1.9, we have that $\deg M = |\Omega| = n = p + k$, with $k \geq 3$. Also M contains a Sylow p-subgroup of G, so it contains a p-cycle. Then, by Theorem 3.2.10, M is either G or $\mathrm{Alt}(\Omega)$. But, by Lemma 5.5.1, $B \nleq \mathrm{Alt}(\Omega)$ and so we get that $M = G$.
Suppose now that $n = p + 2$. Then, by Theorem 5.4.1, $B = N_H(T) \times \mathrm{Sym}(2)$, where $H = \mathrm{Sym}(p)$, and so M contains a transposition. Hence, by Theorem 3.2.9, $M = G$. $\square$

Lemma 5.5.3. *Let $n \in \mathbb{N}$ and p be a prime. Let $n = k_t p^t + \cdots + k_1 p + k_0$ be the p-adic decomposition of n, that is, $0 \leq k_j < p$, for all $j = 0, \dots, t$. If d divides n, then either $d = n$ or $d < k_t p^t$.*

Proof. Write $n = k_t p^t + m$, with $m = k_{t-1} p^{t-1} + \cdots + k_1 p + k_0$. Since, for $j = 0, \dots, t-1$, $0 \leq k_j < p$, we have that

$$m \leq (p-1)(1 + p + \cdots + p^{t-1}) = p^t - 1 < p^t \leq k_t p^t.$$

Hence $n = k_t p^t + m < 2k_t p^t$ and so a proper divisor of n must be smaller than $k_t p^t$. $\square$

Theorem 5.5.4. *Let $G = \mathrm{Sym}(\Omega)$ and $T \in \mathrm{Syl}_p(G)$. Let M be a subgroup of G containing the normalizer of T in G and suppose that M is imprimitive. Then every block of M has length a power of p.*

Proof. Suppose that $|\Omega| = n$ and let $n = k_t p^t + \cdots + k_1 p + k_0$ be the p-adic decomposition of n. Set $B = N_G(T)$ and let $\Omega_0, \Omega_1, \ldots, \Omega_t$, with $|\Omega_j| = k_j p^j$, for all $j = 0, \ldots, t$, be the orbits of B on Ω. Also write $B = B_0 \times B_1 \times \cdots \times B_t$, where, for each $j = 0, \ldots, t$, B_j is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$.
Suppose that M is an imprimitive subgroup of G containing B. Let Δ be a nontrivial block of M and set $d = |\Delta|$, with $1 < d < n$. Then, since M is transitive on Ω, we have that d is a proper divisor of n and so, by Lemma 5.5.3, $d < k_t p^t$. Also the complete block system determined by Δ forms a partition of Ω. Thus, up to taking the appropriate conjugate of Δ in M, we can assume that $\Delta \cap \Omega_t \neq \emptyset$.
Suppose that $\Delta \subseteq \Omega_t$. If $\Delta = \Omega_t$, then $d = k_t p^t$, which is a contradiction. Thus we have that $\Delta \subset \Omega_t$ and so Δ is a nontrivial block of $B_{|\Omega_t} = B_t$. Hence, by Proposition 5.3.2, d is a power of p. Assume now that $\Delta \nsubseteq \Omega_t$. Since the orbits Ω_j form a partition of Ω,

$$\Delta = \bigcup_{j=0}^{t} (\Delta \cap \Omega_j),$$

where, for $j = 0, \ldots, t-1$, $\Delta \cap \Omega_j$ is fixed pointwise by B_t. Therefore, since Δ is a block of M, Δ must be fixed by B_t. But Ω_t is an orbit of B_t and so, as $\Delta \cap \Omega_t \neq \emptyset$, we have that $\Omega_t \subseteq \Delta$, which implies that $d \geq k_t p^t$, against the fact that $d < k_t p^t$. Therefore we must conclude that $\Delta \subset \Omega_t$ and $|\Delta|$ is a power of p. $\square$

Corollary 5.5.5. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Let $n = k_t p^t + \cdots + k_1 p + k_0$ be the p-adic decomposition of n. Suppose that M is an imprimitive subgroup of G containing B. Then there exists $1 \leq r \leq t$ such that $p^r | n$ and M is isomorphic to a subgroup of $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(n/p^r)$. In particular, $k_0 = k_1 = \cdots = k_{r-1} = 0$.*

Proof. Let Δ be a nontrivial block of M. Then, by Theorem 5.5.4, Δ has length p^r, for some $1 \leq r \leq t$, with p^r dividing n. Also, by Corollary 3.5.2, M embeds in the stabilizer in G of the complete block system $\{\Delta^x \mid x \in M\}$ determined by Δ, which is isomorphic to $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(n/p^r)$. $\square$

Chapter 6

Symmetric groups which are minimal parabolic subgroups

The aim of this chapter is to classify all the symmetric groups which are themselves minimal parabolic subgroups. As a result of this, we shall be able to reduce the investigation of minimal parabolic subgroups to some critical cases.
We start by examining some specific cases. When we come to consider the symmetric groups $\mathrm{Sym}(p)$ and $\mathrm{Sym}(p+1)$ some facts about linear groups, for which the reader can refer to [36], are used.

6.1 Sym(p)

In this section we shall prove that the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p)$ is a maximal subgroup of $\mathrm{Sym}(p)$. The following result on the subgroups of the projective special linear group $\mathrm{PSL}(2,q)$ will be used in the proof.

Theorem 6.1.1. ([36, Thm. 6.25, pg. 412]) *Let q be a power of a prime t and $d = (2, q-1)$. Then a subgroup of $\mathrm{PSL}(2,q)$ is isomorphic to one of the following groups:*

(i) *the dihedral groups of order $2(q \pm 1)/d$ and their subgroups;*

(ii) *a group H of order $q(q-1)/d$ and its subgroups. A Sylow t-subgroup Q of H is elementary abelian, $Q \trianglelefteq H$ and the factor group H/Q is a cyclic group of order $(q-1)/d$;*

(iii) $\mathrm{Alt}(4), \mathrm{Sym}(4)$ *or* $\mathrm{Alt}(5)$*;*

(iv) $\mathrm{PSL}(2,r)$ *or* $\mathrm{PGL}(2,r)$*, where r is a power of t such that $r^m = q$, $m > 1$.*

Let p be a prime and $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p$. Suppose that $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. If $p = 2, 3$, then $B = G$ and there is nothing to prove. So assume that $p \neq 2, 3$. By Theorem 4.2.1, we know that T is a cyclic group of order p. Also, by Theorem 5.2.4, we have that $|B| = p(p-1)$ and $B \cong \mathrm{Hol}(T) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$. Hence the stabilizer in B of a point $\alpha \in \Omega$ is a cyclic group of order $p-1$ and so is transitive on $\Omega \setminus \{\alpha\}$. Thus, by Theorem 3.3.2, B is 2-transitive on Ω.

Let $M < G$ such that $B < M$. Then M is 2-transitive and, in particular, primitive on Ω. So, by Corollary 3.4.6, M has a unique minimal normal subgroup N, which is either elementary abelian of order equal to the degree of M or simple. We shall reach a contradiction by arguing on the minimal normal subgroup N of M.

Suppose that M is soluble. Then, by Theorem 3.2.8, M has a unique Sylow p-subgroup, which is then T. So $T \trianglelefteq M$ and $M \leqslant B$, which is a contradiction.

So assume that M is not soluble. If N is abelian, then $|N| = \deg M = p$ and N is a Sylow p-subgroup of G. But $N \trianglelefteq M$, so M has a unique Sylow p-subgroup N and, by Theorem 3.2.8, M is soluble, against our previous assumption. Hence we must have that N is nonabelian simple. Then N is one of the groups in Table 3.1 for which the degree n of M is prime. But $T \in \mathrm{Syl}_p(M)$ and $N_M(T) = B$. Thus $|N_M(T)| = p(p-1)$ and M is an insoluble transitive group of degree p such that the normalizer of a Sylow p-subgroup has even order. Then, by [22], M is 3-transitive on Ω. Hence N must be one of the groups in Table 6.1.

N	n	k	Remarks
$\mathrm{Alt}(p), p \geq 5$	p	p	
M_{11} (Mathieu)	11	4	
M_{23} (Mathieu)	23	4	
$\mathrm{PSL}(2,q)$	$q+1$	3	$q \neq 2, 3$, $q+1 = p$

Table 6.1: Nonabelian simple minimal normal subgroups of a 3-transitive group in $\mathrm{Sym}(p)$

We shall show that each of the cases in Table 6.1 yields a contradiction.

Let us start by considering the alternating group $\mathrm{Alt}(p)$, with $p \geq 5$ prime. As $B \leqslant M$, we have that $\mathrm{Alt}(p) \nleqslant M$, for otherwise M would also contain the subgroup $\mathrm{Alt}(p)B$, which is equal, by the Frattini argument, to G. So $N \neq \mathrm{Alt}(p)$.

Consider now the cases $N = M_{11}$ and $N = M_{23}$. By Proposition 3.4.4, it follows that $N \leqslant M \cap \mathrm{Alt}(\Omega)$ and so M has a subgroup of index 2, which contains N. Therefore

$$|M : N| = |M : M \cap \mathrm{Alt}(\Omega)||M \cap \mathrm{Alt}(\Omega) : N| = 2\,|M \cap \mathrm{Alt}(\Omega) : N|$$

and 2 divides $|M/N|$. Now $M \lesssim \mathrm{Aut}(N)$ and $N \cong \mathrm{Inn}(N)$. Thus $M/N \lesssim \mathrm{Out}(N)$ and we get that 2 must divide $|\mathrm{Out}(N)|$. But, by the ATLAS ([7]), $\mathrm{Out}(M_{11}) = \mathrm{Out}(M_{23}) = 1$ and so N can be neither M_{11} nor M_{23}.

Hence we are left with the case $N = \mathrm{PSL}(2,q)$. By Table 6.1, we know that the degree p of M is equal to $q+1$ and that $q \neq 2$, 3. Also, q is a prime power, say $q = t^{\alpha}$, with t prime and $\alpha > 1$. If t were odd, then t^{α} would be odd and so $p = q+1 = t^{\alpha}+1$ would be even, which is a contradiction, as p is prime. So t is an even prime, that is, $t = 2$ and $q = 2^{\alpha}$. Now suppose that α is odd. Then $p = q+1 = 2^{\alpha}+1$ is divisible by $2+1$ [1], which is again a contradiction. Thus $\alpha = 2\beta$ is even and $q = 2^{2\beta}$. Again, by the same argument, if β were odd, then $p = q+1 = (2^2)^{\beta}+1$ would be divisible by 2^2+1. Recursively we get that α must be a power of 2, that is,

$$q = 2^{2^a}, \quad \text{with } a \geq 1$$

and p is a Fermat number (see [8, pg. 137] for a definition). Therefore, by the ATLAS [7, pg. xvi], the order of the outer automorphism group of N is given by

$$|\mathrm{Out}(N)| = 2^a.$$

Also note that, as $q = 2^{2^a}$, the characteristic of the underlying field is 2 and so $N = \mathrm{PSL}(2,q) = \mathrm{SL}(2,q)$. Moreover, by [14, Thm. 8.1, pg. 40], as $q+1 = p$, we have that

$$|N| = (q-1)q(q+1) = (p-2)(p-1)p,$$

so $T \in \mathrm{Syl}_p(N)$.

We now want to determine the normalizer of T in N. In order to do this we investigate the

[1] Using the formula $a^k + b^k = (a+b)(a^{k-1} - ba^{k-2} + \cdots - b^{k-2}a + b^{k-1})$, which holds only for k odd.

cases described in Theorem 6.1.1. First notice that, since $q = 2^{2^a}$, with $a \geq 1$, we have that $d = 1$ and $p \geq 5$. Also $|N_N(T)|$ must be divisible by $|T| = p = q + 1$.

Now, of the two dihedral groups given in case (i) only D_{2p} has order divisible by p and so from this case we can only have $N_N(T) = D_{2p}$.

Consider next the group H described in case (ii). Then $|H| = q(q-1)$ is not divisible by $q + 1$, since $q + 1$ is a prime greater than all the factors and so $N_N(T) \neq H$.

Next, since $p \geq 5$, the only group from case (iii) whose order is divisible by p is $\mathrm{Alt}(5)$, for which we must have $p = 5$. Then $q = 4$ and $N = \mathrm{SL}(2, 4) \cong \mathrm{Alt}(5)$, which is a contradiction.

Finally, suppose that $q = r^m$, for some r and some $m > 1$. Then r is a power of 2 and, by [14, Thm. 8.1, pg. 40], $|\mathrm{PSL}(2, r)| = |\mathrm{PGL}(2, r)| = (r + 1)r(r - 1)$. But, since $m > 1$, $p = q + 1 = r^m + 1$ is a prime greater than $r + 1$ and so $p \nmid (r + 1)r(r - 1)$. Thus $N_N(T)$ can be neither $\mathrm{PSL}(2, r)$ nor $\mathrm{PGL}(2, r)$.

Hence we must conclude that $N_N(T) = D_{2p}$, which implies, as $|\mathrm{Aut}(N)| = |\mathrm{Out}(N)||N|$, that

$$|N_{\mathrm{Aut}(N)}(T)| = |\mathrm{Out}(N)||N_N(T)| = 2^a 2p = p\, 2^{a+1}.$$

On the other hand, we know that $|N_M(T)| = p(p - 1)$, as $N_M(T) = B$. Thus we get that $p(p - 1)$ divides $p\, 2^{a+1}$, that is, $p - 1$ divides 2^{a+1}. But $p = q + 1 = 2^{2^a} + 1$ and so it follows that 2^{2^a} divides 2^{a+1}, which implies that

$$2^a \leq a + 1,$$

where $a \geq 1$. Now, if $a > 1$, this relation does not hold. If $a = 1$, then $2^a = 2 = a + 1$ and we get $N = \mathrm{PSL}(2, 4)$. But, acting on the set of one dimensional subspaces, $\mathrm{PSL}(2, 4)$ is a subgroup of $\mathrm{Sym}(5)$ isomorphic to $\mathrm{Alt}(5)$ and $N \neq \mathrm{Alt}(5)$. Therefore N cannot be $\mathrm{PSL}(2, q)$ and N is none of the groups in Table 6.1. This contradiction follows from the assumption that there exists a subgroup M of G such that $B < M < G$. Hence we have proved the following:

Theorem 6.1.2. *Let p be a prime, $p \neq 2, 3$, and $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p$. Suppose that $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then B is a maximal subgroup of G.*

Corollary 6.1.3. *Let p be a prime, $p \neq 2, 3$, and $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p$. Suppose that $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then G has a unique minimal parabolic subgroup P with* *respect to B and $P = G$. In particular, there is a unique minimal parabolic system $\mathcal{S}$ of G; $\mathcal{S}$ has rank 1 and consists of only G.*

6.2 Sym$(p+1)$

We begin the study of $\mathrm{Sym}(p+1)$ with the following consequence of Sylow's Theorem.

Lemma 6.2.1. *Let q be a prime, H be a group of order $(q-1)q(q+1)$ and $Q \in \mathrm{Syl}_q(H)$. If $|H : N_H(Q)| = q+1$, then there is a unique conjugacy class of subgroups of H of index $q+1$.*

Proof. Let $K \leqslant H$ such that $|H : K| = q+1$. Without loss of generality we may assume that $Q \leqslant K$. If $K \nleqslant N_H(Q)$, then there exists $k \in K$ such that $Q^k \neq Q$. Thus K has at least two distinct Sylow q-subgroups Q and Q^k. By Sylow's Theorems the number n_q of Sylow q-subgroups of K is equal to $|K : N_K(Q)|$ and $n_q \equiv 1 \pmod q$. Hence it follows that $n_q \geq q+1$, which contradicts the fact that $|K| = (q-1)q$. Thus $K = N_H(Q)$, which completes the proof. □

Theorem 6.2.2. *Let p be a prime and $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p+1$. Suppose that $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then*

(i) *if $p = 2, 3$, there is a unique minimal parabolic subgroup of G with respect to B and it is G itself; in particular, the unique minimal parabolic system of G is given by $\{G\}$;*

(ii) *if $p \neq 2, 3$, there are only two minimal parabolic subgroups P_1 and P_2 of G with respect to B; P_1 is isomorphic to $\mathrm{Sym}(p)$ embedded as a point stabilizer and P_2 is isomorphic to $\mathrm{PGL}(2,p)$ acting on one dimensional subspaces. In particular, there is a unique minimal parabolic system $\mathcal{S}$ of G and it is $\{P_1, P_2\}$.*

Proof. For $p = 2$, $T = B \cong \mathrm{Sym}(2)$ and, for $p = 3$, $T \cong \mathrm{Alt}(3)$ and $B \cong \mathrm{Sym}(3)$. So, in both cases, B is a maximal subgroup of G and, thus, G is the unique minimal parabolic subgroup with respect to B.

Suppose that $p \neq 2, 3$ and let $H \cong \mathrm{Sym}(p)$ be the stabilizer in G of a point in Ω, say $H = G_\alpha$, for some $\alpha \in \Omega$. By order we may assume that $T \in \mathrm{Syl}_p(H)$. Then, by Theorem 5.4.1, $N_H(T) = B$ and, by Theorem 6.1.2, $N_H(T)$ is a maximal subgroup of H. Therefore H is a minimal parabolic subgroup of G with respect to B.

Consider now the group $\mathrm{GL}(2,p)$ acting on the set of 1-dimensional subspaces, which is a set of order $(p^2-1)/(p-1) = p+1$. This gives us a homomorphism

$$\rho\colon \mathrm{GL}(2,p) \longrightarrow G.$$

The kernel of this action is the subgroup of all scalar matrices, that is, the centre of $\mathrm{GL}(2,p)$. Thus $\mathrm{GL}(2,p)/\ker(\rho) \cong \mathrm{PGL}(2,p)$ can be regarded as a subgroup of G. Hence let $K \leqslant G$ such that $K \cong \mathrm{PGL}(2,p)$. By [14, Thm. 8.1, pg. 40], we know that

$$|K| = (p-1)p(p+1),$$

which implies, as $p \neq 2, 3$, that $K \neq G$. Also, as K is transitive on Ω, $K \nleqslant H$ and, by Proposition 2.1.7, we have that $G = HK$.

By order, we may assume that $T \in \mathrm{Syl}_p(K)$. Then $N_K(T) = B \leqslant K$, since $|N_K(T)| = p(p-1)$. Therefore K is a proper subgroup of G containing the normalizer in G of T. Also, as B is a maximal subgroup of H, we get that

$$H \cap K = B$$

and B is a point stabilizer in K, namely $B = K_\alpha$. But we know that B is 2-transitive on $\Omega \setminus \{\alpha\}$, so, by Theorem 3.3.2, K is 3-transitive on Ω. In particular, K is 2-transitive and thus primitive. Therefore, by Theorem 3.2.6, B is a maximal subgroup of K, which implies that K is a minimal parabolic subgroup of G with respect to B.

It remains to prove that H and K are the only minimal parabolic subgroups of G with respect to B. So let L be a minimal parabolic subgroup of G with respect to B, that is, B is contained in a unique maximal subgroup of L. First notice that from $G = HK$ it follows that G is not a minimal parabolic subgroup with respect to B and so, in particular, $L \neq G$.

Suppose that L does not stabilize any point of Ω. In particular, L moves α and so, as B is transitive on $\Omega \setminus \{\alpha\}$, we get that L is transitive on Ω. Thus, by Proposition 2.1.7, $G = HL$. Consider now the intersection $L \cap H$. By the maximality of B in H, $L \cap H$ is either H or B. But, if $L \cap H$ is H, then $H < L$, which is a contradiction, since H is a maximal subgroup of G. Thus $L \cap H = B$ and B is a point stabilizer in L, namely $B = L_\alpha$. Then, since B is 2-transitive on $\Omega \setminus \{\alpha\}$, we get that L is 3-transitive on Ω. In particular, L is 2-transitive and then primitive on Ω and so, by Theorem 3.2.6, B is a maximal subgroup of L. Moreover, as

L is transitive on Ω, applying the Orbit-Stabilizer Theorem, we get that

$$|L : B| = p + 1$$

and so $|L| = (p-1)p(p+1)$. In particular, this shows that every subgroup of G properly containing B and not stabilizing any point has order $(p-1)p(p+1)$ and so is a maximal subgroup of G.

Now, since L is 3-transitive and has order $(p-1)p(p+1)$, L is sharply 3-transitive, by Proposition 3.3.5. Thus, by Theorem 3.3.6, since $\deg L = p+1$, we get that $L \cong \mathrm{PGL}(2,p)$. In conclusion we have that either $L = G_\beta$, for some $\beta \in \Omega$, or $L \cong K$.

If $L = G_\beta$, then L is conjugate with H. Hence, as $B \leqslant L \cap H$, by Proposition 1.1.7, $L = H$. Thus it remains to show that, if $L \cong K$, then $L = K$. As before, it will be enough to prove that L and K are conjugate in G.

Let X and Y be subgroups of $\mathrm{PGL}(2,p)$ of index $p+1$. By Lemma 6.2.1, X and Y are conjugate in $\mathrm{PGL}(2,p)$. Consider now the representations ρ_X and ρ_Y of $\mathrm{PGL}(2,p)$ on the set of right cosets of X and Y in $\mathrm{PGL}(2,p)$. Since $|\mathrm{PGL}(2,p) : X| = |\mathrm{PGL}(2,p) : Y| = p+1$, we can regard ρ_X and ρ_Y as representations of $\mathrm{PGL}(2,p)$ on the set Ω, that is,

$$\rho_X,\ \rho_Y \colon \mathrm{PGL}(2,p) \longrightarrow \mathrm{Sym}(\Omega) = G.$$

Because X and Y are conjugate, the representations ρ_X and ρ_Y are equivalent, that is, the subgroups $(\mathrm{PGL}(2,p))\rho_X$ and $(\mathrm{PGL}(2,p))\rho_Y$ are conjugate in G ([10, Section 1.6]).

Now $\ker \rho_X \trianglelefteq \mathrm{PGL}(2,p)$ and, by Proposition 2.4.2, $\ker \rho_X \leqslant X$. But the only nontrivial proper normal subgroup of $\mathrm{PGL}(2,p)$ is $\mathrm{PSL}(2,p)$, which has order $(p-1)p(p+1)/2$ and so cannot be contained in X. Therefore we have that $\ker \rho_X = 1$. Similarly, $\ker \rho_Y = 1$. Hence the subgroups $(\mathrm{PGL}(2,p))\rho_X$ and $(\mathrm{PGL}(2,p))\rho_Y$ are both isomorphic to $\mathrm{PGL}(2,p)$. Since any transitive permutation representation of a group W is a equivalent to a ρ_Z, for some $Z \leqslant W$, this shows that any two transitive subgroups of G which are isomorphic to $\mathrm{PGL}(2,p)$ are conjugate.

Hence, if $L \cong \mathrm{PGL}(2,p) \cong K$, then L and K are conjugate in G. Thus, by Proposition 1.1.7, they are equal and this completes the proof. $\square$

6.3 Sym(kp)

Theorem 6.3.1. *Let $G = \mathrm{Sym}(kp)$, with $1 < k < p$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then there are only two minimal parabolic subgroups of G with respect to B and they are G itself and the subgroup $\mathrm{Sym}(p) \wr \mathrm{Sym}(k)$. In particular, there is a unique minimal parabolic system $\mathcal{S}$ of G and $\mathcal{S} = \{G\}$.*

Proof. Let $P = \mathrm{Sym}(p) \wr \mathrm{Sym}(k)$. By Theorem 5.3.1, $B \leqslant P$. We shall first prove that P is the unique maximal subgroup of G containing B. By Theorem 3.6.2, P is a maximal subgroup of G. Now let M be a subgroup of G containing B. By Theorem 5.5.2, we may assume that M is imprimitive. By Proposition 5.3.2, B has blocks of length 1, p or kp. So it follows that every nontrivial block of M must have length p and, by Corollary 3.5.2, M is isomorphic to a subgroup of P. Therefore P is the unique maximal subgroup of G containing B and G is a minimal parabolic subgroup with respect to B. Moreover, by Lemma 2.6.8, B is a maximal subgroup of P. Thus P and G are the only minimal parabolic subgroups of G with respect to B. $\square$

6.4 Sym(p^2)

Theorem 6.4.1. *Let $G = \mathrm{Sym}(p^2)$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then G is a minimal parabolic subgroup with respect to B. In particular, there is a unique minimal parabolic system of G and it is given by $\{G\}$.*

Proof. Let $U = \mathrm{Sym}(p) \wr \mathrm{Sym}(p)$. By Corollary 5.2.6, we have that $B \leqslant U$. We shall prove that U is the unique maximal subgroup of G containing B. By Theorem 3.6.2, U is a maximal subgroup of G. Now let M be a subgroup of G containing B. By Theorem 5.5.2, we may assume that M is imprimitive. By the transitivity of B, it follows that every subgroup containing B can only have blocks of length 1, p and p^2. So every nontrivial block of M has length p and, by Corollary 3.5.2, M is isomorphic to a subgroup of U. Therefore U is the unique maximal subgroup of G containing B. $\square$

6.5 $\mathbf{Sym}(k_1p^a + k_0)$

Lemma 6.5.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Suppose that $n = k_1p^a + k_0$, with $a \geq 1$ and $1 \leq k_0, k_1 < p$, is the p-adic decomposition of n. Then every transitive subgroup of G containing B is 2-transitive on Ω; in particular, such subgroups are primitive on Ω.*

Proof. Suppose that M is a transitive subgroup of G containing B. By Theorem 5.4.1, B has two orbits Ω_0 and Ω_1 on Ω and they have length k_0 and k_1p^a, respectively. Let $\gamma \in \Omega_0$ and $\delta \in \Omega_1$ and consider the stabilizers B_γ and B_δ. By Theorem 5.4.4, the stabilizer B_γ has three orbits on Ω and they have lengths k_1p^a, 1 and $k_0 - 1$ and the stabilizer B_δ has $a+3$ orbits on Ω and they have lengths $(k_1 - 1)p^a$, $p^a - p^{a-1}, \ldots, p - 1$, 1 and k_0.
Now let $\alpha \in \Omega$ and consider the stabilizer M_α. The orbits of M_α on Ω are the union of the orbits of B_α on Ω. Also, as M is transitive on Ω, all stabilizers in M are conjugate and so, by Proposition 2.1.4, for all $\alpha \in \Omega$, the M_α's produce on Ω the same kind of decomposition into orbits. Therefore, looking at the orbits of B_α on Ω, of which there are either three or $a + 3$, with $a \geq 1$, we have that M_α has at most three orbits on Ω.
If M_α has three orbits on Ω, then they must have lengths k_1p^a, 1 and $k_0 - 1$, with $k_0 \neq 1$. Compare the orbits of B_γ with the orbits of B_δ. Since $k_0 \neq 1$ and $k_0 - 1$ can be neither $(k_1 - 1)p^a$ nor $p^i - p^{i-1}$, for $i > 1$, as $k_0 - 1$ is not divisible by p, it follows that $k_0 - 1 = p - 1$, which yields the contradiction $k_0 = p$. Hence M_α has two orbits on Ω and they are $\{\alpha\}$ and $\Omega \setminus \{\alpha\}$. Thus M_α is transitive on $\Omega \setminus \{\alpha\}$ and M is 2-transitive on Ω. □

Theorem 6.5.2. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Suppose that $n = k_1p^a + k_0$, with $a \geq 1$ and $1 \leq k_0, k_1 < p$, is the p-adic decomposition of n. If $n \geq p + 2$, then G is a minimal parabolic subgroup with respect to B and there is a unique minimal parabolic system of G and it is given by $\{G\}$.*

Proof. Let $U = \mathrm{Sym}(k_1p^a) \times \mathrm{Sym}(k_0)$. By Theorem 5.4.1, U contains B and from Theorem 3.6.1 we know that U is a maximal subgroup of G. It remains to show that U is the unique maximal subgroup of G containing B. Let M be a subgroup of G containing B and assume that $M \not\leq U$. Then M fuses the two orbits of U on Ω and so is transitive on Ω. Thus, by Lemma 6.5.1, M is primitive on Ω. Then Theorem 5.5.2 implies that $M = G$. Hence every proper subgroup of G containing B is contained in U and this completes the proof. $\square$

Theorem 6.5.3. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p + k_0$, where p is a prime and k_0 is an integer such that $1 < k_0 < p$. Suppose that $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Then there are exactly two minimal parabolic subgroups of G with respect to B and they are $\mathrm{Sym}(p) \times \mathrm{Sym}(k_0)$ and G itself.*

Proof. By Theorem 6.5.2, we know that G is a minimal parabolic subgroup and that the unique maximal subgroup of G containing B is given by $\mathrm{Sym}(p) \times \mathrm{Sym}(k_0)$. Thus all proper subgroups of G containing B are contained in $\mathrm{Sym}(p) \times \mathrm{Sym}(k_0)$. But, as $k_0 < p$, $T \in \mathrm{Syl}_p(\mathrm{Sym}(p))$ and $B = N_{\mathrm{Sym}(p)}(T) \times \mathrm{Sym}(k_0)$, where, by Theorem 6.1.2, $N_{\mathrm{Sym}(p)}(T)$ is a maximal subgroup of $\mathrm{Sym}(p)$. Therefore B is a maximal subgroup of $\mathrm{Sym}(p) \times \mathrm{Sym}(k_0)$ and we have the result. $\square$

6.6 All symmetric groups which are minimal parabolic subgroups

We now want to show that those examined in the previous sections are the only symmetric groups which are minimal parabolic subgroups with respect to the normalizer of a Sylow p-subgroup. This will have important consequences for the general study of minimal parabolic subgroups in the symmetric groups, as we shall see in the next section.

Theorem 6.6.1. *Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. Suppose that $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Then G is a minimal parabolic subgroup with respect to B if and only if one of the following occurs:*

(i) *$n = p$ and $p \neq 2, 3$;*

(ii) *$n = p + 1$ and $p = 2, 3$;*

(iii) *$n = kp$, with $1 < k \leq p$;*

(iv) *$n = k_1 p^{\alpha_1} + k_0$, with $1 \leq k_0, k_1 < p$, $\alpha_1 \geq 1$ and $(k_0, k_1, \alpha_1) \neq (1, 1, 1)$.*

Proof. Thanks to the study carried out in the previous sections, we only need to show that, if G is a minimal parabolic subgroup with respect to B, then one of (i)–(iv) occurs. We shall prove the negation of this statement, that is, we shall prove that if one of

(a) $n = p + 1$, with $p \neq 2, 3$;

(b) $n = kp^a$, with $(k, a) \neq (1, 2),\ a \geq 2$;

(c) $n = k_2p^{a_2} + k_1p^{a_1}$, with $0 < a_1 < a_2$ and $0 < k_1, k_2 < p$;

(d) B has at least three orbits on Ω,

holds, then G is not a minimal parabolic subgroup with respect to B.
So assume that $n = p+1$, with $p \neq 2, 3$. Then Theorem 6.2.2 implies that $G \notin \mathcal{M}(G, B)$.
Suppose now that $n = kp^a$, with $(k, a) \neq (1, 2),\ a \geq 2$. For $r = 1, \ldots, a$, the subgroup $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(kp^{a-r})$ is a maximal subgroup of G containing, by Proposition 5.3.2, B. Therefore, for $a \geq 2$ and $(k, a) \neq (1, 2)$, we have at least two distinct such subgroups and so G is not a minimal parabolic subgroup with respect to B.
Next let $n = k_2p^{a_2} + k_1p^{a_1}$, with $0 < a_1 < a_2$ and $0 < k_1, k_2 < p$. By Theorem 3.6.1, $\mathrm{Sym}(k_2p^{a_2}) \times \mathrm{Sym}(k_1p^{a_1})$ is a maximal subgroup of G and, clearly, contains B. But, by Theorem 3.6.2, $\mathrm{Sym}(p^r) \wr \mathrm{Sym}(k_2p^{a_2-r} + k_1p^{a_1-r})$ is also a maximal subgroup of G and, by Proposition 5.4.2, contains B, for all $r = 1, \ldots, a_1$. Therefore, as $a_1 \geq 1$, we have at least two distinct maximal subgroups of G containing B.
Finally, suppose that B has at least three orbits on Ω. Then G is not a minimal parabolic subgroup, as there are at least three different maximal subgroups of G containing B. They are of the form $\mathrm{Sym}(n-r) \times \mathrm{Sym}(r)$, where r is the length of a B-orbit. They are maximal subgroups of G by Theorem 3.6.1 and contain B by Theorem 5.4.1. □

The cases arising from the statement of Theorem 6.6.1 are summarized in Table 6.2, where, for each symmetric group which is a minimal parabolic subgroup, the unique maximal subgroup containing the normalizer is also given.
Recall that, by Theorem 1.4.5, all the groups G in Table 6.2 have a unique minimal parabolic system, which is $\{G\}$.

Symmetric groups which are minimal parabolics	Conditions on the degree	Unique maximal subgroup containing the normalizer
$\mathrm{Sym}(p)$	$p \neq 2, 3$	$N_G(T)$
$\mathrm{Sym}(p+1)$	$p = 2, 3$	$N_G(T) \cong \mathrm{Sym}(p)$
$\mathrm{Sym}(kp)$	$1 < k < p$	$\mathrm{Sym}(p) \wr \mathrm{Sym}(k)$
$\mathrm{Sym}(p^2)$		$\mathrm{Sym}(p) \wr \mathrm{Sym}(p)$
$\mathrm{Sym}(k_1 p^a + k_0)$	$a \geq 1, 1 \leq k_0, k_1 < p,$ $(k_0, k_1, a) \neq (1, 1, 1)$	$\mathrm{Sym}(sp^a) \times \mathrm{Sym}(k)$

Table 6.2: Symmetric groups which are minimal parabolic subgroups

6.7 An overview of the problem

Thanks to the results achieved so far, and in particular Theorem 6.6.1, we can draw some conclusions about the general problem of determining all minimal parabolic subgroups of the symmetric group. More specifically, we shall produce a list of critical cases to study by first reducing to the imprimitive case and then deriving some restrictions on the degree of the symmetric group.

Suppose that $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = n$. Let $T \in \mathrm{Syl}_p(G)$, for some prime p dividing $|G|$, and set $B = N_G(T)$. Let $n = k_t p^t + \cdots + k_1 p + k_0$, be the p-adic decomposition of n and, according to Theorem 5.4.1, let $\Omega_0, \Omega_1, \ldots, \Omega_t$, with $|\Omega_j| = k_j p^j$, for all $j = 0, \ldots, t$, be the orbits of B on Ω. Recall that $B = B_0 \times B_1 \times \cdots \times B_t$, where, for each $j = 0, \ldots, t$, B_j is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega_j)$.

Our first result reduces the study of intransitive minimal parabolic subgroups to the study of those that are transitive, that is, either primitive or imprimitive.

Theorem 6.7.1. *Let P be a subgroup of G containing B. Suppose that P is intransitive on Ω and let $\Delta_1, \ldots, \Delta_r$, for $2 \leq r \leq t$, be the P-orbits. Then $P \in \mathcal{M}(G, B)$ if and only if*

$$P = (P \cap \mathrm{Sym}(\Delta_i)) \times \prod_{j \neq i} (B \cap \mathrm{Sym}(\Delta_j)),$$

for some $i = 1, \ldots, r$, with $B \cap \mathrm{Sym}(\Delta_j)$ normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Delta_j)$*, for all $j = 1, \ldots, r$, and $P \cap \mathrm{Sym}(\Delta_i)$ minimal parabolic subgroup of* $\mathrm{Sym}(\Delta_i)$ *with respect to*

$B \cap \mathrm{Sym}(\Delta_i)$ *and transitive.*

Proof. By assumption, P is a subgroup of $\mathrm{Sym}(\Delta_1) \times \cdots \times \mathrm{Sym}(\Delta_r)$ containing the normalizer of a Sylow p-subgroup, namely B. Hence the result follows from Corollary 1.4.11. □

The next theorem describes all minimal parabolic subgroups that are primitive, telling us also when this case arises.

Theorem 6.7.2. *Let P be a subgroup of G containing B and suppose that P is primitive. Then $P \in \mathcal{M}(G, B)$ if and only if*

(i) $P \cong \mathrm{PGL}(2, p)$ *and* $n = p + 1$, *with* $p \neq 2, 3$; *or*

(ii) $P = G$ *and one of the following holds:*

  (a) $n = p$ *and* $p \neq 2, 3$.

  (b) $n = p + 1$ *and* $p = 2, 3$;

  (c) $n = kp$, *with* $1 < k \leq p$;

  (d) $n = k_1 p^{\alpha_1} + k_0$, *with* $1 \leq k_0, k_1 < p$, $\alpha_1 \geq 1$ *and* $(k_0, k_1, \alpha_1) \neq (1, 1, 1)$.

In particular, the p-adic decomposition of n contains at most two nonzero terms.

Proof. Let P be primitive and suppose that $P \in \mathcal{M}(G, B)$. If $n \geq p + 2$, then Theorem 5.5.2 implies that $P = G$ and, by Theorem 6.6.1, one of (ii)(c) or (ii)(d) holds. Assume now that $n = p + 1$. By Theorem 6.2.2, if $p = 2, 3$, then $P = G$ and (ii)(b) holds; otherwise, since P is primitive, we must have that $P \cong \mathrm{PGL}(2, p)$ and so (i). Finally, let $n = p$. Then, since $P \neq B$, we have that $p \neq 2, 3$ and, by Corollary 6.1.3, $P = G$, completing the first part of the proof.
Conversely, suppose that one of the cases listed above holds. Then the result follows from Theorems 6.2.2 and 6.6.1. □

As a result of Theorems 6.7.1 and 6.7.2, from now on we shall restrict our investigation to the imprimitive case.
So let P be a minimal parabolic subgroup of G with respect to B and suppose that P is imprimitive. Let Δ be a nontrivial block of P and recall that, by Theorem 5.5.4, the length of Δ is a power of p dividing n. Denote by $\mathcal{B}_\Delta$ the complete block system determined by Δ,

that is, $\mathcal{B}_\Delta = \{\Delta^x \mid x \in P\}$. Then, by Corollary 3.5.2, P is contained in the stabilizer S of $\mathcal{B}_\Delta$ in G, which is isomorphic to $\mathrm{Sym}(\Delta) \wr \mathrm{Sym}(\mathcal{B}_\Delta)$.

Let K_Δ denote the kernel of the action of P on $\mathcal{B}_\Delta$, that is, K_Δ is the base group of P with respect to $\mathcal{B}_\Delta$. By Lemma 1.4.7, either $P/K_\Delta = BK_\Delta/K_\Delta$ or P/K_Δ is a minimal parabolic subgroup with respect to BK_Δ/K_Δ. Notice that, in the former case, we can write $P = K_\Delta \rtimes \bar{B}$, with $\bar{B} \leqslant \mathrm{Sym}(\mathcal{B}_\Delta)$ the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\mathcal{B}_\Delta)$.

Our next result is concerned with the case when P/K_Δ is a minimal parabolic subgroup with respect to BK_Δ/K_Δ. Recall that, by Proposition 1.4.9, this happens if and only if $K_\Delta = U \cap K_\Delta$, where U denotes the unique maximal subgroup of P containing B.

Lemma 6.7.3. *Let $P \in \mathcal{M}(G, B)$ and suppose that P is imprimitive. Let Δ be a nontrivial block of P and let $|\Delta| = p^r$, for some $1 \le r \le t$. If P/K_Δ is a minimal parabolic subgroup with respect to BK_Δ/K_Δ, then P is isomorphic to a subgroup of $B_r \wr \mathrm{Sym}(n/p^r)$, where $B_r \leqslant \mathrm{Sym}(p^r)$ is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^r)$. In particular, P has blocks of length p^s, for all $s = 1, \ldots, r$.*

Proof. Let $P \in \mathcal{M}(G, B)$ and let Δ be a nontrivial block of P of length, say, p^r, with $1 \le r \le t$. Then $P \leqslant S$, where $S \cong \mathrm{Sym}(p^r) \wr \mathrm{Sym}(n/p^r)$ is the stabilizer in G of $\mathcal{B}_\Delta$. By assumption, P/K_Δ is a minimal parabolic subgroup with respect to BK_Δ/K_Δ and so, in particular, $P \neq BK_\Delta$. Then Lemma 1.4.6 implies that $T \cap K_\Delta \trianglelefteq P$ and so $P \leqslant N_S(T \cap K_\Delta)$. But $T \cap K_\Delta = T \cap L$, where L is the base group of S and is isomorphic to the direct product of n/p^r copies of $\mathrm{Sym}(p^r)$. Therefore

$$P \leqslant N_S(T \cap K_\Delta) = N_S(T \cap L) \cong B_r \wr \mathrm{Sym}(n/p^r),$$

where $B_r \leqslant \mathrm{Sym}(p^r)$ is the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^r)$. In particular, by Theorem 5.2.9, we have that $B_r \leqslant \mathrm{Sym}(p^s) \wr \mathrm{Sym}(p^{r-s})$, for all $s = 1, \ldots, r$, and so it follows that P has blocks of length p^s, for all $s = 1, \ldots, r$. $\square$

We can now prove the main result of this section. The notation $P \lesssim R$, with R any group, will denote that P is isomorphic to a subgroup of R.

