University of L'Aquila

Two Different Approaches to the Study of Abelian Regular Subgroups of the Symmetric Group

Department of Information Engineering, Computer Science and Mathematics

PhD program in Mathematics and modeling – 38th Cycle

SSD : MATH-02/A

Candidate

Giuseppe Nozzi
ID number 289063

Thesis Supervisors

Prof. Norberto Gavioli
Prof. Riccardo Aragona

PhD Coordinator

Prof. Debora Amadori

Two Different Approaches to the Study of Abelian Regular Subgroups of the Symmetric Group

Ph.D. thesis. University of L'Aquila

This thesis has been typeset by LaTeX and the uaqthesis class.

Author's email: giuseppenozzi@hotmail.com

PREFACE

This doctoral thesis incorporates and expands upon research that I have previously developed and disseminated through four articles. All of them have been published in peer-reviewed mathematics journals.

- *Transfinite hypercentral iterated wreath product of integral domains*, Aragona R., Gavioli N., Nozzi G., 2025 , *Annali di Matematica Pura e Applicata*, https://doi.org/10.1007/s10231-025-01616-6.
- *Normality conditions in the Sylow p-subgroup of* $\mathrm{Sym}(p^n)$ *and its associated Lie algebra*, Aragona R., Gavioli N., Nozzi G., 2025 , *Journal of Algebra*, https://doi.org/10.1016/j.jalgebra.2025.10.033.
- *A classification of module braces over the ring of p-adic integers*, Aragona R., Gavioli N., Nozzi G., 2025 , *Ricerche di Matematica*, https://doi.org/10.1007/s11587-025-00972-y.
- *Classification of a specific class of* $\mathbb{F}_{p^k}$*-braces using bilinear forms*, Aragona R., Nozzi G., 2025 , *Journal of Algebra and Its Applications*, https://doi.org/10.1142/S0219498826502592.

Some notational or expository changes have been made for consistency and clarity.

CONTENTS

INDEX OF NOTATION

$\mathbb{F}_p$	field of characteristic p.
Sym	symmetric group.
AGL	affine general linear group.
σ	right regular representation.
D	integral domain of characteristic 0.
F	field of fractions of D.
$\mathrm{Fun}(A, B)$	group of functions from A to B with pointwise multiplication.
N	normalizer.
$\mathfrak{N}$	idealizer.
U_n	p-Sylow subgroup of $\mathrm{AGL}(V)$.
W_n	wreath product of n copies of $\mathbb{F}_p$.
W_n^∞	wreath product of n-copies of D.
$\gamma_*(G)$	$*$-term of lower central series of G.
$Z_*(G)$	$*$-term of the upper central series of G.
Stab	stabilizer.
$\mathrm{wt}(*)$	weight function of the partition $*$.
$\mathcal{P}(*)$	Partitions with maximal part at most $*$.
lt	leading term.

$\mathbf{N}_*^{(p)}$	$*$-term of the normalizer chain originating from T in W_n.
$\mathbf{N}_*^{(\infty)}$	$*$-th term of the normalizer chain originating from T in W_n^∞.
$\mathfrak{N}_*^{(p)}$	$*$-term of the idealizer chain originating from $\mathfrak{T}$ in $\mathfrak{L}_n$.
$\mathfrak{N}_*^{(\infty)}$	$*$-th term of the idealizer chain originating from $\mathfrak{T}$ in $\mathfrak{L}_n^\infty$.
R	principal ideal domain.
$\mathrm{Hol}(*)$	holomorph of the group $*$.
M	free module over R.
$\mathrm{Aff}(*)$	affine group of $*$.
$\mathrm{Ann}(*)$	annihilator of the algebra (or brace) $*$.
$\mathfrak{s}(*)$	scale of the lattice $*$.
$d(*)$	discriminant of the matrix $*$.

ABSTRACT

Let $n \geq 2$ and V be a vector space over a finite field of dimension n. This thesis is devoted to the study of elementary abelian regular subgroups of the symmetric group $\mathrm{Sym}(V)$. After recalling the necessary background and summarizing previous results in the literature, we investigate the p-Sylow subgroup W_n of the symmetric group on p^n elements. We introduce a weighted degree order on its elements, compute its central series, and study the Lie algebra associated with its lower central series. Moreover we study the normal subgroups of W_n and the normalizer chain originating from the canonical elementary abelian regular subgroup of W_n.

We extend this analysis to characteristic zero by constructing an analogue of W_n as an iterated wreath product over an integral domain, proving that it is transfinite hypercentral and explicitly describing its ascending central series and normal subgroups.

In the final part of the thesis, we study abelian regular subgroups of affine groups over free modules by exploiting their correspondence with bi-brace structures. Under suitable assumptions, we reduce the classification problem to the study of bilinear forms, and we obtain classification results over finite fields of odd characteristic and over the ring of p-adic integers, both in the torsion-free and torsion cases.

INTRODUCTION

Let $n \geq 2$ and V be a vector space over a finite field of dimension n. Although this is not the only topic covered, the common thread connecting all chapters of this work is the study of elementary abelian regular subgroups of the symmetric group $\mathrm{Sym}(V)$. In Chapter 2 and Chapter 3 of this thesis, we approach this theme by studying the normalizer chain arising from the image of the regular representation of V (which we call the canonical elementary abelian regular subgroup), introduced for the first time in [5]. In the final chapter (4) of the thesis, using the well-known bijective correspondence between these subgroups and algebraic structures known as bi-braces (see, for example, [17] or Theorem 1.6.4 in this thesis), we provide a classification for specific types of these bi-braces.

The motivation for studying this class of subgroups of the symmetric group arises from the increasing interest in this area within the field of cryptography (see [14–16, 18]). We briefly outline the reasons below.

Let V be a vector space partitioned into b blocks, that is,

$$V = V_1 \oplus \cdots \oplus V_b,$$

with $\dim(V_i) = s$, and $s \in \{4, 8\}$. This decomposition forms the basis of the design of many modern ciphers based on Substitution-Permutation Networks (SPN), such as AES (see e.g. [25]). For $R \geq 1$, a classical round function E_k is a nonlinear permutation in $\mathrm{Sym}(V)$ with the following structure: $E_k = \varepsilon_{k_1} \cdots \varepsilon_{k_R}$, and for

$c \in \{1, \ldots, R\}$ we have $\varepsilon_c = \bar{\gamma}\lambda\sigma_c$. Where

- $\bar{\gamma}(V)$ is the *confusion layer* and denotes the application of b copies of a nonlinear map $\gamma \in \mathrm{Sym}(2^s)$, called *s-box*. In other words,

$$\bar{\gamma}((x_1, \ldots, x_n)) = (\gamma((x_1, \ldots, x_s)), \ldots, \gamma((x_{s(b-1)}, \ldots, x_n))).$$

- λ is the *diffusion layer* and is a linear map in $\mathrm{GL}(n, 2)$.

- $\sigma_c : x \mapsto x + c$ represents the key addition, where $+$ is the bitwise XOR on $\mathbb{F}_2$.

Remark 0.0.1. The round keys k_i are derived from the master key k through a public algorithm called the key schedule, $k \mapsto (k_1, \ldots, k_R) \in V^R$.

Definition 0.0.2. A block cipher on the plaintext space V is a family $\{E_k\}_{k \in \mathcal{K}}$ of encryption functions (as defined above) indexed by a key space $\mathcal{K}$.

The security of a block cipher mainly depends on how far its encryption functions are from being linear, i.e., roughly speaking, on the distance of the s-box γ from the affine group $\mathrm{AGL}(V)$. For a definition of non-linearity see [19, 38].

Notice that $\mathrm{Sym}(V)$ contains several isomorphic copies of $\mathrm{AGL}(V)$, each corresponding to a different operation induced on V. To be more precise, let T be the group of translations of V. If we take any element $g \in \mathrm{Sym}(V)$ such that the conjugate subgroup $\mathrm{AGL}(V)^g \neq \mathrm{AGL}(V)$, this new group $\mathrm{AGL}(V)^g$ acts on V in a distinct way. This new action is inherited from the group of translations T^g, which is itself a new elementary abelian regular subgroup of $\mathrm{Sym}(V)$.

This leads to a new research direction in cryptanalysis: studying the non-linearity of encryption functions with respect to these alternative affine structures. Indeed, an alternative operation on V may cause encryption functions to be closer to linear, potentially exposing new vulnerabilities.

Recent works [14, 15] have demonstrated the practical implications of these ideas. The authors construct a cipher resistant to classical differential attacks [13], but which can be attacked using another operation. This motivates a deeper algebraic study of elementary abelian regular subgroups and their conjugacy classes within $\mathrm{Sym}(V)$.

This line of research has been developed mainly in the series of papers [2–7]. The present PhD thesis fits into this framework and provides a unified and comprehensive treatment of the subject, collecting and extending the results obtained in those works.

We also emphasize that, although the cryptographic setting provided the original motivation for the study of elementary abelian regular subgroups of the symmetric group, the continuation of this analysis in odd and zero characteristic does not currently have direct cryptographic applications, and is pursued for its intrinsic algebraic interest.

Organization of the Thesis and Principal Results

The first chapter of this thesis aims to provide all the preliminaries necessary for a smooth reading of the work. In particular, it presents the main results obtained in the series of papers [2–7], of which this thesis serves as the conclusion. It also introduces the preliminary notions concerning the theory of skew braces that will be used in the final chapter.

In the second chapter, we focus our attention on the p-Sylow subgroup W_n of the symmetric group over p^n elements. We introduce a total order on the elements of W_n through a weighted degree with respect to p (see Subsection 2.0.1). Subsequently, we compute the ascending and descending central series of W_n and prove that they coincide (see Theorem 2.1.8). This result was already established in [34], but here we provide a different proof using alternative techniques.

We then introduce the Lie algebra associated with the lower central series of W_n, denoted by $\mathfrak{L}_n$. We also prove that its central series coincide (see Corollary 2.2.11). Using the descending central series of W_n, we define a map φ that sends group elements to elements of the algebra.

After introducing the concept of a saturated subgroup of W_n (see Definition 2.1.1) and a homogeneous subring of $\mathfrak{L}_n$ (see Definition 2.2.1), we prove that the normalizer of a saturated subgroup of W_n and the idealizer of the image of the saturated subgroup under φ in $\mathfrak{L}_n$ have the same cardinality (see Equation (2.12)). This allows us to refer to the results in [2] to determine the growth of the chain of normalizers

originating from T (see Theorem 2.3.12).

We conclude this chapter by proving that any normal subgroup of W_n always contains a term of the descending central series, and we provide an estimate of its index (see Equation (2.17)).

In the third chapter, we turn our attention to infinite groups. Specifically, we construct the analogue of the group W_n, which we denote by W_n^∞, in characteristic zero. To this end, since W_n can be seen as the iterated wreath product of n copies of $\mathbb{F}_p$, in this chapter we consider the iterated wreath product of n-copies of an integral domain of characteristic zero.

Subsequently, we prove that, under suitable restrictions on the base subgroups of the wreath product, the group W_n^∞ is transfinite hypercentral (see Appendix A.2 and Theorem 3.1.13) and we explicitly compute its ascending central series (see Equation (3.9)). Analogously to our work in characteristic p, we demonstrate that the full normal subgroups (see Definition 3.3.1) coincide with the terms of the ascending central series of W_n^∞ (see Theorem 3.3.4).

We then determine the growth of the chain of normalizers originating from the abelian regular subgroup generated by constant functions (see Subsection 3.4). In the final section of the second chapter, we find the characteristic zero counterpart of Proposition 1.1.4 and Theorem 1.1.5.

In the fourth chapter, we let M be a free module of rank n over a principal ideal domain R. We denote by T_+ the group of translations of $(M,+)$, and by $T_\circ$ another abelian regular subgroup of the affine group of M. These two regular subgroups induce two operations, $+$ and $\circ$, on M, and under the assumption that T_+ normalizes $T_\circ$ (see Assumption 4.1.2), the triple $(M,+,\circ)$ becomes a bi-brace. Equivalently, T_+ normalizes $T_\circ$ if and only if the algebra $(M,+,\cdot)$ is nilpotent of class 3 (see Proposition 4.1.3), where the operation $\cdot$ is defined by $a\cdot b = a\circ b - a - b$ for $a,b\in M$.

Assuming that $M\cdot M$ is a cyclic R-submodule of M, we associate to every bi-brace structure on M (or, equivalently, to every abelian regular subgroup of the affine group of M) a bilinear form (see Equation 4.7). We emphasize that assumptions 4.1.2 and 4.2.1 are the same as those made in [15, 22], where their

relevance in cryptographic applications is also discussed.

This allows us to reduce the problem of classifying bi-braces to a problem of classifying bilinear forms. We have therefore studied two particular cases. The first one is the case where $R = \mathbb{F}_{p^k}$, a finite field of odd characteristic. In this setting, we show that there exist either one or two isomorphism classes of $(M, +, \circ)$, depending on the dimension of M as a vector space (see Theorem 4.3.7).

Next, we examine the case where $R = \mathbb{Z}_p$, the ring of p-adic integers. It is natural to treat separately the case in which M is torsion-free and the case in which it has torsion. In the torsion-free case, we obtain results that closely resemble those for $R = \mathbb{F}_{p^k}$ (see Theorem 4.4.8), using the Jordan decomposition of non-degenerate bilinear forms over $\mathbb{Z}_p$ (see [24, Chapter 15]). In the torsion case, we rely on the notion of isoclinism between braces introduced in [36] (we note that in our setting, this definition coincides with the notion of isoclinism between R-algebras), and we determine the number of isoclinism classes of bi-braces $(M, +, \circ)$ (see Theorem 4.5.10).

CHAPTER 1

PRELIMINARIES

1.1 Regular Elementary Abelian Subgroups of $\mathrm{Sym}(V)$

Let V be a vector space over $\mathbb{F}_p$ of dimension $n \geq 2$, and let $\{e_1, e_2, \ldots, e_n\}$ be a fixed basis for V. We begin by describing the regular subgroups of the symmetric group $\mathrm{Sym}(V)$ associated with two different regular embeddings of the vector space V, leading to different group structures T_+ and $T_\circ$. These embeddings induce distinct group operations on V. Let us denote by $\sigma\colon V \to \mathrm{Sym}(V)$ the right regular representation and by T_+ the image σ_V of this representation, i.e.,

$$T_+ = \{\sigma_v \mid v \in V,\ x \mapsto x + v\}. \tag{1.1}$$

We consider $\tau : V \to \mathrm{Sym}(V)$ another regular embedding of V into $\mathrm{Sym}(V)$ and $T_\circ = \{\tau_v \mid v \in V\}$, where τ_v is the unique (by regularity of $T_\circ$) map sending $0 \mapsto v$. Notice that using the group $T_\circ$ we can define a new operation on V by setting

$$u \circ v \coloneqq u\tau_v \text{ for all } u, v \in V. \tag{1.2}$$

Although this fact is straightforward, it is worth emphasizing that the groups $T_\circ$ and T_+ are elementary abelian regular groups.

Let us introduce the subspace W of both $(V, +)$ and $(V, \circ)$, defined as

$$W = \{v \in V \mid v + u = v \circ u \text{ for all } u \in V\}. \tag{1.3}$$

Notice that $\sigma_W = \tau_W = T_+ \cap T_\circ$.

Remark 1.1.1. As we will show in Section 4.1, we can endow V with a multiplication by setting $u \cdot v = u \circ v - u - v$ for $u, v \in V$. The triple $(V, +, \cdot)$ is actually a nilpotent algebra, and so the subspace $W = \{v \in V \mid v \cdot V = 0\}$ is nontrivial. This has been already observed in [18].

The following classical result allows us to conclude that isomorphic regular subgroups of the symmetric group are conjugate, a fact that is crucial in our context. For a proof of this theorem see e.g. [4, Theorem 1].

Theorem 1.1.2 (Dixon)**.** *Let* $X = \{x_1, x_2, \ldots, x_m\}$ *be a finite set and let* H *and* K *be regular subgroups of* $\mathrm{Sym}(X)$*. If* $H \cong K$*, then there exists* $g \in \mathrm{Sym}(X)$ *such that* $K = H^g$*.*

As a consequence there exists $g \in \mathrm{Sym}(V)$ such that $T_+ = T_\circ^g$. Moreover, since $N_{\mathrm{Sym}(V)}(T_+) = \mathrm{AGL}(V, +)$, we have that

$$N_{\mathrm{Sym}(V)}(T_\circ) = \mathrm{AGL}(V, +)^g := \mathrm{AGL}(V, \circ). \tag{1.4}$$

From now on, until the end of this section, we assume $p = 2$.

Proposition 1.1.3. *[16] Let* $T_\circ$ *be such that* $T_+ \neq T_\circ$*. If* $W \leq V$ *is such that* $\sigma_W = T_+ \cap T_\circ$*, then* $\dim(W) \leq n - 2$*.*

Proof. Assume by way of contradiction that $\dim(W) = n - 1$. Let $\{v_1, \ldots, v_{n-1}\}$ be a basis for W and $v \in V \setminus W$. We claim that $a\tau_v = a\sigma_v$ for any $a \in V$, that is $v \in T_+ \cap T_\circ$. If $a \in W$ there is nothing to prove. We consider $a = w + v$, for some $w \in W$. We get that

$$\begin{aligned} a\tau_v &= (w + v)\tau_v = (w\sigma_v)\tau_v \\ &= (w\tau_v)\tau_v = w(\tau_v)^2 = w \\ &= a\sigma_v. \end{aligned}$$

□

In particular, none of the subgroups $T_\circ$ has maximal intersection with T_+. The authors of [4] focus on the study of elementary abelian regular subgroups of $\mathrm{Sym}(V)$ which intersect T_+ in a second-maximal subgroup, that is $|T_+ \cap T_\circ| = 2^{n-2}$.

Let W be as in Equation (1.3) and of dimension $n-2$. Without loss of generality, we may assume $W = \mathrm{span}\{e_3, \ldots, e_n\}$. We denote by $v^{(i:j)}$ the vector consisting of

the coordinates of v from the i-th to the j-th, for $1 \leq i < j \leq n$. The following result characterizes the structure of elementary abelian regular subgroups of $\mathrm{Sym}(V)$ that intersect T_+ in a second-maximal subgroup. We will provide an analogous characterization in the case of characteristic zero in Proposition 3.5.5.

Proposition 1.1.4. *[4, Proposition 2] The elementary abelian regular subgroups of* $\mathrm{Sym}(V)$ *intersecting* T_+ *in a second-maximal subgroup are subgroups of* $\mathrm{AGL}(V)$. *Moreover, they are of the form*

$$T_b \stackrel{\text{def}}{=} \langle\, \pi_b, \varepsilon_b, \sigma_{e_i} \mid 3 \leq i \leq n \,\rangle\,,$$

where

$$\pi_b = \left(\begin{array}{c|c} 1_2 & \begin{matrix} 0 \\ b^{(3:n)} \end{matrix} \\ \hline 0 & 1_{n-2} \end{array}\right)\sigma_{e_1}, \quad \varepsilon_b = \left(\begin{array}{c|c} 1_2 & \begin{matrix} b^{(3:n)} \\ 0 \end{matrix} \\ \hline 0 & 1_{n-2} \end{array}\right)\sigma_{e_2}, \tag{1.5}$$

for some $b \in W \setminus \{0\}$.

Notice that, since $T_+ \trianglelefteq \mathrm{AGL}(V,+)$, it follows that T_+ is a normal subgroup of every Sylow 2-subgroup of $\mathrm{AGL}(V,+)$. Moreover, interchanging the roles of T_+ and $T_\circ$ in the previous statement, we also have that $T_+ \leq \mathrm{AGL}(V,\circ)$.

The following theorem is the main result of [4]. We will later provide an analogous result stated for characteristic zero (see Corollary 3.5.6).

Theorem 1.1.5. *Any Sylow* 2*-subgroup* U *of* $\mathrm{AGL}(V,+)$ *contains, as normal subgroups, exactly two elementary abelian regular subgroups conjugated to* T_+. *Moreover, the normalizer* $N_{\mathrm{Sym}(2^n)}(U)$ *of* U *in* $\mathrm{Sym}(V)$ *interchanges by conjugation these two subgroups.*

1.2 Chief Series of T and Sylow p-subgroup of $\mathrm{Sym}(V)$

From this point onward, we assume that p is an odd prime unless otherwise explicitly specified. In this section, let V be a vector space over $\mathbb{F}_p$ of dimension $n \geq 2$. As before, $\{e_1, \ldots, e_n\}$ denotes a basis of V. We set T as the image of the right regular representation of V in $\mathrm{Sym}(V)$, and denote by $\mathrm{AGL}(V)$ the normalizer of T within $\mathrm{Sym}(V)$.

First, we recall that there is a one-to-one correspondence between the Sylow p-subgroups of $\mathrm{AGL}(V)$, the set of all chief series of T, and the Sylow p-subgroups of $\mathrm{Sym}(V)$.

Since T is an elementary abelian p-group of order p^n, every subgroup of T of order p^i is isomorphic to $\mathbb{F}_p^i$. A chief series $\mathfrak{F}\colon 1 = T_0 < T_1 < \cdots < T_n = T$ in T has length n, and each factor T_{i+1}/T_i is a cyclic group of order p. It follows that every such series corresponds to a maximal flag $\mathcal{F}$ of subspaces $\{0\} < V_1 < \cdots < V_n = V$ in V.

Let U be a Sylow p-subgroup of $\mathrm{AGL}(V)$. Up to conjugation by an element in $\mathrm{AGL}(V)$, we may assume $U := \mathcal{U} \ltimes T$, where $\mathcal{U}$ is the group of upper unitriangular matrices, a Sylow p-subgroup of $\mathrm{GL}(V)$. The vector space V is an uniserial $\mathcal{U}$-module, that is, any $\mathcal{U}$-submodule of V is contained in the *maximal flag* $\{0\} = V_0 < V_1 < \ldots < V_n = V$, with $V_i = \langle\, e_{n-i+1}, \ldots, e_n \,\rangle$ and $1 \leq i \leq n$. For any given maximal flag

$$\mathcal{F}\colon\ \{0\} = V_0 < V_1 < \ldots < V_n = V,$$

if $\mathcal{U}$ is the stabilizer of $\mathcal{F}$ in $\mathrm{GL}(V)$, then $\mathcal{U}T$ is a Sylow p-subgroup of $\mathrm{AGL}(V)$. Thus, there is a one-to-one correspondence between the Sylow p-subgroups of $\mathrm{AGL}(V)$ and the set of maximal flags of subspaces of V. Indeed, given a maximal flag $V_0 < V_1 < \ldots < V_n$, the corresponding Sylow p-subgroup of $\mathrm{AGL}(V)$ is exactly the stabilizer under conjugation of the associated chief series

$$1 = \sigma_{V_0} < \sigma_{V_1} < \ldots < \sigma_{V_n} = T.$$

To establish the correspondence between the chief series in T and the Sylow p-subgroups of $\mathrm{Sym}(V)$, we introduce the following notion.

Definition 1.2.1. Let $T \leq G$ be finite p-groups, and let $\mathfrak{F}\colon 1 = T_0 < T_1 < \cdots < T_m = T$ be a chief series in T. We say that the chief series $\mathfrak{F}$ is induced by the chief series $1 = G_0 < \cdots < G_n = G$ in G if

$$\{T \cap G_j \mid 0 \leq j \leq n\} = \{T_i \mid 0 \leq i \leq m\}. \tag{1.6}$$

Notice that, since chief factors of finite p-groups are cyclic of order p, every chief series in G induces a chief series in T. If, for any chief series $\mathfrak{F}$ in T, there exists a

finite p-group $G_{\mathfrak{F}} \geq T$ such that every chief series in $G_{\mathfrak{F}}$ induces $\mathfrak{F}$ in T, we say that $G_{\mathfrak{F}}$ *controls* $\mathfrak{F}$.

Theorem 1.2.2 ([35]). *Let T be the image of the right regular representation of V in $\mathrm{Sym}(V)$.*

- *Every Sylow p-subgroup of $\mathrm{Sym}(V)$ containing T controls a chief series in T.*
- *For every chief series $\mathfrak{F}$ in T there exists a unique Sylow p-subgroup $W_{\mathfrak{F}}$ of $\mathrm{Sym}(V)$ which contains T and controls $\mathfrak{F}$.*

As a consequence of the previous theorem, the number of chief series in T corresponds to the number of Sylow p-subgroups of $\mathrm{Sym}(V)$. Furthermore, each Sylow p-subgroup $U_{\mathfrak{F}}$ of $\mathrm{AGL}(V)$ uniquely determines a chief series $\mathfrak{F}$ of T and a Sylow p-subgroup $W_{\mathfrak{F}}$ of $\mathrm{Sym}(V)$ that contains T, controls $\mathfrak{F}$, and satisfies $U_{\mathfrak{F}} = W_{\mathfrak{F}} \cap \mathrm{AGL}(V)$. It follows that

$$N_{W_{\mathfrak{F}}}(T) = U_{\mathfrak{F}} = W_{\mathfrak{F}} \cap \mathrm{AGL}(V). \tag{1.7}$$

From now on, we will fix the chief series $\mathfrak{F}$ in T and we will refer to $W_{\mathfrak{F}}$ and $U_{\mathfrak{F}}$ as W_n and U_n, respectively.

The Sylow p-subgroup of $\mathrm{Sym}(V)$ can be seen as a group of permutations that stabilizes the chain of imprimitivity (see Appenidix A.1) defined as follows. For each integer $0 \leq m \leq n$ and for each $0 \leq k \leq p^m - 1$, we define the fundamental blocks

$$\Theta^n_{m,k} := \{kp^{n-m} + 1, \ldots, (k+1)p^{n-m}\}$$

each of them with cardinality p^{n-m}. These blocks partition $\{1, \ldots, p^n\}$ into p^m blocks of equal size. Let Θ^n_m be the partition at the level m. That is,

$$\Theta^n_m := \left\{\Theta^n_{m,0}, \ldots, \Theta^n_{m,p^m-1}\right\}.$$

This yields a chain of imprimitivity

$$\mathcal{C}_n \colon \Theta^n_0 \succ \cdots \succ \Theta^n_m \succ \cdots \succ \Theta^n_n$$

where $\Theta^n_0 = \{1, \ldots, p^n\}$ and $\Theta^n_n = \{\{1\}, \{2\}, \ldots, \{p^n\}\}$. The Sylow p-subgroup W_n of $\mathrm{Sym}(V)$ is exactly the stabilizer of the entire chain $\mathcal{C}_n$

$$W_n := \bigcap_{m=1}^{n} \mathrm{Stab}_{\mathrm{Sym}(p^n)}(\Theta^n_m).$$

Moreover, for $1 \leq i \leq n$, the set $\{s_1, \ldots, s_n\}$ with

$$s_i := \prod_{j=1}^{p^{i-1}} (j, j+p^{i-1}, \ldots, j+(p-1)p^{i-1})$$

is a minimal generating set. Notice that each s_i acts non-trivially on the blocks of the partition Θ_j^n with $j > i$, permuting them cyclically.

Remark 1.2.3. Notice that the chain $\mathcal{C}_n$ is a maximal imprimitivity chain for the translation group T. Moreover, every maximal imprimitivity chain for T corresponds to a chief series in T, namely $1 = T_0 < \cdots < T_n = T$, such that Θ_i^n is the set of orbits of T_{n-i}. In view of the previous discussion, $\mathcal{C}_n$ is the unique maximal imprimitivity chain that is stabilized by the group U_n, under conjugation.

Our aim is to calculate the normalizer chain originating from T and defined as follows.

$$\mathbf{N}_i^{(p)} = \begin{cases} T & \text{if } i = -1 \\ U_n & \text{if } i = 0 \\ N_{\mathrm{Sym}(V)}(\mathbf{N}_{i-1}^{(p)}) & \text{if } i \geq 1. \end{cases} \tag{1.8}$$

We already observed in Equation (1.7) that $U_n = N_{W_n}(T)$. The following result of [5] shows that the chain remains unchanged when computed in W_n instead of $\mathrm{Sym}(V)$.

Theorem 1.2.4. *[5] For every $k \geq 1$, we have $\mathbf{N}_k^{(p)} = N_{W_n}(\mathbf{N}_{k-1}^{(p)})$.*

Proof. Let Θ be a system of imprimitivity for $\mathbf{N}_{k-1}^{(p)}$. For each $x \in \mathbf{N}_k^{(p)}$, Θ^x is a system of imprimitivity for $(\mathbf{N}_{k-1}^{(p)})^x = \mathbf{N}_{k-1}^{(p)}$. Thus, for a given $x \in \mathbf{N}_k^{(p)}$ and an imprimitivity chain $\mathcal{C}$ for $\mathbf{N}_{k-1}^{(p)}$, the set $\mathcal{C}^x$ is also an imprimitivity chain for $\mathbf{N}_{k-1}^{(p)}$ and a fortiori for U_n. By Remark 1.2.3, $\mathcal{C}_n$ is the unique maximal one for U_n, and so $\mathcal{C}_n^x = \mathcal{C}_n$. It follows that $\mathcal{C}_n$ is stabilized by $\mathbf{N}_k^{(p)}$ for every k, i.e. $\mathbf{N}_k^{(p)} \leq W_n$. □

1.3 Yang-Baxter Equation and Set-Theoretic Solutions

In Chapter 4 of this thesis, the analysis of regular abelian subgroups of the symmetric group makes use of recently introduced algebraic structures known as

skew braces. Owing to the relatively recent development of skew brace theory, the remainder of this chapter is devoted to outlining the fundamental notions and the key results in the field, with the aim of guiding readers who may not yet be familiar with it. All results and proofs presented from this point on, up to the end of the chapter, are well established and can be found in [20, 28, 30, 31, 37, 42, 44].

We start by introducing the algebraic framework in which skew braces naturally arise.

A solution to the Yang-Baxter equation (YBE) is a linear map $R\colon V\otimes V \to V\otimes V$ such that

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12},$$

where V is a vector space and R_{ij} denotes the map from $V\otimes V\otimes V$ to $V\otimes V\otimes V$ acting as R on the (i,j) factor and as the identity on the remaining factor.

An interesting class of solutions of the YBE arises when V has an R-invariant basis X. In such a case, the solution is said to be *set-theoretic*.

Definition 1.3.1. A set-theoretic solution to the YBE is a pair (X,r), where X is a non-empty set and $r\colon X\times X\to X\times X$ is a map such that

$$(r\times \mathrm{id})(\mathrm{id}\times r)(r\times \mathrm{id}) = (\mathrm{id}\times r)(r\times \mathrm{id})(\mathrm{id}\times r). \tag{1.9}$$

Let (X,r) be a set-theoretic solution. We will write

$$r(x,y) = (\lambda_x(y), \rho_y(x)) \tag{1.10}$$

where $\lambda_x, \rho_y\colon X\to X$. We shall say that (X,r) is non-degenerate if λ_x, ρ_x are bijective for all $x\in X$, and that (X,r) is finite if X is a finite set.

Remark 1.3.2. Notice that a set-theoretic solution can be bijective and degenerate (i.e., not non-degenerate). For example, if X is a non-empty set, then $(X, \mathrm{id}_{X\times X})$ is bijective, with

$$r(x,y) = (\lambda_x(y), \rho_y(x)) = (x,y).$$

while the maps λ_x and ρ_y are not bijective. However, non-degenerate solutions are automatically bijective (see e.g. [33]).

