



รายงานวิจัยฉบับสมบูรณ์

โครงการ

เรขาคณิตแบบ p -โลคัลที่ใหญ่สุดเฉพาะกลุ่มสำหรับกรุป

สมมาตร

โดย

ดร.ทิพวัลย์ พัฒนางูร

ศาสตราจารย์ ดร. สมพงษ์ ธรรมพงษา

30 มิถุนายน พ.ศ. 2549



รายงานวิจัยฉบับสมบูรณ์

โครงการ

เรขาคณิตแบบ p -โกลคัลที่ใหญ่ที่สุดเฉพาะกลุ่มสำหรับกรุปสมมาตร

โดย

ดร.ทิพัลย์ พัฒนางกูร

ศาสตราจารย์ ดร. สมพงษ์ ธรรมพงษา

30 มิถุนายน พ.ศ. 2549

รายงานวิจัยฉบับสมบูรณ์

โครงการ

เรขาคณิตแบบ p -โลคัลที่ใหญ่ที่สุดเฉพาะกลุ่มสำหรับกรุปสมมาตร

โดย

ดร.ทิพัลย์ พัฒนางกูร

มหาวิทยาลัยธรรมศาสตร์

ศาสตราจารย์ ดร. สมพงษ์ ธรรมพงษ์

มหาวิทยาลัยเชียงใหม่

สนับสนุนโดยสำนักงานคณะกรรมการการอุดมศึกษา

และสำนักงานกองทุนสนับสนุนการวิจัย

(ความเห็นในรายงานนี้เป็นของผู้วิจัย สกอ. และ สกว. ไม่จำเป็นต้องเห็นด้วยเสมอไป)

กิตติกรรมประกาศ

โครงการวิจัยนี้สำเร็จลงด้วยดี จากความช่วยเหลืออย่างดียิ่งของคณาจารย์ทุกท่านที่ได้ชี้แนะแนวทางและมอบความรู้แก่ผู้วิจัย โดยเฉพาะอย่างยิ่งขอกราบขอบคุณ ศาสตราจารย์ ดร. สมพงษ์ ธรรมพงษา ซึ่งเป็นนักวิจัยที่ปรึกษา ที่กรุณาให้คำปรึกษา แนะนำ ตลอดจนตรวจแก้ไขข้อบกพร่องต่าง ๆ จนกระทั่งโครงการวิจัยฉบับนี้สมบูรณ์ และขอขอบคุณ Professor Peter J. Rowley สำหรับคำแนะนำต่าง ๆ ในการทำโครงการวิจัยนี้

ขอขอบคุณสำนักงานคณะกรรมการการอุดมศึกษาและสำนักงานกองทุนสนับสนุนการวิจัย ที่กรุณามอบทุนพัฒนาศักยภาพในการทำงานวิจัยของอาจารย์รุ่นใหม่ให้แก่ผู้วิจัย ซึ่งทำให้โครงการวิจัยฉบับนี้แล้วเสร็จด้วยดี

สุดท้าย ขอขอบคุณภาควิชาคณิตศาสตร์และสถิติ มหาวิทยาลัยธรรมศาสตร์ ที่ให้การสนับสนุนในโครงการวิจัยนี้ตลอดมา

ดร. ทิพวัลย์ พัฒนางูร

หัวหน้าโครงการวิจัยผู้รับทุน

30 มิถุนายน พ.ศ. 2549

บทคัดย่อ

รหัสโครงการ : MRG4780092

ชื่อโครงการ : เรขาคณิตแบบ p -โลคัลที่ใหญ่ที่สุดเฉพาะกลุ่มสำหรับกรุปสมมาตร

ชื่อนักวิจัย : ดร.ทิพัลย์ พัฒนงกูร มหาวิทยาลัยธรรมศาสตร์
ศาสตราจารย์ ดร. สมพงษ์ ธรรมพงษา มหาวิทยาลัยเชียงใหม่

E-mail Address : tipaval@mathstat.sci.tu.ac.th และ sompong@chiangmai.ac.th

ระยะเวลาโครงการ : 2 ปี (ตั้งแต่วันที่ 1 กรกฎาคม 2547 ถึงวันที่ 30 มิถุนายน 2549)

จุดมุ่งหมายของโครงการวิจัยนี้คือการศึกษากรุ๊ปย่อยแบบ p -โลคัลของกรุปสมมาตร $Sym(n)$ ในที่นี้จะเน้นการศึกษาเซต $N_{\max}(G, B)$ ซึ่งเป็นเซตที่ประกอบด้วยกรุ๊ปย่อยแบบ p -โลคัลที่ใหญ่ที่สุดเฉพาะกลุ่มทั้งหมดสำหรับกรุปสมมาตร $G = Sym(n)$ ที่มี T เป็นกรุ๊ปย่อยซิโลว์ (สำหรับจำนวนเฉพาะ p) ของ G เมื่อ $B = N_G(T)$ หลังการศึกษาทำให้ทราบเกี่ยวกับโครงสร้างของกรุ๊ปย่อยที่เป็นสมาชิกของ $N_{\max}(G, B)$ ในบางกรณี เช่น กรุปสมมาตร $Sym(p)$, $Sym(kp)$ และ $Sym(p+k)$ เมื่อ p เป็นจำนวนเฉพาะใด ๆ เป็นต้น จากการศึกษาดังกล่าวจึงได้ผลงานวิจัย อาทิ เช่น

Theorem 1 Let $G = Sym(\Omega)$ with $|\Omega| = p$, where p is a prime. Suppose that $T \in Syl_p(G)$ and $B = N_G(T)$. Then $N_{\max}(G, B) = \{B\}$.

Theorem 2 Let $G = Sym(\Omega)$ with $|\Omega| = n$. Suppose that $T \in Syl_p(G)$ and $B = N_G(T)$, where p is a prime. Then B is a maximal p -local subgroup with respect to B if one of the following occurs:

- (i) $n = p$
- (ii) $n = kp$ with $1 < k < p$
- (iii) $n = p + k$ with $1 \leq k < p$.

ข้อเสนอแนะสำหรับงานวิจัยในอนาคตคือ ศึกษาความสัมพันธ์ของกรุ๊ปย่อยใน $N_{\max}(G, B)$ กับกรุ๊ปย่อยเชิงพาราโบลาที่เล็กที่สุดเฉพาะกลุ่มของ G (สำหรับจำนวนเฉพาะ p)

คำหลัก : Symmetric group, Sylow p -subgroup, Normalizer, Maximal p -local subgroup

Abstract

Project Code : MRG4780092

Project Title: Maximal p -local geometries for the symmetric groups.

Investigator : Dr. Tipaval Phatthanangkul Thammasat University
Professor Sompong Dhompongsa Chiang Mai University

E-mail Address : tipaval@mathstat.sci.tu.ac.th and sompong@chiangmai.ac.th

Project Period : 2 years (1 July 2004 – 30 June 2006)

The purpose of this project is to investigate certain p -local subgroups of the symmetric group $Sym(n)$. Our main focus is the subgroups in the set $N_{\max}(G, B)$ consisting of all maximal p -local subgroups of $G = Sym(n)$ with respect to B , the normalizer of a Sylow p -subgroup of G in G . The structure of the subgroups in $N_{\max}(G, B)$ is determined for some critical cases. The main results is the following:

Theorem 1 Let $G = Sym(\Omega)$ with $|\Omega| = p$, where p is a prime. Suppose that $T \in Syl_p(G)$ and $B = N_G(T)$. Then $N_{\max}(G, B) = \{B\}$.

Theorem 2 Let $G = Sym(\Omega)$ with $|\Omega| = n$. Suppose that $T \in Syl_p(G)$ and $B = N_G(T)$, where p is a prime. Then B is a maximal p -local subgroup with respect to B if one of the following occurs:

- (i) $n = p$
- (ii) $n = kp$ with $1 < k < p$
- (iii) $n = p + k$ with $1 \leq k < p$.

The future work is to study the relationship between the maximal p -local subgroups and the minimal parabolic subgroups of G with respect to B (for the prime p).

Keywords : Symmetric group, Sylow p -subgroup, Normalizer, Maximal p -local subgroup

MAXIMAL p -LOCAL GEOMETRIES FOR THE
SYMMETRIC GROUPS

by

Tipaval Phatthanangkul

and

Sompong Dhompongsa

The Commission On Higher Education
and The Thailand Research Fund

June, 2006

บทคัดย่อ

จุดมุ่งหมายของโครงการวิจัยนี้คือการศึกษากรุปย่อยแบบ p -โลคัลของกรุปสมมาตร $Sym(n)$ ในที่นี้จะเน้นการศึกษาเซต $N_{\max}(G, B)$ ซึ่งเป็นเซตที่ประกอบด้วยกรุปย่อยแบบ p -โลคัลที่ใหญ่ที่สุดเฉพาะกลุ่มทั้งหมดสำหรับกรุปสมมาตร $G = Sym(n)$ ที่มี T เป็นกรุปย่อยซิโลว์ (สำหรับจำนวนเฉพาะ p) ของ G เมื่อ $B = N_G(T)$ หลังการศึกษาทำให้ทราบเกี่ยวกับโครงสร้างของกรุปย่อยที่เป็นสมาชิกของ $N_{\max}(G, B)$ ในบางกรณี

Abstract

The purpose of this research is to investigate certain p -local subgroups of the symmetric group $\text{Sym}(n)$. Our main focus is the subgroups in the set $\mathcal{N}_{\max}(G, B)$ consisting of all maximal p -local subgroups of $G = \text{Sym}(n)$ with respect to B , the normalizer of a Sylow p -subgroup of G in G . The structure of the subgroups in $\mathcal{N}_{\max}(G, B)$ is determined for some critical cases.

Acknowledgements

Firstly, I would like to thank Professor Sompong Dhompongsa for his invaluable advice and guidance throughout my work. Words cannot express my gratitude because without his help, my work would not have been possible.

Special thanks to Professor Peter J. Rowley for valuable comments and helpful suggestions.

Appreciation is extended to the Commission On Higher Education and the Thailand Research Fund (contract number MRG4780092) for the financial support that made this research project possible.