Theorem 6.7.4. *Let $P \in \mathcal{M}(G, B)$ and suppose that P is imprimitive. Let p^m, with $1 \le m \le t$, be the length of a maximal nontrivial block Δ of P. Denote by K_Δ the kernel of* *the action of P on Δ, by B_m the normalizer of a Sylow p-subgroup of* $\mathrm{Sym}(p^m)$ *and by* $N_p \cong \mathrm{Hol}(\mathbb{Z}_p)$ *the normalizer of a Sylow p-subgroup of* $\mathrm{Sym}(p)$. *Then one of the following cases occurs:*

(i) $n = p^{m+1}$ *and* $P \cong K_\Delta \rtimes N_p$;

(ii) $n = p^{m+1}$, *with* $p \neq 2, 3$, $P/K_\Delta \cong \mathrm{Sym}(p)$ *and* $P \lesssim B_m \wr \mathrm{Sym}(p)$;

(iii) $n = p^{m+2}$, $P/K_\Delta \cong \mathrm{Sym}(p^2)$ *and* $P \lesssim B_m \wr \mathrm{Sym}(p^2)$;

(iv) $n = kp^m$, *with* $1 < k < p$, *and* $P \cong K_\Delta \rtimes \mathrm{Sym}(k)$;

(v) $n = kp^{m+1}$, *with* $1 < k < p$, $P/K_\Delta \cong \mathrm{Sym}(kp)$ *and* $P \lesssim B_m \wr \mathrm{Sym}(kp)$;

(vi) $n = p^m(p+1)$, *with* $p = 2, 3$, $P/K_\Delta \cong \mathrm{Sym}(p+1)$ *and* $P \lesssim B_m \wr \mathrm{Sym}(p+1)$;

(vii) $n = p^m(p+1)$, *with* $p \neq 2, 3$, $P/K_\Delta \cong \mathrm{PGL}(2,p)$ *and* $P \lesssim B_m \wr \mathrm{PGL}(2,p)$;

(viii) $n = p^m(k_1 p^{\alpha_1} + k_0)$, *with* $1 \leq k_0, k_1 < p$, $1 \leq \alpha_1$ *and* $(k_0, k_1, \alpha_1) \neq (1,1,1)$, $P/K_\Delta \cong \mathrm{Sym}(k_1 p^{\alpha_1} + k_0)$ *and* $P \lesssim B_m \wr \mathrm{Sym}(k_1 p^{\alpha_1} + k_0)$.

In particular, the p-adic decomposition of n contains only two nonzero terms.

Proof. Let $P \in \mathcal{M}(G,B)$ and let Δ be a nontrivial block of P of maximal length. Set $|\Delta| = p^m$, with $1 \leq m \leq t$. From the maximality of Δ it follows that P/K_Δ is isomorphic to a primitive subgroup of $\mathrm{Sym}(n/p^m)$ containing the normalizer $\bar{B}$ of a Sylow p-subgroup. Moreover, by Lemma 1.4.7, either $P/K_\Delta \cong \bar{B}$ or P/K_Δ is isomorphic to a minimal parabolic subgroup of $\mathrm{Sym}(n/p^m)$ with respect to $\bar{B}$.

If $P/K_\Delta \cong \bar{B}$, then $P \cong K_\Delta \rtimes \bar{B}$ and either $n/p^m = p$ and $\bar{B} = N_p$, or $n/p^m = k$, with $1 < k < p$, and $\bar{B} = \mathrm{Sym}(k)$. Thus either $n = p^{m+1}$ and $P \cong K_\Delta \rtimes N_p$, or $n = kp^m$ and $P \cong K_\Delta \rtimes \mathrm{Sym}(k)$, and we have (i) or (iv).

Suppose now that P/K_Δ is isomorphic to a minimal parabolic subgroup of $\mathrm{Sym}(n/p^m)$. Then, by Lemma 6.7.3, P is isomorphic to a subgroup of $B_m \wr \mathrm{Sym}(n/p^m)$. Moreover, since P/K_Δ is primitive, by Theorem 6.7.2, either $P/K_\Delta \cong \mathrm{PGL}(2,p)$ and $n/p^m = p+1$, with $p \neq 2, 3$, and (vii) follows; or $P/K_\Delta \cong \mathrm{Sym}(n/p^m)$ and n/p^m is one of the following

(A) $n/p^m = p$ and $p \neq 2, 3$;

(B) $n/p^m = p+1$ and $p = 2, 3$;

(C) $n/p^m = kp$, with $1 < k \leq p$;

(D) $n/p^m = k_1 p^{\alpha_1} + k_0$, with $1 \leq k_0, k_1 < p$, $\alpha_1 \geq 1$ and $(k_0, k_1, \alpha_1) \neq (1, 1, 1)$,

which imply (ii), (vi), (iii) and (v),(viii), respectively. □

A first immediate consequence of Theorem 6.7.4 is the following:

Corollary 6.7.5. *Let $P \in \mathcal{M}(G, B)$ and suppose that P is imprimitive. Suppose that $p \neq 2$ and denote by p^m, with $1 \leq m \leq t$, the length of a maximal nontrivial block of P. If one of (ii), (iii), (v), (vii) or (viii) from Theorem 6.7.4 occurs, then P is nonsoluble.*

Proof. For each of the cases listed, Theorem 6.7.4 implies that P has a nonsoluble quotient. Thus P is nonsoluble. □

Next we prove an interesting property of soluble minimal parabolic subgroups of $\mathrm{Sym}(p^r)$.

Lemma 6.7.6. *Let $G = \mathrm{Sym}(p^r)$, with $r \geq 1$ and $p \geq 3$. Let $T \in \mathrm{Syl}_p(G)$ and $B = N_G(T)$. Suppose that $P \in \mathcal{M}(G, B)$. If P is soluble, then $P \leqslant H$, where H is a subgroup of G containing T and isomorphic to the wreath product of r copies of $\mathrm{Hol}(\mathbb{Z}_p)$. In particular, if M is a subgroup of G containing B and M is soluble, then $M \leqslant H$.*

Proof. Let $P \in \mathcal{M}(G, B)$ and suppose that P is soluble. Let $r = 1$. If $p = 3$, then $B = G$ and there are no minimal parabolic subgroups of G with respect to B; if $p > 3$, then, by Corollary 6.1.3, G is the only minimal parabolic subgroup with respect to B and G is nonsoluble. Hence the case $r = 1$ is trivial.
Suppose that $r > 1$. Then G is nonsoluble and so $P \neq G$. Also, as $B \leqslant P$, we have that P is transitive and so, by Theorem 6.7.2, P is imprimitive. Then, since P is soluble and $p \neq 2$, Theorem 6.7.4 and Corollary 6.7.5 imply that $P \cong K \rtimes \mathrm{Hol}(\mathbb{Z}_p)$, where $K = P \cap L$ and

$$L = \mathrm{Sym}(\Gamma_1) \times \cdots \times \mathrm{Sym}(\Gamma_p),$$

with $|\Gamma_i| = p^{r-1}$ and $\mathrm{Hol}(\mathbb{Z}_p)$ acting on the set $\{\Gamma_1, \ldots, \Gamma_p\}$.
Now $(P \cap L)_{|\Gamma_1}$ is isomorphic to a soluble subgroup of $\mathrm{Sym}(\Gamma_1)$ containing the normalizer of a Sylow p-subgroup and so, by induction on r, $(P \cap L)_{|\Gamma_1}$ is contained in the wreath product

H_{r-1} of $r-1$ copies of $\mathrm{Hol}(\mathbb{Z}_p)$, since, by Proposition 1.4.3, $(P\cap L)_{|\Gamma_1}$ is generated by soluble minimal parabolic subgroups of $\mathrm{Sym}(\Gamma_1)$. Hence, as

$$K = P\cap L \leqslant (P\cap L)_{|\Gamma_1} \times \cdots \times (P\cap L)_{|\Gamma_p},$$

we have that K is contained in the direct product of p copies of H_{r-1} and so

$$P \cong K \rtimes \mathrm{Hol}(\mathbb{Z}_p) \leqslant \left(\underbrace{H_{r-1}\times\cdots\times H_{r-1}}_{p}\right) \rtimes \mathrm{Hol}(\mathbb{Z}_p) \cong H,$$

as required. □

Notice that Lemma 6.7.6 fails for $p=2$. Indeed, from [21] we know that all minimal parabolic subgroups of $\mathrm{Sym}(2^r)$ are soluble.

Last we shall illustrate how to derive case (iv) from Theorem 6.7.4 by induction.

Let us first reset our notation. Let $G=\mathrm{Sym}(\Omega)$, with $|\Omega|=n$, $T\in\mathrm{Syl}_p(G)$ and $B=N_G(T)$. Suppose that $n=kp^a$, with $1<k<p$ and $a\geq 1$. Let $\Omega_1,\ldots,\Omega_k$ be the orbits of T on Ω, so $|\Omega_i|=p^a$, for all $i=1,\ldots,k$. Set $G_i=\mathrm{Sym}(\Omega_i)$ and $L=G_1\times\cdots\times G_k$. Then, according to Theorem 5.3.1, $B=(B\cap L)\rtimes\mathrm{Sym}(k)\cong(B\cap G_1)\wr\mathrm{Sym}(k)$, with $B\cap G_1$ the normalizer in G_1 of $T\cap G_1$.

Lemma 6.7.7. *Let M be a subgroup of G containing B and suppose that $M\leqslant L\rtimes\mathrm{Sym}(k)$. Then $M\cong(M\cap G_1)\wr\mathrm{Sym}(k)$.*

Proof. Let M be a subgroup of G containing B and suppose that $M\leqslant L\rtimes\mathrm{Sym}(k)$. Then, by Dedekind's Modular Law,

$$M = M\cap(L\rtimes\mathrm{Sym}(k)) = (M\cap L)\rtimes\mathrm{Sym}(k),$$

with $B\cap L\leqslant M\cap L\leqslant L$ and $B\cap L$ the normalizer of a Sylow p-subgroup of L. Thus, by Corollary 1.1.12, $M\cap L=(M\cap G_1)\times\cdots\times(M\cap G_k)$. Furthermore $M\cap L$ is normalized by $\mathrm{Sym}(k)$ and $\mathrm{Sym}(k)$ acts transitively on $\{G_1,\ldots,G_k\}$. Thus $M\cap G_i\cong M\cap G_j$, for all $i,j=1,\ldots,k$, and so $M\cong(M\cap G_1)\wr\mathrm{Sym}(k)$. □

Theorem 6.7.8. *Let P be a subgroup of G containing B and suppose that $P\leqslant L\rtimes\mathrm{Sym}(k)$. Then $P\in\mathcal{M}(G,B)$ if and only if $P\cong(P\cap G_1)\wr\mathrm{Sym}(k)$, with $P\cap G_1$ minimal parabolic subgroup of G_1 with respect to $B\cap G_1$. Furthermore the unique maximal subgroup of P*

containing B is isomorphic to $U_1 \wr \mathrm{Sym}(k)$, where U_1 is the unique maximal subgroup of $P \cap G_1$ containing $B \cap G_1$.

Proof. Let P be a subgroup of G containing B and suppose that $P \leqslant L \rtimes \mathrm{Sym}(k)$. Then, by Lemma 6.7.7, $P \cong (P \cap G_1) \wr \mathrm{Sym}(k)$.

Suppose that $P \cap G_1$ is a minimal parabolic subgroup of G_1 with respect to $B \cap G_1$, with U_1 unique maximal subgroup containing $B \cap G_1$. Let U be a subgroup of P isomorphic to $U_1 \wr \mathrm{Sym}(k)$. We shall show that U is the unique maximal subgroup of P containing B. Let M be a subgroup of P containing B. Then, by Lemma 6.7.7, $M \cong (M \cap G_1) \wr \mathrm{Sym}(k)$, with $B \cap G_1 \leqslant M \cap G_1 \leqslant P \cap G_1$. Thus either $M \cap G_1 = P \cap G_1$, and $M = P$, or $M \cap G_1 \leqslant U_1$, and $M \leqslant U$, and we can conclude that $P \in \mathcal{M}(G, B)$.

Conversely, let $P \in \mathcal{M}(G, B)$ and suppose that there exist two distinct maximal subgroups M_1 and N_1 of $P \cap G_1$ containing $B \cap G_1$. Then, by Lemma 2.6.8, there are two distinct maximal subgroups of P containing B, namely $M \cong M_1 \wr \mathrm{Sym}(k)$ and $N \cong N_1 \wr \mathrm{Sym}(k)$, against the assumption that $P \in \mathcal{M}(G, B)$. Hence we must have $P \cap G_1 \in \mathcal{M}(G_1, B \cap G_1)$. □

Notice that, for $a = 1$, Theorem 6.7.8 is equivalent to Theorem 6.3.1.

Chapter 7

Minimal parabolic subgroups of $\mathbf{Sym}(p^2)$

Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^2$ and p a prime. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. We describe all minimal parabolic subgroups of G with respect to B. Recall that, by Theorem 6.4.1, G is itself a minimal parabolic subgroup. In particular, G has a unique minimal parabolic system, namely $\{G\}$, and so minimal parabolic systems of G have already been determined.

7.1 Notation

We shall first recall some notation from Sections 5.1 and 5.2.

Write $T = \langle x_1, x_2\rangle$, with x_1 cycle of length p and x_2 product of p disjoint cycles of length p. Set $T_1 = \langle x_2\rangle$ and $S_1 = \langle x_1\rangle^{T_1}$. Then S_1 is a homocyclic p-group of order p^p with generators, say, $g_1, \dots, g_p$ and $T = S_1 \rtimes T_1$. Let Δ be the set of orbits of S_1 on Ω. Then $\Delta = \{\Omega_1, \dots, \Omega_p\}$, where, for $i = 1, \dots, p$, $\Omega_i = \Omega \setminus \mathrm{Fix}_\Omega(g_i)$. Set $G_i = \mathrm{Sym}(\Omega_i)$ and $L = G_1 \times \cdots \times G_p$.

For $i = 1, 2$, let $y_i \in G$ be an element of order $p-1$ normalizing $\langle x_i\rangle$ and acting on the same set of points as x_i and let $H = \langle x_1, y_1, x_2, y_2\rangle$. Set $L_1 = \langle y_1\rangle^{T_1}$ and $K = S_1 \rtimes L_1$. Then L_1 is the direct product of p cyclic groups of order $p-1$ and has generators, say, $k_1, \dots, k_p$ such that, for $i = 1, \dots, p$, $k_i \in G_i$.

Now let B_1 be the normalizer of T_1 in $\mathrm{Sym}(\Delta)$. Then, by Corollary 5.2.6, $B_1 = \langle x_2, h_2\rangle$ and

$$B = \langle x_1, h_1, x_2, h_2\rangle = (S_1 \rtimes \langle h_1\rangle) \rtimes B_1 = (B \cap K) \rtimes B_1,$$

with $h_1 = k_1 \dots k_p$ and $h_2 = y_2$. Notice that $B_1 = \langle x_2 \rangle \rtimes \langle y_2 \rangle$ acts on the set $\{k_1, \dots, k_p\}$, with $\langle x_2 \rangle$ acting transitively on the whole set and $\langle y_2 \rangle$ fixing one of the k_i's, say k_1, and acting transitively on the remaining ones.

Finally, for $i = 1, \dots, p$, set $N_i = \langle g_i, k_i \rangle$. Then $N_i \cong \mathrm{Hol}(\mathbb{Z}_p)$ is equal to the normalizer of $\langle g_i \rangle$ in G_i and N_i is a maximal subgroup of G_i. Also $K = N_1 \times \cdots \times N_p$ and

$$H = K \rtimes B_1 = (N_1 \times \cdots \times N_p) \rtimes B_1 \cong N_1 \wr B_1 \cong \mathrm{Hol}(\mathbb{Z}_p) \wr \mathrm{Hol}(\mathbb{Z}_p),$$

so H is a maximal subgroup of $L \rtimes B_1$.

We can now proceed with our investigations.

7.2 Preliminary results

Lemma 7.2.1. *Let r be a natural number greater than 5. Then*

$$2^r < (r-1)!.$$

Proof. We prove the result by induction on r. For $r = 6$, we have $2^r = 64 < 120 = 5! = (r-1)!$ and the inequality holds. Suppose now that $r > 6$ and that $2^{r-1} < (r-2)!$. Then, since $2 < r - 1$, we get that

$$2^r = 2^{r-1} 2 < 2(r-2)! < (r-1)(r-2)! = (r-1)!.$$

$\square$

Lemma 7.2.2. *Let P be a minimal parabolic subgroup of G with respect to B such that $P \leqslant K \rtimes \mathrm{Sym}(\Delta)$ and $PK/K \cong \mathrm{Sym}(\Delta)$. Then $P = \langle B, ks \rangle$, with $k \in K$ and s any element of $\mathrm{Sym}(\Delta) \setminus B_1$.*

Proof. By Lemma 1.4.2, we know that $P = \langle B, z \rangle$, for all $z \in P \setminus U$, where U is the unique maximal subgroup of P containing B. Set $S = \mathrm{Sym}(\Delta)$ and write $z = ks$, with $k \in K$ and $s \in S$. Consider the projection $\pi \colon P \to PK/K$. Then, by Proposition 1.4.8, UK/K is the unique maximal subgroup of PK/K containing BK/K and so $PK/K = \langle BK/K, zK \rangle$, for all $zK = sK \in PK/K \setminus UK/K$. But $BK/K \cong B_1$ and $PK/K \cong S$, with B_1 maximal subgroup of S. Therefore we must have $UK/K = BK/K$ and $PK/K = \langle BK/K, sK \rangle$, for all $s \in S \setminus B_1$, which gives the result. $\square$

We shall now study the subgroups of H containing B.

Lemma 7.2.3. *Let M be a subgroup of $H = K \rtimes B_1$ and suppose that $M = \langle B, z\rangle$, for some $z \in K$. Then $M = \langle B, k_1^{\alpha}\rangle$, with $1 \le \alpha \le p-1$.*

Proof. Let $M = \langle B, z\rangle$, with $z \in K$, and write $z = k_1^{\alpha_1} k_2^{\alpha_2} \dots k_p^{\alpha_p}$. Set

$$W = \langle B, k_1^{\alpha_i - \alpha_j} \mid i, j \in \{1, \dots, p\}\rangle.$$

We shall first prove that $M = W$. Since $\langle x_2\rangle$ is transitive on $\{k_1, k_2, \dots, k_p\}$, we have that, for all $j = 1, \dots, p$, there exists $e \in \{1, \dots, p\}$ such that $k_j^{x_2^e} = k_1$. Then consider the element $v = z^{x_2^e} = k_1^{\alpha_j} w \in M$, with $w \in \langle k_2, \dots, k_p\rangle$. Since $\langle y_2\rangle$ is transitive on $\{k_2, \dots, k_p\}$ and fixes k_1, we get that

$$\prod_{i=1}^{p-1} v^{y_2^i} = k_1^{\alpha_j(p-1)} \prod_{i=1}^{p-1} w^{y_2^i} = k_1^{\alpha_j(p-1)} k_2^{\beta_j} \dots k_p^{\beta_j} = (k_2 \dots k_p)^{\beta_j} \in M,$$

where $\beta_j = \sum_{i \neq j} \alpha_i$. Thus, for all $j = 1, \dots, p$, $k_1^{-\beta_j} = (k_2 \dots k_p)^{\beta_j} h_1^{-\beta_j} \in M$. Therefore, for $i, j \in \{1, \dots, p\}$, $i \neq j$, we also have

$$k_1^{\alpha_i - \alpha_j} = k_1^{\beta_j} k_1^{-\beta_i} \in M$$

and, of course, we can assume $k_1^{\alpha_j - \alpha_j} \in M$, for all $j = 1, \dots, p$. Hence $W \leqslant M$.
Conversely, we want to prove that $z \in W$. If $k_1^{\beta} \in W$, then $(k_1^{\beta})^{x_2^e} = (k_1^{x_2^e})^{\beta} \in W$, for all $e = 1, \dots, p$. By the transitivity of $\langle x_2\rangle$ on $\{k_1, k_2, \dots, k_p\}$, this implies that $k_j^{\beta} \in W$, for all $j = 1, \dots, p$. Thus $k_l^{\alpha_i - \alpha_j} \in W$, for all $i, j, l = 1, \dots, p$, and, in particular, $k_i^{\alpha_i - \alpha_j} \in W$. Hence

$$z = k_1^{\alpha_1} k_2^{\alpha_2} \dots k_p^{\alpha_p} = (k_1^{\alpha_1 - \alpha_j} k_2^{\alpha_2 - \alpha_j} \dots k_p^{\alpha_p - \alpha_j}) h_1^{\alpha_j} \in W$$

and so $W = M$.
Look now at the subgroup $W' = \langle k_1^{\alpha_i - \alpha_j} \mid i, j \in \{1, \dots, p\}\rangle$ such that $W = \langle B, W'\rangle$. Then W' is a subgroup of the cyclic group generated by k_1. Thus there exists $\alpha = 1, \dots, p-1$, such that $W' = \langle k_1^{\alpha}\rangle$ and $M = W = \langle B, k_1^{\alpha}\rangle$, as required. ☐

Corollary 7.2.4. *Let M be a subgroup of H containing B. Then $M = \langle B, k_1^{\alpha}\rangle$, for some $\alpha = 1, \dots, p-1$.*

Proof. Since M is a finite group, M is finitely generated and so can be written as $M = \langle B, z_1, \ldots, z_s \rangle$, with $z_1, \ldots, z_s \in K$. By Lemma 7.2.3, each z_i can be replaced by a suitable power of k_1, $k_1^{\beta_i}$, say, and so $M = \langle B, k_1^{\beta_1}, \ldots, k_1^{\beta_s} \rangle$. But now $\langle k_1^{\beta_1}, \ldots, k_1^{\beta_s} \rangle$ is a subgroup of the cyclic group $\langle k_1 \rangle$ and so there exists α such that $\langle k_1^{\beta_1}, \ldots, k_1^{\beta_s} \rangle = \langle k_1^{\alpha} \rangle$. Hence $M = \langle B, k_1^{\alpha} \rangle$. $\square$

For j dividing $p-1$, define the following subgroup

$$K_j = S_1 \rtimes \langle h_1, k_1^{(p-1)/j}, \ldots, k_p^{(p-1)/j} \rangle = (B \cap K)\langle k_1^{(p-1)/j}, \ldots, k_p^{(p-1)/j} \rangle.$$

Clearly, K_j is normalized by B_1 and $K_j \cap B_1 = 1$. Thus $\langle K_j, B_1 \rangle = K_j \rtimes B_1$. Moreover, since the k_i's are all conjugate in $\langle x_2 \rangle \leqslant B$, we have that

$$K_j \rtimes B_1 = \langle B, k_i^{(p-1)/j} \rangle,$$

for all $i = 1, \ldots, p$.

Corollary 7.2.5. *The lattice of subgroups of H containing B is isomorphic to the lattice of subgroups of $\langle k_1 \rangle$, cyclic group of order $p-1$. The subgroup of H corresponding to the cyclic subgroup of $\langle k_1 \rangle$ of order j is given by $K_j \rtimes B_1$. In particular, B corresponds to the identity subgroup of $\langle k_1 \rangle$ and H corresponds to the whole of $\langle k_1 \rangle$.*

Proof. The result follows immediately from Corollary 7.2.4, since $K_j \rtimes B_1 = \langle B, k_1^{(p-1)/j} \rangle$. $\square$

Lemma 7.2.6. *Let j divide $p-1$ and set $K'_j = K_j \cap L_1$, with $L_1 = \langle k_1, \ldots, k_p \rangle$. Then $k \in K'_j$ if and only if k is of the form*

$$k_1^{\alpha_1} k_2^{\alpha_2} \ldots k_p^{\alpha_p},$$

with $\alpha_i \equiv \beta \pmod{(p-1)/j}$, for some $\beta \in \mathbb{Z}_{(p-1)/j}$ and for all $i = 1, \ldots, p$.

Proof. First, from the definition of K_j it follows that $K'_j = \langle h_1, k_1^{(p-1)/j}, \ldots, k_p^{(p-1)/j} \rangle$. Consider now the element $k_1^{\alpha_1} k_2^{\alpha_2} \ldots k_p^{\alpha_p}$, with $\alpha_i \equiv \beta \pmod{(p-1)/j}$, for all $i = 1, \ldots, p$, and write $\alpha_i = \beta + \beta_i (p-1)/j$. Then, since the k_i's commute, we get that

$$\begin{aligned}
k_1^{\alpha_1} k_2^{\alpha_2} \ldots k_p^{\alpha_p} &= k_1^{\beta+\beta_1(p-1)/j} k_2^{\beta+\beta_2(p-1)/j} \ldots k_p^{\beta+\beta_p(p-1)/j} \\
&= (k_1^{\beta} k_2^{\beta} \ldots k_p^{\beta})(k_1^{\beta_1(p-1)/j} k_2^{\beta_2(p-1)/j} \ldots k_p^{\beta_p(p-1)/j}) \\
&= (k_1 k_2 \ldots k_p)^{\beta} (k_1^{(p-1)/j})^{\beta_1} (k_2^{(p-1)/j})^{\beta_2} \ldots (k_p^{(p-1)/j})^{\beta_p},
\end{aligned}$$

which is the generic element of K'_j. $\square$

7.3 Main theorems

By Theorem 6.4.1, G is a minimal parabolic subgroup with respect to B, whose unique maximal subgroup containing B is

$$U = (G_1 \times \cdots \times G_p) \rtimes \mathrm{Sym}(\Delta) = L \rtimes \mathrm{Sym}(\Delta) \cong \mathrm{Sym}(p) \wr \mathrm{Sym}(p).$$

Therefore all proper subgroups of G containing B lie in U. In particular, all proper minimal parabolic subgroups with respect to B do so. Thus they are imprimitive and, as $|\Omega| = p^2$, every nontrivial proper block system has blocks of length p.

Now, if $p = 2$, then $T = B = U$ is a maximal subgroup of G and, if $p = 3$, then $U = K \rtimes B_1$ is the unique proper subgroup of G containing B. Therefore these two cases are trivial and from now on we shall assume that $p > 3$.

Suppose that P is a minimal parabolic subgroup of G with respect to B and $P \neq G$. Thus $P \leqslant U = L \rtimes \mathrm{Sym}(\Delta)$ and, by Lemma 1.4.7, either $P/(P \cap L) \cong B_1$ or $P/(P \cap L) \cong \mathrm{Sym}(\Delta)$. In the first case, it follows immediately that $P = (P \cap L) \rtimes B_1$ and so $P \leqslant L \rtimes B_1$. In the second case, since $P \neq B(P \cap L)$, by Lemma 1.4.6, we have that $S_1 = T \cap L \trianglelefteq P$ and so $P \leqslant N_U(S_1) = K \rtimes \mathrm{Sym}(\Delta)$. Thus either

$$P \leqslant L \rtimes B_1 \quad \text{or} \quad P \leqslant K \rtimes \mathrm{Sym}(\Delta)$$

and, in particular, $U = L \rtimes \mathrm{Sym}(\Delta)$ is not a minimal parabolic subgroup with respect to B. Also notice that both $L \rtimes B_1$ and $K \rtimes \mathrm{Sym}(\Delta)$ are maximal subgroups of U, the latter following from Lemma 2.6.8.

We shall first study the case when $P \leqslant K \rtimes \mathrm{Sym}(\Delta)$. So let P be a minimal parabolic subgroup of G with respect to B and suppose that $P \leqslant K \rtimes \mathrm{Sym}(\Delta)$. Then there exists $P_1 \leqslant K \rtimes B_1$, namely $P_1 = (P \cap K) \rtimes B_1$, such that $B \leqslant P_1$. Thus, by Corollary 7.2.5, $P_1 = K_j \rtimes B_1$, for some j dividing $p-1$, and so $P \cap K = P_1 \cap K = K_j$. Also, by Lemma 1.4.7, we have that either

$$P/(P \cap K) \cong B_1 \quad \text{or} \quad P/(P \cap K) \cong \mathrm{Sym}(\Delta).$$

Finally notice that $K \rtimes \mathrm{Sym}(\Delta)$ is not a minimal parabolic subgroup with respect to B, because it contains the subgroups $K \rtimes B_1$ and $(B \cap K) \rtimes \mathrm{Sym}(\Delta)$, both containing B, which together generate the whole $K \rtimes \mathrm{Sym}(\Delta)$. So, in particular, $P \neq K \rtimes \mathrm{Sym}(\Delta)$.

Lemma 7.3.1. *Let $p > 3$ be a prime. Suppose that $P \leqslant K \rtimes \mathrm{Sym}(\Delta)$ is a minimal parabolic subgroup of G with respect to B such that $P/(P \cap K) \cong \mathrm{Sym}(\Delta)$ and let $K_j = P \cap K$, for some j dividing $p-1$. If $P \leqslant K_r \rtimes \mathrm{Sym}(\Delta)$, with $r \neq j$ dividing $p-1$, then $P \leqslant K_q \rtimes \mathrm{Sym}(\Delta)$, for all q dividing r and divisible by j such that r/q is a prime.*

Proof. Let q be an integer dividing r and divisible by j such that r/q is a prime, that is, r/q is a prime divisor of r/j. Then $K_j \leqslant K_q \leqslant K_r$. Since K_q is normalized by P, we can consider the subgroup $P^* = PK_q$. Then it will be enough to show that $P^* = K_q \rtimes \mathrm{Sym}(\Delta)$.
Now $P \cap K_q = P \cap K_r = P \cap K = K_j$ and so, by assumption,

$$P^*/K_q = PK_q/K_q \cong P/(P \cap K_q) \cong \mathrm{Sym}(\Delta).$$

Thus $|P^*| = |K_q||\mathrm{Sym}(\Delta)|$ and we only need to prove that $\mathrm{Sym}(\Delta) \leqslant P^*$.
According to Lemma 1.4.2, write $P = \langle B,\ sk \rangle$, with $s \in \mathrm{Sym}(\Delta)$ and $k \in K_r$. Our aim is to show that $k \in P^*$. If $k \in B$, we are done. Hence assume that $k \in K_r \setminus (B \cap K_r)$, that is, $k \in \langle k_i^{(p-1)/r} \mid i = 1, \ldots, p \rangle$ and write

$$k = k_1^{\alpha_1} k_2^{\alpha_2} \ldots k_p^{\alpha_p},$$

with $\alpha_i = \beta_i (p-1)/r$, for all $i = 1, \ldots, p$.
Suppose that $p-1$ is not a prime power. Then there exists $t \neq 1$ prime, $t|(p-1)$ such that $t \neq r/q$. Now y_2 is a product of p cycles of length $p-1$ and acts on the set $\{k_1, \ldots, k_p\}$ fixing k_1 and permuting transitively the elements $k_2, \ldots, k_p$, that is, y_2 acts on $\{k_1, \ldots, k_p\}$ as a cycle of length $p-1$. Then $y_2^{(p-1)/t}$ is a product of $p(p-1)/t$ disjoint cycles of length t and acts on $\{k_1, \ldots, k_p\}$ fixing k_1 and breaking the set $\{k_2, \ldots, k_p\}$ into orbits of length t. This implies that we can factorize $y_2^{(p-1)/t}$ as

$$y_2^{(p-1)/t} = s_1 s_2,$$

with $s_1, s_2 \in \mathrm{Sym}(\Delta) \setminus B_1$, s_1 moving the elements $k_2, \ldots, k_{t+1}$ and fixing all the other k_j's and s_2 fixing $k_1, k_2, \ldots, k_{t+1}$. In particular, s_1 and s_2 have order t.
According to Lemma 7.2.2, choose $s = s_1$. Then

$$(s_1 k)^t = k^{s_1^{(t-1)}} \ldots k^{s_1^2} k^{s_1} k \in P,$$

which implies, since $\mathrm{Sym}(\Delta)$ normalizes K_r, that $(s_1k)^t \in P \cap K_r = K_j \leqslant K_q$. Moreover, since $k = k_1^{\alpha_1}k_2^{\alpha_2}\dots k_p^{\alpha_p}$ and s_1 moves only $k_2, \dots, k_{t+1}$, writing $(s_1k)^t$ in terms of the k_i's, we get that

$$(s_1k)^t = k_1^{t\alpha_1}k_2^{\alpha_2+\dots+\alpha_{t+1}}\dots k_{t+1}^{\alpha_2+\dots+\alpha_{t+1}}k_{t+2}^{t\alpha_{t+2}}\dots k_p^{t\alpha_p}$$

and $(s_1k)^t$ is a p'-element. Hence $(s_1k)^t \in K_q'$, which implies, by Lemma 7.2.6, that

$$t\alpha_1 = t\alpha_j \pmod{r/q}, \quad \text{for all } j = t+2, \dots, p.$$

Since, by the choice made, t is not a zero–divisor of r/q, it follows that

$$\alpha_1 = \alpha_j \pmod{r/q}, \quad \text{for all } j = t+2, \dots, p.$$

Now consider the element $s_2^{-1}k$ and recall that $s_1s_2 = y_2^{(p-1)/t} \in B_1 \leqslant P$. Thus $(s_1k)(s_2^{-1}k)^{-1} = s_1s_2 \in P$, which implies that $s_2^{-1}k \in P$. Hence, as before,

$$(s_2^{-1}k)^t = k^{s_2}k^{s_2^2}\dots k^{s_2^{(t-1)}}k \in P \cap K_r = K_j \leqslant K_q$$

and, since s_2 fixes $k_1, k_2, \dots, k_{t+1}$, we also get

$$(s_2^{-1}k)^t = k_1^{t\alpha_1}k_2^{t\alpha_2}\dots k_{t+1}^{t\alpha_{t+1}}w,$$

with $w \in \langle k_{t+2}, \dots, k_p\rangle$. Thus $(s_2^{-1}k)^t \in K_q'$ and, by Lemma 7.2.6,

$$t\alpha_1 = t\alpha_j \pmod{r/q}, \quad \text{for all } j = 2, \dots, t+1$$

that is, since t is not a zero–divisor of r/q,

$$\alpha_1 = \alpha_j \pmod{r/q}, \quad \text{for all } j = 2, \dots, t+1.$$

Therefore, $\alpha_1 = \alpha_j \pmod{r/q}$, for all $j = 1, \dots, p$, which implies that $k \in K_q' \leqslant K_q$. Then $k \in P^*$ and $s = (sk)k^{-1} \in P^*$. So, as $s \in \mathrm{Sym}(\Delta) \setminus B_1$, we get that $\mathrm{Sym}(\Delta) \leqslant P^*$, which implies that $P^* = K_q \rtimes \mathrm{Sym}(\Delta)$.

It remains to consider the case when $p-1$ is a prime power, that is, $p-1 = 2^a$, for some $a > 1$. Then $r/q = 2$ and so, for $r = 2^b$, we have $q = 2^{b-1}$. Therefore $|K_r| = p^p(2^b)^p2^{a-b}$ and $|K_q| = p^p(2^{b-1})^p2^{a-b+1}$. Thus $|K_r : K_q| = 2^{p-1}$, which, for $p \geq 7$, is, by Lemma 7.2.1, less than $(p-2)!$. Then, assuming that $K_q = P^* \cap K_r = 1$, that is, working in the quotient group

$P^*/K_q \cong PK_r/K_r$, we have that P^* is a complement to K_r in $K_r \rtimes \mathrm{Sym}(\Delta)$ and $B_1 \leqslant P^*$, with $|K_r| < |\mathrm{Sym}(\Delta) : B_1|$ and B_1 maximal subgroup of $\mathrm{Sym}(\Delta)$. Hence, by Lemma 2.6.9, $P^* = \mathrm{Sym}(\Delta)$, that is, because of the assumption $K_q = 1$, $P^* = K_q \rtimes \mathrm{Sym}(\Delta)$. Finally, for $p = 5$ the factorization of P^* can be obtained by hands as one can see in the example at the end of the chapter. $\square$

Theorem 7.3.2. *Suppose that $p > 3$ is a prime and let P be a subgroup of $K \rtimes \mathrm{Sym}(\Delta)$ containing B. Then $P \in \mathcal{M}(G, B)$ if and only if P is one of the following:*

(i) *$K_j \rtimes B_1$, with j prime power dividing $p-1$, $j \neq 1$; or*

(ii) *$(B \cap K) \rtimes \mathrm{Sym}(\Delta)$.*

Furthermore, if U denotes the unique maximal subgroup of P containing B, then, for $P = K_{q^\alpha} \rtimes B_1$, with q prime and q^α dividing $p-1$, we have $U = K_{q^{\alpha-1}} \rtimes B_1$; and, for $P = (B \cap K) \rtimes \mathrm{Sym}(\Delta)$, we have $U = B$.

Proof. Let $P = K_j \rtimes B_1$, with $j = q^\alpha$ dividing $p-1$ and q prime. Then, by Corollary 7.2.5, there exists a unique maximal subgroup of P containing B, namely $K_{q^{\alpha-1}} \rtimes B_1$, and so $P \in \mathcal{M}(G, B)$. Now assume that $P = (B \cap K) \rtimes \mathrm{Sym}(\Delta)$. Then B is a maximal subgroup of P and so $P \in \mathcal{M}(G, B)$.

Conversely, let $P \leqslant K \rtimes \mathrm{Sym}(\Delta)$ and suppose that $P \in \mathcal{M}(G, B)$. Then, by Lemma 1.4.7, either $P/(P \cap K) \cong B_1$, and so $P = (P \cap K) \rtimes B_1 \leqslant K \rtimes B_1$, or $P/(P \cap K) \cong \mathrm{Sym}(\Delta)$.

Let us first assume that $P \leqslant K \rtimes B_1$. Then, by Corollary 7.2.5, $P = K_j \rtimes B_1 = \langle B, k_1^{(p-1)/j} \rangle$, with $j \neq 1$ dividing $p-1$. Furthermore, since P is a minimal parabolic subgroup, $\langle k_1^{(p-1)/j} \rangle$ is a subgroup of $\langle k_1 \rangle$ having a unique maximal subgroup. But in a cyclic group maximal subgroups are those of prime index, since cyclic groups verify the inverse of Lagrange's Theorem. Hence subgroups which have a unique maximal subgroup must have prime power order. Thus j is a prime power dividing $p-1$ and (i) is proved.

Suppose now that $P/(P \cap K) \cong \mathrm{Sym}(\Delta)$ and let $K_j = P \cap K$, with $j | (p-1)$. Since $K \rtimes \mathrm{Sym}(\Delta)$ is not a minimal parabolic subgroup, we have that $P \neq K \rtimes \mathrm{Sym}(\Delta)$. Thus $K_j \neq K$, that is, $j \neq p-1$. We shall first prove that P splits as $K_j \rtimes \mathrm{Sym}(\Delta)$. Since $|P| = |K_j||\mathrm{Sym}(\Delta)|$, it will be enough to show that $P \leqslant K_j \rtimes \mathrm{Sym}(\Delta)$.

If $(p-1)/j$ is a prime, then, by Lemma 7.3.1, $P \leqslant K_j \rtimes \mathrm{Sym}(\Delta)$. Assume now that $(p-1)/j$

is not a prime. Then there exists r dividing $p-1$ and divisible by j such that $(p-1)/r$ is a prime. Then, by Lemma 7.3.1, $P \leqslant K_r \rtimes \mathrm{Sym}(\Delta)$. Consider now r/j. If r/j is a prime, then, by Lemma 7.3.1, $P \leqslant K_j \rtimes \mathrm{Sym}(\Delta)$. Otherwise, repeating the previous argument, we get that $P \leqslant K_q \rtimes \mathrm{Sym}(\Delta)$, for some q such that r/q is a prime. Recursively, we get that $P \leqslant K_j \rtimes \mathrm{Sym}(\Delta)$ and so $P = K_j \rtimes \mathrm{Sym}(\Delta)$.

Now look at the subgroups $K_j \rtimes B_1$ and $(B \cap K) \rtimes \mathrm{Sym}(\Delta)$ of P. If $K_j \neq B \cap K$, then they both properly contain B and the subgroup generated by them is the whole of P, against the assumption that P is a minimal parabolic subgroup with respect to B. Thus we must have that $K_j = B \cap K$ and $P = (B \cap K) \rtimes \mathrm{Sym}(\Delta)$, proving case (ii). $\square$

Theorem 7.3.2 suggests a new piece of notation. For $q \in \pi(p-1)$, let q^{α_q} be the highest power of q dividing $p-1$. For $\alpha = 0, \ldots, \alpha_q$, set

$$P(q, \alpha) = K_{q^\alpha} \rtimes B_1,$$

Then $B = P(q, 0)$, for any $q \in \pi(p-1)$, and, for $P = P(q, \alpha)$, $U = P(q, \alpha - 1)$.

