Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master in Advanced Mathematics and Mathematical Engineering

Master's thesis

The degree of commutativity for group rings

Pere Llorens i Domingo

Supervised by Enric Ventura Capell

January, 2024

Thanks to my tutor, Enric Ventura, who has guided me in completing this work. And thanks to my family, for their support in my studies and for always taking care of me.

Abstract

The degree of commutativity is a classic topic studied in non-commutative algebra (see Gustafson [8], MacHale [11] [12] or Gallagher [7]). Nevertheless, nowadays is still an active field, as seen in [5], extending the concept to some specific algebraic structures; or [1], where a generalization to infinite groups is given; or other recent researches as [4] or [9]. The aim of this thesis is to extend the notion of the degree of commutativity for infinite group rings, inspired by these recent results, and prove an analogous result as [1] but for these structures. Therefore, we will see that the degree of commutativity of an infinite non-commutative group ring is at most $5/8$, and is strictly positive if and only if the group ring is virtually commutative.

Keywords

degree of commutativity, group ring

Contents

Introduction **3**

0 Basic definitions and results **4**

1 Degree of commutativity for finite algebraic structures **9**

1.1 Degree of commutativity for finite groups 9

1.2 The degree of commutativity for finite rings 13

1.3 Degree of commutativity for finite group rings 17

2 Degree of commutativity for infinite algebraic structures **23**

2.1 The degree of commutativity for finitely generated groups 23

2.2 Degree of commutativity for infinite group rings 25

Conclusions **33**

References **35**

Introduction

Non-commutative algebra is a branch of mathematics with an eloquent name since it consists of working with structures where the commutative property is generally unsatisfied. However, one does not need to go deep into the topic to realize that in non-commutative structures you often have commuting elements. A reasonable question arises: how is the commutativity inside non-commutative structures? This question can be approached with different perspectives depending on where do you center your attention: you could either ask for the "amount" of commutativity or whether there is or is not a specific structure of the commuting elements. A natural, but also key, concept to work with this topic is the degree of commutativity: the probability that a pair of elements of an algebraic structure $(G, \cdot)$, selected uniformly random (with replacement), commutes. For a finite structure, it has the intuitive mathematical expression:

$$dc(G) = \frac{|\{(x, y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

In the first chapter of this thesis, we will see some of the results about the degree of commutativity for finite algebraic structures. In particular, we will prove that the upper bound for the degree of commutativity of non-commutative groups and rings is $5/8$ (see Gustafson [8] and MacHale [11]), and for group rings is $11/32$ (see Chashiani and Rezaei [5]). Also, we will see that the degree of commutativity of a group is bounded above by the product of degrees of commutativity of a normal subgroup and the respective quotient (see Gallagher [7]). The analogous result is true for group rings and its ideals (see [5]), and it can be extended to rings in general, as we will see.

Working with the degree of commutativity as we defined it, a natural question arises: can this notion of the degree of commutativity be generalized to infinite structures? Note that this cannot be done straightforwardly, because if G is infinite, $dc(G)$ would be undetermined. However, a reasonable generalization can be made for finitely presented groups, denoted by $dc_X(G)$, depending on a generating set X; as Antolín, Martino, and Ventura did in [1]. Equipped with this more general definition, they also proved an analogous result to Gustafson, getting the same bound of $5/8$, and a significant result regarding the structure of commutativity in an infinite group. This was covered as well in my bachelor's thesis [10], and will be presented shortly in the second section of this thesis. One may ask himself if this generalization to finitely generated groups can be done somehow for rings as well. In the final part of the thesis, we approach this question and prove an analogous version of the Antolín-Martino-Ventura result for a specific type of ring: the group rings. Intuitively we might think that this result is no big surprise, however, the structure of rings and groups is different: given a ring $(R, +, \cdot)$, restricted to the product $(R, \cdot)$ we have a monoid, but not a group. Hence, this is not a consequence of the result for groups, but a different one. This will be the main contribution of this thesis: an original approximation bounding the commutativity degree, and getting, analogously to Antolín-Martino-Ventura, that for residually finite ring groups, the degree of commutativity is positive if and only if it is virtually abelian.

0. Basic definitions and results

We will begin this thesis with an introductory section with basic definitions and results that will be useful afterward, and we will also present the notation that we will use. These are well-known results that can be found in an introductory course about group and ring theory (you can check, for example [13] or [3]), so they will be presented without including proofs. For the same reason, one may skip this section without any problem.

Definition 0.1. A **group** is a pair $(G, \cdot)$ where G is a non-empty set and $\cdot$ is a binary operation:

$$\begin{aligned} G \times G &\to G \\ (a, b) &\mapsto a \cdot b, \end{aligned}$$

which satisfies the following properties:

- associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in G$,
- identity element: $\exists 1 \in G$ such that $g \cdot 1 = 1 \cdot g = g$, $\forall g \in G$,
- every element has an inverse: $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

If, in addition, the group satisfies the commutative property ($a \cdot b = b \cdot a$, $\forall a, b \in G$), we say that it is an **abelian group** or a commutative group.

Remark. When the operation of the group is clear or can be inferred from the context, we write G instead of $(G, \cdot)$. Additionally, we often write ab instead of $a \cdot b$. For abelian groups, we frequently use additive notation, i.e., expressing the operation as $+$ and the identity element as 0.

Definition 0.2. Let G be a group, and let $H \subseteq G$ be a subset of G. We say that H is a **subgroup of** G, denoted $H \leq G$, if $(H, \cdot)$ is a group, where $\cdot$ is the operation of G restricted to H.

Remark. From this definition, it is easy to see that if $H \leq G$, the identity element and inverses of elements in H must coincide with those in G (i.e., $1_H = 1_G$, and for all $x \in H$, we have $x_H^{-1} = x^{-1}$).

Definition 0.3. For a set G, we write $|G|$ to denote its cardinality, i.e., the number of elements in G. If G is a group, this can also be denoted as the **order** of the group.

Proposition 0.4. *Every non-abelian group of order less than or equal to* 8 *is isomorphic to either: the symmetric group on a set of three elements, S_3; the dihedral group of degree four, D_4; or the quaternion group Q_8.* □

Proposition 0.5. *Let H be a subset of the group G. Then $H \leq G$ if and only if H is non-empty and $xy^{-1} \in H$ for all $x \in H$ and $y \in H$.* □

Definition 0.6. Given a subgroup $H \leq G$ of a group G, we can define two equivalence relations: $x \sim_H y$ if and only if $x = yh$ for some $h \in H$ (resp. $x \sim_H y$ if and only if $x = hy$ for some $h \in H$). Thus, we define the equivalence classes $xH = \{xh \mid h \in H\}$ (resp. $Hx = \{hx \mid h \in H\}$), called **left cosets** (resp. **right cosets**). Since the relation is an equivalence, the cosets are disjoint and partition G. Moreover, we define the **index of** H **in** G, denoted $[G : H]$, as the cardinality of the set of left (or right) cosets. The index is the same for left and right cosets because the map $xH \to Hx^{-1}$ is clearly a bijection. If a subgroup $H \leq G$ has $[G : H] < \infty$, we call it a **finite index subgroup** and write $H \leq_{f.i.} G$. From these observations, we derive Lagrange's theorem, presented below.

Theorem 0.7 (Lagrange's theorem)**.** *If G is a group and $H \leq G$ is a subgroup, then $|G| = [G : H] \cdot |H|$. In the case where G is finite, we have $[G : H] = |G|/|H|$. Therefore, the size of a subgroup always divides the size of the group if it is finite.* □

Definition 0.8. A subgroup $N \leq G$ of G is called a **normal subgroup**, denoted $N \trianglelefteq G$, if for every $g \in G$, we have $gN = Ng$.

Proposition 0.9. *If $N \trianglelefteq G$, then the two equivalence relations modulo N coincide, are compatible with the operation of G, and hence the quotient G/N is a group.* □

We now introduce homomorphisms, which are functions between groups that preserve their structure, and present the three isomorphism theorems.

Definition 0.10. Let $(G, \cdot_G)$ and $(H, \cdot_H)$ be two groups. A function $f : G \to H$ is called a **homomorphism** if it preserves the structure of G, i.e., for all $x, y \in G$, we have $f(x \cdot_G y) = f(x) \cdot_H f(y)$.

If f is also a bijection, we say f is a **group isomorphism** and that G and H are **isomorphic**, denoted $G \cong H$.

Proposition 0.11. *If $f : G \to H$ is a homomorphism, then* $\ker f = \{g \in G \mid f(g) = 1\} \trianglelefteq G$. □

Theorem 0.12 (First Isomorphism Theorem)**.** *Let $f : G \to H$ be a homomorphism. Then the induced map $\overline{f} : G/\ker f \to \operatorname{Im} f$ is a group isomorphism. That is, $G/\ker f \cong \operatorname{Im} f$.* □

Theorem 0.13 (Second Isomorphism Theorem)**.** *Let H be a subgroup and N a normal subgroup of a group G. Then $N \cap H \trianglelefteq H$ and the map $(N \cap H)x \mapsto Nx$ is an isomorphism from $H/N \cap H$ to NH/N.* □

Theorem 0.14 (Third Isomorphism Theorem)**.** *Let M and N be normal subgroups of a group G such that $N \leq M$. Then $M/N \trianglelefteq G/N$ and $(G/N)/(M/N) \cong G/M$.* □

Definition 0.15. The **center** of G is the set of elements in G that commute with every element of the group, $Z(G) = \{x \in G \mid xy = yx,\ \forall y \in G\}$.

Definition 0.16. The **centralizer** of $x \in G$ is $C_G(x) = \{y \in G \mid xy = yx\}$. For a subset $S \subseteq G$ and an element $x \in G$, we write $C_S(x) = C_G(x) \cap S$.

Proposition 0.17. *For a group G, its center is a normal subgroup, $Z(G) \trianglelefteq G$. Moreover, for any element $x \in G$, the centralizer of x is a subgroup, $C_G(x) \leq G$.* □

Definition 0.18. Given two elements $x, y \in G$, we say that x and y are **conjugate** if there exists $g \in G$ such that $y = g^{-1}xg$, denoted x^g. Similarly, two subsets $X, Y \subseteq G$ are called conjugate if there exists $g \in G$ such that $Y = g^{-1}Xg = X^g$.

Proposition 0.19. *Conjugation is an equivalence relation. The equivalence classes are called the* **conjugacy classes** *of G. Given a $g \in G$ and a subset $S \subseteq G$, we will denote $g^S = \{s^{-1}gs \mid s \in S\}$. In particular, g^G is the conjugacy class of g. The conjugacy application, $G \to G, g \mapsto x^g$, is an isomorphism.* □

Definition 0.20. A **ring** is a triple $(R, +, \cdot)$ where R is a non-empty set equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that:

- $(R, +)$ is an abelian group.
- Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in R$,

- Multiplication is distributive over addition:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c), \quad \forall a, b, c \in R.$$

If, in addition, $\cdot$ is commutative, we say that R is a **commutative ring**. If R has a multiplicative identity $1 \neq 0$ such that $a \cdot 1 = 1 \cdot a = a$, $\forall a \in R$, we call R a **ring with unity**.

Remark. For simplicity, we often write R instead of $(R, +, \cdot)$ and use juxtaposition ab instead of $a \cdot b$.

Proposition 0.21. *Every non-commutative ring R satisfying $|R| = 8$ is isomorphic to the ring of 2×2 upper triangular matrices over F_2, denoted by $U_2(F_2)$.* □

Definition 0.22. A **subring** of a ring R is a subset $S \subseteq R$ that is itself a ring under the operations of R restricted to S.

Remark. The additive identity 0 and the multiplicative identity 1 (if R has one) must belong to S.

Proposition 0.23. *Let R be a ring and $S \subseteq R$. Then S is a subring of R if and only if the following conditions hold:*

1. *S is non-empty.*
2. *S is closed under subtraction: $a - b \in S$, $\forall a, b \in S$.*
3. *S is closed under multiplication: $a \cdot b \in S$, $\forall a, b \in S$.* □

Definition 0.24. Let R be a ring. A subset $I \subseteq R$ is called a **left ideal** (resp. **right ideal**) of R if $(I, +)$ is a subgroup of $(R, +)$; and $\forall r \in R$ and $\forall a \in I$, we have $ra \in I$ (resp. $ar \in I$). If I is both a left ideal and a right ideal, then I is called a **two-sided ideal** or simply an **ideal** of R.

Remark. An ideal I of a ring R is itself a ring under the addition and multiplication inherited from R. However, if R is a ring with identity, it is not necessarily the case that I has an identity element. For example, every proper ideal does not have a multiplicative identity.

Proposition 0.25 (Lagrange's Theorem for Subrings and Ideals)**.** *Lagrange's Theorem, which states that the order of a subgroup divides the order of the group, applies to subrings and ideals of a ring R because, in particular, they are subgroups of $(R, +)$, the additive group of R. The concepts of index of an ideal and finite index ideal are completely analogous to its groups version.* □

Definition 0.26. The **center** of a ring R and the **centralizer** of an element $a \in R$ are defined analogously as its group version: $Z(R) = \{z \in R \mid zr = rz \text{ for all } r \in R\}$ and $C_R(a) = \{r \in R \mid ar = ra\}$. Both $Z(R)$ and $C_R(a)$ are subrings of R.