Finally, further thanks to the Department of Mathematics and Statistics, Thammasat University, for their support.

Contents

1	Introduction	1
2	Preliminary Results	5
2.1	Sylow's Theorems	5
2.2	The subgroup $O_p(H)$	10
2.3	Semidirect products	10
2.4	Finite permutation groups	11
2.5	Imprimitive and primitive groups	17
2.6	Sylow p -subgroups of the symmetric group	22
2.7	The normalizer of a Sylow p -subgroup of the symmetric group	29
2.8	Maximal subgroups of the symmetric groups	34
3	Maximal p-local subgroups of symmetric groups	36
3.1	$\text{Sym}(p^m)$	36
3.2	$\text{Sym}(kp^m)$	39
3.3	$\text{Sym}(k_1p^m + k_0)$	39
3.4	An overview of the problem	42
3.5	$\mathcal{N}_{\max}(G^*, T^*)$ for $G^* \cong \text{Alt}(\Omega)$	44
A	Examples of the maximal p-local subgroups of G	46

List of Figures

A.1	The lattice of the maximal 2-local subgroups of $\text{Sym}(12)$	47
A.2	The lattice of the maximal 2-local subgroups of $\text{Sym}(6)$	48
A.3	The lattice of the maximal 2-local subgroups of $\text{Sym}(9)$	49
A.4	The lattice of the maximal 3-local subgroups of $\text{Sym}(27)$	50

Notation

$\mathcal{N}(H, B)$	2
$\mathcal{N}_{max}(H, B)$	2
$\text{Sym}(\Omega)$	3
$\text{Syl}_p(H)$	6
$O_p(H)$	10
$K \rtimes L$	11
$\text{Stab}_H(\alpha)$	14
$H \wr K$	14

Any unexplained notation follows that of the ATLAS [6].

Chapter 1

Introduction

Maximal 2-local geometries for certain sporadic simple groups were firstly introduced by Ronan and Smith [20]. These geometries were inspired by the theory of buildings for the groups of Lie type which was developed by Tits ([24], [25]) in the fifties. For each finite simple group of Lie type, there is a natural geometry associated with it called its building. For G a group of Lie type of characteristic p , its building is a geometric structure whose vertex stabilizers are the maximal parabolic subgroups which are also p -local subgroups of G containing a Sylow p -subgroup. As is well-known, each building has a Coxeter diagram associated with it. In [3], Buekenhout generalized these concepts to obtain diagrams for many geometries related to sporadic simple groups. Ronan and Smith [20] pursued these ideas further and introduced the maximal 2-local geometries. Other variants on buildings for the sporadic simple groups have been defined, notably the minimal parabolic geometries as described in [21] by Ronan and Stroth.

We now define what we mean, generally, by a minimal parabolic subgroup. Suppose that H is a finite group and p is a prime dividing the order of H . Let S be a Sylow p -subgroup of H and B the normalizer of S in H . A subgroup P of H properly containing B is said to be a *minimal parabolic subgroup* of H with respect to B if B lies in exactly one maximal subgroup of P .

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 [20] and Ronan and Stroth [21], in which they study minimal parabolic geometries for the 26 sporadic finite simple groups. The connection between minimal parabolic subgroups and group

geometries is the best illustrated in the case of groups of Lie type in their defining characteristic. For a group of Lie type, its minimal parabolic system is always geometric. This is not always the case in general (see [21]). Many studies on the minimal parabolic system of special subgroups have been done over the years. For example, in [18], Lempken, Parker and Rowley determined all the minimal parabolic subgroups and system for the symmetric and alternating groups, with respect to the prime $p = 2$. Later, Covello [8] has studied minimal parabolic subgroups and systems for the symmetric group with respect to an odd prime p dividing the order of the group. The main results are about the symmetric groups of degree p^r , she also establishes some more general results. More recently, in [22], Rowley and Saninta investigated the maximal 2-local geometries for the symmetric groups. Furthermore, Saninta [23] considered the relationship between the maximal 2-local subgroups and the minimal parabolic subgroups for the symmetric groups. In this paper we shall investigate maximal p -local geometries for the symmetric groups.

Let H , p , S and B be defined as above. Define

$$\mathcal{N}(H, B) = \{K \mid B \leq K \leq H \text{ and } O_p(K) \neq 1\}$$

where $O_p(K)$ is a maximal normal p -subgroup of K . A subgroup in $\mathcal{N}(H, B)$ is said to be a **p -local subgroup** of H with respect to B and a subgroup in $\mathcal{N}(H, B)$ which is maximal under inclusion is said to be a **maximal p -local subgroup** of H with respect to B . We denoted the collection of maximal p -local subgroups of H with respect to B by $\mathcal{N}_{max}(H, B)$.

Our aim is to extend the results obtained by Rowley and Saninta for the symmetric groups to any prime p .

However, the general case looks, already from the first approach, more complicated. In fact, for $p \neq 2$, a Sylow p -subgroup of the symmetric group is not selfnormalized and so much more work needs to be done in understanding the structure of the normalizer. Moreover, since $p - 1 \neq 1$, the prime divisors of $p - 1$ play a certain role in the investigation of the overgroups of the normalizer. For instance, in the case of $\text{Sym}(p^2)$, 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.

Throughout all groups considered, and in particular all our sets, will be finite. Let Ω be a set of cardinality $n > 1$. Set $G = \text{Sym}(\Omega)$, the symmetric group on the finite set Ω . We also use $\text{Sym}(m)$ to denote the symmetric group of degree m . Now let T be a Sylow p -subgroup of G and B be the normalizer of T in G .

The work is organized as follows.

Chapter 2 contains basic definitions, notations, and results for the symmetric groups and general group theory, which will be used later. Basic facts of a Sylow p -subgroup of the symmetric group are proved and some fundamental results on the normalizer of a Sylow p subgroup are presented.

Chapter 3 starts the investigation of maximal p -local subgroups and plays a fundamental role for a further study on the topic. Some specific cases are analyzed (see Theorems 3.1.3, 3.2.1, 3.2.2, 3.3.2) and, in particular, the following Theorems, which demonstrates a further difference from the untypical case $p = 2$, is proved (see Theorems 3.1.1, 3.3.1).

Theorem A. *Let $G = \text{Sym}(\Omega)$ with $|\Omega| = p$, where p is a prime. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Then $\mathcal{N}_{\max}(G, B) = \{B\}$.*

Theorem B. *Let $G = \text{Sym}(\Omega)$ with $|\Omega| = p + 1$, where p is a prime. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Then $\mathcal{N}_{\max}(G, B) = \{B\}$.*

The study undertaken also leads to the classification of all normalizer of a Sylow p -subgroup of the symmetric group which are themselves maximal p -local subgroups (see Theorem 3.3.3).

Theorem C. *Let $G = \text{Sym}(\Omega)$, with $|\Omega| = n$. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$, where p is a prime. Then B is a maximal p -local subgroup with respect to B if one of the following occurs:*

- (i) $n = p$
- (ii) $n = kp$ with $1 < k < p$
- (iii) $n = p + k$ with $1 \leq k < p$.

Our next theorem concerns subgroups in $\mathcal{N}_{\max}(G, B)$ which do not act transitively on Ω .

Theorem D. *Let $G = \text{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Let $n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0$, where p is a prime, with $0 \leq k_j \leq 1$, for all $j = 0, \dots, t$, be the p -adic decomposition of n and $\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_t$, with $|\Omega_j| = k_j p^j$, for all $j = 0, \dots, t$, be the corresponding partition of Ω into B -orbits. Let J be a proper subset of $\{0, 1, \dots, t\}$. Set $\Delta = \bigcup_{i \in J} \Omega_i$, $U = \text{Sym}(\Delta)$ and $V = \text{Sym}(\Omega \setminus \Delta)$. Suppose that $N \in \mathcal{N}_{\max}(G, B)$ and $N \leq U \times V$. Then either $N = N_U \times V$, where $N_U \in \mathcal{N}_{\max}(U, B \cap U)$ and N_U is transitive on Δ , or $N = U \times N_V$, where $N_V \in \mathcal{N}_{\max}(V, B \cap V)$ and N_V is transitive on $\Omega \setminus \Delta$.*

We conclude this introduction with an example related to the main result achieved.

Example: $\text{Sym}(p+1)$

Let $G = \text{Sym}(\Omega)$, with $|\Omega| = p+1$ and p is a prime. Suppose that T is a Sylow p -subgroup of G and B is the normalizer of T in G . Then $T \cong Z_p$ is also a Sylow p -subgroup of $\text{Sym}(p)$ and B is equal to the normalizer in $\text{Sym}(p)$ of T . Hence, $B \cong \text{Hol}(T)$, the holomorph of T , (see Proposition 2.5.1 of [8] and Theorem 2.7.14) is a maximal subgroup of $\text{Sym}(p)$. Therefore B is a maximal p -local subgroup of G with respect to B .

Chapter 2

Preliminary Results

In this chapter, we give a brief description of some concepts and results of group theory we shall use later. We start with Sylow's Theorems ([1], [13]), which are the premise for everything which follows. Recall that all groups considered are finite.

2.1 Sylow's Theorems

Lemma 2.1.1 *If a group H of order p^m (p prime) acts on a finite set F and if $F_0 = \{x \in F \mid hx = x \text{ for all } h \in H\}$, then $|F| \equiv |F_0| \pmod{p}$.*

Proof. See Hungerford [14] (Lemma 5.1).

Theorem 2.1.2 (Cauchy) *If H is a finite group whose order is divisible by a prime p , then H contains an element of order p .*

Proof. See Hungerford [14] (Theorem 5.2).

A group H is a p -group if every element in H has order a power of the prime p . A subgroup of a group H is a p -subgroup of H if the subgroup is itself a p -group. In particular $\langle e \rangle$ is a p -subgroup of H for every prime p since $|\langle e \rangle| = 1 = p^0$, where e is the identity of H .

Corollary 2.1.3 *A finite group H is a p -group if and only if $|H|$ is a power of p .*

Proof. See Hungerford [14] (Corollary 5.3).