We shall now look at the case when P is a minimal parabolic subgroup of G with respect to B such that $P \leqslant L \rtimes B_1$ and $P \nleqslant K \rtimes B_1$, that is, $P = (P \cap L) \rtimes B_1$, with $P \cap K < P \cap L$. For $i = 1, \ldots, p$, set $A_i = \mathrm{Alt}(\Omega_i)$ and $A = A_1 \times \cdots \times A_p$. Then $A \trianglelefteq L$ and so A is normalized by $\langle h_1 \rangle$. Moreover $A\langle h_1 \rangle$ is normalized by B_1. Set

$$P_A = (A\langle h_1 \rangle) \rtimes B_1.$$

Since p is an odd prime, we have that $g_i \in A_i$, for all $i = 1, \ldots, p$. So $S_1 \leqslant A$ and

$$B = (S_1 \rtimes \langle h_1 \rangle) \rtimes B_1 \leqslant P_A.$$

Also $P_A \leqslant L \rtimes B_1$ and $P_A \nleqslant K \rtimes B_1$, since $A\langle h_1 \rangle \nleqslant K$. Furthermore, $K \rtimes B_1 \nleqslant P_A$, because $K \nleqslant A$. Since, by Lemma 2.6.8, $K \rtimes B_1$ is a maximal subgroup of $L \rtimes B_1$, this implies, in particular, that $\langle K \rtimes B_1, P_A \rangle = L \rtimes B_1$ and so $L \rtimes B_1$ is not a minimal parabolic subgroup of G with respect to B.

Finally, since the square of any cycle is an even permutation, we have that $k_i^2 \in A_i$, for all $i = 1, \ldots, p$, and so

$$K_{(p-1)/2} = S_1 \rtimes \langle h_1, k_1^2, \ldots, k_p^2 \rangle \leqslant A\langle h_1 \rangle,$$

which implies that $K_{(p-1)/2} \rtimes B_1 \leqslant P_A$.

Lemma 7.3.3. *P_A is a maximal subgroup of $L \rtimes B_1$.*

Proof. Let M be a subgroup of $L \rtimes B_1$ containing P_A. Then, by Dedekind's Modular Law, we have that

$$M = M \cap (L \rtimes B_1) = (M \cap L) \rtimes B_1,$$

where $A\langle h_1\rangle \leqslant M \cap L \leqslant L$. Now $A\langle h_1\rangle \trianglelefteq L$, so $A\langle h_1\rangle \trianglelefteq M \cap L$ and $S_1 \in \mathrm{Syl}_p(A\langle h_1\rangle)$. Then, by the Frattini argument, $M \cap L = A\langle h_1\rangle N_{M\cap L}(S_1)$, with $N_{M\cap L}(S_1) \leqslant N_L(S_1) = K$. Thus

$$M = A\langle h_1\rangle N_{M\cap L}(S_1)B_1 = P_A N_{M\cap L}(S_1)$$

and M contains the subgroup

$$M_0 = \langle K_{(p-1)/2} \rtimes B_1, N_{M\cap L}(S_1)\rangle \leqslant K \rtimes B_1.$$

Now, by Corollary 7.2.5, $K_{(p-1)/2} \rtimes B_1$ is a maximal subgroup of $K \rtimes B_1$ and so it follows that either $M_0 = K_{(p-1)/2} \rtimes B_1$ or $M_0 = K \rtimes B_1$.
If $M_0 = K_{(p-1)/2} \rtimes B_1$, then $N_{M\cap L}(S_1) \leqslant K_{(p-1)/2} \rtimes B_1 \leqslant P_A$ and $M = P_A$. If $M_0 = K \rtimes B_1$, then M contains the subgroup $\langle K \rtimes B_1, P_A\rangle = L \rtimes B_1$ and so $M = L \rtimes B_1$. □

Lemma 7.3.4. *Suppose that $p > 3$ is a prime. Let M be a subgroup of $L \rtimes B_1$ containing B. Then either $M \leqslant K \rtimes B_1$ or $P_A \leqslant M$.*

Proof. Let M be a subgroup of $L \rtimes B_1$ containing B. Then, by Dedekind's Modular Law, we have that

$$M = M \cap (L \rtimes B_1) = (M \cap L) \rtimes B_1,$$

with $B \cap K < M \cap L \leqslant L$. Consider the action of $B \cap K$, $M \cap L$ and L on the block Ω_1. Then

$$N_1 = (B \cap K)_{|\Omega_1} \leqslant (M \cap L)_{|\Omega_1} \leqslant L_{|\Omega_1} = G_1$$

and, because N_1 is a maximal subgroup of G_1, we have that $(M \cap L)_{|\Omega_1}$ is either equal to N_1 or to G_1. Moreover, since B_1 permutes transitively the subgroups $(M \cap L)_{|\Omega_i}$, we have that $(M \cap L)_{|\Omega_i} \cong (M \cap L)_{|\Omega_j}$, for all $i, j = 1, \dots, p$. Hence either $(M \cap L)_{|\Omega_i} \cong N_i$ or $(M \cap L)_{|\Omega_i} \cong G_i$, for all $i = 1, \dots, p$. If the former holds, then

$$M \cap L \leqslant (M \cap L)_{|\Omega_1} \times \cdots \times (M \cap L)_{|\Omega_p} = N_1 \times \cdots \times N_p = K$$

and so $M = (M \cap L) \rtimes B_1 \leqslant K \rtimes B_1$.

Suppose now that $(M \cap L)_{|\Omega_i} \cong G_i$, for all $i = 1, \dots, p$. Then $M \cap L$ contains the subgroup

$$\langle g_1 \rangle^{M \cap L} = \langle g_1 \rangle^{(M\cap L)_{|\Omega_1}} = \langle g_1 \rangle^{G_1} \trianglelefteq G_1.$$

Since $g_1 \in A_1$, this implies that $\langle g_1 \rangle^{G_1} \trianglelefteq A_1$ and so, as $p \geq 5$, it follows that $\langle g_1 \rangle^{G_1} = A_1$ and $A_1 \leqslant M \cap L$. Similarly, we get that $A_i \leqslant M \cap L$, for all $i = 1, \dots, p$, and so $A = A_1 \times \cdots \times A_p \leqslant M \cap L$. Therefore $P_A \leqslant M$, completing the proof. $\square$

Theorem 7.3.5. *Suppose that $p > 3$ is a prime. Let P be a subgroup of $L \rtimes B_1$ containing B and such that $P \nleqslant K \rtimes B_1$. Then $P \in \mathcal{M}(G, B)$ if and only if $P = P_A$. Furthermore the unique maximal subgroup of P_A containing B is given by $K_{(p-1)/2} \rtimes B_1$.*

Proof. Let M be a subgroup of P_A properly containing B. Then, by Lemma 7.3.4, either $P_A \leqslant M$ or $M \leqslant K \rtimes B_1$, that is, either $P_A = M$ or

$$M \leqslant P_A \cap (K \rtimes B_1) = K_{(p-1)/2} \rtimes B_1,$$

which implies that $K_{(p-1)/2} \rtimes B_1$ is the unique maximal subgroup of P_A containing B. Hence $P_A \in \mathcal{M}(G, B)$.

Conversely, let P be a subgroup of $L \rtimes B_1$ containing B and such that $P \nleqslant K \rtimes B_1$ and suppose that $P \in \mathcal{M}(G, B)$. Then, by Lemma 7.3.4, we must have have that $P_A \leqslant P$ and so, by Lemma 7.3.3, either $P = P_A$ or $P = L \rtimes B_1$. But, by assumption, P is a minimal parabolic subgroup of G with respect to B, whereas $L \rtimes B_1$ is not. Hence we must conclude that $P = P_A$. $\square$

Corollary 7.3.6. *Suppose that $p > 3$ is a prime and let P be a subgroup of G containing B. Then $P \in \mathcal{M}(G, B)$ if and only if P is one of the following*

(i) *G;*

(ii) *P_A;*

(iii) *$P(q, \alpha)$, for $q \in \pi(p-1)$ and $1 \leq \alpha \leq \alpha_q$;*

(iv) *$(B \cap K) \rtimes \mathrm{Sym}(\Delta)$.*

In particular, G has $3 + \sum_{q \in \pi(p-1)} \alpha_q$ minimal parabolic subgroups with respect to B.

The results established in Theorems 7.3.2 and 7.3.5 can be summarized as in Table 7.1, where P denotes a minimal parabolic subgroup of G with respect to B and U denotes the unique maximal subgroup of P containing B.

P	U	Additional conditions
G	$L \rtimes \mathrm{Sym}(\Delta)$	
P_A	$K_{(p-1)/2} \rtimes B_1$	
$P(q, \alpha)$	$P(q, \alpha - 1)$	$q \in \pi(p-1), 1 \leq \alpha \leq \alpha_q$
$(B \cap K) \rtimes \mathrm{Sym}(\Delta)$	$B = (B \cap K) \rtimes B_1$	

Table 7.1: Minimal parabolic subgroups of $\mathrm{Sym}(p^2)$

7.4 An example

We shall conclude the chapter by working out all minimal parabolic subgroups of the symmetric group Sym(25). So let $p = 5$ and $G = \mathrm{Sym}(p^2)$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Write $T = \langle x_1, x_2 \rangle$, with

$$x_1 = (1\ 2\ 3\ 4\ 5),$$

$$x_2 = (1\ 6\ 11\ 16\ 21)(2\ 7\ 12\ 17\ 22)(3\ 8\ 13\ 18\ 23)(4\ 9\ 14\ 19\ 24)(5\ 10\ 15\ 20\ 25),$$

and let

$$y_1 = (2\ 3\ 5\ 4),$$

$$y_2 = (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20).$$

Then $H = \langle T, y_1, y_2 \rangle \cong 5^5 : 4^5 : 5 : 4$ and $B = T \rtimes \langle h_1, h_2 \rangle \cong 5^5 : 4 : 5 : 4$, with

$$h_1 = (2\ 3\ 5\ 4)(7\ 8\ 10\ 9)(12\ 13\ 15\ 14)(17\ 18\ 20\ 19)(22\ 23\ 25\ 24)$$

and $h_2 = y_2$. Since $p - 1 = 2^2$, there are five minimal parabolic subgroups of G with respect to B, of which only two are contained in H, and they are

$$
\begin{aligned}
P_1 &= G = \mathrm{Sym}(25),\\
P_2 &= P_A \cong \mathrm{Alt}(5)^5 : 2 : 5 : 4,\\
P_3 &= P(2,1) \cong 5^5 : 2^{5\cdot}2 : 5 : 4,\\
P_4 &= P(2,2) \cong 5^5 : 4^5 : 5 : 4,\\
P_5 &= (B \cap K) \rtimes \mathrm{Sym}(\Delta) \cong 5^5 : 4 : \mathrm{Sym}(5),
\end{aligned}
$$

where, in describing the shape of each P_i, we have used the notation from the ATLAS ([7]). Furthermore, by Lemma 1.4.2, each of them can be written as $P_i = \langle B, z_i \rangle$, with $z_i \in G$ not uniquely determined. For instance we can choose

$$
\begin{aligned}
z_1 &= (1\ 6),\\
z_2 &= (1\ 2\ 3),\\
z_3 &= (2\ 5)(3\ 4),\\
z_4 &= (2\ 3\ 5\ 4),\\
z_5 &= (1\ 6)(2\ 7)(3\ 8)(4\ 9)(5\ 10).
\end{aligned}
$$

Notice that in this case, since $p-1$ is a prime power, H is a minimal parabolic subgroup of G with respect to B, namely $H = P(2,2)$.

Figure 7.1 on the next page shows the full lattice of subgroups of Sym(25) containing B. The subgroups which are coloured are the minimal parabolic subgroups with respect to B and every other subgroup is expressed in terms of those. In particular, we have

$$
\begin{aligned}
\langle P_2, P_4 \rangle &\cong \mathrm{Sym}(5)^5 : 5 : 4,\\
\langle P_2, P_5 \rangle &\cong \mathrm{Alt}(5)^5 : 2 : \mathrm{Sym}(5),\\
\langle P_3, P_5 \rangle &\cong 5^5 : 2^{5\cdot}2 : \mathrm{Sym}(5),\\
\langle P_4, P_5 \rangle &\cong 5^5 : 4^5 : \mathrm{Sym}(5),\\
\langle P_2, P_4, P_5 \rangle &\cong \mathrm{Sym}(5)^5 : \mathrm{Sym}(5).
\end{aligned}
$$

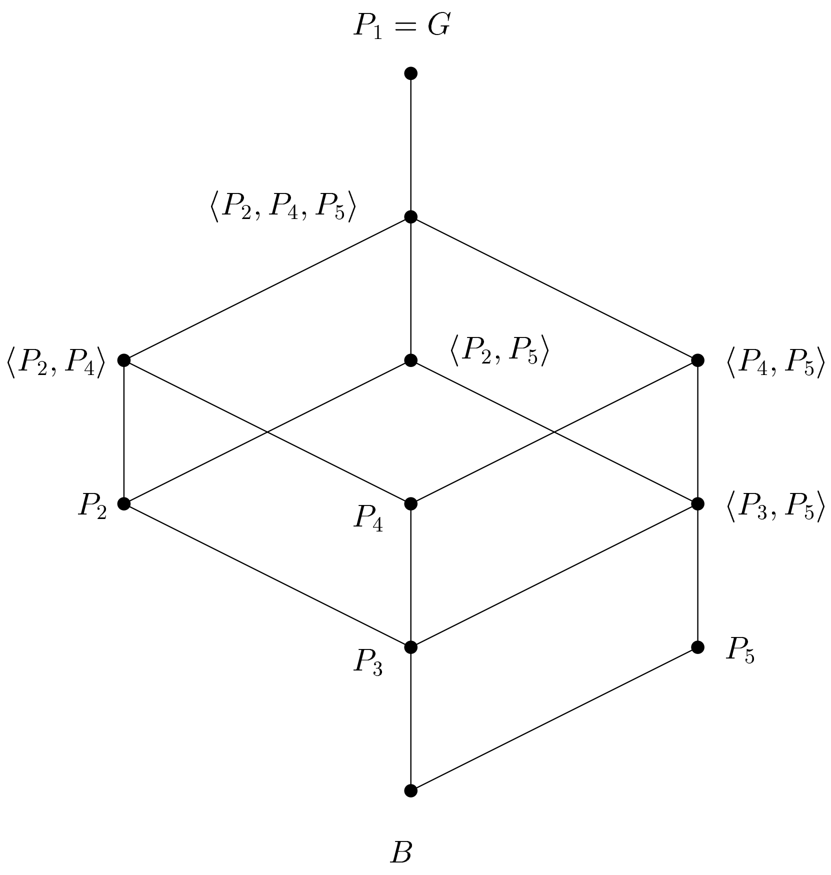

Figure 7.1: The lattice of subgroups of $\mathrm{Sym}(5^2)$ containing B

Chapter 8

Some FG-modules related to minimal parabolic subgroups

We study certain modules which are invariant under the natural action of the normalizer of a Sylow p-subgroup of the symmetric group $\mathrm{Sym}(p^r)$. These will be used in Chapter 10 to describe all soluble minimal parabolic subgroups of $\mathrm{Sym}(\Omega)$, with $|\Omega|$ a power of p.

8.1 General facts about FG-modules

Definition 8.1.1. *Let F be a finite field and V be a vector space over F. Let G be a group and suppose that V is an FG-module. Then V is said to be* **irreducible** *if V has no nontrivial proper FG-submodule.*

Definition 8.1.2. *Let F be a finite field and V be a vector space over F. Let G be a group and suppose that V is an FG-module. Then V is* **completely reducible** *if V can be written as the direct sum of some irreducible FG-submodules of V.*

Lemma 8.1.3. *Let F be a finite field, G be a group and V be an FG-module. Suppose that V is completely reducible and that the irreducible submodules appearing in the decomposition of V are pairwise nonisomorphic, that is,*

$$V = V_1 \oplus \cdots \oplus V_t,$$

where, for all $i, j = 1, \ldots, t$, $i \neq j$, V_i is an irreducible FG-submodule of V and $V_i \not\cong V_j$. Then $V_1, \ldots, V_t$ are the only irreducible FG-submodules of V.

Proof. Let U be an irreducible FG-submodule of V. Suppose that $U \cong V_j$, for some $j = 1, \ldots, t$, and consider the submodule $U \oplus V_j$. Then the quotient $(U \oplus V_j)/V_j \cong U$ is an irreducible FG-submodule of $V/V_j \cong \bigoplus_{i \neq j} V_i$, which implies that U is isomorphic to V_h, for some $h \neq j$. Therefore $V_h \cong U \cong V_j$, with $h \neq j$, contradicting the assumption that the V_i's are pairwise nonisomorphic. Hence we must have $U = V_j$. $\square$

Definition 8.1.4. *Let F be a finite field and G be a group. Let V be an irreducible FG-module. Then V is called* **absolutely irreducible** *if* $\mathrm{Hom}_G(V, V) = F$.

Absolutely irreducible modules can be characterized in terms of tensor products.

Definition 8.1.5. *Let F be a finite field and let V and W be vector spaces over F. The* **tensor product** *of V and W over F, denoted by $V \otimes_F W$, is a pair (U, μ), where U is a vector space over F and $\mu \colon V \times W \to U$ is a bilinear map such that for every F-space U' and every bilinear map $\mu' \colon V \times W \to U'$ there exists a unique linear transformation $\phi \colon U \to U'$ such that $\mu' = \mu\phi$. Furthermore, if V and W are FG-modules, then so is $V \otimes_F W$.*

Lemma 8.1.6. ([16, Lemma 2.2, pg. 27]) *Let F be a finite field and G be a group. Denote by $\bar{F}$ the algebraic closure of F and regard $\bar{F}$ as an FG-module with G acting trivially. Suppose that V is an irreducible FG-module. Then V is absolutely irreducible if, and only if, $V_{\bar{F}} = V \otimes_F \bar{F}$ is irreducible as an $\bar{F}G$-module.*

Proposition 8.1.7. *Let F be a finite field and G be a group. Let V be an FG-module and let $H \leqslant G$. If V is absolutely irreducible as an FH-module, then V is absolutely irreducible also as an FG-module.*

Proof. By assumption, V is an irreducible FH-module and so V is irreducible also as an FG-module, since $H \leqslant G$. Moreover, by Lemma 8.1.6, $V_{\bar{F}}$ is an irreducible $\bar{F}H$-module. In particular, $V_{\bar{F}}$ is irreducible as an $\bar{F}G$-module and so V is absolutely irreducible as an FG-module. $\square$

Finally, notice that if V is a vector space over some finite field F and $\dim_F(V) = m$, then V can be regarded as an FG-module, for any permutation group G acting on m points. If $\mathcal{B} = \{v_1, \ldots, v_m\}$ is a basis for V, the action of G will be given by

$$v_i^g = v_{i^g},$$

for all $g \in G$ and for all $i = 1, \ldots, m$. This action will be referred to later as the **natural action** of G on V and G will be said to act on V in the **natural way**.

8.2 Modules invariant under the action of the normalizer

For $r \in \mathbb{N}$, let $G_r = \mathrm{Sym}(\Omega_r)$, with $|\Omega_r| = p^r$ and p prime. Let $T_r \in \mathrm{Syl}_p(G_r)$ and denote by B_r the normalizer of T_r in G_r. Set $F = \mathrm{GF}(q)$, for some $q \neq p$ prime. Suppose that V_r is a vector space over F of dimension p^r. Then V_r can be regarded as an FB_r-module, with B_r acting on it in the natural way. We want to find all irreducible FB_r-submodules of V_r and decompose V_r in terms of those.

Before proceeding further we would like to remind the reader some facts from Sections 5.1 and 5.2 about the structure of B_r and about its action on the set Ω_r.

Following Theorem 5.2.9, denote by Δ_i the unique complete block system of B_r of blocks of length p^i, with $i = 1, \ldots, r-1$. By Lemma 5.1.1, we know that, for $i = 2, \ldots, r-1$, every element of Δ_i is the union of p blocks belonging to Δ_{i-1}. Therefore, if we write $\Omega_r = \{1, \ldots, p^r\}$, we can assume that, for $i = 1, \ldots, r-1$, the blocks belonging to Δ_i have the form

$$\{(j-1)p^i + 1, \ldots, jp^i\},$$

with $j = 1, \ldots, p^{r-i}$. Furthermore, by Corollary 5.2.6, we can factorize B_r in terms of the normalizer B_i of a Sylow p-subgroup of $\mathrm{Sym}(\Delta_{r-i})$ and write

$$B_r = A_{r-i} \rtimes B_i,$$

where A_{r-i} is the base group of B_r with respect to Δ_{r-i} and the elements of Δ_{r-i} are the orbits of A_{r-i} on Ω_r. Similarly, B_i can be factorized as $B_i = A \rtimes B_{i-1}$, with B_{i-1} normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Delta_{r-i+1})$ and A the base group of B_i with respect to Δ_{r-i+1}.

Now let $\mathcal{B} = \{v_1, \ldots, v_{p^r}\}$ be a basis for V_r and define the following submodules of V_r:

$$V_{0,r} = \langle (v_1 + \cdots + v_{p^r})^{B_r} \rangle,$$

$$V_{1,r} = \langle ((v_1 + \cdots + v_{p^{r-1}}) - (v_{p^{r-1}+1} + \cdots + v_{2p^{r-1}}))^{B_r} \rangle,$$

$$\vdots$$

$$V_{r-1,r} = \langle ((v_1 + \cdots + v_p) - (v_{p+1} + \cdots + v_{2p}))^{B_r} \rangle,$$

$$V_{r,r} = \langle (v_1 - v_2)^{B_r} \rangle,$$

where, according to our standard notation, for $v \in V_r$, v^{B_r} is the orbit of B_r containing v.

Lemma 8.2.1. *Let $r \in \mathbb{N}$. Then $V_{0,r}$ has dimension 1 and, for all $i = 1, \ldots, r$, $V_{i,r}$ has dimension $p^{i-1}(p-1)$.*

Proof. Clearly $V_{0,r}$ has dimension 1, since $(v_1 + \cdots + v_{p^r})^{B_r} = \{v_1 + \cdots + v_{p^r}\}$.
Let $i \in \{1, \ldots, r\}$. Then

$$V_{i,r} = \langle ((v_1 + \cdots + v_{p^{r-i}}) - (v_{p^{r-i}+1} + \cdots + v_{2p^{r-i}}))^{B_r} \rangle.$$

For $j = 1, \ldots, p^i$, set $w_j = v_{(j-1)p^{r-i}+1} + \cdots + v_{jp^{r-i}}$. Then $V_{i,r} = \langle (w_1 - w_2)^{B_r} \rangle$ and each w_j corresponds to a block belonging to Δ_{r-i}. Write $B_r = A_{r-i} \rtimes B_i$. Since the elements of Δ_{r-i} are fixed blocks of A_{r-i}, it follows that each w_j is fixed by A_{r-i} and so $V_{i,r} = \langle (w_1 - w_2)^{B_i} \rangle$. Next factorize B_i as $B_i = A \rtimes B_{i-1}$ and partition the set $\{w_1, \ldots, w_{p^i}\}$ in p^{i-1} subsets of size p in the following way:

$$\{w_1, \ldots, w_p\},\ \{w_{p+1}, \ldots, w_{2p}\},\ \ldots,\ \{w_{(p^{i-1}-1)p+1}, \ldots, w_{p^i}\}.$$

Each of these subsets corresponds to a block of Δ_{r-i+1} on which A acts as the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p)$. Therefore

$$\langle (w_1 - w_2)^A \rangle = \langle w_1 - w_2, \ldots, w_{p-1} - w_p \rangle$$

and, since B_{i-1} is transitive on Δ_{r-i+1}, we get that

$$\begin{aligned}\langle (w_1 - w_2)^{B_i} \rangle &= \langle (w_1 - w_2)^{A \rtimes B_{i-1}} \rangle = \langle (w_1 - w_2, \ldots, w_{p-1} - w_p)^{B_{i-1}} \rangle \\ &= \langle w_1 - w_2, \ldots, w_{p-1} - w_p, \ldots, w_{(p^{i-1}-1)p+1} - w_{(p^{i-1}-1)p+2}, \ldots, w_{p^i-1} - w_{p^i} \rangle.\end{aligned}$$

This shows that $\mathcal{B}_i = \{w_j - w_{j+1} \mid j = 1, \ldots, p^i - 1; j \not\equiv 0 \bmod p\}$ is a set of generators for $V_{i,r}$. It remains to prove that the vectors in $\mathcal{B}_i$ are linearly independent. We shall first show that the vectors w_j's, with $j = 1, \ldots, p^i$, are linearly independent.
Suppose that $w_1 = \alpha_2 w_2 + \cdots + \alpha_{p^i} w_{p^i}$, for some $\alpha_2, \ldots, \alpha_{p^i} \in F$. Then

$$v_1 = -v_2 - \cdots - v_{p^{n-1-i}} + \alpha_2 w_2 + \cdots + \alpha_{p^i} w_{p^i}$$

and v_1 would be a linear combination of the v_i's, for $i \neq 1$, contradicting the assumption that $\mathcal{B} = \{v_1, \dots, v_{p^r}\}$ is a basis for V_r. Hence the w_j's are linearly independent.
Now assume that

$$w_1 - w_2 = \sum_{j=2,\ p\not| j}^{p^i - 1} \alpha_j (w_j - w_{j+1}),$$

for some $\alpha_j \in F$. Then

$$w_1 = (\alpha_2 + 1) w_2 + \sum_{j=3,\ p\not| j}^{p^i - 1} (\alpha_j - \alpha_{j-1}) w_j - \sum_{h=1}^{p^{i-1}} \alpha_{hp-1} w_{hp},$$

which is a contradiction, since the vectors $w_1, \dots, w_{p^i}$ are linearly independent. Therefore $\mathcal{B}_i$ is a basis for $V_{i,r}$ and so $\dim(V_{i,r}) = p^{i-1}(p-1)$. $\square$

Lemma 8.2.2. *Suppose that $r = 1$. Then $V_{0,r}$ and $V_{1,r}$ are irreducible FB_r-modules. Furthermore $V_{0,r}$ and $V_{1,r}$ are absolutely irreducible.*

Proof. Let $r = 1$. Then V_r is a vector space of dimension p over F and, by Theorem 5.2.4, $B_r = B_1 \cong \mathrm{Hol}(\mathbb{Z}_p)$. Write $T_1 = \langle x \rangle$ and $B_1 = \langle x, y \rangle = T_1 \rtimes \langle y \rangle$, with x a cycle of length p and y a cycle of length $p - 1$. Consider the submodules

$$\begin{aligned} V_{0,r} &= \langle (v_1 + \cdots + v_p)^{B_1} \rangle = \langle v_1 + \cdots + v_p \rangle, \\ V_{1,r} &= \langle (v_1 - v_2)^{B_1} \rangle = \langle v_1 - v_2, \dots, v_{p-1} - v_p \rangle, \end{aligned}$$

where $\mathcal{B} = \{v_1, \dots, v_p\}$ is a basis for V_r which is permuted in the natural way by B_1.
We want to show that $V_{0,r}$ and $V_{1,r}$ are irreducible FB_1-submodules of V_r.
Let $\bar{F}$ be the algebraic closure of F. Then both $\bar{F}$ and V_r are vector spaces over F and we can form the tensor product

$$\bar{V}_r = V_r \otimes_F \bar{F}.$$

Then $\bar{V}_r$ is a vector space over $\bar{F}$ and $\dim_{\bar{F}}(\bar{V}_r) = \dim_F(V_r) = p$, a basis being given by the set $\bar{\mathcal{B}} = \{v_1 \otimes 1, \dots, v_p \otimes 1\}$. Moreover $\bar{V}_r$ is an $\bar{F}B_1$-module and, by restriction, an $\bar{F}T_1$-module. More generally, for any FB_1-submodule U of V_r, $U \otimes_F \bar{F}$ is an $\bar{F}B_1$-submodule of $\bar{V}_r$ such that $\dim_{\bar{F}}(\bar{U}) = \dim_F(U)$.
Regard $\bar{V}_r$ as an $\bar{F}T_1$-module. As $q \neq p$ and T_1 is a p-group, Maschke's Theorem ([9, 10.8])

implies that $\bar{V}_r$ is completely reducible.

Now T_1 is a transitive permutation group of order p acting on p points and so, by Proposition 2.1.10, T_1 is regular. Therefore $\bar{V}_r$ is the $\bar{F}T_1$-module corresponding to the regular representation of T_1 over $\bar{F}$. This implies, in particular, that every irreducible $\bar{F}T_1$-submodule must appear in the decomposition of $\bar{V}_r$ (see [37, 1.1 pg. 261]). But, since $\bar{F}$ is algebraically closed and $\mathrm{char}(\bar{F}) = q$ is coprime to $|T_1| = p$, [9, 27.22] implies that there are p equivalence classes of irreducible $\bar{F}T_1$-submodules of $\bar{V}_r$. Hence, since $\dim_{\bar{F}}(\bar{V}_r) = p$, the decomposition of $\bar{V}_r$ contains one and only one irreducible $\bar{F}T_1$-submodule for each equivalence class and all irreducible $\bar{F}T_1$-submodules of $\bar{V}_r$ have dimension 1. So we can write

$$\bar{V}_r = \bar{U}_{0,r} \oplus \cdots \oplus \bar{U}_{p-1,r},$$

where, for all $i, j = 0, \ldots, p-1$, $i \neq j$, $\bar{U}_{i,r}$ is an irreducible $\bar{F}T_1$-submodule of $\bar{V}_r$, $\dim(\bar{U}_{i,r}) = 1$ and $\bar{U}_{i,r} \not\cong \bar{U}_{j,r}$. Furthermore, by Lemma 8.1.3, the $\bar{U}_{i,r}$'s are the only irreducible $\bar{F}T_1$-submodules of $\bar{V}_r$, that is, each equivalence class has order 1 and the decomposition of $\bar{V}_r$ given above is unique.

Now regard $\bar{V}_r$ as an $\bar{F}B_1$-module. Since $\bar{U}_{i,r}$ is an $\bar{F}T_1$-submodule and $T_1 \trianglelefteq B_1$, for $x \in T_1$ and $y \in B_1$, we have that

$$(\bar{U}_{i,r}y)x = (\bar{U}_{i,r}yxy^{-1})y = (\bar{U}_{i,r}x^{y^{-1}})y = \bar{U}_{i,r}y,$$

which shows that $\bar{U}_{i,r}y$ is also an $\bar{F}T_1$-submodule. But $\bar{U}_{i,r}y$ is irreducible as $\bar{F}T_1$-submodule, since so is $\bar{U}_{i,r}$. Hence, since the $\bar{U}_{i,r}$'s are the only irreducible $\bar{F}T_1$-submodules of $\bar{V}_r$, we must have $\bar{U}_{i,r}y = \bar{U}_{j,r}$, for some $j = 0, \ldots, p-1$, and thus B_1 acts on the set $\{\bar{U}_{0,r}, \ldots, \bar{U}_{p-1,r}\}$.

We now want to determine the orbits of B_1 on $\{\bar{U}_{0,r}, \ldots, \bar{U}_{p-1,r}\}$.

For $i = 0, \ldots, p-1$, let ρ_i be the representation afforded by $\bar{U}_{i,r}$. Since T_1 acts on $\bar{V}_r$ via the regular representation, we can take ρ_i to be the right regular representation defined by

$$\rho_i \colon x \in T_1 \longmapsto \omega^i \in \mathrm{GL}_1(\bar{F}),$$

where $T_1 = \langle x \rangle$ and ω is a p-th root of unity. This tells us how T_1 acts on each $\bar{U}_{i,r}$.

Let $y \in B_1$ such that $B_1 = \langle x, y \rangle$ and let $\alpha \in \mathbb{N}$ such that $x^\alpha = x^{y^{-1}}$. To determine what $\bar{U}_{i,r}y$ is we study the action of T_1 on it.

We start with $\bar{U}_{0,r}$:

$$(\bar{U}_{0,r}y)x = (\bar{U}_{0,r}yxy^{-1})y = (\bar{U}_{0,r}x^{y^{-1}})y = (\rho_0(x^{y^{-1}})\bar{U}_{0,r})y$$
$$= (1\bar{U}_{0,r})y = \bar{U}_{0,r}y = \rho_0(x)(\bar{U}_{0,r}y).$$

This says that T_1 is acting on $\bar{U}_{0,r}y$ via ρ_0, that is, $\bar{U}_{0,r}y = \bar{U}_{0,r}$, since $\bar{U}_{0,r}$ is the submodule corresponding to the representation ρ_0. Therefore $\{\bar{U}_{0,r}\}$ is an orbit for B_1.

Next we consider $\bar{U}_{1,r}$:

$$(\bar{U}_{1,r}y)x = (\bar{U}_{1,r}yxy^{-1})y = (\bar{U}_{1,r}x^{y^{-1}})y = (\bar{U}_{1,r}x^{\alpha})y = (\rho_1(x^{\alpha})\bar{U}_{1,r})y$$
$$= (\rho_1(x)^{\alpha}\bar{U}_{1,r})y = (\omega^{\alpha}\bar{U}_{1,r})y = \rho_{\alpha}(x)(\bar{U}_{1,r}y).$$

This means that T_1 is acting on $\bar{U}_{1,r}y$ via ρ_α and so $\bar{U}_{1,r}y = \bar{U}_{\alpha,r}$. But $\langle y\rangle$ is transitive on $\{x, x^2, \ldots, x^{p-1}\}$ in its action by conjugation and so

$$\{\bar{U}_{1,r}z \mid z \in B_1\} = \{\bar{U}_{1,r}y^e \mid e = 1, \ldots, p-1\} = \{\bar{U}_{1,r}, \ldots, \bar{U}_{p-1,r}\}.$$

Hence B_1 has two orbits on $\{\bar{U}_{0,r}, \ldots, \bar{U}_{p-1,r}\}$ and they are $\{\bar{U}_{0,r}\}$ and $\{\bar{U}_{1,r}, \ldots, \bar{U}_{p-1,r}\}$. This implies that $\bar{U}_{0,r}$ and $\bar{U}_{1,r} \oplus \cdots \oplus \bar{U}_{p-1,r}$ are $\bar{F}B_1$-submodules of $\bar{V}_r$.

Now $\bar{U}_{0,r}$ has dimension 1 and so $\bar{U}_{0,r}$ is irreducible. Let $\bar{U}$ be an $\bar{F}B_1$-submodule of $\bar{U}_{1,r} \oplus \cdots \oplus \bar{U}_{p-1,r}$. In particular, $\bar{U}$ is an $\bar{F}T_1$-submodule and so $\bar{U}$ is a direct sum of some of $\bar{U}_{1,r}, \ldots, \bar{U}_{p-1,r}$. But, being an $\bar{F}B_1$-submodule, if $\bar{U}$ contains one of $\bar{U}_{1,r}, \ldots, \bar{U}_{p-1,r}$, then it must contain them all, since they are in the same B_1-orbit. Hence $\bar{U} = \bar{U}_{1,r} \oplus \cdots \oplus \bar{U}_{p-1,r}$ and $\bar{U}_{1,r} \oplus \cdots \oplus \bar{U}_{p-1,r}$ is an irreducible $\bar{F}B_1$-submodule.

Set $\bar{V}_{0,r} = \bar{U}_{0,r}$ and $\bar{V}_{1,r} = \bar{U}_{1,r} \oplus \cdots \oplus \bar{U}_{p-1,r}$. Then $\bar{V}_r = \bar{V}_{0,r} \oplus \bar{V}_{1,r}$, with $\dim(\bar{V}_{0,r}) = 1$ and $\dim(\bar{V}_{1,r}) = p-1$ and $\bar{V}_{0,r}, \bar{V}_{1,r}$ irreducible $\bar{F}B_1$-submodules of $\bar{V}_r$.

We now want to switch back to the vector space V_r we started with and show that the submodules $V_{0,r}$ and $V_{1,r}$, introduced at the beginning of the proof, are irreducible. Since $\dim(V_{0,r}) = 1$, we only need to show that $V_{1,r}$ is irreducible.

Let $R \neq \{0\}$ be a proper FB_1-submodule of $V_{1,r}$. Then, by considering the dimensions, $R \otimes_F \bar{F}$ is a proper nontrivial $\bar{F}B_1$-submodule of $\bar{V}_{1,r}$, which is a contradiction, since $\bar{V}_{1,r}$ is an irreducible $\bar{F}B_1$-module. Hence $V_{1,r}$ is irreducible.

Moreover, by looking at the dimensions, we must have $\bar{V}_{0,r} = V_{0,r} \otimes_F \bar{F}$ and $\bar{V}_{1,r} = V_{1,r} \otimes_F \bar{F}$, with $\bar{V}_{0,r}$ and $\bar{V}_{1,r}$ irreducible $\bar{F}B_1$-submodules. Therefore, by Lemma 8.1.6, $V_{0,r}$ and $V_{1,r}$ are absolutely irreducible as FB_1-modules. $\square$

Lemma 8.2.3. *Let $r \in \mathbb{N}$. Then, for all $i = 0, \dots, r$, $V_{i,r}$ is an irreducible FB_r-submodule of V_r. Furthermore each $V_{i,r}$ is absolutely irreducible.*

Proof. We shall proceed by induction on r, with $r \geq 1$. For $r = 1$ the result follows from Lemma 8.2.2. So assume that $r > 1$. The induction hypothesis can be formulated as follows.

Induction hypothesis: let V' be a vector space over F of dimension p^{r-1} and let $\mathcal{B}' = \{v'_1, \dots, v'_{p^{r-1}}\}$ be a basis for V'. Consider the natural action of B_{r-1} on V', with B_{r-1} the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^{r-1})$. Then, for $i \in \{0, \dots, r-1\}$, the submodules

$$V'_i = \langle ((v'_1 + \cdots + v'_{p^{r-1-i}}) - (v'_{p^{r-1-i}+1} + \cdots + v'_{2p^{r-1-i}}))^{B_{r-1}} \rangle$$

are absolutely irreducible FB_{r-1}-submodules of V'.

Write B_r as $B_r = A_1 \rtimes B_{r-1}$, with A_1 the base group of B_r with respect to Δ_1. First we consider the submodules $V_{0,r}, V_{1,r}, \dots, V_{r-1,r}$. For $j = 1, \dots, p^{r-1}$ set $w_j = v_{(j-1)p+1} + \cdots + v_{jp}$ and $W = \langle w_1, \dots, w_{p^{r-1}} \rangle$. Then each w_j corresponds to an element of Δ_1 and so, since Δ_1 is a complete block system of B_{r-1}, W is an FB_{r-1}-module of dimension p^{r-1}. Also, since the elements of Δ_1 are the orbits of A_1 on Ω_r, we have that the w_j's are fixed by A_1 and so

$$V_{i,r} = \langle ((w_1 + \cdots + w_{p^{r-1-i}}) - (w_{p^{r-1-i}+1} + \cdots + w_{2p^{r-1-i}}))^{B_{r-1}} \rangle,$$

for all $i = 0, \dots, r-1$. Therefore, by the induction hypothesis, the $V_{i,r}$'s are absolutely irreducible as FB_{r-1}-submodules of W and so, by Proposition 8.1.7, they are absolutely irreducible, and so irreducible, also as FB_r-submodules of V_r.
Next we need to look at the submodule $V_{r,r}$. Recall that $V_{r,r} = \langle (v_1 - v_2)^{B_r} \rangle$ and $\dim(V_{r,r}) = p^{r-1}(p-1)$. Regard $V_{r,r}$ as an FA_1-module and, for $i = 1, \dots, p^{r-1}$, define the submodule

$$U_i = \langle (v_{(i-1)p+1})^{A_1} \rangle = \langle v_{(i-1)p+1}, \dots, v_{ip} \rangle.$$

So $\dim(U_i) = p$. Also, for $i = 1, \dots, p^{r-1}$, define

$$R_i = \langle (v_{(i-1)p+1} - v_{(i-1)p+2})^{A_1} \rangle = \langle v_{(i-1)p+1} - v_{(i-1)p+2}, \dots, v_{ip-1} - v_{ip} \rangle.$$

Then R_i is an FA_1-submodule of U_i of dimension $p-1$ over F. Moreover, A_1 acts on R_i and U_i in the natural way as the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p)$. Therefore Lemma 8.2.2

implies that R_i is an absolutely irreducible FA_1-submodule of U_i, for all $i = 1, \ldots, p^{r-1}$. This implies, in particular, that $R_i \cap R_j = \{0\}$, for all $i \neq j$, and so, by considering dimensions, we get that

$$V_{r,r} = R_1 \oplus \cdots \oplus R_{p^{r-1}}$$

and $V_{r,r}$ is completely reducible as an FA_1-module. Also $R_i \ncong R_j$, for $i \neq j$, since they have different centralizers. Hence, by Lemma 8.1.3, the R_i's are the only irreducible FA_1-submodules of $V_{r,r}$.

Now let U be an FB_r-submodule of $V_{r,r}$. In particular, U is an FA_1-submodule and so it must be a direct sum of some of the R_i's. But B_r is transitive on $\{R_1, \ldots, R_{p^{r-1}}\}$, because so is B_{r-1}. So, since U is an FB_r-submodule, if U contains one of the R_i's, then it must contain them all. Hence $U = V_{r,r}$ and $V_{r,r}$ is an irreducible FB_r-submodule of V_r.