Remark 1.3.3 (A graphical interpretation). Let $r_1 = r \times \mathrm{id}$ and $r_2 = \mathrm{id} \times r$. We can write the Yang-Baxter equation as $r_1 r_2 r_1 = r_2 r_1 r_2$. The following figures provide an interpretation of r and the YBE in terms of graphs.

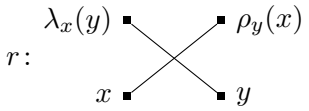

Figure 1.1. Graphical representation of r

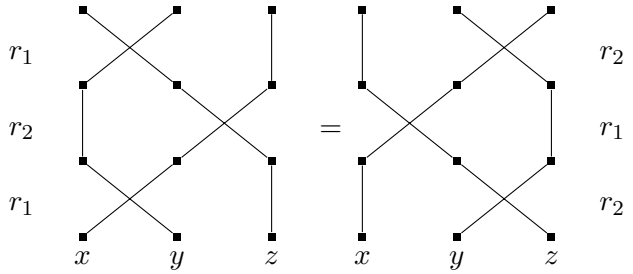

Figure 1.2. Graphical representation of the YBE

Proposition 1.3.4. *Let X be a non-empty set and let $r\colon X \times X \to X \times X$ be a map. Writing $r = (\lambda_x(y), \rho_y(x))$, we have that (X, r) is a set-theoretic solution to the YBE if and only if the following equalities hold*

- $\lambda_x \lambda_y = \lambda_{\lambda_x(y)} \lambda_{\rho_y(x)}$,
- $\lambda_{\rho_{\lambda_y(z)}(x)} \rho_z = \rho_{\lambda_{\rho_y(x)}(z)} \lambda_x$,
- $\rho_z \rho_y = \rho_{\rho_z(y)} \rho_{\lambda_y(z)}$.

Proof. Let $r_1 = r \times \mathrm{id}$ and $r_2 = \mathrm{id} \times r$. We have that

$$\begin{aligned} r_1 r_2 r_1(x, y, z) &= r_1 r_2(\lambda_x(y), \rho_y(x), z) \\ &= r_1(\lambda_x(y), \lambda_{\rho_y(x)}(z), \rho_z \rho_y(x)) \\ &= (\lambda_{\lambda_x(y)} \lambda_{\rho_y(x)}(z), \rho_{\lambda_{\rho_y(x)}(z)} \lambda_x(y), \rho_z \rho_y(x)) \end{aligned} \tag{1.11}$$

and, analogously,

$$r_2 r_1 r_2(x, y, z) = (\lambda_x \lambda_y(z), \lambda_{\rho_{\lambda_y(z)}(x)} \rho_z(y), \rho_{\rho_z(y)} \rho_{\lambda_y(z)}(x)). \tag{1.12}$$

□

Example 1.3.5. Let X be a non-empty set and let $\triangleleft\colon X \times X \to X$ be a binary operation on X. We define $r\colon X \times X \to X \times X$ such that $r(x,y) = (y, x \triangleleft y)$. The pair (X,r) is a set-theoretic solution to the YBE if and only if

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z).$$

The maps $\lambda_x = \mathrm{id}_x$ and $\rho_y(x) = x \triangleleft y$ satisfy the conditions of Proposition 1.3.4.

From now on, when we talk about a solution of the YBE, we mean a bijective non-degenerate set-theoretical solution of the YBE.

Theorem 1.3.6. *[37, Theorem 1] Let G be a group. Let $\lambda\colon G \times G \to G$ and $\rho\colon G\times \to G$ be a left and a right group action of G on itself, respectively. If λ and ρ satisfy the condition*

$$uv = \lambda_u(v)\rho_v(u), \tag{1.13}$$

then (G,r) is a solution of the YBE, where $r(u,v) = (\lambda_u(v), \rho_v(u))$.

Proof. Let $r_1 = r \times \mathrm{id}$ and $r_2 = \mathrm{id} \times r$. By Equation (1.11) and Equation (1.12) we have that

$$r_1 r_2 r_1(u,v,w) = (\lambda_{\lambda_u(v)}\lambda_{\rho_v(u)}(w), \rho_{\lambda_{\rho_v(u)}(w)}\lambda_u(v), \rho_w\rho_v(u))$$

and

$$r_2 r_1 r_2(u,v,w) = (\lambda_u\lambda_v(w), \lambda_{\rho_{\lambda_v(w)}(u)}\rho_w(v), \rho_{\rho_w(v)}\rho_{\lambda_v(w)}(u)).$$

Since $uv = \lambda_u(v)\rho_v(u)$, we get that

$$\lambda_{\lambda_u(v)}\lambda_{\rho_v(u)}(w) = \lambda_{\lambda_u(v)\rho_v(u)}(w) = \lambda_{uv}(w) = \lambda_u\lambda_v(w)$$
$$\rho_w\rho_v(u) = \rho_{vw}(u) = \rho_{\lambda_v(w)\rho_w(v)}(u) = \rho_{\rho_w(v)}\rho_{\lambda_v(w)}(u)$$

and that

$$\lambda_{\lambda_u(v)}\lambda_{\rho_v(u)}(w)\rho_{\lambda_{\rho_v(u)}(w)}\lambda_u(v)\rho_w\rho_v(u) = uvw$$
$$= \lambda_u\lambda_v(w)\lambda_{\rho_{\lambda_v(w)}(u)}\rho_w(v)\rho_{\rho_w(v)}\rho_{\lambda_v(w)}(u).$$

It follows that (G,r) satisfies the YBE. Notice that, by hypothesis, λ and ρ, are bijective, and so the solution is non-degenerate. It remains to prove that r is bijective. Let us set $r(u,v) = (\lambda_u(v), \rho_v(u)) = (x,y)$, then we obtain

$$\lambda_y(v^{-1})u = \lambda_y(v^{-1})\rho_{v^{-1}}(y) = yv^{-1} = x^{-1}u = (\lambda_u(v))^{-1}u$$

and, as a consequence, $(\lambda_u(v))^{-1} = \lambda_{\rho_v(u)}(v^{-1})$. In the same way we have that $(\rho_v(u))^{-1} = \rho_{\lambda_u(v)}(u^{-1})$. It is immediate to see that the inverse map of r is

$$r'(x,y) = ((\rho_{x^{-1}}(y^{-1}))^{-1}, (\lambda_{y^{-1}}(x^{-1}))^{-1}). \qquad \square$$

Definition 1.3.7. A solution (X, r) is said to be involutive if $r^2 = \mathrm{id}$.

Remark 1.3.8. We note that if (X, r) is an involutive solution of the YBE, then

$$(x,y) = r^2(x,y) = (\lambda_{\lambda_x(y)}\rho_y(x), \rho_{\rho_y(x)}\lambda_x(y)). \tag{1.14}$$

Thus, $\rho_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$. This means that for involutive solutions, it is enough to know the set $\{\lambda_x \mid x \in X\}$.

We remind the reader that a non-unitary ring A is a (Jacobson) radical ring if it is isomorphic to the Jacobson radical of a unitary ring.

Remark 1.3.9. Let S be a unitary ring, it is well-known that an element s lies in the Jacobson radical $\mathrm{J}(S)$ of S if and only if $1 + r \cdot s$ is invertible for all $r \in S$.

Lemma 1.3.10. *Let A be a non-unitary ring. The following statements are equivalent.*

1. *A is a radical ring.*
2. *For all $a \in A$ there exists a unique $b \in A$ such that*

$$a + b + a \cdot b = a + b + b \cdot a = 0.$$

Proof. Let A be a radical ring. There exists a unitary ring S and an isomorphism $\psi\colon A \to \mathrm{J}(S)$, where $\mathrm{J}(S)$ is the Jacobson radical of S. Let $a \in A$. By the previous remark, we know that $1 + \psi(a) \in S$ is invertible. Let $s \in S$ be such that $(1 + \psi(a))(1 + s) = 1$. From this, we can immediately deduce that $s \in \mathrm{J}(S)$. Therefore, there exists a unique $b \in A$ such that $s = \psi(b)$. We have that

$$1 = (1 + \psi(a))(1 + \psi(b)) = 1 + \psi(a) \cdot \psi(b) + \psi(a) + \psi(b)$$

and so $\psi(a + b + a \cdot b) = 0$. Since ψ is an isomorphism, we must have $a + b + a \cdot b = 0$. Conversely, assume that for every $a \in A$, there exists a unique $b \in A$ such that $a + b + a \cdot b = 0$. We define the unitary ring

$$A_1 = \mathbb{Z} \times A,$$

with operations given by: $(n,a)+(m,b) = (n+m, a+b)$ and $(n,a)(m,b) = (nm, ma+nb+a\cdot b)$. Let $a \in A$, we have that

$$(1,a)(1,b) = (1, a+b+a\cdot b) = (1,0),$$

and so $(1,a)$ is invertible in A_1.

Now let $(k,a) \in \mathrm{J}(A_1)$. Then,by the previous remark, the element

$$(1,0)+(5,0)(k,a) = (1+5k, 5a)$$

must be invertible in A_1 for all $(k,a) \in \mathrm{J}(A_1)$. Thus, $1+5k \in \{1,-1\}$ and $k=0$. This shows that $\mathrm{J}(A_1) \subseteq \{0\}\times A$. On the other hand, take any $(0,a) \in \{0\}\times A$. We have that the element

$$(1,0)+(k,b)(0,a) = (1, ka+b\cdot a),$$

is invertible for every $(k,b) \in A_1$. Hence, $(0,a) \in \mathrm{J}(A_1)$ for all $a \in A$. □

Let A be any ring. Define on A the binary operation $\circ\colon A\times A \to A$ by setting

$$a\circ b = a+b+a\cdot b \tag{1.15}$$

for all $a,b \in A$. In general, the pair $(A,\circ)$ is a monoid, but in the case where A is a radical ring, as an immediate consequence of the previous lemma, we have the following result.

Corollary 1.3.11. *A is a radical ring if and only if $(A,\circ)$ is a group.*

Example 1.3.12. Let p be a prime number and let $A = \mathbb{Z}/p^2\mathbb{Z}$. The couple $(A,+)$, endowed with the multiplication $a\cdot b = pab$ for all $a,b \in A$, is a radical ring.

The next theorem was first proved by W. Rump in [42] and it shows that a radical ring always defines an involutive solution of the YBE. The proof can be deduced as a consequence of Theorem 1.3.6.

Theorem 1.3.13. *Let A be a radical ring. Then (A,r) is an involutive solution of the YBE, where*

$$r(x,y) = (-x+x\circ y, (-x+x\circ y)'\circ x\circ y). \tag{1.16}$$

1.4 Foundations of Skew Braces and Their Role in the YBE

In order to find a generalization of Theorem 1.3.13, in this section we introduce the structure of a skew brace. In particular, we show that an involutive solution to the Yang–Baxter Equation can be constructed starting from an arbitrary skew brace.

Definition 1.4.1. A skew left brace is a triple $(A, +, \circ)$ where $(A, +)$ and $(A, \circ)$ are groups (not necessarily abelian) and for all $a, b, c \in A$ the following equality holds

$$a \circ (b + c) = (a \circ b) - a + (a \circ c). \tag{1.17}$$

We highlight that, although it is denoted additively, the group $(A, +)$ is not necessarily abelian. We shall denote the identity of the group $(A, +)$ by 0 and we shall denote the inverse of an element $a \in (A, +)$ by $-a$. The inverse element of $a \in (A, \circ)$ will be denoted by a'.

Remark 1.4.2. A skew right brace satisfies the equality

$$(a + b) \circ c = (a \circ c) - c + (b \circ c) \tag{1.18}$$

for all $a, b, c \in A$. There exists a bijective correspondence between skew left braces and skew right braces. When we talk about skew braces we refer to skew left braces, unless otherwise specified.

Definition 1.4.3. A skew brace $(B, +, \circ)$ is a bi-skew brace if $(B, \circ, +)$ is also a skew brace.

Let χ be a family of groups. A skew brace B is said to be of χ-type if its additive group belong to χ. The skew braces of abelian type are skew braces with abelian additive group. We shall call a bi-skew brace of abelian type simply a bi-brace.

Example 1.4.4 (First examples of skew-braces). Let $(A, +)$ be a group.

1. A is a skew brace with $a \circ b := a + b$ for all $a, b \in A$. This skew brace is called *trivial* brace. Similarly if $a \circ b := b + a$, then $(A, +, \circ)$ is a skew brace. This skew brace is called the *almost trivial* brace.

2. Let A, B be skew braces. The triple $(A \times B, +, \circ)$ defined via

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &\coloneqq (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1) \circ (a_2, b_2) &\coloneqq (a_1 \circ a_2, b_1 \circ b_2)\end{aligned} \tag{1.19}$$

is a skew braces (the direct product of A and B).

3. Let $(A, +)$ and $(G, +)$ be groups and let $\alpha \colon A \to \mathrm{Aut}(G)$ be a group homomorphism. The triple $(G \times A, +, \circ)$ with

$$\begin{aligned}(g, a) + (h, b) &\coloneqq (g + h, a + b) \\ (g, a) \circ (h, b) &\coloneqq (g + \alpha_a(h), a + b)\end{aligned} \tag{1.20}$$

is a skew brace.

4. Let $(A, +)$ be a group with an exact factorization through the subgroups B and C, i.e. for all $a \in A$ there exist unique $a_B \in B$ and $a_C \in C$ such that $a = a_B + a_C$. The triple $(A, +, \circ)$ such that for all $a, b \in A$

$$a \circ b = a_B + b + a_C \tag{1.21}$$

is a skew brace. Notice that $(A, \circ)$ is a group isomorphic to $B \times C$. This provides an example of skew brace $(A, +, \circ)$ such that $(A, +) \cong (A, \circ)$ and which is not necessary trivial.

Lemma 1.4.5. *Let B be a skew brace.*

1. *If 1 denotes the identity of $(B, \circ)$, then $1 = 0$.*
2. *For all $a, b \in B$ we have that $-(a \circ b) = -a + a \circ (-b) - a$.*

Proof. 1. We have that

$$0 = 0 + 0 = 1 \circ (0 + 0) = 1 \circ 0 - 1 + 1 \circ 0 = 0 - 1 + 0 = -1.$$

2. It suffices to note that

$$a = a \circ 0 = a \circ (b - b) = a \circ b - a + a \circ (-b). \qquad \square$$

Proposition 1.4.6. *Let B be a skew brace. For each $a \in B$ the map $\lambda_a \colon B \to B$ sending $b \mapsto -a + a \circ b$ is an automorphism of $(B, +)$. Moreover*

$$\begin{aligned} \lambda \colon (B, \circ) &\to \mathrm{Aut}(B, +) \\ a &\mapsto \lambda_a \end{aligned} \tag{1.22}$$

is a group homomorphism.

Proof. The map λ_a is an endomorphism of $(B, +)$. Indeed we have that

$$\lambda_a(b + c) = -a + a \circ (b + c) = -a + a \circ b - a + a \circ c = \lambda_a(b) + \lambda_a(c),$$

By definition $\lambda_0(a) = -0 + 0 \circ a = a$, and so $\lambda_0 = \mathrm{id}$. Moreover, using Lemma 1.4.5 we get that

$$\begin{aligned} \lambda_a\lambda_b(c) &= -a + a \circ (-b + b \circ c) \\ &= -a + a \circ (-b) - a + a \circ (b \circ c) \\ &= (-a \circ b) + a \circ (b \circ c) \\ &= -(a \circ b) + (a \circ b) \circ c = \lambda_{a \circ b}(c) \end{aligned}$$

Finally, the map λ_a is bijective and ${\lambda_a}^{-1} = \lambda_{a'}$. □

We get the following characterization of skew left braces.

Proposition 1.4.7. *Let B be a set endowed with two operation $+$ and $\circ$ such that $(B, +)$ and $(B, \circ)$ are groups. Let $\lambda \colon B \to \mathrm{Sym}(B)$, $a \mapsto \lambda_a$, given by $\lambda_a(b) = -a + a \circ b$. The following data are equivalent:*

1. *B is a skew left braces.*
2. *$\lambda_a\lambda_b(c) = \lambda_{a \circ b}(c)$ for all $a, b, c \in B$.*
3. *$\lambda_a(b + c) = \lambda_a(b) + \lambda_a(c)$ for all $a, b, c \in B$*

Proof. By Proposition 1.4.6 it remains to prove that (3) $\implies$ (2).

$$\begin{aligned} \lambda_a\lambda_b(c) = \lambda_a(-b + b \circ c) &= \lambda_a(-b) + \lambda_a(b \circ c) \\ &= -a + a \circ (-b) - a + a \circ (b \circ c) = -(a \circ b) + (a \circ b) \circ c = \lambda_{a \circ b}(c). \end{aligned}$$

Notice that the last equality follows by $0 = \lambda_a(b + (-b)) = \lambda_a(b) + \lambda_a(-b)$, i.e. $-(a \circ b) = a \circ (-b)$. □

Proposition 1.4.8. *Let B be a skew brace. For each $a \in B$, the map $\rho_b \colon B \to B$, sending $a \mapsto (\lambda_a(b))' \circ a \circ b$, is bijective. Moreover*

$$\begin{aligned} \rho \colon (B, \circ) &\to \mathrm{Sym}(B) \\ b &\mapsto \rho_b \end{aligned} \tag{1.23}$$

is an anti-homomorphism (i.e. $\rho_c \rho_b = \rho_{b \circ c}$).

Proof. We first note that $\lambda_a(b) = a \circ (a' + b)$, indeed $a \circ (a' + b) = a \circ a' - a + a \circ b = 0 - a + a \circ b = \lambda_a(b)$. Hence, we obtain

$$\begin{aligned} \rho_b(a) &= (\lambda_a(b)') \circ a \circ b \\ &= (a \circ (a' + b))' \circ a \circ b \\ &= (a' + b)' \circ a' \circ a \circ b \\ &= (a' + b)' \circ b. \end{aligned}$$

It follows that $\rho_0(a) = (a' + 0)' \circ 0 = a$, and so $\rho_0 = \mathrm{id}$. Finally, it is easy to verify that $\rho_c \rho_b = \rho_{b \circ c}$ and that $\rho_b^{-1} = \rho_{b'}$. □

Theorem 1.4.9. *[31, 42] Let B be a skew brace. The couple (B, r) is a bijective solution of the YBE, with*

$$r(x, y) = (-x + x \circ y, (-x + x \circ y)' \circ x \circ y). \tag{1.24}$$

Proof. It is a direct consequence of Proposition 1.4.6, Proposition 1.4.8 and Theorem 1.3.6. □

By Remark 1.3.8, if $r = (\lambda_x(y), \rho_y(x))$ is involutive, then $\rho_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$. As a consequence, we get the following.

Corollary 1.4.10. *(B, r) is involutive if and only if $(B, +)$ is abelian.*

1.5 Basic Concepts in the Theory of Skew Braces

We now set aside the study of solutions to the Yang–Baxter Equation and turn our attention to the study of skew braces. We provide some definitions and prove several properties that will be useful in Chapter 4 of this work.

Definition 1.5.1. Let B be a skew brace.

- A *sub-brace* of B is a subset C of B such that $(C,+) \leq (B,+)$ and $(C,\circ) \leq (B,\circ)$.
- A *left ideal* of B is a subgroup $(I,+)$ of $(B,+)$ which is λ- invariant.
- A *strong left ideal* of B is a left ideal I of B such that $(I,+) \trianglelefteq (B,+)$.

Remark 1.5.2. A left ideal I of B is clearly a sub-brace of B. Indeed, if $\lambda_b(I) \subseteq I$ for all $b \in B$, then $(I,\circ) \leq (B,\circ)$. If B is a skew brace of abelian type, then the definitions of left ideal and strong left ideal coincide.

Definition 1.5.3. An ideal of B is a strong left ideal I of B such that $(I,\circ) \trianglelefteq (B,\circ)$.

Thus, an ideal I of B is a normal subgroup of $(B,\circ)$ and a normal subgroup of $(B,+)$ which is λ-invariant.

Example 1.5.4. We construct an example of left ideal which is not an ideal. First we need to introduce the notion of semidirect product of skew braces.

Let A and B be two skew braces and consider the semidirect product $A \rtimes_\alpha B$ defined as follows. Let $\alpha\colon (B,\circ) \to \mathrm{Aut}(A,+,\circ)$ be a homomorphism of groups and define two operation on the direct product $A \times B$. For all $a,b \in A$ and $x,y \in B$ we set

$$(a,x) + (b,y) := (a+b, x+y)$$
$$(a,x) \circ (b,y) := (a \circ \alpha_x(b), x \circ y).$$

The semidirect product of A and B via α is the skew brace $A \rtimes_\alpha B := (A \times B, +, \circ)$. For a more general construction of semidirect product of skew braces see also e.g. [29].

As an application consider $B = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ be the semidirect product of the trivial braces $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ via the non-trivial action of $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}/3\mathbb{Z}$. Then, the set

$$\mathrm{Fix}(B) = \{b \in B \mid \lambda_x(b) = b \text{ for all } x \in B\}$$

is a left ideal of B that is not an ideal of B. Indeed, $\mathrm{Fix}(B)$ is equal to $\{(0,0),(0,1)\}$ which is not a normal subgroup of $(B,\circ)$.

Definition 1.5.5. Let A and B be two skew left braces. A *homomorphism* between A and B is a map $f\colon A \to B$ such that $f(a+b) = f(a)+f(b)$ and $f(a\circ b) = f(a)\circ f(b)$ for all $a, b \in A$.

Let $f\colon (A,+,\circ) \to (B,+,\diamond)$ be a homomorphism of skew braces. Notice that $\ker(f) = \{a \in A \mid f(a) = 0\}$ is a normal subgroup of both $(A,+)$ and $(A,\circ)$. Moreover, if $a \in A$ and $b \in \ker(f)$ we have that

$$f(\lambda_a(b)) = f(-a + a \circ b) = -f(a) + f(a) \diamond f(b) = -f(a) + f(a) = 0.$$

Thus, $\ker(f)$ is an ideal of $(A,+,\circ)$.

Definition 1.5.6. Let B be a skew brace. We define *socle* of B as the subset $\mathrm{Soc}(B) = \ker(\lambda) \cap Z(B,+)$.

Lemma 1.5.7. *Let B be a skew brace. Then, $\lambda_a(x) \in \mathrm{Soc}(B)$ for all $a \in B$ and for all $x \in \mathrm{Soc}(B)$.*

Proof. Notice that for all $x \in \mathrm{Soc}(B)$, we have that $\lambda_a(x) = a \circ x - a = a \circ x \circ a'$. Indeed

$$\lambda_a(x) = -a + (a \circ x) = a \circ (a' + x) = a \circ (x + a') = a \circ x - a.$$

and $a \circ x - a = a \circ (x + a') = a \circ (x \circ a') = a \circ x \circ a'$. The result now follows by showing that $\lambda_a(x) + b = b + \lambda_a(x)$ and that $\lambda_{\lambda_a(x)} = \mathrm{id}$. □

Remark 1.5.8. The socle of B is an ideal of B, and $x \in \mathrm{Soc}(B)$ if and only if $x \circ b = x + b$ and $x + b = b + x$ for all $b \in B$.

The following definition gives us another example of an ideal of a skew brace.

Definition 1.5.9. Let B be a skew brace. The subset $\mathrm{Ann}(B) = \mathrm{Soc}(B) \cap \mathrm{Fix}(B)$ is called the annihilator of B.

Definition 1.5.10. A skew left brace B is said to be a skew two-sided brace if, for all $a, b, c \in B$,

$$(a + b) \circ c = a \circ c - c + b \circ c. \tag{1.25}$$

Thus, a skew two-sided brace is a skew left and skew right brace.

Remark 1.5.11. Any skew brace with an abelian multiplicative group is two-sided.

Proposition 1.5.12. *A skew brace of abelian type $(B, +, \circ)$ is two sided if and only if $(B, +, \cdot)$ is a radical ring.*

Proof. Since $(B, \circ)$ is a group and $(B, +)$ is an abelian group, the only thing left to prove is that $(B, +, \cdot)$ is a ring. In particular, it remains to show the associativity and distributivity properties. Using Lemma 1.4.5, it is straightforward to verify that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ and the distributivity laws. Conversely, let $(B, +, \cdot)$ be a radical ring and define $a \circ b = a + a \cdot b + b$. Since $(B, +, \cdot)$ is a radical ring, we have that $(B, \circ)$ is a group and $(B, +)$ is an abelian group. Finally, we have

$$\begin{aligned} a \circ (b + c) &= a \cdot (b + c) + a + b + c \\ &= a \cdot b + a \cdot c + a + b + c \\ &= a \circ b - a + a \circ c \end{aligned}$$

and

$$\begin{aligned} (a + b) \circ c &= a + b + (a + b) \cdot c + c \\ &= a + b + c + a \cdot c + b \cdot c \\ &= a \circ c - c + b \circ c. \end{aligned}$$

□

1.6 Skew Braces and Regular Subgroups of the Holomorph

In this section, we prove that there is a bijective correspondence between the class of skew braces with additive group $(B, +)$ and the set of all regular subgroups of $\mathrm{Hol}(B)$.

Let $(B, +)$ be a group. The operation $\circ$ which turns $(B, +, \circ)$ into a skew brace can be characterized as

$$a \circ b = a + \gamma_a(b) \tag{1.26}$$

where $\gamma \colon B \to \mathrm{Aut}(B, +)$ is a function, satisfying

$$\gamma_{a+\lambda_a(b)} = \gamma_a \gamma_b. \tag{1.27}$$

We shall refer to such functions as *gamma functions*. The map λ_a defined in Proposition 1.4.6 is the gamma function of the skew brace B.

We denote by $\mathrm{Hol}(B) \coloneqq B \rtimes \mathrm{Aut}(B)$ the holomorph of B. Notice that every subgroup G of $\mathrm{Hol}(B)$ acts on B. More in particular, let $(a, \alpha) \in G$ and $b \in B$, and consider π_1 the projection onto B, we have that

$$(a, \alpha) \cdot b = \pi_1((a, \alpha)(b, \mathrm{id})) = \pi_1((a + \alpha(b), \alpha)) = a + \alpha(b).$$

We shall say that $G \leq \mathrm{Hol}(B)$ is regular if it acts regularly on B, i.e. given $a, b \in B$ there exists a unique $(c, \gamma) \in G$ such that $b = (c, \gamma) \cdot a = c + \gamma(a)$.

Lemma 1.6.1. *A subgroup G of $\mathrm{Hol}(B)$ is regular if and only if there exists a gamma function $\gamma \colon B \to \mathrm{Aut}(B)$ and $G = \{(a, \gamma_a) \mid a \in B\}$.*

Proof. By regularity of G, we can index the elements of G by way of the elements of B. Hence we can express G as $G = \{(a, \gamma_a) \mid a \in B\}$. Let $b \in B$ and (c, γ_c) the unique element of G such that $(c, \gamma_c) \cdot 0 = b$. Since $\gamma_c(0) = 0$ and $b = (c, \gamma_c) \cdot 0 = c + \gamma_c(0)$, we get that $c = b$. We define the map $\gamma \colon B \to \mathrm{Aut}(B)$ by sending $b \mapsto \gamma_b$. Notice that

$$(a, \gamma_a)(b, \gamma_b) = (a + \gamma_a(b), \gamma_a\gamma_b),$$

which gives $\gamma_a\gamma_b = \gamma_{a+\gamma_a(b)}$.

Conversely, let $G = \{(a, \gamma_a) \mid a \in B\}$ and $\gamma_a\gamma_b = \gamma_a\gamma_{a+\gamma_a(b)}$. Let $(a, \gamma_a) \in G$ and let $(a', \gamma_{a'}) \in G$ be the inverse element of (a, γ_a). We have that

$$\begin{cases} a + \gamma_a(a') = 0 = a' + \gamma_{a'}(a) \\ \gamma_a\gamma_{a'} = \gamma_{a'}\gamma_a = \mathrm{id}\,. \end{cases} \tag{1.28}$$

Let $c, d \in B$. We claim that $(d + \gamma_d(c'), \gamma_{d+\gamma_d(c')}) \cdot c = d$. Indeed, by Equation (1.28), we obtain that

$$\begin{aligned} (d + \gamma_d(c'), \gamma_{d+\gamma_d(c')}) \cdot c &= (d, \gamma_d)(c', \gamma_{c'}) \cdot c \\ &= (d, \gamma_d)((c', \gamma_{c'}) \cdot c) \\ &= (d, \gamma_d) \cdot (c' + \gamma_{c'}(c)) \\ &= (d, \gamma_d) \cdot 0 = d. \end{aligned}$$

Notice that the uniqueness of $(d+\gamma_d(c'), \gamma_{d+\gamma_d(c')})$ follows from the uniqueness of the inverse of an element in a group. □

The following theorem, first proved by D. Bachiller in [12], provides a bijective correspondence between the class $\mathcal{B}$ of skew braces with additive group $(B,+)$ and the set $\mathcal{R}$ of all regular subgroups of $\mathrm{Hol}(B)$.

Theorem 1.6.2. *Let $(B,+)$ be a group. If $B^\circ = (B,+,\circ)$ belongs to $\mathcal{B}$, then $G_{B^\circ} = \{(a,\lambda_a) \mid a \in B\}$ is in $\mathcal{R}$. The map*

$$\begin{aligned} f\colon \mathcal{B} &\to \mathcal{R} \\ B^\circ &\mapsto G_{B^\circ} \end{aligned}$$

is a bijection, and isomorphism classes of skew braces correspond to conjugacy classes of regular subgroups of $\mathrm{Hol}(B)$ *under the action of* $\mathrm{Aut}(B)$.

Proof. We recall that the map $\lambda_a\colon B \to B$ which sends $b \mapsto -a + a \circ b$ is an automorphism of the group $(B,+)$. We define the map

$$\begin{aligned} \psi\colon (B,\circ) &\to G_{B^\circ} \\ a &\mapsto (a,\lambda_a) \end{aligned}$$

Applying Proposition 1.4.7, we have that

$$\psi(a)\psi(b) = (a,\lambda_a)(b,\lambda_b) = (a+\lambda_a(b), \lambda_a\lambda_b) = (a\circ b, \lambda_{a\circ b}) = \psi(a\circ b),$$

hence ψ is an isomorphism. It follows that G_{B° is a group and, since $\lambda_a\lambda_b = \lambda_{a\circ b} = \lambda_{a+\lambda_a(b)}$, by Lemma 1.6.1 it is a regular subgroup of $\mathrm{Hol}(B)$.

Let G be a regular subgroup of $\mathrm{Hol}(B)$. By Lemma 1.6.1, there exists a map $\gamma\colon B \to \mathrm{Aut}(B)$ such that $G = \{(a,\gamma_a) \mid a \in B\}$. We define $a \circ b := a + \gamma_a(b)$ and we claim that $(B,+,\circ)$ is a skew brace. Since the map $G \to (B,\circ)$ defined by $(a,\gamma_a) \mapsto a$ is a isomorphism, $(B,\circ)$ is a group. Moreover, we have that

$$a\circ(b+c) = a + \gamma_a(b+c) = a + \gamma_a(b) + \gamma_a(c) = a\circ b - a + a\circ c$$

proving the first part of the statement.