Theorem 0.27 (Isomorphism Theorems for Rings)**.** *The following isomorphism theorems hold as well for rings. Let R be a ring, and let I be an ideal of R:*

- **First Isomorphism Theorem:** *If $f : R \to S$ is a ring homomorphism, then $R/\ker(f) \cong \mathrm{Im}(f)$.*
- **Second Isomorphism Theorem:** *Let S be a subring of R, and let I be an ideal of R. Then $S \cap I$ is an ideal of S, and there is an isomorphism: $(S + I)/I \cong S/(S \cap I)$.*
- **Third Isomorphism Theorem:** *If $I \subseteq J$ are ideals of R, then: $R/J \cong (R/I)/(J/I)$.* □

Proposition 0.28. *Given an ideal $I \subseteq R$, the cosets of R/I are equivalence classes under the relation $a \sim b$ if and only if $a - b \in I$. Each equivalence class, or coset, is of the form $a + I = \{a + i \mid i \in I\}$.* □

Remark. The cosets of R/I are typically written as $a + I$. When the ideal I is clear from context, we may use the shorthand $\overline{a}$ to represent the coset $a + I$.

Definition 0.29. A **field** $(F, +, \cdot)$ is a ring in which every element has a multiplicative inverse. A **finite field** F is a field with a finite number of elements. We will write F_k to refer to the finite field of k elements.

Definition 0.30. Let F be a field, and let G be a group. The **group ring** $F[G]$ is the set of formal sums:

$$F[G] = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in F, \text{ and only finitely many } \lambda_g \neq 0 \right\},$$

where the $\lambda_g \in F$ are called the **coefficients** of u, and $g \in G$ are the **basis elements**.

The operations in $F[G]$ are defined as follows:

- **Addition:** For $u = \sum_{g \in G} \lambda_g g$ and $v = \sum_{g \in G} \mu_g g$, their sum is:

$$u + v = \sum_{g \in G} (\lambda_g + \mu_g) g.$$

- **Multiplication:** For $u = \sum_{g \in G} \lambda_g g$ and $v = \sum_{h \in G} \mu_h h$, their product is:

$$u \cdot v = \sum_{g,h \in G} \lambda_g \mu_h (g \cdot h).$$

Here, the group operation in G is used to combine basis elements.

Definition 0.31. The **support** of an element $u = \sum_{g \in G} \lambda_g g \in F[G]$, denoted supp(u), is the set of group elements with nonzero coefficients in u: $\text{supp(u)} = \{g \in G \mid \lambda_g \neq 0\}$. Note that $|\text{supp(u)}| < \infty$.

Proposition 0.32. *A group ring $(F[G], +, \cdot)$ is a ring.* □

Definition 0.33. We will denote the **zero element** of $F[G]$ as $0 = \sum_{g \in G} 0 \cdot g$, and the **identity element** as $1 = 1_F \cdot 1_G$, where 1_G is the identity element of the group G, and 1_F is the multiplicative identity of the field F. When it is clear by the context, we may not use the subindex indicating the structure for whom one element 1 is the identity.

Proposition 0.34. *The group ring $F[G]$ can be interpreted as a vector space over the field F. The elements of G form a basis for $F[G]$, and every $u \in F[G]$ can be expressed uniquely as a linear combination: $u = \sum_{g \in G} \lambda_g g$, where $\lambda_g \in F$. Hence, we can use vectorial space concepts with group rings.* □

Definition 0.35. Let F be a field, V a vector space over F, and $S \subseteq V$ a subset. The **span** of S, denoted $\text{span}(S)$, is the set of all finite linear combinations of elements of S, that is:

$$\text{span}(S) = \left\{ \sum_{i=1}^{n} c_i v_i \;\middle|\; n \in \mathbb{N},\ v_i \in S,\ c_i \in F \right\}.$$

In other words, $\text{span}(S)$ is the smallest subspace of V that contains S.

Definition 0.36. Let F be a field, V a vector space over F, and $S \subseteq V$ a subset. The subset S is called a **basis** of V if: S is **linearly independent**, meaning no element of S can be written as a linear combination of the other elements of S; and S **spans** V, meaning $\text{span}(S) = V$. Equivalently, S is a basis of V if every element of V can be uniquely expressed as a linear combination of elements of S.

Proposition 0.37. *If F is a finite field with $|F| = q$ elements, and G is a finite group with $|G| = n$, then the group ring $F[G]$ is finite, with $|F[G]| = q^n$.*

1. Degree of commutativity for finite algebraic structures

This section covers a variety of results about the degree of commutativity in some finite algebraic structures, specifically about finding upper bounds. Because of that, if the opposite is not specified, along the section; G, R, and $F[G]$ will respectively denote a finite group, a finite ring, and a finite group ring, even if the finitude is not explicitly stated.

Definition 1.1. The **commutative fraction** of a finite algebraic structure with an operation, $(G, \cdot)$, is the set of ordered pairs of elements of the structure such that they commute. This is $C = \{(x, y) \in G \times G \mid xy = yx\}$.

Observation 1.2. We can express the commutative fraction in terms of the centralizers of the elements of G as $C = \bigsqcup_{x \in G} \{(x, y) \mid y \in C_G(x)\}$. In particular, taking cardinals we get the following expression:

$$|C| = \sum_{x \in G} |C_G(x)|.$$

Proof. The elements of C are of the form $(x, y) \in G \times G$. If we fix the first coordinate x, the second coordinate, y, has to be an element commuting with x, this is $y \in C_G(x)$. Moreover, for each $y \in C_G(x)$, there is exactly one element of the form (x, y) in C. Doing that for each possible first coordinate, we get the expression $C = \bigsqcup_{x \in G} \{(x, y) \mid y \in C_G(x)\}$. Since this is a disjoint union, taking cardinals it follows that $|C| = \sum_{x \in G} |C_G(x)|$. □

Definition 1.3. The **degree of commutativity** of a finite algebraic structure with an operation, $(G, \cdot)$, is the probability that a pair of elements of G, selected uniformly random (with replacement), commutes:

$$dc(G) = \frac{|C|}{|G|^2}.$$

Remark. Indeed, if we choose elements uniformly random, each pair has the same probability of being picked, so the degree of commutativity is just the number of commuting pairs divided by the total number of ordered pairs, which is $|G|^2$.

One may note that we have used the group notation to define the commutative fraction and the degree of commutativity. However, these definitions are general and work for any finite algebraic structure with operation. That is why we will not need to define the degree of commutativity every time that we use it into a different object.

1.1 Degree of commutativity for finite groups

Proposition 1.4. *Let G be a group and $x \in G$. Then $x \in Z(G)$ if and only if $x^G = x$.*

Proof. $x \in Z(G) \iff \forall g \in G,\ xg = gx \iff \forall g \in G,\ g^{-1}xg = x \iff x^G = \{x\}$. □

Lemma 1.5 (MacHale, 1974 [12])**.** *Given a group G, if $G/Z(G)$ is cyclic, then G is abelian.*

Proof. If $G/Z(G)$ is cyclic it must have a generator of the form $Z(G)g$, and so:

$$G = Z(G) \cup Z(G)g \cup (Z(G)g)^2 \cup \cdots \cup (Z(G)g)^i \cup \ldots .$$

But since $(Z(G)g)^i = Z(G)g^i$, we have

$$G = Z(G) \cup Z(G)g \cup Z(G)g^2 \cup \cdots \cup Z(G)g^i \cup \ldots .$$

Thus, for every $g_1, g_2 \in G$, we can write them with the form $g_1 = z_1 g^{i_1}$,$g_2 = z_2 g^{i_2}$, where $z_1, z_2 \in Z(G)$. Therefore, $g_1 g_2 = z_1 g^{i_1} z_2 g^{i_2} = z_1 z_2 g^{i_1+i_2} = z_2 g^{i_2} z_1 g^{i_1} = g_2 g_1$, and so, G is abelian. □

Observation 1.6. Let G be a group. If $|G/Z(G)| = p$, for a prime p, then G is abelian.

Proof. If $|G/Z(G)| = p$, with p prime, Lagrange theorem implies that $G/Z(G)$ does not have proper subgroups, and so it is cyclic. Then, the result follows from the previous Lemma 1.5. □

Proposition 1.7. *If G is a non-abelian group, then $|Z(G)| \leq |G|/4$.*

Proof. If $|G/Z(G)| = 1$, then $G = Z(G)$, and so G is abelian. Moreover, if $|G/Z(G)| = 2, 3$, since these are primes, G is abelian as well. Therefore, if G is non-abelian, we must have $|G/Z(G)| \geq 4$, implying $|Z(G)| \leq |G|/4$. □

Theorem 1.8 (Gustafson, 1973 [8])**.** *If G is a non-abelian finite group, then $dc(G) \leq 5/8$.*

Proof. We will first do some observations. Given an element $x \in G$, we have that: if $x \in Z(G)$, then $C_G(x) = G$, since x would commute with all elements in G; if $x \notin Z(G)$, then $|C_G(x)| \leq |G|/2$, since the centralizer would be a proper subgroup of G. Using this, we can bound the degree of commutativity in the following way:

$$\begin{aligned}
dc(G) =& \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)| \\
&= \frac{1}{|G|^2} \left(\sum_{x \in Z(G)} |C_G(x)| + \sum_{x \in G \setminus Z(G)} |C_G(x)| \right) \\
&\leq \frac{1}{|G|^2} \left(|Z(G)||G| + (|G| - |Z(G)|) \cdot \frac{1}{2}|G| \right) \\
&= \frac{1}{|G|^2} \left(\frac{1}{2}|G|(|Z(G)| + |G|) \right) \\
&\leq \frac{1}{|G|^2} \left(\frac{1}{2}|G| \left(\frac{1}{4}|G| + |G| \right) \right) \\
&= \frac{1}{|G|^2} \left(\frac{5}{8}|G|^2 \right) \\
&= \frac{5}{8}
\end{aligned}$$

Where we used $|Z(G)| \leq |G|/4$ from Proposition 1.7. □

The bound given by Theorem 1.8 is indeed tight because there are groups that satisfy the equality.

Observation 1.9. The quaternion group, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, defined by $i^2 = j^2 = k^2 = ijk = -1$ and $1, -1 \in Z(Q_8)$, satisfies $dc(Q_8) = 5/8$.

Proof. We will see that the inequalities of the proof of the Gustafson theorem, are equalities in the case of the quaternions. Moreover, we just need to see that $4 \cdot |Z(Q_8)| = |Q_8|$ and that $\forall x \in Q_8 \backslash Z(Q_8)$, we have $|C_G(x)| = |Q_8|/2$. The operation table of Q_8 is:

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

We have that $|Q_8| = 8$ and $|Z(Q_8)| = |\{\pm 1\}| = 2$, and so $|Q_8| = 4|Z(Q_8)|$. On the other hand $C_{Q_8}(i) = C_{Q_8}(-i) = \{\pm 1, \pm i\}$, $C_{Q_8}(j) = C_{Q_8}(-j) = \{\pm 1, \pm j\}$, $C_{Q_8}(k) = C_{Q_8}(-k) = \{\pm 1, \pm k\}$, implying that $\forall x \in Q_8 \backslash Z(Q_8)$ it is satisfied $|C_G(x)| = 4 = |Q_8|/2$. It follows that $dc(Q_8) = 5/8$.

Note that with the product table, we could also just have counted the commuting pairs and divide the result by $|Q_8|^2 = 64$, leading to the same result. □

We have just proven the upper bound on the degree of commutativity of a non-abelian group given by Gustafson. Now we will see another important classical result regarding the relation between the degrees of commutativity of a group, its normal subgroups, and the correspondent quotients.

Proposition 1.10. *Let G be a group and $x, y \in G$ be conjugates. Then, $C_G(x)$ and $C_G(y)$ are conjugates. In particular $|C_G(x)| = |C_G(y)|$.*

Proof. Since x i y are conjugate, exists a $g \in G$ such that $gx = yg$, which is equivalent to $xg^{-1} = g^{-1}y$. Then,

$$h \in C_G(x) \Leftrightarrow hx = xh \Leftrightarrow ghxg^{-1} = gxhg^{-1} \Leftrightarrow ghg^{-1}y = yghg^{-1} \Leftrightarrow ghg^{-1} = h' \in C_G(y).$$

Therefore, $C_G(x) = g^{-1}C_G(y)g$, and so, we have a bijection $\phi : C_G(x) \to C_G(y), h \to g^{-1}hg$, with inverse $\phi^{-1} : C_G(y) \to C_G(x), h \to ghg^{-1}$. In particular, $|C_G(x)| = |C_G(y)|$ holds. □

Proposition 1.11. *Let G be a group and $x \in G$. Then, $|x^G| = [G : C_G(x)]$ holds.*

Proof. We define the function

$$\begin{aligned} \phi : G/C_G(x) &\to x^G \\ gC_G(x) &\mapsto gxg^{-1}. \end{aligned}$$

This is well-defined, because:

$$gC_G(x) = hC_G(x) \Leftrightarrow h^{-1}gC_G(x) = C_G(x) \Leftrightarrow h^{-1}g \in C_G(x) \Leftrightarrow h^{-1}gx = xh^{-1}g \Leftrightarrow gxg^{-1} = hxh^{-1}.$$

This reasoning in the opposite way proves the injectivity of ϕ. It is also exhaustive because for every $gxg^{-1} \in x^G$, we have $gxg^{-1} = \phi(gC_G(x))$. Thus, ϕ is a bijection and $|x^G| = |G/C_G(x)| = [G : C_G(x)]$. □

Definition 1.12. Let G be a group. We will denote by $k(G)$ the **number of conjugacy classes of** G.