Furthermore, since the R_i's are absolutely irreducible as FA_1-modules, we have that the modules $\bar{R}_i = R_i \otimes_F \bar{F}$ are irreducible $\bar{F}A_1$-submodules of $\bar{V}_{r,r} = V_{r,r} \otimes_F \bar{F}$ and $\bar{V}_{r,r} = \bar{R}_1 \oplus \cdots \oplus \bar{R}_{p^{r-1}}$. Thus, using the same argument as before with $\bar{V}_{r,r}$ in place of $V_{r,r}$, we get that $\bar{V}_{r,r}$ is an irreducible $\bar{F}B_r$-module, that is, $V_{r,r}$ is absolutely irreducible as an FB_r-module. □

Lemma 8.2.4. *Let $r \in \mathbb{N}$. Then, for $i, j = 0, \ldots, r$ and $i \neq j$, the following hold:*

(i) *$V_{i,r} \ncong V_{j,r}$, as FB_r-modules;*

(ii) *$V_{i,r} \cap V_{j,r} = \{0\}$.*

Proof. Let $r \in \mathbb{N}$ and let $i, j = 0, \ldots, r$. If $i \neq j$, then, by Lemma 8.2.1, $V_{i,r}$ and $V_{j,r}$ have different dimensions over F and so $V_{i,r}$ and $V_{j,r}$ are not isomorphic. Furthermore, $V_{i,r} \cap V_{j,r}$ is an FB_r-submodule of both $V_{i,r}$ and $V_{j,r}$. But, by Lemma 8.2.3, $V_{i,r}$ and $V_{j,r}$ are irreducible FB_r-modules. Hence $V_{i,r} \cap V_{j,r} = \{0\}$. □

Theorem 8.2.5. *Let $r \in \mathbb{N}$. Then V_r is completely reducible as an FB_r-module. In particular, $V_r = V_{0,r} \oplus \cdots \oplus V_{r,r}$ and the $V_{i,r}$'s are the only irreducible FB_r-submodules of V_r.*

Proof. By Lemmas 8.2.1 and 8.2.4 (ii), $V_{0,r} + \cdots + V_{n-1,r} = V_{0,r} \oplus \cdots \oplus V_{n-1,r}$ is a submodule of V_r of dimension

$$1 + p - 1 + p(p-1) + \cdots + p^{r-1}(p-1) = p^r.$$

Hence $V_r = V_{0,r} \oplus \cdots \oplus V_{n-1,r}$, where, by Lemma 8.2.3, each $V_{i,r}$ is an irreducible FB_r-module. So V_r is completely reducible. Also, by Lemma 8.2.4 (i), the $V_{i,r}$'s are pairwise nonisomorphic and so, by Lemma 8.1.3, it follows that the $V_{i,r}$'s are the only irreducible FB_r-submodules of V_r. $\square$

Chapter 9

G-subgroups of homocyclic q-groups of finite exponent

Let q be a prime and let A be a homocyclic q-group of finite exponent. We shall illustrate various properties related to A, the final aim being to determine, for some $G \leqslant \mathrm{Aut}(A)$ such that $A/\Phi(A)$ is an absolutely irreducible $\mathrm{GF}(q)G$-module, the number and the structure of all G-subgroups R of the direct sum of t copies of A such that R is G-isomorphic to a nontrivial quotient of A. As we shall see in Chapter 10, such subgroups are closely related to some minimal parabolic subgroups of $\mathrm{Sym}(p^n)$.

9.1 G-homomorphisms of A

Let A be an abelian q-group of finite exponent, for some prime q, and write A additively. Denote by $\Omega_1(A)$ the set $\{a \in A \mid qa = 0\}$. Recall that $\mathrm{Hom}(A/\Phi(A), \Omega_1(A))$ is a group with respect to addition, with $\Phi(A) = qA$ the Frattini subgroup of A and $A/\Phi(A) \cong \Omega_1(A)$.
The following lemma tells us how to define an action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}(A/\Phi(A), \Omega_1(A))$.

Lemma 9.1.1. *Let A be an abelian q-group of finite exponent. Then* $\mathrm{Hom}(A/\Phi(A), \Omega_1(A))$ *is an* $\mathrm{Aut}(A)$*-group, where, for $\alpha \in \mathrm{Hom}(A/\Phi(A), \Omega_1(A))$ and $h \in \mathrm{Aut}(A)$, α^h is defined by*

$$\alpha^h(a + \Phi(A)) = h^{-1}(\alpha(h(a) + \Phi(A))),$$

for all $a \in A$.

Proof. Let A be an abelian q-group of finite exponent and $H = \mathrm{Aut}(A)$. Set $F = \Phi(A)$ and $E = \Omega_1(A)$. For $\alpha \in \mathrm{Hom}(A/F, E)$ and $h \in H$ define $\alpha^h \colon A/F \to E$ by

$$\alpha^h(a+F) = h^{-1}(\alpha(h(a)+F)),$$

for all $a \in A$. First, α^h is well-defined. In fact, let $a, b \in A$ such that $a + F = b + F$. Then $a - b \in F$, which implies that $h(a-b) = h(a) - h(b) \in F$, since F is a characteristic subgroup of A. Therefore $h(a) + F = h(b) + F$ and so $h^{-1}(\alpha(h(a)+F)) = h^{-1}(\alpha(h(b)+F))$, that is, $\alpha^h(a+F) = \alpha^h(b+F)$.
Also, $\alpha^h \in \mathrm{Hom}(A/F, E)$. For, if $a, b \in A$, then

$$\begin{aligned}\alpha^h(a+b+F) &= h^{-1}(\alpha(h(a+b)+F)) = h^{-1}(\alpha(h(a)+h(b)+F))\\ &= h^{-1}(\alpha(h(a)+F)+\alpha(h(b)+F)) = h^{-1}(\alpha(h(a)+F)) + h^{-1}(\alpha(h(b)+F))\\ &= \alpha^h(a+F) + \alpha^h(b+F).\end{aligned}$$

Next we need to show that, for $h, h_1, h_2 \in H$ and $\alpha, \beta \in \mathrm{Hom}(A/F, E)$, $\alpha^{h_1h_2} = (\alpha^{h_1})^{h_2}$ and $(\alpha+\beta)^h = \alpha^h + \beta^h$. So let $a \in A$. Then

$$\begin{aligned}\alpha^{h_1h_2}(a+F) &= (h_1h_2)^{-1}(\alpha((h_1h_2)(a)+F)) = h_2^{-1}(h_1^{-1}(\alpha(h_1(h_2(a))+F))\\ &= h_2^{-1}(\alpha^{h_1}(h_2(a)+F)) = (\alpha^{h_1})^{h_2}(a+F).\end{aligned}$$

Hence $\alpha^{h_1h_2} = (\alpha^{h_1})^{h_2}$. Moreover,

$$\begin{aligned}(\alpha+\beta)^h(a+F) &= h^{-1}((\alpha+\beta)(h(a)+F)) = h^{-1}(\alpha(h(a)+F)+\beta(h(a)+F))\\ &= h^{-1}(\alpha(h(a)+F)) + h^{-1}(\beta(h(a)+F)) = \alpha^h(a+F) + \beta^h(a+F)\\ &= (\alpha^h + \beta^h)(a+F).\end{aligned}$$

Therefore $(\alpha+\beta)^h = \alpha^h + \beta^h$ and we have defined an action of H on $\mathrm{Hom}(A/F, E)$. ☐

Define the map

$$\psi \colon \sigma \in \mathrm{Aut}(A) \longmapsto \sigma_{|\Phi(A)} \in \mathrm{Aut}(\Phi(A)).$$

Recall that, since $\Phi(A)$ is a characteristic subgroup of A, $\sigma_{|\Phi(A)}$ is an element of $\mathrm{Aut}(\Phi(A))$. Also, for $\sigma, \tau \in \mathrm{Aut}(A)$, we have that $(\sigma\tau)_{|\Phi(A)} = (\sigma_{|\Phi(A)})(\tau_{|\Phi(A)})$ and so ψ is a homomorphism. We are interested in the kernel of ψ.

Theorem 9.1.2. *Let A be an abelian q-group of finite exponent such that $\Omega_1(A) \subseteq \Phi(A)$. Consider the homomorphism ψ defined by*

$$\psi\colon \sigma \in \mathrm{Aut}(A) \longmapsto \sigma_{|\Phi(A)} \in \mathrm{Aut}(\Phi(A)).$$

Then the groups $\ker\psi$ *and* $\mathrm{Hom}(A/\Phi(A), \Omega_1(A))$ *are isomorphic as* $\mathrm{Aut}(A)$*-groups.*

Proof. Set $F = \Phi(A)$ and $E = \Omega_1(A)$. Let $H = \mathrm{Aut}(A)$ and

$$K = \ker\psi = \{h \in H \mid h_{|F} = id_{|F}\}.$$

Then $K \trianglelefteq H$ and, by Lemma 9.1.1, $\mathrm{Hom}(A/F, E)$ can be regarded as a H-group.
For an element $k \in K$, define the map $1-k$ from A/F to A by setting

$$(1-k)(a+F) = a - k(a),$$

for all $a \in A$. First,

$$q(a - k(a)) = qa - qk(a) = qa - k(qa) = qa - qa = 0,$$

since $qa \in F$ and $k_{|F} = id_{|F}$. So $a - k(a) \in E$ and $1-k$ is indeed a map from A/F to E.
Furthermore, let $a, b \in A$ such that $a + F = b + F$. Then $a = b + x$, for some $x \in F$, and so

$$\begin{aligned}(1-k)(a+F) &= a - k(a) = b + x - k(b+x) = b - k(b) + x - k(x)\\ &= b - k(b) + x - x = b - k(b) = (1-k)(b+F),\end{aligned}$$

since $x \in F$ and $k \in K$. Therefore $1-k$ is well-defined.
Next, we want to show that $1-k \in \mathrm{Hom}(A/F, E)$. So let $a, b \in A$. Then

$$\begin{aligned}(1-k)(a+b+F) &= a + b - k(a+b) = a + b - k(a) - k(b)\\ &= (1-k)(a+F) + (1-k)(b+F).\end{aligned}$$

Thus we have a map

$$\pi\colon K \longrightarrow \mathrm{Hom}(A/F, E),$$

defined by

$$\pi\colon k \longmapsto 1-k.$$

We shall prove that π is a H-isomorphism between K and $\mathrm{Hom}(A/F, E)$.

First, let $k_1, k_2 \in K$ such that $1 - k_1 = 1 - k_2$. Then, for all $a \in A$, $a - k_1(a) = a - k_2(a)$, that is, $k_1(a) = k_2(a)$. Hence $k_1 = k_2$ and π is one-to-one.

We shall now show that π is onto. For $\beta \in \mathrm{Hom}(A/F, E)$, define $k_\beta \colon A \to A$ by setting $k_\beta(a) = a - \beta(a + F)$, for all $a \in A$. Then $k_\beta \in \mathrm{Hom}(A, A)$, since, for all $a, b \in A$,

$$k_\beta(a + b) = a + b - \beta(a + b + F) = a + b - \beta(a + F) - \beta(b + F) = k_\beta(a) + k_\beta(b).$$

Next we shall see that k_β is one-to-one and so, since A is finite, it will follow that $k_\beta \in \mathrm{Aut}(A)$. Suppose that $k_\beta(a) = a - \beta(a + F) = 0$. Then $a = \beta(a + F) \in E \leqslant F$ and $a + F = F$. Hence

$$0 = k_\beta(a) = a - \beta(a + F) = a - \beta(F) = a - 0 = a.$$

Moreover, if $a \in F$, then $\beta(a + F) = \beta(F) = 0$ and $k_\beta(a) = a - \beta(a + F) = a$. Therefore $(k_\beta)_{|F} = id_{|F}$ and $k_\beta \in K$. Finally, we need to show that $\beta = \pi(k_\beta)$. So let $a \in A$. Then

$$(1 - k_\beta)(a + F) = a - k_\beta(a) = a - (a - \beta(a + F)) = \beta(a + F).$$

Hence $\beta = 1 - k_\beta = \pi(k_\beta)$ and π is a bijection.

Now recall that K is a group with respect to multiplication, whereas $\mathrm{Hom}(A/F, E)$ is a group with respect to addition. Thus, for $k_1, k_2 \in K$, we need to show that $\pi(k_1 k_2) = \pi(k_1) + \pi(k_2)$. Let $a \in A$. Then

$$\begin{aligned}
\pi(k_1 k_2)(a + F) &= (1 - k_1 k_2)(a + F) = a - (k_1 k_2)(a) \\
&= a - k_1(k_2(a)) + k_1(a) - k_1(a) = a - k_1(a) + k_1(a - k_2(a)) \\
&= a - k_1(a) + a - k_2(a) = (1 - k_1)(a + F) + (1 - k_2)(a + F) \\
&= \pi(k_1)(a + F) + \pi(k_2)(a + F) = (\pi(k_1) + \pi(k_2))(a + F),
\end{aligned}$$

since $a - k_2(a) \in E \leqslant F$ and $(k_1)_{|F} = id_{|F}$.

Last, we have to prove that π preserves the action of H. Let $h \in H$, $k \in K$ and $a \in A$. Then

$$\begin{aligned}
\pi(k)^h(a + F) &= h^{-1}(\pi(k)(h(a) + F)) = h^{-1}((1 - k)(h(a) + F)) \\
&= h^{-1}(h(a) - k(h(a))) = h^{-1}(h(a)) - h^{-1}(k(h(a))) \\
&= a - k^h(a) = (1 - k^h)(a + F) = \pi(k^h)(a + F).
\end{aligned}$$

We can at last conclude that the H-groups K and $\mathrm{Hom}(A/F, E)$ are isomorphic via the map π.

□

Corollary 9.1.3. *Let A be an abelian q-group of finite exponent such that $\Omega_1(A) \subseteq \Phi(A)$. Suppose that $G \leqslant \mathrm{Aut}(A)$ and let ψ_G be the homomorphism defined by*

$$\psi_G \colon \sigma \in \mathrm{Aut}_G(A) \longmapsto \sigma_{|\Phi(A)} \in \mathrm{Aut}_G(\Phi(A)).$$

Then the groups $\ker \psi_G$ *and* $\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))$ *are G-isomorphic.*

Proof. Set $F = \Phi(A)$ and $E = \Omega_1(A)$. Let $K = \ker \psi = \{\sigma \in \mathrm{Aut}(A) \mid \sigma_{|F} = id_{|F}\}$, with ψ defined as in Theorem 9.1.2. Then

$$C_K(G) = \{k \in K \mid gk = kg, \text{ for all } g \in G\} = \{\sigma \in \mathrm{Aut}_G(A) \mid \sigma_{|F} = id_{|F}\} = \ker \psi_G.$$

Similarly, $C_{\mathrm{Hom}(A/F,E)}(G) = \mathrm{Hom}_G(A/F, E)$. But, by Theorem 9.1.2, $K \cong \mathrm{Hom}(A/F, E)$ as $\mathrm{Aut}(A)$-groups. Therefore $\ker \psi_G$ and $\mathrm{Hom}_G(A/F, E)$ are isomorphic as G-groups, with G acting trivially on them. $\square$

Corollary 9.1.4. *Let A be an abelian q-group of finite exponent such that $\Omega_1(A) \subseteq \Phi(A)$. Suppose that $G \leqslant \mathrm{Aut}(A)$. Then*

$$|\mathrm{Aut}_G(A)| \leq |\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))||\mathrm{Aut}_G(\Phi(A))|.$$

Proof. Consider the homomorphism ψ_G defined in Corollary 9.1.3. Then, by the homomorphism Theorem, $|\mathrm{Aut}_G(A)| \leq |\ker \psi_G||\mathrm{Aut}_G(\Phi(A)))|$. But, by Corollary 9.1.3, $\ker \psi_G$ is isomorphic to $\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))$ and so we have the result. $\square$

Proposition 9.1.5. *Let A be an abelian q-group of exponent q^n and let $G \leqslant \mathrm{Aut}(A)$. Then*

$$|\mathrm{Aut}_G(A)| \geq q^{n-1}(q-1).$$

Proof. Set $Z = \mathbb{Z}_{q^n}$. By assumption, A is the direct sum of some, say d, cyclic groups of order q^e, with $1 \leq e \leq n$, of which at least one has order q^n. We shall regard the elements of A as d-ples of elements of Z, that is, $A \subseteq Z^d$. Thus at least one direct summand of A equals Z. For $\alpha \in \mathrm{Aut}(Z)$ define the map $\hat{\alpha} \colon A \to A$ by

$$\hat{\alpha} \colon (z_1, \ldots, z_d) \longmapsto (\alpha(z_1), \ldots, \alpha(z_d)).$$

Then $\hat{\alpha}$ is clearly a homomorphism of A and is one-to-one, since so is α. Hence $\hat{\alpha} \in \mathrm{Aut}(A)$. Furthermore, by [24, 1.5.5], every element $\alpha \in \mathrm{Aut}(Z)$ is of the form $z \mapsto kz$, with $1 \leq k < q^n$

and $(k,q)=1$. Hence $\hat{\alpha}$ acts like

$$\hat{\alpha}\colon (z_1,\dots,z_d) \longmapsto (kz_1,\dots,kz_d)$$

and, in particular, $\hat{\alpha}$ commutes with the action of G, that is, $\hat{\alpha} \in \mathrm{Aut}_G(A)$.

Now consider the map that takes α to $\hat{\alpha}$. This is clearly a homomorphism and, as we shall see, is also one-to-one. In fact, let $\alpha_1,\alpha_2 \in \mathrm{Aut}(Z)$ such that $\hat{\alpha}_1=\hat{\alpha}_2$. Let z be a generator of Z. Then, up to changing the order of the direct summands of A, the d-ple having z as its first coordinate and 0 elsewhere is an element of A, since at least one of the direct summands of A is equal to Z. Then $\hat{\alpha}_1(z,0,\dots,0)=\hat{\alpha}_2(z,0,\dots,0)$ and, in particular, $\alpha_1(z)=\alpha_2(z)$. Hence, since α_1 and α_2 coincide on a generator, α_1 and α_2 are the same on the whole of Z and so $\alpha_1=\alpha_2$.

Therefore the map $\alpha \mapsto \hat{\alpha}$ is an embedding of $\mathrm{Aut}(Z)$ in $\mathrm{Aut}_G(A)$, which implies that

$$|\mathrm{Aut}_G(A)| \geq |\mathrm{Aut}(Z)| = q^{n-1}(q-1),$$

where the latter equality follows from [24, 1.5.5]. □

In the next result, though written additively, A will be any group, not necessarily abelian. We shall also write $K \leqslant_G A$, if K is a G-subgroup of A, and denote by $\mathrm{Isom}_G(A/K,L)$ the group of all G-isomorphisms from A/K to a G-subgroup L of A.

Proposition 9.1.6. *Let A be a group and let $G \leqslant \mathrm{Aut}(A)$. Denote by Γ the set of all pairs (K,L), such that $K,L \leqslant_G A$, $K \trianglelefteq A$ and L is G-isomorphic to a quotient of A. Then there exists a bijection between the set $\mathrm{Hom}_G(A,A)$ and the disjoint union of the sets $\mathrm{Isom}_G(A/K,L)$, for $(K,L)\in\Gamma$.*

Proof. Set Θ to be the disjoint union of the sets $\mathrm{Isom}_G(A/K,L)$, with $(K,L)\in\Gamma$. Let $\alpha \in \mathrm{Hom}_G(A,A)$ and let $\bar{\alpha}$ be the homomorphism from $A/\ker\alpha$ to A determined by α, that is,

$$\begin{aligned}\bar{\alpha}\colon A/\ker\alpha &\longrightarrow A\\ a+\ker\alpha &\longmapsto \alpha(a).\end{aligned}$$

Then $\bar{\alpha} \in \mathrm{Isom}_G(A/\ker\alpha,\alpha(A))$ and, of course, $(\ker\alpha,\alpha(A))\in\Gamma$. Therefore $\bar{\alpha}\in\Theta$ and we can define the map

$$\kappa\colon \alpha\in\mathrm{Hom}_G(A,A) \longmapsto \bar{\alpha}\in\Theta,$$

which we shall prove to be a bijection.

Let $\alpha, \beta \in \mathrm{Hom}_G(A, A)$ such that $\bar{\alpha} = \bar{\beta}$. Then, in particular, $\ker \alpha = K = \ker \beta$ and

$$\alpha(a) = \bar{\alpha}(a + K) = \bar{\beta}(a + K) = \beta(a),$$

for all $a \in A$. So $\alpha = \beta$ and κ is one-to-one.

Now, let $\hat{\beta} \in \mathrm{Isom}_G(A/K, L)$, for some $(K, L) \in \Gamma$. Define the map $\beta\colon A \to A$ by

$$\beta\colon a \longmapsto \hat{\beta}(a + K) \in L \leqslant A.$$

Then, for $a, b \in A$,

$$\beta(a + b) = \hat{\beta}(a + b + K) = \hat{\beta}(a + K) + \hat{\beta}(b + K) = \beta(a) + \beta(b),$$

and so $\beta \in \mathrm{Hom}(A, A)$. Also, for $g \in G$,

$$\beta(a^g) = \hat{\beta}(a^g + K) = \hat{\beta}((a + K)^g) = \hat{\beta}(a + K)^g = \beta(a)^g,$$

and $\beta \in \mathrm{Hom}_G(A, A)$. Furthermore, since $\hat{\beta}$ is one-to-one, we have that

$$\ker \beta = \{a \in A \mid \beta(a) = 0\} = \{a \in A \mid \hat{\beta}(a + K) = 0\} = \{a \in A \mid a + K = K\} = K,$$

and, since $\hat{\beta}$ is onto, we also have that

$$\mathrm{Im}\beta = \{\beta(a) \mid a \in A\} = \{\hat{\beta}(a + K) \mid a \in A\} = \mathrm{Im}\hat{\beta} = L.$$

This shows that $\kappa(\beta) = \hat{\beta}$ and so that the map κ is onto. Hence κ is a bijection from $\mathrm{Hom}_G(A, A)$ to Θ. $\square$

Corollary 9.1.7. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is an irreducible* $\mathrm{GF}(q)G$*-module. Then*

$$|\mathrm{Hom}_G(A, A)| = \sum_{e=0}^{n} |\mathrm{Aut}_G(A/\Phi^e(A))|.$$

Proof. By Proposition 1.3.11, every G-subgroup L of A is G-isomorphic to a quotient of A. Also, for $e = 0, \ldots, n$, there is a unique G-subgroup of A having exponent q^e, namely, $\Phi^{n-e}(A)$. Therefore, for $\alpha \in \mathrm{Hom}_G(A, A)$, $\ker \alpha$ determines uniquely $\alpha(A)$ and so the set Γ defined in Proposition 9.1.6 can be replaced by the set

$$\{K \mid K \leqslant_G A\} = \{\Phi^e(A) \mid e = 0, \ldots, n\}.$$

Then the result follows from Proposition 9.1.6. $\square$

Proposition 9.1.8. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)G$-module. Then*

(i) $|\mathrm{Aut}_G(A)| = q^{n-1}(q-1)$*; and*

(ii) $|\mathrm{Hom}_G(A, A)| = q^n$.

Proof. (i) By Corollary 9.1.4, we have that

$$|\mathrm{Aut}_G(A)| \leq |\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))||\mathrm{Aut}_G(\Phi(A))|.$$

Since A is homocyclic, by Proposition 1.3.7, $\Omega_1(A) = \Phi^{n-1}(A) \subseteq \Phi^e(A)$, for all $e = 1, \ldots, n-1$. Therefore induction applies and we get that

$$|\mathrm{Aut}_G(A)| \leq |\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))|^{n-1}|\mathrm{Aut}_G(\Phi^{n-1}(A))|.$$

Now, by assumption, $A/\Phi(A)$ is an absolutely irreducible $\mathrm{GF}(q)G$-module and so, by definition, $\mathrm{Hom}_G(A/\Phi(A), A/\Phi(A)) = \mathrm{GF}(q)$. Also $A/\Phi(A) \cong \Phi^{n-1}(A) = \Omega_1(A)$. Therefore

$$|\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))| = |\mathrm{Hom}_G(A/\Phi(A), A/\Phi(A))| = |\mathrm{GF}(q)| = q$$

and

$$|\mathrm{Aut}_G(\Phi^{n-1}(A))| = |\mathrm{Aut}_G(A/\Phi(A))| = q - 1.$$

Hence $|\mathrm{Aut}_G(A)| \leq q^{n-1}(q-1)$. But, by Proposition 9.1.5, $|\mathrm{Aut}_G(A)| \geq q^{n-1}(q-1)$. Thus $|\mathrm{Aut}_G(A)| = q^{n-1}(q-1)$.

(ii) For $e = 0, \ldots, n$, the group $A/\Phi^e(A)$ is a homocyclic q-group of exponent q^e. Also

$$\frac{A/\Phi^e(A)}{\Phi(A/\Phi^e(A))} \cong \Phi^{n-e}(A)/\Phi(\Phi^{n-e}(A)) = \Phi^{n-e}(A)/\Phi^{n-e+1}(A) \cong A/\Phi(A)$$

and so the Frattini quotient of $A/\Phi^e(A)$ is an absolutely irreducible $\mathrm{GF}(q)G$-module. Therefore, by part (i), $|\mathrm{Aut}_G(A/\Phi^e(A))| = q^{e-1}(q-1)$ and so, by Corollary 9.1.7, we get that

$$\begin{aligned}|\mathrm{Hom}_G(A, A)| &= \sum_{e=0}^{n} |\mathrm{Aut}_G(A/\Phi^e(A))| = 1 + \sum_{e=1}^{n} q^{e-1}(q-1) \\ &= 1 + (q-1)(1 + \cdots + q^{n-1}) = 1 + q^n - 1 = q^n.\end{aligned}$$

□

Corollary 9.1.9. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a* $\mathrm{GF}(q)G$*-module. Then the homomorphism ψ_G defined by*

$$\psi_G \colon \sigma \in \mathrm{Aut}_G(A) \longmapsto \sigma_{|\Phi(A)} \in \mathrm{Aut}_G(\Phi(A))$$

is onto.

Proof. By Proposition 9.1.8 we have that

$$|\mathrm{Aut}_G(A)| = q^{n-1}(q-1) = qq^{n-2}(q-1) = |\mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))||\mathrm{Aut}_G(\Phi(A))|.$$

But, by Corollary 9.1.3, $\ker \psi_G \cong \mathrm{Hom}_G(A/\Phi(A), \Omega_1(A))$, which implies that ψ_G is onto. □

Corollary 9.1.10. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a* $\mathrm{GF}(q)G$*-module. Then* $\mathrm{Aut}_G(A)$ *is isomorphic to* $\mathrm{Aut}(\mathbb{Z}_{q^n})$ *and, in particular,* $\mathrm{Aut}_G(A)$ *is abelian.*

Proof. From the proof of Proposition 9.1.5 we know that $\mathrm{Aut}(\mathbb{Z}_{q^n})$ is isomorphic to a subgroup of $\mathrm{Aut}_G(A)$. But, since $A/\Phi(A)$ is an absolutely irreducible $\mathrm{GF}(q)G$-module, Proposition 9.1.8 implies that $|\mathrm{Aut}_G(A)| = q^{n-1}(q-1) = |\mathrm{Aut}(\mathbb{Z}_{q^n})|$. Hence $\mathrm{Aut}_G(A) \cong \mathrm{Aut}(\mathbb{Z}_{q^n})$ and, by [24, 1.5.5], $\mathrm{Aut}_G(A)$ is abelian. □

9.2 G-subgroups of the direct sum of some copies of A

Let A be a homocyclic q-group of finite exponent, for some prime q. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)$G-module. Recall that $\mathrm{Hom}_G(A, A)$ is a group with respect to addition. In particular, the identity of $\mathrm{Hom}_G(A, A)$, which we shall denote by 0, is the map that takes every element $a \in A$ to $0 \in A$.
Denote by D the direct sum of t copies of A. Thanks to Proposition 9.1.8, we can work out the number of distinct G-subgroups of D which are G-isomorphic to a nontrivial quotient of A. First we need to remind the reader a well known result about $\mathrm{Hom}_G(A, D)$.

Lemma 9.2.1. *Let A be an abelian q-group of finite exponent and suppose that $G \leqslant \mathrm{Aut}(A)$. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \ldots, t$. Then* $\mathrm{Hom}_G(A, D)$ *is G-isomorphic to* $\mathrm{Hom}_G(A, Q_1) \oplus \cdots \oplus \mathrm{Hom}_G(A, Q_t)$*.*

Proof. See [14, Thm. 5.4, pg. 77]. □

Theorem 9.2.2. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)G$-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \ldots, t$. Then, for $e = 1, \ldots, n$, there are $q^{(e-1)(t-1)}(q^t - 1)/(q-1)$ distinct G-subgroups of D of exponent q^e which are G-isomorphic to a nontrivial quotient of A. In particular, the total number of distinct G-subgroups of D which are G-isomorphic to a nontrivial quotient of A is n, if $t = 1$, and, for $t > 1$, is given by*

$$\frac{q^t - 1}{q - 1} \, \frac{q^{(t-1)n} - 1}{q^{t-1} - 1}.$$

Proof. Let R be a G-subgroup of D of exponent q^e, for $e = 1, \ldots, n$, and suppose that R is G-isomorphic to a nontrivial quotient of A. Then, by Proposition 1.3.11, $R \cong \Phi^{n-e}(A)$.
By the homomorphism Theorem, we also have that $R = \psi(A)$, for some $\psi \in \mathrm{Hom}_G(A, D)$, $\psi \neq 0$, that is, by Lemma 9.2.1, $R = \psi(A)$, where $\psi = \sum_{j=1}^{t} \psi_j$, with $\psi_j \in \mathrm{Hom}_G(A, Q_j)$ and $(\psi_1, \ldots, \psi_t) \neq (0, \ldots, 0)$.
Next we shall prove that R is uniquely determined by ψ up to multiplication by an element of $\mathrm{Aut}_G(R)$ and this will allow us to count the number of distinct subgroups R.
Let $\psi, \chi \in \mathrm{Hom}_G(A, D)$ such that $\psi(A) = R = \chi(A)$. Then $A/\ker\psi \cong R \cong A/\ker\chi$. Furthermore $A/\ker\psi = A/\ker\chi$, since, by Proposition 1.3.11, a G-subgroup of A is uniquely determined by its exponent and so $\ker\psi = \ker\chi$. Thus we can consider the map

$$\alpha = \chi\psi^{-1} \colon R = \psi(A) \longrightarrow A/\ker\psi = A/\ker\chi \longrightarrow \chi(A) = R.$$

Then $\alpha \in \mathrm{Aut}_G(R)$ and $\chi = \alpha\psi$. Conversely, if $R = \psi(A)$, for some $\psi \in \mathrm{Hom}_G(A, D)$, then, of course, $R = \alpha(\psi(A))$, for all $\alpha \in \mathrm{Aut}_G(R)$, and $\alpha\psi \in \mathrm{Hom}_G(A, D)$.
Therefore the number of distinct G-subgroups R of D which are G-isomorphic to a nontrivial quotient of A and having exponent q^e is equal to

$$\frac{|\mathrm{Hom}_G(\Phi^{n-e}(A), \Phi^{n-e}(A))|^t - |\mathrm{Hom}_G(\Phi^{n-e+1}(A), \Phi^{n-e+1}(A))|^t}{|\mathrm{Aut}_G(\Phi^{n-e}(A))|},$$

which is, by Proposition 9.1.8, equal to

$$\frac{q^{et} - q^{(e-1)t}}{q^{e-1}(q-1)} = \frac{q^{(e-1)t}(q^t - 1)}{q^{e-1}(q-1)} = q^{(e-1)(t-1)} \, \frac{q^t - 1}{q - 1}.$$

In particular, for $t = 1$, there are n distinct G-subgroups of D which are G-isomorphic to a nontrivial quotient of A, whereas, for $t > 1$, there are

$$\sum_{e=1}^{n} q^{(e-1)(t-1)} \frac{q^t - 1}{q - 1} = \frac{q^t - 1}{q - 1} \sum_{e=1}^{n} (q^{t-1})^{e-1} = \frac{q^t - 1}{q - 1} \frac{q^{(t-1)n} - 1}{q^{t-1} - 1},$$

such subgroups. □

Denote by $\mathcal{R}_G$ the set of G-subgroups of D which are G-isomorphic to a nontrivial quotient of A.

Corollary 9.2.3. *Let A and D be as in Theorem 9.2.2. Then the number of G-subgroups of D which are G-isomorphic to a nontrivial quotient of A depends only on the exponent q^n of A, on the number t of direct summands of D and on G being absolutely irreducible on $A/\Phi(A)$, but not on the group structure of G. In particular, $\mathcal{R}_G = \mathcal{R}_H$, for any group H such that $G \leqslant H$ and A is a H-group.*

Proof. Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a GF(q)G-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \ldots, t$. Finally let $H \leqslant \mathrm{Aut}(A)$ and suppose that $G \leqslant H$. Then D becomes a H-group. Moreover, by Proposition 8.1.7, $A/\Phi(A)$ is absolutely irreducible as a GF(q)H-module. Therefore, by Theorem 9.2.2, $|\mathcal{R}_H| = |\mathcal{R}_G|$ and, since $\mathcal{R}_H \subseteq \mathcal{R}_G$, we can conclude that $\mathcal{R}_H = \mathcal{R}_G$. □

We now give an explicit description of the G-subgroups of D which are G-isomorphic to a quotient of A.

First, since $A/\Phi(A)$ is an irreducible GF$(q)G$-module, we have that $A = \langle a \rangle^G$, for all $a \in A \setminus \Phi(A)$. So, for $j = 1, \ldots, t$, let $x_j \in Q_j$ such that $Q_j = \langle x_j \rangle^G$. Thus $D = \langle x_1 \rangle^G \oplus \cdots \oplus \langle x_t \rangle^G$ and, of course, $\mathrm{o}(x_j) = q^n$, since A has exponent q^n.

In particular, if $R \in \mathcal{R}_G$, then $R \cong \Phi^{n-e}(A)$, for some $e = 1, \ldots, n$. Hence $R/\Phi(R) \cong \Phi^{n-e}(A)/\Phi^{n-e+1}(A) \cong A/\Phi(A)$ and $R/\Phi(R)$ is an absolutely irreducible GF$(q)G$-module. Thus $R = \langle x \rangle^G$, for all $x \in R \setminus \Phi(R)$ and so, since $D = \langle x_1 \rangle^G \oplus \cdots \oplus \langle x_t \rangle^G$, we can write $R = \langle (\alpha_1 x_1, \ldots, \alpha_t x_t) \rangle^G$, with $0 \leq \alpha_i \leq q^n - 1$.

We want to produce all distinct elements of $\mathcal{R}_G$. We shall do this by looking at the sequences $(\alpha_1, \ldots, \alpha_t)$ of integers such that $R = \langle (\alpha_1 x_1, \ldots, \alpha_t x_t) \rangle^G$.

Set $Z = \mathbb{Z}_{q^n} = \{0, \ldots, q^n - 1\}$ and denote by Z^t the set of all t-ples of elements of Z. For

$\alpha \in Z^t$, set $x_\alpha = (\alpha_1 x_1, \ldots, \alpha_t x_t)$ and $R_\alpha = \langle x_\alpha \rangle^G$. For $j = 1, \ldots, t$ define the set $\Gamma_j(n)$ as follows

$$\Gamma_j(n) = \{(\alpha_1, \ldots, \alpha_t) \in Z^t \mid \alpha_j = 1 \text{ and, for } i < j,\ q|\alpha_i\}.$$

For $e = 1, \ldots, n-1$, define by induction the set $\Gamma_j(e)$ as

$$\Gamma_j(e) = \{q\alpha = (q\alpha_1, \ldots, q\alpha_t) \in Z^t \mid \alpha \in \Gamma_j(e+1)\},$$

where $q\alpha_1, \ldots, q\alpha_t$ are all taken modulo q^n, that is, $\Gamma_j(e) = \{q^{n-e}\alpha \mid \alpha \in \Gamma_j(n)\}$. For $e = 1, \ldots, n$, let

$$\Gamma(e) = \bigcup_{j=1}^{t} \Gamma_j(e) \quad \text{and} \quad \Gamma = \bigcup_{e=1}^{n} \Gamma(e).$$

We shall show that $\mathcal{R}_G = \{R_\alpha \mid \alpha \in \Gamma\}$.

Theorem 9.2.4. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)G$-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \ldots, t$. Then, for $e = 1, \ldots, n$, the set of distinct G-subgroups of D of exponent q^e which are G-isomorphic to a nontrivial quotient of A is given by $\{R_\alpha \mid \alpha \in \Gamma(e)\}$, where R_α and $\Gamma(e)$ are defined as above. In particular, $\mathcal{R}_G = \{R_\alpha \mid \alpha \in \Gamma\}$.*

Proof. We shall first show that, for $e = 1, \ldots, n$ and $\alpha \in \Gamma(e)$, R_α is a G-subgroup of D of exponent q^e which is G-isomorphic to a nontrivial quotient of A.

Let $R_\alpha = \langle x_\alpha \rangle^G$, for some $\alpha \in \Gamma(e)$ and $e = 1, \ldots, n$. Clearly, R_α is a G-subgroup of D. Suppose that $\alpha \in \Gamma_j(e)$, for some $j \in \{1, \ldots, t\}$. Then $\alpha_j = q^{n-e}$, which implies that $x_\alpha = (\alpha_1 x_1, \ldots, \alpha_t x_t)$ has order q^e and so R_α has exponent q^e.

Now, without loss of generality, assume that $\alpha \in \Gamma_1(e)$, so $\alpha_1 = q^{n-e}$, and consider the map τ taking $x_\alpha = (q^{n-e}x_1, \alpha_2 x_2, \ldots, \alpha_t x_t)$ to $q^{n-e}x_1$. Then τ is a G-isomorphism from R_α to $q^{n-e}Q_1 = \Phi^{n-e}(Q_1) \cong Q_1/\Phi^e(Q_1)$ and so R_α is G-isomorphic to a nontrivial quotient of A.

Next we want to show that the subgroups R_α, for $\alpha \in \Gamma(e)$, are all distinct.

Let $\alpha, \beta \in \Gamma(e)$, for some $e = 1, \ldots, n$. First suppose that α and β belong to the same set $\Gamma_j(e)$, say, $\alpha, \beta \in \Gamma_1(e)$, and assume that $R_\alpha = R_\beta$. Then $\alpha_1 = q^{n-e} = \beta_1$ and

$$x_\alpha - x_\beta = (0, (\alpha_2 - \beta_2)y_2, \ldots, (\alpha_t - \beta_t)y_t) \in R_\alpha.$$

But, since $o(\alpha_1 x_1) = q^e$ and $o(\alpha_j x_j) | q^e$, for all j, an element of R_α that has 0 as first coordinate must have 0 everywhere. Therefore $x_\alpha - x_\beta = (0, \dots, 0)$, that is, $x_\alpha = x_\beta$.
Suppose now, without loss of generality, that $\alpha \in \Gamma_1(e)$ and $\beta \in \Gamma_2(e)$. Then $x_\alpha = (q^{n-e}x_1, \alpha_2 x_2, \dots, \alpha_t x_t)$ and $x_\beta = (\beta_1 x_1, q^{n-e}x_2, \dots, \beta_t x_t)$, with $o(\beta_1 x_1) < q^e$, since q^{n-e+1} divides β_1. Then R_β is a subgroup of

$$\Phi^{n-e+1}(Q_1) \oplus \Phi^{n-e}(Q_2) \oplus \cdots \oplus \Phi^{n-e}(Q_t),$$

whereas R_α is not. Therefore R_α and R_β cannot be equal. Hence, for all $\alpha \in \Gamma(e)$, the subgroups R_α are all distinct. This implies that the number of subgroups R_α, for $\alpha \in \Gamma(e)$, equals the cardinality of the set $\Gamma(e)$. But, for $j = 1, \dots, t$, $\Gamma_j(e) = \{q^{n-e}\alpha \mid \alpha \in \Gamma_j(n)\}$, that is,

$$\Gamma_j(e) = \{(\alpha_1, \dots, \alpha_t) \in Z^t \mid \alpha_j = q^{n-e};\ \text{for } i < j,\ q^{n-e+1}|\alpha_i;\ \text{for } j < i,\ q^{n-e}|\alpha_i\}$$

and so

$$|\Gamma_j(e)| = q^{(e-1)(j-1)}q^{e(t-j)} = q^{e(t-1)+1-j}.$$

Hence

$$|\Gamma(e)| = \sum_{j=1}^{t} |\Gamma_j(e)| = q^{e(t-1)+1} \sum_{j=1}^{t} q^{-j} = \frac{q^{e(t-1)+1}}{q^t}\ (q^{t-1} + \cdots + 1) = q^{(e-1)(t-1)}\ \frac{q^t - 1}{q - 1},$$

which is precisely the number given in Theorem 9.2.2. Hence we can conclude that the set of distinct G-subgroups of D of exponent q^e which are G-isomorphic to a nontrivial quotient of A is equal to $\{R_\alpha \mid \alpha \in \Gamma(e)\}$.
Finally, for $\alpha \in \Gamma(e)$ and $\beta \in \Gamma(r)$, with $e, r = 1, \dots, n$ and $e \neq r$, we have that $R_\alpha \neq R_\beta$, since R_α and R_β have different exponent. So it follows that $\mathcal{R}_G = \{R_\alpha \mid \alpha \in \Gamma\}$. □

Notice that, for $t = 1$, we have $\Gamma(e) = \Gamma_1(e) = \{q^{n-e}\}$, for all $e = 1, \dots, n$. Therefore $\mathcal{R}_G = \{R_\alpha \mid \alpha \in \Gamma\} = \{\Phi^{n-e}(Q_1) \mid e = 1, \dots, n\}$, in accordance with Proposition 1.3.11.