Corollary 2.1.4 *The center $Z(H)$ of a nontrivial finite p -group H contains more than one element.*

Proof. See Hungerford [14] (Corollary 5.4).

Lemma 2.1.5 *If P is a p -subgroup of a finite group H , then $|N_H(P) : P| \equiv |H : P| \pmod{p}$.*

Proof. See Hungerford [14] (Lemma 5.5).

Corollary 2.1.6 (Hungerford [14]) *If P is p -subgroup of a finite group H such that p divides $|H : P|$, then $N_H(P) \neq P$.*

Proof. $0 \equiv |H : P| \equiv |N_H(P) : P| \pmod{p}$. Since $|N_H(P) : P| \geq 1$ in any case, we must have $|N_H(P) : P| > 1$. Therefore $N_H(P) \neq P$.

Definition 2.1.7 *Let p be a prime and H be a finite group. If $|H| = p^\alpha m$, with $(p, m) = 1$, then a Sylow p -subgroup P of H is a subgroup of H of order p^α .*

The set of all Sylow p -subgroups of a group H will be denote by

$$\text{Syl}_p(H)$$

Theorem 2.1.8 (First Sylow Theorem) *Let H be a group of order $p^n m$, with $n \geq 1$, p prime, and $(p, m) = 1$. Then H contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of H of order p^i ($i < n$) is normal in some subgroup of order p^{i+1} .*

Proof. See Hungerford [14] (Theorem 5.7).

Corollary 2.1.9 *Let H be a group of order $p^n m$ with p prime, $n \geq 1$ and $(p, m) = 1$. Let P be a p -subgroup of H .*

(i) *P is a Sylow p -subgroup of H if and only if $|P| = p^n$.*

- (ii) Every conjugate of a Sylow p -subgroup is a Sylow p -subgroup.
- (iii) If there is only one Sylow p -subgroup S , then S is normal in H .

Proof. See Hungerford [14] (Corollary 5.8).

Theorem 2.1.10 (Second Sylow Theorem) *If K is a p -subgroup of a finite group H , and P is any Sylow p -subgroup of H , then there exists $h \in H$ such that $K \leq hPh^{-1}$. In particular, any two Sylow p -subgroups of H are conjugate.*

Proof. See Hungerford [14] (Theorem 5.9).

Theorem 2.1.11 (Third Sylow Theorem) *If H is a finite group and p a prime, then the number of Sylow p -subgroups of H divides $|H|$ and is of the form $kp + 1$ for some $k \geq 0$.*

Proof. See Hungerford [14] (Theorem 5.10).

Proposition 2.1.12 (Humphreys [13], Proposition 11.14) *Suppose that H is a finite group. Let S be a Sylow p -subgroup of H and let N be a normal subgroup of H . Then $S \cap N$ is a Sylow p -subgroup of N .*

Proof. First notice that one way to show that a subgroup K of a group H is a Sylow p -subgroup of H is to check that K is a p -subgroup and also that the index of K in H is not divisible by p . Since N is a normal subgroup of H , so that $\langle S, N \rangle = SN$. Since $S \cap N$ is a subgroup of S , its order is a power of p . By the opening remark, it only remains to show that $|N : S \cap N|$ is not divisible by p . We see that $|N : S \cap N| = |SN : S|$. However,

$$|H : S| = |H : SN| |SN : S|,$$

so that $|SN : S|$ divides $|H : S|$. It follows that $|SN : S|$ is not divisible by p , so that $S \cap N$ is a subgroup of N of index not divisible by p . Hence, $S \cap N$ is a Sylow p -subgroup of N .

Lemma 2.1.13 (The Frattini argument) (*Aschbacher [1]*) Suppose N is a normal subgroup of a finite group H and p is a prime. If S is a Sylow p -subgroup of N , then $H = N_H(S)N = NN_H(S)$.

Proof. Let $h \in H$. Since S^h is a Sylow p -subgroup of N , $S^h = S^n$ for some $n \in N$. Now $hn^{-1} \in N_H(S)$. Thus $h \in N_H(S)N = NN_H(S)$.

Proposition 2.1.14 (*Covello [8], Proposition 1.1.6*) Let S be a Sylow p -subgroup of a group H . If $N_H(S) \leq K \leq H$, then $K = N_H(K)$. In particular, if $K \trianglelefteq H$, then $K = G$.

Proof. Set $N = N_H(K)$. Then, by the Frattini argument, we have that $N = KN_N(S) \leq KN_H(S) = K$, since $N_H(S) \leq K$. Hence $N = K$, as $K \trianglelefteq N_H(K)$.

Proposition 2.1.15 (*Covello [8], Proposition 1.1.7*) Let H be a group and $S \in \text{Syl}_p(H)$. Let L and K be subgroups of H both containing $N_H(S)$. If $L^h = K$, for some $h \in H$, then $L = K$.

Proof. Since $S \leq L$, we have that $S^h \leq L^h = K$. Then S and S^h are both Sylow p -subgroups of K and so there exists $k \in K$ such that $S^{hk} = S$. Hence $hk \in N_H(S) \leq K$ and so $h \in K$. Thus $L = L^{hh^{-1}} = K^{h^{-1}} = K$.

Proposition 2.1.16 (*Covello [8], Proposition 1.1.10*) Let H be a group and suppose that $H = A \times B$. Let $S \in \text{Syl}_p(H)$. Then $S = (S \cap A) \times (S \cap B)$ and

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

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

Proof. Since A and B are normal subgroups of H , we have that $S \cap A \in \text{Syl}_p(A)$ and $S \cap B \in \text{Syl}_p(B)$ 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 $S_A \in \text{Syl}_p(A)$ and $S_B \in \text{Syl}_p(B)$, then $S_A \times S_B \in \text{Syl}_p(H)$. Thus,

$$|H : N_H(S)| = |A : N_A(S \cap A)| |B : N_B(S \cap B)|$$

and so $|N_H(S)| = |N_A(S \cap A)| |N_B(S \cap B)|$.

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

Lemma 2.1.17 (*Lempken, Parker and Rowley [18], Lemma 2.5*) Suppose that $H = X \times Y$ is a direct product of groups X and Y and suppose that $S \in \text{Syl}_p(H)$ where p is a prime which divides the order of both X and Y . Assume that L is a subgroup of H which contains $B := N_H(S)$. Then $L = (L \cap X) \times (L \cap Y)$, with $L \cap X = (B \cap X)^L$ and $L \cap Y = (B \cap Y)^L$.

Proof. Set $B_X = B \cap X$ and $B_Y = B \cap Y$. By Proposition 2.1.16, $B = B_X \times B_Y$ and, since $B \leq L$, we have that $B = N_L(S)$. Thus $B_X^L \times B_Y^L$ is a normal subgroup of L containing $N_L(S)$ and from Proposition 2.1.14 it follows that $L = B_X^L \times B_Y^L$. Furthermore $B_X = N_X(S \cap X) = N_{L \cap X}(S \cap X)$ and so B_X^L is a normal subgroup of $L \cap X$ containing $N_{L \cap X}(S \cap X)$. Therefore, by Proposition 2.1.14, we have that $B_X^L = L \cap X$. Similarly, $B_Y^L = L \cap Y$ and so $L = (L \cap X) \times (L \cap Y)$.

Applying induction, Proposition 2.1.16 and Lemma 2.1.17, gives

Corollary 2.1.18 Suppose that $H = \prod_{k \in \mathcal{K}} X_k$ where each $X_k, k \in \mathcal{K}$, has order divisible by the prime p . If L is a subgroup of H which contains $B := N_H(S)$, where $S \in \text{Syl}_p(H)$, then the following hold:

- (i) $S = \prod_{k \in \mathcal{K}} (S \cap X_k)$;
- (ii) $B = \prod_{k \in \mathcal{K}} (B \cap X_k)$;
- (iii) $L = \prod_{k \in \mathcal{K}} (B \cap X_k)^L$ and $L = \prod_{k \in \mathcal{K}} (L \cap X_k)$.

Proposition 2.1.19 (*Covello [8], Proposition 1.1.13*) Let H be a group, $K \trianglelefteq H$ and $S \in \text{Syl}_p(H)$. Then $N_H(SK) = N_H(S)K$.

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

2.2 The subgroup $O_p(H)$

Definition 2.2.1 Let H be a group and p be a prime. Define the subgroup $O_p(H)$ to be the largest normal subgroup of H whose order is a power of p .

Notice that the subgroup $O_p(H)$ is well define. For, if H is a finite group and $A, B \trianglelefteq H$, with $|A|$ and $|B|$ powers of p , then $\langle A, B \rangle = AB \trianglelefteq H$ and $|AB|$ is a power of p , since $|AB| = |A||B|/|A \cap B|$.

Clearly, $O_p(H)$ is a characteristic subgroup of H . Furthermore $O_p(H)$ can be characterized in terms of the Sylow p -subgroups of H .

Proposition 2.2.2 (Covello [8], Proposition 1.2.2) Let H be a group and p be a prime. Then $O_p(H)$ is equal to the intersection of all the Sylow p -subgroups of H .

Proof. Let X denote the intersection of all Sylow p -subgroups of H . Then X is a p -group and $X \trianglelefteq H$, since Sylow p -subgroup are all conjugate. Hence $X \leq O_p(H)$.

Conversely, by definition, $O_p(H)$ is a p -group and so there exists $S \in \text{Syl}_p(H)$ such that $O_p(H) \leq S$. But $O_p(H)$ is also normal in H . Therefore $O_p(H) \leq S^h$, for all $h \in H$. Since Sylow p -subgroups are all conjugate, so $O_p(H) \leq X$.

2.3 Semidirect products

Definition 2.3.1 Suppose that H is a group and let K , L and N be subgroups of H . Then the following is satisfied :

1. $L \trianglelefteq N$.
2. $L \leq N$ such that $N = LK$.
3. $L \cap K = 1$.

Then N is said to be the internal semidirect product of K by L and denoted by either $K \rtimes L$ or $L \ltimes K$.