Proposition 1.13. *Let G be a finite group. Then, the number of conjugacy classes and the degree of commutativity of G are related according to:*

$$k(G) = |G| \cdot dc(G).$$

Proof. Let $x_1, \dots, x_{k(G)} \in G$ be representatives of each conjugacy class of G. Applying propositions 1.10 and 1.11, we have that:

$$\begin{aligned} |G| \cdot dc(G) &= \frac{1}{|G|} \sum_{x \in G} |C_G(x)| \\ &= \frac{1}{|G|} \sum_{i=1}^{k(G)} |x_i^G| |C_G(x_i)| \\ &= \frac{1}{|G|} \sum_{i=1}^{k(G)} [G : C_G(x_i)] |C_G(x_i)| \\ &= \frac{k(G)|G|}{|G|} \\ &= k(G). \end{aligned}$$

□

Proposition 1.14. *Let G be a finite group and $N \trianglelefteq G$ a normal subgroup. Then, for every $x \in G$:*

$$C_G(x)/C_N(x) \cong C_G(x)N/N \leq C_{G/N}(xN).$$

Proof. We will first prove that $C_G(x)N/N \leq C_{G/N}(xN)$. Recall the definitions of $C_G(x)N/N = \{yN \in G/N \mid y \in C_G(x)\}$, and $C_{G/N}(xN) = \{yN \in G/N \mid yNxN = xNyN\}$. Then, given $yN \in C_G(x)N/N$, by definition and normality it is satisfied $xy = yx$ and $yN = Ny$, and so $yNxN = NyxN = NxyN = xNyN$. That is $yN \in C_{G/N}(xN)$.

To prove the isomorphism $C_G(x)/C_N(x) \cong C_G(x)N/N$, we will use the second isomorphism theorem for G, which states that given a subgroup, $H \leq G$, and a normal subgroup, $N \trianglelefteq G$, then $HN/N \cong H/H \cap N$. Taking $H = C_G(x)$, it results on $C_G(x)N/N \cong C_G(x)/N \cap C_G(x) = C_G(x)/C_N(x)$. □

Proposition 1.15. *Let $N \trianglelefteq G$ be a normal subgroup. Given some $y \in G$ and $n \in N$, either $C_{yN}(n) = \emptyset$ or there exists $yn_0 \in C_{yN}(n)$ such that $C_{yN}(n) = yn_0 C_N(n)$, that is, $C_{yN}(n)$ is a coset of $C_N(n)$. In particular, $|C_{yN}(n)| \leq |C_N(n)|$ holds.*

Proof. If $C_{yN}(n) = \emptyset$, we have $0 = |C_{yN}(n)| \leq |C_N(n)|$.

Now, suppose that $C_{yN}(n)$ is not empty, that is, it contains some $yn_0 \in C_{yN}(n)$. We will see that, if so, $C_{yN}(n) = yn_0 C_N(n)$. For the first inclusion, $C_{yN}(n) \subseteq yn_0 C_N(n)$, given a $yn' \in C_{yN}(n)$, we can write $yn' = yn_0(n_0^{-1}n')$. Since yn' and yn_0 commute with n, we have that $n_0^{-1}n' \in N$ also does it, implying $n_0^{-1}n' \in C_N(n)$. For the converse, $C_{yN}(n) \supseteq yn_0 C_N(n)$, let $n' \in C_N(n)$. Since yn_0 also commutes with n, we have that $yn_0 n'$ also does so, implying $yn_0 n' = y(n_0 n') \in C_{yN}(n)$.

Finally, if $C_{yN}(n) = yn_0 C_N(n)$, then $C_{yN}(n)$ is a coset of $C_N(n) \leq G$. Therefore $|C_{yN}(n)| = |C_N(n)|$, and in particular, $|C_{yN}(n)| \leq |C_N(n)|$ holds. □

Theorem 1.16 (Gallagher, 1970 [7]). *Let G be a finite group and $N \trianglelefteq G$ a normal subgroup. Then:*

$$dc(G) \leq dc(G/N)dc(N).$$

Proof. From the expression in Proposition 1.14, $C_G(x)/C_N(x) \cong C_G(x)N/N \leq C_{G/N}(xN)$, we deduce:

$$|C_G(x)| \leq |C_{G/N}(xN)||C_N(x)|.$$

Adding for all elements in G:

$$\sum_{x\in G} |C_G(x)| \leq \sum_{x\in G} |C_{G/N}(xN)||C_N(x)| = \sum_{yN\in G/N} \left(|C_{G/N}(yN)| \sum_{x\in yN} |C_N(x)| \right).$$

Note that for every $x \in yN$, we have $n \in C_N(x) \iff n \in N, xn = nx \iff n \in N, x \in C_{yN}(n)$. Using this on the previous inequality:

$$\sum_{x\in G} |C_G(x)| \leq \sum_{yN\in G/N} \left(|C_{G/N}(yN)| \sum_{n\in N} |C_{yN}(n)| \right) \leq \sum_{yN\in G/N} |C_{G/N}(yN)| \sum_{n\in N} |C_N(n)|,$$

where we used $|C_{yN}(n)| \leq |C_N(n)|$, given by Proposition 1.15. Finally, dividing by $1/|G|^2$ on each side, we get:

$$dc(G) = \frac{1}{|G|^2} \sum_{x\in G} |C_G(x)| \leq \left(\frac{1}{(|G|/|N|)^2} \sum_{yN\in G/N} |C_{G/N}(yN)| \right) \left(\frac{1}{|N|^2} \sum_{n\in N} |C_N(n)| \right) = dc(G/N)dc(N).$$

□

Proposition 1.13 shows the tight relation between the degree of commutativity and the number of conjugacy classes of a group. Actually, the Gallagher theorem 1.16 has an equivalent expression in terms of the number of conjugacy classes, as it is done in the original paper [7].

Corollary 1.17. *Let G be a finite group and $N \trianglelefteq G$ a normal subgroup. Then:*

$$k(G) \leq k(G/N)k(N).$$

Proof. It follows from applying the formula $k(G) = |G| \cdot dc(G)$ to the last theorem. □

1.2 The degree of commutativity for finite rings

Since a ring, $(R, +, \cdot)$, has two operations, one could define the degree of commutativity over each, the addition, or the multiplication. However, $(R, +)$ is a commutative group by definition. Thus, the degree of commutativity of $(R, +)$ is always 1. On the other hand, $(R, \cdot)$ is only a monoid, and its degree of commutativity appears to be more interesting to study. Because of this, given a finite ring, R, $dc(R)$ will refer to the degree of commutativity over its multiplication operation unless stated otherwise. In the same sense, the center and centralizers of the ring will be over the multiplication operation.

One may note that, since $(R, \cdot)$ is not necessarily a group (because it can miss the multiplicative inverses), we cannot apply the results we have for groups. However, we can find an analogous result to Gustafson for rings adapting its proof, as MacHale [11] did, getting the same bound of $5/8$. On the other hand, an analogous result to the Gallagher theorem can be proven for rings, extending the result for group rings by Chashiani and Rezaei [5]. In this subsection, we will cover these results.

Observation 1.18. Let R be a ring. Then, $Z(R) = \{u \in R \mid \forall r \in R, ur = ru\}$ and $C_R(r) = \{u \in R \mid ur = ru\}$, for any $r \in R$, are subrings of R.

Proof. Recall that a subset of R is a subring if and only if it contains the multiplicative identity $1 \in R$ and is closed over multiplication and substraction. For $Z(R)$, note that 1 commutes with every element in R and so $1 \in Z(R)$. And given $u, v \in Z(R)$ and $r \in R$, we have that $uvr = urv = ruv$ and $(u - v)r = ur - vr = ru - rv = r(u - v)$, meaning $uv, u - v \in Z(R)$, proving that $Z(R)$ is a subring of R. Moreover, this proof also works for the centralizer of an element $r \in R$, meaning that $C_R(r)$ is also a subring of R. □

We will see that, in particular, we can prove an analogous version of Lemma 1.5, which is key in the proof of Gustafson theorem. This will be useful to prove the version for rings.

Lemma 1.19. *Given a ring R, if $R/Z(R)$ is additively cyclic, then R is commutative.*

Proof. Let $R/Z(R)$ be cyclic with generator $r + Z(R)$. Since the addition is commutative, every pair of elements $r_1, r_2 \in R$ can be expressed in the form $r_1 = m_1 r + z_1$ and $r_2 = m_2 r + z_2$, for some $m_1, m_2 \in \mathbb{Z}$ and $z_1, z_2 \in Z(R)$. Thus, $r_1 r_2 = (m_1 r + z_1)(m_2 r + z_2) = m_1 m_2 r^2 + (m_1 r)z_2 + z_1(m_2 r) + z_1 z_2 = m_2 m_1 r^2 + z_2(m_1 r) + (m_2 r)z_1 + z_2 z_1 = (m_2 r + z_2)(m_1 r + z_1) = r_2 r_1$, meaning that R is commutative. □

Corollary 1.20. *If R is non-commutative, $|Z(R)| \leq |R|/4$.*

Proof. The results follows from Lemma 1.19. The proof is completely analogous to the version for groups from Proposition 1.7. □

Theorem 1.21 (MacHale, 1976 [11])**.** *If R is a non-commutative finite ring, then $dc(R) \leq 5/8$.*

Proof. The proof is completely analogous to the version for groups. We will first do some observations. Given an element $r \in R$, we have that: if $r \in Z(R)$, then $C_R(r) = R$, since r would commute with all elements in R; if $r \notin Z(R)$, then $|C_R(r)| \leq |R|/2$, since the centralizer would be a proper additive subgroup

of R. Using this, we can bound the degree of commutativity in the following way:

$$\begin{aligned}
dc(R) &= \frac{1}{|R|^2}\sum_{r\in R}|C_R(r)| \\
&= \frac{1}{|R|^2}\left(\sum_{r\in Z(R)}|C_R(r)| + \sum_{r\in R\setminus Z(R)}|C_R(r)|\right) \\
&\leq \frac{1}{|R|^2}\left(|Z(R)||R| + (|R| - |Z(R)|)\cdot\frac{1}{2}|R|\right) \\
&= \frac{1}{|R|^2}\left(\frac{1}{2}|R|(|Z(R)| + |R|)\right) \\
&\leq \frac{1}{|R|^2}\left(\frac{1}{2}|R|\left(\frac{1}{4}|R| + |R|\right)\right) \\
&= \frac{1}{|R|^2}\left(\frac{5}{8}|R|^2\right) \\
&= \frac{5}{8},
\end{aligned}$$

where we used $|Z(R)| \leq |R|/4$ from 1.20. □

Observation 1.22. Note that the proof of MacHale Theorem does not require the existence of a multiplicative identity in the ring R. In particular, given an ideal I of a finite ring R, since I is a ring itself (even if it may not have a multiplicative identity), we have that either I is commutative or $dc(I) \leq 5/8$.

Observation 1.23. The bound of Theorem 1.21 is tight.

Proof. Indeed, the ring of upper triangular 2×2 matrices over F_2, $U_2(F_2) = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in F_2\right\}$ satisfies $dc(U_2(F_2)) = 5/8$, proving that the bound is tight. The elements of $U_2(F_2)$ are:

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

$$E = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

And the resulting multiplication table is:

$\cdot$	A	B	C	D	E	F	G	H
A	A	A	A	A	A	A	A	A
B	A	B	C	D	A	B	C	D
C	A	A	A	A	C	C	C	C
D	A	B	C	D	B	D	A	B
E	A	A	A	A	E	E	E	E
F	A	B	C	D	E	F	G	H
G	A	A	A	A	G	G	G	G
H	A	B	C	D	G	H	E	F.

There is a total of 64 different pairs of elements and, checking the symmetry of the multiplication table, one can see that 40 of them commutate. Hence, $dc(U_2(F_2)) = 40/64 = 5/8$.

□

Proposition 1.24. *Let R be a ring and I an ideal of R. Then for all $u \in R$, we have*

$$\frac{C_R(u) + I}{I} \subseteq C_{R/I}(u + I).$$

Proof. Let $v + I \in (C_R(u) + I)/I$ be a coset, where $v \in C_R(u)$, that is $vu = uv$. Then $(v + I)(u + I) = vu + I = uv + I = (u + I)(v + I)$. This means that $v + I \in C_{R/I}(u + I)$. □

Lemma 1.25. *Let R be a ring and I an ideal of R. Then for any $u + I \in R/I$, we have:*

$$\sum_{v \in u+I} |C_I(v)| = \sum_{v \in I} |C_I(v)|.$$

Proof. If $C_{u+I}(v) \neq \emptyset$, we can choose the representative u of the coset $u + I$ such that $u \in C_{u+I}(v)$. We will first prove that $C_{u+I}(v) = u + C_I(v)$. Indeed, for any $w \in C_{u+I}(v) \subseteq u + I$, it exists an $r \in I$ such that $w = u + r$. Then, $r = w - u \in C_I(v)$, because, both w and u do commute with v, proving the inclusion $C_{u+I}(v) \subseteq u + C_I(v)$. For the opposite inclusion, given $w = u + r \in u + C_I(v)$, with $r \in C_I(v)$, then w does commute with v because both u and r do so by definition, and it belongs to $(u + I)$ because $u \in u + C_I(v) \subseteq u + I$.

