Universität Regensburg - Università degli Studi di Padova

Fakultät für Mathematik - Dipartimento di Matematica

ALGANT Master Program

Counterexamples to Kaplansky's Unit Conjecture

Master's thesis

Supervisors:
Prof. Dr. Clara Löh
Prof. Remke Kloosterman

Candidate:
Angela Pellone
2023833

Academic year 2022/2023

Part of a Mathematician's work
is to make mistakes
and fix them.

Clara Löh

Contents

Introduction

The unit conjecture concerns units in group rings. A group ring $R[G]$ is a an algebra over a commutative ring R freely generated as an R-module by a group G and such that the ring product of $R[G]$ restricted to G coincides with the group operation of G. A trivial unit in a group ring $R[G]$ is a unit that can be represented as a scalar multiple of an element of the group G. The problem of determining the existence of non-trivial units in the group ring was first posed by Graham Higman in 1940 in his D.Phil thesis and, afterwards, it has been revived by Kaplansky [5] in 1970 under the conjecture that nowadays is known as the *Kaplansky unit conjecture*. This conjecture asserts that in every group ring of torsion free groups over a field the units are all trivial. Kaplansky actually formulated three conjectures concerning group rings and related to each other: alongside the unit conjecture there are the *Kaplansky zero divisor conjecture* (formulated by Kaplansky as an open problem in 1957 [6, Problem 6]) and the *Kaplansky idempotent conjecture*. The zero divisor conjecture and the idempotent conjecture deal with the problems of determining the existence of non-zero zero divisors and non-trivial idempotents (non-trivial under the usual meaning), respectively. These conjectures are related to each other: the unit conjecture is stronger than the zero divisor conjecture and the zero divisor conjecture is in turn stronger than the idempotent conjecture. The unit conjecture has been proved for many classes of groups (for example, for torsion free abelian groups and, more generally, for unique product groups). The search of a general proof of the unit conjecture took a turn in 2021 (more than 80 years after the first formulation by Higman), when Giles Gardam published an article [3] in which he exhibited a counterexample to the Kaplansky unit conjecture. Shortly afterwards, Alan G. Murray [9] and Donald S. Passman [11] extended Gardam's research to a larger class of group rings. To the best knowledge of the author Gardam's counterexample and its generalizations provided by Passman and Murray are, currently, the only published counterexamples to the Kaplansky unit conjecture.

The purposes of this Master Thesis are, briefly, to present the three Kaplansky conjectures concerning group rings and their relations, to prove the conjectures for special and important classes of groups and to describe counterexamples provided by Gardam, Murray and Passman in their articles of 2021.

In the first chapter we formally define group rings and trivial units in group rings. We state and prove just one property of group rings: group rings over fields are prime rings; this is the only property (inside the huge branch of mathematics of group rings theory) we will need in this thesis and we will use it to prove one relation between the three Kaplansky conjectures. The second part of the first chapter is dedicated to generally introduce Kaplansky conjectures:

we formally give their statements and we prove both that the unit conjecture is stronger then the zero divisor conjecture and that the zero divisor conjecture, in turn, is stronger then the idempotent conjecture.

In the second chapter we present important classes of group rings that satisfy Kaplansky unit and zero divisors conjectures. For all the positive results on the conjectures we discuss here, positivity only depends on the properties of the group G that freely generates the group ring $K[G]$ as a K-module, where K is any field. First section of this chapter is devoted to group theory: we formally define unique product groups and ordered groups; we characterize them through properties equivalent to their definitions and we prove that ordered groups are unique product groups. The main classes of ordered groups that we consider here are abelian torsion free groups and some special virtually abelian groups. In the second section of this chapter, the most important result that we prove states that group rings of unique product groups satisfy both the zero divisor and the unit conjecture. As a corollary, we get that all group rings of torsion free abelian groups satisfy both the zero divisor and the unit conjecture.

The third chapter is devoted to the construction of the counterexamples to the Kaplansky unit conjecture provided by Gardam, Murray and Passman: every group ring of the *Promislow group* over a field of finite characteristic has non-trivial units. The chapter is divided into three sections. The first one is once again entirely of group theory: we define here the Promislow group as a finitely presented group and we include the proofs of all the properties of the Promislow group we need to develop second and third section of this chapter; in particular, the Promislow group is torsion free, virtually abelian where it extends an abelian group by a $\mathbb{Z}/2 \times \mathbb{Z}/2$ group and the infinite dihedral group is a homomorphic image of the Promislow group. The second section treats general group rings $K[P]$ of the Promislow group P, where K is any field. Elements in $K[P]$ can be uniquely represented as linear combinations of four suitable elements of P with coefficients in a suitable subring of $K[P]$. Thanks to this, we can develop our argument to find out sufficient conditions for elements in $K[P]$ to be units and necessary and sufficient conditions for units in $K[P]$ to be non-trivial units. In the third section we start by proving that a certain fixed element (the one exhibited by Gardam in his article) of $\mathbb{Z}/2\mathbb{Z}[P]$ is a non-trivial unit. Eventually, following Murray's idea and mixing this idea with additions of Passman, we find out a triple (i.e., depending on three parameters) family of non-trivial units in group rings of the Promislow group over any field of finite characteristic.