To prove the last part, let $B^\circ = (B,+,\circ)$ and $B^\diamond = (B,+,\diamond)$ be two isomorphic skew braces, and let g be an isomorphism. Consider the associated groups $G_{B^\circ} =$

$\{(a, \lambda_a) \mid a \in B\}$ and $G_{B^\diamond} = \{(a, \bar{\lambda}_a) \mid a \in B\}$ with $\lambda_a = -a + a \circ b$ and $\bar{\lambda}_a = -a + a \diamond b$. Observe that

$$g\lambda_a g^{-1}(b) = g(-a + a \circ g^{-1}(b)) = -g(a) + g(a) \diamond b = \bar{\lambda}_{g(a)}(b)$$

so that $(0, g)G_{B^\circ}(0, g^{-1}) = G_{B^\diamond}$. The converse is analogous. For a detailed proof see e.g. [12, 31]. □

The following theorem is a consequence of the results proven so far.

Theorem 1.6.3. *Let $(B, +)$ be a group. The following data are equivalent:*

- *a binary operation $\circ$ on B such that $(B, +, \circ)$ forms a skew brace;*
- *a regular subgroup $G \leq \mathrm{Hol}(B)$;*
- *a gamma function $\gamma \colon B \to \mathrm{Aut}(B)$.*

In Chapter 4, we will make extensive use of the above theorem, as well as of the following analogous correspondence established by Caranti in [17].

Theorem 1.6.4. *Let $(B, +)$ be a group. There exists a bijective correspondence between bi-brace structures on $(B, +)$ and the regular subgroups N of $\mathrm{Hol}(B)$ normalized by the right regular representation $\sigma(B)$ of B.*

CHAPTER 2

ITERATED WREATH PRODUCT IN ODD CHARACTERISTIC CASE

This chapter is primarily based on the results presented in [10].

Let $n \geq 2$ and V be a vector space over $\mathbb{F}_p$ of dimension n. Kaloujnine and Krasner in [34] showed that the Sylow p-subgroup W_n of $\mathrm{Sym}(V)$ can be realized as the iterated wreath product of n copies of $\mathbb{Z}/p\mathbb{Z}$ (see Appendix A.3). In other words,

$$W_n := \wr_{i=1}^{n} \mathbb{Z}/p\mathbb{Z} = \mathrm{Fun}(\mathbb{F}_p^{n-1}, \mathbb{F}_p) \rtimes W_{n-1}. \tag{2.1}$$

The pointwise multiplication endows $\mathrm{Fun}(\mathbb{F}_p^{n-1}, \mathbb{F}_p)$ with a group structure. It may be identified with the additive group of the polynomials in $n-1$ variables in which every variable appears with degree at most $p-1$. More precisely, the k-th base subgroup B_k of W_n is defined as

$$B_k := \mathrm{Fun}(\mathbb{F}_p^{k-1}, \mathbb{F}_p) \cong \mathbb{F}_p[x_1, \ldots, x_{k-1}]/(x_1^p - x_1, \ldots, x_{k-1}^p - x_{k-1})$$

and consequently we have the decomposition $W_n = B_n \rtimes \cdots \rtimes B_1$. To avoid ambiguity, since the same polynomial element may belong to different base subgroups, we will denote a polynomial $f \in B_k$ as $f\Delta_k$. As a result of Equation (2.1), every element $w \in W_n$ can be uniquely written as a product of the form $w = f_n\Delta_n \cdots f_1\Delta_1$, where $f_i \in B_i$.

Definition 2.0.1. Let $x = (x_1, \ldots, x_{k-1})$ be a vector of $\mathbb{F}_p^{k-1}$ and consider the integers $1 \leq i < k \leq n$. For each element $h\Delta_i \in B_i$, we define the operator Δ_i by

$$\Delta_i(h)(f(x)\Delta_k) = (f(x + he_i) - f(x))\Delta_k.$$

This operator can be used to express the conjugation action of an element $h\Delta_i \in B_i$ on an element $f\Delta_k \in B_k$ by way of the commutator

$$[f\Delta_k, h\Delta_i] = \Delta_i(h)(f\Delta_k).$$

Since the functions in the base subgroups are polynomials in which every variable appears with degree at most $p-1$, we can use the Taylor formula to write the above commutator as follows

$$[f\Delta_k, h\Delta_i] = \sum_{j=1}^{p-1} \frac{1}{j!} \frac{\partial^j f}{\partial x_i^j} h^j \Delta_k. \tag{2.2}$$

Notice that the element $f\Delta_k \in B_k$ acts on $(x_1, \ldots, x_n) \in V$ via the translation

$$(x_1, \ldots, x_n) \to (x_1, \ldots, x_n) - e_k f(x_1, \ldots, x_{k-1}).$$

Under this notation, the subgroup T can be seen as

$$T = \langle \Delta_1, \ldots, \Delta_n \rangle. \tag{2.3}$$

We will refer to T as the *canonical elementary abelian regular subgroup* of W_n.

2.0.1 Power Monomials and p-degree

To describe the elements of W_n, we introduce notation which makes use of integer partitions. This will also help in understanding the structure of the normalizer chain defined in Equation 1.8. Let $\Lambda = \{\lambda_i\}_{i=1}^{\infty}$ be a sequence of non-negative integers with finite support and weight

$$\mathrm{wt}(\Lambda) := \sum_{i=1}^{\infty} i\lambda_i < \infty. \tag{2.4}$$

We shall say that Λ is a partition of N if $\mathrm{wt}(\Lambda) = N$. The maximal part of Λ is the integer $\max\{i \mid \lambda_i \neq 0\}$. The set of partitions whose maximal part is less than or equal to k is denoted by $\mathcal{P}(k)$ and we define for each $m \geq 1$

$$\mathcal{P}_m(k) = \{\Lambda \in \mathcal{P}(k) \mid \lambda_i \leq m - 1 \text{ for all } i\}.$$

Let $\Lambda \in \mathcal{P}(k)$. We define the *power monomial* x^Λ by

$$x^\Lambda = \prod_{i=1}^{\infty} x_i^{\lambda_i}.$$

Throughout this chapter, unless otherwise stated, we will consider partitions in $\mathcal{P}_p(k)$ for $k = 1, \ldots, n$. The set $\mathcal{B}$ consists of all power monomials in W_n, i.e.

$$\mathcal{B} = \left\{ x^\Lambda \Delta_k \mid \Lambda \in \mathcal{P}_p(k) \text{ and } 1 \leq k \leq n \right\}. \tag{2.5}$$

Definition 2.0.2. We define the *p-degree* of the power monomial $x^\Lambda = x_1^{\lambda_1} \cdots x_{n-1}^{\lambda_{n-1}}$, written $\mathrm{pdeg}(x^\Lambda)$, by

$$\mathrm{pdeg}(x^\Lambda) = \lambda_{n-1}p^{n-2} + \cdots + \lambda_2 p + \lambda_1.$$

Let $1 \leq j \leq n$, and set $\mu_j = p^{n-1} - p^{j-1}$. Then

$$\mathrm{pdeg}(x^\Lambda \Delta_j) = \mathrm{pdeg}(x^\Lambda) + \mu_j. \tag{2.6}$$

Notice that if $\mathrm{pdeg}(x^\Lambda \Delta_k) < \mu_k$, then $x^\Lambda \Delta_k = 1$. For a homogeneous element $f\Delta_k = (c_1 x^{\Lambda_1} + \cdots + c_t x^{\Lambda_t})\Delta_k \in B_k$ we define $\mathrm{pdeg}(f\Delta_k)$ as

$$\max \left\{ \mathrm{pdeg}(x^{\Lambda_i}\Delta_k) \mid i = 1, \ldots, t \right\}.$$

The *leading term* $\mathrm{lt}(f\Delta_k)$ of $f\Delta_k$is the monomial element of the form $c_j x^{\Lambda_j}\Delta_k$ which attains that maximum.

We are now equipped with all the necessary tools to compute the central series of W_n.

2.1 The Lower and the Upper Central Series of W_n

In this section we compute the lower and upper central series of W_n and we give a proof of the equality between the terms of the two series. We begin with a definition that also appears in [3].

Definition 2.1.1. A subgroup $S \leq W_n$ is said to be saturated if

1. $S = S_1 \cdots S_n$, where $S_i \leq B_i$,

2. if $f\Delta_k \in S$, then for each monomial cx^{Λ} of f, with $c \in \mathbb{F}_p^*$, the element $x^{\Lambda}\Delta_k$ is in S.

Notice that a saturated subgroup S of W_n is spanned by the set $S \cap \mathcal{B}$.

Now consider $x^{\Lambda}\Delta_k \in B_k$ and $x^{\Theta}\Delta_\ell \in B_\ell$ with $k > \ell$. the following equalities hold.

$$\operatorname{pdeg}([x^{\Lambda}\Delta_k, x^{\Theta}\Delta_\ell]) = \operatorname{pdeg}\left(\sum_{i=1}^{p-1} \frac{1}{i!}\frac{\partial x^{\Lambda}}{\partial x_\ell} x^{\Theta}\Delta_k\right) = \operatorname{pdeg}\left(\frac{\partial x^{\Lambda}}{\partial x_\ell} x^{\Theta}\Delta_k\right).$$

Thus, if $[x^{\Lambda}\Delta_k, x^{\Theta}\Delta_\ell] \neq 0$, then

$$\operatorname{pdeg}([x^{\Lambda}\Delta_k, x^{\Theta}\Delta_\ell]) < \operatorname{pdeg}(x^{\Lambda}\Delta_k). \tag{2.7}$$

Lemma 2.1.2. *Let $x^{\Lambda}\Delta_k \in B_k$. There exists a monic monomial element $w \in W_n$ such that $[x^{\Lambda}\Delta_k, w]$ lies in B_k and*

$$\operatorname{pdeg}([x^{\Lambda}\Delta_k, w]) = \operatorname{pdeg}(x^{\Lambda}\Delta_k) - 1.$$

Proof. Let $\Lambda = (\lambda_1, \ldots, \lambda_{k-1})$ and $j = \min\{j \mid \lambda_j \neq 0\}$. If $j = 1$, then take $w = \Delta_1$. Indeed, we have that

$$\operatorname{pdeg}([x^{\Lambda}\Delta_k, \Delta_1]) = \operatorname{pdeg}\left(\frac{\partial x^{\Lambda}}{\partial x_1}\Delta_k\right) = \operatorname{pdeg}(x^{\Lambda}\Delta_k) - 1.$$

If $j > 1$, then take $w = x_1^{p-1} \cdots x_{j-1}^{p-1}\Delta_j$. Indeed

$$\begin{aligned}\operatorname{pdeg}([x^{\Lambda}\Delta_k, x_1^{p-1} \cdots x_{j-1}^{p-1}\Delta_j]) &= \operatorname{pdeg}\left(\frac{\partial x^{\Lambda}}{\partial x_j} x_1^{p-1} \cdots x_{j-1}^{p-1}\Delta_k\right) \\ &= (\operatorname{pdeg}(x^{\Lambda}) - p^{j-1}) + (p-1)\sum_{i=0}^{j-2} p^i + \mu_k \\ &= \operatorname{pdeg}(x^{\Lambda}\Delta_k) - 1.\end{aligned}$$

□

Corollary 2.1.3. *If $x^{\Lambda}\Delta_k \in B_k$, then there exist monic monomial elements $w_1, \ldots, w_\ell \in W_n$ such that the commutator $[x^{\Lambda}\Delta_k, w_1, \ldots, w_\ell]$ lies in B_k and*

$$\operatorname{pdeg}([x^{\Lambda}\Delta_k, w_1, \ldots, w_\ell]) = \operatorname{pdeg}(x^{\Lambda}\Delta_k) - \ell \tag{2.8}$$

where $1 \leq \ell \leq \operatorname{pdeg}(x^{\Lambda})$.

As a consequence we have the following result.

Lemma 2.1.4. *Let $i \geq 1$, then $\gamma_i(W_n) \cap B_k = \langle x^\Lambda \Delta_k \mid \mathrm{pdeg}(x^\Lambda \Delta_k) \leq p^{n-1} - i \rangle$.*

Proof. By Equation (2.7) and Corollary 2.1.3, it is enough to notice that

$$\max\{\mathrm{pdeg}(x^\Lambda \Delta_k) \mid x^\Lambda \Delta_k \in \gamma_i(W_n) \cap B_k\} = p^{n-1} - i.$$

That maximum is reached by applying Corollary 2.1.3 to the maximal monic monomial element $x_1^{p-1} \cdots x_{k-1}^{p-1}$ of B_k. Furthermore, by applying Corollary 2.1.3 to a monic monomial in B_k with $\mathrm{pdeg} = s + i$, we obtain an element with $\mathrm{pdeg} = s$ lying in $\gamma_i(W_n) \cap B_k$, for every $s < p^{n-1} - i$. □

Lemma 2.1.5. *Let A be an abelian subgroup of G and $B \trianglelefteq G$ such that*

1. *$AB = A \ltimes B$ is normal in G,*
2. *there exists $H \leq G$ such that $H \leq N_G(A)$ and $G = H(AB)$.*

Then $[AB, G] = ([A, G] \cap A)[B, G]$.

Proof. Let $g = h\bar{a}\bar{b} \in G$ with $h \in H$, $\bar{a} \in A$, $\bar{b} \in B$ and $ab \in AB$. Note that the commutator

$$[ab, g] = [a, g][a, g, b][b, g] \in [a, g][B, G].$$

Moreover, since A is abelian we have

$$[g, a] = [h, a][h, a, \bar{b}][\bar{b}, a] \in ([G, A] \cap A)[B, G]$$

Hence $[ab, g] \in ([G, A] \cap A)[B, G]$, so $[AB, G] \leq ([G, A] \cap A)[B, G]$. Since the opposite inclusion is trivial we have the claim. □

Corollary 2.1.6. *In the same hypotheses of the previous lemma the following equality holds*

$$[AB, \underbrace{G, \ldots, G}_{k \text{ times}}] = ([A, \underbrace{G, \ldots, G}_{k \text{ times}}] \cap A)[B, \underbrace{G, \ldots, G}_{k \text{ times}}]$$

The following is another straight consequence

Corollary 2.1.7. $\gamma_i(W_n) = (\gamma_i(W_n) \cap B_n) \rtimes \cdots \rtimes (\gamma_i(W_n) \cap B_1)$.

Notice that the terms of the lower central series of W_n are saturated subgroups and

$$\gamma_i(W_n) = \gamma_{i+1}(W_n) \rtimes \langle cx^{\Lambda}\Delta_k \mid \mathrm{pdeg}(x^{\Lambda}) = p^{n-1} - i,\ 1 \leq k \leq n \text{ and } c \in \mathbb{F}_p \rangle.$$

The remaining part of this section is devoted to proving the following theorem.

Theorem 2.1.8. *The upper and the lower central series of W_n coincide.*

Before providing the proof, we need some preliminary results.

Lemma 2.1.9. $Z_i \cap B_n = \gamma_{p^{n-1}-i}(W_n) \cap B_n = [(Z_{i+1}(W_n) \cap B_n), W_n]$.

Proof. We know that $Z_i(W_n) \cap B_n \geq \gamma_{p^{n-1}-i}(W_n) \cap B_n$. Since B_n is a uniserial W_n-module, for all $i, j \geq 1$ we have the following

1. $\gamma_j(W_n) \cap B_n = [B_n, \underbrace{W_n, \ldots, W_n}_{j-1 \text{ times}}]$;
2. $|(\gamma_{p^{n-1}-i}(W_n) \cap B_n) : (\gamma_{p^{n-1}-i-1}(W_n) \cap B_n)| = p$;
3. $|Z_i(W_n) : Z_{i-1}(W_n)| \geq p$;
4. $Z_{p^{n-1}-1}(W_n) \cap B_n \neq B_n$;
5. $Z_{p^{n-1}}(W_n) \cap B_n = B_n$.

Thus, $p^{n-1} = \prod_{j=1}^{p^{n-1}} |(Z_j(W_n) \cap B_n) : (Z_{j-1}(W_n) \cap B_n)| \geq \prod_{j=1} p = p^{n-1}$ and so $|(Z_j(W_n) \cap B_n) : (Z_{j-1}(W_n) \cap B_n)| = p$ for all j. The statement follows inductively noting that $Z_1(W_n) \cap B_n = \gamma_{p^{n-1}}(W_n) \cap B_n$ □

Lemma 2.1.10. *If $g = g_k \ldots g_n \in Z_i(W_n)$ with $g_s \in B_s$ then $g_k \in Z_i(W_n)$.*

Proof. Let $\psi \colon W_n \to W_k$ be the canonical map whose kernel is $B_{k+1} \cdots B_n$. Note that $\psi(Z_i(W_n)) \leq Z_{i-p^{n-1}+p^{k-1}}(W_k)$. By Lemma 2.1.9 it follows that

$$\psi(g) = g_k \in Z_{i-p^{n-1}+p^{k-1}}(W_k) \cap B_k = \gamma_{p^{n-1}-i}(W_k) \cap B_k = \gamma_{p^{n-1}-i}(W_n) \cap B_k.$$

Thus, $g_k \in \gamma_{p^{n-1}-i}(W_n) \cap B_k \leq Z_i(W_n) \cap B_k$. □

Corollary 2.1.11. *If $g = g_1 \ldots g_n \in Z_i(W_n)$ with $g_s \in B_s$ then $g_s \in Z_i(W_n)$ for all s. In particular*

$$Z_i(W_n) = (Z_i(W_n) \cap B_1) \cdots (Z_i(W_n) \cap B_n).$$

Proof of Theorem 2.1.8. Notice that

$$(Z_i(W_n) \cap B_1) \cdots (Z_i(W_n) \cap B_n) = (\gamma_{p^{n-1}-i}(W_n) \cap B_1) \cdots (\gamma_{p^{n-1}-i}(W_n) \cap B_n).$$

Indeed, by Lemma 2.1.9, we have that $(Z_i(W_n) \cap B_n) = \gamma_{p^{n-1}-i}(W_n) \cap B_n$ and the claim follows easily by arguing induction considering the quotient $W_{n-1} = W_n/B_n$.

Finally, by Corollaries 2.1.7 and 2.1.11, we have

$$\begin{aligned} Z_i(W_n) &= (Z_i(W_n) \cap B_1) \cdots (Z_i(W_n) \cap B_n) \\ &= (\gamma_{p^{n-1}-i}(W_n) \cap B_1) \cdots (\gamma_{p^{n-1}-i}(W_n) \cap B_n) = \gamma_{p^{n-1}-i}(W_n). \quad \square \end{aligned}$$

2.2 The Lie Algebra associated to W_n

In this section, we introduce the Lie algebra $\mathfrak{L}_n$ associated to the group W_n, and we define a map between these structures.

We start by noting that each base subgroup B_i is a uniserial module for W_n. Hence, by Corollary 2.1.7 the quotient of two consecutive terms of the lower central series is an elementary abelian p-group for a prime p. This implies that the graded Lie ring $\mathfrak{L}_n$ associated with the lower central series of W_n inherits the structure of a Lie algebra over $\mathbb{F}_p$. As shown in [46], this Lie algebra may be described as the iterated wreath product $\mathfrak{L}_n = \wr^n \mathfrak{L}_1$, where $\mathfrak{L}_1$ is the one dimensional algebra over $\mathbb{F}_p$.

Let ∂_k be the derivation given by the standard partial derivative with respect to the variable x_k, with $1 \leq k \leq n$. We identify $\mathfrak{L}_n$ as the subalgebra of the Witt algebra (see Appendix A.4) over $\mathbb{F}_p$ in n variables spanned by the basis

$$\mathfrak{B} = \bigcup_{k=1}^{n} \mathfrak{B}_k \text{ where } \mathfrak{B}_k = \left\{ x^{\Lambda}\partial_k \mid \Lambda \in \mathcal{P}_p(k-1) \right\}.$$

The product of $\mathfrak{L}_n$ is defined on the basis $\mathfrak{B}$ as follows

$$\begin{aligned} \left[x^{\Lambda}\partial_k, x^{\Theta}\partial_j\right] := \quad & \partial_j(x^{\Lambda})x^{\Theta}\partial_k - x^{\Lambda}\partial_k(x^{\Theta})\partial_j \\ = \quad & \begin{cases} \partial_j(x^{\Lambda})x^{\Theta}\partial_k & \text{if } j < k, \\ -x^{\Lambda}\partial_k(x^{\Theta})\partial_j & \text{if } j > k, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

This operation is then extended by bilinearity to the whole $\mathfrak{L}_n$.

The lower central series of W_n allows us to establish a connection between the Lie algebra $\mathfrak{L}_n$ and the group W_n. In particular, let $cx^{\Lambda}\Delta_k \in W_n$ with $c \in \mathbb{F}_p$. We define

$$\varphi_i(cx^{\Lambda}\Delta_k) = \begin{cases} cx^{\Lambda}\partial_k & \text{if } x^{\Lambda}\Delta_k \in \gamma_i(W_n) \setminus \gamma_{i+1}(W_n) \\ 0 & \text{otherwise} \end{cases}$$

Notice that $\varphi_i(x^{\Lambda}\Delta_k) \neq 0$ if and only if $\operatorname{pdeg}(x^{\Lambda}\Delta_k) = p^{n-1} - i$. Let $f\Delta_k$ be a homogeneous element of $\gamma_i(W_n)$, we define $\varphi_i(f\Delta_k) \coloneqq \varphi_i(\operatorname{lt}(f\Delta_k))$. Given a generic element $g = g_1 \dots g_n \in W_n$, we set

$$\varphi_i(g) = \begin{cases} \sum_{j=1}^{n} \varphi_i(\operatorname{lt}(g_j)) & \text{if } g \in \gamma_i(W_n) \setminus \gamma_{i+1}(W_n), \\ 0 & \text{otherwise.} \end{cases}$$

This defines a map $\varphi\colon W_n \to \mathfrak{L}_n$ by setting $\varphi(g) = \varphi_i(g)$ whenever $g \in \gamma_i(W_n) \setminus \gamma_{i+1}(W_n)$.

We now introduce the concept of homogeneous subring of $\mathfrak{L}_n$ which, as we will see later, is related to Definition 2.1.1 of saturated subgroup.

Definition 2.2.1. A Lie subring $\mathfrak{h}$ of $\mathfrak{L}_n$ is said to be homogeneous if it is the span over $\mathbb{F}_p$ of some subset $\mathfrak{H}$ of $\mathfrak{B}$.

Remark 2.2.2. Let $\mathfrak{L}_i$ be the $\mathbb{F}_p$-span of $\mathfrak{B}_i$, and define $\mathfrak{L}(i) = \bigoplus_{j=1}^{i} \mathfrak{L}_j$. Consider the $\mathbb{F}_m$-submodule $\mathfrak{T}$ of $\mathfrak{L}$, generated by the set $\{\partial_1, \dots, \partial_n\}$. This submodule forms a homogeneous and abelian Lie subring. Moreover, for each i, the element ∂_i generates the center of $\mathfrak{L}(i)$. The subring $\mathfrak{T}$ provides a natural counterpart to the elementary abelian regular subgroup of W_n.

Definition 2.2.3. If $\mathfrak{U}$ is a subset of $\mathfrak{B}$, then its idealizer is defined as

$$\mathfrak{N}_{\mathfrak{B}}(\mathfrak{U}) = \{b \in \mathfrak{B} \mid [b, u] \in \mathbb{F}_p\,\mathfrak{U} \text{ for all } h \in \mathfrak{U}\}.$$

Theorem 2.2.4. *Let $\mathfrak{H}$ be a homogeneous subring of $\mathfrak{L}_n$ having basis $\mathfrak{U} \subseteq \mathfrak{B}$. The idealizer $\mathfrak{N}_{\mathfrak{L}_n}(\mathfrak{H})$ of $\mathfrak{H}$ in $\mathfrak{L}_n$ is the homogeneous subring of $\mathfrak{L}_n$ spanned over $\mathbb{F}_p$ by $\mathfrak{N}_{\mathfrak{B}}(\mathfrak{U})$.*

Proof. Let $\mathfrak{N} = N_{\mathfrak{L}_n}(\mathfrak{H})$ be the idealizer of $\mathfrak{H}$ in $\mathfrak{L}_n$ and let

$$z = \sum_{x^\Lambda \partial_k \in \mathcal{B}} l_{\Lambda,k} x^\Lambda \partial_k$$

be an element of $\mathfrak{N}$. We aim to show that each term in this sum belongs to $\mathfrak{N}$. Notice that, since $\mathfrak{H}$ is a homogeneous subring, it suffices to show that $\left[l_{\Lambda,k} x^\Lambda \partial_k, x^\Theta \partial_j\right] \in \mathbb{F}_p \mathcal{H}$ for all $x^\Theta \partial_j \in \mathcal{H}$. We know that

$$\mathfrak{H} \ni [z, x^\Theta \partial_j] = \sum_{x^\Lambda \partial_k \in \mathcal{B}} l_{\Lambda,k} [x^\Lambda \partial_k, x^\Theta \partial_j],$$

where the sum is taken over all $x^\Lambda \partial_k \in \mathfrak{B}$ such that $\left[x^\Lambda \partial_k, x^\Theta \partial_j\right] \neq 0$. Observe that for $x^{\Lambda_1} \partial_{k_1} \neq x^{\Lambda_2} \partial_{k_2}$, the commutators

$$[x^{\Lambda_1} \partial_{k_1}, x^\Theta \partial_j] \neq [x^{\Lambda_2} \partial_{k_2}, x^\Theta \partial_j]$$

and so each non-zero bracket $[x^\Lambda \partial_k, x^\Theta \partial_j]$ is an element of $\mathbb{F}_p \mathcal{H}$. □

2.2.1 Lower and Upper Central Series of $\mathfrak{L}_n$

Thanks to the map $\varphi\colon W_n \to \mathfrak{L}_n$, we can easily compute the central series of $\mathfrak{L}_n$. The terms of these series provide further examples of homogeneous subrings.

First, observe that if $[x^\Lambda \partial_j, x^\Theta \partial_k] = c x^\Gamma \partial_u$, for some $c \in \mathbb{F}_p$, then

$$u = \max(j,k) \text{ and } \operatorname{wt}(\Gamma) = \operatorname{wt}(\Lambda) + \operatorname{wt}(\Theta) - \min(j,k).$$

This formula will be used implicitly in the results that follow.

Lemma 2.2.5. *Let $x^\Lambda \Delta_k \in \gamma_i(W_n) \setminus \gamma_{i+1}(W_n)$ and $x^\Theta \Delta_h \in \gamma_j(W_n) \setminus \gamma_{j+1}(W_n)$. If the commutator $[x^\Lambda \Delta_k, x^\Theta \Delta_h]$ is not trivial, then it lies in $\gamma_{i+j}(W_n) \setminus \gamma_{i+j+1}(W_n)$, and the following equality holds*

$$\varphi_{i+j}([x^\Lambda \Delta_k, x^\Theta \Delta_h]) = [\varphi_i(x^\Lambda \Delta_k), \varphi_j(x^\Theta \Delta_h)]. \tag{2.9}$$

Proof. Without loss of generality we can assume $k > h$, $\varphi_i(x^\Lambda \Delta_k) \neq 0 \neq \varphi_j(x^\Theta \Delta_h)$ and $\dfrac{\partial x^\Lambda}{\partial x_h} \neq 0$. Since

$$\operatorname{pdeg}([x^\Lambda \Delta_k, x^\Theta \Delta_h]) = \operatorname{pdeg}\left(\frac{\partial x^\Lambda}{\partial x_h} x^\Theta \Delta_k\right) = p^{n-1} - i - j,$$

we have that

$$\begin{aligned}\varphi_{i+j}([x^{\Lambda}\Delta_k, x^{\Theta}\Delta_h]) &= \varphi_{i+j}\left(\frac{\partial x^{\Lambda}}{\partial x_h}x^{\Theta}\Delta_k\right)\\ &= \frac{\partial x^{\Lambda}}{\partial x_h}x^{\Theta}\partial_k\\ &= [x^{\Lambda}\partial_k, x^{\Theta}\partial_h]\\ &= [\varphi_i(x^{\Lambda}\Delta_k), \varphi_j(x^{\Theta}\Delta_h)].\end{aligned}$$

□

Let S be a saturated subgroup of W_n. We shall denote by S^{φ} the homogeneous Lie subring of $\mathfrak{L}_n$ spanned by the set $\varphi(S \cap \mathcal{B})$.

Remark 2.2.6. A straightforward consequence of the previous lemma is that if S is a saturated subgroup of W_n, then $|S| = |S^{\varphi}|$.

Corollary 2.2.7. *For each $i \geq 1$ we have $\gamma_i(W_n)^{\varphi} = \mathfrak{L}_n^i$ is the i-th Lie power of $\mathfrak{L}_n$.*

We now compute the upper central series of $\mathfrak{L}_n$.

Definition 2.2.8. Let $1 \leq j \leq n$. We define ξ_m as the $\mathbb{F}_p$-span of the set

$$\left\{x^{\Lambda_n}\partial_n, \ldots, x^{\Lambda_1}\partial_1 \mid \operatorname{pdeg}(x^{\Lambda_i}\partial_i) < m \text{ for all } i = 1, \ldots, n\right\}.$$

Notice that, by Lemma 2.1.4, $\xi_m = \gamma_{p^{n-1}-m}(W_n)^{\varphi}$, and so $\xi_m \subseteq \xi_{m+1}$.

Lemma 2.2.9. *For each $x^{\Theta}\partial_\ell \in \mathfrak{L}_n$ and $x^{\Lambda}\partial_i \in \xi_m$ the commutator $[x^{\Lambda}\partial_i, x^{\Theta}\partial_\ell]$ belongs to ξ_{m-1}.*

Proof. Without loss of generality, we may assume $x^{\Lambda}\partial_i \neq 0 \neq x^{\Theta}\partial_\ell$. For $\ell < i$, the claim is easily verified noting that

$$\operatorname{pdeg}\left(\frac{\partial x^{\Lambda}}{\partial x_\ell}x^{\Theta}\partial_i\right) \leq \operatorname{pdeg}(x^{\Lambda}\partial_i) - 1 < m - 1.$$

If $\ell > i$, we have that $[x^{\Theta}\partial_\ell, x^{\Lambda}\partial_i] = \dfrac{\partial x^{\Theta}}{\partial x_i}x^{\Lambda}\partial_\ell$. We observe that, since $x^{\Lambda}\partial_i \neq 0$, we must have $m > \mu_i$. Hence

$$\operatorname{pdeg}\left(\frac{\partial x^{\Theta}}{\partial x_i}x^{\Lambda}\partial_\ell\right) \leq p^{n-1} - 1 - p^{i-1} = \mu_i - 1 < m - 1.$$

Thus, $x^{\Lambda}\partial_i \in \xi_{m-1}$. □

Lemma 2.2.10. *Let $x^{\Lambda}\partial_i$ be such that $\operatorname{pdeg}(x^{\Lambda}\partial_i) = r+\mu_i$. Then for each $k+1 < r$ there exists $x^{\Theta}\partial_\ell \in \mathfrak{L}_n$ such that $\operatorname{pdeg}([x^{\Theta}\partial_\ell, x^{\Lambda}\partial_i]) > k + \mu_i$.*

Proof. Let $r = \lambda_1 + \lambda_2 p + \cdots + \lambda_{i-1}p^{i-2}$ and $k+1 = \gamma_1 + \gamma_2 p + \cdots + \gamma_{i-1}p^{i-2}$. Let j be the maximum index such that $\lambda_j > \gamma_j$. If $\lambda_j - \gamma_j > 1$, then

$$\operatorname{pdeg}([x^{\Lambda}\partial_i, \partial_j]) > k + \mu_i.$$

If $\lambda_j - \gamma_j = 1$ and there exists $s < j$ such that $\lambda_s \neq 0$, then $\operatorname{pdeg}([x^{\Lambda}\partial_i, \partial_s]) > k+\mu_i$. If such s does not exist and $j \neq 1$, then $\operatorname{pdeg}([x^{\Lambda}\partial_i, x_1^{p-1}\dots x_{j-1}^{p-1}\partial_j]) = r-1+\mu_i > k+\mu_i$. If $j = 1$, then $\operatorname{pdeg}([x^{\Lambda}\partial_i, \partial_1]) = r - 1 + \mu_i > k + \mu_i$. □

Corollary 2.2.11. *For all $i = 1, \dots, n$ the following equalities hold*

$$\xi_m \cap \mathfrak{B}_i = \mathfrak{Z}_m(\mathfrak{L}_n) \cap \mathfrak{B}_i = \mathfrak{L}_n^{p^{n-1}-m} \cap \mathfrak{B}_i.$$

In particular, $\mathfrak{Z}_m(\mathfrak{L}_n) = \mathfrak{L}_n^{p^{n-1}-m}$.