Lemma 9.2.5. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)G$-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \dots, t$. Set $C = \Omega_1(D)$ and let S/C be a G-subgroup of D/C. If S/C is G-isomorphic to a nontrivial quotient of $A/\Omega_1(A)$, then $S/C = RC/C$, for some $R \in \mathcal{R}_G$.*

Proof. Set $C = \Omega_1(D)$ and $\bar{D} = D/C$. Then $\bar{D}$ is the direct sum of t copies of $\bar{A}$, with $\bar{A} = A/\Omega_1(A)$ homocyclic q-group of exponent q^{n-1} whose Frattini quotient $\bar{A}/\Phi(\bar{A})$ is an absolutely irreducible $\mathrm{GF}(q)G$-module. Also, if we set $D = \langle x_1\rangle^G \oplus \cdots \oplus \langle x_t\rangle^G$, then $\bar{D} = \langle \bar{x}_1\rangle^G \oplus \cdots \oplus \langle \bar{x}_t\rangle^G$.

Let $\bar{S}$ be a G-subgroup of $\bar{D}$ of exponent, say, p^e, for some $e = 1, \ldots, n-1$, and suppose that $\bar{S}$ is G-isomorphic to a nontrivial quotient of $\bar{A}$. Then, by Theorem 9.2.4, $\bar{S} = \langle(\alpha_1\bar{x}_1, \ldots, \alpha_t\bar{x}_t)\rangle^G$, where $\alpha = (\alpha_1, \ldots, \alpha_t)$ is a sequence of elements of $\mathbb{Z}_{q^{n-1}}$ such that, for some fixed $j = 1, \ldots, t$, $\alpha_j = q^{n-1-e}$, $q^{n-e}|\alpha_i$, for $i < j$, and $q^{n-1-e}|\alpha_i$, for $i > j$.

Set $R = \langle(\alpha_1 x_1, \ldots, \alpha_t x_t)\rangle^G \leqslant D$. Then, regarding α as a sequence of elements of $\mathbb{Z}_{q^n}$, we have that $\alpha \in \Gamma_j(e+1)$ and so, by Theorem 9.2.4, $R \in \mathcal{R}_G$. Furthermore $\bar{S} = RC/C$ and this completes the proof. ∎

Proposition 9.2.6. *Let A be a homocyclic q-group of exponent q^n. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a $\mathrm{GF}(q)G$-module. Let D be the direct sum of t copies of A, that is, $D = Q_1 \oplus \cdots \oplus Q_t$, with Q_j G-isomorphic to A, for all $j = 1, \ldots, t$. Let S be a G-subgroup of D. If S has a unique maximal G-subgroup, then S is G-isomorphic to a nontrivial quotient of A, that is, $S \in \mathcal{R}_G$.*

Proof. We shall proceed by induction on n and t. If $t = 1$, then $D = Q_1 \cong A$ and the result follows by Proposition 1.3.11. If $n = 1$, then A has exponent q and A is an irreducible $\mathrm{GF}(q)G$-module. Therefore, when regarded as a $\mathrm{GF}(q)G$-module, D is completely reducible, which implies, since S is a G-subgroup of D, that also S is completely reducible and S is G-isomorphic to the direct sum of some copies of A. Now, if S is G-isomorphic to the direct sum of more than one copy of A, then $S = S_1 \oplus S_2$, with S_1 and S_2 G-subgroups of S, against the assumption that S has a unique maximal G-subgroup. Hence S must be G-isomorphic to A and so, in this case, the theorem holds.

Suppose that $t > 1$ and $n > 1$. If $S \cap Q_1 = \{0\}$, then

$$S \cong SQ_1/Q_1 \leqslant DQ_1/Q_1 \cong Q_2 \oplus \cdots \oplus Q_t$$

and, by induction on t, S is G-isomorphic to a nontrivial quotient of A.

So assume that $S \cap Q_i \neq \{0\}$, for all $i = 1, \ldots, t$. We shall prove that this assumption yields a contradiction. Since S is G-invariant, $S \cap Q_i \neq \{0\}$ implies that $\Omega_1(Q_i) \leqslant S \cap Q_i$ and so

$$\Phi^{n-1}(D) \cong \Omega_1(D) = \langle \Omega_1(Q_i) \mid i = 1, \ldots, t \rangle \leqslant S.$$

Set $C = \Omega_1(D)$. Then S/C is a G-subgroup of D/C, where D/C is isomorphic to the direct sum of t copies of $A/\Omega_1(A)$ and has exponent q^{n-1}. Also S/C has a unique maximal G-subgroup, since so does S. Hence, by induction on n, we have that S/C is G-isomorphic to a nontrivial quotient of $A/\Omega_1(A)$. Thus, by Lemma 9.2.5, $S/C = RC/C$, for some $R \in \mathcal{R}_G$, that is, $S = RC$, where both R and C are G-invariant. Since S has a unique maximal G-subgroup, this implies that either $S = C$ or $S = R$. Now, since $C = \Omega_1(D) = \Omega_1(Q_1) \oplus \cdots \oplus \Omega_1(Q_t)$, with $t > 1$, the former case cannot occur. So assume that $S = R$. Then $C \leqslant R$ and $\Omega_1(R) = C = \Omega_1(D)$. But, since $R \in \mathcal{R}_G$, $\Omega_1(R) \cong R/\Phi(R)$ is irreducible. Hence we reach again a contradiction and this completes the proof. $\square$

9.3 Minimal generating sets

Let A be a homocyclic q-group of finite exponent, for some prime q. Let $G \leqslant \mathrm{Aut}(A)$ and assume that $A/\Phi(A)$ is absolutely irreducible as a GF(q)G-module. Denote by D the direct sum of t copies of A and by $\mathcal{R}_G$ the set of all G-subgroups of D which are G-isomorphic to a nontrivial quotient of A. Recall that, by Theorem 9.2.4, $\mathcal{R}_G = \{R_\alpha \mid \alpha \in \Gamma\}$, with R_α and Γ defined as in Section 9.2. We are interested in certain subsets of $\mathcal{R}_G$.

Definition 9.3.1. *A subset $\mathcal{G}$ of $\mathcal{R}_G$ is called a minimal generating set for D in $\mathcal{R}_G$ if $D = \langle \mathcal{G} \rangle = \langle R_\alpha \mid R_\alpha \in \mathcal{G} \rangle$ and no proper subset of $\mathcal{G}$ generates D.*

Clearly, the set $\{Q_1, \ldots, Q_t\} \subseteq \mathcal{R}_G$ is a minimal generating set for D in $\mathcal{R}_G$, since $D = Q_1 \oplus \cdots \oplus Q_t$, and this justifies the above definition.

We want to determine all minimal generating sets for D in $\mathcal{R}_G$, our interest being motivated by the link, which will be established in Section 10.2, between the subgroups R_α and some minimal parabolic subgroups of $\mathrm{Sym}(\Omega)$, with $|\Omega|$ a power of p.

First notice that, since, for $\alpha \in \Gamma(e)$, R_α is G-isomorphic to a nontrivial quotient of A of exponent q^e, for a minimal generating set it will be enough to consider the subgroups R_α such that $\alpha \in \Gamma(n)$.

For $R_\alpha \in \mathcal{R}_G$, denote by $\bar{R}_\alpha$ the quotient group $R_\alpha \Phi(D)/\Phi(D)$, and set

$$\bar{\mathcal{R}}_G = \{\bar{R}_\alpha | R_\alpha \in \mathcal{R}_G\} = \{\bar{R}_\alpha \mid \alpha \in \Gamma(n)\}.$$

In particular, every element of $\bar{\mathcal{R}}_G$ is a G-subgroup of $D/\Phi(D)$ which is G-isomorphic to $A/\Phi(A)$. As our next result shows, it will be enough to look at the minimal generating sets for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$.

Proposition 9.3.2. *A subset $\mathcal{G}$ of $\mathcal{R}_G$ is a minimal generating set for D in $\mathcal{R}_G$ if and only if the set $\bar{\mathcal{G}} = \{\bar{R}_\alpha \mid R_\alpha \in \mathcal{G}\}$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$.*

Proof. Let $\mathcal{G} \subseteq \mathcal{R}_G$ and suppose that $D = \langle \mathcal{G} \rangle = \langle R_\alpha \mid R_\alpha \in \mathcal{G} \rangle$. Then

$$D/\Phi(D) = \langle R_\alpha \mid R_\alpha \in \mathcal{G} \rangle \Phi(D)/\Phi(D) = \langle R_\alpha \Phi(D) \mid R_\alpha \in \mathcal{G} \rangle/\Phi(D) = \langle \bar{R}_\alpha \mid R_\alpha \in \mathcal{G} \rangle$$

and so $D/\Phi(D)$ is generated by $\bar{\mathcal{G}}$.
Conversely, let $\bar{\mathcal{G}} \subseteq \bar{\mathcal{R}}_G$ and suppose that $D/\Phi(D) = \langle \bar{\mathcal{G}} \rangle = \langle \bar{R}_\alpha \mid \bar{R}_\alpha \in \bar{\mathcal{G}} \rangle$. Then

$$D = \langle R_\alpha \Phi(D) \mid \bar{R}_\alpha \in \bar{\mathcal{G}} \rangle$$

and so, by Proposition 1.3.2, $D = \langle R_\alpha \mid \bar{R}_\alpha \in \bar{\mathcal{G}} \rangle = \langle \mathcal{G} \rangle$.
Therefore $D = \langle \mathcal{G} \rangle$ if and only if $D/\Phi(D) = \langle \bar{\mathcal{G}} \rangle$. In particular, it follows that $\mathcal{G}$ is a minimal generating set for D in $\mathcal{R}_G$ if and only if $\bar{\mathcal{G}}$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$. $\square$

We shall now focus our attention on minimal generating sets for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$.

Proposition 9.3.3. *A minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$ consists of precisely t elements of $\bar{\mathcal{R}}_G$.*

Proof. Let $\bar{\mathcal{G}} = \{\bar{R}_1, \ldots, \bar{R}_s\} \subseteq \bar{\mathcal{R}}_G$ be a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$. Set $V = D/\Phi(D)$. Then $V = V_1 \oplus \cdots \oplus V_t$, where $V_i = Q_i\Phi(D)/\Phi(D) \cong Q_i/\Phi(Q_i)$ and so V is the direct sum of t copies of $A/\Phi(A)$.
We shall proceed by induction on t. If $t = 1$, then the result is obvious. Suppose that $t > 1$ and set $W = \langle \bar{R}_2, \ldots, \bar{R}_s \rangle$. Then, since, for $\alpha \in \Gamma(n)$, $\bar{R}_\alpha$ is G-isomorphic to $A/\Phi(A)$, W is the direct sum of $t-1$ copies of $A/\Phi(A)$. Also $V = \langle \bar{R}_1, W \rangle$ and, by the minimality of $\bar{\mathcal{G}}$, W is a proper subgroup of V. Moreover, $\{\bar{R}_2, \ldots, \bar{R}_s\}$ is a minimal generating set for W in $\bar{\mathcal{R}}_G$, because, if W were generated by a proper subset $\bar{\mathcal{G}}_1$ of $\{\bar{R}_2, \ldots, \bar{R}_s\}$, then V would

be generated by a proper subset of $\bar{\mathcal{G}}$, namely $\{\bar{R}_1\} \cup \bar{\mathcal{G}}_1$, against the assumption that $\bar{\mathcal{G}}$ is a minimal generating set for V in $\bar{\mathcal{R}}_G$. Then, by the induction hypothesis, $|\{\bar{R}_2, \ldots, \bar{R}_s\}| = s - 1 = t - 1$, that is, $|\bar{\mathcal{G}}| = s = t$. $\square$

Set $Z = \mathbb{Z}_{q^n}$. For $\alpha, \beta \in Z^t$, we shall say that α is congruent β modulo q, and write $\alpha \equiv \beta \pmod q$, if $\alpha_i \equiv \beta_i \pmod q$, for all $i = 1, \ldots, t$.
Notice that, for $\alpha \in Z^t$, $x_\alpha = (\alpha_1 x_1, \ldots, \alpha_t x_t) \in \Phi(D)$ if and only if $\alpha \equiv \mathbf{0} \pmod q$, where $\mathbf{0} = (0, \ldots, 0) \in Z^t$.

Proposition 9.3.4. *A subset $\bar{\mathcal{G}} = \{\bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t}\}$ of $\bar{\mathcal{R}}_G$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$ if and only if, for $i = 1, \ldots, t$,*

$$\alpha_i \not\equiv \sum_{j \neq i} \lambda_j \alpha_j \pmod q,$$

for all $\lambda_j \in \mathrm{GF}(q)$.

Proof. By Proposition 9.3.3, a set $\bar{\mathcal{G}} = \{\bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t}\}$ of t elements of $\bar{\mathcal{R}}_G$ is a minimal generating set for $\bar{D} = D/\Phi(D)$ in $\bar{\mathcal{R}}_G$ if and only if $\bar{D} = \langle \bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t} \rangle$, that is, if and only if, for $i = 1, \ldots, t$, $\bar{R}_{\alpha_i} \nleqslant \langle \bar{R}_{\alpha_j} \mid j \neq i \rangle$.
But, for $i = 1, \ldots, t$, $\bar{R}_{\alpha_i} = \langle \bar{x}_{\alpha_i} \rangle^G = \langle x_{\alpha_i} \Phi(D) \rangle^G$. Thus $\bar{R}_{\alpha_i} \nleqslant \langle \bar{R}_{\alpha_j} \mid j \neq i \rangle$ if and only if $x_{\alpha_i}\Phi(D) \notin \langle x_{\alpha_j} \Phi(D) \mid j \neq i \rangle^G$ and this is equivalent to saying that, for all $\lambda_j \in \mathrm{GF}(q)$,

$$x_{\alpha_i} - \sum_{j \neq i} \lambda_j x_{\alpha_j} \notin \Phi(D).$$

But

$$x_{\alpha_i} - \sum_{j \neq i} \lambda_j x_{\alpha_j} = (\alpha_{i1} x_1, \ldots, \alpha_{it} x_t) - \sum_{j \neq i} (\lambda_j \alpha_{j1} x_1, \ldots, \lambda_j \alpha_{jt} x_t) = x_\beta,$$

where $\beta = \alpha_i - \sum_{j \neq i} \lambda_j \alpha_j$, and $x_\beta \notin \Phi(D)$ if and only if $\beta \not\equiv \mathbf{0} \pmod q$, that is,

$$\alpha_i \not\equiv \sum_{j \neq i} \lambda_j \alpha_j \pmod q.$$

$\square$

We are now able to count the number of minimal generating sets for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$.

Lemma 9.3.5. *For $\alpha \in \Gamma(n)$, there are $q^{(n-1)(t-1)}$ elements $\beta \in \Gamma(n)$ such that $\bar{R}_\alpha = \bar{R}_\beta$.*

Proof. For $\alpha, \beta \in \Gamma(n)$ consider the subgroups $\bar{R}_\alpha = \langle x_\alpha \Phi(D) \rangle^G$ and $\bar{R}_\beta = \langle x_\beta \Phi(D) \rangle^G$. Then $\bar{R}_\alpha = \bar{R}_\beta$ if and only if $x_\alpha - x_\beta = x_{\alpha-\beta} \in \Phi(D)$, that is, if and only if $\alpha \equiv \beta \pmod q$. Hence, given $\alpha \in \Gamma(n)$, we need to count how many $\beta \in \Gamma(n)$ there are such that $\alpha \equiv \beta \pmod q$.
Choose $\alpha \in \Gamma(n)$ and let $\beta \in \Gamma(n)$ such that $\alpha \equiv \beta \pmod q$. Suppose that $\alpha \in \Gamma_j(n)$, for some $j = 1, \ldots, t$. We shall first show that also β belongs to $\Gamma_j(n)$. By way of a contradiction, suppose that $\beta \in \Gamma_i(n)$, for some $i \neq j$, and, without loss of generality, assume $j < i$. Then, since $\alpha_j = 1$ and $\alpha \equiv \beta \pmod q$, we must have that $\beta_j \equiv 1 \pmod q$. But, by construction, $q | \beta_j$, since $j < i$ and $\beta \in \Gamma_i(n)$, that is, $\beta_j \equiv 0 \pmod q$ and we have reached a contradiction. Therefore we must have $i = j$ and $\alpha, \beta \in \Gamma_j(n)$. In particular, this implies that $\alpha_j = \beta_j = 1$ and so β_j is uniquely determined. Furthermore, for $i = 1, \ldots, t$ and $i \neq j$, $\alpha_i \equiv \beta_i \pmod q$, where $\alpha_i, \beta_i \in \mathbb{Z}_{q^n}$, and so, given α_i, there are q^{n-1} possible values for β_i. Therefore, given α, there are $q^{(n-1)(t-1)}$ possible choices for β such that $\alpha \equiv \beta \pmod q$, that is, $\bar{R}_\alpha = \bar{R}_\beta$. $\square$

Theorem 9.3.6. *The number of minimal generating sets for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$ is given by*

$$\frac{1}{t!} \frac{q^{t(t-1)(2n-1)/2}}{(q-1)^t} \prod_{s=1}^{t} (q^s - 1).$$

Proof. We need to count the number of possible choices for the set $\{\alpha_1, \ldots, \alpha_t\} \subseteq \Gamma(n)$ such that $\{\bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t}\}$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$. This means that at each step we look for an element $\alpha_i \in \Gamma(n)$ such that $\bar{R}_{\alpha_i} \not\leqslant \langle \bar{R}_{\alpha_j} \mid j < i \rangle$.
As first step, we can choose α_1 to be any element of $\Gamma(n)$, so we count $|\Gamma(n)|$ choices for α_1. Given α_1, we want to find $\alpha_2 \in \Gamma(n)$ such that $\bar{R}_{\alpha_1} \neq \bar{R}_{\alpha_2}$. By Lemma 9.3.5, there are $q^{(n-1)(t-1)}$ elements $\beta \in \Gamma(n)$ such that $\bar{R}_{\alpha_1} = \bar{R}_\beta$, giving us

$$|\Gamma(n)| - q^{(n-1)(t-1)}$$

choices for α_2. Given α_1 and α_2, we search for $\alpha_3 \in \Gamma(n)$ such that $\bar{R}_{\alpha_3} \not\leqslant \langle \bar{R}_{\alpha_1}, \bar{R}_{\alpha_2} \rangle = \bar{R}_{\alpha_1} \oplus \bar{R}_{\alpha_2}$. Now $\bar{R}_{\alpha_1} \oplus \bar{R}_{\alpha_2}$ is the direct sum of two copies of $A/\Phi(A)$, that is, $\bar{R}_{\alpha_1} \oplus \bar{R}_{\alpha_2}$ is the direct sum of two isomorphic irreducible $\mathrm{GF}(q)G$-modules. Hence, by [14, Thm. 5.6, pg 79], $\bar{R}_{\alpha_1} \oplus \bar{R}_{\alpha_2}$ has $(q^2-1)/(q-1)$ G-subgroups which are G-isomorphic to $A/\Phi(A)$ and so of the form $\bar{R}_\beta$. Also, by Lemma 9.3.5, each of these $(q^2-1)/(q-1)$ subgroups can be obtained from $q^{(n-1)(t-1)}$ different elements of $\Gamma(n)$. Therefore there are $q^{(n-1)(t-1)}(q^2-1)/(q-1)$ elements $\beta \in \Gamma(n)$ such that $\bar{R}_\beta \leqslant \bar{R}_{\alpha_1} \oplus \bar{R}_{\alpha_2}$ and so we have

$$|\Gamma(n)| - q^{(n-1)(t-1)}(q^2-1)/(q-1)$$

possible choices for α_3. Using the same argument for any $i \geq 3$, we find that the number of choices for α_i is given by

$$|\Gamma(n)| - q^{(n-1)(t-1)} \ \frac{q^{i-1}-1}{q-1}\ .$$

All together this gives us

$$\prod_{s=0}^{t-1} \left(|\Gamma(n)| - q^{(n-1)(t-1)} \ \frac{q^s-1}{q-1} \right)$$

choices. However this number counts the ordered t-ples $(\alpha_1, \ldots, \alpha_t)$ of elements of $\Gamma(n)$, rather than the sets $\{\alpha_1, \ldots, \alpha_t\} \subseteq \Gamma(n)$, such that $\{\bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t}\}$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$. This means that each set $\{\alpha_1, \ldots, \alpha_t\}$ is counted $t!$ times. Hence, the number of sets $\{\alpha_1, \ldots, \alpha_t\} \subseteq \Gamma(n)$, such that $\{\bar{R}_{\alpha_1}, \ldots, \bar{R}_{\alpha_t}\}$ is a minimal generating set for $D/\Phi(D)$ in $\bar{\mathcal{R}}_G$ will be given by

$$\frac{1}{t!} \prod_{s=0}^{t-1} \left(|\Gamma(n)| - q^{(n-1)(t-1)} \ \frac{q^s-1}{q-1} \right)$$

and, since $|\Gamma(n)| = q^{(n-1)(t-1)}(q^t-1)/(q-1)$, this number is equal to

$$\begin{aligned}
\frac{1}{t!} \prod_{s=0}^{t-1} \frac{q^{(n-1)(t-1)}}{q-1} \ (q^t - q^s) &= \frac{1}{t!} \ \frac{q^{t(n-1)(t-1)}}{(q-1)^t} \ \prod_{s=0}^{t-1} q^s(q^{t-s}-1) \\
&= \frac{1}{t!} \ \frac{q^{t(n-1)(t-1)}}{(q-1)^t} \ q^{t(t-1)/2} \prod_{s=1}^{t} (q^s-1) \\
&= \frac{1}{t!} \ \frac{q^{t(2n-1)(t-1)/2}}{(q-1)^t} \ \prod_{s=1}^{t} (q^s-1).
\end{aligned}$$

$\square$

Corollary 9.3.7. *A minimal generating set $\mathcal{G}$ for D in $\mathcal{R}_G$ consists of t subgroups $R_{\alpha_1}, \ldots, R_{\alpha_t} \in \mathcal{R}_G$ such that, for $i = 1, \ldots, t$, $\alpha_i \in \Gamma(n)$ and*

$$\alpha_i \not\equiv \sum_{j \neq i} \lambda_j \alpha_j \pmod{q},$$

for all $\lambda_j \in \mathrm{GF}(q)$. Furthermore the number of minimal generating sets for D in $\mathcal{R}_G$ is

$$\frac{1}{t!} \ \frac{q^{t(t-1)(2n-1)/2}}{(q-1)^t} \ \prod_{s=1}^{t} (q^s-1).$$

Chapter 10

Soluble minimal parabolic subgroups and systems of Sym(p^n)

We classify all soluble minimal parabolic subgroups, and the corresponding minimal parabolic systems, of Sym(p^n) with respect to the normalizer of a Sylow p-subgroup. Recall that, by Lemma 6.7.6, such minimal parabolic subgroups are contained in a subgroup of Sym(p^n) isomorphic to the wreath product of n copies of Hol($\mathbb{Z}_p$).

10.1 The building blocks

Let $G = \mathrm{Sym}(\Omega)$, with $|\Omega| = p^n$, p prime and $n \in \mathbb{N}$. Let $T \in \mathrm{Syl}_p(G)$ and set $B = N_G(T)$. Let H be a subgroup of G containing B and isomorphic to the wreath product of n copies of Hol($\mathbb{Z}_p$). This section will be devoted to introducing and studying certain subgroups R of H such that every minimal parabolic subgroup of H with respect to B has the form BR.

We shall first revise some of the notation introduced in Sections 5.1 and 5.2. Write

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

with x_i element of order p acting on p^i points, and

$$H = \langle x_1, y_1, \ldots, x_n, y_n \rangle,$$

where y_i is an element of order $p - 1$ acting on the same p^i points as x_i and normalizing $\langle x_i \rangle$. So H is isomorphic to the wreath product of n copies of Hol($\mathbb{Z}_p$). Then, according to

Corollary 5.2.6, B has the form

$$B = T \rtimes \langle h_1, \dots, h_n \rangle$$

and the complement to T in B is a homocyclic group of order $(p-1)^n$. Set $S_n = T$ and $L_n = \langle y_n \rangle$ and, for $k = 1, \dots, n-1$, set

$$T_{n-k} = \langle x_{k+1}, \dots, x_n \rangle,$$
$$S_k = \langle x_1, \dots, x_k \rangle^{T_{n-k}},$$
$$H_{n-k} = \langle x_{k+1}, y_{k+1}, \dots, x_n, y_n \rangle,$$
$$L_k = \langle y_k \rangle^{T_{n-k}}.$$

In particular, T_{n-k} is isomorphic to a Sylow p-subgroup of $\mathrm{Sym}(p^{n-k})$ and S_k is the direct product of p^{n-k} copies of a Sylow p-subgroup of $\mathrm{Sym}(p^k)$. Also $H = TL_1 \dots L_n$, with $L_k \cap \langle L_h \mid h \neq k \rangle = 1$.

Denote by Δ_k the set of orbits of S_k on Ω and by B_{n-k} the normalizer of T_{n-k} in $\mathrm{Sym}(\Delta_k)$. Recall that $B \leqslant N_G(S_k)$, for all $k = 1, \dots, n-1$, and that $N_G(S_k) = K_k \rtimes \mathrm{Sym}(\Delta_k)$, with K_k the base group of $N_G(S_k)$ with respect to Δ_k and isomorphic to the direct product of p^{n-k} copies of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^k)$.

Finally, notice that, by Corollary 2.6.5, S_k is equal to the normal closure $\langle x_1, \dots, x_k \rangle^M$, for any $M \leqslant \mathrm{Sym}(\Delta_k)$ containing T_{n-k}, and similarly for L_k. This implies, in particular, that S_k and L_k are normalized by any subgroup of $\mathrm{Sym}(\Delta_k)$ that contains T_{n-k}.

We can now move to the new setting. For $k = 1, \dots, n$, define the subgroup J_k of H by setting $J_k = BL_k$. If we write $B = A_{k-1} \rtimes B_{n-k+1}$, with $A_{k-1} = S_{k-1} \rtimes \langle h_1, \dots, h_{k-1} \rangle$ the base group of B with respect to Δ_{k-1}, then J_k can be written as

$$J_k = A_{k-1} \rtimes (((\langle x_k \rangle^{B_{n-k}} \rtimes L_k) \rtimes B_{n-k}).$$

In particular $J_n = B\langle y_n \rangle = B$ and $H = TL_1 \dots L_n = J_1 \dots J_{n-1}$.

Proposition 10.1.1. *For $k = 1, \dots, n$, S_k is the largest normal p-subgroup of J_k, that is, $O_p(J_k) = S_k$.*

Proof. By Lemma 5.2.8, we know that L_k is contained in the base group of $N_G(S_k)$. Thus $J_k = BL_k \leqslant N_G(S_k)$ and $S_k \trianglelefteq J_k$. Now suppose there exists $1 \neq x \in O_p(J_k) \setminus S_k$. Then

$x \in B_{n-k}$ and, in particular, x normalizes L_k. Thus, since $L_k \leqslant J_k$ and $x \in O_p(J_k)$, we have that $[x, L_k] \leqslant L_k \cap O_p(J_k) = 1$. Therefore x centralizes L_k, which is a contradiction, since $x \in B_{n-k} \leqslant \mathrm{Sym}(\Delta_k)$ and so x acts nontrivially on the set Δ_k, whose elements are unions of blocks of L_k. $\square$

For $q \in \pi(p-1)$, denote by q^{α_q} the highest power of q dividing $p-1$. For $e = 1, \ldots, \alpha_q$, set

$$Z(k,q,e) = (O_q(L_k))^{q^{\alpha_q - e}} = \Phi^{\alpha_q - e}(O_q(L_k)),$$

that is, since $L_k = \langle y_k \rangle^{B_{n-k}}$,

$$Z(k,q,e) = \langle y_k^{(p-1)/q^e} \rangle^{B_{n-k}}.$$

Then $Z(k,q,e)$ is a homocyclic q-group of exponent q^e and order $(q^e)^{p^{n-k}}$, with generators, say, $z_1, \ldots, z_{p^{n-k}}$. For $i = 0, \ldots, n-k$, define the subgroup $Q(k,q,e,i)$ of Z by setting $Q(k,q,e,i) = \langle w(k,q,e,i) \rangle^{B_{n-k}}$, with

$$w(k,q,e,i) = (z_1 \ldots z_{p^{n-k-i}})(z_{p^{n-k-i}+1} \ldots z_{2p^{n-k-i}})^{-1}.$$

Then $Q(k,q,e,i)$ is a homocyclic B_{n-k}-invariant q-group of exponent q^e. In particular, $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ is an elementary abelian q-group invariant under the action by conjugation of B_{n-k} and so $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ can be regarded as a $\mathrm{GF}(q)B_{n-k}$-module. Also

$$Q(k,q,e-1,i) = \Phi(Q(k,q,e,i))$$

and $Q(k,q,e,0) = \langle h_k^{(p-1)/q^e} \rangle \leqslant B$. Finally, for $q \in \pi(p-1)$ and $i = 0, \ldots, n-1$, set

$$D_{q,i} = \langle Q(k,q,\alpha_q,i) \mid k = 1, \ldots, n-i \rangle$$

and

$$D_i = \langle D_{q,i} \mid q \in \pi(p-1) \rangle.$$

The construction of the subgroups $Q(k,q,e,i)$, $D_{q,i}$ and D_i for the group $\mathrm{Sym}(5^3)$ is presented in the following example.

Example 10.1:

Let $G = \mathrm{Sym}(125)$, that is, $p = 5$ and $n = 3$. Let T be a Sylow 5-subgroup of G and let

$x_1 = (1\ 2\ 3\ 4\ 5)$,

$x_2 = (1\ 6\ 11\ 16\ 21)(2\ 7\ 12\ 17\ 22)(3\ 8\ 13\ 18\ 23)(4\ 9\ 14\ 19\ 24)(5\ 10\ 15\ 20\ 25)$,

$x_3 = (1\ 26\ 51\ 76\ 101)(2\ 27\ 52\ 77\ 102)(3\ 28\ 53\ 78\ 103)(4\ 29\ 54\ 79\ 104)(5\ 30\ 55\ 80\ 105)$
$(6\ 31\ 56\ 81\ 106)(7\ 32\ 57\ 82\ 107)(8\ 33\ 58\ 83\ 108)(9\ 34\ 59\ 84\ 109)(10\ 35\ 60\ 85\ 110)$
$(11\ 36\ 61\ 86\ 111)(12\ 37\ 62\ 87\ 112)(13\ 38\ 63\ 88\ 113)(14\ 39\ 64\ 89\ 114)(15\ 40\ 65\ 90\ 115)$
$(16\ 41\ 66\ 91\ 116)(17\ 42\ 67\ 92\ 117)(18\ 43\ 68\ 93\ 118)(19\ 44\ 69\ 94\ 119)(20\ 45\ 70\ 95\ 120)$
$(21\ 46\ 71\ 96\ 121)(22\ 47\ 72\ 97\ 122)(23\ 48\ 73\ 98\ 123)(24\ 49\ 74\ 99\ 124)(25\ 50\ 75\ 100\ 125)$

be its generators. Recall that $S_1 = \langle x_1 \rangle^{T_2}$ and $S_2 = \langle x_1, x_2 \rangle^{T_1}$, where $T_1 = \langle x_3 \rangle$ and $T_2 = \langle x_2, x_3 \rangle$. Denote by H a subgroup of G containing T and isomorphic to the wreath product of three copies of $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ and write $H = \langle T, y_1, y_2, y_3 \rangle$, where

$y_1 = (2\ 3\ 5\ 4)$,

$y_2 = (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20)$,

$y_3 = (26\ 51\ 101\ 76)(27\ 52\ 102\ 77)(28\ 53\ 103\ 78)(29\ 54\ 104\ 79)(30\ 55\ 105\ 80)$
$(31\ 56\ 106\ 81)(32\ 57\ 107\ 82)(33\ 58\ 108\ 83)(34\ 59\ 109\ 84)(35\ 60\ 110\ 85)$
$(36\ 61\ 111\ 86)(37\ 62\ 112\ 87)(38\ 63\ 113\ 88)(39\ 64\ 114\ 89)(40\ 65\ 115\ 90)$
$(41\ 66\ 116\ 91)(42\ 67\ 117\ 92)(43\ 68\ 118\ 93)(44\ 69\ 119\ 94)(45\ 70\ 120\ 95)$
$(46\ 71\ 121\ 96)(47\ 72\ 122\ 97)(48\ 73\ 123\ 98)(49\ 74\ 124\ 99)(50\ 75\ 125\ 100)$.

Recall that $L_1 = \langle y_1 \rangle^{T_2}$, $L_2 = \langle y_2 \rangle^{T_1}$ and $L_3 = \langle y_3 \rangle$. Also $H_1 = \langle x_3, y_3 \rangle$ and $H_2 = \langle x_2, x_3, y_2, y_3 \rangle$. The normalizer B of T in G can be described as $B = T \rtimes \langle h_1, h_2, h_3 \rangle$, with $h_3 = y_3$ and

$h_1 = (2\ 3\ 5\ 4)(7\ 8\ 10\ 9)(12\ 13\ 15\ 14)(17\ 18\ 20\ 19)(22\ 23\ 25\ 24)$
$(27\ 28\ 30\ 29)(32\ 33\ 35\ 34)(37\ 38\ 40\ 39)(42\ 43\ 45\ 44)(47\ 48\ 50\ 49)$
$(52\ 53\ 55\ 54)(57\ 58\ 60\ 59)(62\ 63\ 65\ 64)(67\ 68\ 70\ 69)(72\ 73\ 75\ 74)$
$(77\ 78\ 80\ 79)(82\ 83\ 85\ 84)(87\ 88\ 90\ 89)(92\ 93\ 95\ 94)(97\ 98\ 100\ 99)$
$(102\ 103\ 105\ 104)(107\ 108\ 110\ 109)(112\ 113\ 115\ 114)(117\ 118\ 120\ 119)(122\ 123\ 125\ 124)$,

$$
\begin{aligned}
h_2 = {} & (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20) \\
& (31\ 36\ 46\ 41)(32\ 37\ 47\ 42)(33\ 38\ 48\ 43)(34\ 39\ 49\ 44)(35\ 40\ 50\ 45) \\
& (56\ 61\ 71\ 66)(57\ 62\ 72\ 67)(58\ 63\ 73\ 68)(59\ 64\ 74\ 69)(60\ 65\ 75\ 70) \\
& (81\ 86\ 96\ 91)(82\ 87\ 97\ 92)(83\ 88\ 98\ 93)(84\ 89\ 99\ 94)(85\ 90\ 100\ 95) \\
& (106\ 111\ 121\ 116)(107\ 112\ 122\ 117)(108\ 113\ 123\ 118)(109\ 114\ 124\ 119)(110\ 115\ 125\ 120).
\end{aligned}
$$

Moreover $B_1 = \langle x_3, h_3 \rangle$ and $B_2 = \langle x_2, h_2, x_3, h_3 \rangle$.
For any choice of the parameters k, q, e and i, we shall build the subgroup $Q(k, q, \alpha_q, i)$ using the definition and shall derive the subgroup $Q(k, q, e, i)$, for $e < \alpha_q$, by taking the Frattini subgroup of $Q(k, q, e+1, i)$. Also each $Q(k, q, e, i)$ will be described in terms of the element $w(k, q, e, i)$ such that $Q(k, q, e, i) = \langle w(k, q, e, i) \rangle^{B_{n-k}}$.
Since $p - 1 = 2^2$, we have that $q = 2$ and $\alpha_q = 2$ and so, as $n = 3$, the choices for the parameters k, e and i are as follows: $k = 1, 2, 3$; $e = 1, 2$; $i = 0, 1, 2$ and $k + i \leq 3$. Then

$$
\begin{aligned}
Z(1,2,2) = \langle y_1 \rangle^{B_2} = {} & \langle (2\ 3\ 5\ 4) \rangle \times \langle (7\ 8\ 10\ 9) \rangle \times \langle (12\ 13\ 15\ 14) \rangle \times \langle (17\ 18\ 20\ 19) \rangle \times \\
& \langle (22\ 23\ 25\ 24) \rangle \times \langle (27\ 28\ 30\ 29) \rangle \times \langle (32\ 33\ 35\ 34) \rangle \times \langle (37\ 38\ 40\ 39) \rangle \times \\
& \langle (42\ 43\ 45\ 44) \rangle \times \langle (47\ 48\ 50\ 49) \rangle \times \langle (52\ 53\ 55\ 54) \rangle \times \langle (57\ 58\ 60\ 59) \rangle \times \\
& \langle (62\ 63\ 65\ 64) \rangle \times \langle (67\ 68\ 70\ 69) \rangle \times \langle (72\ 73\ 75\ 74) \rangle \times \langle (77\ 78\ 80\ 79) \rangle \times \\
& \langle (82\ 83\ 85\ 84) \rangle \times \langle (87\ 88\ 90\ 89) \rangle \times \langle (92\ 93\ 95\ 94) \rangle \times \langle (97\ 98\ 100\ 99) \rangle \times \\
& \langle (102\ 103\ 105\ 104) \rangle \times \langle (107\ 108\ 110\ 109) \rangle \times \langle (112\ 113\ 115\ 114) \rangle \times \\
& \langle (117\ 118\ 120\ 119) \rangle \times \langle (122\ 123\ 125\ 124) \rangle = L_1, \\
Z(2,2,2) = \langle y_2 \rangle^{B_1} = {} & \langle (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20) \rangle \times \\
& \langle (31\ 36\ 46\ 41)(32\ 37\ 47\ 42)(33\ 38\ 48\ 43)(34\ 39\ 49\ 44)(35\ 40\ 50\ 45) \rangle \times \\
& \langle (56\ 61\ 71\ 66)(57\ 62\ 72\ 67)(58\ 63\ 73\ 68)(59\ 64\ 74\ 69)(60\ 65\ 75\ 70) \rangle \times \\
& \langle (81\ 86\ 96\ 91)(82\ 87\ 97\ 92)(83\ 88\ 98\ 93)(84\ 89\ 99\ 94)(85\ 90\ 100\ 95) \rangle \times \\
& \langle (106\ 111\ 121\ 116)(107\ 112\ 122\ 117)(108\ 113\ 123\ 118) \\
& \quad (109\ 114\ 124\ 119)(110\ 115\ 125\ 120) \rangle = L_2, \\
Z(3,2,2) = \langle y_3 \rangle = L_3. &
\end{aligned}
$$

Therefore we have

$$\begin{aligned}
w(1,2,2,0) &= h_1,\\
w(1,2,2,1) &= (2\ 3\ 5\ 4)(7\ 8\ 10\ 9)(12\ 13\ 15\ 14)(17\ 18\ 20\ 19)(22\ 23\ 25\ 24)\\
&\quad (27\ 29\ 30\ 28)(32\ 34\ 35\ 33)(37\ 39\ 40\ 38)(42\ 44\ 45\ 43)(47\ 49\ 50\ 48),\\
w(1,2,2,2) &= (2\ 3\ 5\ 4)(7\ 9\ 10\ 8),\\
w(2,2,2,0) &= h_2,\\
w(2,2,2,1) &= (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20)\\
&\quad (31\ 41\ 46\ 36)(32\ 42\ 47\ 37)(33\ 43\ 48\ 38)(34\ 44\ 49\ 39)(35\ 45\ 50\ 40),\\
w(3,2,2,0) &= h_3
\end{aligned}$$

and, by taking the square of each of those, we get

$$\begin{aligned}
w(1,2,1,0) &= h_1^2,\\
w(1,2,1,1) &= (2\ 5)(3\ 4)(7\ 10)(8\ 9)(12\ 15)(13\ 14)(17\ 20)(18\ 19)(22\ 25)(23\ 24)\\
&\quad (27\ 30)(28\ 29)(32\ 35)(33\ 34)(37\ 40)(38\ 39)(42\ 45)(43\ 44)(47\ 50)(48\ 49),\\
w(1,2,1,2) &= (2\ 5)(3\ 4)(7\ 10)(8\ 9),\\
w(2,2,1,0) &= h_2^2,\\
w(2,2,1,1) &= (6\ 21)(7\ 22)(8\ 23)(9\ 24)(10\ 25)(11\ 16)(12\ 17)(13\ 18)(14\ 19)(15\ 20)\\
&\quad (31\ 46)(32\ 47)(33\ 48)(34\ 49)(35\ 50)(36\ 41)(37\ 42)(38\ 43)(39\ 44)(40\ 45),\\
w(3,2,1,0) &= h_3^2.
\end{aligned}$$

Finally, $D_0 = D_{2,0} = \langle h_1, h_2, h_3 \rangle$, $D_1 = D_{2,1} = \langle \langle w(1,2,2,1) \rangle^{B_2}, \langle w(2,2,2,1) \rangle^{B_1} \rangle$ and $D_2 = D_{2,2} = \langle w(1,2,2,2) \rangle^{B_2} = Q(1,2,2,2)$. ■

We shall now illustrate some properties of the subgroups $Q(k,q,e,i)$, $D_{q,i}$ and D_i. We start by looking at the relation between these subgroups and the normalizer in G of S_{n-i}.