Proposition 2.3.2 *Let H be a group and let K , L and N be subgroups of H . Suppose that K normalizes N and let $U = L \rtimes N$ and $M = L \rtimes K$. Then M normalizes U . In particular, if $N \leq K$, then $U \leq M$.*

Proof. By hypothesis, $K \leq N_H(N)$ and $K \leq N_M(L)$. Thus

$$K \leq N_H(N) \cap N_H(L) \leq N_H(LN) = N_H(U)$$

Moreover $L \leq N_H(U)$. So $KL = M \leq N_H(U)$.

Lemma 2.3.3 *Let K be a finite group and H be a finite 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 $M \leq L$. Firstly, since any two complements are isomorphic, we have that $L \cong H$ and so $|L| = |H|$. Moreover

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

Now $M \leq L \cap H \leq H$. 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 gives the result.

2.4 Finite permutation groups

This section contains basic notation and results about the permutation group structure. We introduce finite permutation groups and their basic properties, for which the main reference will be ([1], [4], [9], [13], [28]). Some related concepts are also illustrated, like the wreath product, 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.

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

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

the *symmetric group* on Ω and by

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

the *alternating group* on Ω . Recall that, for $n \geq 5$, every element of $\text{Alt}(n)$ is a commutator of elements in $\text{Sym}(n)$ and so, in particular, $\text{Alt}(n)$ is equal to the commutator subgroup of $\text{Sym}(n)$.

Theorem 2.4.1 *$\text{Alt}(n)$ is a normal subgroup of $\text{Sym}(n)$ of index 2, for all $n \geq 2$.*

Proof. Consider the map $\phi : \text{Sym}(n) \rightarrow \mathbb{Z}_2$ defined by

$$\phi(\pi) = \begin{cases} 1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$$

Then ϕ is a surjective homomorphism of $\text{Sym}(n)$ onto $\mathbb{Z}_2$ and $\ker \phi = \text{Alt}(n)$. So $\text{Alt}(n) \trianglelefteq \text{Sym}(n)$ and $\text{Sym}(n)/\text{Alt}(n) \cong \mathbb{Z}_2$.

Theorem 2.4.2 *The group $\text{Alt}(n)$ is simple for $n \geq 5$.*

Proof. See Humphreys [13] (Theorem 16.16).

Jordan [16] prove that $\text{Alt}(n)$ is generated by 3-cycles and also that $\text{Alt}(n)$ is the only non-trivial normal subgroup of $\text{Sym}(n)$ for $n \geq 5$.

Lemma 2.4.3 *Suppose that $n \geq 5$. Then $O_p(\text{Alt}(n)) = 1$.*

Proof. Assume that $O_p(\text{Alt}(n)) \neq 1$. This implies that $O_p(\text{Alt}(n))$ is a proper non-trivial normal subgroup of $\text{Alt}(n)$, so $\text{Alt}(n)$ is not simple, a contradiction. Hence, $O_p(\text{Alt}(n)) = 1$.

The subgroups of $\text{Sym}(\Omega)$ 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 $K \subseteq \text{Sym}(\Omega)$, we denote by Δ^K the set

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

Definition 2.4.4 Let H be a permutation group on Ω . A subset $\Delta \subseteq \Omega$ is a *fixed block* of H or is *fixed* by H if

$$\Delta^H = \Delta,$$

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

$$H^\Delta = \{h^\Delta \mid h \in H\}$$

is a permutation group on Δ , called the *constituent* of H on Δ . Clearly, the intersection and the union of two fixed blocks of H are again fixed by H and, for every set $\Delta \subseteq \Omega$, Δ^H is the smallest fixed block of H containing Δ . Also every permutation group H has the trivial fixed blocks $\emptyset$ and Ω .

Definition 2.4.5 A permutation group H on Ω is called *transitive* if its only fixed blocks are $\emptyset$ and Ω . Otherwise H is called *intransitive*.

Definition 2.4.6 Let $H \leq \text{Sym}(\Omega)$ and let $\emptyset \neq \Delta \subseteq \Omega$. Then Δ is called an *orbit* of H on Ω if Δ is a minimal fixed block of H . The order of Δ is called the *length* of the orbit.

The orbit of H containing the point $\alpha \in \Omega$ can be denote by either α^H or $\text{Orb}_H(\alpha)$ and is equal to $\{\alpha^h \mid h \in H\}$.

Proposition 2.4.7 If Δ is an orbit of H and $k \in \text{Sym}(\Omega)$, then Δ^k is an orbit of $k^{-1}Hk$.

Proof. See Covello [8] (Proposition 2.1.4).

Definition 2.4.8 Let $H \leq \text{Sym}(\Omega)$ and $\Delta \subseteq \Omega$. The set

$$S_\Delta = \{h \in H \mid \delta^h = \delta, \text{ for all } \delta \in \Delta\}$$

of all permutations of H which fix each point of Δ forms a subgroup of H , called the pointwise stabilizer of Δ in H . If $\Delta = \{\alpha\}$, then $H_\Delta = H_\alpha$ is called the point stabilizer of α in H and is denoted by $\text{Stab}_H(\alpha)$.

Proposition 2.4.9 Let H be a permutation group on Ω . If $K \leq H$ is transitive on Ω , then $H = H_\alpha K$, for all $\alpha \in \Omega$.

Proof. Let $\alpha \in \Omega$ and $h \in H$. Then, as K is transitive on Ω , there is $k \in K$ such that $\alpha^h = \alpha^k$. Hence $hk^{-1} \in H_\alpha$, that is, $h \in H_\alpha K$, which gives the result.

Theorem 2.4.10 (Orbit-Stabilizer Theorem) Let H be a permutation group on Ω and $\alpha \in \Omega$. Then the following holds:

$$|H| = |H_\alpha| |\alpha^H|.$$

Proof. We determine the length of the orbit α^H . Consider $\alpha^h, \alpha^k \in \alpha^H$. Then

$$\alpha^h = \alpha^k \Leftrightarrow hk^{-1} \in H_\alpha \Leftrightarrow H_\alpha h = H_\alpha k.$$

Hence the number of distinct points of α^H is equal to the number of distinct right cosets of H_α , which is $|H : H_\alpha|$. So

$$|\alpha^H| = |H : H_\alpha| = |H|/|H_\alpha|.$$

Definition 2.4.11 Let H and K be permutation groups on set A and B , respectively. We define the wreath product of H by K , written

$$H \wr K$$

in the following way:

$H \wr K$ is the group of all permutations θ on $A \times B$ of the following kind:

$$(a, b)\theta = (a\gamma_b, b\eta), \text{ for } a \in A \text{ and } b \in B,$$

where for each $b \in B$, γ_b is a permutation of H on A , but for different b 's the choices of the permutations γ_b are independent. The permutation η is a permutation of K on B .

Proposition 2.4.12 *Let H, K and L be permutation groups on the sets Γ, Ω and Δ , respectively. Then, identifying the sets $(\Gamma \times \Omega) \times \Delta$ and $\Gamma \times (\Omega \times \Delta)$ by the mapping*

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

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

Proof. See Covello [8] (Theorem 2.6.7).

Theorem 2.4.13 (Humphreys [13], Proposition 9.20) *Let $\alpha, \theta \in \text{Sym}(n)$. The conjugate $\theta\alpha\theta^{-1}$ has the same cycle type as α and is obtained from α by applying θ to each of the numbers appearing in each cycle of α .*

Proof. Consider first the case where $\alpha = (a_1 a_2 \dots a_k)$ is a cycle of length k . Let $b_1 = \theta(a_1), b_2 = \theta(a_2), \dots, b_k = \theta(a_k)$ and let β be the cycle $(b_1 b_2 \dots b_k)$. We want to show that $\theta\alpha\theta^{-1} = \beta$. To show that two permutations in $\text{Sym}(n)$ are equal we need to show that they have the same effect on each number x in $\{1, 2, \dots, n\}$. If x appears in β then we can rewrite the cycles, without changing their cyclic order, so that $x = b_1$. Then

$$\theta\alpha\theta^{-1}(b_1) = \theta\alpha(a_1) = \theta(a_2) = b_2 = \beta(b_1).$$

Thus, $\theta\alpha\theta^{-1}(x) = \beta(x)$ for all x appearing in β . On the other hand, if x does not appear in β then $\beta(x) = x$ and, because $\theta^{-1}(x)$ does not appear in α , $\alpha\theta^{-1}(x) = \theta^{-1}(x)$. Hence

$$\theta\alpha\theta^{-1}(x) = \theta\theta^{-1}(x) = x = \beta(x).$$

We have now shown that $\beta(x) = \theta\alpha\theta^{-1}(x)$ for all x and so $\beta = \theta\alpha\theta^{-1}$. This establishes the formula

$$\theta(a_1 a_2 \dots a_k)\theta^{-1} = (\theta(a_1)\theta(a_2) \dots \theta(a_k)).$$

Now consider the general case where α has cycle decomposition $\alpha_1 \alpha_2 \dots \alpha_s$. For each i , let β_i be the cycle obtained by applying θ to each number appearing in α_i . By the above formula, each $\theta\alpha_i\theta^{-1} = \beta_i$. Hence

$$\theta\alpha\theta^{-1} = \theta(\alpha_1 \alpha_2 \dots \alpha_s)\theta^{-1} = \theta\alpha_1\theta^{-1}\theta\alpha_2\theta^{-1}\theta \dots \theta^{-1}\theta\alpha_s\theta^{-1} = \beta_1 \beta_2 \dots \beta_s$$

has the same cycle type as α .

Given any two permutations α and β in $\text{Sym}(n)$ of the same cycle type, there is a permutation $\theta \in \text{Sym}(n)$ such that β can be obtained from α by applying θ to each number appearing in α . By Theorem 2.4.13, $\beta = \theta\alpha\theta^{-1}$. Thus, any two permutations in $\text{Sym}(n)$ of the same cycle type are conjugates in $\text{Sym}(n)$. Combining this with Theorem 2.4.13, we see that each conjugacy class in $\text{Sym}(n)$ consists of all permutations with a given cycle type.

Lemma 2.4.14 *If H is transitive on X then X has cardinality $|H : H_x|$ for each $x \in X$.*

Proof. See Aschbacher [1] (Theorem 5.11).