2.3 A Chain of Normalizers

We now have all the necessary tools to return to the original goal we set at the beginning: to compute the chain of normalizers originating from the subgroup T of W_n, and defined in Equation (1.8). We recall that Theorem 1.2.4 shows that the normalizers can be computed inside W_n rather than inside $\operatorname{Sym}(V)$. For the reader's convenience, we restate the definition of the normalizer chain.

Let $T = \langle \Delta_1, \dots, \Delta_n \rangle$ be the canonical elementary abelian regular subgroup of W_n, and define the sequence $\{\mathbf{N}_i^{(p)}\}_{i \geq -1}$ as follows.

$$\mathbf{N}_i^{(p)} = \begin{cases} T & \text{if } i = -1 \\ N_{W_n}(\mathbf{N}_{i-1}^{(p)}) & \text{if } i \geq 0. \end{cases} \tag{2.10}$$

In this section, we prove that the growth of that normalizer chain coincides with the growth of the corresponding chain of idealizers in $\mathfrak{L}_n$ originating from the subring $\mathfrak{T}$ defined in Remark 2.2.2.

Proposition 2.3.1. *Let $S \leq W_n$ be a saturated subgroup. The normalizer $N_{W_n}(S)$ of S in W_n is a saturated subgroup.*

Proof. Let $g = hg_k \in N_{W_n}(S)$ with $g_k \in B_k \setminus \{1\}$ and $h \in B_{k+1} \cdots B_n$. Since S is saturated, we have that the condition $g \in N_{W_n}(S)$ is equivalent to requiring that $[g, s] \in S$ for every $s \in B_i \cap S$ and all $i \in \{1, \ldots, n\}$. Notice that, in order to prove that $N_{W_n}(S)$ is saturated, it is enough to show that $g_k \in N_{W_n}(S)$. Indeed, since $g_k \in N_{W_n}(S)$, we obtain $h = gg_k^{-1} \in N_{W_n}(S)$ and we can then argue by induction on k. Let $s \in B_i \cap S$, we have

$$S \ni [g, s] = [h, s]^{g_k}[g_k, s].$$

If $k = i$, then $[g_k, s] = 1$ and we are done.

Without loss of generality, we can suppose $[g_k, s] \neq 1$. If $k > i$, then $[h, s]^{g_k} \in B_{k+1} \cdots B_n$ and $[g_k, s] \in B_k$. In particular, since S is saturated, we get $[g_k, s] \in S$.

If $k < i$, write $h = \hat{h}\bar{h}$ with $\bar{h} \in B_{k+1} \cdots B_{i-1}$ and $\hat{h} \in B_i \cdots B_n$. Then

$$S \ni [g, s] = [\hat{h}\bar{h}g_k, s] = [\hat{h}, s]^{\bar{h}g_k}[\bar{h}g_k, s].$$

Here, $[\bar{h}g_k, s] \in B_i$ and $[\hat{h}, s]^{\bar{h}g_k} \in B_{i+1} \cdots B_n$, so $[\bar{h}g_k, s] \in B_i \cap S$. Now decompose $\bar{h} = h_{i-1} \cdots h_{k+1}$ with $h_j \in B_j$. Then

$$S \ni [\bar{h}g_k, s] = [h_{i-1}, s]^{h_{i-2} \cdots h_{k+1} g_k} \cdots [h_{k+1}, s]^{g_k}[g_k, s]. \tag{2.11}$$

Note that in each monomial term of $[g_k, s]$ the variable x_j appears with the same degree as in s. In contrast, in each monomial element of $[h_j, s]^{h_{j-1} \cdots h_{k+1} g_k}$, the degree of x_j is strictly less than in s. This means that the monomial elements coming from $[g_k, s]$ are distinct from those coming from the other commutators $[h_j, s]^{h_{j-1} \cdots h_{k+1} g_k}$ for $j = k+1, \ldots i-1$. Thus, since S is saturated, and the whole product $[h_{i-1}, s]^{h_{i-2} \cdots h_{k+1} g_k} \cdots [h_{k+1}, s]^{g_k}[g_k, s]$ lies in S, each monomial element coming from the decomposition of $[g_k, s]$ must lie in S, proving the statement. □

The following result is a technical lemma aiming to intertwine idealizers and normalizers.

Lemma 2.3.2. *Let H be a saturated subgroup of W_n and let $n \in B_\ell$. If $\mathrm{lt}([n, h]) \in H$ for all $h \in H$, then $[n, h] \in H$.*

Proof. Since H is a saturated subgroup, without loss of generality, we may assume that $h = g\Delta_i \in B_i$ for some i, and $n = f\Delta_\ell$. If $\ell > i$, then

$$[n,h] = \sum_{s=1}^{p-1} \frac{1}{s!} \frac{\partial^s f}{\partial x_i^s} g^s \Delta_\ell$$

and $\mathrm{lt}([n,h]) = \dfrac{\partial f}{\partial x_i} g\Delta_\ell \in H$. The statement follows noting that $[\mathrm{lt}([n,h]),h] \in H$ so that $\dfrac{\partial^s f}{\partial x_i^s} g^s \Delta_\ell \in H$ for $s = 2, \dots, p-1$. If $\ell < i$, then

$$[n,h] = \sum_{s=1}^{\infty} \frac{1}{s!} \frac{\partial^s g}{\partial x_\ell^s} f^s \Delta_i$$

and $\mathrm{lt}([n,h]) = \dfrac{\partial g}{\partial x_\ell} f\Delta_i \in H$. By hypothesis, $\mathrm{lt}([n,\mathrm{lt}([n,h])]) = \dfrac{\partial^2 g}{\partial x_\ell^2} f^2 \Delta_i \in H$. Iterating the process we obtain the desired result. □

Proposition 2.3.3. *Let H be a saturated subgroup of W_n. The following equality holds*

$$(N_{W_n}(H))^\varphi = \mathfrak{N}_{\mathfrak{L}_n}(H^\varphi).$$

Proof. By Proposition 2.3.1 we know that $N_{W_n}(H)$ is a saturated subgroup of W_n. Let $n \in N_{W_n}(H) \cap \mathcal{B}$ and i an integer such that $n \in \gamma_i(W_n) \setminus \gamma_{i+1}(W_n)$. For every $h \in H \cap \mathcal{B}$, there exists an integer j such that $h \in \gamma_j(W_n) \setminus \gamma_{j+1}(W_n)$ and we have the following equality by Lemma 2.2.5

$$\varphi([n,h]) = \varphi_{i+j}([n,h]) = [\varphi_i(n), \varphi_j(h)].$$

Since $\varphi([n,h]) \in H^\varphi$ for all $h \in H \cap \mathcal{B}$, it follows that $\varphi_i(n) = \varphi(n) \in \mathfrak{N}_{\mathfrak{L}_n}(H^\varphi)$.

We now prove the opposite inclusion. Let $t \in \mathfrak{N}_{\mathfrak{L}_n}(H^\varphi) \cap \mathfrak{B}$. For some positive integer i, there exists $n \in \mathcal{B} \cap (\gamma_i(W_n) \setminus \gamma_{i+1}(W_n))$ such that $\varphi(n) = t$. For all $\varphi(h) \in H^\varphi \cap \mathfrak{B}$, there exists an integer j such that $\varphi(h) = \varphi_j(h)$ and

$$H^\varphi \ni [\varphi_i(n), \varphi_j(h)] = \varphi_{i+j}([n,h] = \varphi(\mathrm{lt}([n,h]))).$$

Thus, $\mathrm{lt}([n,h]) \in H$ for all $h \in H$ and, by Lemma 2.3.2, we have $[n,h] \in H$. □

Remark 2.3.4. By Proposition 2.3.3, we obtain that the correspondence sending H to H^φ maps normal saturated subgroups of W_n into homogeneous ideals of $\mathfrak{L}_n$.

Moreover, we define a new map $\varepsilon\colon \mathfrak{B} \to \mathcal{B}$ by $x^{\Lambda}\partial_k \mapsto x^{\Lambda}\Delta_k$. If $\mathfrak{I}$ is an homogeneous ideal of $\mathfrak{L}_n$, we denote by $\mathfrak{I}^{\varepsilon}$ the saturated subgroup of W_n generated by $\varepsilon(\mathfrak{I} \cap \mathfrak{B})$. As

$$\varphi[\varepsilon(x^{\Lambda}\partial_k), \varepsilon(x^{\Theta}\partial_h)] = [\varphi\varepsilon(x^{\Lambda}\partial_k), \varphi\varepsilon(x^{\Theta}\partial_h)] = [x^{\Lambda}\partial_k, x^{\Theta}\partial_h],$$

it follows that $\mathfrak{I}^{\varepsilon}$ is a normal saturated subgroup of W_n such that $(\mathfrak{I}^{\varepsilon})^{\varphi} = \mathfrak{I}$. Similarly, if N is a saturated normal subgroup of W_n, then $(N^{\varphi})^{\varepsilon} = N$. This shows that the maps $(\cdot)^{\varphi}$ and $(\cdot)^{\varepsilon}$ establish a bijection between the poset of normal saturated subgroups of W_n and the poset of homogeneous ideals of $\mathfrak{L}_n$.

By Remark 2.2.6 and Proposition 2.3.3 we have that

$$|\mathfrak{N}_{\mathfrak{L}_n}(H^{\varphi})| = |N_{W_n}(H)|. \tag{2.12}$$

Thus, the growth of the normalizer chain defined in Equation (2.10) is equal to the growth of the following idealizer chain originating from $\mathfrak{T}$.

$$\mathfrak{N}_i^{(p)} = \begin{cases} \mathfrak{T} & \text{if } i = -1 \\ \mathfrak{N}_{\mathfrak{L}_n}(\mathfrak{N}_{j-1}^{(p)}) & \text{if } i \geq 0 \end{cases} \tag{2.13}$$

where $\mathfrak{T}$ is the homogeneous subring of $\mathfrak{L}_n$ spanned by the set $\{\partial_1, \ldots, \partial_n\}$.

2.3.1 The Idealizer Chain

The idealizer chain defined in Equation (2.13) has already been studied in [2]. In this subsection, we recall the results obtained in [2] in order to enhance the clarity of the exposition. First, we introduce the following subsets of $\mathfrak{B}$. Let $\mathcal{U} = \mathcal{T} \cup \{x_j\partial_k \mid 1 \leq j < k \leq n\}$ and for $1 \leq i \leq n-1$, define

$$\mathcal{W}_i = \left\{ x^{\Lambda}\partial_k \in \mathfrak{B} \mid n-i+1 \leq k \leq n \text{ and } \operatorname{wt}(\Lambda) = k+i-n+1 \right\}. \tag{2.14}$$

Theorem 2.3.5. *The Lie subring $\mathfrak{N}_i^{(p)}$ is homogeneous and it is the $\mathbb{F}_p$-linear span of $\mathcal{N}_i^{(p)}$ which is recursively defined by*

$$\mathcal{N}_i^{(p)} = \begin{cases} \mathcal{T} & \textit{if } i = -1 \\ \mathcal{U} & \textit{if } i = 0 \\ \mathcal{N}_{i-1}^{(p)} \dot{\cup}\, \mathcal{W}_i & \textit{otherwise.} \end{cases} \tag{2.15}$$

Remark 2.3.6. Note that, by Equation (2.15) for $1 \leq i \leq n-1$

$$\mathcal{N}_{n-i}^{(p)} = \left\{ x^{\Lambda}\partial_k \in \mathcal{B} \mid \mathrm{wt}(\Lambda) \leq k - i + 1 \right\} \cup \mathcal{U}. \tag{2.16}$$

Lemma 2.3.7. *The set $\mathcal{N}_0^{(p)}$ is equal to $N_{\mathcal{B}}(\mathcal{T})$.*

Proof. We first show that $\mathcal{U} \subseteq \mathfrak{N}_{\mathfrak{B}}(\mathcal{T})$. The fact that $\mathcal{T} \subseteq \mathfrak{N}_{\mathfrak{B}}(\mathcal{T})$ is trivial. Moreover, for all $x_i\partial_j \in \mathcal{U}$ with $i < j$, the bracket $[x_i\partial_j, \partial_k]$ is an element of $\mathbb{F}_p\mathcal{T}$, since

$$[x_i\partial_j, \partial_k] = \begin{cases} \partial_j & k = i, \\ 0 & k \neq i. \end{cases}$$

Conversely, let $x^{\Lambda}\partial_j \in \mathfrak{N}_{\mathfrak{B}}(\mathcal{T})$. For $1 \leq k \leq n$,

$$\mathbb{F}_p\mathcal{T} \ni [x^{\Lambda}\partial_j, \partial_k] = \begin{cases} 0 & \text{for } k \geq j \\ \partial_k(x^{\Lambda})\partial_j & \text{for } k < j. \end{cases}$$

It follows that $\Lambda = 0$ or $x^{\Lambda} = x_k$ for some $1 \leq k \leq n$, concluding the proof. □

Lemma 2.3.8. *If $1 \leq i \leq n-1$, then $[\mathcal{U}, \mathcal{W}_i] \subseteq \mathbb{F}_p\mathcal{N}_{i-1}^{(p)}$.*

Proof. Let $x^{\Lambda}\partial_j \in \mathcal{W}_i$ and $x^{\Theta}\partial_k \in \mathcal{U}$. We set $cx^{\Gamma}\partial_u = [x^{\Lambda}\partial_j, x^{\Theta}\partial_k]$, for some $c \in \mathbb{F}_p$. In the case $x^{\Theta}\partial_k = \partial_k \in \mathcal{T}$, then either $c = 0$ or

$$\mathrm{wt}(\Gamma) = \mathrm{wt}(\Lambda) - k.$$

Since $\mathrm{wt}(\Lambda) = j + i - n + 1$ and $k \geq 1$, it follows that $\mathrm{wt}(\Gamma) \leq j - n + i$.

Now consider $x^{\Theta}\partial_k = x_h\partial_k \in \mathcal{U} \setminus \mathcal{T}$. If $k \leq j$, then

$$\begin{aligned} \mathrm{wt}(\Gamma) = \mathrm{wt}(\Lambda) + h - k &\leq \mathrm{wt}(x^{\Lambda}) + (k-1) - k \\ &= j + i - n. \end{aligned}$$

If $k > j$, then

$$\begin{aligned} \mathrm{wt}(\Gamma) = \mathrm{wt}(\Lambda) + h - j &= j + (j + i - n + 1) - j \\ &\leq k + i - n. \end{aligned}$$

In both cases the resulting monomial $x^{\Gamma}\partial_u$ satisfies the condition to lie in $\mathcal{N}_{i-1}^{(p)}$. □

Lemma 2.3.9. *If $1 \leq i < h \leq n-1$, then $[\mathcal{W}_i, \mathcal{W}_h] \subseteq \mathbb{F}_p \mathcal{N}_{h-1}^{(p)}$.*

Proof. Let us consider $x^\Lambda \partial_j \in \mathcal{W}_i$, $x^\Theta \partial_k \in \mathcal{W}_h$ and their bracket $[x^\Lambda \partial_j, x^\Theta \partial_k] = cx^\Gamma \partial_u$ with $c \neq 0$. Notice that if $x^\Gamma \partial_u \in \mathcal{U}$, there is nothing to prove. Otherwise, by the definitions of $\mathcal{W}_i$ and of $\mathcal{W}_h$, we know that $\mathrm{wt}(\Lambda) = j + i - (n-1)$ and $\mathrm{wt}(\Theta) = k + h - (n-1)$. Thus,

$$\begin{aligned}
\mathrm{wt}(\Gamma) &= \mathrm{wt}(\Lambda) + \mathrm{wt}(\Theta) - \min(j,k) \\
&= j + i - (n-1) + k + h - (n-1) - \min(j,k) \\
&= (j + k - \min(j,k)) + i + h - 2n + 2 \\
&= u + h - n + (i - n + 2) \\
&\leq u + h - n.
\end{aligned}$$

□

Proposition 2.3.10. *If $1 \leq i \leq n-1$, then $\mathcal{N}_i^{(p)} = \mathfrak{N}_{\mathfrak{B}}(\mathcal{N}_{i-1}^{(p)})$.*

Proof. By the previous lemmas, it remains to prove the inclusion $\mathfrak{N}_{\mathfrak{B}}(\mathcal{N}_{i-1}^{(p)}) \subseteq \mathcal{N}_i^{(p)}$. Let $x^\Lambda \partial_j \in \mathfrak{N}_{\mathfrak{B}}(\mathcal{N}_{i-1}^{(p)})$. By definition for each $x^\Theta \partial_k \in \mathfrak{B}$ we have that $[x^\Lambda \partial_j, x^\Theta \partial_k] \in \mathcal{N}_{i-1}^{(p)}$. Let $k < j$ be the minimum index such that $\lambda_k \neq 0$, and consider $x^\Theta \partial_k = x_{k-1} \partial_k$. By construction $[x^\Lambda \partial_j, x_{k-1} \partial_k] = cx^\Gamma \partial_j \neq 0$ for some nonzero $c \in \mathbb{F}_p$ and $x^\Gamma \partial_j \in \mathcal{N}_{i-1}^{(p)}$. It follows that

$$\mathrm{wt}(\Lambda) = \mathrm{wt}(\Gamma) + 1 \leq j + i - n + 1,$$

and so $x^\Lambda \partial_j \in \mathcal{N}_i^{(p)}$. □

It is now clear that Theorem 2.3.5 is a direct consequence of Theorem 2.2.4, Lemma 2.3.7, and Proposition 2.3.10.

2.3.2 Connections with Integer Partitions

Let $t_{p,i}$ be the number of partitions of i into at least two parts, where each part can be repeated at most $p-1$ times, and let $q_{p,i}$ be the partial sum

$$q_{p,i} = \sum_{j=1}^{i} t_{p,j}.$$

By Theorem 2.3.5 we get the following result.

Theorem 2.3.11. *Let $1 \leq i \leq n-1$ and $p > 2$ a prime integer. Then, for $n-i+1 \leq k \leq n$ we have $|\,\mathcal{W}_i \cap \mathfrak{B}_k\,| = t_{p,k+1+i-n}$ and therefore the $\mathbb{F}_p$-vector space $\mathfrak{N}_i^{(p)}/\mathfrak{N}_{i-1}^{(p)}$ has dimension $q_{p,i+1}$.*

By way of Equation (2.12), the previous theorem can be immediately restated in the group case as follows.

Theorem 2.3.12. *Let $1 \leq i \leq n-1$, then $|\mathbf{N}_i^{(p)}/\mathbf{N}_{i-1}^{(p)}| = p^{q_{p,i+1}}$.*

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	OEIS
$t_{3,i}$	0	1	1	3	4	6	8	12	15	21	26	35	43	56	A000726
$q_{3,i}$	0	1	2	5	9	15	23	35	50	71	97	132	175	231	
$t_{5,i}$	0	1	2	4	5	9	12	18	24	33	43	59	75	99	A035959
$q_{5,i}$	0	1	3	7	12	21	33	51	75	108	151	210	285	384	
$t_{7,i}$	0	1	2	4	6	10	13	20	27	38	50	69	89	118	No ref.
$q_{7,i}$	0	1	3	7	13	23	36	56	83	121	171	240	329	447	

Table 2.1. First values of the sequences $(t_{p,i})$ and $(q_{p,i})$ for $p = 3, 5, 7$.

Remark 2.3.13. In the case $p = 2$, Aragona et al. [2] prove that for every $1 \leq i \leq n-2$, the $\mathbb{F}_2$-vector space

$$\mathfrak{N}_i^{(2)}/\mathfrak{N}_{i-1}^{(2)}$$

has dimension $q_{2,i+2}$.

2.4 Normal Subgroups of W_n

To conclude the work on iterated wreath product in odd characteristic, we study the normal subgroups of W_n. We show that if a normal subgroup $N \trianglelefteq W_n$ is contained in the last $n-k$ base subgroups of W_n, then it contains a term of the lower central series with an index bounded only by k and p.

Lemma 2.4.1. *Let N be a normal subgroup of W_n and $f\Delta_k \in N$. Every monomial element $x^\Lambda\Delta_k$ of p-degree at most $\mathrm{pdeg}(f\Delta_k)$ belongs to N.*

Proof. We argue by induction on the p-degree of $f\Delta_k$. The base of the induction is when f is constant of minimum possible p-degree μ_k. In this case, the claim is trivial. Otherwise $t = \mathrm{pdeg}(f\Delta_k) \geq \mu_k$. By Lemma 2.1.2 applied to the leading term $x^\Lambda\Delta_k$ of $f\Delta_k$, there exists an element in N of p-degree equal to $t-1$. By induction, $N \cap B_k$ contains every monomial element of p-degree at most $t-1$. In particular, $f\Delta_k - x^\Lambda\Delta_k$ lies in N and so also $x^\Lambda\Delta_k \in N$, proving the statement. □

Lemma 2.4.2. *If $N \trianglelefteq W_n$, then $(N \cap B_k)(N \cap B_{k+1}) \cdots (N \cap B_n) \trianglelefteq W_n$ for all $1 \leq k \leq n$.*

Proof. Since the elements in N of the form $f\Delta_h$, where $h \geq k$, generate $(N \cap B_k)(N \cap B_{k+1}) \cdots (N \cap B_n)$, it suffices to note that the commutator $[f\Delta_h, x^\Lambda\Delta_s]$ belongs to $N \cap B_\ell$ for each generator $x^\Lambda\Delta_s$ of W_n, where $\ell = \max(s,h)$. □

Lemma 2.4.3. *Let N be the normal closure of $\langle f\Delta_k \rangle$. Then*

$$N = (N \cap B_k)(N \cap B_{k+1}) \cdots (N \cap B_n).$$

Proof. On the one hand, note that $N \geq (N \cap B_k)(N \cap B_{k+1}) \cdots (N \cap B_n)$. On the other hand, by Lemma 2.4.2, $(N \cap B_k)(N \cap B_{k+1}) \cdots (N \cap B_n)$ is a normal subgroup of W_n containing $f\Delta_k$, hence it contains its normal closure N. Thus we have the equality. □

Lemma 2.4.4. *If $1 \neq x^\Lambda\Delta_k \in \gamma_t(W_n) \setminus \gamma_{t+1}(W_n)$, then*

$$[\langle x^\Lambda\Delta_k \rangle, W_n] = \big(\gamma_{t+1}(W_n) \cap B_k\big)\big(\gamma_{p^{k-1}+1}(W_n) \cap (B_{k+1} \cdots B_n)\big).$$

Proof. The inclusion $[\langle x^\Lambda\Delta_k \rangle, W_n] \leq \big(\gamma_{t+1}(W_n) \cap B_k\big)\big(\gamma_{p^{k-1}+1}(W_n) \cap (B_{k-1} \cdots B_n)\big)$ is trivial. In order to prove the opposite inclusion, consider the monomial element $x^\Theta\Delta_h \in \big(\gamma_{t+1}(W_n) \cap B_k\big)\big(\gamma_{p^{k-1}+1}(W_n) \cap (B_{k-1} \cdots B_n)\big)$. Let us first analyze the case $h = k$. We know that $\mathrm{pdeg}(x^\Lambda\Delta_k) = \mathrm{pdeg}(x^\Lambda) + \mu_k = p^{n-1} - t$ and $\mathrm{pdeg}(x^\Theta\Delta_k) = \mathrm{pdeg}(x^\Theta) + \mu_k \leq p^{n-1} - t - 1 = \mathrm{pdeg}(x^\Lambda\Delta_k) - 1$. By Lemma 2.4.1, $\gamma_{t+1}(W_n) \cap B_k \leq [\langle x^\Lambda\Delta_k \rangle, W_n]$.

If $h > k$ it suffices to consider the commutator

$$[x^{\Lambda}\Delta_k, x_1^{p-1-\lambda_1}\cdots x_{h-1}^{p-1-\lambda_{h-1}}\Delta_h]$$

which has pdeg equal to $\mu_k - 1$, and apply Lemma 2.4.1 as above. □

Proposition 2.4.5. *The normal closure of the subgroup of W_n generated by $x^{\Lambda}\Delta_k$ is*

$$\langle x^{\Lambda}\Delta_k\rangle[\langle x^{\Lambda}\Delta_k\rangle, W_n] = \langle x^{\Lambda}\Delta_k\rangle\big(\gamma_{t+1}(W_n)\cap B_k\big)\big(\gamma_{p^{k-1}+1}(W_n)\cap(B_{k+1}\cdots B_n)\big),$$

where $t = \mathrm{pdeg}(x^{\Lambda}\Delta_k)$.

Proof. Since by Lemmas 2.4.2 and 2.4.4, the subgroup $[\langle x^{\Lambda}\Delta_k\rangle, W_n]$ is normal in W_n, the claim follows. □

The proposition above together with Lemma 2.4.1 give the following results.

Corollary 2.4.6. *The normal closure of the subgroup of W_n generated by $f\Delta_k$ is the saturated subgroup*

$$\langle f\Delta_k\rangle[\langle f\Delta_k\rangle, W_n] = \langle f\Delta_k\rangle\big(\gamma_{t+1}(W_n)\cap B_k\big)\big(\gamma_{p^{k-1}+1}(W_n)\cap(B_{k+1}\cdots B_n)\big),$$

where $t = \mathrm{pdeg}(f\Delta_k)$.

Proposition 2.4.7. *Let $g = f\Delta_k\cdot h$, with $h \in B_{k+1}\cdots B_n$. The normal closure $\langle g\rangle^{W_n}$ contains $\gamma_{p^{k-1}+1}(W_n)$.*

Proof. If $h = 1$ the statement follows by Corollary 2.4.6. If $h \neq 1$, let $x^{\Lambda}\Delta_k$ be the leading term of $f\Delta_k$. Observe that $[x_1^{p-1-\lambda_1}\dots x_{n-1}^{p-1-\lambda_{n-1}}\Delta_n, g]$ has p-degree $p^{n-1}-p^{k-1}-1$, and so we can apply Lemma 2.4.1 to get $\gamma_{p^{k-1}+1}(W_n)\cap B_n \leq \langle g\rangle^{W_n}$. Next, the commutator $[x_1^{p-1-\lambda_1}\cdots x_{n-2}^{p-1-\lambda_{n-2}}\Delta_{n-1}, g] = s\Delta_n q\Delta_{n-1}$ is such that

$$\mathrm{pdeg}(s\Delta_n) \leq \mathrm{pdeg}([x_1^{p-1-\lambda_1}\cdots x_{n-2}^{p-1-\lambda_{n-2}}\Delta_{n-1}, x_1^{p-1}\dots x_{n-1}^{p-1}\Delta_n]) \leq p^{n-1}-p^{k-1}-1.$$

It follows that $s\Delta_n \in \langle g\rangle^{W_n}$ by the argument above. In particular, $q\Delta_{n-1}\in\langle g\rangle^{W_n}$ and has p-degree equal to $p^{n-2}-p^{k-1}-1$. Thus, by Lemma 2.4.1, $\gamma_{p^{k-1}+1}(W_n)\cap B_{n-1}\leq\langle g\rangle^{W_n}$. The rest of the proof is obtained by iterating this argument inductively. □

A straightforward consequence is the following estimate.

Corollary 2.4.8. *If $N \trianglelefteq W_n$ is a normal subgroup such that $N \subseteq (B_k \cdots B_n) \setminus (B_{k+1} \cdots B_n)$, then N contains $\gamma_{p^{k-1}+1}(W_n)$ and*

$$|N : \gamma_{p^{k-1}+1}(W_n)| \leq \left(p^{p^{k-1}}\right)^{n-k+1}. \tag{2.17}$$

In particular this index is bounded above by a function depending only on p and k.

Remark 2.4.9. Notice that if $k = n$, then N coincides with a term of the lower central series that depends only on the maximal monomial term appearing in N.

CHAPTER 3

ITERATED WREATH PRODUCT IN ZERO CHARACTERISTIC CASE

This chapter is primarily based on the results presented in [9].

In this chapter, we focus our attention on infinite groups. We construct a group W_n^∞, the analogue of the p-Sylow subgroups of $\mathrm{Sym}(V)$, by means of an iterated wreath product of integral domains of characteristic zero. Within W_n^∞, we identify a counterpart of the elementary abelian regular subgroup T of W_n, and we compute its normalizer chain, following the approach of the previous chapter. In this setting we again obtain interesting connections with certain integer partitions.

We begin with a non-standard definition that restricts the base group of the unrestricted standard wreath product of two groups.

Definition 3.0.1. Let K, H be two groups. If $L \leq K^H$ is an H-invariant subgroup, we define

$$K \wr_L H := L \rtimes H.$$

When $L = K^H$, we obtain the classical notion of unrestricted standard wreath product and, in this case, we will omit the subscript L. The base subgroup of $K \wr_L H$ is defined as usual by $B = \{(f, 1_H) \mid f \in L\} \cong L$.

Let D be an integral domain of characteristic 0 with fraction field F. We shall denote by R_i an additive subgroup of D^{D^i} containing a copy of D seen as the

subring of constant functions. We ask furthermore that D^i acts faithfully on R_i by translations, and that $f(g_0, \dots, g_{i-1}) \in R_i$ whenever $f \in R_i$ and $g_j \in R_j$. We consider the iterated wreath product

$$W_n^\infty = D \wr_{R_{n-1}} D \wr_{R_{n-2}} \cdots \wr_{R_1} D$$

of n copies of D.

Let $f \in R_{k-1}$, we shall denote by $f\Delta_k$ an element in the base group B_k of

$$W_k^\infty = D \wr_{R_{k-1}} W_{k-1}^\infty$$

corresponding to the function f when regarded as an element of B_k. The elements of W_n^∞ are then n-tuples $(f_{n-1}\Delta_n, \dots, f_0\Delta_1)$ with $f_i \in R_i$. It is worth noting that R_0 is an additive subgroup of D.

The group W_n^∞ is a permutation group acting on the set D^n. The action of W_n^∞ on D^n is defined as follows

$$(x_1, x_2, \dots, x_n) \cdot (f_{n-1}\Delta_n, \dots, f_1\Delta_2, f_0\Delta_1) = \\ (x_1 - f_0, x_2 - f_1(x_1), \dots, x_n - f_{n-1}(x_1, \dots, x_{n-1})).$$

Notice that, each base subgroup B_k is endowed with a structure of D-module by setting

$$d \cdot (f\Delta_k) = (df)\Delta_k$$

for all $d \in D$. If $f = \prod_{k=n}^1 f_k\Delta_k$ is a generic element of the group W_n^∞, then $d \cdot \prod_{k=n}^1 f_k\Delta_k = \prod_{k=n}^1 df_k\Delta_k$.

We rewrite the definition of the operator Δ in this new setting, even though it is entirely analogous to Definition 2.0.1.