We have that, for $u \in R$,

$$\begin{aligned}
\sum_{v \in u+I} |C_I(v)| &= \sum_{r \in I} |C_I(u + r)| \\
&= \sum_{r \in I} |\{v \in I \mid v \in C_I(u + r)\}| \\
&= |\{(r, v) \in I \times I \mid v \in C_I(u + r)\}| \\
&= |\{(r, v) \in I \times I \mid (u + r) \in C_{u+I}(v)\}|.
\end{aligned}$$

Now, one may note that in the set of the last expression, for the pairs (r, v) satisfying $u + r \in C_{u+I}(v) \neq \emptyset$, we have $C_{u+I}(v) = u + C_I(v)$; and the ones satisfying $C_{u+I}(v) \neq \emptyset$ do not affect the counting of elements. Using this:

$$\begin{aligned}
\sum_{v \in u+I} |C_I(v)| &= |\{(r, v) \in I \times I \mid (u + r) \in u + C_I(v)\}| \\
&= |\{(r, v) \in I \times I \mid r \in C_I(v)\}| \\
&= \sum_{v \in I} |\{r \in I \mid r \in C_I(v)\}| \\
&= \sum_{v \in I} |C_I(v)|.
\end{aligned}$$

□

Theorem 1.26. *Let R be a finite ring and I be an ideal of R. Then*

$$dc(R) \leq dc\,(R/I)\, dc(I).$$

Proof. By definition,

$$\begin{aligned}|R|^2 dc(R) &= \sum_{u\in R} |C_R(u)| \\ &= \sum_{u+I\in R/I} \sum_{w\in I} |C_R(u+w)| \\ &= \sum_{u+I\in R/I} \sum_{w\in I} \left| \left(\frac{C_R(u+w)}{C_R(u+w)\cap I} \right) \right| |C_I(u+w)|,\end{aligned}$$

and using the 2nd Isomorphism theorem on the last expression and the Propositions 1.24 and 1.25,

$$\begin{aligned}|R|^2 dc(R) &= \sum_{u+I\in R/I} \sum_{w\in I} \left| \left(\frac{C_R(u+w)+I}{I} \right) \right| |C_I(u+w)| \\ &\leq \sum_{u+I\in R/I} |C_{R/I}(u+I)| \sum_{w\in I} |C_I(u+w)| \\ &= \left(\sum_{u+I\in R/I} |C_{R/I}(u+I)| \right) \left(\sum_{v\in I} |C_I(v)| \right).\end{aligned}$$

Finally, dividing each side by $|R|^2$, we get the desired expression:

$$dc(R) \leq \frac{1}{|R|^2} \frac{|I|^2}{|I|^2} \left(\sum_{u+I\in R/I} |C_{R/I}(u+I)| \right) \left(\sum_{v\in I} |C_I(v)| \right) = dc(R/I)dc(I).$$

□

1.3 Degree of commutativity for finite group rings

We will finish this section by studying the degree of commutativity on finite group rings. Recall that a group ring, $F[G]$, is finite if and only if both the field F and the group G are finite. It is relevant to notice that all the results we covered in the last subsection about finite rings also apply to group rings, since these are, in particular, rings. However, by focusing on this specific kind of ring, we can get a bound for its degree of commutativity of $11/32$, quite smaller than the $5/8$ from MacHale Theorem (1.21) for general rings. Chashiani and Rezaei proved this result recently in [5], and we will cover it in this subsection.

Lemma 1.27. *Let $\mathcal{C}_1, \dots, \mathcal{C}_{k(G)}$ be the conjugacy classes of a finite group G and $C_i = \sum_{x\in\mathcal{C}_i} x$. Then $\{C_1, \dots, C_{k(G)}\}$ forms a F-basis for $Z(F[G])$.*

Proof. Let us observe that the number of conjugacy classes, $k(G)$, is finite because G is finite. We will first see that the vectorial subspace generated by $\{C_1, \cdots, C_{k(G)}\}$, this is, all the linear combinations generated by these elements, lies in $Z(F[G])$. For any $g \in G$ we have

$$C_i g = \left(\sum_{x\in\mathcal{C}_i} x \right) g = \sum_{x\in\mathcal{C}_i} xg = \sum_{x\in\mathcal{C}_i} gx^g = g \sum_{x\in\mathcal{C}_i} x^g = g \sum_{y\in\mathcal{C}_i} y = gC_i,$$

where $1 \leq i \leq k(G)$. Then $C_i \in Z(F[G])$, and so will do every element generated by $\{C_1, \cdots, C_{k(G)}\}$. Note that $\sum_{x \in \mathcal{C}_i} x^g = \sum_{y \in \mathcal{C}_i} y$ is satisfied because the conjugacy application by g,

$$\begin{aligned} G &\to G \\ g &\mapsto x^g, \end{aligned}$$

is an isomorphism. Restricting to every conjugacy class, $\mathcal{C}_i$, it follows the equality.

Now we will see that $\{C_1, \ldots, C_{k(G)}\}$ is a F-generating set of $Z(F[G])$. For any $v = \sum \lambda_g g \in Z(F[G])$ and $h \in G$, we have

$$\sum_{g \in G} \lambda_g g = v = v^h = \left(\sum_{g \in G} \lambda_g g \right)^h = \sum_{g \in G} \lambda_g g^h.$$

Comparing the coefficients of g^h on both sides, we obtain $\lambda_{g^h} = \lambda_g$. Since this is true for any $h \in G$, the coefficients λ_g must have a constant value λ_i for all $g \in \mathcal{C}_i$, for each conjugacy class. Therefore $v = \sum \lambda_g g = \sum \lambda_i C_i$, and so $C_1, \ldots, C_{k(G)}$ generate $Z(F[G])$.

Finally, note that $C_1, \cdots, C_{k(G)}$ are linearly independent since they are sums of disjoint sets of elements of G. Hence, the result follows. □

Observation 1.28. The size of the center of a finite group ring, $F[G]$, is $|Z(F[G])| = |F|^{|k(G)|}$.

Proof. This is a direct consequence of the last lemma since it proves that the center of a group ring, $Z(F[G])$, has a vectorial basis of size $k(G)$. □

Lemma 1.29. *For every $v \in F[G] \setminus Z(F[G])$,*

$$|F|^{k(G)+1} \leq |C_{F[G]}(v)| \leq |F|^{|G|-2}.$$

Proof. We will start by proving the first inequality. For all $v \in F[G] \setminus Z(F[G])$, we have $v \in C_{F[G]}(v)$ and $Z(F[G]) \subseteq C_{F[G]}(v)$. Thus, the F-subspace generated by $Z(F[G]) \cup \{v\}$ is contained in $C_{F[G]}(v)$. Since $Z(F[G])$ has a basis of size $k(G)$ by the previous lemma and $v \notin Z(F[G])$ by definition, $span(Z(F[G]), v)_F$ is a subspace of dimension $k(G) + 1$. Hence, $|C_{F[G]}(v)| \geq |F|^{k(G)+1}$.

The proof of the second inequality, $|C_{F[G]}(v)| \leq |F|^{|G|-2}$, in the original publication [5] is a little bit ambiguous, using some tricky implications without too much justification. That is why we made an alternative proof in this thesis, to present the result with clarity. Let $v = \sum_{g \in G} \lambda_g g \in F[G] \setminus Z(F[G])$, with $\lambda_g \in F$ fixed. Since v is not from the center, by Lemma 1.27, there must be a couple of conjugated elements of G with different coefficients. This is, exist $c, d \in G$ such that $\lambda_c \neq \lambda_{c^d}$. For $a = cd \in G$ and $b = d^{-1} \in G$, this is equivalent to $\lambda_{ab} \neq \lambda_{ba}$.

One can easily check that $C_{F[G]}(v)$ is a F-subspace of $F[G]$. We will find the system of equations that define $C_{F[G]}(v)$, and prove that it has rank at least 2, concluding that the dimension of the centralizer is at most $|G| - 2$, which implies $|C_{F[G]}(v)| \leq |F|^{|G|-2}$. Writing $u = \sum_{g \in G} x_g g \in F[G]$, with unfixed coefficients $x_g \in F$, the centralizer of v is defined by:

$$
\begin{aligned}
C_{F[G]}(v) &= \{u \mid vu = uv\} \\
&= \left\{ \sum_{g\in G} x_g g \mid \left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{g\in G} x_g g\right) = \left(\sum_{g\in G} x_g g\right)\left(\sum_{g\in G} \lambda_g g\right) \right\} \\
&= \left\{ \sum_{g\in G} x_g g \mid \sum_{h\in G}\left(\sum_{g\in G} \lambda_g x_{g^{-1}h}\right) h = \sum_{h\in G}\left(\sum_{g\in G} x_g \lambda_{g^{-1}h}\right) h \right\} \\
&= \left\{ \sum_{g\in G} x_g g \mid \forall h \in G, \sum_{g\in G} \lambda_g x_{g^{-1}h} = \sum_{g\in G} x_g \lambda_{g^{-1}h} \right\}.
\end{aligned}
$$

Now, making a change of variable in the left side with $z = g^{-1}h$, $g = hz^{-1}$, and relabelling afterward z as g again, we get:

$$
\begin{aligned}
C_{F[G]}(v) &= \left\{ \sum_{g\in G} x_g g \mid \forall h \in G, \sum_{z\in G} \lambda_{hz^{-1}} x_z = \sum_{g\in G} x_g \lambda_{g^{-1}h} \right\} \\
&= \left\{ \sum_{g\in G} x_g g \mid \forall h \in G, \sum_{g\in G} (\lambda_{hg^{-1}} - \lambda_{g^{-1}h}) x_g = 0 \right\}.
\end{aligned}
$$

Meaning that $C_{F[G]}(v)$ is defined by $|G|$ equations, one for each $h \in G$. To see that this system has rank at least 2, we will find a $2x2$ minor with determinant different from zero. If we take the coordinates $g = a^{-1}$ and $g = b^{-1}$ for each of the equations $h = a$ and $h = b$, we get:

- The equation for $h = a$ is $\sum_{g\in G}(\lambda_{ag^{-1}} - \lambda_{g^{-1}a})x_g = 0$.
  - Coordinate $g = a^{-1}$: $\lambda_{a^2} - \lambda_{a^2} = 0$.
  - Coordinate $g = b^{-1}$: $\lambda_{ab} - \lambda_{ba} \neq 0$.
- The equation for $h = b$ is $\sum_{g\in G}(\lambda_{bg^{-1}} - \lambda_{g^{-1}b})x_g = 0$.
  - Coordinate $g = a^{-1}$: $\lambda_{ba} - \lambda_{ab} \neq 0$.
  - Coordinate $g = b^{-1}$: $\lambda_{b^2} - \lambda_{b^2} = 0$.

Hence, the determinant of the 2×2 minor of of rows $h = a$ and $h = b$, and coordinates $g = a^{-1}$ and $g = b^{-1}$ is:

$$
\begin{vmatrix} 0 & \lambda_{ab} - \lambda_{ba} \\ \lambda_{ba} - \lambda_{ab} & 0 \end{vmatrix} = (\lambda_{ab} - \lambda_{ba})^2 \neq 0,
$$

which is different from zero because $\lambda_{ab} \neq \lambda_{ba}$ and, in a field F, the only divisor of 0 is 0 itself. □

Theorem 1.30 (Chashiani and Rezaei, 2021 [5]). *Let G be a finite group and F be a finite field. Then*

$$
\frac{1 + |F| - |F|^{k(G)-|G|+1}}{|F|^{|G|-k(G)}} \leq dc(F[G]) \leq \frac{1 - |F|^{-2} + |F|^{|G|-k(G)-2}}{|F|^{|G|-k(G)}}.
$$

Proof. Using the definition of commutativity degree 1.3 for $F[G]$, and Lemmas 1.27 and 1.29, we have:

$$\begin{aligned}
dc(F[G]) &= \frac{1}{|F[G]|^2}\sum_{v\in F[G]}|C_{F[G]}(v)| \\
&= \frac{1}{|F[G]|^2}\left(\sum_{v\in Z(F[G])}|C_{F[G]}(v)| + \sum_{v\in F[G]\setminus Z(F[G])}|C_{F[G]}(v)|\right) \\
&\geq \frac{1}{|F[G]|^2}\left(|Z(F[G])||F[G]| + |F|^{k(G)+1}(|F[G]| - |Z(F[G])|)\right) \\
&= \frac{1}{|F|^{2|G|}}\left(|F|^{k(G)}|F|^{|G|} + |F|^{k(G)+1}\left(|F|^{|G|} - |F|^{k(G)}\right)\right) \\
&= \frac{1}{|F|^{2|G|}}\left(|F|^{k(G)+|G|}(1 + |F| - |F|^{k(G)+1-|G|})\right) \\
&= |F|^{k(G)-|G|}(1 + |F| - |F|^{k(G)+1-|G|}).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
dc(F[G]) &= \frac{1}{|F[G]|^2}\sum_{v\in F[G]}|C_{F[G]}(v)| \\
&= \frac{1}{|F[G]|^2}\left(\sum_{v\in Z(F[G])}|C_{F[G]}(v)| + \sum_{v\in F[G]\setminus Z(F[G])}|C_{F[G]}(v)|\right) \\
&\leq \frac{1}{|F[G]|^2}\left(|Z(F[G])||F[G]| + |F|^{|G|-2}(|F[G]| - |Z(F[G])|)\right) \\
&= \frac{1}{|F|^{2|G|}}\left(|F|^{k(G)}|F|^{|G|} + |F|^{|G|-2}(|F|^{|G|} - |F|^{k(G)})\right) \\
&= \frac{1}{|F|^{2|G|}}\left(|F|^{k(G)+|G|}(1 - |F|^{-2} + |F|^{|G|-k(G)-2})\right) \\
&= |F|^{k(G)-|G|}(1 - |F|^{-2} + |F|^{|G|-k(G)-2}).
\end{aligned}$$

□

Observation 1.31. The bounds of Theorem 1.30 are tight.