Lemma 10.1.2. *Let $i = 0, \ldots, n-1$. Then, for all $k = 1, \ldots, n-i$, $q \in \pi(p-1)$ and $e = 1, \ldots, \alpha_q$, the subgroup $Q(k,q,e,i)$ is contained in the base group K_{n-i} of $N_G(S_{n-i})$. In particular, $Q(k,q,e,i)$ normalizes S_{n-i}.*

Proof. By Lemma 5.2.8, we have that $K_{n-i} \cap L_{n-i} = L_{n-i} = \langle y_{n-i} \rangle^{B_i}$ and so $Q(n-i, q, e, i) \leqslant L_{n-i} \leqslant K_{n-i}$. Also

$$K_{n-i} \cap L_k = (F_n \circ \cdots \circ F_{n-i+1})(\langle (f_{n-i} \circ \cdots \circ f_{k+1})(y_k) \rangle)$$

and from the definition we know that, for $k = 1, \dots, n-i-1$,

$$w(k, q, e, i) = (f_{n-i} \circ \cdots \circ f_{k+1})(z_1)((f_{n-i} \circ \cdots \circ f_{k+1})(z_1)^{-1})^{x_{n-i+1}},$$

with $z_1 = y_k^{(p-1)/q^e}$. Therefore $w(k, q, e, i) \in K_{n-i} \cap L_k$ and $Q(k, q, e, i)$ is equal to the normal closure in B_{n-k} of a subgroup of $K_{n-i} \cap L_k$. Then, since $B_{n-k} \leqslant B \leqslant N_G(S_{n-i})$ and K_{n-i} is a normal subgroup of $N_G(S_{n-i})$, we have that $Q(k, q, e, i) \leqslant K_{n-i}$. □

Corollary 10.1.3. *Let $i = 0, \dots, n-1$. Then $D_{q,i}$ is contained in the base group of $N_G(S_{n-i})$, for all $q \in \pi(p-1)$. In particular, $D_{q,i} \leqslant N_G(S_{n-i})$ and $D_{q,i}$ is abelian. Furthermore*

$$D_{q,i} = Q(1, q, \alpha_q, i) \times \cdots \times Q(n-i, q, \alpha_q, i).$$

Proof. By definition, $D_{q,i}$ is generated by the subgroups $Q(k, q, \alpha_q, i)$, for $k = 1, \dots, n-i$, and so from Lemma 10.1.2 it follows that $D_{q,i} \leqslant K_{n-i} \leqslant N_G(S_{n-i})$. In particular, since $D_{q,i}$ is a q-group, we have that $D_{q,i}$ is contained in a Hall p'-subgroup of K_{n-i} and so, by Corollary 5.2.7, we can conclude that $D_{q,i}$ is abelian. Moreover, since $L_k \cap \langle L_h \mid h \neq k \rangle = 1$, we also have that

$$Q(k, q, \alpha_q, i) \cap \langle Q(h, q, \alpha_q, i) \mid h \neq k \rangle = 1$$

and so $D_{q,i}$ is the direct product of the subgroups $Q(k, q, \alpha_q, i)$, for $k = 1, \dots, n-i$. □

Corollary 10.1.4. *For all $i = 0, \dots, n-1$, the subgroup D_i is contained in the base group of $N_G(S_{n-i})$. In particular, $D_i \leqslant N_G(S_{n-i})$ and D_i is abelian. Furthermore D_i is equal to the direct product of the subgroups $D_{q,i}$, for all $q \in \pi(p-1)$.*

Proof. By definition, D_i is generated by the subgroups $D_{q,i}$, for all $q \in \pi(p-1)$. Thus, by Corollary 10.1.3, $D_i \leqslant K_{n-i} \leqslant N_G(S_{n-i})$ and, in particular, D_i is contained in a Hall p'-subgroup of K_{n-i}. So D_i is abelian. Furthermore

$$D_{q,i} \cap \langle D_{r,i} \mid r \in \pi(p-1), r \neq q \rangle = 1$$

and so D_i is the direct product of the subgroups $D_{q,i}$, for all $q \in \pi(p-1)$. □

Proposition 10.1.5. *Let $i = 1, \dots, n-1$ and $j < i$. Then, $D_{q,j}$ is contained in $N_G(S_{n-i})$, for all $q \in \pi(p-1)$.*

Proof. Let $i = 1, \dots, n-1$ and $q \in \pi(p-1)$. Suppose that $j < i$ and let $k = 1, \dots, n-i$. Then, by Lemma 5.2.8, $K_{n-j} \cap L_k \leqslant K_{n-i} \cap L_k$ and so Lemma 10.1.2 implies that $Q(k, q, \alpha_q, j) \leqslant K_{n-i} \leqslant N_G(S_{n-i})$. Now let $n-i < k \leq n-j$. Then $Q(k, q, \alpha_q, j) \leqslant L_k \leqslant H_i$ and, since $S_{n-i} = \langle x_1, \dots, x_{n-i}\rangle^{H_i}$, we have that $Q(k, q, \alpha_q, j)$ normalizes S_{n-i}. Hence $D_{q,j} \leqslant N_G(S_{n-i})$. $\square$

Proposition 10.1.6. *Let $i = 1, \dots, n-1$. Then the subgroup*

$$\langle D_i, D_j \cap L_k \mid j < i, k = 1, \dots, n-i\rangle$$

is abelian. In particular, D_i and $\langle h_1, \dots, h_{n-i}\rangle$ commute.

Proof. Let $i = 1, \dots, n-1$ and let $j < i$. Then $D_i \leqslant K_{n-i}$ and, by Lemma 5.2.8, $D_j \cap L_k \leqslant K_{n-j} \cap L_k \leqslant K_{n-i}$, for all $k = 1, \dots, n-i$. Therefore $\langle D_i, D_j \cap L_k \mid j < i, k = 1, \dots, n-i\rangle$ is all contained in K_{n-i} and, in particular, in a Hall p'-subgroup of K_{n-i}. Then Corollary 5.2.7 implies that $\langle D_i, D_j \cap L_k \mid j < i, k = 1, \dots, n-i\rangle$ is abelian. Finally notice that $D_0 \cap L_k = \langle h_k\rangle$ and so, in particular, D_i and $\langle h_1, \dots, h_{n-i}\rangle$ commute. $\square$

Proposition 10.1.7. *Let $i = 0, \dots, n-1$ and $j > i$. Then, for all $k = 1, \dots, n-j$, $q \in \pi(p-1)$ and $e = 1, \dots, \alpha_q$, $K_{n-i} \cap Q(k, q, e, j) = 1$. In particular, $(K_{n-i} \cap L_k) \cap D_{q,j} = 1$.*

Proof. Let $i = 0, \dots, n-1$, $j > i$ and $k = 1, \dots, n-j$. Let $q \in \pi(p-1)$ and $e = 1, \dots, \alpha_q$ and set $Q_j = Q(k, q, e, j)$. Let $x \in Q_j \cap K_{n-i} \leqslant Q_j S_{n-j} \cap K_{n-i}$ and suppose that x has order q. Then, since $Q_j S_{n-j} \cap K_{n-i}$ is B-invariant, it follows that $\Omega_1(Q_j) \leqslant Q_j S_{n-j} \cap K_{n-i}$.
Now look at the commutator subgroup $[S_{n-i}, \Omega_1(Q_j) S_{n-j}]$. For $j > i$, we have that $S_{n-j} \leqslant S_{n-i}$ and so, since $\Omega_1(Q_j) \leqslant K_{n-i}$, it follows that $[S_{n-i}, \Omega_1(Q_j) S_{n-j}] \leqslant S_{n-i}$. But, $S_{n-i} \leqslant B$ and $\Omega_1(Q_j) S_{n-j}$ is B-invariant. So we also have $[S_{n-i}, \Omega_1(Q_j) S_{n-j}] \leqslant \Omega_1(Q_j) S_{n-j}$, that is,

$$[S_{n-i}, \Omega_1(Q_j) S_{n-j}] \leqslant S_{n-i} \cap \Omega_1(Q_j) S_{n-j} = S_{n-j}.$$

Hence S_{n-i}/S_{n-j} centralizes $\Omega_1(Q_j) S_{n-j}/S_{n-j} \cong \Omega_1(Q_j)$, which is a contradiction, since, for $n-j < n-i$, $x_{n-j+1} \in S_{n-i} \setminus S_{n-j}$ and x_{n-j+1} does not centralize Q_j. $\square$

Proposition 10.1.8. *Let $k = 1, \dots, n-1$, $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 0, \dots, n-k$. Then $Q(k, q, e, i)$ is normalized by B modulo S_k. In particular, $Q(k, q, e, i)B$ is a group.*

Proof. By definition, $Q(k, q, e, i)$ is equal to the normal closure in B_{n-k} of some subgroup of L_k and so $Q(k, q, e, i)$ is normalized by B_{n-k}. Also, by Proposition 10.1.6, $Q(k, q, e, i)$ is centralized by $\langle h_1, \ldots, h_k \rangle$ and so $Q(k, q, e, i)$ is normalized by $\langle h_1, \ldots, h_k \rangle B_{n-k}$. But, since $Q(k, q, e, i) \leqslant L_k \leqslant J_k$ and $O_p(J_k) = S_k$, $Q(k, q, e, i)$ normalizes S_k and so we can conclude that $Q(k, q, e, i)S_k$ is normalized by B. In particular, it follows that $Q(k, q, e, i)S_k B = Q(k, q, e, i)B$ is a group. $\square$

Proposition 10.1.9. *Let $q \in \pi(p-1)$ and $i = 0, \ldots, n-1$. Then $D_{q,i}S_{n-i}$ is a B-invariant subgroup of H. In particular, $D_{q,i}B$ is a group.*

Proof. For $k = 1, \ldots, n-i$, $Q(k, q, \alpha_q, i)$ is normalized by $\langle h_1, \ldots, h_{n-i} \rangle B_i$. Therefore, since $D_{q,i}$ is the direct product of the subgroups $Q(k, q, \alpha_q, i)$, it follows that $D_{q,i}$ is also normalized by $\langle h_1, \ldots, h_{n-i} \rangle B_i$ and so $D_{q,i}S_{n-i}$ is B-invariant. In particular, $D_{q,i}S_{n-i}B = D_{q,i}B$ is a group. $\square$

Proposition 10.1.10. *Let $i = 1, \ldots, n-1$, $q \in \pi(p-1)$, $e = 1, \ldots, \alpha_q$ and $k = 1, \ldots, n-i$. Then, for all $j < i$, $Q(k, q, e, i)$ is normalized by D_j. In particular, D_i and D_j permute, for all $i, j = 0, \ldots, n-1$.*

Proof. Let $i = 1, \ldots, n-1$ and let $j < i$. Then, by Proposition 10.1.6, $Q(k, q, e, i)$ is centralized by $D_j \cap L_h$, for all $h = 1, \ldots, n-i$. Moreover, for $h > n-i$, $D_j \cap L_h \leqslant H_{n-k}$ and so $D_j \cap L_h$ normalizes $Q(k, q, e, i)$, since, by Corollary 2.6.5, $Q(k, q, e, i)$ is equal to the normal closure in H_{n-k} of some subgroup of L_k. Hence $Q(k, q, e, i)$ is normalized by the whole D_j. In particular, D_i is normalized by D_j and so D_i and D_j permute, for all $i, j = 0, \ldots, n-1$. $\square$

Lemma 10.1.11. *Let $i = 0, \ldots, n-1$, $q \in \pi(p-1)$, $e = 1, \ldots, \alpha_q$ and $k = 1, \ldots, n-i$. Set $B_0 = \{1\}$ and write $Q(k, q, e, i) = \langle w(k, q, e, i) \rangle^{B_{n-k}}$. Then $Q(k, q, e, i) = \langle w(k, q, e, i) \rangle^{B_i}$. In particular, $Q(k, q, e, i)$ and $Q(h, q, e, i)$ are isomorphic as B_i-groups, for all $h, k = 1, \ldots, n-i$.*

Proof. Write $Q(k, q, e, i) = \langle w(k, q, e, i) \rangle^{B_{n-k}}$. We want to show that the action by conjugation of B_{n-k} on $Q(k, q, e, i)$ reduces to the action of B_i. So let us start by factorizing B_{n-k} in terms of B_i. First recall that

$$B_{n-k} = \langle x_{k+1}, \ldots, x_n \rangle \rtimes \langle h_{k+1}, \ldots, h_n \rangle$$

and that $B_i = \langle x_{n-i+1}, \dots, x_n \rangle \rtimes \langle h_{n-i+1}, \dots, h_n \rangle \leqslant B_{n-k}$. Therefore we can write

$$B_{n-k} = (S \rtimes \langle h_{k+1}, \dots, h_{n-i} \rangle) \rtimes B_i,$$

with $S = \langle x_{k+1}, \dots, x_{n-i} \rangle^{B_i} \cong S_{n-i}/S_k$. We shall now look at the action of the subgroups S and $\langle h_{k+1}, \dots, h_{n-i} \rangle$ on $Q(k,q,e,i)$. Since $S \leqslant B_{n-k}$, we have that S normalizes $Q(k,q,e,i)$. But, $S \leqslant S_{n-i}$ and $Q(k,q,e,i) \leqslant N_G(S_{n-i})$. Therefore we can conclude that

$$[Q(k,q,e,i), S] \leqslant Q(k,q,e,i) \cap S_{n-i} = 1$$

and so S centralizes $Q(k,q,e,i)$. Moreover, by Proposition 10.1.6, also $\langle h_{k+1}, \dots, h_{n-i} \rangle$ centralizes $Q(k,q,e,i)$ and so we get that $Q(k,q,e,i) = \langle w(k,q,e,i) \rangle^{B_i}$.
Now let $h = 1, \dots, n-i$ and write $Q(h,q,e,i) = \langle w(h,q,e,i) \rangle^{B_i}$. Recall from the definition that

$$w(k,q,e,i) = (z_1 \dots z_{p^{n-k-i}})(z_{p^{n-k-i}+1} \dots z_{2p^{n-k-i}})^{-1},$$
$$w(h,q,e,i) = (z'_1 \dots z'_{p^{n-h-i}})(z'_{p^{n-h-i}+1} \dots z'_{2p^{n-h-i}})^{-1},$$

where $z_1, \dots, z_{p^{n-k}}$ are the generators of $Z(k,q,e)$ and $z'_1, \dots, z'_{p^{n-h}}$ are the generators of $Z(h,q,e)$. Then the map

$$w(k,q,e,i) \longmapsto w(h,q,e,i)$$

defines a B_i-isomorphism between $Q(k,q,e,i)$ and $Q(h,q,e,i)$. □

Lemma 10.1.12. *Let $i = 0, \dots, n-1$ and set $B_0 = \{1\}$. Then, for all $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $k = 1, \dots, n-i$, the group $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ is isomorphic as a $GF(q)B_i$-module to the module $V_{i,i}$ defined at the beginning of Section 8.2. In particular, $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ is an absolutely irreducible $GF(q)B_i$-module.*

Proof. According to Lemma 10.1.11, write $Q(k,q,e,i) = \langle w_k \rangle^{B_i}$, with

$$w_k = w(k,q,e,i) = (z_1 \dots z_{p^{n-k-i}})(z_{p^{n-k-i}+1} \dots z_{2p^{n-k-i}})^{-1},$$

where $z_1, \dots, z_{2p^{n-k-i}}$ are some of the generators of $Z(k,q,e)$. Then $\Phi(Q(k,q,e,i)) = \langle w_k^q \rangle^{B_i}$ and

$$Q(k,q,e,i)/\Phi(Q(k,q,e,i)) \cong \langle w_k^{q^{e-1}} \rangle^{B_i}.$$

Also recall from Section 8.2 that $V_{i,i} = \langle (v_1 - v_2)^{B_i} \rangle$, where v_1 and v_2 are elements of a basis of V_i, with V_i $\mathrm{GF}(q)B_i$-module of dimension p^i over $\mathrm{GF}(q)$. Then the map

$$w_k^{q^{e-1}} \longmapsto v_1 - v_2$$

induces a B_i-isomorphism between the $\mathrm{GF}(q)B_i$-modules $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ and $V_{i,i}$, where, by Lemma 8.2.3, $V_{i,i}$ is an absolutely irreducible $\mathrm{GF}(q)B_i$-module. □

Corollary 10.1.13. *Let $k = 1, \dots, n$, $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 0, \dots, n-k$. Then $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ is isomorphic as a $GF(q)B_{n-k}$-module to $V_{i,n-k}$.*

Proof. Write $Q(k,q,e,i) = \langle w_k \rangle^{B_i}$, with $w_k = (z_1 \dots z_{p^{n-k-i}})(z_{p^{n-k-i}+1} \dots z_{2p^{n-k-i}})^{-1}$ and recall from Section 8.2 that $V_{i,n-k} = \langle v^{B_{n-k}} \rangle$, with

$$v = (v_1 + \cdots + v_{p^{n-k-i}}) - (v_{p^{n-k-i}+1} + \cdots + v_{2p^{n-k-i}}),$$

where $v_1, \dots, v_{2p^{n-k-i}}$ are elements of a basis of V_{n-k} and V_{n-k} is a $\mathrm{GF}(q)B_{n-k}$-module of dimension p^{n-k} over $\mathrm{GF}(q)$. Then the map $w_k^{q^{e-1}} \mapsto v$ defines a B_{n-k}-isomorphism between the B_{n-k}-modules $Q(k,q,e,i)/\Phi(Q(k,q,e,i))$ and $V_{i,n-k}$. □

Corollary 10.1.14. *Let $k = 1, \dots, n$. Then*

$$L_k = \prod_{q \in \pi(p-1)} (Q(k,q,\alpha_q,0) \times \cdots \times Q(k,q,\alpha_q,n-k)).$$

In particular, $L_1 L_2 \dots L_n = D_0 D_1 \dots D_{n-1}$ and $H = T D_0 D_1 \dots D_{n-1}$.

Proof. We shall first show that, for $q \in \pi(p-1)$,

$$O_q(L_k) = Q(k,q,\alpha_q,0) \times \cdots \times Q(k,q,\alpha_q,n-k).$$

Since L_k is a homocyclic group of order $(p-1)^{p^{n-k}}$, we have that $O_q(L_k)$ is a homocyclic q-group of order $(q^{\alpha_q})^{p^{n-k}}$ and so $O_q(L_k)/\Phi(O_q(L_k))$ is an elementary abelian q-group of order $q^{p^{n-k}}$. Let V_{n-k} be a $\mathrm{GF}(q)B_{n-k}$-module of dimension p^{n-k} over $\mathrm{GF}(q)$. Then $V_{n-k} \cong O_q(L_k)/\Phi(O_q(L_k))$ as $\mathrm{GF}(q)B_{n-k}$-modules and, by Theorem 8.2.5, $V_{n-k} = V_{0,n-k} \oplus \cdots \oplus V_{n-k,n-k}$, where the submodules $V_{i,n-k}$ are defined as in Section 8.2. But, by Corollary 10.1.13, for all $i = 0, \dots, n-k$,

$$V_{i,n-k} \cong Q(k,q,\alpha_q,i)/\Phi(Q(k,q,\alpha_q,i)) \cong Q(k,q,\alpha_k,i)\Phi(O_q(L_k))/\Phi(O_q(L_k)),$$

as $\mathrm{GF}(q)B_{n-k}$-modules. Hence we have that

$$O_q(L_k)/\Phi(O_q(L_k)) = \prod_{i=0}^{n-k} Q(k,q,\alpha_k,i)\Phi(O_q(L_k))/\Phi(O_q(L_k)),$$

which implies that

$$O_q(L_k) = \Phi(O_q(L_k)) \prod_{i=0}^{n-k} Q(k,q,\alpha_k,i) = \prod_{i=0}^{n-k} Q(k,q,\alpha_k,i).$$

Then the result follows from being $L_k = \prod_{q\in\pi(p-1)} O_q(L_k)$. $\square$

One last piece of notation to introduce and we shall be able to start our investigation of the minimal parabolic subgroups of H with respect to B.

Let $i = 1,\dots,n-1$ and $q \in \pi(p-1)$. According to Lemma 10.1.11, let $A(q,i)$ denote a q-group such that $B_i \leqslant \mathrm{Aut}(A(q,i))$ and $A(q,i) \cong Q(k,q,\alpha_q,i)$ as B_i-groups, for all $k = 1,\dots,n-i$. Then $A(q,i)$ is a homocyclic q-group of exponent q^{α_q} and, by Lemma 10.1.12, $A(q,i)/\Phi(A(q,i)) \cong V_{i,i}$ is an absolutely irreducible $\mathrm{GF}(q)B_i$-module. Also $D_{q,i}$ is the direct product of $n-i$ copies of $A(q,i)$.

Recall that, by Proposition 1.3.11, a B_i-subgroup R of $A(q,i)$ is equal to some term of the Frattini series of $A(q,i)$. In particular, if $R = \Phi^e(A(q,i))$, $e = 1,\dots,\alpha_q$, then R is B_i-isomorphic to the quotient $A(q,i)/\Phi^{\alpha_q-e}(A(q,i))$.

Denote by $\mathcal{R}_{q,i}$ the collection of all B_i-subgroups R of $D_{q,i}$ such that R is B_i-isomorphic to a nontrivial quotient of $A(q,i)$ and by $\mathcal{R}$ the union of all the sets $\mathcal{R}_{q,i}$, for $q \in \pi(p-1)$ and $i = 1,\dots,n-1$. Notice that, for all $k = 1,\dots,n-i$ and $e = 1,\dots,\alpha_q$, $Q(k,q,e,i) \in \mathcal{R}_{q,i}$.

Proposition 10.1.15. *For all $R \in \mathcal{R}$, BR is a group.*

Proof. Suppose that $R \in \mathcal{R}_{q,i}$, for some $q \in \pi(p-1)$ and $i = 1,\dots,n-1$. Then $R \leqslant D_{q,i}$ and R is B_i-invariant. Thus, by Corollary 10.1.3 and by Proposition 10.1.6, R normalizes S_{n-i} and is centralized by $\langle h_1,\dots,h_{n-i}\rangle$. Therefore RS_{n-i} is B-invariant and $BRS_{n-i} = BR$ is a group. $\square$

Proposition 10.1.16. *Let $R \in \mathcal{R}_{q,i}$, for some $q \in \pi(p-1)$ and $i = 1,\dots,n-1$. Then $R/\Phi(R) \cong V_{i,i}$ as $GF(q)B_i$-modules.*

Proof. Let $R \in \mathcal{R}_{q,i}$, with $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Then R is B_i-isomorphic to a nontrivial quotient of $A(q,i)$, say,

$$R \cong A(q,i)/\Phi^{\alpha_q - e}(A(q,i)) \cong \Phi^e(A(q,i)),$$

for some $e = 1, \dots, \alpha_q$. Then, by Corollary 1.3.10,

$$R/\Phi(R) \cong \Phi^e(A(q,i))/\Phi^{e+1}(A(q,i)) \cong A(q,i)/\Phi(A(q,i)) \cong V_{i,i}$$

as $\mathrm{GF}(q)B_i$-modules. □

10.2 Soluble minimal parabolic subgroups

In this section we shall describe all minimal parabolic subgroups of H with respect to B, that is, by Lemma 6.7.6, all minimal parabolic subgroups of G with respect to B which are soluble. We shall first determine all minimal parabolic subgroups of J_k with respect to B, for $k = 1, \dots, n-1$. Recall that $H = J_1 \dots J_{n-1}$.

By Proposition 10.1.8, we can define the subgroup $P(k,q,e,i)$ of J_k by

$$P(k,q,e,i) = BQ(k,q,e,i).$$

Notice that $P(k,q,e,i) = \langle B, z \rangle$, for all $z \in L_k$ such that $Q(k,q,e,i) = \langle z \rangle^{B_{n-k}}$. In particular, $P(k,q,e,i) = \langle B, w(k,q,e,i) \rangle$.

Theorem 10.2.1. *Let $k = 1, \dots, n-1$. Then $P \in \mathcal{M}(J_k, B)$ if and only if $P = P(k,q,e,i)$, for some $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 1, \dots, n-k$. Moreover the unique maximal subgroup of $P(k,q,e,i)$ containing B is given by $P(k,q,e-1,i)$.*

Proof. Let $k = 1, \dots, n-1$. Set $Q = Q(k,q,e,i)$ and $P = P(k,q,e,i) = BQ$, with $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 1, \dots, n-k$. Set $R = S_k \rtimes Q$. Then $P = BR$ and, by Proposition 10.1.8, $R \trianglelefteq P$. Also $R/O_p(R) = R/S_k \cong Q$ and so

$$Q/\Phi(Q) \cong \frac{R/O_p(R)}{\Phi(R/O_p(R))} = \frac{R/O_p(R)}{\Phi_p(R)/O_p(R)} \cong R/\Phi_p(R),$$

as $\mathrm{GF}(q)B_i$-modules, since both groups are B_i-invariant. But, by Lemma 10.1.12, $Q/\Phi(Q)$ is an irreducible $\mathrm{GF}(q)B_i$-module. Therefore so is $R/\Phi_p(R)$ and, in particular, $R/\Phi_p(R)$ has no nontrivial proper B_i-subgroup. Hence $R/\Phi_p(R)$ has no nontrivial proper B-subgroup. Then, by Proposition 1.4.15, we have that $P \in \mathcal{M}(J_k, B)$ and the subgroup

$$B\Phi_p(R) = BS_k\Phi(Q) = BQ(k, q, e-1, i)$$

is the unique maximal subgroup of P containing B.

Conversely, let $P \in \mathcal{M}(J_k, B)$. We shall first consider the case when $k = 1$. So suppose that $P \leqslant J_1 = C_1 \rtimes B_{n-1}$, with $C_1 = S_1 \rtimes L_1$. By Dedekind's Modular Law, we have that

$$P = P \cap J_1 = P \cap (C_1 \rtimes B_{n-1}) = (P \cap C_1) \rtimes B_{n-1}.$$

In particular, $P = (P \cap C_1)B$, where $P \cap C_1 \trianglelefteq P$. We want to show that $(P \cap C_1)/O_p(P \cap C_1)$ is nilpotent. Clearly, $O_p(P \cap C_1) = O_p(C_1) = S_1$. Therefore

$$(P \cap C_1)/O_p(P \cap C_1) \leqslant C_1/O_p(C_1) = C_1/S_1 \cong L_1$$

and, since L_1 is abelian, we have that $(P \cap C_1)/O_p(P \cap C_1)$ is nilpotent. Then Proposition 1.4.14 implies that

$$P = O_{p,q}(P \cap C_1)B,$$

for some uniquely determined $q \in \pi(P \cap C_1) \setminus \{p\}$. Set $P_q = O_{p,q}(P \cap C_1)$. Then $P_q \trianglelefteq P$ and $P = P_qB$. Also $P_q \cap T = S_1$ and $P_q \cap B = S_1 \rtimes D$, where $D = O_q(\langle h_1 \rangle)$.

Take quotients modulo S_1 and denote the images by bars. Then, by Lemma 1.4.7, $\bar{P}$ is a minimal parabolic subgroup of $\bar{J}_1$ with respect to $\bar{B}$. Also $\bar{P} = \bar{P}_q\bar{B}$, with $\bar{P}_q \cap \bar{B} = \bar{D}$ and $\bar{P}_q \trianglelefteq \bar{P}$. Next step is to produce a factorization of $\bar{P}$ as $\bar{R} \rtimes \bar{B}$, for some $\bar{R} \leqslant \bar{P}_q$.

Since $S_1 = O_p(P \cap C_1) = O_p(C_1)$, we have that

$$\bar{P}_q = O_{p,q}(P \cap C_1)/S_1 = O_q(\overline{P \cap C_1}) \leqslant O_q(\bar{C}_1) \cong O_q(L_1).$$

Therefore $\bar{P}_q$ is an abelian q-group. But $\bar{T}$ is a p-group acting on $\bar{P}_q$ by conjugation and $(q, p) = 1$. Hence, by [1, 24.6], we have that

$$\bar{P}_q = [\bar{P}_q, \bar{T}] \times C_{\bar{P}_q}(\bar{T}),$$

which implies that

$$\bar{P} = \bar{P}_q\bar{B} = [\bar{P}_q, \bar{T}]C_{\bar{P}_q}(\bar{T})\bar{B} = [\bar{P}_q, \bar{T}]\bar{B},$$

since $C_{\bar{P}_q}(\bar{T}) \leqslant N_{\bar{P}_q}(\bar{T}) \leqslant N_{\bar{P}}(\bar{T}) = \bar{B}$. Set $\bar{R} = [\bar{P}_q, \bar{T}] \leqslant \bar{P}_q$. Then $\bar{R} \trianglelefteq \bar{P}$ and $\bar{R} \cap \bar{B} = \bar{R} \cap \bar{P}_q \cap \bar{B} = \bar{R} \cap \bar{D}$. But, since, by Lemma 5.2.1, B_{n-1} centralizes $\langle h_1 \rangle$, we have that $[D, B] \leqslant S_1$ and so $[D, T] \leqslant S_1$. Thus $\bar{D} \leqslant C_{\bar{P}_q}(\bar{T})$ and $\bar{R} \cap \bar{D} = 1$. Therefore $\bar{R} \cap \bar{B} = 1$ and

$$\bar{P} = \bar{R} \rtimes \bar{B}.$$

We shall now concentrate our attention on the subgroup $\bar{R}$. Set $\bar{Z} = \bar{Z}_{\alpha_q} = O_q(\bar{C}_1)$ and $\bar{Z}_s = \Phi(\bar{Z}_{s+1})$, for $s = 0, \ldots, \alpha_q - 1$. Recall that $\bar{Z}$ is a homocyclic q-group of exponent q^{α_q} and order $(q^{\alpha_q})^{p^{n-1}}$. Since $\bar{R} \leqslant \bar{P}_q \leqslant \bar{Z}$, there exists e such that $\bar{R} \leqslant \bar{Z}_e$ and $\bar{R} \nleqslant \bar{Z}_{e-1}$, that is, $\bar{R}$ is an abelian q-group of exponent q^e.

Now $\bar{Z}_e/\bar{Z}_{e-1}$ is an elementary abelian $\bar{B}$-invariant q-group of order $q^{p^{n-1}}$. Thus it can be regarded as a $\mathrm{GF}(q)\bar{B}$-module of dimension p^{n-1} over $\mathrm{GF}(q)$, with $\bar{B}$ acting in the natural way. But, since $\bar{B} \cong \langle h_1 \rangle B_{n-1}$ and $h_1 \in L_1 \cong \bar{C}_1$, which is abelian, for a subgroup of $\bar{C}_1$ being B_{n-1}-invariant is the same as being $\bar{B}$-invariant. Therefore, from Theorem 8.2.5 it follows that

$$\bar{Z}_e/\bar{Z}_{e-1} \cong V_{0,n-1} \oplus V_{1,n-1} \oplus \cdots \oplus V_{n-1,n-1},$$

as $\mathrm{GF}(q)B_{n-1}$-modules, with $V_{i,n-1}$ defined as at the beginning of Section 8.2.

Set $\bar{R}_0 = \bar{R} \cap \bar{Z}_{e-1} = \{x \in \bar{R} \mid \ \mathrm{o}(x) \leq q^{e-1}\}$. Since $\Phi(\bar{R}) \leqslant \bar{R}_0$, $\bar{R}/\bar{R}_0$ is an elementary abelian q-group and

$$\bar{R}/\bar{R}_0 \cong \bar{R}\bar{Z}_{e-1}/\bar{Z}_{e-1} \leqslant \bar{Z}_e/\bar{Z}_{e-1}.$$

Hence $\bar{R}/\bar{R}_0$ is isomorphic to a $\mathrm{GF}(q)\bar{B}$-submodule of $\bar{Z}_e/\bar{Z}_{e-1}$ and so is isomorphic to the direct sum of some of the submodules $V_{i,n-1}$. If $\bar{R}/\bar{R}_0$ is isomorphic to the direct sum of more than one $V_{i,n-1}$, then there exist $\bar{R}_1$ and $\bar{R}_2$, proper $\bar{B}$-invariant subgroups of $\bar{R}$ containing $\bar{R}_0$, such that $\bar{R} = \langle \bar{R}_1, \bar{R}_2 \rangle$. But, by Proposition 1.4.12, this is a contradiction. Therefore it follows that $\bar{R}/\bar{R}_0 \cong V_{i,n-1}$, for some $i = 0, \ldots, n-1$, and $\bar{R}/\bar{R}_0$ is an irreducible $\mathrm{GF}(q)\bar{B}$-module. Moreover, by Corollary 10.1.13,

$$V_{0,n-1} \cong Q(1, q, e, 0)/\Phi(Q(1, q, e, 0)),$$

with $Q(1, q, e, 0) \leqslant \langle h_1 \rangle B_{n-1} \cong \bar{B}$, and so, since $\bar{R} \cap \bar{B} = 1$, we must have $i \neq 0$.

Next we show that $\bar{R} = \bar{Q}_1$, with $Q_1 = Q(1, q, e, i)$, which will prove the theorem for $k = 1$.

We shall use some information about the number of $\bar{B}$-composition factors of $\bar{R}$, and of $\bar{Q}_1$, which are isomorphic to $V_{i,n-1}$.

Now $\bar{Z}_e$ has exactly e $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$, one for each quotient of the form $\bar{Z}_s/\bar{Z}_{s-1}$, with $s = 1, \ldots, e$, since each of these quotients is isomorphic to $\bar{Z}_e/\bar{Z}_{e-1}$ and so to $V_{0,n-1} \oplus \cdots \oplus V_{n-1,n-1}$. In particular, since $\bar{R} \leqslant \bar{Z}_e$, it follows that $\bar{R}$ has at most e $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$.

On the other hand, by Proposition 1.3.9, we have that, for all $s = 1, \ldots, e-1$,

$$\bar{R}/\bar{R}_0 = \bar{R}/(\bar{R} \cap \bar{Z}_{e-1}) \cong \bar{R}^{q^s}/(\bar{R}^{q^s} \cap \bar{Z}_{e-1-s}),$$

as $\mathrm{GF}(q)\bar{B}$-modules, and so, since $\bar{R}/\bar{R}_0 \cong V_{i,n-1}$, $\bar{R}$ has at least e $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$. Hence $\bar{R}$ has exactly e $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$.

Consider the subgroup $\bar{Q}_1$, that is, Q_1S_1/S_1, where $Q_1 = Q(1, q, e, i)$. Since $\bar{Q}_1 \cong Q_1$, by Corollary 10.1.13, we have that $\bar{Q}_1$ is a homocyclic q-group such that $\bar{Q}_1/\Phi(\bar{Q}_1) \cong V_{i,n-1}$ and so $\bar{Q}_1$ has exactly e $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$, namely the factors of its Frattini series.

Now look at the group $\bar{Q}_1\bar{R}/\bar{R}$. Either $\bar{Q}_1\bar{R}/\bar{R} = 1$ or $\bar{Q}_1\bar{R}/\bar{R}$ has a $\bar{B}$-composition factor isomorphic to $V_{i,n-1}$. But $\bar{Q}_1\bar{R}/\bar{R} \leqslant \bar{Z}_e/\bar{R}$ and $\bar{Z}_e/\bar{R}$ has no $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$, since both $\bar{Z}_e$ and $\bar{R}$ have the same number of $\bar{B}$-composition factors isomorphic to $V_{i,n-1}$. Therefore it must be $\bar{Q}_1\bar{R}/\bar{R} = 1$, that is, $\bar{Q}_1 \leqslant \bar{R}$. But, since $\bar{R}/\bar{R}_0 \cong V_{i,n-1}$ and $V_{i,n-1}$ is an irreducible $\mathrm{GF}(q)\bar{B}$-module, $\bar{R}_0$ is a maximal $\bar{B}$-invariant subgroup of $\bar{R}$ and so $\bar{R}_0\bar{Q}_1 = \bar{R}$. Then Proposition 1.4.12 implies that $\bar{R} = \bar{Q}_1$ and so $\bar{P} = \bar{R} \rtimes \bar{B} = \bar{Q}_1 \rtimes \bar{B}$.

Then, back to the preimages, we get that

$$P = Q_1S_1B = Q_1B = Q(1, q, e, i)B = P(1, q, e, i)$$

and this completes the proof of the case $k = 1$.

Now suppose that $k > 1$. Then $P \leqslant J_k = A_{k-1} \rtimes (C_k \rtimes B_{n-k})$, with $C_k = \langle x_k^{B_{n-k}} \rangle \rtimes L_k$, and so, by Dedekind's Modular Law,

$$P = P \cap J_k = A_{k-1} \rtimes (P \cap C_kB_{n-k}).$$

By Lemma 1.4.7, P/A_{k-1} is a minimal parabolic subgroup of J_k/A_{k-1} with respect to B/A_{k-1}, that is, $P \cap C_kB_{n-k}$ is a minimal parabolic subgroup of C_kB_{n-k} with respect to B_{n-k+1}.

Hence the result proved above for $k=1$ implies that $P \cap C_k B_{n-k} = B_{n-k+1} Q_k$, with $Q_k = Q(k,q,e,i)$, for some $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 1, \dots, n-k$. Then

$$P = A_{k-1}(P \cap C_k B_{n-k}) = A_{k-1} B_{n-k+1} Q_k = BQ_k = P(k,q,e,i),$$

as required. $\square$

Using Theorem 10.2.1 as base of induction, we can now attack the general case.

Recall that, for $q \in \pi(p-1)$ and $i = 1, \dots, n-1$, $\mathcal{R}_{q,i}$ denotes the collection of all B_i-subgroups R of $D_{q,i}$ such that R is B_i-isomorphic to a nontrivial quotient of $A(q,i)$ and $\mathcal{R}$ is the union of all the sets $\mathcal{R}_{q,i}$.

Theorem 10.2.2. *$P \in \mathcal{M}(H,B)$ if and only if $P = BR$, for some $R \in \mathcal{R}$. Moreover, for $R \in \mathcal{R}$, the unique maximal subgroup of BR containing B is given by $B\Phi(R)$.*

Proof. Let $P = BR$, for some $R \in \mathcal{R}$, and suppose that $R \in \mathcal{R}_{q,i}$, for some $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Set $R_1 = S_{n-i} \rtimes R$. Then $P = BR = BR_1$ and $R_1 \trianglelefteq P$, since R is $\langle h_1, \dots, h_{n-i} \rangle B_i$-invariant. Moreover $R_1/O_p(R_1) = R_1/S_{n-i} \cong R$ and so

$$R/\Phi(R) \cong \frac{R_1/O_p(R_1)}{\Phi(R_1/O_p(R_1))} = \frac{R_1/O_p(R_1)}{\Phi_p(R_1)/O_p(R_1)} \cong R_1/\Phi_p(R_1),$$

as $\mathrm{GF}(q)B_i$-modules. But, since $R \in \mathcal{R}_{q,i}$, by Proposition 10.1.16, $R/\Phi(R) \cong V_{i,i}$. Therefore $R_1/\Phi_p(R_1) \cong V_{i,i}$, with $V_{i,i}$ irreducible $\mathrm{GF}(q)B_i$-module. So $R_1/\Phi_p(R_1)$ has no nontrivial proper B_i-subgroup and, in particular, $R_1/\Phi_p(R_1)$ has no nontrivial proper B-subgroup. Then, by Proposition 1.4.15, we can conclude that $P \in \mathcal{M}(H,B)$ and the subgroup

$$B\Phi_p(R_1) = BS_{n-i}\Phi(R) = B\Phi(R)$$

is the unique maximal subgroup of P containing B.

Conversely, let $P \in \mathcal{M}(H,B)$. Since $H = J_1 \dots J_{n-1}$, we can proceed by induction on the number t such that $P \leqslant J_{k_1} \dots J_{k_t}$, where $k_1, \dots, k_t \in \{1, \dots, n-1\}$ and $k_1 < k_2 < \dots < k_t$. For $t = 1$, Theorem 10.2.1 implies that $P = BQ(k_1, q, e, i)$, for some $q \in \pi(p-1)$, $e = 1, \dots, \alpha_q$ and $i = 1, \dots, n-k_1$, and so the result holds, since $Q(k_1, q, e, i) \in \mathcal{R}_{q,i} \subseteq \mathcal{R}$.