Definition 3.0.2. Let $x \in D^j$ and let $\{e_1, \dots, e_j\}$ be a basis for D^j. For each $h \in D$, and $i < j$, we define the operator $\Delta_i(h)\colon R_j \to R_j$ by

$$\Delta_i(h)f(x) = f(x + he_i) - f(x).$$

Also in this case, by way of the operator Δ , we can express the commutator

between two elements, $f\Delta_k$ and $h\Delta_i$, in the group W_n^∞ as follows

$$[f\Delta_k, h\Delta_i] = \begin{cases} (\Delta_i(h)f)\Delta_k & \text{if } k > i \\ -(\Delta_k(f)h)\Delta_i & \text{if } i > k \\ 0 & \text{if } k = i \end{cases} \tag{3.1}$$

Moreover, if $k > i$, by Taylor formula, in the case of f being a polynomial function, we have

$$[f\Delta_k, h\Delta_i] = \sum_{s=1}^{\infty} \frac{1}{s!} \frac{\partial^s f}{\partial x_i^s} h^s \Delta_k. \tag{3.2}$$

We refer to the Appendix A.5 for some results on difference equations that will be useful later.

3.0.1 Power Monomials and Transfinite Degree

We refer to Subsection 2.0.1 for the definition of power monomial elements of W_n^∞. As done previously, we denote by $\mathcal{P}(k)$ the set of partitions whose maximal part is less than or equal to k. In this case there will be no further restrictions on the degree of the x_is. Let $\mathcal{B}$ be the set of all power monomial elements of W_n^∞, that is

$$\mathcal{B} = \{x^\Lambda \Delta_k \mid 1 \leq k \leq n,\ \Lambda \in \mathcal{P}(k-1)\}. \tag{3.3}$$

We call monomial elements those elements of the form $dx^\Lambda \Delta_k$, where $d \in D$.

Definition 3.0.3. Let $k \geq 1$ be an integer, $0 \neq d \in D$ and $\Lambda \in \mathcal{P}(k)$, we define the *transfinite degree* of the monomial dx^Λ, written $\mathrm{tdeg}(dx^\Lambda)$, by

$$\mathrm{tdeg}(dx^\Lambda) = \omega^{n-2}\lambda_{n-1} + \cdots + \omega\lambda_2 + \lambda_1.$$

We set

$$\mathrm{tdeg}(dx^\Lambda \Delta_k) = \sum_{i=1}^{n-k} \omega^{n-i} + \mathrm{tdeg}(x^\Lambda)$$

where, for $k = n$, the sum has to be intended empty.

It is easy to see that for every non-limit ordinal α, satisfying $0 \leq \alpha \leq \sum_{i=1}^{n} \omega^{n-i}$, there exists a unique monic monomial element $b_\alpha \in \mathcal{B}$ such that $\mathrm{tdeg}\, b_\alpha = \alpha$. Notice that this definition endows the set $\mathcal{B}$ with a total ordering. In particular, every

polynomial element $f \in W_n^\infty$ can be uniquely decomposed as $f = \prod_\alpha c_\alpha b_\alpha$, where $c_\alpha \in D$ and b_α is the unique monic monomial element with transfinite degree equal to α. We shall denote by $\mathrm{lt}(f)$ the *leading term* of a non-identity element f, i.e. the monomial appearing in f with non-zero coefficient and with maximum transfinite degree, together with its corresponding Δ_* component. We define

$$\mathrm{tdeg}(f) = \begin{cases} \mathrm{tdeg}(\mathrm{lt}(f)) & \text{if } f \neq d \cdot 1, \\ 0 & \text{otherwise.} \end{cases}$$

We shall write $f \prec g$ to mean that $\mathrm{tdeg}(f) < \mathrm{tdeg}(g)$.

Lemma 3.0.4. *Let $x^\Lambda \Delta_k, x^\Theta \Delta_u \in W_n^\infty$ be two monomials such that $k > u$. The following equality holds*

$$\mathrm{lt}\left([x^\Lambda \Delta_k, x^\Theta \Delta_u]\right) = \frac{\partial x^\Lambda}{\partial x_u} x^\Theta \Delta_k.$$

Proof. If $\lambda_u = 0$, then $[x^\Lambda \Delta_k, x^\Theta \Delta_u] = 0$ and there is anything to prove. Otherwise, by Equation (3.2) we have that

$$[x^\Lambda \Delta_k, x^\Theta \Delta_u] = \sum_{s=1}^{\infty} \frac{\partial^s x^\Lambda}{\partial x_u^s} \frac{(x^\Theta)^s}{s!} \Delta_k.$$

It is enough to prove that, for $s \geq 1$, the following inequality holds

$$\frac{\partial^s x^\Lambda}{\partial x_u^s} \frac{(x^\Theta)^s}{s!} \prec \frac{\partial^{s-1} x^\Lambda}{\partial x_u^{s-1}} \frac{(x^\Theta)^{s-1}}{(s-1)!}.$$

We denote by $x^{\bar{\Lambda}}$ the monomial x^Λ with the variable x_u removed and by λ_u the exponent with which x_u appears in the monomial x^Λ. We get

$$\begin{aligned} \frac{\partial^s x^\Lambda}{\partial x_u^s} \frac{(x^\Theta)^s}{s!} &= x^{\bar{\Lambda}} x^{s\Theta} x_u^{\lambda_u - s} \\ &\prec x^{\bar{\Lambda}} x^{(s-1)\Theta} x_u^{\lambda_u - (s-1)} \\ &= \frac{\partial^{s-1} x^\Lambda}{\partial (x_u^{s-1})} \frac{(x^\Theta)^{s-1}}{(s-1)!}. \end{aligned}$$

□

3.1 Transfinite Hypercentral Series of W_n^∞

In this section we aim to give necessary and sufficient conditions on the modules R_i in order to have W_n^∞ transfinite hypercentral (see Appendix A.2 for the definition of transfinite hypercentral groups).

Let $f\colon D^i \to D$, $d = \sum_{j=1}^{i} c_j e_j$, and $d_j = \sum_{s=1}^{j-1} c_s e_s$. We define

$$\Delta(d)(f) \coloneqq f_d - f = \sum_{j=1}^{i} \Delta_j(c_j)(f_{d_j}), \tag{3.4}$$

where $f_c(x) = f(x + c)$.

Definition 3.1.1. For $i \geq 0$, the subring VP_i of virtual polynomials in $\mathrm{Fun}(D^i, D)$ is defined as

$$VP_i = \{f \in \mathrm{Fun}(D^i, D) \mid \exists k \in \mathbb{N} \text{ s.t. } (\Delta(d_1)\cdots\Delta(d_k))(f) = 0 \text{ for all } d_1, \ldots, d_k \in D^i\} \tag{3.5}$$

If k is the minimum non-negative integer such that $(\Delta(d_1)\cdots\Delta(d_k))(f) = 0$ for all $d_1, \ldots, d_k \in D^i$, then $f \in VP_i$ is said to be of class k.

Remark 3.1.2. Let $f \in VP_k$ be of class ℓ. By Lemma A.5.1, if $x, d \in D^k$, then the function $\hat{f}_{x,d}\colon \mathbb{Z} \to D$ defined by

$$\hat{f}_{x,d}(m) = f(x + md)$$

is a polynomial function in m of degree at most $\ell - 1$, with coefficients in F, that is, f behaves like a polynomial along affine integral lines. We will use the same notation $\hat{f}_{x,d}$ to denote the natural extension of this function to a map $\hat{f}_{x,d}\colon \mathbb{Q} \to F$. In particular, $\hat{f}_{x,d}$ is a polynomial function with coefficients in F such that $\hat{f}_{x,d}(\mathbb{Z}) \subseteq D$.

In general, we denote by P_k the subring of $F[x_1, \ldots, x_k]$ consisting of those polynomials $f \in F[x_1, \ldots, x_k]$ such that

$$f(d_1, \ldots, d_k) \in D \quad \text{for all } (d_1, \ldots, d_k) \in D^k.$$

This ring is also known as the *ring of numerical polynomials* in k variables. Moreover, $P_k \subseteq VP_k$, and in the special case $D = \mathbb{Z}$, we have $P_k = VP_k$. We point out that this is not always the case, e.g., if $D = \mathbb{C}$ the function $z \mapsto \mathrm{Re}(z)$, associating to a complex number its real part, is an example of a virtual polynomial of class 2 that belongs to VP_1 but not to P_1.

With the same notation as in Remark 3.1.2 we have the following result.

Lemma 3.1.3. *Let $f \in VP_i$, and suppose $x, d \in D^i$ and $r \in \mathbb{Q}$ are such that $x + rd \in D^i$. Then*

$$f(x + rd) = \hat{f}_{x,d}(r).$$

Proof. Write $r = s/t$, with $s, t \in \mathbb{Z}$, and set $d' = rd$, so that $td' = sd$. Note that $\hat{f}_{x,td'} = \hat{f}_{x,sd}$. We have $f(x + td'm) = \hat{f}_{x,td'}(m) = \hat{f}_{x,d'}(tm)$, and similarly, $f(x + sdm) = \hat{f}_{x,sd}(m) = \hat{f}_{x,d}(sm)$. Thus,

$$f(x + rd) = f(x + d') = \hat{f}_{x,d'}(1) = \hat{f}_{x,td'}(1/t) = \hat{f}_{x,sd}(1/t) = \hat{f}_{x,d}(s/t) = \hat{f}_{x,d}(r). \quad \square$$

It is well known that the F-vector space F^i can be regarded as a $\mathbb{Q}$-vector space. Given vectors $u_1, \ldots, u_k \in F^i$, we denote by $\langle u_1, \ldots, u_k \rangle$ the $\mathbb{Q}$-vector subspace of F^i spanned by $\{u_1, \ldots, u_k\}$.

Lemma 3.1.4. *Let $u_1, \ldots, u_k \in F^i$, and let $x = r_1u_1 + \cdots + r_ku_k \in \langle u_1, \ldots, u_k \rangle \cap D^i$, where $r_1, \ldots, r_k \in \mathbb{Q}$. If $f \in VP_i$ is of class ℓ, then $f(x)$ is a polynomial function in the variables $r_1, \ldots, r_k$, with degree bounded by a function of ℓ.*

Proof. Let $y = r_2u_2 + \cdots + r_ku_k$. By the previous lemma, we have that $f(x) = \hat{f}_{y,u_1}(r_1)$ is a polynomial function in the variable r_1 of the form

$$\hat{f}_{y,u_1}(r_1) = a_0(y) + a_1(y)r_1 + \cdots + a_m(y)r_1^m,$$

where $m \leq \ell - 1$, and each coefficient $a_j(y)$ is independent of r_1.

By induction on k, we may assume that $a_0(y) = f(r_2u_2 + \cdots + r_ku_k) = f(y)$ is a polynomial function in $r_2, \ldots, r_k$, whose degree is bounded by a function of ℓ. It is easy to see that $\Delta_{u_1}^t(f)(x) = \sum_{j=0}^{m-t} b_j(y)r_1^j \in VP_i$, where $b_0(y) = t!\, a_t(y)$. Hence, for $t = 1, \ldots, m$, also $a_t(y)$ is a polynomial function in $r_2, \ldots, r_k$ whose degree is bounded in terms of ℓ, as claimed. $\square$

Remark 3.1.5. Let W be a $\mathbb{Q}$-vector space, and let f be an element of F^W. We say that f is an *fd-polynomial function* if, for every finite-dimensional $\mathbb{Q}$-vector subspace $V = \langle u_1, \ldots, u_k \rangle$ of W, the map

$$\bar{f}\colon \mathbb{Q}^k \to F, \quad \bar{f}(r_1, \ldots, r_k) := f(r_1u_1 + \cdots + r_ku_k)$$

is a polynomial function in the variables $r_1, \ldots, r_k$.

Furthermore, f is called a *uniform fd-polynomial function* if there exists a positive integer t such that $\deg \bar{f} \leq t$, for every such subspace V. In this case, the *total degree* of f is defined to be the maximum, taken over all such subspaces V, of the degrees of the associated polynomials $\bar{f}$.

Corollary 3.1.6. *Let $f \in \mathrm{Fun}(D^i, D)$. Then $f \in VP_i$ and has class at most ℓ if and only if f is the restriction to D^i of a uniform fd-polynomial function $\tilde{f}\colon F^i \to F$ of total degree at most $\ell - 1$.*

Proof. If f has class at most ℓ, then by the previous lemmas, its natural extension $\tilde{f}$ to F^i restricts on every finite-dimensional $\mathbb{Q}$-vector subspace to a polynomial function of degree at most $\ell - 1$. This shows $\tilde{f}$ is a uniform fd-polynomial function of total degree at most $\ell - 1$.

Conversely, if such a uniform fd-polynomial extension $\tilde{f}$ exists, then the finite differences of order ℓ of f vanish on D^i. Hence, $f \in VP_i$ and has class at most ℓ. □

Let $f \in VP_{i-1}$. There exist non-negative integers $k_1, \ldots, k_{i-1}$ such that the ordinal number $\omega^{i-2}k_{i-1} + \cdots + \omega k_2 + k_1$ is minimal, and

$$\left(\prod_{j=1}^{i-1} \Delta_j(c_{j,1}) \cdots \Delta_j(c_{j,k_j})\right)(f) = 0 \quad \text{for all } c_{j,1}, \ldots, c_{j,k_j} \in D.$$

We then define

$$\mathrm{tdeg}(f) = \omega^{i-2}k_{i-1} + \cdots + \omega k_2 + k_1, \tag{3.6}$$

$$\mathrm{tdeg}(f\Delta_i) = \sum_{j=1}^{n-i} \omega^{n-j} + \mathrm{tdeg}(f). \tag{3.7}$$

Whenever $f \in P_{i-1}$, this notion of tdeg agrees with that given in Definition 3.0.3.

Remark 3.1.7. Let $f \in VP_{t-1}$ with $\mathrm{tdeg}(f) = \omega^{t-2}k_{t-1} + \cdots + \omega k_2 + k_1$ and assume $k_j \neq 0$. For any choice of functions $g_i \in VP_{j-1}$, with $i = 1, \ldots, s \leq k_j$, and $j = 1, \ldots, t-1$, by Corollary 3.1.6, the function

$$F = (\Delta_j(g_1) \cdots \Delta_j(g_s))(f)$$

lies in VP_{t-1}, with transfinite degree

$$\mathrm{tdeg}(F) = \omega^{t-2}h_{t-1} + \cdots + \omega h_2 + h_1,$$

for some integers h_i such that $h_i = k_i$ for $i = j+1, \dots, t-1$, and $h_j < k_j$. In particular, if $s = k_j$, then $h_j = 0$ and F does not depend on x_j.

Definition 3.1.8. Let α be a countable ordinal. We define

$$\zeta_\alpha = \{ f\Delta_n \mid f \in VP_{n-1} \text{ and } \operatorname{tdeg}(f\Delta_n) < \alpha \}.$$

Note that if α is a limit ordinal, then $\zeta_\alpha = \bigcup_{\beta<\alpha} \zeta_\beta$.

Lemma 3.1.9. *Let $p \in VP_{\ell-1}$ and $f\Delta_n \in \zeta_\alpha$. Then there exists an ordinal $\beta < \alpha$ such that $[f\Delta_n, p\Delta_\ell] \in \zeta_\beta$.*

Proof. Let $\operatorname{tdeg}(f) = \omega^{n-2}k_{n-1} + \cdots + k_1$. Then the commutator $[f\Delta_n, p\Delta_\ell]$ lies in VP_{n-1} and either vanishes or by Remark 3.1.7 it has transfinite degree strictly less than $\operatorname{tdeg}(f\Delta_n)$. Indeed

$$\begin{aligned} \operatorname{tdeg}\left([f\Delta_n, p\Delta_\ell]\right) &= \operatorname{tdeg}\left(\Delta_\ell(p)(f)\Delta_n\right) \\ &= \omega^{n-2}k_{n-1} + \cdots + \omega^{\ell}k_{\ell+1} + \omega^{\ell-1}h_\ell + \cdots + h_1, \end{aligned}$$

for some integers h_i with $h_\ell < k_\ell$. □

Remark 3.1.10. Since D^i acts faithfully on R_i by translations, a standard argument shows that the center of W_n is given by

$$Z(W_n) = \{ c\Delta_n \mid c \in D \}.$$

Lemma 3.1.11. *If $\alpha < \omega^{n-1}$ is an ordinal, then $Z_\alpha(W_n) \cap B_n \leq \zeta_\alpha$.*

Proof. We argue induction on α, the case $\alpha = 1$ being obvious by the previous remark. Let $f\Delta_n \in Z_\alpha(W_n) \cap B_n$ and $c \in D$. The commutator $[f\Delta_n, c\Delta_\ell] \in Z_\beta(W_n) \cap B_n$ for some ordinal $\beta < \alpha$. By induction $[f\Delta_n, c\Delta_\ell] \in \zeta_\beta$ for every choice of $\ell \leq n$, i.e., $\operatorname{tdeg}(\Delta_\ell(c)(f)) < \beta$ and hence $\operatorname{tdeg}(f\Delta_n) < \beta + 1 \leq \alpha$ as required. □

A direct consequence of the previous lemmas is the following.

Corollary 3.1.12. *Let $\alpha \leq \omega^{n-1}$ be an ordinal. If for every $i = 1, \dots, n-1$, the ring R_i is contained in VP_i, then:*

1. *$[\zeta_{\alpha+1}, W_n] \subseteq \zeta_\alpha$ if α is not a limit ordinal;*

2. $[\zeta_\alpha, W_n] \subseteq \zeta_\alpha$ *if* α *is a limit ordinal.*

In particular, $\zeta_\alpha = Z_\alpha(W_n) \cap B_n$.

Theorem 3.1.13. *The group* W_n *is transfinite hypercentral if and only if* $n = 1$ *or* $R_i \subseteq VP_i$ *for all* $i = 1, \ldots, n-1$.

Proof. We may assume $n \geq 2$, the result being trivial for $n = 1$. First, assume that W_n is transfinite hypercentral. Let $f\Delta_\ell \in Z_\alpha(W_n)$ with $f \in R_{\ell-1}$. We proceed by transfinite induction on α, with the goal of showing that $f \in VP_{\ell-1}$.

If $\alpha = 1$, then by Remark 3.1.10 we must have $\ell = n$ and $f = c$ for some $c \in D$. Thus, $\Delta(d)(f) = 0$ for all $d \in D^{n-1}$.

Now, assume α a countable non-limit ordinal. For every $i = 1, \ldots, \ell - 1$ and every $c \in D$, we have

$$[f\Delta_\ell, c\Delta_i] = \Delta_i(c)(f)\Delta_\ell \in Z_{\alpha-1}(W_n).$$

By the inductive hypothesis, there exists $m \in \mathbb{N}$ such that

$$(\Delta(d_1) \cdots \Delta(d_m)\Delta_i(c_i))(f) = 0$$

for all $d_1, \ldots, d_m \in D^{\ell-1}$ and all $c_i \in D$.

Let $d_{m+1} = \sum_{i=1}^{\ell-1} c_i e_i$. By Equation (3.4) and the translation invariance of $VP_{\ell-1}$, we have

$$(\Delta(d_1) \cdots \Delta(d_m)\Delta(d_{m+1}))(f) = 0$$

for all $d_1, \ldots, d_{m+1} \in D^{\ell-1}$, showing that $f \in VP_{\ell-1}$.

If α is a limit ordinal, observe that $f\Delta_\ell \in \bigcup_{\beta<\alpha} Z_\beta(W_n)$, so there exists a non-limit ordinal $\beta < \alpha$ such that $f\Delta_\ell \in Z_\beta(W_n)$, and the previous argument applies.

Conversely, suppose $R_i \subseteq VP_i$ for all $i = 1, \ldots, n-1$. We proceed by induction on n. The case $n = 1$ is trivial. Assume the result holds for $n-1$. By Corollary 3.1.12, we have $Z_{\omega^{n-1}}(W_n) \supseteq B_n$, so that the quotient $W_n/Z_{\omega^{n-1}}$ is a quotient of $W_{n-1} = W_n/B_n$, which is transfinite hypercentral by the inductive hypothesis. Hence, W_n is also transfinite hypercentral. □

Theorem 3.1.14. *If $R_i \leq VP_i$ and $R_i \otimes_D F \supseteq F[x_1, \ldots, x_i]$ for all $i = 1, \ldots, n-1$, then*

$$W_n = Z_{\omega^{n-1}+\cdots+\omega+1}(W_n). \tag{3.8}$$

We split the proof into several Lemmas.

We remind the reader that the symbol Δ_i is used to denote both the element $1\Delta_i$ of the i-th base subgroup, and the difference operator with respect to the i-th variable. It will be clear from the context which one we are using.

From now on, we assume that $R_i \subseteq VP_i$ and that $R_i \otimes_D F \supseteq F[x_1, \ldots, x_{n-1}]$ for all i. This is equivalent to requiring that for every monomial $x^\Lambda \in F[x_1, \ldots, x_{n-1}]$ there exists a non-zero element $d_\Lambda \in D$ such that $d_\Lambda x^\Lambda \in R_i$.

Lemma 3.1.15. *Let $\alpha < \omega^{n-1}$ be an ordinal. There exist $f \in VP_{n-1}$ with $\operatorname{tdeg}(f\Delta_n) = \alpha$ such that for every ordinal β such that $\beta + 1 < \alpha$, there exists an element $h_\beta \in W_n$ such that*

$$\operatorname{tdeg}([f\Delta_n, h_\beta]) > \beta.$$

In particular $\zeta_{\alpha+1} \supsetneq \zeta_\alpha$.

Proof. Write the ordinals α and $\beta + 1$ in their Cantor normal form:

$$\alpha = \omega^{n-2}a_{n-1} + \cdots + \omega a_2 + a_1, \quad \beta + 1 = \omega^{n-2}b_{n-1} + \cdots + \omega b_2 + b_1.$$

Let $f = cx^\Lambda \in R_{n-1}$ with $0 \neq c \in D$ and with $\Lambda = (a_1, \ldots, a_{n-1})$. We have $\operatorname{tdeg}(x^\Lambda \Delta_n) = \alpha$. Let $j \in \{1, \ldots, n-1\}$ be the maximum index such that $a_j > b_j$. If $a_j - b_j > 1$, then

$$\operatorname{tdeg}([f\Delta_n, \Delta_j]) > \beta.$$

If $a_j - b_j = 1$, then

$$\begin{aligned} \operatorname{tdeg}([f\Delta_n, cx_{j-1}^{|a_{j-1}-b_{j-1}|+1}\Delta_j]) > \beta, &\quad \text{if } j \neq 1, \\ \operatorname{tdeg}([f\Delta_n, \Delta_1]) > \beta, &\quad \text{if } j = 1. \end{aligned}$$

□

Lemma 3.1.16. *Let $g \in W_n \setminus B_n$. Then there exists $h \in W_n$ such that $[g, h] \notin B_n$, unless $g \in Z(W_{n-1})B_n$.*

Proof. Let $g = \sum_{i=1}^{n-1} g_i\Delta_i \in W_n \setminus B_n$, and suppose $g \notin Z(W_{n-1})B_n$. Then, the image of g in the quotient $W_n/B_n \simeq W_{n-1}$ is not central. We can choose $i \in \{1, \dots, n-1\}$ minimal such that g_i depends nontrivially on the variable x_j, for some $j < i$.

Consider the commutator

$$[g, \Delta_j] = [g_i\Delta_i, \Delta_j]^{g_{i-1}\Delta_{i-1}\cdots g_1\Delta_1} \mod (B_{i+1}\cdots B_n)$$

by minimality of i. Hence, the term $[g, \Delta_j]$ lies in B_i modulo $(B_{i+1}\cdots B_n)$ and therefore $[g, \Delta_j] \notin B_n$. □

Lemma 3.1.17. *Let $0 \neq c \in D$ be such that $c\Delta_{n-1} \in \mathrm{W}_{n-1}$. For every ordinal $\alpha < \omega^{n-1}$ there exists $h \in W_n$ such that $[c\Delta_{n-1}, h] \notin \zeta_\alpha$.*

Proof. Write $\alpha = \omega^{n-2}a_{n-1} + \cdots + \omega a_2 + a_1$. If $\Lambda = (a, \dots, a_{n-2}, a_{n-1} + 2)$, then $h = x^\Lambda\Delta_n$ is the desired element. □

A direct consequence of the previous results is the following.

Corollary 3.1.18. *$Z_{\omega^{n-1}+1}(W_n) = Z(W_{n-1})B_n$ and $Z_{\omega^{n-1}}(W_n) = B_n$. In particular $\zeta_\alpha = Z_\alpha(W_n) \subseteq B_n$ whenever $\alpha \leq \omega^{n-1}$.*

We are now ready to give the claimed proof.

Proof of Theorem 3.1.14. We argue by induction on n, the case $n = 1$ being trivial.

By Corollary 3.1.18, we know that $Z_{\omega^{n-1}}(W_n) = B_n$ and by inductive hypothesis we may assume that

$$Z_{\omega^{n-2}+\cdots+\omega+1}(W_{n-1}) = W_{n-1} \cong W_n/B_n = W_n/(Z_{\omega^{n-1}}(W_n)).$$

Hence W_n is transfinite hypercentral and $W_n = Z_{\omega^{n-1}+\cdots+\omega+1}(W_{n-1})$. □

Remark 3.1.19. When $R_i \otimes F = F[x_1, \dots, x_i]$ we can give an explicit description of the α-th term of the upper central series of W_n by way of the definition of transfinite degree, more specifically

$$Z_\alpha(W_n) = \{g \in W_n \mid \mathrm{tdeg}(g) < \alpha\} \tag{3.9}$$

and

$$Z_{\alpha+1}(W_n) = \{cx^\Lambda\Delta_k \mid c \in D\} \ltimes Z_\alpha \tag{3.10}$$

where $\mathrm{tdeg}(x^\Lambda\Delta_k) = \alpha$.

3.2 The Lie Algebra associated to W_n^∞

As similarly described in Section 2.2, we present the Lie algebra associated with W_n^∞ as an iterated wreath product $\wr_{i=1}^n \mathfrak{L}_1^\infty$, where $\mathfrak{L}_1^\infty = D\partial_u$ is the one-dimensional Lie algebra over D. This Lie algebra can be identified with the subalgebra of the Witt algebra whose basis elements are of the form $x_{i_1}^{\lambda_{i_1}} \dots x_{i_h}^{\lambda_{i_h}}$ with $1 \leq i_1 < \dots < i_h \leq n$. We briefly outline its construction, although it is entirely analogous to the one presented in the previous chapter.

We follow the same construction given as in [3]. Let ∂_k be the derivation given by the standard partial derivative with respect to x_k, where $1 \leq k \leq n$. We define $\mathfrak{L}_n^\infty$ to be the free D-module spanned by the basis

$$\mathfrak{B} := \left\{ x^\Lambda \partial_k \mid 1 \leq k \leq n \text{ and } \Lambda \in \mathcal{P}(k-1) \right\}. \tag{3.11}$$

In the same fashion as Definition 3.0.3, we define the transfinite degree of an element $x^\Lambda \partial_k$ in $\mathfrak{B}$ as $\operatorname{tdeg}(x^\Lambda \partial_k) = \sum_{i=1}^{n-k} \omega^{n-i} + \operatorname{tdeg}(x^\Lambda)$ and $\operatorname{tdeg}(0) = 0$. As with the group W_n, the function tdeg can be extended to $\mathfrak{L}_n^\infty$.

The product of the algebra is defined on the basis $\mathfrak{B}$ via

$$\begin{aligned} [x^\Lambda \partial_k, x^\Theta \partial_j] := \quad & \partial_j(x^\Lambda) x^\Theta \partial_k - x^\Lambda \partial_k(x^\Theta) \partial_j \\ = \quad & \begin{cases} \partial_j(x^\Lambda) x^\Theta \partial_k & \text{if } j < k, \\ -x^\Lambda \partial_k(x^\Theta) \partial_j & \text{if } j > k, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

This operation is then extended by bilinearity on the whole $\mathfrak{L}_n^\infty$, endowing it with a D-Lie ring structure.

With the same notation as in Equation (3.11), we may define a map connecting the structures of W_n^∞ and $\mathfrak{L}_n^\infty$.

Let $\varphi \colon \mathcal{B} \cup \{1\} \to \mathfrak{B} \cup \{0\}$ be defined by setting $\varphi(x^\Lambda \Delta_k) = x^\Lambda \partial_k$ and $\varphi(1) = 0$. We extend this map to the group W_n^∞ as follows. For each element $1 \neq g \in W_n^\infty$, there exists a unique ordinal α such that $g \in Z_{\alpha+1} \setminus Z_\alpha$. By way of Equation (3.10), $g = cx^\Lambda \Delta_k \cdot h$ for unique $cx^\Lambda \Delta_k \in Z_{\alpha+1} \setminus Z_\alpha$ and $h \in Z_\alpha$. Thus, we set $\varphi(g) = cx^\Lambda \partial_k$. Observe that the map φ is not injective.

Lemma 3.2.1. *For every pair $g, h \in D\mathcal{B}$, the following equality holds*

$$\varphi([g,h]) = [\varphi(g), \varphi(h)].$$

Proof. It suffices to note that if $g = cx^\Lambda \Delta_k$ and $h = dx^\Theta \Delta_\ell$ with $k > \ell$ and $c, d \in D$, then, by Lemma 3.0.4, we get that

$$\mathrm{lt}([cx^\Lambda \Delta_k, dx^\Theta \Delta_\ell]) = cd\frac{\partial x^\Lambda}{\partial x_\ell} x^\Theta \Delta_k.$$

Therefore, $\varphi([g,h]) = cd\dfrac{\partial x^\Lambda}{\partial x_\ell} x^\Theta \partial_k = [cx^\Lambda \partial_k, dx^\Theta \partial_\ell]$ as required. □

3.2.1 Saturated Subgroups and Homogeneous Subring

From now on, unless explicitly stated otherwise, we consider $R_i = D[x_1, \ldots, x_i]$, for $i = 1, \ldots, n-1$.

Definition 3.2.2. Let $G \leq W_n^\infty$. We shall say that G is a D-subgroup of W_n^∞ if G is closed under multiplication by elements of D, i.e.,

$$G = D \cdot G.$$

From now on, all the subgroups of W_n^∞ will be regarded as D-subgroups, unless otherwise stated.

Definition 3.2.3. Let H be a D-subgroup of W_n^∞. We shall say that H is a saturated subgroup of W_n^∞ if whenever $f = \prod_\alpha c_\alpha b_\alpha$ belongs to H, with $c_\alpha \in D$, then $b_\alpha \in H$ for all ordinals α.

Remark 3.2.4. Notice that for H to be saturated, it is sufficient that if $f \in H$ and $\mathrm{lt}(f) = c_\alpha b_\alpha$, where $c_\alpha \in D$ and $b_\alpha \in \mathcal{B}$, then $b_\alpha \in H$. An equivalent condition is that

$$H = \langle c_\alpha b_\alpha \mid c_\alpha \in D \text{ and } b_\alpha \in H \cap \mathcal{B} \rangle .$$

An immediate consequence is that

$$H = (H \cap B_n) \rtimes \cdots \rtimes (H \cap B_1).$$

Theorem 3.2.5. *The normalizer in W_n^∞ of a saturated subgroup is also saturated.*

Proof. By the definition of a saturated subgroup, it suffices to show that if $f \in N_{W_n^\infty}(H)$ and $\mathrm{lt}(f) = cx^\Theta \Delta_k$, then $x^\Theta \Delta_k \in N_{W_n^\infty}(H)$.