Proof. If the group G satisfies $|G| - k(G) = 3$, both bounds from theorem 1.30 become equal,

$$\frac{1 + |F| - |F|^{k(G)-|G|+1}}{|F|^{|G|-k(G)}} = |F|^{-2} + |F|^{-3} - |F|^{-5} = \frac{1 - |F|^{-2} + |F|^{|G|-k(G)-2}}{|F|^{|G|-k(G)}},$$

implying that the bounds are tight. We will see that such a group exists. Indeed, the quaternion group,

Q_8, has conjugacy table:

Element	1	-1	i	$-i$	j	$-j$	k	$-k$	Conjugacy Class
1	1	1	1	1	1	1	1	1	$\{1\}$
-1	-1	-1	-1	-1	-1	-1	-1	-1	{-1}
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$	$\{i,-i\}$
$-i$	$-i$	$-i$	$-i$	$-i$	i	i	i	i	$\{i,-i\}$
j	j	j	$-j$	$-j$	j	j	$-j$	$-j$	$\{j,-j\}$
$-j$	$-j$	$-j$	j	j	$-j$	j	j	j	$\{j,-j\}$
k	k	k	$-k$	$-k$	$-k$	$-k$	k	k	$\{k,-k\}$
$-k$	$-k$	$-k$	k	k	k	k	$-k$	$-k$	$\{k,-k\}$.

Hence, it has five conjugacy classes, which are: $\{1\}$,$\{-1\}$,$\{i,-i\}$,$\{j,-j\}$ and $\{k,-k\}$. Thus, the quaternions group satisfies $|Q_8| - k(Q_8) = 8 - 5 = 3$.

□

Proposition 1.32. *Let G be a finite non-abelian group. Then $|G| - k(G) \geq 3$, and the equality holds if and only if $|G| \leq 8$.*

Proof. Recall from Proposition 1.4, given a $x \in G$, it satisfies $g \in Z(G)$ if and only if $|g^G| = 1$. This is equivalent to $g \notin Z(G)$ if and only if $|g^G| \geq 2$. With this, we can bound the number of conjugacy classes of G,

$$\begin{aligned} k(G) &= |\{g^G || g^G| = 1\}| + |\{g^G || g^G| \geq 2\}| \\ &\leq |Z(G)| + \left\lfloor \frac{|G| - |Z(G)|}{2} \right\rfloor \\ &= \left\lfloor \frac{|G| + |Z(G)|}{2} \right\rfloor. \end{aligned}$$

Recall that if G is non-abelian, the group size can only be $|G| = 6$ or $|G| \geq 8$, and from Proposition 1.7, $|Z(G)| \leq |G|/4$. Moreover, since the center size is an integer, we have $|Z(G)| \leq \lfloor |G|/4 \rfloor$. Therefore:

- $|G| = 6 \Rightarrow |Z(G)| \leq 1 \Rightarrow k(G) \leq \left\lfloor \frac{6+1}{2} \right\rfloor = 3 \Rightarrow |G| - k(G) \geq 3$,
- $|G| = 8 \Rightarrow 1 \leq |Z(G)| \leq 2 \Rightarrow k(G) \leq \left\lfloor \frac{8+2}{2} \right\rfloor = 5 \Rightarrow |G| - k(G) \geq 3$,
- $|G| \geq 9 \Rightarrow |Z(G)| \leq |G|/4 \Rightarrow k(G) \leq \left\lfloor \frac{|G|+|Z(G)|}{2} \right\rfloor \leq \left\lfloor \frac{5}{8}|G| \right\rfloor \Rightarrow |G| - k(G) \geq \left\lceil \frac{3}{8}|G| \right\rceil \geq \left\lceil \frac{3}{8} \cdot 9 \right\rceil = 4 > 3$.

And the proof concludes because every non-abelian group, G, with $|G| \leq 8$ is isomorphic to either S_3, D_4, or Q_8, and one can check that the three of them satisfy the equality $|G| - k(G) = 3$. □

Corollary 1.33. *Let G be a finite group and F be a finite field. Then*

$$dc(F[G]) \leq |F|^{-2} + |F|^{-3} - |F|^{-5}$$

and the equality holds if and only if $|G| - k(G) = 3$.

Proof. Using the upper bound from Theorem 1.30 and Proposition 1.32,

$$dc(F[G]) \leq \frac{1-|F|^{-2}+|F|^{|G|-k(G)-2}}{|F|^{|G|-k(G)}} = \frac{1-|F|^{-2}}{|F|^{|G|-k(G)}} + |F|^{-2} \leq |F|^{-2}+|F|^{-3}-|F|^{-5}.$$

One may note that, due to the proof of Observation 1.31, if $|G|-k(G)=3$, the equality holds in every step. □

We have already seen that there is a tight relation between the degree of commutativity of a group and its number of conjugacy classes. This fact can be used to get the bounds of $dc(F[G])$ in terms of $dc(G)$ instead of $k(G)$, as seen in the next corollary.

Corollary 1.34. *Let G be a finite group and F be a finite field. Then*

$$\frac{1+|F|-|F|^{|G|(dc(G)-1)}}{|F|^{|G|(1-dc(G))}} \leq dc(F[G]) \leq \frac{1-|F|^{-2}+|F|^{|G|(1-dc(G))-2}}{|F|^{|G|(1-dc(G))}}.$$

Proof. It follows straight from applying $k(G)=|G|\cdot dc(G)$ from Proposition 1.13 to the bounds of Theorem 1.30. □

Theorem 1.35 (Chashiani and Rezaei, 2021 [5])**.** *Let G be a finite non-abelian group and F be a finite field. Then $dc(F[G]) \leq 11/32$ and the equality holds if and only if $F=F_2$ is the finite field of two elements, and G is isomorphic to one of the groups S_3, D_8 or Q_8.*

Proof. Note that the sequence $\{|F|^{-2}+|F|^{-3}-|F|^{-5}\}_{|F|}$ is decreasing for any finite field F. Indeed, since the function $f(k)=k^{-2}+k^{-3}-k^{-5}$ has derivative $f'(k)=-2k^{-3}-3k^{-4}+5k^{-6}=-k^{-6}(k-1)(2k^2+5k+5)$ with clearly a unique positive zero at $k=1$, and $f''(1)=6+12-30=-10<0$, we deduce that $f(k)$ has only one maximum point at $k=1$ and it is decreasing for the values $k>1$, which are the values that $|F|$ can take.

Thus, we can find an upper bound for all $dc(F[G])$ values, picking F such that $|F|$ has the smallest possible value and using Corollary 1.33. For finite field of two elements, $F=F_2$, we have $dc(F[G]) \leq |F|^{-2}+|F|^{-3}-|F|^{-5}=2^{-2}+2^{-3}-2^{-5}=11/32$.

To find the equality, assume that $dc(F[G])=11/32$. Using the corollary,

$$|F|^{-2}+|F|^{-3}-|F|^{-5} \geq 11/32$$

and so $F=F_2$. Since

$$dc(F[G]) = |F|^{-2}+|F|^{-3}-|F|^{-5} = \frac{11}{32},$$

then $|G|-k(G)=3$. We have seen that this equality hold only for non-abelian groups with $|G|\leq 8$. On the other hand, every non-abelian group of order less than or equal to 8 is isomorphic to one of the groups S_3, D_8 or Q_8. □

2. Degree of commutativity for infinite algebraic structures

Trying to work with the degree of commutativity in non-finite structures presents some difficulties. Through this section, $(G, \cdot)$ will not necessarily be a finite structure. The Definition 1.3 of the degree of commutativity would be undetermined for an infinite G. Thus, we can ask ourselves which would be a natural way to extend the definition onto non-finite structures. Antolín, Martino, and Ventura proposed an answer to this question for groups in [1], giving a generalized definition for finitely generated groups. With that, it is possible to find interesting results for the degree of commutativity for finitely generated groups, as they did. In particular, you can find a generalized version of Gustafson Theorem, and you can also see that the degree of commutativity of a group is positive if and only if it is a virtually abelian group. Note that this last result, instead of giving bounds to the degree of commutativity, tells us about the structure of the commutativity inside the group, a topic that becomes meaningful in infinite groups. These results of [1], were covered in detail in my Bachelor's Thesis. We will present them in this section without proof to avoid overlapping, but the detailed proofs can be checked in [10].

However, taking as an inspiration this result for infinite groups, one may ask if it is possible to get similar results for other infinite structures. In this Master's thesis, we contributed to this question, finding an analogous result for group rings. Trying to do that for rings in general seems reasonable since in the finite case you can find a certain analogy between the structures. However, it is not a trivial issue. Even so, the group rings have a specific structure that allows us to do it, as we will see in this section.

2.1 The degree of commutativity for finitely generated groups

We first need to present some concepts about finitely generated groups. A wider introduction to the topic can be found in [6].

Definition 2.1. Let G be a group and $X \subseteq G$. We will call X **a set of generators of** G, and write $\langle X \rangle = G$ if every element of G can be written as a finite product of elements of X. We can also say that X is a generating set for G or that X generates G. If X is a finite set of generators for G, we will say that G is **finitely generated**.

Definition 2.2. Let G be a group and X be a set of generators of G. Given a $g \in G$, we define $|g|_X$**, the length of** g **over** X**,** as the minimum number of factors that a product of elements of X can have giving g as a result.

Remark. $|\cdot|_X$ satisfies the triangle inequatily. Indeed, given $g, h \in G$, we have $|g \cdot h|_X \leq |g|_X + |h|_X$.

Definition 2.3. Let G be a group and X be a set of generators of G. The **ball of size** n **of** G **over** X, $\mathbb{B}_X(n)$, is the subset of elements of G with length at most n, this is $\mathbb{B}_X(n) = \{g \in G \mid |g|_X \leq n\}$. Note that this is always finite.

With all these concepts, we are prepared to define the degree of commutativity for finitely generated groups.

Definition 2.4. Let $G = \langle X \rangle$ be a finitely generated group and X a finite set. The **degree of commutativity of** G **with respect to** X, denoted by $dc_X(G)$, is

$$dc_X(G) = \limsup_{n \to \infty} \frac{|\{(u, v) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) \mid uv = vu\}|}{|\mathbb{B}_X(n)|^2} \in [0, 1].$$

Remark. The notation of the last definition, $dc_X(G)$, is slightly different from the one given for finite groups in Definition 1.3, $dc(G)$. We will keep this distinction in the notation depending on whether we work with finite or infinite structures. However, both definitions are coherent for finite groups. That is, if G is a finite group, $dc(G) = dc_X(G)$. Actually, the degree of commutativity for finitely presented groups is a generalization of the other definition.

Proof. Indeed, for every finite group G and any generating set X, due to the finiteness of G, there will exist a $N = \max_{g \in G} |g|_X < \infty$. Then, for all $n > N$, we have $G = \mathbb{B}_X(n)$. Hence, $dc_X(G) = dc(G)$. □

From Definition 2.4, a couple of natural questions arise for discussion. First, we used a lim sup instead of a lim because, a priori, we do not know if the limit should exist for any group G and generating set X. But is it necessary? It turns out that the issue is quite complex: on the one hand, no example has been found where the limit does not exist and the superior limit is necessary; on the other hand, no proof has yet been found that shows the limit always exists.

Another interesting observation is that the definition of $dc_X(G)$, apparently depends on the generating set of the group, X. This is true in general, but there are certain types of groups where the degree of commutativity obtained is independent of the generating set [10]. This is very important because it implies that the degree of commutativity is an inherent property of the group. This issue is closely related to the growth of the group.

Definition 2.5. Let G be a group. We say that G has: **polynomial growth of degree** d, where d is an integer, if $0 < Cn^d \leq |\mathbb{B}_X(n)| \leq Dn^d$ for certain constants C, D, and d; **subexponential growth** if there exists a generating set $\langle X \rangle = G$ such that $\lim_{n\to\infty} \frac{|\mathbb{B}_X(n+1)|}{|\mathbb{B}_X(n)|} = 1$; **exponential growth** if $\lim_{n\to\infty} \frac{|\mathbb{B}_X(n+1)|}{|\mathbb{B}_X(n)|} = \lambda > 1$ for every generating set X.

Definition 2.6. A group G is **residually finite** if, for every non-trivial element $1 \neq g \in G$, a finite quotient of G exists such that the coset of g is not trivial.