Let $t > 1$ and suppose first that $k_1 = 1$. Then

$$P \leqslant BL_1 L_{k_2} \dots L_{k_t} = C_1 \rtimes M,$$

where $M = B_{n-1}L_{k_2}\dots L_{k_t}$ and $C_1 = S_1 \rtimes L_1$. By Lemma 1.4.7, either $PC_1/C_1 = BC_1/C_1$ or PC_1/C_1 is isomorphic to a minimal parabolic subgroup of M with respect to B_{n-1}. If the former case applies, then $P \leqslant PC_1 = BC_1 = J_1$, against the assumption that $t > 1$. So PC_1/C_1 is isomorphic to a minimal parabolic subgroup of M with respect to B_{n-1} and the induction hypothesis implies that

$$PC_1/C_1 = BRC_1/C_1,$$

for some $R \in \mathcal{R}$ and $R \leqslant L_{k_2}\dots L_{k_t}$. Then $P \leqslant BRC_1 = BRL_1$ and, by Dedekind's Modular Law, we have that

$$P = P \cap (BRL_1) = B(P \cap RL_1).$$

Assume that $R \in \mathcal{R}_{q,i}$, for some $q \in \pi(p-1)$ and some $i = 1,\dots,n-1$. Then both B and R normalize S_{n-i}, since $R \leqslant D_{q,i} \leqslant N_G(S_{n-i})$. So $S_{n-i}L_1 \trianglelefteq BRL_1$ and $P \cap S_{n-i}L_1 \trianglelefteq P$. Then Lemma 1.4.6 implies that either $P = B(P \cap S_{n-i}L_1)$ or $T \cap P \cap S_{n-i}L_1 \trianglelefteq P$. If $P = B(P \cap S_{n-i}L_1)$, then $P \leqslant J_1$, against the assumption that $t > 1$. Hence we must have that $T \cap S_{n-i}L_1 \trianglelefteq P$, that is, $S_{n-i} \trianglelefteq P$.

Set $R_1 = P \cap (S_{n-i}RL_1) = S_{n-i}(P \cap RL_1)$. Then $R_1 \trianglelefteq P$, since $S_{n-i}RL_1$ is normalized by B, and

$$P = B(P \cap RL_1) = BR_1.$$

Also, since $S_{n-i} \trianglelefteq P$, we have that $O_p(R_1) = S_{n-i}$ and $R_1 \cap B = S_{n-i} \rtimes \langle h_1 \rangle$.

Consider the commutator subgroup $[B, R_1]$ and notice that, by Lemma 5.2.1, $h_1 \notin [B, R_1]$, since L_1H_{n-1} centralizes h_1. Also, by Proposition 1.1.9, we have that $P = B[B, R_1]$. Therefore, by replacing R_1 with $[B, R_1]$, we can assume that $P = BR_1$, with $R_1 \trianglelefteq P$ and $B \cap R_1 = S_{n-i}$.

Now $R_1 \leqslant S_{n-i}RL_1$ and so $R_1 = S_{n-i} \rtimes (R_1 \cap RL_1)$. Also $R_1 \cap RL_1 \leqslant R_1 \cap D_{q,i}L_1$ and, by Corollary 10.1.3, $R_1 \cap RL_1$ is contained in a Hall p'-subgroup of the base group K_{n-i} of $N_G(S_{n-i})$, which is, by Corollary 5.2.7, abelian. Therefore $R_1/O_p(R_1) = R_1/S_{n-i} \cong R_1 \cap RL_1$ is abelian and so nilpotent. Then, by Proposition 1.4.14,

$$P = BP_q,$$

with $P_q = O_{p,q}(R_1) \leqslant S_{n-i}RO_q(L_1)$ and so $P_q \trianglelefteq P$ and $P_q \cap B = S_{n-i}$. Recall that $O_q(L_1) = Q(1,q,\alpha_q,0) \times \cdots \times Q(1,q,\alpha_q,n-1)$. Also, by Propositions 10.1.5 and 10.1.7, $O_q(L_1) \cap N_G(S_{n-i}) = Q(1,q,\alpha_q,0) \times \cdots \times Q(1,q,\alpha_q,i)$, with $Q(k,q,e,0) \leqslant B$. Hence, as $P_q \leqslant P \leqslant N_G(S_{n-i})$ and $P_q \cap B = S_{n-i}$, we have that

$$P_q \leqslant S_{n-i}RQ(1,q,\alpha_q,1) \times \cdots \times Q(1,q,\alpha_q,i).$$

Consider the commutator subgroup $[S_{n-i+1}, P_q] \leqslant P_q$. For $j < i$, Proposition 10.1.5 implies that $Q(1,q,\alpha_q,j)$ is contained in $N_G(S_{n-i+1})$. Thus $[S_{n-i+1}, Q(1,q,\alpha_q,j)] \leqslant S_{n-i+1}$. Hence we have that $[S_{n-i+1}, P_q] \leqslant S_{n-i}RQ(1,q,\alpha_q,i)$.

Now take quotients modulo S_{n-i} and denote the images by bars. Then $\bar{P}_q = P_q/S_{n-i} \cong P_q \cap (RQ(1,q,\alpha_q,1) \times \cdots \times Q(1,q,\alpha_q,i))$ and so, by Proposition 10.1.6, $\bar{P}_q$ is abelian. Thus from [1, 24.6] it follows that

$$\bar{P}_q = [\bar{S}_{n-i+1}, \bar{P}_q] \times C_{\bar{P}_q}(\bar{S}_{n-i+1}),$$

with both $[\bar{S}_{n-i+1}, \bar{P}_q]$ and $C_{\bar{P}_q}(\bar{S}_{n-i+1})$ $\bar{B}$-invariant and $[\bar{S}_{n-i+1}, \bar{P}_q] \leqslant \overline{S_{n-i}RQ(1,q,\alpha_q,i)}$. Hence, since $\bar{P} = \bar{B}\bar{P}_q$, with $\bar{P}_q \cap \bar{B} = 1$, applying Proposition 1.4.12, we get that either $[\bar{S}_{n-i+1}, \bar{P}_q] = 1$ or $C_{\bar{P}_q}(\bar{S}_{n-i+1}) = 1$. Suppose that $[\bar{S}_{n-i+1}, \bar{P}_q] = 1$. Then $[S_{n-i+1}, P_q] = S_{n-i} \leqslant S_{n-i+1}$ and P_q normalizes S_{n-i+1}. But, by Proposition 10.1.7, $RQ(1,q,\alpha_q,i) \cap N_G(S_{n-i+1}) = 1$ and so we get that $P_q \leqslant S_{n-i}Q(1,q,\alpha_q,1) \times \cdots \times Q(1,q,\alpha_q,i-1) \leqslant S_{n-i}L_1$, against the assumption that $P = BP_q$ is not contained in J_1. Therefore $[\bar{S}_{n-i+1}, \bar{P}_q] \neq 1$ and we must have $C_{\bar{P}_q}(\bar{S}_{n-i+1}) = 1$, which implies that $\bar{P}_q = [\bar{S}_{n-i+1}, \bar{P}_q] \leqslant \overline{S_{n-i}RQ(1,q,\alpha_q,i)} \leqslant \bar{D}_{q,i}$. Thus $\bar{P}_q$ is a $\bar{B}$-subgroup of $\bar{D}_{q,i} \cong D_{q,i}$ and, by Proposition 1.4.12, $\bar{P}_q$ has a unique maximal $\bar{B}$-subgroup. Then Proposition 9.2.6 implies that $\bar{P}_q$ is $\bar{B}$-isomorphic to a nontrivial quotient of $\overline{A(q,i)} \cong A(q,i)$.

Now looking back at P, we get that $P_q = [S_{n-i+1}, P_q] \leqslant S_{n-i}RQ(1,q,\alpha_q,i) \leqslant S_{n-i}D_{q,i}$ and so $P = BR'$, where $R' = P_q \cap RQ(1,q,\alpha_q,i) \leqslant D_{q,i}$ and R' is B_i-invariant, since so are P_q, R and $Q(1,q,\alpha_q,i)$. Hence, since $R' \cong P_q/S_{n-i} = \bar{P}_q$, we have that R' is a B_i-subgroup of $D_{q,i}$ which is B_i-isomorphic to a nontrivial quotient of $A(q,i)$, that is, $R' \in \mathcal{R}_{q,i}$, completing the proof of the case $k_1 = 1$.

Now suppose that $k_1 > 1$. Then $P \leqslant A_{k_1-1} \rtimes (L_{k_1} \ldots L_{k_t} B_{n-k_1+1})$ and so, by Dedekind's

Modular Law,

$$P = P \cap (A_{k_1-1} \rtimes (L_{k_1} \dots L_{k_t} B_{n-k_1+1})) = A_{k_1-1}(P \cap (L_{k_1} \dots L_{k_t} B_{n-k_1+1})).$$

By Lemma 1.4.7, we know that $P \cap (L_{k_1} \dots L_{k_t} B_{n-k_1+1})$ is a minimal parabolic subgroup of $L_{k_1} \dots L_{k_t} B_{n-k_1+1}$ with respect to B_{n-k_1+1}. Hence the result proved above for $k_1 = 1$ implies that $P \cap (L_{k_1} \dots L_{k_t} B_{n-k_1+1}) = B_{n-k_1+1}R$, for some $R \in \mathcal{R}$. Then $P = A_{k_1-1}(P \cap (L_{k_1} \dots L_{k_t} B_{n-k_1+1})) = A_{k_1-1}B_{n-k_1+1}R = BR$, with $R \in \mathcal{R}$, as required. □

From Theorem 10.2.2 it follows that $\mathcal{M}(H, B)$ is the union of the sets $\mathcal{M}(BD_{q,i}, B)$, for all $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Furthermore a minimal parabolic subgroup of $BD_{q,i}$ with respect to B has the form BR, for some $R \in \mathcal{R}_{q,i}$, where $\mathcal{R}_{q,i}$ denotes the collection of all B_i-subgroups of $D_{q,i}$ which are B_i-isomorphic to a nontrivial quotient of $A(q, i)$.

Now, recall that $A(q, i)$ is a homocyclic B_i-invariant q-group of exponent q^{α_q} such that $A(q, i)/\Phi(A(q, i))$ is an absolutely irreducible $\mathrm{GF}(q)B_i$-module and that $D_{q,i}$ is the direct product of $n-i$ copies of $A(q, i)$. Therefore, by Theorem 9.2.4, we can describe all the distinct elements of $\mathcal{R}_{q,i}$ in terms of some sequences of integers and, by Theorem 9.2.2, also the cardinality of $\mathcal{R}_{q,i}$ is known. Hence, applying Theorem 9.2.4 for all $q \in \pi(p-1)$ and $i = 1, \dots, n-1$, we get a complete picture of all minimal parabolic subgroups of H with respect to B.

Finally notice that the method provided by Theorem 9.2.4 to build the distinct elements of $\mathcal{R}_{q,i}$, and thus all the distinct minimal parabolic subgroups of H with respect to B, can be easily implemented into a computer program. An example of how this can be done using the algebra package MAGMA is given in Chapter 11.

We shall now recall from Section 9.2 few details of this construction.

Let $i = 1, \dots, n-1$ and $q \in \pi(p-1)$ and set $t = n-i$. By Corollary 10.1.3, $D_{q,i}$ can be written as $D_{q,i} = \langle w_1, \dots, w_t \rangle^{B_i}$, where, for $k = 1, \dots, t$, $w_k = w(k, q, \alpha_q, i) \in L_k$ and $Q(k, q, \alpha_q, i) = \langle w_k \rangle^{B_i}$.

Set $Z = \mathbb{Z}_{q^{\alpha_q}} = \{0, \dots, q^{\alpha_q} - 1\}$ and denote by Z^t the set of all t-ples of elements of Z.

For $\alpha \in Z^t$, set $w_\alpha = w_1^{\alpha_1} \dots w_t^{\alpha_t}$ and $R_\alpha = \langle w_\alpha \rangle^{B_i}$. For $j = 1, \dots, t$ define the subset $\Gamma_{q,i}(\alpha_q, j)$ of Z^t as follows

$$\Gamma_{q,i}(\alpha_q, j) = \{(\alpha_1, \dots, \alpha_t) \in Z^t \mid \alpha_j = 1 \text{ and, for } h < j,\ q | \alpha_h\}.$$

For $e = 1, \dots, \alpha_q - 1$, define by induction the set $\Gamma_{q,i}(e,j)$ as

$$\Gamma_{q,i}(e,j) = \{q\alpha \in Z^t \mid \alpha \in \Gamma_{q,i}(e+1,j)\} = \{q^{\alpha_q - e}\alpha \mid \alpha \in \Gamma_{q,i}(\alpha_q, j)\}.$$

Finally, let $\Gamma_{q,i}(e)$ be the union of the sets $\Gamma_{q,i}(e,j)$, for $j = 1, \dots, t$, and $\Gamma_{q,i}$ be the union of the sets $\Gamma_{q,i}(e)$, for $e = 1, \dots, \alpha_q - 1$. Then Theorem 9.2.4 implies that $\mathcal{R}_{q,i} = \{R_\alpha \mid \alpha \in \Gamma_{q,i}\}$ and so, by Theorem 10.2.2, we have the following:

Theorem 10.2.3. *$P \in \mathcal{M}(H,B)$ if and only if $P = BR_\alpha = \langle B, w_\alpha \rangle$, for some $\alpha \in \Gamma$, where Γ is the union of the sets $\Gamma_{q,i}$, for $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. In particular,*

$$|\mathcal{M}(H,B)| = \sum_{q \in \pi(p-1)} \alpha_q + \sum_{t=2}^{n-1} \left(\sum_{q \in \pi(p-1)} \frac{q^t - 1}{q - 1} \, \frac{q^{(t-1)\alpha_q} - 1}{q^{t-1} - 1} \right).$$

As an application of Theorem 10.2.3 we construct all minimal parabolic subgroups of $\mathrm{Sym}(5^3)$ which are contained in H.

Example 10.2:

Let $G = \mathrm{Sym}(125)$, that is, $p = 5$ and $n = 3$. So $q = 2 = \alpha_q$ and $i = 1, 2$. Let T be a Sylow 5-subgroup of G and H be a subgroup of G containing T and isomorphic to the wreath product of three copies of $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$. Set $B = N_G(T)$. By Theorem 10.2.2,

$$\mathcal{M}(H,B) = \mathcal{M}(BD_{2,2}, B) \cup \mathcal{M}(BD_{2,1}, B).$$

From Example 10.1, we have that $D_{2,1} = \langle w_{1,1}, w_{2,1} \rangle^{B_1}$ and $D_{2,2} = \langle w_{1,2} \rangle^{B_2}$, where

$$\begin{aligned} w_{1,1} = w(1,2,2,1) &= (2\ 3\ 5\ 4)(7\ 8\ 10\ 9)(12\ 13\ 15\ 14)(17\ 18\ 20\ 19)(22\ 23\ 25\ 24) \\ &\quad (27\ 29\ 30\ 28)(32\ 34\ 35\ 33)(37\ 39\ 40\ 38)(42\ 44\ 45\ 43)(47\ 49\ 50\ 48), \\ w_{2,1} = w(2,2,2,1) &= (6\ 11\ 21\ 16)(7\ 12\ 22\ 17)(8\ 13\ 23\ 18)(9\ 14\ 24\ 19)(10\ 15\ 25\ 20) \\ &\quad (31\ 41\ 46\ 36)(32\ 42\ 47\ 37)(33\ 43\ 48\ 38)(34\ 44\ 49\ 39)(35\ 45\ 50\ 40), \\ w_{1,2} = w(1,2,2,2) &= (2\ 3\ 5\ 4)(7\ 9\ 10\ 8). \end{aligned}$$

Next we build the sets $\Gamma_{2,i}$, for $i = 1, 2$. Each $\Gamma_{2,i}$ is a set of sequences in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ of length $n - i$ and is the union of the sets $\Gamma_{2,i}(e)$, with $e = 1, 2$. So we have that

$$\begin{aligned} \Gamma_{2,1} &= \Gamma_{2,1}(2) \cup \Gamma_{2,1}(1) = \{(1,0), (1,1), (1,2), (1,3), (0,1), (2,1)\} \cup \{(2,0), (2,2), (0,2)\} \\ \Gamma_{2,2} &= \Gamma_{2,2}(2) \cup \Gamma_{2,2}(1) = \{(1)\} \cup \{(2)\}. \end{aligned}$$

For $(\alpha) \in \Gamma_{2,2}$, set $z[\alpha] = w_{1,2}^{\alpha}$ and, for $(\alpha_1, \alpha_2) \in \Gamma_{2,1}$, set $z[\alpha_1, \alpha_2] = w_{1,1}^{\alpha_1} w_{2,1}^{\alpha_2}$. We can now write down the elements that together with B generate all minimal parabolic subgroups of H:

$z[1,0] = w_{1,1} =$ (2 3 5 4)(7 8 10 9)(12 13 15 14)(17 18 20 19)(22 23 25 24)(27 29 30 28)
(32 34 35 33)(37 39 40 38)(42 44 45 43)(47 49 50 48),

$z[1,1] = w_{1,1}w_{2,1} =$ (2 3 5 4)(6 11 21 16)(7 13 25 19)(8 15 24 17)(9 12 23 20)(10 14 22 18)
(27 29 30 28)(31 41 46 36)(32 44 50 38)(33 42 49 40)
(34 45 48 37)(35 43 47 39),

$z[1,2] = w_{1,1}w_{2,1}^2 =$ (2 3 5 4)(6 21)(7 23 10 24)(8 25 9 22)(11 16)(12 18 15 19)(13 20 14 17)
(27 29 30 28)(31 46)(32 49 35 48)(33 47 34 50)(36 41)
(37 44 40 43)(38 42 39 45),

$z[1,3] = w_{1,1}w_{2,1}^3 =$ (2 3 5 4)(6 16 21 11)(7 18 25 14)(8 20 24 12)(9 17 23 15)(10 19 22 13)
(27 29 30 28)(31 36 46 41)(32 39 50 43)(33 37 49 45)
(34 40 48 42)(35 38 47 44),

$z[0,1] = w_{2,1} =$ (6 11 21 16)(7 12 22 17)(8 13 23 18)(9 14 24 19)(10 15 25 20)(31 41 46 36)
(32 42 47 37)(33 43 48 38)(34 44 49 39)(35 45 50 40),

$z[2,1] = w_{1,1}^2 w_{2,1} =$ (2 5)(3 4)(6 11 21 16)(7 15 22 20)(8 14 23 19)(9 13 24 18)(10 12 25 17)
(27 30)(28 29)(31 41 46 36)(32 45 47 40)(33 44 48 39)
(34 43 49 38)(35 42 50 37),

$z[2,0] = w_{1,1}^2 =$ (2 5)(3 4)(7 10)(8 9)(12 15)(13 14)(17 20)(18 19)(22 25)(23 24)(27 30)
(28 29)(32 35)(33 34)(37 40)(38 39)(42 45)(43 44)(47 50)(48 49),

$z[2,2] = w_{1,1}^2 w_{2,1}^2 =$ (2 5)(3 4)(6 21)(7 25)(8 24)(9 23)(10 22)(11 16)(12 20)(13 19)(14 18)
(15 17)(27 30)(28 29)(31 46)(32 50)(33 49)(34 48)(35 47)(36 41)
(37 45)(38 44)(39 43)(40 42),

$z[0,2] = w_{2,1}^2 =$ (6 21)(7 22)(8 23)(9 24)(10 25)(11 16)(12 17)(13 18)(14 19)(15 20)(31 46)
(32 47)(33 48)(34 49)(35 50)(36 41)(37 42)(38 43)(39 44)(40 45),

$z[1] = w_{1,2} =$ (2 3 5 4)(7 9 10 8),

$z[2] = w_{1,2}^2 =$ (2 5)(3 4)(7 10)(8 9).

Then Theorem 10.2.3 implies that

$$\begin{aligned}\mathcal{M}(H,B) &= \mathcal{M}(BD_{2,2},B) \cup \mathcal{M}(BD_{2,1},B) \\ &= \{P[\alpha] \mid \alpha \in \Gamma_{2,2}\} \cup \{P[\alpha_1,\alpha_2] \mid (\alpha_1,\alpha_2) \in \Gamma_{2,1}\},\end{aligned}$$

where $P[\alpha] = \langle B, z[\alpha]\rangle$ and $P[\alpha_1,\alpha_2] = \langle B, z[\alpha_1,\alpha_2]\rangle$. In particular, there are eleven minimal parabolic subgroups of H with respect to B. Also notice that all the subgroups of the form $P(k,2,e,i) = \langle B, w(k,2,e,i)\rangle$, with $k,e,i = 1,2$ and $k+i \leq 3$, belong to $\mathcal{M}(H,B)$, where the elements $w(k,2,e,i)$ are described in Example 10.1. ■

We shall conclude this section by proving a remarkable property of the minimal parabolic subgroups of H.

Theorem 10.2.4. *Any two minimal parabolic subgroups of H with respect to B permute.*

Proof. According to Theorem 10.2.2, let $P_i = BR_i$ and $P_j = BR_j$ be two minimal parabolic subgroups of H with respect to B, where $R_i \in \mathcal{R}_{q,i}$ and $R_j \in \mathcal{R}_{r,j}$, with $q,r \in \pi(p-1)$ and $i,j = 1,\dots,n-1$. We shall show that R_i and R_j permute.
First suppose that $i = j$. Then R_i and R_j are both subgroups of D_i, which is abelian. Hence R_i and R_j commute and P_i and P_j permute.
Let $i \neq j$ and assume that $j < i$. We shall first notice that R_jB_i is a group. By definition, R_j is a B_j-group and, since $j < i$, we know that $B_j < B_i$. Thus we need to look at the action on R_j of a complement to B_j in B_i. So write

$$B_i = (S \rtimes \langle h_{n-i+1},\dots,h_{n-j}\rangle) \rtimes B_j,$$

where $S = \langle x_{n-i+1},\dots,x_{n-j}\rangle^{B_j} \cong S_{n-j}/S_{n-i}$. By Corollary 10.1.3 and by Proposition 10.1.5, $D_{r,j}$ normalizes both S_{n-j} and S_{n-i}. Thus $D_{r,j}$ normalizes S and, since $R_j \leqslant D_{r,j}$, so does R_j. Hence R_jS is a group. Moreover $S \trianglelefteq B_i$ and R_j is normalized by B_j and, by Proposition 10.1.6, centralized by $\langle h_{n-i+1},\dots,h_{n-j}\rangle$. Therefore we can conclude that R_jS is normalized by B_i and so $R_jSB_i = R_jB_i$ is a group.
Next we shall prove that R_i is an R_jB_i-group. This will imply, in particular, that R_i is R_j-invariant and so that R_i and R_j permute, proving the result.
Recall that

$$D_{q,i} = Q(1,q,\alpha_q,i) \times \cdots \times Q(n-i,q,\alpha_q,i)$$

and so, by Lemma 10.1.12, $D_{q,i}$ is the direct product of $n-i$ copies of a homocyclic q-group of exponent q^{α_q}, whose Frattini quotient is an absolutely irreducible $\mathrm{GF}(q)B_i$-module. But, by Proposition 10.1.10, $Q(k,q,\alpha_q,i)$ is normalized by $D_{r,j}$, and so by R_j, for all $k=1,\dots,n-i$. Therefore each direct factor of $D_{q,i}$ is also an R_jB_i-group. Then Corollary 9.2.3 implies that $\mathcal{R}_{q,i}$ equals the set of R_jB_i-subgroups of $D_{q,i}$ which are R_jB_i-isomorphic to a nontrivial quotient of $A(q,i)$. In particular, since $R_i \in \mathcal{R}_{q,i}$, it follows that R_i is R_jB_i-invariant. Hence R_i is R_j-invariant and so R_i and R_j permute, implying that P_i and P_j permute. □

Corollary 10.2.5. *Any two subgroups belonging to the collection $\mathcal{R}$ permute.*

Proof. This follows from the proof of Theorem 10.2.4. □

Corollary 10.2.6. *Any two subgroups of H containing B permute.*

Proof. By Proposition 1.4.3, any two such subgroups are generated by minimal parabolic subgroups of H with respect to B and so the result follows from Theorem 10.2.4. □

10.3 Minimal parabolic systems whose elements are soluble

Having described all minimal parabolic subgroups of G with respect to B which are contained in H, we now want to classify all minimal parabolic systems of H, that is, by Lemma 6.7.6, all the minimal parabolic systems of G whose elements are soluble.

We shall first reduce the problem to determining all minimal parabolic systems of the group $BD_{q,i}$, for $q \in \pi(p-1)$ and $i=1,\dots,n-1$.

Theorem 10.3.1. *Let $\mathcal{S}$ be a minimal parabolic system of H with respect to B. Then $\mathcal{S}$ is the disjoint union of minimal parabolic systems of the groups BD_i, for $i=1,\dots,n-1$.*

Proof. Recall, from Corollary 10.1.14, that $H = BD_1\dots D_{n-1}$ and so $|H| = |B||D_1|\dots|D_{n-1}|$. Let $\mathcal{S}$ be a minimal parabolic system of H with respect to B. For $i=1,\dots,n-1$ set

$$\mathcal{S}_i = \{P \in \mathcal{S} \mid P \leqslant BD_i\}.$$

We want to show that $\mathcal{S}_i$ is a minimal parabolic system of BD_i, for all i. Suppose this is false and let $i \in \{1,\dots,n-2\}$ such that $\langle \mathcal{S}_i \rangle \neq BD_i$. Also, assume that $\langle \mathcal{S}_j \rangle = BD_j$, for all

$j \neq i$. Set $P_i = \langle \mathcal{S}_i \rangle$ and write $P_i = BR_i$, with $R_i < D_i$. Then, since $H = \langle \mathcal{S} \rangle = \langle \mathcal{S}_i \mid i = 1, \dots, n-1 \rangle$, we also have that

$$H = BR_i \prod_{j \neq i} BD_j = B(R_i \prod_{j \neq i} D_j),$$

where BR_i and BD_j, $j \neq i$, permute, by Corollary 10.2.6. But then

$$|H| = |B||R_i| \prod_{j \neq i} |D_j| < |B||D_1| \dots |D_{n-1}|,$$

which is a contradiction. Hence $\mathcal{S}$ is the union of the sets $\mathcal{S}_i$, where each $\mathcal{S}_i$ is a minimal parabolic system of BD_i with respect to B. $\square$

Corollary 10.3.2. *Let $\mathcal{S}$ be a minimal parabolic system of H with respect to B. Then $\mathcal{S}$ contains at least one minimal parabolic subgroup of BD_i, for all $i = 1, \dots, n-1$.*

Proof. Let $\mathcal{S}$ be a minimal parabolic system of H with respect to B. For $i = 1, \dots, n-1$, the set $\mathcal{S}_i = \{P \in \mathcal{S} \mid P \leqslant BD_i\}$ is, by Theorem 10.3.1, a minimal parabolic system of BD_i with respect to B. In particular, $\mathcal{S}_i \neq \emptyset$. $\square$

Theorem 10.3.3. *Let $i = 1, \dots, n-1$ and let $\mathcal{S}_i$ be a minimal parabolic system of BD_i with respect to B. Then $\mathcal{S}_i$ is the disjoint union of minimal parabolic systems of the groups $BD_{q,i}$, for all $q \in \pi(p-1)$.*

Proof. By Corollary 10.1.4, D_i is the direct product of the subgroups $D_{q,i}$, for $q \in \pi(p-1)$, and so

$$BD_i = B \prod_{q \in \pi(p-1)} D_{q,i} = \prod_{q \in \pi(p-1)} BD_{q,i}.$$

Let $\mathcal{S}_i$ be a minimal parabolic system of BD_i with respect to B. For $q \in \pi(p-1)$ set

$$\mathcal{S}_{q,i} = \{P \in \mathcal{S}_i \mid P \leqslant BD_{q,i}\}.$$

Suppose there exists $r \in \pi(p-1)$ such that $\mathcal{S}_{r,i}$ is not a minimal parabolic system of $BD_{r,i}$ and assume that $\langle \mathcal{S}_{q,i} \rangle = BD_{q,i}$, for all $q \in \pi(p-1)$, $q \neq r$. Let $BR_i = \langle \mathcal{S}_{r,i} \rangle$. Then, since $BD_i = \langle \mathcal{S}_i \rangle = \langle \mathcal{S}_{q,i} \mid q \in \pi(p-1) \rangle$, we also have that

$$BD_i = BR_i \prod_{q \in \pi(p-1) \setminus \{r\}} BD_{q,i} = B(R_i \prod_{q \in \pi(p-1) \setminus \{r\}} D_{q,i}),$$

which implies that

$$|BD_i| = |B||R_i| \prod_{q\in\pi(p-1)\setminus\{r\}} |D_{q,i}| < |B| \prod_{q\in\pi(p-1)} |D_{q,i}|,$$

against the fact that BD_i equals $B\prod_{q\in\pi(p-1)} D_{q,i}$. Hence each $\mathcal{S}_{q,i}$ is a minimal parabolic system of $BD_{q,i}$. $\square$

Corollary 10.3.4. *Let $\mathcal{S}$ be a minimal parabolic system of H with respect to B. Then $\mathcal{S}$ is the disjoint union of minimal parabolic systems of the groups $BD_{q,i}$, for all $q \in \pi(p-1)$ and $i = 1, \dots, n-1$.*

We shall now focus our attention on the minimal parabolic systems of $BD_{q,i}$ with respect to B, for $q \in \pi(p-1)$ and $i = 1, \dots, n-1$.

Recall that $D_{q,i}$ is the direct sum of $n-i$ copies of $A(q,i)$, with $A(q,i)$ homocyclic B_i-invariant q-group of exponent q^{α_q} such that $A(q,i)/\Phi(A(q,i))$ is an absolutely irreducible $\mathrm{GF}(q)B_i$-module. By Theorem 10.2.2, a minimal parabolic subgroup of $BD_{q,i}$ has the form BR, for some B_i-subgroup R of $D_{q,i}$ such that R is B_i-isomorphic to a nontrivial quotient of $A(q,i)$. Furthermore, if we denote by $\mathcal{R}_{q,i}$ the collection of all B_i-subgroups of $D_{q,i}$ which are B_i-isomorphic to a nontrivial quotient of $A(q,i)$, then, by Theorem 9.2.4, we have that

$$\mathcal{R}_{q,i} = \{R_\alpha \mid \alpha \in \Gamma_{q,i}\},$$

where $\Gamma_{q,i}$ is defined as in Section 10.2. Hence we can consider the map

$$\pi_{q,i} \colon P \in \mathcal{M}(BD_{q,i}, B) \longmapsto \pi_{q,i}(P) \in \mathcal{R}_{q,i}$$

such that $P = B\pi_{q,i}(P)$.

Recall, from Section 9.3, that a subset $\mathcal{G}$ of $\mathcal{R}_{q,i}$ is a minimal generating set for $D_{q,i}$ in $\mathcal{R}_{q,i}$ if $D_{q,i} = \langle \mathcal{G} \rangle = \langle R_\alpha \mid R_\alpha \in \mathcal{G} \rangle$ and no proper subset of $\mathcal{G}$ generates $D_{q,i}$.

The next result establishes a link between minimal parabolic systems of $BD_{q,i}$ with respect to B and minimal generating sets for $D_{q,i}$ in $\mathcal{R}_{q,i}$.

Lemma 10.3.5. *Let $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Then the map*

$$\pi_{q,i} \colon P \in \mathcal{M}(BD_{q,i}, B) \longmapsto \pi_{q,i}(P) \in \mathcal{R}_{q,i}$$

such that $P = B\pi_{q,i}(P)$ is a bijection taking minimal parabolic systems of $BD_{q,i}$ with respect to B into minimal generating sets for $D_{q,i}$ in $\mathcal{R}_{q,i}$.

Proof. Let $q \in \pi(p-1)$ and $i = 1, \dots, n-1$ and consider the map

$$\pi_{q,i} \colon P \in \mathcal{M}(BD_{q,i}, B) \longmapsto \pi_{q,i}(P) \in \mathcal{R}_{q,i}$$

such that $P = B\pi_{q,i}(P)$. Then $\pi_{q,i}(P) = P \cap D_{q,i}$ and, by Theorem 10.2.2, $\pi_{q,i}$ is a bijection. Now let $\mathcal{S} = \{P_1, \dots, P_r\}$ be a subset of $\mathcal{M}(BD_{q,i}, B)$. It will suffice to show that $\mathcal{S}$ generates $BD_{q,i}$ if and only if $\pi_{q,i}(\mathcal{S}) = \{\pi_{q,i}(P_1), \dots, \pi_{q,i}(P_r)\}$ generates $D_{q,i}$.
So suppose that $BD_{q,i} = \langle \mathcal{S} \rangle$. Then

$$BD_{q,i} = P_1 \dots P_r = B\pi_{q,i}(P_1) \dots B\pi_{q,i}(P_r) = B\pi_{q,i}(P_1) \dots \pi_{q,i}(P_r)$$

and, by looking at the orders, it follows that $D_{q,i} = \pi_{q,i}(P_1) \dots \pi_{q,i}(P_r)$. Thus $\pi_{q,i}(\mathcal{S})$ generates $D_{q,i}$. Conversely, let $D_{q,i} = \langle \mathcal{G} \rangle$, with $\mathcal{G} = \{R_1, \dots, R_s\} \subseteq \mathcal{R}_{q,i}$. Then

$$BD_{q,i} = BR_1 \dots R_s = BR_1 \dots BR_s$$

and $BD_{q,i}$ is generated by the set $\{BR_1, \dots, BR_s\}$, with $BR_j = \pi_{q,i}^{-1}(R_j)$, for $j = 1, \dots, s$. $\square$

Now we only need to apply Corollary 9.3.7 to get a complete description of all minimal parabolic systems of $BD_{q,i}$ with respect to B, for all $q \in \pi(p-1)$ and $i = 1, \dots, n-1$.

Theorem 10.3.6. *Let $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Then a minimal parabolic system of $BD_{q,i}$ with respect to B has rank $n-i$ and consists of some subgroups $R_{\alpha_1}, \dots, R_{\alpha_{n-i}} \in \mathcal{R}_{q,i}$ such that, for $j = 1, \dots, n-i$, $\alpha_j \in \Gamma_{q,i}(\alpha_q)$ and*

$$\alpha_j \not\equiv \sum_{h \neq j} \lambda_h \alpha_h \pmod{q},$$

for any $\lambda_h \in \mathrm{GF}(q)$. Furthermore the number of minimal parabolic systems of $BD_{q,i}$ with respect to B is

$$\frac{1}{(n-i)!} \, \frac{q^{(n-i)(n-i-1)(2\alpha_q-1)/2}}{(q-1)^{(n-i)}} \prod_{s=1}^{n-i} (q^s - 1).$$

Corollary 10.3.7. *Let $i = 1, \dots, n-1$ and let $\Gamma_i(\alpha_q)$ be the union of the sets $\Gamma_{q,i}(\alpha_q)$, for $q \in \pi(p-1)$. Then a minimal parabolic system of BD_i with respect to B has rank $|\pi(p-1)|(n-i)$ and consists of some subgroups R_α, with $\alpha \in \Gamma_i(\alpha_q)$, such that the set $\{R_\alpha \mid \alpha \in \Gamma_{q,i}(\alpha_q)\}$ is a minimal parabolic system of $BD_{q,i}$ with respect to B, for all $q \in \pi(p-1)$. Furthermore the number of minimal parabolic systems of BD_i with respect to B is given by*

$$\prod_{q \in \pi(p-1)} \left(\frac{1}{(n-i)!} \, \frac{q^{(n-i)(n-i-1)(2\alpha_q-1)/2}}{(q-1)^{(n-i)}} \prod_{s=1}^{n-i} (q^s - 1) \right).$$

Corollary 10.3.8. *Let $\Gamma(\alpha_q)$ be the union of the sets $\Gamma_i(\alpha_q)$, for $i = 1, \ldots, n-1$. A minimal parabolic system of H with respect to B has rank $|\pi(p-1)|n(n-1)/2$ and consists of some subgroups R_α, with $\alpha \in \Gamma(\alpha_q)$, such that the set $\{R_\alpha \mid \alpha \in \Gamma_i(\alpha_q)\}$ is a minimal parabolic system of BD_i with respect to B, for all $i = 1, \ldots, n-1$. Furthermore the number of minimal parabolic systems of H with respect to B is given by*

$$\prod_{q\in\pi(p-1)} \left(\frac{q^{(n^3/3-n^2+2n/3)(2\alpha_q-1)/2}}{(q-1)^{n(n-1)/2}} \prod_{s=1}^{n-1} \left(\frac{q^s-1}{s}\right)^{n-s} \right).$$

Proof. By Theorem 10.3.1 and Corollary 10.3.7, the rank of a minimal parabolic system of H with respect to B is given by

$$\sum_{i=1}^{n-1} |\pi(p-1)|(n-i) = |\pi(p-1)| \sum_{t=1}^{n-1} t = |\pi(p-1)|n(n-1)/2.$$

Furthermore, for $i = 1, \ldots, n-1$ and $q \in \pi(p-1)$, denote by $\gamma(q,i)$, $\gamma(i)$ and γ the number of minimal parabolic systems of $BD_{q,i}$, BD_i and H, respectively. Then, by Theorems 10.3.1 and 10.3.3,

$$\gamma = \prod_{i=1}^{n-1} \gamma(i) = \prod_{i=1}^{n-1} \prod_{q\in\pi(p-1)} \gamma(q,i) = \prod_{q\in\pi(p-1)} \prod_{i=1}^{n-1} \gamma(q,i) = \prod_{q\in\pi(p-1)} \gamma(q),$$

with $\gamma(q)$ product of the $\gamma(q,i)$'s, for $i = 1, \ldots, n-1$. We shall compute the number $\gamma(q)$. From Theorem 10.3.6 it follows that

$$\gamma(q) = \prod_{t=1}^{n-1} \left(\frac{1}{t!} \frac{q^{t(t-1)(2\alpha_q-1)/2}}{(q-1)^t} \prod_{s=1}^{t} (q^s-1) \right).$$

Let us compute separately each factor of $\gamma(q)$. First we have that

$$\prod_{t=1}^{n-1} \frac{1}{t!} = \prod_{t=1}^{n-1} \prod_{s=1}^{t} s^{-1} = \prod_{s=1}^{n-1} (s^{-1})^{n-s}.$$

Now recall the formula

$$\sum_{t=1}^{n-1} t(t-1) = n^3/3 - n^2 + 2n/3,$$

which can be easily derived by induction on n. Then it follows that

$$\prod_{t=1}^{n-1} q^{t(t-1)(2\alpha_q-1)/2} = \prod_{t=1}^{n-1} \left(q^{(2\alpha_q-1)/2}\right)^{t(t-1)} = \left(q^{(2\alpha_q-1)/2}\right)^{\sum_{t=1}^{n-1} t(t-1)}$$
$$= q^{(n^3/3-n^2+2n/3)(2\alpha_q-1)/2}.$$

Next we have that

$$\prod_{t=1}^{n-1} \frac{1}{(q-1)^t} = (q-1)^{-\sum_{t=1}^{n-1} t} = (q-1)^{-n(n-1)/2}.$$

Finally,

$$\prod_{t=1}^{n-1} \prod_{s=1}^{t} (q^s - 1) = \prod_{s=1}^{n-1} (q^s - 1)^{n-s}.$$

Hence it follows that

$$\gamma(q) = \frac{q^{(n^3/3 - n^2 + 2n/3)(2\alpha_q - 1)/2}}{(q-1)^{n(n-1)/2}} \prod_{s=1}^{n-1} \left(\frac{q^s - 1}{s} \right)^{n-s},$$

which implies the result. □

A first immediate example of a minimal parabolic system of H is the following:

Theorem 10.3.9. *Let $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. Then the set*

$$\mathcal{S}_{q,i} = \{P(k, q, \alpha_q, i) \mid k = 1, \dots, n-i\}$$

is a minimal parabolic system of $BD_{q,i}$ with respect to B.

Proof. Let $q \in \pi(p-1)$ and $i = 1, \dots, n-1$. By definition, $P(k, q, \alpha_q, i) = BQ(k, q, \alpha_q, i)$, for all $k = 1, \dots, n-i$. Furthermore, by Corollary 10.1.3,

$$D_{q,i} = Q(1, q, \alpha_q, i) \times \cdots \times Q(n-i, q, \alpha_q, i).$$

Hence the result follows from Lemma 10.3.5 and Theorem 10.3.6. □

Corollary 10.3.10. *Let $i = 1, \dots, n-1$. Then the set*

$$\mathcal{S}_i = \{P(k, q, \alpha_q, i) \mid k = 1, \dots, n-i; q \in \pi(p-1)\}$$

is a minimal parabolic system of BD_i with respect to B.

Corollary 10.3.11. *The set $\mathcal{S}$ of all minimal parabolic subgroup of H with respect to B of the form $P(k, q, \alpha_q, i)$, with $k = 1, \dots, n-i, q \in \pi(p-1)$ and $i = 1, \dots, n-1$, is a minimal parabolic system of H with respect to B.*

Last, carrying on with Examples 10.1 and 10.2, we shall produce all minimal parabolic systems of H with respect to B for the case $p = 5$ and $n = 3$.

Example 10.3:

Let $p = 5$ and $n = 3$, so $q = 2 = \alpha_q$ and $i = 1, 2$. We shall determine all minimal parabolic systems of the groups $BD_{2,1}$ and $BD_{2,2}$. From Example 10.2 we have that

$$\mathcal{M}(BD_{2,2}, B) = \{P[1], P[2]\},$$
$$\mathcal{M}(BD_{2,1}, B) = \{P[1,0], P[1,1], P[1,2], P[1,3], P[0,1], P[2,1], P[2,0], P[2,2], P[0,2]\}.$$

We first need to select, for each group $D_{2,i}$, those minimal parabolic subgroups that have maximal exponent, that is, those corresponding to the sequences in $\Gamma_{2,i}(2)$.