Lemma 2.4.15 *If H is a p -group then all orbits of H on X have order a power of p .*

Proof. This follows from Lemma 2.4.14 and the fact that the index of any subgroup of G divides the order of H .

Proposition 2.4.16 (Wielandt [28]) *Let $H \leq \text{Sym}(\Omega)$, with $|\Omega| = n$. If H is transitive, then $\deg H = n = |\Omega|$.*

Proof. For all $\alpha \in \Omega$, $H_\alpha \neq G$, that is, for all $\alpha \in \Omega$, there exists $h \in H$ such that $\alpha^h \neq \alpha$.

Proposition 2.4.17 *Let $H \leq \text{Sym}(\Omega)$ and let Δ be the set of points fixed by H . Then the centralizer C of H in $\text{Sym}(\Omega)$ contains the symmetric group $\text{Sym}(\Delta)$ and so is transitive on Δ . In particular, this holds for the normalizer of H in $\text{Sym}(\Omega)$.*

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

Lemma 2.4.18 *Suppose that R is a transitive permutation group of degree n . Let $H = L \wr R$ and $P = K \wr R$, 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 P .*

Proof. Let $H = L \wr R$ and $P = K \wr R$, 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 P , respectively. Then $H = \bar{L} \rtimes R$ and $P = \bar{K} \rtimes R$ and, in particular, H can be regarded as a subgroup of P . Also notice that, by Corollary 2.1.18, $\bar{L}$ contains the normalizer of a Sylow p -subgroup of $\bar{K}$. Now let M be a subgroup of P properly containing H . By Dedekind's Modular Law, we have that

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

with $\bar{L} \leq M \cap \bar{K} \leq \bar{K}$. 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 2.1.18,

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

with $M_i = M \cap K_i$ and $L_i \leq M_i \leq K_i$, for all $i = 1, \dots, n$. Since $M \neq H$, from the factorization of M it follows that $M \cap \bar{K} \neq \bar{L}$ and so there exists $j \in \{1, \dots, n\}$ 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 $\{M_1, \dots, M_n\}$, this implies that $M_i = K_i$, for all $i = 1, \dots, n$. Hence $M \cap \bar{K} = \bar{K}$ and $M = \bar{K} \rtimes R = P$.

2.5 Imprimitive and primitive groups

Definition 2.5.1 *Let H be a permutation group on a set Ω and $\Gamma \subseteq \Omega$. We say that Γ is a block of H if for all $h \in H$, Γ^h either is equal to Γ or has no point in common with Γ , that is*

$$\Gamma^h \cap \Gamma \in \{\Gamma, \emptyset\}.$$

The length of the block Γ is $|\Gamma|$.

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

Proposition 2.5.2 *The intersection of two blocks of a permutation group H is also a block of H .*

Proof. See Covello [8] (Proposition 3.1.2).

Proposition 2.5.3 *Let K be a subgroup of a permutation group H and $h \in H$. If Γ is a block of K , then Γ^h is a block of $h^{-1}Kh$.*

Proof. Let $k \in K$ and suppose that $(\Gamma^h)^{h^{-1}Kh} \cap \Gamma^h \neq \emptyset$. Applying h^{-1} , it follows that

$$\Gamma^k \cap \Gamma \neq \emptyset,$$

which implies $\Gamma^k = \Gamma$ and, applying h , we get that

$$\Gamma^{hh^{-1}kh} = \Gamma^{kh} = \Gamma^h.$$

Proposition 2.5.4 *If Γ is a block of a permutation group H , then, for all $h \in H$, Γ^h is a block of H .*

Proof. See Covello [8] (Proposition 3.1.3).

The block Γ and Γ^h are called *conjugate*. By definition, conjugate blocks are either equal or disjoint. Let Γ be a block of H , where H is a permutation group on Ω . Then the set of all blocks conjugate to Γ is called a *complete block system* of H . All blocks of a complete block system have the same length. Also, if H is transitive on Ω , then Ω is the union of all blocks of a complete block system of H .

Proposition 2.5.5 (Wielandt [28]) *Let H be a permutation group on Ω . The length of a block of a transitive group H divides the degree of H .*

Proof. Let Γ be a block of H , with $H \leq \text{Sym}(\Omega)$. Since H 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 $|\Omega|$.

Proposition 2.5.6 (Wielandt [28]) *A transitive permutation group H of prime degree is primitive.*

Proof. Since the length of a block of a transitive permutation group divides its degree, so that H has only trivial blocks.

Definition 2.5.7 *A transitive permutation group H is imprimitive if H has at least one nontrivial block Γ , such a block is called a set of imprimitivity; otherwise it is called primitive.*

Corollary 2.5.8 *Every nontrivial normal subgroup of a primitive group is transitive.*

Proof. See Covello [8] (Corollary 3.2.3).

Theorem 2.5.9 *Let $\alpha \in \Omega$ and H be a transitive group on Ω . Then H is imprimitive if and only if there is a group K which lies properly between H_α and H .*

Proof. See Covello [8] (Theorem 3.2.4).

From Theorem 2.5.9 we get the following result:

Theorem 2.5.10 *Let $\alpha \in \Omega$, $|\Omega| > 1$. A transitive group H on Ω is primitive if and only if H_α is a maximal subgroup of H .*

Proof. See Covello [8] (Theorem 3.2.6).

The last two theorems give a way of recognizing symmetric and alternating groups.

Theorem 2.5.11 *A primitive group which contains a transposition is a symmetric group.*

Proof. See Covello [8] (Theorem 3.2.9).

Theorem 2.5.12 *Let p be a prime and H a primitive group of degree $n = p + k$, with $k \geq 3$. If H contains an element of degree and order p , then H is either $\text{Alt}(n)$ or $\text{Sym}(n)$.*

Proof. See Covello [8] (Theorem 3.2.10).

Lemma 2.5.13 *Let H be transitive on X and $y \in X$.*

- (i) *If Q is a system of imprimitivity for H on X and $y \in Y \in Q$, then H is transitive on Q , the stabilizer K of Y in H is a proper subgroup of H properly containing H_y , Y is an orbit of K on X , $|X| = |Y||Q|$, $|Q| = |H : K|$, and $|Y| = |K : H_y|$.*
- (ii) *If $H_y < K < H$ then $Q = \{Yg : g \in H\}$ is a system of imprimitivity for H on X , where $Y = yK$ and K is the stabilizer of Y in H .*

Proof. See Aschbacher [1] (Theorem 5.18).

We recall that a primitive permutation group is a transitive permutation group which only preserves trivial systems of blocks.

Lemma 2.5.14 (Jordan, Marggraf) *Suppose that Σ is a finite set and L is a primitive subgroup of $\text{Sym}(\Sigma)$.*

- (i) *If L contains a transposition, then $L = \text{Sym}(\Sigma)$.*
- (ii) *Suppose L contains a fours group which is transitive on 4 points and fixes all the other points of Σ . If $|\Sigma| > 9$, then $L \geq \text{Alt}(\Sigma)$.*

Proof. See Wielandt [28] (Theorems 13.3 and 13.5).

Theorem 2.5.15 *Let $L \cong K \wr H$, with $K \leq \text{Sym}(k)$, $H \leq \text{Sym}(m)$. If K is transitive and H is primitive on the respective sets, then every nontrivial block of L corresponds to a block of K . In particular, the length of every nontrivial block of L divides k .*

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

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

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

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

For $l \in L_\alpha$, $\alpha^l = \alpha$ and so, since Γ is a block of L , we get that $\Gamma^l = \Gamma$ and Γ is preserved by L_α . Moreover, for $i \neq 1$, L_α is transitive on Ω_i , since $K_i \leq L_\alpha$ 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 L_α is transitive on Ω_2 and Γ is preserved by L_α , it follows that $\Gamma \supseteq \Omega_2$. The same argument applied with L_β in place of L_α implies that $\Gamma \supseteq \Omega_1 \cup \Omega_2$ 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 .

Proposition 2.5.16 *Let Ω be a set and $H = \text{Sym}(\Omega)$. Let $\mathcal{B} = \{\Omega_1, \dots, \Omega_m\}$ be a partition of Ω into m subsets of the same cardinality. Then the stabilizer L of $\mathcal{B}$ in H is isomorphic to*

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

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

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

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

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

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

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

Corollary 2.5.17 *Let Ω be a set and $H = \text{Sym}(\Omega)$. Let $K \leq H$ be imprimitive and Γ be a block of K . Then the stabilizer in H of the complete block system $\mathcal{B}_\Gamma = \{\Gamma^k \mid k \in K\}$ is isomorphic to $\text{Sym}(\Gamma) \wr \text{Sym}(\mathcal{B}_\Gamma)$. In particular, K is isomorphic to a subgroup of $\text{Sym}(\Gamma) \wr \text{Sym}(\mathcal{B}_\Gamma)$.*

Proof. See Covello [8] (Corollary 3.5.2).

2.6 Sylow p -subgroups of the symmetric group

This section are concerned with the structure of a Sylow p -subgroup of the symmetric group. The order and the structure of Sylow p -subgroup 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 [9] and Huppert [15], who both refer to the same paper by Kaloujnine [17] from 1948. Further references are a paper by Findlay [11] from 1904 and a paper by Weir [26] from 1955. Particular emphasis is given to the case when the degree of the symmetric group is a power of p .

Lemma 2.6.1 (*Findlay [11]*) *Suppose that p is a prime and n is an integer. Then the order of a Sylow p -subgroup of $\text{Sym}(p^n)$ is*

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

Proof. Let $S \in \text{Syl}_p(\text{Sym}(p^n))$. 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 exists 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

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

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

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

Lemma 2.6.2 *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 $\text{Sym}(kp^n)$ is*

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

Proof. The result follows by using the same approach as in the proof of Lemma 2.6.1.

Lemma 2.6.3 *Suppose that p is a prime and k_j 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 $j = 0, \dots, t$, be the p -adic decomposition of n . Then a Sylow p -subgroup S of $\text{Sym}(n)$ 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. See Covello [8] (Lemma 4.1.4).