Lemma 2.7 (Burillo-Ventura, 2002 [2])**.** *Let G be a subexponentially growing group and $H \leq_{f.i.} G$ a finite index subgroup. Then for every X, set of generators of G, and every $g \in G$:*

$$\lim_{n\to\infty} \frac{|\mathbb{B}_X(n) \cap gH|}{|\mathbb{B}_X(n)|} = \lim_{n\to\infty} \frac{|\mathbb{B}_X(n) \cap Hg|}{|\mathbb{B}_X(n)|} = \frac{1}{[G : H]}.$$

□

Remark. One can prove that for exponentially growing groups, the limit in the previous lemma may not even exist, and so the subexponentially growing hypothesis is indispensable for the statement to be true. Since this lemma is essential for the proof of Theorem 2.8 (see [1]), the subexponentially growing hypothesis is inherited.

Theorem 2.8 (Martino-Antolín-Ventura, 2016 [1])**.** *Let G be a finitely generated residually finite group of subexponential growth, and let X be a finite generating set for G. Then:*

(i) $dc_X(G) > 0$ if and only if G is virtually abelian;

(ii) $dc_X(G) > 5/8$ if and only if G is abelian.

As a corollary, we obtain that the positivity of $dc_X(G)$ is independent of X. □

Remark. Note that this (i) tells us about the structure of commutativity inside a finitely generated group. This last result is significant only for infinite groups since all finite groups are virtually abelian, the trivial subgroup is always abelian and has a finite index for a finite group G.

2.2 Degree of commutativity for infinite group rings

This subsection contains the main contribution of this thesis: a generalization of the concept of degree of commutativity onto infinite group rings and some consequent results.

One may note that given a finite group ring, $F[G]$, one could build an infinite version in several ways. You can make either the field F or the group G infinite (or both, of course). Both approaches have their interest and difficulties. However, in order to get an analogous result of Theorem 2.8, which is a result for infinite groups, it seems reasonable to make the group infinite. On the other hand, making F infinite causes inconvenience already when adapting the definition of degree of commutativity given for groups. Thus, in this section, when we refer to a group ring $F[G]$, F will be a finite field and G a finitely generated group, and X will be a finite generating set of G.

First of all, we need to generalize the definition of the degree of commutativity for a group ring.

Definition 2.9. Let $F[G]$ be a group ring and X be a set of generators of G. Given a $u \in F[G]$, we define **the length of u over X,** as $|u|_X = \max\limits_{g \in \text{supp(u)}} |g|_X$.

Remark. Note that we are using the same notation, $|\cdot|_X$, for the length of an element of G and of an element of $F[G]$, but the definitions are different. We will understand that the length is referring each of the definitions depending on the element we are taking the length of. This is an abuse of notation that we allow ourselves to do, as well because using the natural inclusion $G \hookrightarrow F[G], g \mapsto 1_F g$, the two definitions of lengths coincide: $|g|_X = |1_F g|_X$.

One may ask why to choose this particular definition of the length of a $u \in F[G]$. It is important to realize that, in the context of this thesis, the length is only useful to define the degree of commutativity for infinite structures. Then, we need a length where we can define balls of size n which must be finite, contain the balls of less size, and contain the whole structure when we make n tend to infinity. This allows multiple choices of length, but we picked one that seemed a natural extension of the length over G. Moreover, this choice of length has a really useful property that we will see next.

Proposition 2.10. *Given $u, v \in F[G]$. Then $|u+v|_X \leq \max\{|u|_X, |v|_X\}$.*

Proof. Let $u = \sum\limits_{g \in G} \lambda_g g$ and $v = \sum\limits_{g \in G} \mu_g g$, where $\lambda_g = 0$ if $g \notin \text{supp(u)}$ and $\mu_g = 0$ if $g \notin \text{supp(v)}$. Then $u + v = \sum\limits_{g \in G} (\lambda_g + \mu_g) g$, with $(\lambda_g + \mu_g) = 0$ if $g \notin \text{supp(u)} \cup \text{supp(v)}$, that is $\text{supp(u + v)} \subseteq \text{supp(u)} \cup \text{supp(v)}$. Thus $|u+v|_X \leq \max\limits_{g \in \text{supp(u)} \cup \text{supp(v)}} |g|_X = \max\{|u|_X, |v|_X\}$.

Note that sometimes the inequality is strict, for example, given a $u \in F[G]$ such that $|u|_X > 0$, then $|u + (-u)|_X = |0|_X = 0 < |u|_X = \max\{|u|_X, |-u|_X\}$. □

Definition 2.11. Let $F[G]$ be a group ring and X be a generating set for G. The **ball of size n of $F[G]$ over X**, $\mathbb{B}_X^{F[G]}(n)$, is the subset of elements of $F[G]$ with length at most n, this is $\mathbb{B}_X^{F[G]}(n) = \{u \in F[G] \mid |u|_X \leq n\}$.

Observation 2.12. Let $F[G]$ be a group ring and X be a generating set for G. Then, $\mathbb{B}_X^{F[G]}(n) = F[B_X(n)]$, an F-vectorial subspace of $F[G]$. In particular, $|\mathbb{B}_X^{F[G]}(n)| = |F|^{|B_X(n)|}$.

Proof. Given $u = \sum\limits_{g \in G} \lambda_g g \in F[G]$. Then, $u \in \mathbb{B}_X^{F[G]}(n) \Leftrightarrow |u|_X \leq n \Leftrightarrow \forall g \in \text{supp(u)}, |g|_X \leq n \Leftrightarrow u \in F[B_X(n)]$. In particular, $|\mathbb{B}_X^{F[G]}(n)| = |F[B_X(n)]| = |F|^{|B_X(n)|}$. □

From now on, we will rather write $F[B_X(n)]$ instead of $\mathbb{B}_X^{F[G]}(n)$.

Definition 2.13. Let $F[G]$ be a group ring and X a generating set for G. The **degree of commutativity of** $F[G]$ **with respect to** X, denoted by $dc_X(F[G])$, is

$$dc_X(F[G]) = \limsup_{n\to\infty} \frac{|\{(u,v) \in F[\mathbb{B}_X(n)] \times F[\mathbb{B}_X(n)] \mid uv = vu\}|}{|F[\mathbb{B}_X(n)]|^2} \in [0,1].$$

Moreover, if S is a subset of $F[G]$, we will define its degree of commutativity as:

$$dc_X(S) = \limsup_{n\to\infty} \frac{|\{(u,v) \in (F[\mathbb{B}_X(n)] \cap S)^2 \mid uv = vu\}|}{|F[\mathbb{B}_X(n)] \cap S|^2} \in [0,1].$$

Remark. Note that the definition of $dc_x(S)$ is the one we will use, for example, with the ideals of $F[G]$. We need to make this distinction because not every ideal or vectorial subspace of $F[G]$ is itself a group ring. However, the definition using a general subset $S \subseteq F[G]$ is much more general.

Lemma 2.14. *Let $I \trianglelefteq_{f.i} F[G]$ be a finite index ideal of the group ring. Then, there exists a $N > 0$ such that for every $n \geq N$ and every coset $\bar{u} \in F[G]/I$, it is satisfied that $|F[B_X(n)] \cap (\bar{u})| = |F[B_X(n)] \cap I|$.*

Proof. Define $r = [F[G] : I] < \infty$. For each coset $\bar{u} \in F[G]/I$, we select a representative of minimal length, $u_k \in \bar{u}$, so it satisfies $|u_k|_X = \min_{u \in u_k + I} \{|u|_X\}$. Such a representative exists in every coset since the length only takes non-negative integer values, which form a well-ordered set. Define $N = \max_{1\leq k\leq r} |u_k|_X$.

Then, for any $n \geq N$, $F[B_X(n)]$ contains all the representatives chosen, u_k. Consider the function:

$$\begin{aligned} \phi : F[B_X(n)] \cap I &\to F[B_X(n)] \cap (u_k + I) \\ u &\mapsto u_k + u. \end{aligned}$$

Observe that ϕ is well-defined because $|u_k + u|_X \leq \max\{|u_k|_X, |u|_X\} \leq \max\{N, n\} = n$, and as $u \in I$, we have $u_k + u \in u_k + I$. We can also define the function:

$$\begin{aligned} \phi^{-1} : F[B_X(n)] \cap (u_k + I) &\to F[B_X(n)] \cap I \\ v &\mapsto v - u_k. \end{aligned}$$

This is also well-defined because $|v - u_k|_X \leq \max\{|v|_X, |-u_k|_X\} \leq \max\{n, N\} = n$, and as $v \in u_k + I$, then there exists some $u \in I$ such that $v = u_k + u$, and so $v - u_k = u \in I$.

Observe that ϕ^{-1} is the inverse of ϕ because $\phi\phi^{-1}(v) = \phi(v - u_k) = v$ i $\phi^{-1}\phi(u) = \phi^{-1}(u_k + u) = u$. It follows that ϕ is a bijection. Thus, we conclude that $|F[B_X(n)] \cap (u_k + I)| = |F[B_X(n)] \cap I|$ holds for each coset. □

Remark. The choice of $N = \max_{1\leq k\leq r} |u_k|_X$ is the minimal such that the lemma holds. Otherwise, if there is a minimal length representative of a certain coset, $u_k \in u_k + I$, with $N < |u_k|_X$, by the minimality of $|u_k|_X$ we have $|F[B_X(N)] \cap (u_k + I)| = 0$. On the other hand, for every $N \geq 0$, $|F[B_X(N)] \cap I| \geq 1$, since it contains at least the $0 \in I$. Moreover, the finite index condition of the ideal I is necessary for this proof; without it, we would have infinitely many cosets and such an N could not be defined.

From Lemma 2.14 we can obtain several interesting results that will be essential to prove the main result of the thesis (Theorem 2.21). From now on, we will use the same definition for u_k, as one of the minimal length element of the coset $u_k + I$; and as well for N, as the smallest integer such that $F[B_X(N)]$ contains all the u_k.

Proposition 2.15. *Let $I \trianglelefteq_{f.i} F[G]$. For any $n \geq N$ and for any coset $u_k + I \in F[G]/I$, the equality $\frac{|F[B_X(n)] \cap (u_k + I)|}{|F[B_X(n)]|} = \frac{1}{[F[G]:I]}$ holds.*

Proof. Recall that the cosets of $F[G]/I$ form a partition of $F[G] = \bigsqcup_{1 \leq i \leq [F[G]:I]} u_i + I$, from which we can build a partition of the ball of size n:

$$F[B_X(n)] = F[B_X(n)] \cap F[G] = \bigsqcup_{1 \leq i \leq [F[G]:I]} F[B_X(n)] \cap (u_i + I).$$

Taking cardinals, and by Lemma 2.14:

$$\begin{aligned} |F[B_X(n)]| &= \sum_{1 \leq i \leq [F[G]:I]} |F[B_X(n)] \cap (u_i + I)| \\ &= \sum_{1 \leq i \leq [F[G]:I]} |F[B_X(n)] \cap (u_k + I)| \\ &= [F[G] : I] |F[B_X(n)] \cap (u_k + I)|. \end{aligned}$$

Rearranging the terms, we get the desired equality. □

Remark. Note that this result is due to some specific characteristics of group rings. Actually, the proof of the analogous result for groups (Lemma 2.7) is completely different. Moreover, in the mentioned result is indispensable to restrict the growth of the group, which we do not have in the latter version for group rings. This difference comes manly from Proposition 2.10.

Proposition 2.16. *Let $I \trianglelefteq_{f.i} F[G]$. Then, $dc_X(F[G]) \geq \frac{1}{[F[G]:I]^2} dc(I)$.*

Proof. Since $F[B_X(n)] \supseteq F[B_X(n)] \cap I$, we have the inclusion

$$\{(u, v) \in (F[B_X(n)])^2 | uv = vu\} \supseteq \{(u, v) \in (F[B_X(n)] \cap I)^2 | uv = vu\}.$$

For any $n \geq N$, taking cardinals and dividing by $|F[B_X(n)]|^2$ we have:

$$\frac{|\{(u, v) \in (F[B_X(n)])^2 | uv = vu\}|}{|F[B_X(n)]|^2} \geq \frac{|\{(u, v) \in (F[B_X(n)] \cap I)^2 | uv = vu\}|}{|F[B_X(n)]|^2}$$

$$\begin{aligned} &= \frac{|\{(u, v) \in (F[B_X(n)] \cap I)^2 | uv = vu\}|}{|F[B_X(n)]|^2} \cdot \frac{|F[B_X(n)] \cap I|^2}{|F[B_X(n)] \cap I|^2} \\ &= \frac{|\{(u, v) \in (F[B_X(n)] \cap I)^2 | uv = vu\}|}{[F[G] : I]^2 \cdot |F[B_X(n)] \cap I|^2}, \end{aligned}$$

were we used Proposition 2.15 in the last step. Taking $\limsup_{n \to \infty}$ at both sides, we conclude:

$$dc_X(F[G]) \geq \frac{1}{[F[G] : I]^2} dc(I)$$

□

Proposition 2.17. *Let $I \trianglelefteq_{f.i} F[G]$. Then $dc_X(F[G]) \leq dc(F[G]/I)$.*

Proof. As we have seen in the proof of 2.15, using that $F[G]/I$ is a partition of $F[G]$, we can build a partition for $F[B_X(n)] = \bigsqcup_{1\leq i\leq [F[G]:I]} F[B_X(n)] \cap (u_i + I) = \bigsqcup_{1\leq i\leq [F[G]:I]} F[B_X(n)] \cap \overline{u_i}$. Squaring at both sides we get a partition of $(F[B_X(n)])^2$

$$(F[B_X(n)])^2 = \left(\bigsqcup_{1\leq i\leq [F[G]:I]} F[B_X(n)] \cap \overline{u_i}\right)^2 = \bigsqcup_{1\leq i,j\leq [F[G]:I]} (F[B_X(n)])^2 \cap (\overline{u_i} \times \overline{u_j}).$$