The only element of $\mathcal{M}(BD_{2,2}, B)$ of exponent 2^2 is $P[1]$ and so $BD_{2,2}$ has a unique minimal parabolic system, namely $\mathcal{S}_{2,2} = \{P[1]\}$, and $\mathcal{S}_{2,2}$ has rank 1.

For $BD_{2,1}$, the minimal parabolic subgroups of maximal exponent are

$$P[1,0],\ P[1,1],\ P[1,2],\ P[1,3],\ P[0,1],\ P[2,1].$$

So, applying Theorem 10.3.6, we have that a minimal parabolic system $\mathcal{S}_{2,1}$ of $BD_{2,1}$ is one of the following:

$$\begin{array}{llll}
\{P[1,0], P[1,1]\}, & \{P[1,0], P[1,3]\}, & \{P[1,0], P[0,1]\}, & \{P[1,0], P[2,1]\}, \\
\{P[1,1], P[1,2]\}, & \{P[1,1], P[0,1]\}, & \{P[1,1], P[2,1]\}, & \{P[1,2], P[1,3]\}, \\
\{P[1,2], P[0,1]\}, & \{P[1,2], P[2,1]\}, & \{P[1,3], P[0,1]\}, & \{P[1,3], P[2,1]\}.
\end{array}$$

In particular, $BD_{2,1}$ has twelve minimal parabolic systems, each of rank 2. Hence, since a minimal parabolic system of H is the union of $\mathcal{S}_{2,2}$ and $\mathcal{S}_{2,1}$, it follows that there exist twelve minimal parabolic systems of H with respect to B and they all have rank 3. Of these $\{P[1], P[1,0], P[0,1]\}$ is the one described in Corollary 10.3.11. ■

10.4 Conclusions

We want to draw some conclusions about minimal parabolic subgroups of $\mathrm{Sym}(\Omega)$, with $|\Omega|$ any integer. As we have seen in Chapter 6 (Theorems 6.7.1 and 6.7.2), we can always assume that a minimal parabolic subgroup of $\mathrm{Sym}(\Omega)$ is imprimitive and, as a result of this, we can reduce our investigation to some critical cases (see Theorem 6.7.4). This combined with the results established in this chapter leads to the following:

Corollary 10.4.1. *Let $G = \mathrm{Sym}(\Omega)$ and p be a prime dividing the order of G. Then all soluble minimal parabolic subgroups of G with respect to the normalizer of a Sylow p-subgroup are known, except when $p = 3$ and $|\Omega| = 3^{r+1} + 3^r$, with $r \geq 1$.*

Proof. For $p = 2$, all minimal parabolic subgroups of G are known by [21]. For $p \geq 3$, the result follows from Theorem 6.7.4, Corollary 6.7.5, Lemma 6.7.6 and Theorem 6.7.8. ☐

Chapter 11

Computing minimal parabolic subgroups of the symmetric groups

Let $G = \mathrm{Sym}(p^n)$, with $n \in \mathbb{N}$ and p prime, and let $T \in \mathrm{Syl}_p(G)$. Set $B = N_G(T)$ and denote by H a subgroup of G containing B and isomorphic to the wreath product of n copies of $\mathrm{Hol}(\mathbb{Z}_p)$. We present some programs for the computation of the minimal parabolic subgroups of H with respect to B based on the results established in Chapter 10.

All the programs described here have been written using the algebra package MAGMA version 2.3 in the form of procedures, but they can be easily converted into functions. For more details on the MAGMA functions we shall be using, the obvious reference is [2].

The whole chapter should be read in conjunction with Sections 5.1, 5.2, 10.1 and 10.2.

11.1 The normalizer of a Sylow p-subgroup

The first step is to compute the normalizer B of T in G. Given any group L and any subgroup M of L, MAGMA provides the function `Normalizer(L,M)`, which returns the normalizer of M in L. However, for our purposes, this function is not powerful enough, since, even for a small case like $p = 5$ and $n = 3$, the running times are too long.

To overcome this obstacle we have developed the procedure `Normalizer(p,n,~X,~D,~B)`, which is based on the description of B given in Section 5.2.

B is built as a subgroup of the wreath product H of n copies of N, with $N \cong \mathrm{Hol}(\mathbb{Z}_p)$ the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p)$.

The program makes the normalizer N as the Affine General Linear group of dimension 1 over a field with p elements, using the function `AGL( , )`. A control on the number and the order of the generators of N is included to make sure that N is generated by exactly two elements, one of order p and one of order $p-1$.

Next the wreath product H of n copies of N is built using the function `WreathProduct( , )` and adding one factor at the time. The p-generators and the p'-generators of H are ordered by degree and stored in the sequences X and Y, respectively, so that the i-th element of the sequence X corresponds to x_i and the i-th element of Y corresponds to y_i. Notice that, by the choice of the generators of N, we know that X and Y both contain n elements and that all elements belonging to Y have order $p-1$. Moreover, by construction, the Sylow p-subgroup T is the subgroup generated by X.

We now need to make the p'-generators of B. Recall that, for $p=2$, $T=B=H$ and we are done. For $p \neq 2$, the extra generators of B are stored in the sequence D, such that, for $i=1,\dots,n$, the i-th element of D corresponds to $h_i = (f_n \circ \cdots \circ f_{i+1})(y_i)$.

Finally, B is the subgroup generated by X and D.

Given p and n, the procedure returns the sequence X containing the n generators of T; the sequence D containing the n generators of order $p-1$ of B; and the normalizer B.

An argument checking is included which allows the user to assign a new value to p in the case the chosen value is not a prime.

In the construction of N, the choice of using the function `AGL( , )` instead of the function `Normalizer( , )` was induced by the strange behaviour of the latter in relation to the number and the order of the p'-generators of N. For instance, for $p=7$, the function `Normalizer( , )` returns three generators for N and, for $p=73$, it returns four generators; furthermore, for $p=103$, none of the generators produced has order 102. On the contrary, as far as our experience in running different examples goes, the function `AGL( , )` always returns two generators for N, one of order p and one of order $p-1$. Thus, using the function `AGL( , )`, we can expect the procedure `Normalizer(p,n,~X,~D,~B)` to jump the control on the generators of N and to be faster than if using the function `Normalizer( , )`.

The procedure is included below.

```
procedure Normalizer(p,n,~X,~D,~B);
// Argument checking on p
while not IsPrime(p) do
    "Error in input: 1st argument must be a prime number.";
    "Choose another value for it:";
    readi p;
end while;
// Building the symmetric groups Sym(p) and Sym(p^n)
G:=Sym(p);
Gn:=Sym(p^n);
// Building N
N:=AGL(1,p);
// Control on the number and the order of the generators of N
if #Generators(N) gt 2 then
    z:=G!1;
    for i in [1..#Generators(N)] do
        if Order(N.i) eq p then
            S:=sub<G|N.i>;
        end if;
        if Order(N.i) eq p-1 then
            z:=N.i;
        end if;
    end for;
    if z eq Identity(G) then
        for i in [1..#Generators(N)] do
            if Order(N.i) ne p then
                z:=z*N.i;
            end if;
        end for;
    end if;
    Order(z) eq p-1;
```

```
    N:=sub<G|S,z>;
end if;
// Building H
H:=N;
for i in [2..n] do
    H:=WreathProduct(H,N);
end for;
if p eq 2 then
    // The p=2 case
    X:=Generators(H);D:=[];
    B:=H;
    else
    // The p neq 2 case
    // Ordering the generators of H by degree
    X:=[Gn|];
    Y:=[Gn|];
    K:=Generators(H);
    for i in [1..n] do
        for x in K do
            if Degree(x) eq p^i then
                X[i]:=x; aa := x;
            elif
            Degree(x) eq (p-1)*p^(i-1) then
                Y[i]:=x; bb:= x;
            end if;
            if assigned(aa) and assigned(bb) then
                break;
            end if;
        end for;
        delete aa; delete bb;
        K := K diff {X[i],Y[i]};
```

```
    end for;
    // Building the extra generators of B
    D:=[Gn|];
    D[n]:=Y[n];
    for i in [1..n-1] do
        D[i]:=Y[i];d:=Y[i];
        for j in [i+1..n] do
            for e in [1..p-1] do
                d:=d^X[j];
                D[i]*:=d;
            end for;
            d:=D[i];
        end for;
    end for;
    // Generating B
    B:=sub<Gn|X,D>;
end if;
end procedure;
```

The performance of the program in terms of running times is very good. The normalizer of T in $\mathrm{Sym}(5^5)$ is computed in about 0.2 seconds and for $p = 19$ and $n = 3$ the running time is less than half a second.

A further, though very small, improvement can be achieved using the 2-adic decomposition of n to build the wreath product H of n copies of N and a version of the procedure `Normalizer(p,n,~X,~D,~B)` based on this approach has been developed.

Following Theorems 5.3.1 and 5.4.1, a program for the computation of the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$, with $|\Omega|$ any integer, based on the procedure presented here, has also been produced.

11.2 Some minimal parabolic subgroups

Using the results from Chapter 10 and the procedure `Normalizer(p,n,~X,~D,~B)` described in the previous section, we have developed some programs for the computation of the minimal parabolic subgroups of H with respect to B. They are all based on the same ideas, but perform different tasks. We shall present some of them here.

We first want to recall some notation.

Let $q \in \pi(p-1)$ and denote by q^{α_q} the highest power of q dividing $p-1$. For $i = 1, \ldots, n-1$, let B_i be the normalizer of a Sylow p-subgroup of $\mathrm{Sym}(p^i)$. Recall that

$$D_{q,i} = Q(1, q, \alpha_q, i) \times \cdots \times Q(n-i, q, \alpha_q, i),$$

where, for $k = 1, \ldots, n-i$, $Q(k, q, \alpha_q, i) = \langle w(k, q, \alpha_q, i) \rangle^{B_i}$ is a homocyclic q-group of exponent q^{α_q} whose Frattini quotient is an absolutely irreducible $\mathrm{GF}(q)B_i$-module. Furthermore any two factors of $D_{q,i}$ are isomorphic.

In Theorem 10.2.2 we have proved that the minimal parabolic subgroups of H with respect to B are in one-to-one correspondence with the B_i-subgroups of $D_{q,i}$, for $q \in \pi(p-1)$ and $i = 1, \ldots, n-1$, which are isomorphic to a nontrivial quotient of one of the factors $Q(k, q, \alpha_q, i)$.

Furthermore, by Theorem 9.2.4, such subgroups are characterized in terms of certain sequences of integers. More specifically, if we set $w_k = w(k, q, \alpha_q, i)$, for $k = 1, \ldots, n-i$, and $w_a = w_1^{a_1} \ldots w_{n-i}^{a_{n-i}}$, for any sequence of integers $a = (a_1, \ldots, a_{n-i})$, then every minimal parabolic subgroup of H with respect to B has the form $P = \langle B, w_a \rangle$, for some $a \in \Gamma_{q,i}$, $q \in \pi(p-1)$ and $i = 1, \ldots, n-1$, where $\Gamma_{q,i}$ is the union of the sets $\Gamma_{q,i}(e)$, for $e = 1, \ldots, \alpha_q$, defined in Section 10.2. Recall that, for $a \in \Gamma_{q,i}(e)$, w_a is an element of order q^e.

The following is a summary of the programs presented, which includes for each of them a brief description of the task performed.

- `SimpleParabolics(p,n,~X,~D,~Q,~P)`:
  it computes all minimal parabolic subgroups of the form $P(k, q, e, i) = \langle B, w(k, q, e, i) \rangle$, with $k = 1, \ldots, n-1, q \in \pi(p-1)$, $e = 1, \ldots, \alpha_q$ and $i = 1, \ldots, n-k$;

- `ParabolicSubgroups(p,n,~X,~D,~Q,~A,~P)`:
  it computes all minimal parabolic subgroups of H with respect to B;

- `SomeParabolics(p,n,module,prime,exp,~X,~D,~Q,~A,~P)`:
  given i, q, e, it calculates all minimal parabolic subgroups of $BD_{q,i}$ with respect to B which are generated by elements of order q^e;

- `OneParabolic(p,n,module,prime,exp,a,~X,~D,~Q,~z,~P)`:
  given i, q, e and a sequence of integers a such that w_a has order q^{α_q}, it makes the minimal parabolic subgroup of $BD_{q,i}$ generated by the element $z = (w_a)^{(p-1)/q^e}$ of order q^e corresponding to the sequence of integers a.

All programs are very much self explanatory and follow naturally from the description of the minimal parabolic subgroups of H. They all use the procedure `Normalizer(p,n,~X,~D,~B)` to make the sequences X and D containing the generators of B. We also remark that, for all of them, the running times are very short. For instance, for $p = 7$ and $n = 4$, we can calculate all minimal parabolic subgroups of H with respect to B in about half a second.
In the remainder of the section we shall look at each of them separately and make some remarks on their key points. When not required by the context, we shall omit the arguments from the name of the procedures.
We start with the procedure `SimpleParabolics`.
First, recall that, by Corollary 10.3.11, the collection of subgroups of the form $P(k, q, \alpha_q, i)$, with $k = 1, \ldots, n-1, q \in \pi(p-1)$ and $i = 1, \ldots, n-k$, is a minimal parabolic system of H with respect to B. Hence the procedure `SimpleParabolics` can be used to produce a minimal parabolic system of H and a version of it, returning only the minimal parabolic subgroups of the form $P(k, q, \alpha_q, i)$, has also been written.
The procedure returns: the sequences X and D containing the p-generators and the p'-generators of B, respectively; and the sequences Q and P such that, for $k = 1, \ldots, n-1$, $t = 1, \ldots, |F|$, $e = 1, \ldots, F[t][2]$ and $i = 1, \ldots, n-k$, $Q[k][t][i]$ is equal to $w(k, q, \alpha_q, i)$ and $P[k][t][i][e]$ is the subgroup $P(k, q, e, i)$, where F denotes the prime factorization of $p-1$, $q = F[t][1]$ and $\alpha_q = F[t][2]$.
While making D, it stores in a sequence V certain factors of elements of D. More precisely, for $k = 1, \ldots, n-1$ and $i = 1, \ldots, n-k$, $V[k][i]$ is equal to the element

$$(f_{n-i} \circ \cdots \circ f_{k+1})(y_k)((f_{n-i} \circ \cdots \circ f_{k+1})(y_k)^{-1})^{x_{n-i+1}},$$

from which the elements of the form $w(k, q, \alpha_q, i)$ are produced by taking powers.

If the chosen value for p is 2 or is not a prime, or if n is 1, the procedure prints an error message and asks for another value of the parameter.

The procedure is included here.

```
procedure SimpleParabolics(p,n,~X,~D,~Q,~P);
// Argument checking on p
while p eq 2 or not IsPrime(p) do
    if p eq 2 then
        "Error in input: there are no minimal parabolic subgroups"\
        "with respect to the prime 2 contained in H, since H=B=T.";
        "Choose another value for the first argument:";
    else
        "Error in input: 1st argument must be a prime number.";
        "Choose another value for it:";
    end if;
    readi p;
end while;
// Argument checking on n
while n eq 1 do
    "Error in input: in this case there is a unique minimal parabolic"\
    "subgroup and it is Sym(",p,")";
    "Choose another value for the 2nd argument";
    readi n;
end while;
// Prime factorization of p-1
r:= p-1;
F:=Factorization(r);
// Building the symmetric groups Sym(p) and Sym(p^n)
G:=Sym(p);
Gn:=Sym(p^n);
```

```
// Building N
N:=AGL(1,p);
// Control on the number and the order of the generators of N
if #Generators(N) gt 2 then
    z:=G!1;
    for i in [1..#Generators(N)] do
        if Order(N.i) eq p then
            S:=sub<G|N.i>;
        end if;
        if Order(N.i) eq p-1 then
            z:=N.i;
        end if;
    end for;
    if z eq Identity(G) then
        for i in [1..#Generators(N)] do
            if Order(N.i) ne p then
                z:=z*N.i;
            end if;
        end for;
    end if;
    Order(z) eq p-1;
    N:=sub<G|S,z>;
end if;
// Building H
H:=N;
for i in [2..n] do
    H:=WreathProduct(H,N);
end for;
// Ordering the generators of H by degree
X:=[Gn|];
Y:=[Gn|];
```

```
K:=Generators(H);
for i in [1..n] do
    for x in K do
        if Degree(x) eq p^i then
            X[i]:=x; aa := x;
        elif
        Degree(x) eq r*p^(i-1) then
            Y[i]:=x; bb:= x;
        end if;
        if assigned(aa) and assigned(bb) then
            break;
        end if;
    end for;
    delete aa; delete bb;
    K := K diff {X[i],Y[i]};
end for;
// Building the sequences D and V
V:=[];
D:=[Gn|];
D[n]:=Y[n];
for k in [1..n-1] do
    D[k]:=Y[k];d:=Y[k];V[k]:=[];
    for j in [k+1..n] do
        V[k][n-j+1]:=d/d^X[j];
        for e in [1..p-1] do
            d:=d^X[j];
            D[k]*:=d;
        end for;
        d:=D[k];
    end for;
end for;
```

```
// Building the sequences Q and P
Q:=[];P:=[];
for k in [1..n-1] do
    Q[k]:=[];P[k]:=[];
    for t in [1..#F] do
        Q[k][t]:=[];P[k][t]:=[];
        rt:=Integers()!(r/F[t][1]^F[t][2]);
        for i in [1..n-k] do
            Q[k][t][i]:=V[k][i]^rt;
            P[k][t][i]:=[];
            z:=Q[k][t][i];
            P[k][t][i][F[t][2]]:=sub<Gn|X,D,z>;
            for e in [1..F[t][2]-1] do
                z:=z^F[t][1];
                P[k][t][i][F[t][2]-e]:=sub<Gn|X,D,z>;
            end for;
        end for;
    end for;
end for;
end procedure;
```

Next we consider the procedure `ParabolicSubgroups` which computes all minimal parabolic subgroups of G with respect to B which are contained in H.

The procedures returns: the sequences X, D and Q, as in `SimpleParabolics`; a sequence A corresponding to the set Γ defined in Theorem 10.2.3; and a sequence P containing the minimal parabolic subgroups.

We want to describe how the sequence A is made. We do this using the more compact notation from Section 10.2, rather than the notation of the program.

If F is the prime factorization of $p-1$, then, for $t = 1, \ldots, |F|$, $e = 1, \ldots, F[t][2]$, $i = 1, \ldots, n-1$ and $j = 1, \ldots, n-i$, the element $A[t][e][n-i][j]$ of A corresponds to the set of sequences $\Gamma_{q,i}(e, j)$, such that $q = F[t][1]$ and $\alpha_q = F[t][2]$.

We start by making $\Gamma_{q,1}(\alpha_q, n-1)$, which is the set of all sequences a of $\mathbb{Z}_{q^{\alpha_q}}$ of length $n-1$ such that $a_{n-1} = 1$ and $a_h \equiv 0$ modulo q, for all $h < n-1$. Rotating the elements of $\Gamma_{q,1}(\alpha_q, n-1)$ by one position to the left and taking for the last entry all possible values in $\mathbb{Z}_{q^{\alpha_q}}$, we make $\Gamma_{q,1}(\alpha_q, n-2)$ and recursively the set $\Gamma_{q,1}(\alpha_q, j)$, for all $j < n-1$. We have so obtained the set $\Gamma_{q,1}(\alpha_q)$ and can make the set $\Gamma_{q,i}(\alpha_q)$, for $i = 2, \ldots, n-1$, by removing the last entry of the elements of $\Gamma_{q,i+1}(\alpha_q)$. Finally, we only have to multiply by $q^{\alpha_q - e}$ all the sequence of each set $\Gamma_{q,i}(\alpha_q)$ to make the set $\Gamma_{q,i}(e)$.
The procedure is reported below.

```
procedure ParabolicSubgroups(p,n,~X,~D,~Q,~A,~P);
// Argument checking on p
while p eq 2 or not IsPrime(p) do
    if p eq 2 then
        "Error in input: there are no minimal parabolic subgroups"\
        "with respect to the prime 2 contained in H, since H=B=T.";
        "Choose another value for the first argument:";
    else
        "Error in input: 1st argument must be a prime number.";
        "Choose another value for it:";
    end if;
    readi p;
end while;
// Argument checking on n
while n eq 1 do
    "Error in input: in this case there is a unique minimal parabolic"\
    "subgroup and it is Sym(",p,")";
    "Choose another value for the 2nd argument";
    readi n;
end while;
// Prime factorization of p-1
r:= p-1;
```

```
F:=Factorization(r);
// Building the symmetric groups Sym(p) and Sym(p^n)
G:=Sym(p);
Gn:=Sym(p^n);
// Building N
N:=AGL(1,p);
// Control on the number and the order of the generators of N
if #Generators(N) gt 2 then
    z:=G!1;
    for i in [1..#Generators(N)] do
        if Order(N.i) eq p then
            S:=sub<G|N.i>;
        end if;
        if Order(N.i) eq p-1 then
            z:=N.i;
        end if;
    end for;
    if z eq Identity(G) then
        for i in [1..#Generators(N)] do
            if Order(N.i) ne p then
                z:=z*N.i;
            end if;
        end for;
    end if;
    Order(z) eq p-1;
    N:=sub<G|S,z>;
end if;
// Building H
H:=N;
for i in [2..n] do
    H:=WreathProduct(H,N);
```

```
end for;
// Ordering the generators of H by degree
X:=[Gn|];
Y:=[Gn|];
K:=Generators(H);
for i in [1..n] do
    for x in K do
        if Degree(x) eq p^i then
            X[i]:=x; aa := x;
        elif
        Degree(x) eq r*p^(i-1) then
            Y[i]:=x; bb:= x;
        end if;
        if assigned(aa) and assigned(bb) then
            break;
        end if;
    end for;
    delete aa; delete bb;
    K := K diff {X[i],Y[i]};
end for;
// Building the sequences D and V
V:=[];
D:=[Gn|];
D[n]:=Y[n];
for k in [1..n-1] do
    D[k]:=Y[k];d:=Y[k];V[k]:=[];
    for j in [k+1..n] do
        V[k][n-j+1]:=d/d^X[j];
        for e in [1..p-1] do
            d:=d^X[j];
            D[k]*:=d;
```

```
        end for;
        d:=D[k];
    end for;
end for;
// Building the sequence Q
Q:=[];
for k in [1..n-1] do
    Q[k]:=[];
    for t in [1..#F] do
        Q[k][t]:=[];
        rt:=Integers()!(r/F[t][1]^F[t][2]);
        for i in [1..n-k] do
            Q[k][t][i]:=V[k][i]^rt;
        end for;
    end for;
end for;
// Building the sequences of integers
A:=[];
for t in [1..#F] do
    // Sequences of maximal length and maximal exponent
    R:={Integers()|0..F[t][1]^F[t][2]-1};
    S:={Integers()|a*F[t][1] mod F[t][1]^F[t][2]: a in R};
    C:=Subsequences(S,n-1);
    A[t]:=[]; A[t][F[t][2]]:=[]; A[t][F[t][2]][n-1]:=[];
    A[t][F[t][2]][n-1][n-1]:={Remove(x,n-1): x in C};
    A[t][F[t][2]][n-1][n-1]:={Insert(x,n-1,1): x in A[t][F[t][2]][n-1][n-1]};
    for j in [n-2..1 by -1] do
        A[t][F[t][2]][n-1][j]:={Rotate(x,-1): x in A[t][F[t][2]][n-1][j+1]};
        temp:={Remove(x,n-1): x in A[t][F[t][2]][n-1][j]};
        temp:={Append(x,y): x in temp, y in R diff S};
        A[t][F[t][2]][n-1][j]:=A[t][F[t][2]][n-1][j] join temp;
```

```
    end for;
    // Reducing the length of the sequences
    for i in [2..n-1] do
        A[t][F[t][2]][n-i]:=[];
        for j in [1..n-i] do
            A[t][F[t][2]][n-i][j]:={Prune(x): x in A[t][F[t][2]][n-i+1][j]};
        end for;
    end for;
    // Reducing the exponent of the sequences
    for e in [F[t][2]-1 ..1 by -1] do
        A[t][e]:=[];
        for i in [1..n-1] do
            A[t][e][n-i]:=[];
            for j in [1..n-i] do
                A[t][e][n-i][j]:={[x[h]*F[t][1] mod F[t][1]^F[t][2]:\
                    h in [1..n-i]]: x in A[t][e+1][n-i][j]};
            end for;
        end for;
    end for;
end for;
// Building the minimal parabolic subgroups
P:=[];
for i in [1..n-1] do
    P[i]:=[];
    for t in [1..#F] do
        P[i][t]:=[];
        for e in [1..F[t][2]] do
            P[i][t][e]:=[];c:=0;
            for j in [1..n-i] do
                for x in A[t][e][n-i][j] do
                    z:=Q[1][t][i]^x[1];
```

```
                    for k in [2..n-i] do
                        z*:=Q[k][t][i]^x[k];
                    end for;
                    c+:=1;
                    P[i][t][e][c]:=sub<Gn|X,D,z>;
                end for;
            end for;
        end for;
    end for;
end for;
end procedure;
```

The procedure SomeParabolics is derived from ParabolicSubgroups by selecting the sets of sequences $\Gamma_{q,i}(e)$, for some given i, q, e.

It contains the additional parameters module, prime and exp, corresponding to i, q and e, respectively. Note that the parameter prime gives the position of the chosen prime q in the prime factorization F of $p-1$, and not the prime itself.

The parameters are to be chosen as follows: module is an integer between 1 and $n-1$; prime is an integer between 1 and $|F|$, where F is the prime factorization of $p-1$; exp is an integer between 1 and $F[\texttt{prime}][2]$. For any of the parameters not falling in the right range, an error message is printed and a new value is requested.

```
procedure SomeParabolics(p,n,module,prime,exp,~X,~D,~Q,~A,~P);
// Argument checking on p
while p eq 2 or not IsPrime(p) do
    if p eq 2 then
        "Error in input: there are no minimal parabolic subgroups"\
        "with respect to the prime 2 contained in H, since H=B=T.";
        "Choose another value for the first argument:";
    else
        "Error in input: 1st argument must be a prime number.";
        "Choose another value for it:";
```

```
    end if;
    readi p;
end while;
// Argument checking on n
while n eq 1 do
    "Error in input: in this case there is a unique minimal parabolic"\
    "subgroup and it is Sym(",p,")";
    "Choose another value for the 2nd argument";
    readi n;
end while;
// Argument checking on module
while module lt 1 or module gt n-1 do
    "Error in input: 3rd argument must be an integer between 1 and", n-1;
    "Choose another value for it:";
    readi module;
end while;
// Prime factorization of p-1
r:= p-1;
F:=Factorization(r);
// Argument checking on prime
while prime lt 1 or prime gt #F do
    "Error in input: 4th argument must be an integer between 1 and", #F;
    "Choose another value for it:";
    readi prime;
end while;
// Argument checking on exp
while exp lt 1 or exp gt F[prime][2] do
    "Error in input: 5th argument must be an integer between 1 and",\
     F[prime][2];
    "Choose another value for it:";
    readi exp;
```

```
end while;
// Building the symmetric groups Sym(p) and Sym(p^n)
G:=Sym(p);
Gn:=Sym(p^n);
// Building N
N:=AGL(1,p);
// Control on the number and the order of the generators of N
if #Generators(N) gt 2 then
    z:=G!1;
    for i in [1..#Generators(N)] do
        if Order(N.i) eq p then
            S:=sub<G|N.i>;
        end if;
        if Order(N.i) eq p-1 then
            z:=N.i;
        end if;
    end for;
    if z eq Identity(G) then
        for i in [1..#Generators(N)] do
            if Order(N.i) ne p then
                z:=z*N.i;
            end if;
        end for;
    end if;
    Order(z) eq p-1;
    N:=sub<G|S,z>;
end if;
// Building H
H:=N;
for i in [2..n] do
    H:=WreathProduct(H,N);
```

```
end for;
// Ordering the generators of H by degree
X:=[Gn|];
Y:=[Gn|];
K:=Generators(H);
for i in [1..n] do
    for x in K do
        if Degree(x) eq p^i then
            X[i]:=x; aa := x;
        elif
        Degree(x) eq r*p^(i-1) then
            Y[i]:=x; bb:= x;
        end if;
        if assigned(aa) and assigned(bb) then
            break;
        end if;
    end for;
    delete aa; delete bb;
    K := K diff {X[i],Y[i]};
end for;
// Building the sequences D and V
V:=[];
D:=[Gn|];
D[n]:=Y[n];
for k in [1..n-1] do
    D[k]:=Y[k];d:=Y[k];
    for j in [k+1..n] do
        if k le n-module and n-j+1 eq module then
            V[k]:=d/d^X[j];
        end if;
        for e in [1..p-1] do
```

```
            d:=d^X[j];
            D[k]*:=d;
        end for;
        d:=D[k];
    end for;
end for;
// Building the sequence Q
Q:=[];
for k in [1..n-module] do
    e:=Integers()!(r/F[prime][1]^exp);
    Q[k]:=V[k]^e;
end for;
// Building the sequences of integers
A:=[];
R:={Integers()|0..F[prime][1]^exp-1};
S:={Integers()|a*F[prime][1] mod F[prime][1]^exp : a in R};
C:=Subsequences(S,n-module);
A[n-module]:={Remove(x,n-module): x in C};
A[n-module]:={Insert(x,n-module,1) : x in A[n-module]};
for j in [n-module-1..1 by -1] do
    A[j]:={Rotate(x,-1) : x in A[j+1]};
    temp:={Remove(x,n-module) : x in A[j]};
    temp:={Append(x,y) : x in temp, y in R diff S};
    A[j]:=A[j] join temp;
end for;
// Building the sequence P
P:=[];
c:=0;
for j in [1..n-module] do
    for x in A[j] do
        z:=Q[1]^x[1];
```

```
        for h in [2..n-module] do
            z*:=Q[h]^x[h];
        end for;
        c+:=1;
        P[c]:=sub<Gn|X,D,z>;
    end for;
end for;
end procedure;
```

We conclude with the procedure `OneParabolic`, which, based on `SomeParabolics`, returns the minimal parabolic subgroup of $BD_{q,i}$ corresponding to a given sequence of integers.
The procedure has four additional parameters in input: `module`, `prime` and `exp`, corresponding to i, q and e, respectively, and defined as for the procedure `SomeParabolics`; and a sequence of integers a of length at least $n-$`module` such that at least one entry is coprime to $F[$`prime`$][1]$. This guarantees that the element w_a has maximal order. We remark that, except for the restrictions just mentioned, a can be any sequence and, in particular, a does not necessarily belong to any of the sets $\Gamma_{q,i}$.
For any of the parameters not falling in the right range or not satisfying the required conditions the program prints an error message and asks for another value of the parameter.

```
procedure OneParabolic(p,n,module,prime,exp,a,~X,~D,~Q,~z,~P);
// Argument checking on p
while p eq 2 or not IsPrime(p) do
    if p eq 2 then
        "Error in input: there are no minimal parabolic subgroups"\
        "with respect to the prime 2 contained in H, since H=B=T.";
        "Choose another value for the first argument:";
    else
        "Error in input: 1st argument must be a prime number.";
        "Choose another value for it:";
    end if;
    readi p;
```

```
end while;
// Argument checking on n
while n eq 1 do
    "Error in input: in this case there is a unique minimal parabolic"\
    "subgroup and it is Sym(",p,")";
    "Choose another value for the 2nd argument";
    readi n;
end while;
// Argument checking on module
while module lt 1 or module gt n-1 do
    "Error in input: 3rd argument must be an integer between 1 and", n-1;
    "Choose another value for it:";
    readi module;
end while;
// Prime factorization of p-1
r:= p-1;
F:=Factorization(r);
// Argument checking on prime
while prime lt 1 or prime gt #F do
    "Error in input: 4th argument must be an integer between 1 and", #F;
    "Choose another value for it:";
    readi prime;
end while;
// Argument checking on exp
while exp lt 1 or exp gt F[prime][2] do
    "Error in input: 5th argument must be an integer between 1 and",\
     F[prime][2];
    "Choose another value for it:";
    readi exp;
end while;
// Argument checking on the sequence a
```

```
while #a lt n-module do
    "Error in input: 6th argument must be a sequence of integers of"\
    "length at least", n-module;
    "Choose another value for it:";
    a:=[];
    for j in [1..n-module] do
        readi x;
        a:=Append(a,x);
    end for;
end while;
while forall{a[j]:j in [1..n-module]|IsDivisible(a[j],F[prime][1])} do
    "Error in input: 6th argument must be a sequence of integers with at"\
    "least one entry coprime to", F[prime][1];
    "Reassign it:";
    a:=[];
    for j in [1..n-module] do
        readi x;
        a:=Append(a,x);
    end for;
end while;
// Building the symmetric groups Sym(p) and Sym(p^n)
G:=Sym(p);
Gn:=Sym(p^n);
// Building N
N:=AGL(1,p);
// Control on the number and the order of the generators of N
if #Generators(N) gt 2 then
    z:=G!1;
    for i in [1..#Generators(N)] do
        if Order(N.i) eq p then
            S:=sub<G|N.i>;
```

```
        end if;
        if Order(N.i) eq p-1 then
            z:=N.i;
        end if;
    end for;
    if z eq Identity(G) then
        for i in [1..#Generators(N)] do
            if Order(N.i) ne p then
                z:=z*N.i;
            end if;
        end for;
    end if;
    Order(z) eq p-1;
    N:=sub<G|S,z>;
end if;
// Building H
H:=N;
for i in [2..n] do
    H:=WreathProduct(H,N);
end for;
// Ordering the generators of H by degree
X:=[Gn|];
Y:=[Gn|];
K:=Generators(H);
for i in [1..n] do
    for x in K do
        if Degree(x) eq p^i then
            X[i]:=x; aa := x;
        elif
        Degree(x) eq r*p^(i-1) then
            Y[i]:=x; bb:= x;
```

```
        end if;
        if assigned(aa) and assigned(bb) then
            break;
        end if;
    end for;
    delete aa; delete bb;
    K := K diff {X[i],Y[i]};
end for;
// Building the sequences D and V
V:=[];
D:=[Gn|];
D[n]:=Y[n];
for k in [1..n-1] do
    D[k]:=Y[k];d:=Y[k];
    for j in [k+1..n] do
        if k le n-module and n-j+1 eq module then
            V[k]:=d/d^X[j];
        end if;
        for e in [1..p-1] do
            d:=d^X[j];
            D[k]*:=d;
        end for;
        d:=D[k];
    end for;
end for;
// Building the sequence Q
Q:=[];
for k in [1..n-module] do
    e:=Integers()!(r/F[prime][1]^exp);
    Q[k]:=V[k]^e;
end for;
```

```
// Building the extra generator z
z:=Q[1]^a[1];
for h in [2..n-module] do
    z*:=Q[h]^a[h];
end for;
// Making the minimal parabolic subgroup P
P:=sub<Gn|X,D,z>;
end procedure;
```

Bibliography

[1] Aschbacher, M., *Finite Group Theory*, Cambridge Univ. Press, Cambridge, 1986.

[2] Bosma, W. and Cannon, J., *Handbook of MAGMA functions*, Sidney, January 1998.

[3] Buekenhout, F., *Diagram geometries for sporadic groups*, Finite groups–coming of age (Montreal, Que., 1982), Contemp. Math., vol. 45, Amer. Math. Soc., 1985, pp. 1–32.

[4] Cameron, P. J., *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[5] Cárdenas, H. and Lluis, E., *The normalizer of the Sylow p-group of the symmetric group* S_{p^n}, Bol. Soc. Mat. Mexicana (2) **9** (1964), 1–6, Spanish.

[6] Carter, R. W., *Simple Groups of Lie Type*, second ed., John Wiley & Sons, New York, 1989.

[7] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson, R. A., *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[8] Conway, J. H. and Guy, R. K., *The book of numbers*, Copernicus, New York, 1996.

[9] Curtis, C. W. and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, New York, 1962.

[10] Dixon, J. D. and Mortimer, B., *Permutation Groups*, Springer–Verlag, Berlin, 1996.

[11] Dmitruk, Ju. V. and Suščansk′kiĭ, V. Ī., *Construction of Sylow 2-subgroups of alternating groups and normalizers of Sylow subgroups in symmetric and alternating groups*, Ukrain. Mat. Zh. **33** (1981), no. 3, 304–312, Russian.

[12] Findlay, W., *The Sylow subgroups of the symmetric group*, Trans. Amer. Math. Soc. **5** (1904), no. 3, 263–278.

[13] Fisher, T., *A bound for the dimension of $H_0(\mathcal{F}_V)$ of modules $V(\lambda_i + \lambda_j)$ for $A_l(q)$*, J. Algebra **143** (1991), no. 1, 119–129.

[14] Gorenstein, D., *Finite Groups*, second ed., Chelsea Publishing Company, New York, 1980.

[15] Huppert, B., *Endliche Gruppen I*, Springer–Verlag, Berlin, 1967.

[16] Huppert, B. and Blackburn, N., *Finite Groups II*, Springer–Verlag, Berlin, 1982.

[17] Huppert, B. and Blackburn, N., *Finite Groups III*, Springer–Verlag, Berlin, 1982.

[18] Ivanov, A. A., *A geometric characterization of the Monster*, Groups, combinatorics & geometry (Durham, 1990), London Math. Soc. Lecture Note Ser., vol. 165, Cambridge Univ. Press, 1992, pp. 46–62.

[19] Ivanov, A. A. and Meierfrankenfeld, U., *Simple connectedness of the 3-local geometry of the Monster*, J. Algebra **194** (1997), no. 2, 383–407.

[20] Kaloujnine, L., *La structure des p-groupes de Sylow des groupes symmétriques finis*, Ann. Sci. École Norm. Sup. **65** (1948), 235–276.

[21] Lempken, W., Parker, C. W., and Rowley, P., *Minimal parabolic systems of the symmetric and alternating groups*, The Atlas of finite groups: ten years on (Birmingham, 1995) (R. T. Curtis and R. A. Wilson, eds.), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, 1998, pp. 149–162.

[22] Neumann, P. M., *Transitive permutation groups of prime degree*, J. London Math. Soc. (2) **5** (1972), 202–208.

[23] Ore, O., *Some remarks on commutators*, Proc. Americ. Math. Soc. **2** (1951), 307–314.

[24] Robinson, D. J. S., *A Course in the Theory of Groups*, second ed., Springer–Verlag, Berlin, 1996.

[25] Ronan, M. A., *Lectures on Buildings*, Perspectives in Mathematics, vol. 7, Academic Press Inc., Boston, MA, 1989.

[26] Ronan, M. A. and Smith, S. D., 2-*Local Geometries for some Sporadic Groups*, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, CA, 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., 1980, pp. 283–289.

[27] Ronan, M. A. and Smith, S. D., *Sheaves on buildings and modular representations of Chevalley groups*, J. Algebra **96** (1985), no. 2, 319–346.

[28] Ronan, M. A. and Smith, S. D., *Universal presheaves on group geometries, and modular representations*, J. Algebra **102** (1986), no. 1, 135–154.

[29] Ronan, M. A. and Smith, S. D., *Computation of* 2-*modular sheaves and representations for* $L_4(2), A_7, 3S_6$, *and* M_{24}, Comm. Algebra **17** (1989), no. 5, 1199–1237.

[30] Ronan, M. A. and Stroth, G., *Minimal Parabolic Geometries for the Sporadic Groups*, European J. Combin. **5** (1984), no. 1, 59–91.

[31] Rowley, P., *Minimal parabolic systems with diagram* $\circ\!-\!\!\!-\!\!\!-\!\circ\!-\!\!\!-\!\!\!-\!\circ\overset{\sim}{=\!=}\circ$, J. Algebra **141** (1991), no. 1, 204–251.

[32] Shpectorov, S. V., *Natural representations of some tilde and Petersen type geometries*, Geom. Dedicata **54** (1995), no. 1, 87–102.

[33] Smith, S. D., *Irreducible modules and parabolic subgroups*, J. Algebra **75** (1982), 286–289.

[34] Stroth, G., *Parabolics in finite groups*, Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983–1984), Cambridge Univ. Press, 1985, pp. 211–223.

[35] Stroth, G. and Wong, S. K., *Minimal parabolic systems and small representations*, Comm. Algebra **15** (1987), no. 4, 751–790.

[36] Suzuki, M., *Group Theory I*, Springer–Verlag, Berlin, 1982.

[37] Suzuki, M., *Group Theory II*, Springer–Verlag, Berlin, 1986.

[38] Tits, J., *Buildings of spherical type and finite BN-pairs*, Lecture Notes in Mathematics, vol. 386, Springer-Verlag, Berlin, 1974.

[39] Weir, A. J., *The Sylow subgroups of the symmetric groups*, Proc. Amer. Math. Soc. **6** (1955), 534–541.

[40] Weisner, L., *On the Sylow Subgroups of the Symmetric and Alternating Groups*, Amer. J. Math. **47** (1925), 121–124.

[41] Wielandt, H., *Finite Permutation Groups*, Academic Press, New York, 1964.

[42] Wilson, J. S., *Lectures on Group Theory*, Birmingham, November 1995.

[43] Zassenhaus, H., *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 17–44.