Write $f = cx^\Theta \Delta_k \prod_{\beta<\alpha} f_\beta$, where $\mathrm{tdeg}(x^\Theta \Delta_k) = \alpha$, and let $x^\Lambda \Delta_u$ be a generic monic monomial in H. By hypothesis, we have

$$H \ni [f, x^\Lambda \Delta_u] = [cx^\Theta \Delta_k, x^\Lambda \Delta_u] \cdot [cx^\Theta \Delta_k, x^\Lambda \Delta_u, \prod_{\beta<\alpha} f_\beta] \cdot [\prod_{\beta<\alpha} f_\beta, x^\Lambda \Delta_u].$$

Our goal is to show that $[x^\Theta \Delta_k, x^\Lambda \Delta_u] \in H$.

We decompose the commutator $[f_\alpha, x^\Lambda \Delta_u]$ as a product $d_1 \cdots d_i$, where each d_j is a monomial and $d_1 \succ \cdots \succ d_i$.

Case 1: $k = u$**.** In this case, $[x^\Theta \Delta_k, x^\Lambda \Delta_u] = 1 \in H$, and there's nothing more to prove.

Case 2: $k < u$**.** Then

$$[cx^\Theta \Delta_k, x^\Lambda \Delta_u] = \sum_{r=1}^{\lambda_k} \frac{\partial^r x^\Lambda}{\partial x_k^r} \frac{(cx^\Theta)^r}{r!} \Delta_u,$$

where λ_k is the degree of x_k in x^Λ. Hence, the r-th term is:

$$d_r = \frac{\partial^r x^\Lambda}{\partial x_k^r} \cdot \frac{(cx^\Theta)^r}{r!} \Delta_u.$$

It is not difficult to see that d_1 is the leading term of $[f, x^\Lambda \Delta_u] \in H$. Since H is saturated, it follows that $d_1 \in H$. Then, by induction, we argue that $(r+1)d_{r+1}$ is the leading term of $[d_r, f] \in H$, so $d_{r+1} \in H$ as well. Therefore, all $d_r \in H$, and thus $[cx^\Theta \Delta_k, x^\Lambda \Delta_u] \in H$.

Moreover, since each $d_j = c_j b_j \in H$ with $c_j \in D$ and $b_j \in \mathcal{B}$, and H is saturated, we get $b_j \in H$ for all j. In particular, $[x^\Theta \Delta_k, x^\Lambda \Delta_u] \in H$.

Case 3: $k > u$**.** In this case, the argument is analogous to Case 2. Each term is of the form:

$$d_r = c \sum_{r=1}^{\theta_k} \frac{\partial^r x^\Theta}{\partial x_u^r} \frac{(x^\Lambda)^r}{r!} \Delta_k,$$

and again, by induction, we obtain that $(r+1)d_{r+1} = \mathrm{lt}([d_r, x^\Lambda \Delta_u]) \in H$. This shows that all $d_r \in H$, and so $[x^\Theta \Delta_k, x^\Lambda \Delta_u] \in H$. □

We recall the definition of homogeneous subring of $\mathfrak{L}_n^\infty$ already given in Definition 2.2.1.

Definition 3.2.6. A Lie subring $\mathfrak{H}$ of $\mathfrak{L}_n^\infty$ is said to be homogeneous if it is the free D-module spanned by some subset of $\mathfrak{B}$.

The following result concerning homogeneous subrings can be established by an argument entirely analogous to that of Theorem 2.2.4.

Theorem 3.2.7. *[3] The idealizer in $\mathfrak{L}_n^\infty$ of a homogeneous subring is also homogeneous.*

Let $H \leq W_n^\infty$. We denote by H^φ the D-subring of $\mathfrak{L}_n^\infty$ generated by $\varphi(H)$.

Remark 3.2.8. If $H \leq W_n^\infty$ is a saturated subgroup, then H^φ is a homogeneous subring of $\mathfrak{L}_n^\infty$.

The following statement is a straightforward consequence of Lemma 3.2.1 and the previous remark.

Lemma 3.2.9. *The α-th center $\mathfrak{Z}_\alpha$ of $\mathfrak{L}_n^\infty$ is an homogeneous subring of $\mathfrak{L}_n^\infty$. Moreover*

$$\mathfrak{Z}_\alpha = \left\langle cx^\Lambda \partial_k \mid c \in D \text{ and } \operatorname{tdeg}(x^\Lambda \partial_k) < \alpha \right\rangle = Z_\alpha^\varphi.$$

In particular $\mathfrak{L}_n^\infty$ is a transfinite hypercentral Lie ring over D.

Noting that the map φ yields a bijection between the set of saturated normal subgroups of W_n^∞ and the set of homogeneous Lie ideals of $\mathfrak{L}_n^\infty$, we have the following completely analogous result to Proposition 3.3.4.

Proposition 3.2.10. *Every homogeneous ideal of $\mathfrak{L}_n^\infty$ is a term $\mathfrak{Z}_\alpha$ of the transfinite upper central series of $\mathfrak{L}_n^\infty$.*

In general the map φ transforms normalizers into idealizers when restricted to saturated subgroups. The proof is a straightforward consequence of Theorem 3.2.5, Theorem 3.2.7 and Lemma 3.2.1.

Proposition 3.2.11. *Let H be a saturated subgroup of W_n^∞. An element $g \in W_n^\infty$ belongs to the normalizer $N_{W_n^\infty}(H)$ of H in W_n^∞ if and only if $\varphi(g)$ lies in the idealizer $\mathfrak{N}_{\mathfrak{L}_n^\infty}(H^\varphi)$ of H^φ in $\mathfrak{L}_n^\infty$.*

Corollary 3.2.12. *The difference $|N_{W_n^\infty}(H) \cap \mathcal{B}| - |H \cap \mathcal{B}|$ is equal to the rank of $\mathfrak{N}_{\mathfrak{L}_n^\infty}(H^\varphi)/H^\varphi$ as a free D-module.*

3.3 Normality Conditions in D-subgroups of W_n^∞

Analogously to Section 2.4, we aim to provide normality conditions for the subgroups of W_n^∞. We show that, under certain conditions, normal subgroups coincide with the terms of the ascending central series.

Definition 3.3.1. Let $G \leq W_n^\infty$. We say that G is *full* if, for every element $g = \prod_\alpha c_\alpha b_\alpha \in G$, with $c_\alpha = d\bar{c}_\alpha$ for some $d \neq 0$ in D, the element $\bar{g} = \prod_\alpha \bar{c}_\alpha b_\alpha$ also belongs to G.

Note that if D is a field, every D-subgroup is full.

Remark 3.3.2. A straightforward argument shows that a D-subgroup $H \leq W_n^\infty$ is saturated if and only if it is D-generated by $H \cap \mathcal{B}$; that is, the elements of H are precisely those that can be written (uniquely, in decreasing order) as

$$\prod_{g \in H \cap \mathcal{B}} c_g g,$$

where $c_g \neq 0$ for only finitely many g. In particular, every saturated subgroup is full. The converse, however, is false: for instance, the D-subgroup $H = \{d(x_1 + x_2)\Delta_n \mid d \in D\}$ is full but not saturated.

From now on, we call the *full D-normal closure* of a subgroup $H \leq W_n^\infty$ the minimal full normal D-subgroup of W_n^∞ containing H.

Lemma 3.3.3. *Let $g \in W_n^\infty$ be an element of transfinite degree α. The full D-normal closure N of the D-subgroup $H = D\langle g \rangle$ is $Z_{\alpha+1}$.*

Proof. Let $cx^\Lambda \Delta_k$ be the leading term of $g \neq 1$, for some $1 \leq k \leq n$. If $\alpha = 0$, then $H = Z_1$ and there is nothing to prove.

We proceed by transfinite induction on α.

First, suppose that $\Lambda = 0$, so that $\mathrm{lt}(g) = c\Delta_k$ with $k < n$ and $c \in D$. Then the transfinite degree of $\mathrm{lt}(g)$ is $\alpha = w^{n-1} + \cdots + w^k$. For each s, define

$$\beta_s = w^{n-1} + \cdots + w^{k+1} + sw^{k-1}.$$

Observe that $\sup_s \beta_s = \alpha$. Consider the commutator $u_s = [x_k^{s+1}\Delta_{k+1}, g] \in N$, which has transfinite degree $\beta_s < \alpha$. By the inductive hypothesis, the full D-normal closure

of $D\langle u_s\rangle$ is Z_{β_s+1}. It follows that

$$N \geq \bigcup_s Z_{\beta_s+1} = Z_\alpha.$$

Moreover, since $g \equiv c\Delta_k \mod Z_\alpha$ and N is full, we conclude that $\Delta_k \in N$. Thus,

$$N \geq D\langle \Delta_k\rangle \rtimes Z_\alpha = Z_{\alpha+1} \geq H,$$

so $N = Z_{\alpha+1}$.

Now consider the case $\Lambda \neq 0$. Let ℓ be the minimal index such that $\lambda_\ell \neq 0$. Then we can write $x^\Lambda = x_\ell x^\Theta$, where $\theta_i = \lambda_i - \delta_{i\ell}$. Define $x^{\Gamma_s} = (x_{\ell-1})^s$ if $\ell > 1$, and $x^{\Gamma_s} = 1$ otherwise. Consider the commutator

$$[g,\, x^{\Gamma_s}\Delta_\ell] \in N,$$

which has transfinite degree ε_s, where $\sup_s \varepsilon_s = \alpha$ if $\ell > 1$, and $\sup_s \varepsilon_s = \alpha - 1$ if $\ell = 1$. Reasoning as before, we get $Z_\alpha \leq N$, and therefore $N = Z_{\alpha+1}$. □

Proposition 3.3.4. *A normal full D-subgroup H of W_n^∞ is a term Z_α of the transfinite upper central series of W_n^∞. In particular H is saturated.*

Proof. Let $\alpha = \sup_{h\in H}(\mathrm{tdeg}(h)) + 1$. Note that $H \leq Z_\alpha$. By Lemma 3.3.3, the subgroup H contains $\bigcup_{\beta\leq\alpha} Z_\beta = Z_\alpha$. □

3.4 A Sequence of Normalizers

In this section, we define the analogue of the canonical regular elementary abelian group introduced in Equation (2.3). We also compute the corresponding chain of normalizers arising from this group, and highlight the connection between the growth of this sequence and integer partitions.

Let $\mathrm{T}^\infty = \langle \Delta_1, \ldots, \Delta_n\rangle$ be the abelian regular subgroup of W_n^∞ generated by the unit constant function elements. We deal with the normalizer chain in W_n^∞ starting from T^∞, that is the sequence $\{\mathbf{N}_i^{(\infty)}\}_{i\geq -1}$ defined as follows

$$\mathbf{N}_i^{(\infty)} = \begin{cases} \mathrm{T}^\infty & i = -1, \\ N_{W_n^\infty}(\mathrm{T}^\infty) & i = 0, \\ N_{W_n^\infty}(\mathbf{N}_{i-1}^{(\infty)}) & i \geq 1. \end{cases}$$

By means of Proposition 3.2.11 and Corollary 3.2.12, the normalizer chain described above can be interpreted using results previously obtained by Aragona et al. in [3], within the algebra $\mathfrak{L}_n^\infty$ for the following idealizer chain

$$\mathfrak{N}_i^{(\infty)} = \begin{cases} \mathfrak{T}^\infty & \text{if } i = -1 \\ \mathfrak{N}_{\mathfrak{L}_n^\infty}(\mathfrak{N}_{j-1}^{(\infty)}) & \text{if } i \geq 0 \end{cases} \tag{3.12}$$

where $\mathfrak{T}^\infty = \langle \partial_1, \ldots, \partial_n \rangle$. Notice that this idealizer chain is the image under φ of the normalizer chain in the group, since φ is a bijection when restricted to saturated subgroups.

Definition 3.4.1. Let $i \geq 1$ be an integer, and let $1 \leq r_i \leq n-1$ be such that $i \equiv r_i \bmod (n-1)$. We set

$$h_i := \left\lfloor \frac{i-1}{n-1} \right\rfloor + 1.$$

The functions *weight-degree* and *i-th level-function* on power monomials elements are defined as

$$\operatorname{wd}(cx^\Lambda \Delta_k) = \operatorname{wt}(\Lambda) - \deg(x^\Lambda) + n - k,$$

and

$$\operatorname{lev}_i(cx^\Lambda \Delta_k) = h_i \operatorname{wd}(x^\Lambda \Delta_k) + \deg(x^\Lambda) - 1.$$

Let $i \geq -1$. We define the set

$$\mathcal{N}_i^{(\infty)} = \left\{ x^\Lambda \Delta_k \mid \operatorname{lev}_j(x^\Lambda \Delta_k) = j \text{ for some } j \leq i \right\}$$

and we call $\mathcal{L}_i = \mathcal{N}_i^{(\infty)} \setminus \mathcal{N}_{i-1}^{(\infty)}$.

The following results are the analogues of those found by Aragona et al. in [3] for the idealizer chain (3.12), interpreted via the inverse map φ^{-1}.

Theorem 3.4.2. *The first normalizer $N_{W_n^\infty}(\mathrm{T}^\infty)$ of T^∞ coincides with $\langle \mathcal{N}_0^{(\infty)} \rangle$, and in general,*

$$\mathbf{N}_i^{(\infty)} = N_{W_n^\infty}(\langle \mathcal{N}_{i-1}^{(\infty)} \rangle) = \langle \mathcal{N}_i^{(\infty)} \rangle.$$

Let $\{a_i\}_{i=0}^\infty$ denote the sequence of the number of partitions of i. Let $b_i = \sum_{j=0}^i a_j$ be i-th partial sum of $\{a_i\}$ and $c_i = \sum_{j=0}^i b_j$ be the i-th partial sum of $\{b_i\}$. The initial terms of these sequences can be found in [1] at A085360 . Beyond a threshold value that depends quadratically on n, the sequence $\{|\mathcal{L}_i|\}$ exhibits periodic behavior and it is related to the sequence $\{c_i\}$.

Proposition 3.4.3. *If $i > (n-4)(n-1)$ and $1 \leq k \leq n$, then*

$$|\mathcal{L}_i \cap \mathcal{B}_k| = b_{r_i+k-n-1}$$

and

$$|\mathcal{L}_i| = c_{r_i-1},$$

where $\mathcal{B}_k = \mathcal{B} \cap B_k$ and the value r_i is as in Definition 3.4.1.

As a consequence, it follows that the sequence $\{|\mathcal{L}_i|\}$ is ultimately periodic, meaning there exist integers k and j such that $|\mathcal{L}_i| = |\mathcal{L}_{i+k}|$ for all $i \geq j$.

Although Proposition 3.4.3 is stated under the assumption $R_i = D[x_1, \ldots, x_i]$, we prove that its validity extends to a more general framework.

Define

$$\overline{W}_n^{\infty} = D \wr_{\bar{R}_{n-1}} D \wr_{\bar{R}_{n-2}} \cdots \wr_{\bar{R}_1} D,$$

where each $\bar{R}_i$ is a subring of the ring of numerical polynomials P_i, satisfying $\bar{R}_i \otimes_D F = F[x_1, \ldots, x_i]$. Also define

$$\widetilde{W}_n^{\infty} = F \wr_{\tilde{R}_{n-1}} F \wr_{\tilde{R}_{n-2}} \cdots \wr_{\tilde{R}_1} F,$$

where $\tilde{R}_i = F[x_1, \ldots, x_i]$. Clearly, $W_n^{\infty} \leq \overline{W}_n^{\infty} \leq \widetilde{W}_n^{\infty}$. We denote by B_i, $\bar{B}_i$, and $\tilde{B}_i$ the ith base subgroup of W_n^{∞}, $\overline{W}_n^{\infty}$, and $\widetilde{W}_n^{\infty}$, respectively.

We now consider the normalizer chain $\{\overline{\mathbf{N}}_i^{(\infty)}\}_{i \geq -1}$ in $\overline{W}_n^{\infty}$ arising from the subgroup T^{∞}, defined recursively by $\overline{\mathbf{N}}_{-1}^{(\infty)} = \mathrm{T}^{\infty}$ and

$$\overline{\mathbf{N}}_i^{(\infty)} = N_{\overline{W}_n^{\infty}}(\overline{\mathbf{N}}_i^{(\infty)}).$$

Analogously, we define the normalizer chain $\{\widetilde{\mathbf{N}}_i^{(\infty)}\}_{i \geq -1}$ in $\widetilde{W}_n^{\infty}$. Observe that for all $i \geq -1$ and $1 \leq k \leq n$, the following identity holds:

$$(\overline{\mathbf{N}}_i^{(\infty)} \cap \bar{B}_k) \otimes_D F \cong \widetilde{\mathbf{N}}_i^{(\infty)} \cap \tilde{B}_k \cong (\mathbf{N}_i^{(\infty)} \cap B_k) \otimes_D F. \tag{3.13}$$

Define the free rank $\mathrm{frk}(M)$ of a D-module M as $\dim_F(M \otimes_D F)$. Then, from Equation 3.13, we conclude that

$$\mathrm{frk}(\overline{\mathbf{N}}_i^{(\infty)} \cap \bar{B}_k) = \mathrm{frk}(\mathbf{N}_i^{(\infty)} \cap B_k).$$

From Equation 3.13, the following generalization of Proposition 3.4.3 follows.

Theorem 3.4.4. *The free rank of the quotient*

$$(\bar{\mathbf{N}}_i^{(\infty)} \cap \bar{B}_k)/(\bar{\mathbf{N}}_{i-1}^{(\infty)} \cap \bar{B}_k)$$

is equal to the free rank $b_{r_i+k-n-1}$ *of*

$$(\mathbf{N}_i^{(\infty)} \cap B_k)/(\mathbf{N}_{i-1}^{(\infty)} \cap B_k)$$

for all $i > (n-4)(n-1)$. *In particular, it is independent of the choice of the rings* R_j.

3.5 Abelian Regular Normal Subgroups of $\mathbf{N}_0^{(\infty)}$

In this section we find an analog of Theorem 1.1.5 and Proposition 1.1.4 stated in Section 1.1 in the case of characteristic 2.

We begin by proving that any abelian regular subgroup must intersect the center of W_n^∞ non-trivially, which will play a key role in the rest of the section.

Lemma 3.5.1. *If* $T < W_n^\infty$ *is an abelian regular subgroup, then* T *intersects the center* Z *of* W_n^∞ *non-trivially.*

Proof. It is enough to notice that TZ is abelian and transitive, so it is regular (and contains T). This means that $T = TZ$. □

Let $\mathrm{T}^\infty = \langle \Delta_1, \ldots, \Delta_n \rangle$ be the canonical regular subgroup considered in the previous section.

Remark 3.5.2. Notice that $\mathbf{N}_0^{(\infty)} = S \ltimes \mathrm{T}^\infty$, where S is the group generated by $\{x_j\Delta_k \mid 1 \le j < k \le n\}$ acting on T^∞ as the group of upper unitriangular matrices. Indeed, if $k > i$, then

$$[\Delta_i, x_j\Delta_k] = \begin{cases} \Delta_k & \text{if } i = j \\ 1 & \text{otherwise} \end{cases}$$

Moreover, $\mathbf{N}_0^{(\infty)}$ acts on T^∞ by conjugation, i.e.

$$(\Delta_i)^{x_j\Delta_k} = \Delta_i\,[\Delta_i, x_j\Delta_k] = \begin{cases} \Delta_i\Delta_k & \text{if } i = j \\ \Delta_i & \text{otherwise} \end{cases}$$

and $(\Delta_i)^{\Delta_k} = \Delta_i$. We denote by E_{ij} the elementary matrix with 1 in the position (i, j) and 0 elsewhere, by e_i the i-th vector a fixed basis of D^n, and by $\mathbb{1}_n$ the $n \times n$ identity matrix. The vector e_i represents the element Δ_i of T^∞, while the matrix $\mathbb{1}_n + \delta_{ji}E_{jk}$ represents the action of $x_j\Delta_k$ on Δ_i. In other words

$$(\Delta_i)^{x_i\Delta_k} = e_i \cdot (\mathbb{1}_n + E_{ik}) = e_i + e_k = \Delta_i\Delta_k.$$

By varying $1 < i < k < n$, these matrices generate the upper unitriangular group U. Thus, we establish a surjective homomorphism $\pi\colon \mathbf{N}_0^{(\infty)} \to U$ such that $\ker(\pi) = \mathrm{T}^\infty$. Moreover the map $\tau\colon U \to \mathbf{N}_0^{(\infty)}$, defined by sending $E_{jk} \to x_j\Delta_k$, is a homomorphism such that $\tau\pi$ is the identity. It follows that $\mathbf{N}_0^{(\infty)} \cong U \ltimes \mathrm{T}^\infty \cong S \ltimes \mathrm{T}^\infty$.

Let $\bar{T}$ be another abelian regular subgroup normal in $\mathbf{N}_0^{(\infty)}$ and isomorphic to D^n. We set $\bar{T} = \langle \bar{z}_1, \ldots, \bar{z}_n \rangle$ with $\bar{z}_i = t_i v_i$ where $t_i \in T$ and $v_i \in S$.

Lemma 3.5.3. *Let $t_i = \sum_{j=1}^n a_{ij}\Delta_j$, where $a_{ij} \in D$. The matrix $(a_{ij})_{i,j=1,\ldots,n}$ is unimodular.*

Proof. The group $\bar{T}$ is regular, in particular, for each $j = 1, \ldots, n$, there exists a unique permutation $\sigma_j \in \bar{T}$ such that $\sigma_j(0) = e_j$. Since $\bar{z}_i$'s generate $\bar{T}$, there are coefficients $h_{ij} \in D$ such that $\sigma_j = \sum_{i=1}^n h_{ji}\bar{z}_i$ and as a consequence

$$e_j = \sigma_j(0) = \sum_{i=1}^n h_{ji}\bar{z}_i(0) = \sum_{i=1}^n h_{ji}t_i v_i\,(0)\,.$$

Notice that $v_i(0) = 0$ since $v_i \in S$ and $\Delta_s(0) = e_s$, thus

$$\begin{aligned} e_j &= \sum_{i=1}^n h_{ji}t_i v_i\,(0) = \sum_{i=1}^n h_{ji}t_i\,(0) \\ &= \sum_{i=1}^n h_{ji} \sum_{s=1}^n a_{is}\Delta_s\,(0) = \sum_{i=1}^n h_{ji} \sum_{s=1}^n a_{is}e_s \end{aligned}$$

Hence $\sum_{i=1}^n h_{ji}a_{is} = \delta_{js}$ for each $j = 1, \ldots, n$. □

Let us consider the inverse matrix (b_{ij}) of (a_{ij}) and let us define $\bar{t}_i = \sum_{j=1}^n b_{ij}\bar{z}_j$. Notice that

$$\bar{t}_i\,(0) = \sum_{j=1}^n b_{ij}\bar{z}_j\,(0) = \sum_{j=1}^n b_{ij}t_j\,(0) = \Delta_i\,(0) = e_i.$$

Since $\bar{T}$ is regular, the only element of $\bar{T}$ sending 0 to e_j is Δ_j; so, we can write $\bar{T} = \langle \bar{t}_1, \ldots, \bar{t}_n \rangle$ where

$$\bar{t}_i = \Delta_i u_i \text{ with } u_i \in S.$$

Lemma 3.5.4. *If $\Delta_j \in \bar{T}$, then $\Delta_{j+1}, \ldots, \Delta_n \in \bar{T}$.*

Proof. It is enough to notice that $\Delta_i = [x_j\Delta_i, \Delta_j] \in \bar{T}$ for $i = j+1, \ldots, n$. □

We are now ready to describe the group $\bar{T} = \langle \bar{t}_1, \ldots, \bar{t}_n \rangle$ as did in Proposition 1.1.4 in the case of characteristic 2.

Proposition 3.5.5. *If $\bar{T}$ is an abelian regular normal subgroup of $\mathbf{N}_0^{(\infty)}$ isomorphic to D^n, then there exists $c \in D$ such that*

$$\bar{T} = \langle \Delta_1(cx_1\Delta_n), \Delta_2, \ldots, \Delta_n \rangle.$$

Proof. By Lemma 3.5.1, $\Delta_n \in \bar{T}$ and so u_n is the identity 1 of $\bar{T}$. Analogously $\Delta_i \in \bar{T} \bmod (B_n \cdots B_{i+1})$ and so $u_i \in B_n \cdots B_{i+1}$. Hence

$$\bar{t}_i = \Delta_i \prod_{\substack{i+1 \le k \le n \\ j<k}} (x_j\Delta_k)^{c_{ijk}}. \tag{3.14}$$

In particular, $[\bar{t}_i, x_1\Delta_s] = [\Delta_i, x_1\Delta_s]^{u_i}[u_i, x_1\Delta_s] = \Delta_s^{\delta_{i1}u_i^{-1}}[u_i, x_1\Delta_s] \in \bar{T}$. If $i \neq 1$, we have $[u_i, x_1\Delta_s] \in \bar{T} \cap S$, and so $[u_i, x_1\Delta_s] = 1$. This implies that $u_i = \prod (x_1\Delta_k)^{c_{i1k}}$ for $i > 1$ and

$$\bar{t}_i = \Delta_i \prod_{i+1 \le k \le n} (x_1\Delta_k)^{c_{i1k}} \text{ for } 1 < i < n.$$

Let $i \geq 2$ and $i+1 \leq k < n$, then the commutator $[\bar{t}_i, x_k\Delta_n] = [\Delta_i, x_k\Delta_n]^{u_i}[u_i, x_k\Delta_n] = (x_1\Delta_n)^{-c_{i1k}} \in \bar{T} \cap S$. Thus, $(x_1\Delta_n)^{-c_{i1k}} = 1$ and so $c_{i1k} = 0$. This means that

$$u_i = (x_1\Delta_n)^{c_{i1n}} \text{ for } 1 < i < n-1.$$

For $1 < i \leq n-2$ we get that

$$[\bar{t}_i, x_i\Delta_{i+1}] = [\Delta_i, x_i\Delta_{i+1}]^{u_i}[u_i, x_i\Delta_{i+1}] = \Delta_{i+1}^{-1}[u_i, x_i\Delta_{i+1}] = \Delta_{i+1}^{-1} \in \bar{T}.$$

In particular $\Delta_3 \in \bar{T}$ and, by Lemma 3.5.4, we have $\Delta_4, \ldots, \Delta_n \in \bar{T}$. Hence, we obtain

$$\begin{aligned} \bar{t}_i &= \Delta_i \text{ for } 3 \leq i \leq n, \\ \bar{t}_2 &= \Delta_2(x_1\Delta_n)^{c_{21n}} \end{aligned} \tag{3.15}$$

and $\bar{t}_1$ as in Equation (3.14).

When $1 < k < n$, we get

$$[\bar{t}_1, x_k\Delta_n] = [\Delta_1, x_k\Delta_n]^{u_1}[u_1, x_k\Delta_n] = \sum_{j<k\leq n-1} (x_j\Delta_n)^{c_{1jk}} \in \bar{T} \cap S,$$

hence, by regularity, $c_{1jk} = 0$ and

$$\bar{t}_1 = \Delta_1(x_1\Delta_n)^{c_{11n}} \dots (x_{n-1}\Delta_n)^{c_{1,n-1,n}}.$$

If $3 \leq s \leq n$, then the commutator $[\bar{t}_1, x_2\Delta_s] = x_2\Delta_n^{c_{1sn}} \in \bar{T} \cap S$. Thus, it has to be the identity and so $c_{1sn} = 0$ for $3 \leq s < n$, i.e.

$$u_1 = \prod_{j=1,2} (x_j\Delta_n)^{c_{1jn}} = (c_{11n}x_1 + c_{12n}x_2)\Delta_n.$$

Since $\bar{T}$ is abelian, on the one hand we have

$$\begin{aligned} 1 = [\bar{t}_1, \bar{t}_2] &= [\Delta_1 u_1, \Delta_2 u_2] \\ &= [\Delta_1, u_2]^{u_1}[\Delta_1, \Delta_2]^{u_1u_2}[u_1, u_2][u_1, \Delta_2]^{\Delta_2} \\ &= (\Delta_n)^{c_{12n}-c_{21n}}[u_1, u_2] \end{aligned}$$

and so $[u_1, u_2] = 1$ and $\Delta_n^{c_{12n}-c_{21n}} = 1$. In particular

$$c_{12n} = c_{21n}. \tag{3.16}$$

On the other hand, the commutator

$$\begin{aligned} [\bar{t}_1, x_1\Delta_2] &= [\Delta_1, x_1\Delta_2]^{u_1}[u_1, x_1\Delta_2] \\ &= \Delta_2^{-u_1}(x_1\Delta_n)^{c_{12n}} \\ &= \Delta_2^{-1}\Delta_n^{c_{12n}}(x_1\Delta_n)^{c_{12n}} \in \bar{T}. \end{aligned}$$

Since $\Delta_n \in \bar{T}$, we get that $\Delta_2(x_1\Delta_n)^{-c_{12n}} \in \bar{T}$ and by Equation (3.15) $c_{21n} = -c_{12n}$. By (3.16) it follows that $c_{21n} = c_{12n} = 0$, i.e. $\bar{t}_2 = \Delta_2$ and $\bar{t}_1 = \Delta_1(x_1\Delta_n)^{c_{11n}}$. □

Let $\bar{T}_c := \langle \Delta_1(cx_1\Delta_n), \Delta_2, \dots, \Delta_n \rangle$ be as in the previous proposition. We have the following characteristic zero counterpart of Theorem 1.1.5.

Corollary 3.5.6. *If 2 is an invertible element of D, then for every $g \in \mathbf{N}_1^{(\infty)}$ there exists $c_g \in D$ such that $(T^\infty)^g = \bar{T}_{c_g}$. Otherwise in $\mathbf{N}_1^{(\infty)}$ there are two distinct conjugacy classes of abelian regular normal subgroups of $\mathbf{N}_0^{(\infty)}$ isomorphic to D^n.*

Proof. It is enough to notice that $\mathcal{N}_1^{(\infty)} \setminus \mathcal{N}_0^{(\infty)} = \{x_1^2\Delta_n\}$, and $\Delta_i^{x_1^2\Delta_n} = \Delta_i$ for $i = 2, \ldots, n$. Moreover, for $d \in D$

$$\Delta_1^{dx_1^2\Delta_n} = \Delta_1[\Delta_1, dx_1^2\Delta_n] = \Delta_1(2dx_1\Delta_n)$$

and

$$\begin{aligned}(\Delta_1(x_1\Delta_n))^{dx_1^2\Delta_n} &= \Delta_1(x_1\Delta_n)[\Delta_1(x_1\Delta_n), dx_1^2\Delta_n] \\ &= \Delta_1(x_1\Delta_n)[\Delta_1, dx_1^2\Delta_n] = \Delta_1((2d+1)x_1\Delta_n)\end{aligned}$$

The element Δ_1 appears as a member of the second family if and only if 2 is invertible in D, concluding the proof. □

CHAPTER 4

BI-BRACES OVER FINITE FIELDS AND p-ADIC INTEGERS

This chapter is primarily based on the results presented in [8, 11].

In this chapter, we consider M to be a free module of rank n over a principal ideal domain R. We equip M with a bi-brace structure arising from a regular subgroup of the holomorph, normalized by the right regular representation (see Theorem 1.6.4). Under suitable assumptions, we associate to each such structure a bilinear form, which allows us to reduce the classification problem to that of symmetric bilinear forms over specific rings.