Using this partition, we can write the set of pairs of $F[B_X(n)]$ that commute as

$$|\{(u,v) \in (F[B_X(n)])^2 | uv = vu\}| =$$

$$= \sum_{1\leq i,j\leq [F[G]:I]} |\{(u,v) \in (F[B_X(n)])^2 \cap (\overline{u_i} \times \overline{u_j}) | uv = vu\}|$$

$$= \sum_{\substack{(\overline{u_i},\overline{u_j})\in F[G]/I \\ \overline{u_i}\,\overline{u_j}=\overline{u_j}\,\overline{u_i}}} |\{(u,v) \in (F[B_X(n)])^2 \cap (\overline{u_i} \times \overline{u_j}) | uv = vu\}|$$

$$+ \sum_{\substack{(\overline{u_i},\overline{u_j})\in F[G]/I \\ \overline{u_i}\,\overline{u_j}\neq\overline{u_j}\,\overline{u_i}}} |\{(u,v) \in (F[B_X(n)])^2 \cap (\overline{u_i} \times \overline{u_j}) | uv = vu\}|.$$

Now we will do an observation regarding the relation between two cosets commuting in $F[G]/I$ and its elements commuting in $F[G]$. If we have two elements of the group ring, $u, v \in F[G]$, commuting, $uv = vu$; then their classes also commute: $\bar{u}\bar{v} = \overline{uv} = \overline{vu} = \bar{v}\bar{u}$. This is equivalent to its contrapositive statement: if two cosets $\overline{u_i}, \overline{u_j} \in F[G]/I$ do not commute, then no pair of elements $(u, v) \in (\overline{u_i}, \overline{u_j})$ will commute, and so $uv \neq vu$. Conversely, if two cosets $\overline{u_i}, \overline{u_j} \in F[G]/I$ commute, there might be pairs of elements $(u, v) \in (\overline{u_i}, \overline{u_j})$ commuting.

We can apply this to the previous sum, and for any $n \geq N$, we get:

$$|\{(u,v) \in (F[B_X(n)])^2 | uv = vu\}| \leq$$

$$\leq \sum_{\substack{(\overline{u_i},\overline{u_j})\in F[G]/I \\ \overline{u_i}\,\overline{u_j}=\overline{u_j}\,\overline{u_i}}} |F[B_X(n)]^2 \cap (\overline{u_i} \times \overline{u_j})| + \sum_{\substack{(\overline{u_i},\overline{u_j})\in F[G]/I \\ \overline{u_i}\,\overline{u_j}\neq\overline{u_j}\,\overline{u_i}}} 0$$

$$= \sum_{\substack{(\overline{u_i},\overline{u_j})\in F[G]/I \\ \overline{u_i}\,\overline{u_j}=\overline{u_j}\,\overline{u_i}}} |(F[B_X(n)] \cap \overline{u_i}) \times (F[B_X(n)] \cap \overline{u_j})|$$

$$= |\{(\overline{u_i}, \overline{u_j}) \in (F[G]/I)^2 | \overline{u_i}\,\overline{u_j} = \overline{u_j}\,\overline{u_i}\}| |F[B_X(n)] \cap I|^2,$$

were we used Lemma 2.14. If we now divide both sides by $|F[B_X(n)]|^2$, we get:

$$\frac{|\{(u,v) \in (F[B_X(n)])^2 | uv = vu\}|}{|F[B_X(n)]|^2} \leq$$

$$\leq \frac{|\{(\overline{u_i},\overline{u_j}) \in (F[G]/I)^2 | \overline{u_i}\overline{u_j} = \overline{u_j}\overline{u_i}\}||F[B_X(n)] \cap I|^2}{|F[B_X(n)]|^2}$$

$$= \frac{|\{(\overline{u_i},\overline{u_j}) \in (F[G]/I)^2 | \overline{u_i}\overline{u_j} = \overline{u_j}\overline{u_i}\}|}{[F[G]:I]^2} = dc(F[G]/I).$$

Finally, if we take $\limsup_{n\to\infty}$ at both sides, we get $dc_X(F[G]) \leq dc(F[G]/I)$. □

Definition 2.18. A group ring $F[G]$ is **residually finite** if, for every non-trivial element $0 \neq u \in F[G]$, a finite index ideal $I \subseteq F[G]$ exists such that $u \notin I$.

Remark. Equivalently, $F[G]$ is residually finite if for every non-trivial element $0 \neq u \in F[G]$, a finite index ideal $I \subseteq F[G]$ exists such that $\bar{0} \neq \bar{u} \in F[G]/I$.

This definition of a residually finite group ring could be extended to any ring. Still, for group rings of the form $F[G]$, it has a nice relation with the residual finiteness of the group G.

Proposition 2.19. *Let $F[G]$ be a group ring. Then, if G is residually finite, $F[G]$ is also residually finite.*

Proof. Let $0 \neq u = \sum_{g\in G} \lambda_g g \in F[G]$. We will prove the statement by cases. First, if $u = \lambda_1 1$, every proper ideal satisfies the residually finite property, and these always exist in $F[G]$ if G is residually finite.

If $u \neq \lambda_1 1$, but $|\text{supp(u)}| = 1$. Then there exists a $1 \neq g \in G$ such that $u = \lambda_g g$ for a $\lambda_g \neq 0$. By G residually finite, exists a $N_g \trianglelefteq_{f.i.} G$ such that $g \notin N_g$. We can build a natural morphism,

$$\phi : F[G] \to F[G/N_g]$$
$$\sum_{g\in G} \lambda_g g \mapsto \sum_{g\in G} \lambda_g \bar{g},$$

where $\bar{g}$ is the coset of g in G/N_g. Then, since $F[G/N_g]$ is finite, $\ker\phi \subseteq_{f.i} F[G]$ is a finite index ideal, and $\bar{u} = \lambda_g \bar{g} \neq \bar{0}$. Thus, $F[G]$ is residually finite.

Finally, if $|\text{supp(u)}| \geq 2$, for every pair of distinct elements $g, h \in \text{supp(u)}$, exists a $N_{gh^{-1}} \trianglelefteq_{f.i} G$ such that $gh^{-1} \notin N_{gh^{-1}}$. Let $N = \bigcap_{\{g,h\}\in\binom{\text{supp(u)}}{2}} N_{gh^{-1}} \trianglelefteq_{f.i} G$, which inherits the normality and the finite index because it is a finite intersection of subgroups that are so. We can build a natural morphism,

$$\phi : F[G] \to F[G/N] \cong F[G]/\ker\phi$$
$$\sum_{g\in G} \lambda_g g \mapsto \sum_{g\in G} \lambda_g \bar{g}.$$

For every $g, h \in \text{supp(u)}$ we have by definition of N that $\bar{g} \neq \bar{h}$, otherwise we would have $gh^{-1} \in N$, which is not true due to $gh^{-1} \notin N_{gh^{-1}}$. In particular, $\bar{u} \neq \bar{0}$, and so $u \notin \ker\phi \subseteq_{f.i} F[G]$, implying that $F[G]$ is residually finite.

□

Definition 2.20. A ring R is **virtually commutative** if it has a finite index ideal which is commutative.

Theorem 2.21. *Let F be a finite field. Let G be a finitely generated group and let X be a finite generating set for G. Then, if $F[G]$ is residually finite:*

(i) $dc_X(F[G]]) > 0$ *if and only if* $F[G]$ *is virtually commutative;*

(ii) if $dc_X(F[G]) > 5/8$*, then* $F[G]$ *is commutative.*

As a corollary, we obtain that the positivity of $dc_X(F[G])$ *is independent of* X*.*

Proof. We will first prove (*ii*). Let $dc_X(F[G]) > 5/8$. By Lemma 2.17, for every finite index ideal $I \subseteq F[G]$ we have $dc(F[G]/I) > 5/8$. Since $F[G]/I$ is a finite ring, it follows from Mac Hale's Theorem 1.21 that $F[G]/I$ is commutative. Now, given $u, v \in F[G]$, suppose that they do not commute, that is, $uv \neq vu$. This implies that $uv - vu \neq 0$ is a non-trivial element of $F[G]$, and since $F[G]$ is residually finite, it exists a finite index ideal $I \subseteq F[G]$ such that $\bar{0} \neq \overline{uv - vu} \in F[G]/I$, which is a contradiction with $F[G]/I$ commutative. Hence, $F[G]$ is commutative.

Now we will prove (i). For the left implication, let $I \subseteq_{f.i.} F[G]$ be a commutative finite index ideal of $F[G]$. By Proposition 2.16, we have:

$$dc_X(F[G]) \geq \frac{1}{[F[G] : I]^2} dc_X(I) = \frac{1}{[F[G] : I]^2} > 0.$$

For the right implication, we will prove the contrapositive statement. Therefore, assume $F[G]$ is not virtually commutative, that is, it has no finite index commutative ideal. In particular, $F[G]$ is not commutative, so some $u, v \in F[G]$ satisfying $uv \neq vu$ exist. Since $F[G]$ is residually finite, it exists a finite index ideal $I_1 \subseteq_{f.i.} F[G]$ such that $0 \neq uv - vu \notin I_1$. The ideal I_1 has to be non-commutative, otherwise would contradict $F[G]$ not virtually commutative, and so we have some $u_1, v_1 \in I_1$, such that $u_1v_1 \neq v_1u_1$. Repeating the reasoning, it exists a finite index ideal $I_1' \subseteq_{f.i.} F[G]$ such that $0 \neq u_1v_1 - v_1u_1 \notin I_1'$. Now, we define $I_2 = I_1 \cap I_1'$. I_2 is an ideal of $F[G]$ because it is the intersection of two ideals of $F[G]$, and it is of finite index because both I_1 and I_1' are so. Moreover, I_2 is also an ideal of I_1 since it is closed by addition and I_1 is a subset of $F[G]$. Finally, note that $I_2 = I_1 \cap I_1' \neq I_1$, because I_2 does not contain $u_1v_1 - v_1u_1 \in I_1$, by the construction of I_1'. Again, I_2 has to be non-commutative to avoid contradiction, so it has some $u_2, v_2 \in I_2$ satisfying $u_2v_2 \neq v_2u_2$. Now, we can repeat the process: since $F[G]$ is residually finite, it exists an ideal $I_2' \subseteq_{f.i} F[G]$ such that $0 \neq u_2v_2 - v_2u_2 \notin I_2'$, and we can define $I_3 = I_2 \cap I_2'$. Repeating iteratively the reasoning we can build an infinite descending chain of ideals:

$$F[G] = I_0 \supseteq_{f.i.} I_1 \supseteq_{f.i.} I_2 \supseteq_{f.i.} \cdots \supseteq_{f.i.} I_i \supseteq_{f.i.} I_{i+1} \supseteq_{f.i.} \ldots,$$

where each ideal I_{i+1} is a finite index ideal both of I_i and $F[G]$ for all $i \geq 0$; also that there exist some $u_i, v_i \in I_i \subseteq F[G]$ such that $\overline{u_i}\overline{v_i} - \overline{v_i}\overline{u_i} \in I_i \subseteq F[G]$ and $u_iv_i - v_iu_i \notin I_{i+1}$. Therefore, $u_iv_i - v_iu_i$ is a non-trivial element in both I_1/I_{i+1} and $F[G]/I_{i+1}$, and so these are not commutative rings. Recall that $F[G]/I_{i+1}$ is a finite ring and I_1/I_{i+1} its ideal, which has a ring structure itself (the ideal may not have the multiplicative neutral element, but it does not affect the following reasoning). Thus, due to Mac Hale Theorem 1.21, $dc(I_1/I_{i+1}) < 5/8$ and $dc(F[G]/I_{i+1}) < 5/8$.

By using the Third Isomorphism Theorem on the subchain $F[G] \supseteq_{f.i.} I_i \supseteq_{f.i.} I_{i+1}$ we have that $(F[G]/I_{i+1})/(I_i/I_{i+1}) = F[G]/I_i$. If we combine this with Theorem 1.26, we get

$$dc(F[G]/I_{i+1}) \leq dc(I_i/I_{i+1})dc(F[G]/I_i) \leq \frac{5}{8} dc(F[G]/I_i).$$

Inductively, $dc(F[G]/I_{i+1}) \leq \left(\frac{5}{8}\right)^i$. Finally, Proposition 2.17 implies that $dc(F[G]) < \left(\frac{5}{8}\right)^i$ for every $i \geq 0$, concluding that $dc_X(F[G]) = 0$. □

Note that the bound we found for the degree of commutativity of an infinite group ring is $5/8$, which is different from the finite version one, which is $11/32$ (see Theorem 1.35). One may ask why this change. Explained in broad terms, when proving that for an infinite group G, finitely generated by X, $dc_X(G) \leq 5/8$ (Theorem 2.8), we use that the finite quotients of G are finite groups. So they have the bound for the degree of commutativity given by Gustafson in 1.8, which is $5/8$ (see [10]). However, it is not an analogous situation with group rings. Given a group ring $F[G]$ with a finite index ideal I, it is not generally true that $F[G]/I$ is a group ring, we only know that it is a ring. Moreover, such a quotient may satisfy $11/32 < dc(F[G]/I) \leq 5/8$, that is, it is a non-commutative ring with a degree of commutativity greater than $11/32$. Actually, you can find an example of that in the smallest non-commutative group ring.