Proposition 2.6.4 (Humphreys [13], Proposition 19.10) *Let p be a prime integer, and let k be any positive integer. The Sylow p -subgroup of the symmetric group $\text{Sym}(p^k)$ is the iterated wreath product (with k copies of a cyclic group of order p acting on p points C_p)*

$$(\cdots((C_p \wr C_p) \wr C_p \cdots \wr C_p).$$

Proof. The proof is by induction on k . Note that when $k = 1$, the highest power of p dividing $p!$ is p , so that the Sylow p -subgroup is indeed cyclic of order p . We therefore suppose that the result holds for the symmetric group of degree p^k . By Lemma 2.6.1, the highest power of p dividing $(p^n)!$ is $p^{r(n)}$ where

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

The order of a regular wreath product of k copies of the cyclic group C_p is equal to $p^{r(k)}$. It follows that the regular wreath product of $k+1$ copies of C_p has the same order (namely $(p^{r(k)})^p \times p$) as the order of the Sylow p -subgroup of $\text{Sym}(p^{k+1})$, since

$$pr(k) + 1 = p(p^{k-1} + p^{k-2} + \cdots + p + 1) + 1 = r(k+1).$$

It only remains to show that this wreath product occurs as a subgroup of $\text{Sym}(p^{k+1})$. In $\text{Sym}(p^{k+1})$, let N denote the direct product of p copies of $\text{Sym}(p^k)$, where we regard that first copy of $\text{Sym}(p^k)$ as the symmetric group on $\{1, \dots, p^k\}$, the second copy as the symmetric group on the numbers $\{1 + p^k, \dots, 2p^k\}$, and so on. These copies of $\text{Sym}(p^k)$ commute because they act on disjoint sets. Let h be the element of $\text{Sym}(p^{k+1})$ consisting of p^k cycles each of length p , these cycles all being of the form

$$(i, i + p^k, i + 2p^k, \dots, i + (p-1)p^k),$$

for $1 \leq i \leq p^k$. By inductive hypothesis, the Sylow p -subgroup of $\text{Sym}(p^k)$ is an iterated wreath product of k copies of C_p . It is clear that the semidirect product of the Sylow p -subgroup of N by $H = \langle h \rangle$ (where h is the element of $\text{Sym}(p^{k+1})$, defined above), is isomorphic to the regular wreath product of $k+1$ copies of C_p , thus completing the proof.

Proposition 2.6.5 (*Findlay [11]*) *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = kp^t$, p prime and $1 \leq k < p$. Then a Sylow p -subgroup of H is given by the direct product of k factors, each isomorphic to a Sylow p -subgroup of $\text{Sym}(\Delta)$, with $|\Delta| = p^t$.*

Proof. Let $\Omega_1, \dots, \Omega_k$ be a partition of Ω into k subsets of order p^t . For $i = 1, \dots, k$ let S_i be a Sylow p -subgroup of $\text{Sym}(\Omega_i)$ and set $S = S_1 \times \dots \times S_k$. Then, from Lemma 2.6.1, it follows that

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

and so $S \in \text{Syl}_p(H)$.

Proposition 2.6.6 (*Humphreys [13], Corollary 19.11*) *Let p be a prime and n be any positive integer. Let*

$$n = a_0 + a_1p + a_2p^2 + \dots + a_kp^k \quad (\text{with } 0 \leq a_i \leq p-1) \quad (*)$$

be the expansion of n to the base p . The each Sylow p -subgroup of the symmetric group $\text{Sym}(n)$ is a direct product

$$(S_1)^{a_1} \times (S_2)^{a_2} \times \dots \times (S_k)^{a_k},$$

where S_i is a Sylow p -subgroup of the symmetric group $\text{Sym}(p^i)$, so that S_i is the regular wreath product of i copies of the cyclic group C_p .

Proof. We first calculate the power of p dividing $n!$. The number of integers between 1 and n divisible by p is $[n/p]$, where $[]$ denotes the integer part function. Of these integers a further $[n/p^2]$ are divisible by p^2 , and so on. It follows that the power of p dividing $n!$ is p^t , where

$$t = [n/p] + [n/p^2] + [n/p^3] + \dots$$

Using the expansion (*) of n to the base p , this power can also be written as

$$\begin{aligned} t &= (a_1 + a_2p + \cdots + a_kp^{k-1}) + (a_2 + \cdots + a_kp^{k-2}) + \cdots \\ &= a_1 + a_2(p+1) + a_3(p^2 + p + 1) + \cdots, \end{aligned}$$

so that p^t is the order of the group

$$(S_1)^{a_1} \times (S_2)^{a_2} \times \cdots \times (S_k)^{a_k}$$

by Proposition 2.6.4. It only remains to show that $\text{Sym}(n)$ has a subgroup isomorphic to the given direct product. This is done by dividing the set with n elements into disjoint subsets with a_0 of those of size 1, a_1 of size p , $\dots$, a_k of size p^k , and then applying Proposition 2.6.4 to each of those disjoint subsets.

Lemma 2.6.7 *Suppose p is a prime, n is a positive integer and $T_{p^n} \in \text{Syl}_p(\text{Sym}(p^n))$. Then $|Z(T_{p^n})| = p$.*

Proof. This time we start the induction with $n = 1$. We wish to show

$$P(n) : |Z(T_{p^n})| = p.$$

We know that, by Proposition 2.6.4,

$$T_{p^n} = \underbrace{(T_{p^{n-1}} \times T_{p^{n-1}} \times \cdots \times T_{p^{n-1}})}_p \wr C_p$$

where $T_{p^{n-1}} \in \text{Syl}_p(\text{Sym}(p^{n-1}))$. Let, $i = 1, 2, \dots, p$, $A_i = T_{p^{n-1}}$ and let $A = A_1 \times A_2 \times \cdots \times A_p$, $C_p = \langle x \rangle$.

If $n = 1$, then $T_p \cong C_p$, namely $|Z(T_p)| = |Z(C_p)| = |C_p| = p$. Thus $P(1)$ is true. Suppose $P(n-1)$ is true, i.e. $|Z(T_{p^{n-1}})| = p$. Now let $Z = Z(T_{p^n})$. Since $A_i \leq T_{p^n}$ so that $Z \leq C_H(T_{p^n}) \leq C_H(A_i)$ where $H = \text{Sym}(p^n)$, i.e. Z centralized all elements of A_i . Then $[Z, A_i] = 1$ for all $i = 1, 2, \dots, p$, and we get that $\bigcap_{i=1}^p N_{T_{p^n}}(A_i) \geq A$ (since $A_i \trianglelefteq A \leq T_{p^n}$). But $Z \leq C_{T_{p^n}}(A)$, so let $g \in C_{T_{p^n}}(A)$. Then $g = ax^j$, for some $a \in A$ and some j . Assume that $(a_1, 1, \dots, 1) \in A$ where $a_1 \in A_1$. So $(a_1, 1, \dots, 1)^g = (a_1, 1, \dots, 1)^{ax^j} = (a_1^a, 1, \dots, 1)^{x^j}$ with $a_1^a \in A_1$. If $x_j \neq 1$, then $(a_1^a, 1, \dots, 1)^{x^j} = (1, \dots, a_1^a, \dots, 1) \neq (a_1^a, 1, \dots, 1)$. Therefore, $x_j = 1$ implies that $g = a \in A$ and hence $Z \leq A$. It follows that $Z \leq Z(A) = Z(A_1) \times Z(A_2) \times \cdots \times Z(A_p)$, and then $|Z(A)| = p^p$, as $|Z(A_i)| = p$. By Proposition 5.19 of [13],

$Z(A) = \underbrace{C_p \times C_p \times \cdots \times C_p}_p$. Now let $(a_1, a_2, \dots, a_p) \in Z(A)$. We may assume that $(a_1, a_2, \dots, a_p)^x = (a_p, a_1, a_2, \dots, a_{p-1})$. Since $(a_1, a_2, \dots, a_p)^x = (a_1, a_2, \dots, a_p)$ so we get $a_1 = a_2 = \cdots = a_{p-1} = a_p$. Thus $C_{Z(A)}(x) = \{(a, a, \dots, a) \in Z(A) \mid a \in C_p\}$, we see that $C_{Z(A)}(x)$ has order p . But $C_{Z(A)}(x) = Z$, hence $|Z| = p$.

Proposition 2.6.8 *Let H be any finite group and B is the normalizer of a Sylow p -subgroup of H . Let $H = \langle X \mid B \leq X, O_p(X) \neq 1 \rangle$. Then $H = \langle X \mid B \leq X, O_p(X) \neq 1 \text{ such that } B \text{ lies in exactly one maximal subgroup of } X \rangle$.*

Proof. Suppose $B \leq X \leq H$, with $O_p(X) \neq 1$. If M and N are distinct maximal subgroups of X containing B , then clearly $O_p(M) \neq 1, O_p(N) \neq 1$ and $\langle M, N \rangle = X$. Thus if B lies in more than one maximal subgroup of X , then we replace $\{X\}$ by $\{M, N\}$ and by continuing this procedure as necessary we obtain a set of subgroups containing B and generating H such that B lies in exactly one maximal subgroup of each.

Theorem 2.6.9 *Let $H = \text{Sym}(\Omega)$, p be a prime and $n \in \mathbb{N}$.*

- (i) *If $|\Omega| = p^n$, then a Sylow p -subgroup of H is transitive on Ω .*
- (ii) *If $|\Omega| = kp^n$, $1 \leq k < p$, then a Sylow p -subgroup of H has k orbits on Ω , each of length p^n .*
- (iii) *Let $|\Omega| = n$, where*

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

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 H has k_j orbits on Ω , each of length p^j .

Proof. (i) Let Δ be a set of cardinality p and let C_p denote a cyclic group of order p acting on Δ . By Proposition 2.6.4, a Sylow p -subgroup S of H is isomorphic to the wreath product W of n copies of C_p . But, since C_p is transitive on Δ , 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 .