We first deal with the case where R is the finite field $\mathbb{F}_{p^k}$, with p an odd prime; then we turn to the case where R is the ring of p-adic integers $\mathbb{Z}_p$.

We emphasize that the techniques employed in this part of the work closely parallel those developed in [23] in characteristic 2. In particular, we make use of what they (as well as we) refer to as the *defining matrix* of a brace (see Definition 4.2.5); this construction allows us to associate a bilinear form to the brace and subsequently derive a classification up to isomorphism or isoclinism.

4.1 Free Module Braces over a Commutative Ring

Let n be a positive integer and R a principal ideal domain. Consider

$$M = \bigoplus_{i=1}^{n} R, \tag{4.1}$$

the free module of rank n over R, and let $\{e_1, \dots, e_n\}$ be a fixed basis for M. Denote by $\mathrm{Aut}_R(M)$ the automorphism group of the R-module M, and by

$$\mathrm{Aff}(M) = \mathrm{Aut}_R(M) \ltimes M \tag{4.2}$$

the affine group of M. The automorphism group of M is given by

$$\mathrm{Aut}_R(M) = \mathrm{GL}_R(M),$$

which corresponds to the group of unimodular $n \times n$ matrices over R.

Let T_+ be the translation group of the additive group $(M, +)$. For $a \in M$, denote by σ_a the translation that sends 0 to a. Note that the addition on M can be defined via

$$a + b \coloneqq a\sigma_b \quad \text{for } a, b \in M,$$

so that $(M, +) \cong T_+$, and

$$\mathrm{Aff}(M, +) = \mathrm{Hol}(T_+) \cong N_{\mathrm{Sym}(M)}(T_+).$$

If $T_\circ$ is a regular, abelian subgroup of $\mathrm{Aff}(M)$, we can index its elements by the elements of M as

$$T_\circ = \{\tau_a \mid a \in M\},$$

where τ_a is the unique permutation in $T_\circ$ sending 0 to a. By Equation (4.2), each $\tau_a \in T_\circ$ can be uniquely expressed as

$$\tau_a = \gamma_a \sigma_a, \quad \text{with } \gamma_a \in \mathrm{GL}_R(M). \tag{4.3}$$

We define a binary operation $\circ$ on M by

$$a \circ b \coloneqq a\tau_b, \tag{4.4}$$

which endows M with the structure of an abelian regular group $(M, \circ)$ isomorphic to $T_\circ$.

Moreover, for each $a \in M$, define the endomorphism $\delta_a = \gamma_a - \mathbb{1}_M$ of $(M, +)$. Using δ_a, we define a multiplication on M by

$$a \cdot b := a\delta_b \quad \text{for all } a, b \in M. \tag{4.5}$$

In the rest of this chapter, by an *algebra over a ring* R we mean a commutative R-algebra of finite rank as an R-module.

Theorem 4.1.1. *The triple $(M, +, \cdot)$ is a commutative, associative R-algebra such that the resulting ring is radical.*

Proof. The result follows immediately from Corollary 1.3.11, since $(M, \circ)$ is a group. □

In order to endow $(M, +, \circ)$ with a bi-brace structure, we will assume the following condition for the rest of the chapter.

Assumption 4.1.2. $T_+ < \mathrm{Aff}(M, \circ) \cong N_{\mathrm{Sym}(M)}(T_\circ)$.

In [18], the authors prove that for every $a, b \in M$, the commutator $[\sigma_a, \tau_b]$ equals $\sigma_{a\cdot b}$. It follows that

$$T_+ < \mathrm{AGL}(M, \circ) \quad \Longleftrightarrow \quad \sigma_{a\cdot b} \in T_\circ.$$

Therefore,

$$\sigma_{a\cdot b} \in T_\circ \cap T_+ = \{\sigma_x \mid x \in \mathrm{Ann}(M)\},$$

where $\mathrm{Ann}(M) = \{a \in M \mid a \cdot M = 0\}$ denotes the annihilator of the algebra $(M, +, \cdot)$. Hence,

$$T_+ < \mathrm{AGL}(M, \circ) \quad \Longleftrightarrow \quad M^3 = \{0\}.$$

As a consequence, we obtain

$$\gamma_{a\cdot b} = \mathbb{1}_M \quad \text{for all } a, b \in M,$$

and thus,

$$\gamma_{a+b} = \gamma_{a\circ b} = \gamma_a\gamma_b.$$

Indeed, for all $a, b, c \in M$, on the one hand we have:

$$\begin{aligned}\gamma_{a+b}(c) &= -a - b + (a + b) \circ c \\ &= c + a \cdot c + b \cdot c,\end{aligned}$$

and on the other hand:

$$\begin{aligned}\gamma_{a\circ b}(c) &= -(a \circ b) + c \circ (a \circ b) \\ &= -(a + b + a \cdot b) + c \circ (a + b + a \cdot b) \\ &= c + c \cdot a + c \cdot b.\end{aligned}$$

Thus, $T_+ < \mathrm{AGL}(M, \circ)$ if and only if $(M, +, \circ)$ is a bi-brace. In other words, we recover the following well-known result (see also [21, Proposition 4.1] for an alternative proof).

Proposition 4.1.3. *Let $(M, +, \cdot)$ be a nilpotent R-algebra. The triple $(M, +, \circ)$ is a bi-brace if and only if $M^3 = 0$.*

Let $\mathrm{Ann}(M)$ denote the annihilator of the bi-brace $(M, +, \circ)$ (which coincides with the annihilator of the algebra $(M, +, \cdot)$). Since M is 3-nilpotent, we have:

$$M \cdot M \subseteq \mathrm{Ann}(M). \tag{4.6}$$

4.2 The Bilinear Form associated to $(M, +, \circ)$

In this section, we introduce a bilinear form associated with the bi-brace $(M, +, \circ)$, with the aim of classifying such structures using the known classification of bilinear forms up to equivalence (initially over fields of odd characteristic, and later, as we will see, over the ring of p-adic integers). From this point on, we will restrict our attention to those structures that satisfy the following assumption.

Assumption 4.2.1. $M \cdot M$ is a cyclic R-submodule of M.

Since R is a principal ideal domain, if $M \cdot M$ is a cyclic submodule of the free R-module M, then $M \cdot M \cong R$ as a R-module.

Let $(M, +, \cdot)$ be a torsion-free, commutative, 3-nilpotent R-algebra such that $M \cdot M$ is a cyclic R-submodule of M. As shown in the previous section, M inherits

a bi-brace structure from the algebra $(M, +, \cdot)$. We will refer to this structure as a *torsion-free cyclic-square R-bi-brace*.

Let us define the symmetric bilinear form

$$b : M \times M \longmapsto \mathrm{Ann}(M),\ (a, b) \mapsto a \cdot b. \tag{4.7}$$

Notice that the radical $\mathrm{Rad}_M(b) = \{a \in M \mid b(a, M) = 0\}$ of the bilinear form b coincides with $\mathrm{Ann}(M)$. Moreover, $\mathrm{Rad}(M)$ is a submodule of the free module M, so it is also free, say of rank d. As shown in Chapter 8 of [39], we can find a basis for M such that $\mathrm{Rad}(M)$ is spanned by the last d vectors of that basis. Without loss of generality, we may assume

$$\mathrm{Ann}(M) = \mathrm{span}_R\{e_{m+1}, \ldots, e_n\}, \quad m := n - d. \tag{4.8}$$

The next result relates the matrix associated to the bilinear form b with the linear maps described in (4.3).

Lemma 4.2.2. *There exists a $m \times d$ matrix Θ_i with entries in R such that γ_{e_i} has the form*

$$\gamma_{e_i} = \begin{pmatrix} \mathbb{1}_m & \Theta_i \\ 0_{d\times m} & \mathbb{1}_d \end{pmatrix} \quad \textit{for } i = 1, \ldots, m.$$

Moreover $\Theta_i = 0_{m\times d}$ for $i = m + 1, \ldots, n$.

Proof. Notice that $a \in \mathrm{Ann}(M)$ if and only if $a \circ b = a + b$ for all $b \in M$. It follows that $e_j \circ e_i = e_j + e_i$ for $j = m + 1, \ldots, n$ and $i = 1, \ldots, n$. In other words

$$e_j \circ e_i = e_j\gamma_{e_i} + e_i = e_j + e_i. \tag{4.9}$$

On the other hand for $j = 1, \ldots, m$ and $i = 1, \ldots, m$

$$e_j \circ e_i = e_j\gamma_{e_i} + e_i = e_j + e_i + e_j \cdot e_i \tag{4.10}$$

where $e_j \cdot e_i \in \mathrm{Ann}(M) = \mathrm{span}\{e_{m+1}, \ldots, e_n\}$. Thus, by Equation (4.9) and (4.10) we obtain

$$\gamma_{e_i} = \begin{pmatrix} \mathbb{1}_m & \Theta_{e_i} \\ 0 & \mathbb{1}_d \end{pmatrix} \text{ for } i = 1, \ldots, m$$

and $\gamma_{e_i} = \mathbb{1}_n$ for $i = m + 1, \ldots, n$. □

Remark 4.2.3. Denoting by $\Theta_{i,j}$ the *j-th* row of the matrix Θ_i, we get that

$$e_i \cdot e_j = (\underbrace{0, \dots, 0}_{m}, \Theta_{i,j})$$

and so

$$\gamma_a = \begin{pmatrix} \mathbb{1}_m & a_1\Theta_{e_1} + \cdots + a_m\Theta_{e_m} \\ 0 & \mathbb{1}_d \end{pmatrix}$$

for each $a = a_1e_1 + \cdots + a_ne_n \in M$.

Remark 4.2.4. By Equation (4.6), $\mathrm{Ann}(M) = H \oplus K$, where K is a cyclic R-module containing $M \cdot M$. Up to considering the quotient $(M/H, +, \cdot)$, we can assume $M \cdot M = c \cdot \mathrm{Ann}(M)$, with $c \in R$ and $\mathrm{Ann}(M) = \mathrm{span}\{e_n\}$ the sub-brace spanned over R by the last vector of the basis. Therefore, we will consider $m = n - 1$, $M \cdot M = c \cdot \mathrm{span}\{e_n\}$ and $M = N \oplus \mathrm{Ann}(M)$ where $N = \mathrm{span}\{e_1, \dots, e_{n-1}\}$.

Definition 4.2.5. We shall say that the matrix $\Theta := [\Theta_1 \dots \Theta_{n-1}]$ is the *defining matrix* in the given basis of the bi-brace $(M, +, \circ)$.

We notice that the matrix $\Theta = [\Theta_1 \dots \Theta_{n-1}]$ is the matrix associated to the symmetric bilinear form b restricted to the submodule N defined in Remark 4.2.4.

Lemma 4.2.6. *The matrix* Θ *is symmetric of maximal rank.*

Proof. By construction we have that $e_i \cdot e_j = e_j \cdot e_i$ for every $i, j \in \{1, \dots, n\}$ and applying Remark 4.2.3 we get that the matrix Θ is symmetric.

Let us suppose that a non-trivial linear combination of the column vectors $\Theta_1, \dots, \Theta_{n-1}$ is the null vector, i.e.

$$\sum_{i=1}^{n-1} a_i\Theta_i = 0 \qquad a_i \in R \text{ and } a_s \neq 0 \text{ for some } s \in \{1, \dots, n-1\}.$$

Then

$$\gamma_{a_1e_1+\cdots+a_{n-1}e_{n-1}} = \begin{pmatrix} \mathbb{1}_{n-1} & a_1\Theta_1 + \cdots + a_{n-1}\Theta_{n-1} \\ 0 & 1 \end{pmatrix} = \mathbb{1}_n$$

This means that $a_1e_1 + \cdots + a_{n-1}e_{n-1} \in \mathrm{Ann}(M) \cap N = \{0\}$. □

Conversely we have the following result.

Theorem 4.2.7. *Any $(n-1) \times (n-1)$ symmetric matrix with coefficients in R of maximal rank is the defining matrix (with respect to a suitable basis) of torsion-free cyclic-square R-bi-brace.*

Proof. Let $\Theta = [\Theta_1, \dots, \Theta_{n-1}]$ be a $(n-1) \times (n-1)$ symmetric matrix with coefficients in R of maximal rank and let $(M, +)$ be a free R-module of rank n. For $a = a_1 e_1 + \cdots + a_n e_n \in M$, let us define the map $\tau_a = \gamma_a \sigma_a$ where

$$\gamma_a = \begin{pmatrix} \mathbb{1}_{n-1} & a_1\Theta_1 + \cdots + a_{n-1}\Theta_{n-1} \\ 0 & 1 \end{pmatrix},$$

and σ_a is a translation of $(M, +)$. Set $T_\circ = \{\tau_a : \ a \in M\} < \mathrm{Aff}(M)$, where $\circ$ is the operation induced by $T_\circ$ on M as in Equation (4.4).

By Theorem 1.6.4, in order to prove that $(M, +, \circ)$ is a bi-brace, it is enough to prove that $T_\circ$ is an abelian regular subgroup of $\mathrm{Aff}(M)$ normalized by T_+. Let $\cdot$ be as in (4.5), the algebra $(M, +, \cdot)$ is torsion-free and cyclic square by construction.

- $T_\circ$ is a group, indeed $\tau_0 = \mathbb{1}_M$ is the neutral element and $\circ$ is associative by definition. Notice that $\tau_a \tau_b = \tau_{a \circ b}$, indeed

  $$x\tau_a\tau_b = x\gamma_a\gamma_b + a\gamma_b + b = x\gamma_a\gamma_b + a \circ b$$

  and since $a \circ b = a + b + a \cdot b$ and $\gamma_{a \cdot b} = \mathbb{1}_n$

  $$x\tau_{a\circ b} = x\gamma_{a\circ b} + a \circ b = x\gamma_{a+b} + a \circ b = x\gamma_a\gamma_b + a \circ b.$$

  Thus, to prove that every element of $T_\circ$ admits an inverse, we just have to prove that each $a \in M$ admits an inverse with respect to the $\circ$ operation. In other words, if $a = (a_1, \dots, a_n) \in M$, then we have to find $b \in M$ such that $a \circ b = 0$, i.e $a + b + a \cdot b = a \circ b = 0$. By Remark 4.2.4, $M \cdot M$ has rank 1 and is spanned by e_n, so $b = (-a_1, \dots, -a_{n-1}, b_n)$. It remains to find the last component b_n, that is

  $$\begin{aligned} b_n e_n &= -(a_1, \dots, a_n) \cdot (-a_1, \dots, -a_{n-1}, b_n) - a_n e_n \\ &= ((a_1, \dots, a_{n-1})\Theta(a_1, \dots, a_{n-1})^{tr} - a_n)e_n. \end{aligned}$$

- $T_\circ$ is abelian, indeed by definition $a \circ b = b \circ a$ and we have just seen that $\tau_a\tau_b = \tau_{a\circ b}$.

- $T_\circ$ is regular, i.e. for all $a, b \in M$ there exists a unique $c \in M$ such that $a\tau_c = b$. For proving this, it is enough to observe that $c = b\tau_a^{-1}$, where the uniqueness of c follows from the uniqueness of the inverse in $T_\circ$.

- T_+ normalises $T_\circ$, i.e., for all $a, b \in M$, $\sigma_a\tau_b\sigma_a^{-1} \in T_\circ$. Indeed, using the equality $\gamma_a\gamma_b = \gamma_{a\gamma_b+b}$, it follows that

$$\begin{aligned} x\sigma_a\tau_b\sigma_{-a} &= (x+a)\gamma_b\sigma_b\sigma_{-a} \\ &= x\gamma_b + a\gamma_b + b - a \\ &= x\gamma_a\gamma_b\gamma_{-a} + a\gamma_b + b - a \\ &= x\tau_{a\gamma_b+b-a}. \end{aligned}$$

□

4.3 The Case $R = \mathbb{F}_{p^k}$

In this section, we aim to study the case where $M = V$ is a vector space of dimension $n \geq 2$ over the field $\mathbb{F}_{p^k}$ with p^k elements and p an odd prime.

Let V be an n-dimensional vector space over $\mathbb{F}_{p^k}$ with basis $\{e_1, \ldots, e_n\}$. Let $\circ$ and $\cdot$ be as defined in Equations (4.4) and (4.5). Note that, in this case, Assumption 4.2.1 translates into requiring that $V \cdot V$ be a one-dimensional subspace of V. We will refer to the bi-brace $(V, +, \circ)$ as a $\mathbb{F}_{p^k}$-bi-brace with one-dimensional product space. Let us consider b the symmetric bilinear form associated to the bi-brace $(V, +, \circ)$.

Remark 4.3.1. Let the annihilator $\mathrm{Ann}(V)$ of V be a d-dimensional subspace of V. Since $V \cdot V$ is contained in $\mathrm{Ann}(V)$, we get that

$$\mathrm{Ann}(V) = (V \cdot V) \oplus H$$

for a suitable $(d-1)$-dimensional subspace H of V. Thus, up to considering the quotient algebra $(V/H, +, \cdot)$, we may assume that the subspace $V \cdot V$ coincides with $\mathrm{Ann}(V)$ and that it is spanned by the vector e_n. We obtain the following decomposition of V

$$V = W \oplus (V \cdot V)$$

where $V \cdot V = \mathrm{span}\{e_n\}$.

The defining matrix $\Theta = [\Theta_1, \ldots, \Theta_{n-1}]$ is the matrix associated with the bilinear form b restricted to the subspace W of V, as defined in Remark 4.3.1.

Remark 4.3.2. The defining matrix Θ of $(V, +, \circ)$ is an $(n-1) \times (n-1)$ invertible matrix with coefficients in $\mathbb{F}_{p^k}$.

We denote by $\mathbb{F}_{p^k}^{\times}$ the set of invertible elements of $\mathbb{F}_{p^k}$. We need to recall a couple of well-known results concerning the classification of symmetric bilinear forms over a field of odd characteristic.

Definition 4.3.3. Let b be a nondegenerate symmetric bilinear form on a $\mathbb{F}_{p^k}$-vector space with associated matrix B. The discriminant of b, denoted by $d(B)$, is defined to be the coset $\det(B)(\mathbb{F}_{p^k}^{\times})^2$ in $\mathbb{F}_{p^k}^{\times}/(\mathbb{F}_{p^k}^{\times})^2$.

Theorem 4.3.4. *[43, Proposition 5, pg. 34] Let b be a nondegenerate symmetric bilinear form on a $\mathbb{F}_{p^k}$-vector space V of dimension strictly bigger than 1, then there exists a basis for V such that the matrix B associated to b has one of the following non-equivalent diagonal forms*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \quad or \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & q \end{bmatrix},$$

where q is a non-square element of $\mathbb{F}_{p^k}$.

Corollary 4.3.5. *[43, Corollary of Proposition 5, pg. 35] For two nondegenerate symmetric bilinear forms over $\mathbb{F}_{p^k}$ to be equivalent it is necessary and sufficient that they have the same rank and same discriminant.*

A straight consequence of the previous corollary is the following result which gives a relationship between isomorphism classes $\mathbb{F}_{p^k}$-bi-braces with one-dimensional product space and equivalence classes of the associated bilinear forms.

Let A be any matrix. We shall denote by A^{tr} the transpose of the matrix A.

Theorem 4.3.6. *Let $V_1 = (V, +, \circ_1)$ and $V_2 = (V, +, \circ_2)$ be two $\mathbb{F}_{p^k}$-bi-braces with one-dimensional product space. Suppose that $V \cdot_1 V = V \cdot_2 V = \operatorname{span}\{e_n\}$. A matrix*

of the form

$$\begin{pmatrix} A & 0 \\ 0 & l \end{pmatrix}, \quad A \in GL(n-1, p^k),\ l \in \{1, q\}$$

is an isomorphism between $(V, +, \circ_1)$ *and* $(V, +, \circ_2)$ *if and only if*

$$A\Theta_{V_1}A^{tr} = l\Theta_{V_2}, \tag{4.11}$$

where Θ_{V_1} *and* Θ_{V_2} *are the defining matrices of* $(V, +, \circ_1)$ *and* $(V, +, \circ_2)$*, respectively, and* q *is a non-square element of* $\mathbb{F}_{p^k}^{\times}$*.*

We are now ready to give a complete classification of the isomorphism classes of $\mathbb{F}_{p^k}$-bi-braces with one-dimensional product space.

Theorem 4.3.7. *Let* $(V, +, \circ)$ *be a* $\mathbb{F}_{p^k}$*-bi-brace with one-dimensional product space. There are two isomorphism classes of* $(V, +, \circ)$ *if* $n-1$ *is even and there is one class is* $n-1$ *is odd.*

Proof. By Theorem 4.3.4, it suffices to consider the matrices

$$\Theta^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \ \Theta^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & q \end{bmatrix}$$

where q is a non-square element of $\mathbb{F}_{p^k}^{\times}$. By Proposition 4.3.6, we left to check whether Θ^1 and $q\Theta^2$ represent equivalent bilinear forms.

- If $n-1$ is even, then $\det(\Theta^1) = 1$ is a square, while $\det(q\Theta^2) = q^n$ is not a square. Then Θ^1 and $q\Theta^2$ are not congruent.
- If $n-1$ is odd, then $\det(\Theta^1) = 1$ is a square and $\det(q\Theta^2) = q^n$ is a square. Then Θ^1 and $q\Theta^2$ are congruent. □

We notice that the isomorphism classes of $(V, +, \cdot)$ are in one to one correspondence to the isomorphism classes of V/H as defined in Remark 4.2.4. In other words, the results obtained so far also hold in the case of an algebra $(V, +, \cdot)$, where $V \cdot V$ is one-dimensional and $\mathrm{Ann}(V)$ has arbitrary dimension.

4.4 The Case $R = \mathbb{Z}_p$ (Torsion Free)

We now consider the case where $R = \mathbb{Z}_p$, the ring of p-adic integers. We begin by recalling an important decomposition of a bilinear form defined over a $\mathbb{Z}_p$-module.

Definition 4.4.1. Let $(B, +, \circ)$ be a brace with associated gamma function $\gamma\colon B \to \mathrm{Aut}(B)$. Assume that $(B, +)$ has a structure of left (right) module over some ring R. We say that $(B, +, \circ)$ is a left (right) *module brace over* R, or simply R-brace, if $\gamma(B) \subseteq \mathrm{Aut}_R(B)$.

It is worth highlighting that if $(B, +, \circ)$ is a two-sided brace, the notion of R-brace coincides with the classical notion of R-module (see Example 2 in [26]). We will see that the classification of torsion-free cyclic square $\mathbb{Z}_p$-bi-braces closely resembles the one obtained for vector spaces over fields of odd characteristic.

Definition 4.4.2. Let $b\colon M \times M \to \mathbb{Z}_p$ be a symmetric bilinear form on a free $\mathbb{Z}_p$-module. We say that b is a p-adic unit form if its determinant is a unit in $\mathbb{Z}_p$. Otherwise, we say that b is a p-adic degenerate form.

For a proof of the following result see Chapter 15, Theorem 2 of [24] or Chapter 9 of [39]

Theorem 4.4.3. *For $p \neq 2$, any p-adically integral form can be diagonalized by a p-adically integral transformation. In particular, a p-adic unit form is uniquely determined up to equivalence by its discriminant and its rank.*

As a consequence of that we get the so called *Jordan decomposition*. Let $b\colon M \times M \to \mathbb{Z}_p$ be any symmetric bilinear form on a free $\mathbb{Z}_p$-module. We can decompose b as a direct sum

$$b_1 \oplus pb_p \oplus p^2 b_{p^2} \oplus \dots \tag{4.12}$$

where each b_p is a p-adic unit form. We refer to each summand $p^i b_{p^i}$ as the i-th Jordan constituent of b and to the scalar p^i as the *scale* of that Jordan constituent.

Definition 4.4.4. The *scale* of (M, b), denoted by $\mathfrak{s}((M, b))$ (or simply $\mathfrak{s}(M)$), is the principal ideal in $\mathbb{Z}_p$ generated by the subset $b(M, M)$.

Remark 4.4.5. The collection of the powers p^i appearing in the decomposition (4.12), together with the ranks and discriminants of the corresponding p-adic unit forms b_{p^i}, form a complete set of invariants for the bilinear form b.

We obtain the following as an immediate consequence.

Corollary 4.4.6. *Let Θ be the defining matrix of a torsion-free cyclic square $\mathbb{Z}_p$-bi-brace. Then, there exists a p-adically integral transformation which diagonalizes Θ into*

$$\begin{pmatrix} J_{i_1}(\varepsilon_1) & 0 & 0 & 0 \\ 0 & J_{i_2}(\varepsilon_2) & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & J_{i_t}(\varepsilon_t) \end{pmatrix}$$

where $J_{i_j}(\varepsilon_j) = p^{i_j} \begin{pmatrix} \mathbb{1} & 0 \\ 0 & \varepsilon_j \end{pmatrix}$ and the scalars ε_j take values in $\{1, q\}$ where q is a non-square element of $\mathbb{Z}_p$.

The following two results are the analogous of Theorem 4.3.6 and Theorem 4.3.7 of the previous section.

Proposition 4.4.7. *Two torsion-free cyclic square $\mathbb{Z}_p$-bi-braces $M_1 = (M, +, \circ_1)$ and $M_2 = (M, +, \circ_2)$ with defining matrices Θ_{M_1} and Θ_{M_2}, respectively, are isomorphic if and only if there exists a p-adic unimodular $(n-1) \times (n-1)$ matrix A such that*

$$A\Theta_{M_1}A^{tr} = \varepsilon\Theta_{M_2}$$

where $\varepsilon \in \{1, q\}$ and q is a non-square element of $\mathbb{Z}_p$.

Theorem 4.4.8. *Let $(M, +, \circ)$ be a torsion-free cyclic-square $\mathbb{Z}_p$-bi-brace with $\mathrm{Ann}(M)$ of rank d. If the defining matrix Θ of M is unimodular, then there are two isomorphism classes of M when $n - d$ is even, and one isomorphism class when $n - d$ is odd. Moreover, if $n - d$ is even the isomorphism classes are determined by the discriminant $d(\Theta)$ of Θ.*

Remark 4.4.9. In general, the defining matrix of a torsion-free cyclic-square $\mathbb{Z}_p$-bi-brace is not unimodular and there are infinitely many isomorphism classes. Indeed,

counting the isomorphism classes of such bi-brace is equivalent to count all the possible Jordan decompositions of a $n \times n$ symmetric matrix over $\mathbb{Z}_p$. There are infinitely many such decompositions, as the set of possible scales for the Jordan blocks is infinite.

Moreover, let I be an isomorphism class of a torsion-free cyclic-square $\mathbb{Z}_p$-bi-brace and let Θ be the defining matrix (represented in its Jordan form) of a bi-brace in that class. We note that if Θ has at least one Jordan constituent of odd rank, then $|I| = 2$, otherwise $|I| = 1$.

4.5 The Case $R = \mathbb{Z}_p$ (Torsion Case)

In this section, we study the case in which the module M has torsion. We obtain a classification of cyclic-square $\mathbb{Z}_p$-bi-braces up to isoclinism.

We begin by introducing the definition of isoclinism between bi-braces. Note that, in our case, the additive part of the bi-brace is commutative, and the definition coincides with that of isoclinism between R-algebras.

Definition 4.5.1. [36] We shall say that two R-bi-braces M and N are isoclinic if there exist two isomorphisms

$$\psi\colon M/\operatorname{Ann}(M) \to N/\operatorname{Ann}(N) \quad \text{and} \quad \varphi\colon M \cdot M \to N \cdot N$$

such that the following diagram commutes

$$\begin{array}{ccc} M/\operatorname{Ann}(M) \times M/\operatorname{Ann}(M) & \xrightarrow{\psi\times\psi} & N/\operatorname{Ann}(N) \times N/\operatorname{Ann}(N) \\ \downarrow{\scriptstyle (\,\cdot\,)} & & \downarrow{\scriptstyle (\,\cdot\,)} \\ M \cdot M & \xrightarrow{\qquad\varphi\qquad} & N \cdot N \end{array}$$

Isoclinism is an equivalence relation among R-bi-braces. We shall say that a bi-brace M is *stem* if $Ann(M) \subseteq M \cdot M$. For two isoclinic algebras M and N, we shall write $M \sim N$.

According to P.Hall [32], we provide the following characterization.

Lemma 4.5.2. *Let M be an R-bi-brace, $N \subseteq M$ a subalgebra and $I \subseteq \operatorname{Ann}(M)$ an ideal of M such that $I \cap (M \cdot M) = \{0\}$. Then*

- $M \sim M \oplus T$, *where* T *is any algebra such that* $T \cdot T = 0$*;*
- $M \sim M/I$*;*
- $M \sim N$ *if and only if* $M = N + \operatorname{Ann}(M)$*.*

For a proof of the following result see [36, Theorem 2.18].

Theorem 4.5.3. *Every R-bi-brace is isoclinic to a stem brace.*

Definition 4.5.4. Let M and N be two R-bi-braces and let $b\colon M \times M \to N$ be a R-bilinear form such that $N = \langle b(M, M)\rangle$. We define the R-bi-brace

$$(\operatorname{Stem}(b), +, \circ) = ((M/\operatorname{Ann}(M)) \oplus N, +, \circ)$$

where $\circ$ is defined as in Equation (1.15) and $\cdot$ is defined as follows

$$(m_1, n_1) \cdot (m_2, n_2) = (0, b(m_1, m_2)) \text{ for all } m_1, m_2 \in M \text{ and } n_1, n_2 \in N.$$

We now come back to the case $R = \mathbb{Z}_p$ and M a $\mathbb{Z}_p$-module with torsion.

Due to the torsion assumption, the module $M \cdot M$ is a finite cyclic $\mathbb{Z}_p$-submodule of M and $M/\operatorname{Ann}(M)$ is a finite $\mathbb{Z}_p$-module. In particular $M \cdot M \cong \mathbb{Z}_p/p^t\mathbb{Z}_p$ for some $t > 0$.

For any finitely-generated free $\mathbb{Z}_p$-module $\bar{M}$ having $M/\operatorname{Ann}(M)$ as a quotient and projection $\pi\colon \bar{M} \to M/\operatorname{Ann}(M)$, there exists a bilinear form $\bar{b}$ such that the following diagram

$$\begin{array}{ccc} \bar{M}^2 & \xrightarrow{\pi} & (M/\mathrm{Ann}(M))^2 \\ \downarrow{\scriptstyle \bar{b}} & & \downarrow{\scriptstyle b} \\ \mathbb{Z}_p & \xrightarrow{\text{mod } p^t} & M \cdot M \end{array}$$

commutes. The couple $(\bar{M}, \bar{b})$ is said to be a *covering* of (M, b), and $\bar{b}$ is said to be a *lifting* of b. We point out that there are actually infinitely many coverings of M. Observe that $\bar{b}_1$ and $\bar{b}_2$ are two symmetric bilinear forms on $\bar{M}$ turning the previous diagram into a commutative diagram if and only if there exists another bilinear form $\bar{b}_3$ over $\bar{M}$ such that

$$\bar{b}_1 - \alpha\bar{b}_2 = p^t\bar{b}_3,$$

where α is an invertible element of $\mathbb{Z}_p$. We denote by $[b]$ the equivalence class of lattices that are covering of M.

Remark 4.5.5. There exist infinitely many non-degenerate liftings of b. Indeed, let $\bar{b}\colon \bar{M} \times \bar{M} \to \mathbb{Z}_p$ be a symmetric lifting of b with associated matrix $\bar{B}$, then the symmetric lifting with associated matrix $\bar{B} - p^h \mathbb{1}_n$, for p^h not an eigenvalue of $\bar{B}$, and $h \geq t$, provides a non-degenerate covering in the same class.