This fact does not mean that the bound of $dc_X(F[G]) \leq 11/32$ does not apply to the degree of commutativity of infinite group rings, but that with the techniques used for the proof, we can only reach the bound of $dc_X(F[G]) \leq 5/8$. This thesis does not cover whether this bound can be lowered, but it would be a possible future study.

Observation 2.22. $F_2[S_3]$ has an ideal I such that $11/32 < dc(F_2[S_3]/I) \leq 5/8$.

Proof. Recall that F_2 is the finite field of two elements $\{0, 1\}$ and S_3 is the group of permutations of three elements, which is a non-commutative group of six elements: $(1), (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)$. Note that since both are the smallest structures of their kind, then,

$$\begin{aligned} F_2[S_3] =&\{\lambda_{(1)}(1) + \lambda_{(1\ 2)}(1\ 2) + \lambda_{(2\ 3)}(2\ 3) + \lambda_{(1\ 3)}(1\ 3) + \lambda_{(1\ 2\ 3)}(1\ 2\ 3) + \lambda_{(1\ 3\ 2)}(1\ 3\ 2) \mid \\ &\lambda_{(1)}, \lambda_{(12)}, \lambda_{(23)}, \lambda_{(13)}, \lambda_{(123)}, \lambda_{(132)} \in F_2\}, \end{aligned}$$

is the smallest non-commutative group ring, and it has $2^6 = 64$ elements. For simplicity, we will use the vectorial notation to denote elements in this group ring: since every element is determined by its coefficients, we will denote any element by $(\lambda_{(1)}, \lambda_{(12)}, \lambda_{(23)}, \lambda_{(13)}, \lambda_{(123)}, \lambda_{(132)}) \in F_2[S_3]$.

Let I be the ring generated by the element $(0, 1, 0, 0, 1, 0) = (1\ 2) + (1\ 2\ 3) \in F_2[S_3]$. One can easily compute I by calculating the product of this element by each element in $F_2[S_3]$. Doing that, one finds that

$$\begin{aligned} I = \{&(0, 0, 0, 0, 0, 0), (0, 0, 1, 0, 0, 1), (0, 1, 0, 0, 1, 0), (1, 0, 0, 1, 0, 0), \\ &(1, 1, 1, 1, 1, 1), (1, 1, 0, 1, 1, 0), (1, 0, 1, 1, 0, 1), (0, 1, 1, 0, 1, 1)\}. \end{aligned}$$

This is an ideal with $|I| = 8$, and so $|F_2[S_3]/I| = 64/8 = 8$. On the other hand, every non-commutative ring of size 8 is isomorphic to the ring of 2×2 upper triangular matrices over F_2, and we have already calculated its degree of commutativity in the proof of Observation 1.23. Therefore, if we proof that $F_2[S_3]/I$ is non-commutative, we will conclude the proof with $dc(F_2[S_3]/I) = dc(U_2(F_2)) = 5/8 > 11/32$.

One can find as well the cosets of I, by doing the correspondent sums, these cosets are the elements of the ring $F_2[S_3]/I$, which are:

$$F_2[S_3]/I = \{I,$$

$$\{(0,0,0,0,0,1),(0,0,1,0,0,0),(0,1,0,0,1,1),(0,1,1,0,1,0),$$
$$(1,0,0,1,0,1),(1,0,1,1,0,0),(1,1,0,1,1,1),(1,1,1,1,1,0)\},$$

$$\{(0,0,0,0,1,0),(0,0,1,0,1,1),(0,1,0,0,0,0),(0,1,1,0,0,1),$$
$$(1,0,0,1,1,0),(1,0,1,1,1,1),(1,1,0,1,0,0),(1,1,1,1,0,1)\},$$

$$\{(0,0,0,0,1,1),(0,0,1,0,1,0),(0,1,0,0,0,1),(0,1,1,0,0,0),$$
$$(1,0,0,1,1,1),(1,0,1,1,1,0),(1,1,0,1,0,1),(1,1,1,1,0,0)\},$$

$$\{(0,0,0,1,0,0),(0,0,1,1,0,1),(0,1,0,1,1,0),(0,1,1,1,1,1),$$
$$(1,0,0,0,0,0),(1,0,1,0,0,1),(1,1,0,0,1,0),(1,1,1,0,1,1)\},$$

$$\{(0,0,0,1,0,1),(0,0,1,1,0,0),(0,1,0,1,1,1),(0,1,1,1,1,0),$$
$$(1,0,0,0,0,1),(1,0,1,0,0,0),(1,1,0,0,1,1),(1,1,1,0,1,0)\},$$

$$\{(0,0,0,1,1,0),(0,0,1,1,1,1),(0,1,0,1,0,0),(0,1,1,1,0,1),$$
$$(1,0,0,0,1,0),(1,0,1,0,1,1),(1,1,0,0,0,0),(1,1,1,0,0,1)\},$$

$$\{(0,0,0,1,1,1),(0,0,1,1,1,0),(0,1,0,1,0,1),(0,1,1,1,0,0),$$
$$(1,0,0,0,1,1),(1,0,1,0,1,0),(1,1,0,0,0,1),(1,1,1,0,0,0)\}\}.$$

This ring is clearly non-commutative, because, for example, one can easily check in the given explicit expression of $F_2[S_3]/I$ that

$$\overline{(1\ 2)}\overline{(2\ 3)} = \overline{(1\ 2\ 3)} \neq \overline{(1\ 3\ 2)} = \overline{(2\ 3)}\overline{(1\ 2)}.$$

□

Corollary 2.23. *Given a group ring $F[G]$ with a finite index ideal I. Then, in general, $F[G]/I$ is not a group ring.*

Conclusions

Through this thesis, we have studied some results on the degree of commutativity of different algebraic structures. In particular, we have gotten an original result on infinite group rings in Theorem 2.21, previously proved only for groups [1]. However, there are some key differences between the result for groups and for group rings. First of all, both upper bound the degree of commutativity on $5/8$. For groups, we know that this bound is tight, we have already seen in this thesis that it is satisfied for the quaternion group, $dc_X(Q_8) = dc(Q_8) = 5/8$ (Observation 1.9). On the other hand, we do not have such an example for group rings. Even though finding the degree of commutativity of concrete infinite group rings is a heavy task, making this issue already complicated, there are other remarks to make on it. For the degree of commutativity of finitely presented groups, it seems reasonable to find the bound of $5/8$, since this is also the bound for finite groups [8]. But the bound on the degree of commutativity of finite group rings is $11/32$, far below that. One may reasonably conjecture that the bound for infinite group rings is $11/32$ as well. Why we did not get this bound then? At least there is a technical limitation: the strategy followed to find the bound for groups starts by using $dc_X(G) \leq dc(G/N)$, where N is a finite index normal subgroup of G, and then using the bound on the degree of commutativity of the finite group G/N, which is $dc(G/N) \leq 5/8$ [10]. When you do that on $dc_X(F[G])$, you bound it by $dc(F[G]/I)$, where I is a finite index ideal of $F[G]$. However, the finite quotient $F[G]/I$ might not be a group ring again, but just a ring, so you cannot use the $11/32$ bound, but only the $5/8$. Along the process of the thesis, in order to improve the bound, we tried to find out if $F[G]/I$ might be a group ring again, or when. But as soon as you dive a little bit into the question, you can easily find some counterexamples. Another option was to prove that, even without being group rings, the degree of commutativity of non-commutative $F[G]/I$ was below $11/32$; but this did not seem true either as we have seen in Observation 2.22. Therefore, if $dc_X(F[G]) \leq 11/32$ were to be true for infinite group rings, at least we would need to use a very different strategy to prove it. However still it is a bound, and the other part of the theorem, saying that $dc_X(F[G]) > 0$ if and only if $F[G]$ is virtually commutative, holds analogously for group rings as it does for groups.

The other difference between the result for groups and group rings is that for group rings we need fewer hypotheses. Theorem 2.8 has the subexponential growth of the group as a hypothesis, but for group rings we do not need any hypothesis on the growth of $F[G]$, and surprisingly not even on the growth of the group G. This is because the technical Lemma 2.7 demands this hypothesis for groups, but it does not so in the version we proved for rings (Lemma 2.14). The proof we made is independent and relies more on some interesting properties of the balls over $F[G]$, as we have exposed in section 2.2. The key difference is that the cosets of a group rings quotient by an ideal are with respect to the addition operation, and adding two elements from a certain ball of $F[G]$, cannot lie outside of the same ball, as seen in Proposition 2.10. However, this does not happen with groups, where if you operate two elements of length n, the resulting element can reach length $2n$. Then, we could reduce the hypothesis of Theorem 2.21 with respect to its analogous in groups, because this result does not use the groups' result (Theorem 2.8) directly, and so does not require the same hypothesis.

Even though there are fewer hypotheses, the scope of structures that apply is pretty limited in comparison. There are still many possibilities for the continuation of this work in the same direction. In the first place, the result obtained applies specifically to group rings $F[G]$ where G is a finitely presented group and F is a finite field. Already among the group rings, there is a wider diversity that is not contemplated here. For example, $R[G]$ is also a group ring for R just a ring. We have chosen a field F to make sure we always had inverses among the coefficients and facilitate procedures. But this does not seem key in most of the results given (except for Lemma 1.29). This is though the tip of the iceberg: as explained already

in the thesis, making the F infinite, is another way of making $F[G]$ infinite, even though this does bring big technical complications.

Still, the main temptation here is to conjecture a version of Theorem 2.21, but for rings in general. At first glance, having both the bound for finite rings (Theorem 1.21) and the version of Gallagher inequality (Theorem 1.26), the conjecture seems reasonable. Even more, the result for group rings does not use directly the version for groups. However, if the proof of such a result were to be similar to the version for groups, it would require an analogous development of the concept of generation, balls and growth of a ring, allowing a proper definition of the degree of commutativity for rings, and a version of Lemma 2.7. The original proof of this lemma involves the specific structure of groups, reasoning over Cayley's and Schreier's graphs (see [2] and [10]). If the result for rings were to be true, it would require a different proving strategy. It is reasonable to think that such a result would also require some hypothesis on the growth of a ring as it does for groups. It is clear that trying to proof such a result requires so much work, but still is an interesting potential future research in the same direction of this thesis.

References

[1] Yago Antolín, Armando Martino, and Enric Ventura. "Degree of Commutativity of infinite groups". In: *Proceedings of the American Mathematical Society* 145.2 (2017), pp. 479–485. ISSN: 00029939, 10886826. URL: https://www.jstor.org/stable/procamermathsoci.145.2.479 (visited on 06/10/2023).

[2] J. Burillo and E. Ventura. "Counting Primitive Elements in Free Groups". In: *Electronic Notes in Discrete Mathematics* 10 (2001). Comb01, Euroconference on Combinatorics, Graph Theory and Applications, pp. 50–53. ISSN: 1571-0653. DOI: https://doi.org/10.1016/S1571-0653(04)00357-9. URL: https://www.sciencedirect.com/science/article/pii/S1571065304003579.

[3] Pep Burillo. *Estructures algebraiques*. Apunts del curs 2012-2013.

[4] Timothy Burness et al. "On the commuting probability of p-elements in a finite group". In: *Algebra Number Theory* 17 (May 2023), pp. 1209–1229. DOI: 10.2140/ant.2023.17.1209.

[5] Abdollah Chashiani and Rashid Rezaei. "On the commutativity degree of a group algebra". In: *Afrika Matematika* 32 (Feb. 2021). DOI: 10.1007/s13370-021-00887-5.

[6] Jordi Delgado and Enric Ventura i Gatell. "Autòmats de Stallings, un camí d'anada i tornada". In: *Butlletí de la Societat Catalana de Matemàtiques* 37.1 (Jan. 2023), pp. 5–59. URL: https://revistes.iec.cat/index.php/BSCM/article/view/115308.003.

[7] Patrick X. Gallagher. "The Number of Conjugacy Classes in a Finite Group." In: *Mathematische Zeitschrift* 118 (1970), pp. 175–179. URL: http://eudml.org/doc/171450.

[8] W. H. Gustafson. "What is the Probability that Two Group Elements Commute?" In: *The American Mathematical Monthly* 80.9 (1973), pp. 1031–1034. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2318778 (visited on 06/08/2023).

[9] Ilan Levin. *How Associative Can a Non-Associative Moufang Loop Be?* 2025. arXiv: 2501.02294 [math.GR]. URL: https://arxiv.org/abs/2501.02294.

[10] Pere Llorens Domingo. "Grau de commutativitat de grups finitament generats". PhD thesis. UPC, Facultat de Matemàtiques i Estadística, Departament de Matemàtiques, June 2023. URL: http://hdl.handle.net/2117/393152.

[11] Desmond MacHale. "Commutativity in Finite Rings". In: *The American Mathematical Monthly* 83.1 (1976), pp. 30–32. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2318829 (visited on 12/07/2024).

[12] Desmond MacHale. "How Commutative Can a Non-Commutative Group Be?" In: *The Mathematical Gazette* 58.405 (1974), pp. 199–202. ISSN: 00255572. URL: http://www.jstor.org/stable/3615961 (visited on 05/15/2023).

[13] D. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1996. ISBN: 9780387944616. URL: https://books.google.es/books?id=lqyCjUFY6WAC.