(ii) According to Proposition 2.6.5, $S = S_1 \times \cdots \times S_k$, where, for $i = 1, \dots, k$, S_i

is a Sylow p -subgroup of $\text{Sym}(\Omega_i)$ and $\Omega_1, \dots, \Omega_k$ is a partition of Ω into k subsets of order p^n . Then, by part (i), it follows that the orbits of S on Ω are precisely the sets $\Omega_1, \dots, \Omega_k$.

(iii) 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 $S = S_1 \times \dots \times S_t$, where, for $j = 1, \dots, t$, S_j is a Sylow p -subgroup of $\text{Sym}(\Omega_j)$ and, by part (ii), 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 $\Omega_0 = \text{Fix}_\Omega(S)$, S has other k_0 orbits, each of length 1, namely the sets $\{\omega\}$, for $\omega \in \Omega_0$.

Proposition 2.6.10 *Let $H = \text{Sym}(\Omega)$, p be a prime, $n \in \mathbb{N}$, and let $S \in \text{Syl}_p(H)$.*

- (i) *If $|\Omega| = p^n$, then every block of S has length a power of p . Moreover, S has a block of length p^r , for all $r = 1, \dots, n$.*
- (ii) *If $|\Omega| = kp^n$, $1 \leq k < p$, then S has blocks of length p^r , for all $r = 1, \dots, n$.*
- (iii) *Let $|\Omega| = n$, where*

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

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

Proof. (i) By Theorem 2.6.9 (i), S is transitive on Ω and so, by Proposition 2.5.5, the length of every block of S is a power of p . Moreover, by Proposition 2.6.4 and by the associativity of the wreath product, we have that S is isomorphic to a subgroup of $\text{Sym}(p^r) \wr \text{Sym}(p^{n-r})$, for all $r = 1, \dots, n$, where, by Proposition 2.5.16, $\text{Sym}(p^r) \wr \text{Sym}(p^{n-r})$ is the stabilizer of a block system whose blocks have length p^r . Therefore S has blocks of length p^r , for all $r = 1, \dots, n$.

(ii) By Proposition 2.6.5, $S = S_1 \times \dots \times S_k$ with $S_i \in \text{Syl}_p(\text{Sym}(\Omega_i))$ and $|\Omega_i| = p^n$, for all $i = 1, \dots, k$. Now by part (i), each S_i has blocks of length p^r , for all $r = 1, \dots, n$, but a block of S_i is also a block of S and so we get the result.

(iii) We know that $S = S_1 \times \dots \times S_t$ with $S_j \in \text{Syl}_p(\text{Sym}(\Omega_j))$ and $|\Omega_j| = k_j p^j$, for all $j = 1, \dots, t$. 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 part (ii), S_t has blocks of length p^r , for all $r = 1, \dots, t$. But a

block of S_j is also a block of S and so we get the result.

In the investigation of the structure of the normalizer of a Sylow p -subgroup of $\text{Sym}(p^n)$ certain elementary abelian normal subgroups of S play a central role. Let $S \in \text{Syl}_p(\text{Sym}(p^n))$. For all $t = 1, \dots, n$, define

$$K_t = \underbrace{S_t \times \cdots \times S_t}_{p^{n-t}} \cong S_t \wr T_{n-t},$$

with T_{n-t} trivial permutation group on p^{n-t} letters and

$$S_t \in \text{Syl}_p(\text{Sym}(p^t)).$$

By Propositions 2.4.12 and 2.6.4, for all $t = 1, \dots, n$, $S \cong S_t \wr S_{n-t}$. Thus K_t be considered as a subgroup of S , in which case

$$K_t \trianglelefteq S$$

Moreover, for all $t = 1, \dots, n-1$,

$$K_t \leq K_{t+1}.$$

So we have the following normal series of S :

$$K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_{n-1} \trianglelefteq K_n = S,$$

with K_1 abelian of order $p^{p^{n-1}}$ and K_t nonabelian, for all $t = 2, \dots, n$.

Theorem 2.6.11 *Let $H \neq \text{Sym}(p^n)$, where p is a prime and $n \in \mathbb{N}$, and $S \in \text{Syl}_p(H)$. Then every abelian normal subgroup A of S is in K_2 .*

Proof. See Covello [7] (Theorem 4.4.1).

Theorem 2.6.12 *Let $H = \text{Sym}(p^n)$, where p is a prime with $p > 2$ and $n \in \mathbb{N}$, and let $S \in \text{Syl}_p(H)$. Then every abelian normal subgroup A of S is in K_1 .*

Proof. See Covello [7] (Theorem 4.4.2).

Corollary 2.6.13 *Let $H = \text{Sym}(p^n)$, where p is a prime and $n \in \mathbb{N}$, and $S \in \text{Syl}_p(H)$. If $p > 2$, every abelian normal subgroup A of S is in K_t , for all $t = 1, \dots, n$; for $p = 2$ every abelian normal subgroup A of S is contained in K_t , for all $t = 2, \dots, n$.*

Proof. See Covello [7] (Corollary 4.4.3).

Theorem 2.6.14 *Let S be a Sylow p -subgroup of $\text{Sym}(p^n)$, where p is a prime and $n \in \mathbb{N}$. If $p > 2$, S has a unique abelian normal subgroup of order p^{n-1} , which is $K_1 = C_p \wr T_{n-1}$, and this is an elementary abelian p -group.*

Proof. See Covello [7] (Theorem 4.4.6).

Theorem 2.6.15 *Let S be a Sylow p -subgroup of $H = \text{Sym}(p^n)$, where p is a prime and $n \in \mathbb{N}$. Then the normalizer in H of S is contained in the normalizer in H of every abelian normal subgroup of S of order p^{n-1} .*

Proof. See Covello [7] (Theorem 4.4.11).

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

This section is devoted to understanding and describing the structure of the normalizer of a Sylow p -subgroup of the symmetric group.

Theorem 2.7.1 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n$, and let $S \in \text{Syl}_p(H)$. Let*

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

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

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

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

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

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

Proof. Let $\Omega_0, \Omega_1, \dots, \Omega_t$ be a partition of Ω into $t+1$ subsets such that, for $j = 0, \dots, t$, $|\Omega_j| = k_j p^j$ and write $S = S_1 \times \dots \times S_t$, with S_j Sylow p -subgroup of $\text{Sym}(\Omega_j)$. Also let $B_0 = \text{Sym}(\Omega_0)$ and let B_j denote the normalizer of S_j in $\text{Sym}(\Omega_j)$, for all $j > 0$. Then the sets Ω_j are fixed blocks of S all of different length and so, since $S \trianglelefteq B$, they are also fixed blocks of B . Therefore $B \leq \text{Sym}(\Omega_0) \times \dots \times \text{Sym}(\Omega_t)$ and $B = (B \cap \text{Sym}(\Omega_0)) \times \dots \times (B \cap \text{Sym}(\Omega_t)) = B_0 \times \dots \times B_t$. Furthermore, the sets $\Omega_0, \Omega_1, \dots, \Omega_t$ are the orbits of B on Ω .

Notice that, by Theorem 2.7.1, $\text{Sym}(\Omega_0)$ is contained in B and, in particular, in the centralizer of S in H , and so B is transitive on the set of points fixed by S .

Corollary 2.7.2 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = p^n$, and let $S \in \text{Syl}_p(H)$. Then*

$$|N_H(S)| = |S|(p-1)^n.$$

Proof. This follows from Theorem 2.7.1.

Theorem 2.7.3 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = p^n$. Let $S \in \text{Syl}_p(H)$ and set $B = N_H(S)$. Then B is transitive on Ω and every block of B has length a power of p . Furthermore, for $i = 1, \dots, n-1$, B has a unique complete block system of blocks of length p^i and, in particular, B has blocks of length p^r , for all $r = 1, \dots, n$.*

Proof. See Covello [8] (Theorem 5.2.9).

Theorem 2.7.4 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = kp^n$ and $1 \leq k < p$. Let $S \in \text{Syl}_p(H)$ and set $B = N_H(S)$. Then B is isomorphic to the wreath product of $\bar{B}$ by $\text{Sym}(k)$, where $\bar{B}$ is the normalizer in $\text{Sym}(p^n)$ of a Sylow p -subgroup of $\text{Sym}(p^n)$. In particular,*

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

and B is transitive on Ω .

Proof. See Covello [8] (Theorem 5.3.1).

Proposition 2.7.5 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = kp^n$ and $1 \leq k < p$. Let $S \in \text{Syl}_p(H)$ and set $B = N_H(S)$. 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. See Covello [8] (Proposition 5.3.2).

Theorem 2.7.6 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n$, $S \in \text{Syl}_p(H)$ and $B = N_H(S)$. Let*

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

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

Proof. According to Theorem 2.7.1, write $B = B_0 \times B_1 \times \dots \times B_t$, with B_j normalizer of a Sylow p -subgroup of $\text{Sym}(\Omega_j)$ and $\Omega_0, \Omega_1, \dots, \Omega_t$ orbits of B on Ω . Then, for all $s \in \{j \mid k_j \neq 0\}$, Ω_j is also a block of B and has length $k_s p^s$. Moreover, B_t has blocks of length p^r , for all $r = 1, \dots, t$. But a block of B_t is also a block of B and so we get the result.

Theorem 2.7.7 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n$, $S \in \text{Syl}_p(H)$ and $B = N_H(S)$. Let*

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

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

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

with $|\Omega_j| = k_j p^j$, for all $j = 0, \dots, t$, be the corresponding partition of Ω into B -orbits.

- (i) *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 $J \subseteq 0, \dots, t$ and $|J| \geq 1$.

- (ii) If $\alpha \in \Omega_i$, then, in its action on Ω , $\text{Stab}_B(\alpha)$ has t orbits, each of length $k_j p^j$, or $j \neq i$, 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. See Covello [8] (Theorems 5.4.3 and 5.4.4).

Lemma 2.7.8 *Let $H = \text{Sym}(\Omega)$ and let $S \in \text{Syl}_p(H)$. Then the normalizer of S in H is never contained in $\text{Alt}(\Omega)$.*

Proof. Let $K = \text{Alt}(\Omega)$ and set $B = N_H(S)$. If $p = 2$, then $S \not\leq \text{Alt}(\Omega)$ and the result is trivial. So assume that $p \neq 2$. Then $S \in \text{Syl}_p(K)$ and, by the Frattini argument, it follows that $H = BK$, which implies that $B \not\leq K$.