We now introduce an equivalence relation between lattices.

Definition 4.5.6. Two lattices (M, b_M) and (N, b_N) are said to be p^t-*equivalent*, denoted by

$$(M, b_M) \sim_{p^t} (N, b_N),$$

, if there exists $\alpha \in \mathbb{Z}_p^\times$ and two lattices (P_1, g_1) and (P_2, g_2) with $\mathfrak{s}(P_1) = \mathfrak{s}(P_2) = (p^t)$, such that

$$(M, b_M) \perp (P_1, g_1) \cong (N, \alpha b_N) \perp (P_2, g_2).$$

Remark 4.5.7. We observe that $M \sim_{p^t} M'$ if and only if the bilinear forms b and b', respectively of M and M', have proportional Jordan decomposition modulo p^t, in other words, if there exists $\alpha \in \mathbb{Z}_p^\times$ such that

$$(b_1, \ldots, b_{t-1}) \cong \alpha(b'_1, \ldots, b'_{t-1}).$$

With an abuse of language we write $\mathrm{rk}(b_l)$ to denote the rank n_l of the lattice (M_l, b_l).

By the previous remark, using the same notation, the next result follows immediately.

Proposition 4.5.8. *If two coverings $(\bar{M}, \bar{b})$ and $(\bar{N}, \bar{g})$ with Jordan decompositions modulo p^t respectively $(\bar{b}_1, \ldots, \bar{b}_{t-1})$ and $(\bar{g}_1, \ldots, \bar{g}_{t-1})$ are in $[b]$ for some b, then*

1. $\mathrm{rk}(\bar{b}_i) = \mathrm{rk}(\bar{g}_i)$ *for each* $i = 1, \ldots, t-1$, *and*
2. $\bar{b}_i = \bar{g}_i$ *if* $\mathrm{rk}(\bar{b}_i) = \mathrm{rk}(\bar{g}_i)$ *is even.*

Proof. We have already observed that two coverings of M are p^t-equivalent. It follows that $(\bar{b}_1, \ldots, \bar{b}_{t-1}) \cong \alpha(\bar{g}_1, \ldots, \bar{g}_{t-1})$ for some $\alpha \in \mathbb{Z}_p^\times$. Therefore, the ranks must satisfy $\mathrm{rk}(\bar{b}_i) = \mathrm{rk}(\bar{g}_i)$ for each $i = 1, \ldots, t-1$.

Moreover, since multiplication by a unit α does not affect the discriminant of Jordan blocks of even rank, it follows that $\bar{b}_i = \bar{g}_i$ whenever $\mathrm{rk}(\bar{b}_i) = \mathrm{rk}(\bar{g}_i)$ is even. □

We consider now a symmetric bilinear form $\bar{b}\colon \bar{M} \times \bar{M} \to \mathbb{Z}_p$ with p^t-radical $K = \{x \in \bar{M}\colon \bar{b}(x, y) \in p^t\mathbb{Z}_p, \text{ for all } y \in \bar{M}\}$, and $t > 0$ and we construct an algebra M whose product form b is such that $\bar{b} \in [b]$. Clearly K is determined by the Jordan splitting of $\bar{b}$, and it is equal to the orthogonal sum of the h-Jordan components with $h \geq t$. Let $\tilde{b}\colon \bar{M} \times \bar{M} \to \mathbb{Z}_p/p^t\mathbb{Z}_p$ be the reduction of $\bar{b}$ modulo p^t and let $M = \mathrm{Stem}(\tilde{b})$ be as in Definition 4.5.4. We have $\bar{M}/K \cong M/\operatorname{Ann}(M)$ and the following commutative diagram

$$\begin{array}{ccc} (\bar{M})^2 & \longrightarrow & (M/\operatorname{Ann}(M))^2 \\ \downarrow{\scriptstyle \bar{b}} & \searrow^{\tilde{b}} & \downarrow{\scriptstyle b} \\ \mathbb{Z}_p & \xrightarrow{\Theta} & \mathbb{Z}_p/p^t\mathbb{Z}_p \end{array}$$

where b is the symmetric bilinear form induced by the product in the algebra M.

Proposition 4.5.9. *The non-degenerate lattice $(\bar{M}, \bar{b})$ is the covering of any algebra in the isoclinism class of $M = \mathrm{Stem}(\bar{b} \bmod p^t)$.*

Proof. We define $K = \{x \in \bar{M}\colon \bar{b}(x, y) \in p^t\mathbb{Z}_p, \text{ for all } y \in \bar{M}\}$ and we note that $\bar{M}/K \cong M/\operatorname{Ann}(M)$. Let N be an algebra in the isoclinism class of M with ψ and φ isomorphisms as in Definition 4.5.1. It is possible to construct the following diagram

$$\begin{array}{ccccc} (\bar{M})^2 & \xrightarrow{\pi} & (\bar{M}/K)^2 \cong (M/\operatorname{Ann}(M))^2 & \xrightarrow{\psi\times\psi} & (N/\operatorname{Ann}(N))^2 \\ \downarrow{\scriptstyle \bar{b}} & & \downarrow{\scriptstyle b_M} & & \downarrow{\scriptstyle b_N} \\ \mathbb{Z}_p & \xrightarrow{\Theta} & \mathbb{Z}_p/p^t\mathbb{Z}_p \cong M \cdot M & \xrightarrow{\varphi} & N \cdot N \end{array} \tag{4.13}$$

where b_M and b_N are the bilinear maps associated to the products of M and N respectively. The statement follows since the previous diagram is commutative. □

Let $(M, +, \cdot)$ be a 3-nilpotent torsion $\mathbb{Z}_p$-algebra such that $M \cdot M \cong \mathbb{Z}_p/p^t\mathbb{Z}_p$, and let $(M, +, \circ)$ be the associated cyclic-square $\mathbb{Z}_p$-bi-brace. We prove that there are finitely many isoclinism classes of such bi-braces.

In the following statement, we set $\binom{a}{b} = 0$ whenever a is not a non-negative integer.

Theorem 4.5.10. *There are*

$$\sum_{s=1}^{t} \binom{t}{s} 2^{s-1} \left(\binom{n-1}{s-1} + \binom{n/2-1}{s-1} \right)$$

isoclinism classes of cyclic-square $\mathbb{Z}_p$-bi-braces of rank n.

Proof. We start by counting all possible Jordan splittings modulo p^t of a $\mathbb{Z}_p$-lattice.

All possible splittings of $(\bar{M}, \bar{b})$ into s components can be obtained by choosing s scales in $\binom{t}{s}$ ways. Multiplication by a non-square invertible element $\alpha \in \mathbb{Z}_p$ changes the discriminant of Jordan blocks of odd rank while leaving those of even rank unchanged.

Supposing that at least one of the involved ranks is odd, since the discriminant of each block can be chosen in two ways, we obtain

$$\sum_{s=1}^{t} \binom{t}{s} 2^{s-1} H(n, s)$$

possible non-equivalent Jordan splittings, where $H(n, s)$ is the number of decompositions $n = n_1 + n_2 + \cdots + n_s$ with each $n_i \geq 1$ and at least one n_i odd.

We also define $K(n, s)$ as the number of decompositions $n = n_1 + n_2 + \cdots + n_s$ with each $n_i \geq 1$. Finally, we consider the case when all ranks n_i, and in particular n, are even. Such a decomposition corresponds to doubling a decomposition of $n/2$ into s parts. There are $K(n/2, s)$ such decompositions, each carrying 2^s non-equivalent splittings. Hence, the total number of such splittings is

$$\sum_{s=1}^{t} \binom{t}{s} 2^{s-1} H(n, s) + \sum_{s=1}^{t} \binom{t}{s} 2^{s} K(n/2, s) =$$
$$\sum_{s=1}^{t} \binom{t}{s} 2^{s-1} K(n, s) + \sum_{s=1}^{t} \binom{t}{s} 2^{s-1} K(n/2, s).$$

It is well known that $K(n, s) = \binom{n-1}{s-1}$, concluding the proof. □

Appendices

APPENDIX A

APPENDIX

A.1 Imprimitivity Chain

We refer the reader to [47] for the following definitions and results. A permutation group G on Ω is called *semiregular* if for each $\alpha \in \Omega$ the only permutation of G that fixes α is the identity permutation 1. The group G is said to be *regular* if it is semiregular and transitive (i.e., if it has only one orbit on Ω).

Lemma A.1.1. *All orbits of a semiregular group G have the same length, namely, the cardinality of G.*

As a consequence a group G that acts regularly on Ω is such that $|G| = |\Omega|$.

Definition A.1.2. Let G be a permutation group on non-empty set Ω. We call a subset Γ of Ω a block of G if for each $g \in G$ the image set Γ^g either coincides with Γ or is disjoint from Γ.

Notice that the whole set Ω, the empty set $\emptyset$ and the subsets of Ω consisting of only one point are blocks of G. Moreover, if $U \leq G$ and Γ is a block for G, then Γ is a block for U.

Lemma A.1.3. *If Γ is a block for $U \leq G$, then Γ^g is a block for $g^{-1}Ug$.*

From this it follows that if Γ is a block of G then for each $g \in G$, Γ^g is also a block of G. Two such blocks are called conjugate. Any two conjugate blocks are

equal or disjoint. The totality of all blocks conjugate to a block Γ of G form a complete block system. All blocks of a complete block system have the same length. If G is transitive on Ω, the union of the members of a complete block system of G is Ω. It follows that the length of a block of a transitive group G is a divisor of $|G|$.

A transitive group G is called imprimitive if there is at least one nontrivial block Γ (i.e., $\Gamma \neq \emptyset, \{x\}, \Omega$). An imprimitivity system for G is a G-invariant partition of Ω.

Remark A.1.4. The group G is primitive if G has only the trivial partitions $\{\Omega\}$ and the set of the singletons of Ω as imprimitivity systems.

Definition A.1.5. Let G act imprimitively on the set Ω. An imprimitivity chain $\mathcal{B}_0 \succ \cdots \succ \mathcal{B}_t$ of depth t is a sequence of imprimitivity systems for G acting on Ω, where $\mathcal{B}_0$ and $\mathcal{B}_t$ are the trivial partitions. We also require that for each $B \in \mathcal{B}_{m+1}$ there exists $B' \in \mathcal{B}_m$ such that $B \subseteq B'$ for $0 \leq m \leq t-1$.

Example A.1.6. Let $G = \mathrm{Sym}(p^n)$ and $\Omega = \{1, \ldots, p^n\}$. For each integer $0 \leq m \leq n$ and for each $0 \leq k \leq p^m - 1$, we define the fundamental blocks

$$\Theta^n_{m,k} \coloneqq \{kp^{n-m} + 1, \ldots, (k+1)p^{n-m}\}$$

each of which with cardinality p^{n-m}. These blocks partition $\{1, \ldots, p^n\}$ into p^m blocks of equal size. Let Θ^n_m be the partition at the level m. That is,

$$\Theta^n_m \coloneqq \left\{\Theta^n_{m,0}, \ldots, \Theta^n_{m,p^m-1}\right\}.$$

This yields a chain of imprimitivity

$$\mathcal{C}_n \colon \Theta^n_0 \succ \cdots \succ \Theta^n_m \succ \cdots \succ \Theta^n_n$$

where $\Theta^n_0 = \{1, \ldots, p^n\}$ and $\Theta^n_n = \{\{1\}, \{2\}, \ldots, \{p^n\}\}$.

A.2 Transfinite Hypercentral Groups

Let G be a group. We define the terms of the upper central series of G by

$$Z_0(G) = 1 \quad \text{and} \quad Z_{\alpha+1}(G)/Z_\alpha(G) = Z(G/Z_\alpha(G)),$$

and, if α is a limit ordinal, by

$$Z_\alpha(G) = \bigcup_{\beta<\alpha} Z_\beta(G).$$

Equivalently and more conveniently for computations, one can write:

$$Z_\alpha(G) = \{g \in G \mid [g, z] \in Z_{\alpha-1}(G) \text{ for all } z \in Z_{\alpha-1}(G)\}$$

when α a non-limit ordinal.

A group G is called *transfinitely hypercentral* if $G = Z_\alpha(G)$ for some (possibly limit) ordinal α. For more details, see e.g. [41, Chapter 12].

A.3 Wreath Products

Let K and H be two groups acting on the sets Ξ and Γ, respectively. The *unrestricted wreath product* of the two permutation groups K and H is defined as

$$K \wr H \coloneqq \mathrm{Fun}(\Gamma, K) \rtimes H,$$

where $\mathrm{Fun}(\Gamma, K)$ denotes the group of functions from Γ to K, equipped with pointwise multiplication, i.e.,

$$(fg)(\gamma) = f(\gamma)g(\gamma) \quad \text{for all } \gamma \in \Gamma.$$

The group $\mathrm{Fun}(\Gamma, K)$ is referred to as the *base group* of the wreath product.

The group H acts on K^Γ via

$$f^h(\gamma) \coloneqq f(\gamma^{h^{-1}}), \quad \gamma \in \Gamma,\ h \in H.$$

The group operation in $K \wr H$ is then defined by

$$(f_1, h_1) \cdot (f_2, h_2) = \left(f_1 \cdot f_2^{h_1^{-1}},\ h_1 h_2\right).$$

In the case where H and K are arbitrary (not necessarily permutation) groups, they can be viewed as permutation groups acting on themselves via the right regular representation. In this setting, the wreath product $K \wr_H H$, usually denoted simply by $K \wr H$, is called the *standard wreath product*. For further details, see also e.g. [27, 41].

The following result has been proven by Kaloujnin and Krasner in [34].

Theorem A.3.1. *A Sylow p-subgroup of* $\mathrm{Sym}(p^n)$ *is isomorphic to the standard wreath product*

$$W_n = \mathbb{Z}/p\mathbb{Z} \wr \cdots \wr \mathbb{Z}/p\mathbb{Z},$$

where there are n factors.

Proof. We proceed by induction on n. The case $n = 0$ is trivial. Assume that $\mathrm{Sym}(p^n)$ has a Sylow p-subgroup P of the desired form. Consider the permutation $\pi \in \mathrm{Sym}(p^{n+1})$ defined by

$$\pi = (1,\ 1+p^n,\ \ldots,\ 1+(p-1)p^n)(2,\ 2+p^n,\ \ldots,\ 2+(p-1)p^n) \\ \ldots(p^n,\ 2p^n,\ \ldots,\ p^n+(p-1)p^n).$$

Note that $\pi^p = 1$. Moreover, while P acts on the set $\{1, \ldots, p^n\}$, the conjugates $P_i \coloneqq \pi^{-i} P \pi^i$ act on the pairwise disjoint subsets

$$\{1+ip^n,\ 2+ip^n,\ \ldots,\ p^n+ip^n\}$$

for $i = 0, \ldots, p-1$. Since the supports of the P_i are disjoint, they generate their direct product. Furthermore, it is possible to verify that

$$\pi^{-1} P_i \pi = P_{i+1}, \quad \text{and} \quad \pi^{-1} P_{p-1} \pi = P_0 = P.$$

Then the group $\langle P, \pi \rangle$ is isomorphic to $P^{\mathbb{Z}/p\mathbb{Z}} \rtimes \mathbb{Z}/p\mathbb{Z} = P \wr \mathbb{Z}/p\mathbb{Z}$. Furthermore, the order of this group is $|P|^p \cdot p = p^{1+p+\cdots+p^n}$, which coincides with the highest power of p dividing $(p^{n+1})!$. Hence, $\langle P, \pi \rangle$ is a Sylow p-subgroup of $\mathrm{Sym}(p^{n+1})$, completing the proof. □

A.4 Witt Algebras

In this section, we refer to [45]. Let $\mathcal{A}(n)$ denote the associative and commutative $\mathbb{F}_p$-algebra with unit, generated by elements $x_i^{(r)}$, for $i = 1, \ldots, n$ and $r \geq 0$, and relations

$$x_i^{(0)} = 1 \quad \text{and} \quad x_i^{(r)} x_i^{(s)} = \binom{r+s}{r} x_i^{(r+s)} \text{ for all } r, s \geq 0.$$

Denoting by $x^{(a)}$ the element $x_1^{(a_1)} \cdots x_m^{(a_m)}$ for $a \in \mathbb{N}^m$, a basis for $\mathcal{A}(n)$ is given by the set $\{x^{(a)} \mid 0 \leq |a|,\ a \in \mathbb{N}^n\}$, where $|a| = \sum_{i=1}^n a_i$. For each $j \geq 0$, we set

$$\mathcal{A}(n)_j := \operatorname{span}\{x^{(a)} \mid |a| \geq j\}.$$

Then $(\mathcal{A}(n)_j)_{j\geq 0}$ is a descending chain of ideals. Let $\underline{\mathrm{m}} = (m_1, \ldots, m_n) \in (\mathbb{N} \cup \{\infty\})^n$, we set

$$\mathcal{A}(n; \underline{\mathrm{m}}) = \operatorname{span}\left\{x^{(a)} \mid 0 \leq a_i \leq p^{m_i}\right\},$$

where $p^\infty := \infty$. For each $i = 1, \ldots, n$, we define a derivation ∂_i on $\mathcal{A}(n; \underline{\mathrm{m}})$ by setting

$$\partial_i(x_j^{(\ell)}) = \delta_{ij} x_i^{(\ell-1)}.$$

One can verify using Pascal's triangle that ∂_i is indeed a derivation. Moreover,

$$\partial_i(\mathcal{A}(n)_j) \subseteq \mathcal{A}(n)_{j-1}.$$

Define

$$W(n) := \sum_{i=1}^n \mathcal{A}(n)\partial_i, \qquad W(n; \underline{\mathrm{m}}) := \sum_{i=1}^n \mathcal{A}(n; \underline{\mathrm{m}})\partial_i. \tag{A.1}$$

These Lie algebras are called Witt algebras.

Remark A.4.1. The Lie algebra $\mathfrak{L}_n$, introduced in Chapter 2, is a subalgebra of $W(n; \underline{\mathrm{p}})$, where $\underline{\mathrm{p}} = (p, \ldots, p) \in \mathbb{N}^n$. The algebra $\mathfrak{L}_n$ has as a basis the monomial elements of the form

$$x_{i_1}^{\lambda_1} \cdots x_{i_h}^{\lambda_h} \partial_k,$$

where $1 \leq i_1 < i_2 < \cdots < i_h < k \leq n$. In our context, this corresponds to considering, in the k-th summand of the decomposition (A.1), only polynomials involving variables up to the $(k-1)$-th. Similarly, $\mathfrak{L}_n^\infty$ is a subalgebra of $W(n)$.

A.5 Difference Equations and Polynomials

Let D be an integral domain of characteristic zero and let R_j be as in Chapter 3. Let f be a function of $x = (x_1, \ldots, x_j)$. We recall that the operator $\Delta_i(h)\colon R_j \to R_j$ is defined as

$$\Delta_i(h)(f) = f(x + e_i h) - f(x)$$

for $i \leq j$ and $h \in D$. The result of performing this operation denoted by $\Delta_i(h)$ is still a function in R_j on which the operation may be repeated. We then obtain the second difference

$$\Delta_i(h)(\Delta_i(h)(f)) = f(x + 2e_ih) - 2f(x + e_ih) + f(x).$$

We denote the second difference by $\Delta_i(h)^2$. Proceeding in this way, we can form the n-th difference by means of the relation $\Delta_i(h)^n = \Delta_i(h)(\Delta_i(h)^{n-1}(f))$. For simplicity , let us consider now $f \in R_1$. As we did in Section 3.1, we define by $f_n = f(x + n) - f(x)$. Let $n \in \mathbb{Z}$. We want to find the solution of the following homogeneous difference equation

$$f_n(x) + c_1 f_{n-1}(x) + \cdots + c_n f(x) = 0 \tag{A.2}$$

with $c_1, \ldots, c_n \in F$ (the field of fractions of D). The classical way to obtain the general solution of this kind of equations is to set $f(x) = a^x$ and find the values of a for which the equation is satisfied. Substituting $f(x) = a^x$ in Equation A.2, we have

$$a^x(a^n + c_1 a^{n-1} + \cdots + c_n) = 0.$$

Therefore, if a^x is a solution, it is necessary that

$$a^n + c_1 a^{n-1} + \cdots + c_n = 0. \tag{A.3}$$

Conversely, if $a_1, \ldots, a_n$ are n distinct roots of Equation A.3, then $a_1^x, \ldots, a_n^x$ are solution of Equation A.2. So that

$$f(x) = k_1 a_1^x + \cdots + k_n a_n^x$$

is the general solution of Equation A.2. It may happen that Equation A.3 may have multiple roots. Supposing that $a_1 = a_2 = \cdots = a_\ell$, the general solution of Equation A.2 becomes

$$f(x) = (k_1 + k_2 x + \cdots + k_\ell x^{\ell-1})a_\ell^x + k_{\ell+1} a_{\ell+1}^x + \cdots + k_n a_n^x.$$

Although the following result is well known, we include a brief proof for the convenience of the reader.

Lemma A.5.1. *If $f \in \mathrm{Fun}(D, \mathbb{Z})$ then $\Delta_1(1)^k f = 0$ if and only if f is a polynomial of degree at most $k-1$.*

Proof. Let $f \in F[x]$ be a polynomial of degree at most $k-1$, then $f = \sum_{i=0}^{k-1} a_i x^i$. Thus

$$\begin{aligned} g(x) = \Delta_1(1) f(x) &= f(x+1) - f(x) \\ &= \sum_{i=0}^{k-1} a_i (x+1)^i - \sum_{i=0}^{k-1} a_i x^i \end{aligned}$$

is a polynomial of degree at most $k-2$. By induction $\Delta_1(1)^k f = \Delta_1(1)^{k-1} g = 0$.

Conversely, let $f : D \to \mathbb{Z}$ be such that $\Delta_1(1)^k(f) = 0$. Notice that

$$0 = \Delta_1(1)^k f(x) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i f(x+k-i)$$

is a homogeneous linear difference equation with constant coefficients (as in Equation A.2). The general solution is

$$f(x) = c_1 + c_2 x + \ldots + c_{k-1} x^{k-1},$$

where $c_i \in F$. □

The following statements are immediate consequences.

Corollary A.5.2. *$\Delta_1(1)^k f = c \neq 0$ if and only if f is a polynomial of degree k.*

Corollary A.5.3. *$\Delta_1(h)^k f = 0$, where $h \neq 0$, if and only if f is a polynomial of degree at most $k-1$.*

Corollary A.5.4. *Let $f \in \mathrm{Fun}(D^j, \mathbb{Z})$. Then $\Delta_i(h)^k f = 0$ if and only if f is a polynomial of degree at most $k-1$ with respect to the i-th variable.*

For a detailed reference on difference equations see [40].

ACKNOWLEDGMENTS

I would like to thank my two supervisors, Professor Riccardo Aragona and Professor Norberto Gavioli, for introducing me to the world of research, and for their constant support and kindness. Their professionalism is a model I aspire to follow in my academic future.

I also thank the referees for their careful reading of this work and for their valuable comments and suggestions, which significantly contributed to improving its quality.

Finally, I wish to thank Giulia, without whom this experience would not have been as beautiful as it was.

BIBLIOGRAPHY

[1] The On-Line Encyclopedia of Integer Sequences. Published electronically at https://oeis.org.

[2] Riccardo Aragona, Roberto Civino, and Norberto Gavioli. A modular idealizer chain and unrefinability of partitions with repeated parts. *Israel J. Math.*, 260(1):441–461, 2024. doi:10.1007/s11856-023-2559-8.

[3] Riccardo Aragona, Roberto Civino, and Norberto Gavioli. An ultimately periodic chain in the integral Lie ring of partitions. *J. Algebraic Combin.*, 59(4):939–954, 2024. doi:10.1007/s10801-024-01318-x.

[4] Riccardo Aragona, Roberto Civino, Norberto Gavioli, and Carlo Maria Scoppola. Regular subgroups with large intersection. *Ann. Mat. Pura Appl. (4)*, 198(6):2043–2057, 2019. doi:10.1007/s10231-019-00853-w.

[5] Riccardo Aragona, Roberto Civino, Norberto Gavioli, and Carlo Maria Scoppola. A chain of normalizers in the Sylow 2-subgroups of the symmetric group on 2^n letters. *Indian J. Pure Appl. Math.*, 52(3):735–746, 2021. doi:10.1007/s13226-021-00190-w.

[6] Riccardo Aragona, Roberto Civino, Norberto Gavioli, and Carlo Maria Scoppola. Rigid commutators and a normalizer chain. *Monatsh. Math.*, 196(3):431–455, 2021. doi:10.1007/s00605-021-01514-y.

[7] Riccardo Aragona, Roberto Civino, Norberto Gavioli, and Carlo Maria Scoppola. Unrefinable partitions into distinct parts in a normalizer chain. *Discrete Math. Lett.*, 8:72–77, 2022. doi:10.47443/dml.2021.0109.

[8] Riccardo Aragona, Norberto Gavioli, and Giuseppe Nozzi. A classification of module braces over the ring of p-adic integers. *Ricerche di Matematica*, 2025. doi:10.1007/s11587-025-00972-y.

[9] Riccardo Aragona, Norberto Gavioli, and Giuseppe Nozzi. Transfinite hypercentral iterated wreath product of integral domains. *Annali di Matematica Pura ed Applicata (1923 -)*, sep 2025. doi:10.1007/s10231-025-01616-6.

[10] Riccardo Aragona, Norberto Gavioli, and Giuseppe Nozzi. Normality conditions in the Sylow p-subgroup of $\mathrm{Sym}(p^n)$ and its associated lie algebra. *Journal of Algebra*, 689:747–763, 2026. doi:10.1016/j.jalgebra.2025.10.033.

[11] Riccardo Aragona and Giuseppe Nozzi. Classification of a specific class of $\mathbb{F}_{p^k}$-braces using bilinear forms. *Journal of Algebra and Its Applications*, June 2025. doi:10.1142/s0219498826502592.

[12] David Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016. doi:10.1016/j.jalgebra.2016.01.011.

[13] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991. doi:10.1007/BF00630563.

[14] Carlo Brunetta, Marco Calderini, and Massimiliano Sala. On hidden sums compatible with a given block cipher diffusion layer. *Discrete Math.*, 342(2):373–386, 2019. doi:10.1016/j.disc.2018.10.003.

[15] Marco Calderini, Roberto Civino, and Riccardo Invernizzi. Differential experiments using parallel alternative operations. *J. Math. Cryptol.*, 18(1):Paper No. 20230030, 9, 2024. doi:10.1515/jmc-2023-0030.

[16] Marco Calderini, Roberto Civino, and Massimiliano Sala. On properties of translation groups in the affine general linear group with applications to cryptography. *J. Algebra*, 569:658–680, 2021. doi:10.1016/j.jalgebra.2020.10.034.

[17] Andrea Caranti. Bi-skew braces and regular subgroups of the holomorph. *J. Algebra*, 562:647–665, 2020. doi:10.1016/j.jalgebra.2020.07.006.

[18] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala. Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen*, 69(3):297–308, 2006. doi:10.5486/pmd.2006.3594.

[19] Claude Carlet. *Boolean functions for cryptography and coding theory*. Cambridge University Press, New York, 2020. doi:10.1017/9781108606806.

[20] Ferran Cedó. Left braces: solutions of the Yang-Baxter equation. *Adv. Group Theory Appl.*, 5:33–90, 2018. doi:10.4399/97888255161422.

[21] Lindsay N. Childs. Bi-skew braces and Hopf Galois structures. *New York J. Math.*, 25:574–588, 2019.

[22] Roberto Civino, Céline Blondeau, and Massimiliano Sala. Differential attacks: using alternative operations. *Des. Codes Cryptogr.*, 87(2-3):225–247, 2019. doi:10.1007/s10623-018-0516-z.

[23] Roberto Civino and Valerio Fedele. Binary bibraces and applications to cryptography. *Mediterr. J. Math.*, 22(1):Paper No. 29, 37, 2025. doi:10.1007/s00009-024-02793-z.

[24] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. doi:10.1007/978-1-4757-6568-7.

[25] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[26] Ilaria Del Corso. Module braces: relations between the additive and the multiplicative groups. *Ann. Mat. Pura Appl. (4)*, 202(6):3005–3025, 2023. doi:10.1007/s10231-023-01349-4.

[27] John Douglas Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. doi:10.1007/978-1-4612-0731-3.

[28] Pavel Etingof, Travis Schedler, and Alexandre Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999. doi:10.1215/S0012-7094-99-10007-X.

[29] Alberto Facchini and Mara Pompili. Semidirect products of digroups and skew braces. *Bull. Belg. Math. Soc. Simon Stevin*, 31(1):40–53, 2024. doi:10.36045/j.bbms.230825.

[30] Tatiana Gateva-Ivanova. A combinatorial approach to noninvolutive set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat.*, 65(2):747–808, 2021. doi:10.5565/publmat6522111.

[31] Leandro Guarnieri and Leandro Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017. doi:10.1090/mcom/3161.

[32] Philip Hall. The classification of prime-power groups. *J. Reine Angew. Math.*, 182:130–141, 1940. doi:10.1515/crll.1940.182.130.

[33] Přemysl Jedlicka and Agata Pilitowska. Diagonals of solutions of the yang–baxter equation. *Forum Mathematicum*, 2024. doi:10.1515/forum-2024-0409.

[34] Marc Krasner and Léo Kaloujnine. Produit complet des groupes de permutations et problème d'extension de groupes. *Acta Scientiarum Mathematicarum (Szeged)*, 13–14:208–230 (vol. 13); 39–66 (vol. 14); 69–82 (vol. 14), 1950–1951.

[35] Felix Leinen. Chief series and right regular representations of finite p-groups. *J. Austral. Math. Soc. Ser. A*, 44(2):225–232, 1988.

[36] Thomas Letourmy and Leandro Vendramin. Isoclinism of skew braces. *Bull. Lond. Math. Soc.*, 55(6):2891–2906, 2023. doi:10.1112/blms.12900.

[37] Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000. doi:10.1215/S0012-7094-00-10411-5.

[38] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 55–64. Springer, Berlin, 1994. doi:10.1007/3-540-48285-7_6.

[39] Onorato Timothy O'Meara. *Introduction to quadratic forms*, volume Band 117 of *Die Grundlehren der mathematischen Wissenschaften*. Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[40] Clarence Hudson Richardson. *An Introduction to the Calculus of Finite Differences*. New York: Van Nostrand, 1954.

[41] Derek John Scott Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996. doi:10.1007/978-1-4419-8594-1.

[42] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007. doi:10.1016/j.jalgebra.2006.03.040.

[43] Jean-Pierre Serre. *A course in arithmetic*, volume No. 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[44] Alexander Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000. doi:10.4310/MRL.2000.v7.n5.a4.

[45] Helmut Strade. *Simple Lie algebras over fields of positive characteristic. Vol. 1*, volume 38 of *De Gruyter Expositions in Mathematics*. De Gruyter, Berlin, second edition, 2017. Structure theory.

[46] Vitaly Ivanovich Sushchansky and Nataliya V. Netreba. Wreath product of Lie algebras and Lie algebras associated with Sylow p-subgroups of finite symmetric groups. *Algebra Discrete Math.*, (1):122–132, 2005.

[47] Helmut Wielandt. *Finite permutation groups*. Academic Press, New York-London, 1964. Translated from the German by R. Bercov.