Theorem 2.7.9 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n$, and $S \in \text{Syl}_p(H)$. Suppose that M is a primitive subgroup of G containing the normalizer in H of S . If $n \geq p + 2$, then $M = G$.*

Proof. See Covello [8] (Theorem 5.5.2).

Lemma 2.7.10 *Let $n \in \mathbb{N}$ and p be a prime. Let $n = k_t p^t + \dots + k_1 p + k_0$ 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 $m = k_{t-1} p^{t-1} + \dots + k_1 p + k_0$. Since, for $j = 0, \dots, t-1$, $0 \leq k_j < p$, we have that

$$m \leq (p-1)(1 + p + \dots + p^{t-1}) = p^t - 1 < p^t \leq k_t p^t.$$

Hence $n = k_t p^t + m < 2k_t p^t$ and so a proper divisor of n must be smaller than $k_t p^t$.

We establishing some results on imprimitive subgroups of $\text{Sym}(\Omega)$ which contain the normalizer of a Sylow p -subgroup.

Theorem 2.7.11 *Let $H = \text{Sym}(\Omega)$ and $S \in \text{Syl}_p(H)$. Let M be a subgroup of H containing the normalizer of S in H 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 $B = N_H(S)$ and let $\Omega_0, \Omega_1, \dots, \Omega_t$, with $|\Omega_j| = k_j p^j$, for all $j = 0, \dots, t$, be the orbits of B on Ω . Also write $B = B_0 \times B_1 \times \cdots \times B_t$, where, for each $j = 0, \dots, t$, B_j is the normalizer of a Sylow p -subgroup of $\text{Sym}(\Omega_j)$.

Suppose that M is an imprimitive subgroup of H 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 2.7.10, $d < k_t p^t$. Also the complete block system determined by Δ forms a partition on 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_t . Hence, d is a power of p . Assume now that $\Delta \not\subseteq \Omega_t$. Since the orbits Ω_j form a partition of Ω ,

$$\Delta = \bigcup_{j=0}^t (\Delta \cap \Omega_j),$$

where, for $j = 0, \dots, t-1$, $\Delta \cap \Omega_j$ is fixed point wise 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 .

Corollary 2.7.12 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n$, $S \in \text{Syl}_p(H)$ and $B = N_H(S)$. Let $n = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0$ be the p -adic decomposition of n . Suppose that M is an imprimitive subgroup of H containing B . Then there exists $1 \leq r \leq t$ such that $p^r | n$ and M is isomorphic to a subgroup of $\text{Sym}(p^r) \wr \text{Sym}(n/p^r)$. In particular, $k_0 = k_1 = \cdots = k_{r-1} = 0$.*

Proof. Let Δ be a nontrivial block of M . Then, by Theorem 2.7.11, Δ has length p^r , for some $1 \leq r \leq t$, with p^r dividing n . Also, M embeds in the stabilizer in H of the complete block system $\{\Delta^x \mid x \in M\}$ determined by Δ , which is isomorphic to $\text{Sym}(p^r) \wr \text{Sym}(n/p^r)$.

Lemma 2.7.13 *Let $H = \text{Sym}(\Omega)$, $S \in \text{Syl}_p(H)$ and $B = N_H(S)$. If M is an intransitive subgroup of H containing B , then*

$$M \leq \text{Sym}(\Delta_1) \times \text{Sym}(\Delta_2),$$

with $\Omega = \Delta_1 \cup \Delta_2$ and the Δ_i 's unions of orbits of M on Ω . Moreover

$$M = (M \cap \text{Sym}(\Delta_1)) \times (M \cap \text{Sym}(\Delta_2)).$$

Proof. The first part of the statement is obvious. The second follows from Lemma 2.1.17.

Theorem 2.7.14 *Let p be a prime, $p \neq 2, 3$, and $G = \text{Sym}(\Omega)$, with $|\Omega| = p$. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Then B is a maximal subgroup of G .*

Proof. See Covello [8] (Theorem 6.1.2).

Corollary 2.7.15 *Let $G = \text{Sym}(\Omega)$, with $|\Omega| = n$, $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Suppose that $n = k_1 p^m + k_0$, 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 , such subgroups are primitive on Ω .*

Proof. See Covello [8] (Lemma 6.5.1).

2.8 Maximal subgroups of the symmetric groups

According to the O'Nan-Scott theorem, stated as the second theorem in Appendix [2], and the first theorem in [19] we get the following important results:

Theorem 2.8.1 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n > 2$. Then, for all $r \geq 1$ such that $n \neq 2r$, the group*

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

is a maximal (intransitive) subgroup of H .

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 $L = \text{Sym}(\Omega_1) \times \text{Sym}(\Omega_2)$. 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 H 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, 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

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

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

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

This implies, as $n \neq 2r$, that M_α cannot have three orbits on Ω . So M_α has two orbits on Ω 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 Lemma 2.5.14, we get that $M = H$.

Theorem 2.8.2 *Let $H = \text{Sym}(\Omega)$, with $|\Omega| = n > 1$. Then, for all integers k and m such that $n = km$, the group*

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

is a maximal (imprimitive) subgroup of H .

Proof. First, by Proposition 2.5.16, L is the stabilizer in H of a block system of m blocks of length k and L is imprimitive. Now let $M \leq H$ such that $L < M$. If M is primitive, then, as M contains transpositions, by Lemma 2.5.14, $M = H$. 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 $L \leq M$, against Theorem 2.5.15. Thus L is a maximal subgroup of H .

Chapter 3

Maximal p -local subgroups of symmetric groups

We maintain the notation introduced in Chapter 1. The aim of this chapter is to reduce the investigation of maximal p -local subgroups to some critical cases. We start examining some specific cases. When we come to consider the symmetric groups $\text{Sym}(p)$ and $\text{Sym}(p+1)$ some fact about the normalizer of a Sylow p -subgroup, for which the reader can refer to [8], are used.

3.1 $\text{Sym}(p^m)$

Recall that the normalizer of a Sylow p -subgroup of $\text{Sym}(p)$ is a maximal subgroup of $\text{Sym}(p)$.

Theorem 3.1.1 *Let $G = \text{Sym}(\Omega)$ with $|\Omega| = p$, where p is a prime. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. Then $\mathcal{N}_{\max}(G, B) = \{B\}$.*

Proof. If $p = 2, 3$, then $B = G$, $O_p(G) \neq 1$ and there is nothing to prove. So assume that $p \neq 2, 3$. By Proposition 2.6.4, we know that $T \cong C_p$, where C_p is a cyclic group of order p . Since T is a normal p -subgroup of B , we have that $O_p(B) \neq 1$ and Theorem 2.7.14 implies that B is a maximal p -local subgroup of G . Let N be a maximal p -local subgroup of G with respect to B such that $N \neq B$. Then $B < N \leq G$ and $O_p(N) \neq 1$. Using Theorem 2.7.14, $N = G$, which contradicts the fact that $O_p(G) = 1$. Thus B is a unique maximal p -local subgroup of G with

respect to B , which completes the proof.

We now look at those subgroups in $\mathcal{N}_{\max}(G, T)$ which act transitively on Ω . Recall that if $G = \text{Sym}(2^2)$, then $\mathcal{N}_{\max}(G, B) = \{\text{Sym}(4)\}$ because $\text{Sym}(4) = N_G(A)$ where $A = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$. Our next result concerns subgroup in $\mathcal{N}_{\max}(G, B)$, where $G = \text{Sym}(p^2)$ with $p > 2$.

Lemma 3.1.2 *Let $G = \text{Sym}(\Omega)$ with $|\Omega| = p^2$, where p is a prime such that $p > 2$. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. If $N \in \mathcal{N}_{\max}(G, B)$, then N is isomorphic to $\text{Sym}(p) \wr \text{Sym}(p)$.*

Proof. Let $L = \text{Sym}(p) \wr \text{Sym}(p)$. By Theorem 2.7.3, using Corollary 2.5.17, we know that $B \leq L$. By Theorem 2.8.2, L is a maximal subgroup of G . Since N is a subgroup of G containing B , by Theorem 2.7.9, we may assume that N 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 N must have length p and, by Corollary 2.5.17, N is isomorphic to a subgroup of L . Since, by Proposition 2.5.16, L is isomorphic to the stabilizer of $\text{Sym}(p)$ acting on

$$\{\{1, 2, \dots, p\}, \{p+1, p+2, \dots, 2p\}, \dots, \{p(p-1)+1, p(p-1)+2, \dots, p^2\}\}$$

in G . Therefore, $\text{Sym}(p) \wr \text{Sym}(p) \cong N_G(E)$, where

$$E = \langle (1, 2, \dots, p), (p+1, p+2, \dots, 2p), \dots, (p(p-1)+1, p(p-1)+2, \dots, p^2) \rangle.$$

Using Theorem 2.6.14, E is a unique elementary abelian normal p -subgroup of order p^p of T . As $E \leq N_G(E)$, we have that $O_p(N_G(E)) \neq 1$. It follows that $\text{Sym}(p) \wr \text{Sym}(p) \cong N_G(E) \in \mathcal{N}(G, T)$ and hence $N \cong \text{Sym}(p) \wr \text{Sym}(p)$.

Theorem 3.1.3 *Let $G = \text{Sym}(\Omega)$ with $|\Omega| = p^m$, where p is a prime such that $p > 2$ and $m \in \mathbb{N}$ such that $m > 1$. Suppose that $T \in \text{Syl}_p(G)$ and $B = N_G(T)$. If $N \in \mathcal{N}_{\max}(G, B)$, then N leaves invariant a block system with blocks of size p . In particular, N is isomorphic to $\text{Sym}(p) \wr \text{Sym}(p^{m-1})$.*

Proof. Using Theorem 2.6.9, N is transitive on Ω . We argue by induction on m starting with the case $m = 2$. For $m = 2$, by Lemma 3.1.2, the lemma clearly holds.