In this work, with the words *Kaplansky conjectures* we'll always refer to unit, idempotent and zero divisor conjectures (as formulated in Definition 1.2.2). In this work, the modules will be always over commutative rings and module over a commutative ring can be endowed of both a left-module and a right-module structure; therefore, without lost of generality, we will always omit the words "left" and "right".

Chapter 1

Group Rings and the Kaplansky Conjectures

1.1 Group Rings

A group ring is, briefly, an algebra over a commutative ring, freely generated as a module by a group. More precisely, given a group G and a commutative ring R, set theoretically G freely generates an R-module $R^{(G)}$ that is unique up to isomorphism of R-modules (Proposition 1.1.2); G being a group, the additive group $R^{(G)}$ can be endowed of a ring structure in such a way that $R^{(G)}$ becomes an R-algebra (Proposition 1.1.3): this is the key proposition that allows us to formally define group rings. Since the algebraic theory concerning free modules is just a "large" setting in which develop the theory of group rings (and it is probably already known by the reader), we enclose not here, but in Appendix A.1 definitions and results we need about free modules. Anyway, in order to make this subsection easily readable, we put even here the definition of module freely generated by a subset and the proposition that guarantees the existence and uniqueness (up to isomorphism) of free modules generated by arbitrary sets.

Definition 1.1.1. Let R be a commutative ring and M be an R-module. We say that M is *freely generated* by $S \subseteq M$ (equivalently, that S *freely generates* M or that S is a *free set of generators* for M) as an R-module if the submodule generated by S coincides with M and if for every $n \in \mathbb{N} \smallsetminus \{0\}$ and for every choice of $x_1, \ldots, x_n \in S$ pairwise distinct and $r_1, \ldots, r_n \in R$, the equality

$$r_1 x_1 + \cdots + r_n x_n = 0_M$$

implies that at least one coefficient between $r_1, \ldots, r_n$ is zero. We say that an R-module is free if it has a free set of generators.

Proposition 1.1.2. *Let S be a set and R be a commutative ring. There exists an R-module $R^{(S)}$ such that S is a subset of $R^{(S)}$ and $R^{(S)}$ is freely generated by S. Such a module is unique up to a unique isomorphism, that is: if M and M' are R-modules freely generated by S, then there exists a unique R-module isomorphism $M \to M'$ such that its restriction to S behaves like the identity.*

Proof. This is Proposition A.1.5. □

Proposition 1.1.3. *Let G be a group, R be a commutative ring and M be the free R-module generated by G. Then M can be endowed with a product $\cdot : M \times M \to M$ such that*

1. *M together with the product $\cdot$ becomes both a ring and an R-algebra;*
2. *the product $\cdot$ restricted to G coincides with the product that defines the group G.*
3. *the product over M that turns M into an R-algebra and that restricted to G coincides with the product that defines the group G is unique.*

Proof. We start defining how to multiply elements of M on the right by elements of G. Let $x \in G$ and $r_x : G \to G$ be the multiplication on the right by x; composing it with the canonical inclusion $G \hookrightarrow M$, we get a mapping $\rho_x : G \to M$. By the universal property of free modules[1], this map induces a morphism of R-modules $\rho_x^* : M \to M$ such that for every $y \in G$

$$\rho_x^*(y) = y \cdot_G x$$

holds (where with the notation $\cdot_G$ we mean the product that gives to G the group structure). Let α be a fixed element in M. We define a set theoretic map as follows

$$\begin{aligned} \lambda_\alpha : G &\longrightarrow M \\ x &\longmapsto \lambda_\alpha(x) := \rho_x^*(\alpha). \end{aligned}$$

By the universal property of free modules, this map induces a morphism of R-modules $\lambda_\alpha^* : M \to M$ that extends λ_α. We're now ready to define the product: we set

$$\begin{aligned} \cdot : M \times M &\longrightarrow M \\ (\alpha, \beta) &\longmapsto \alpha \cdot \beta := \lambda_\alpha^*(\beta). \end{aligned}$$

We have to prove that this product is associative, R-bilinear and that it has an identity.

- *Associativity.* Proving associativity is equivalent to prove that for every α and β in M, $\lambda_{\alpha\cdot\beta}^* = \lambda_\alpha^* \circ \lambda_\beta^*$ holds, which in turn is equivalent to prove that for every $x \in G$, $\lambda_{\alpha\cdot\beta}^*(x) = \lambda_\alpha^* \circ \lambda_\beta^*(x)$ (by the universal property of free modules). Now

  $$\lambda_{\alpha\cdot\beta}^*(x) = \rho_x^*(\alpha \cdot \beta) = \rho_x^*(\lambda_\alpha^*(\beta))$$

  and

  $$\lambda_\alpha^* \circ \lambda_\beta^*(x) = \lambda_\alpha^*(\rho_x^*(\beta)).$$

  Therefore we have to prove that for every $x \in G$, the mappings ρ_x^* and λ_α^* commutes. Applying again the universal property of free modules, it

[1] In this proof we'll use many times the universal property of free generated modules (Proposition A.1.4); we won't repeat the reference anymore so that the proof will be smoother to read.

suffices to prove that the commutativity of the maps holds over the set G. After some computations, we get that the two maps commute if and only if for every $y \in G$, $\rho^*_{yx} = \rho^*_x \circ \rho^*_y$ holds. Applying once again the universal property of free modules, it suffices to prove that the equality holds over the set G but this is quite immediate.

- *Linearity on the right.* Proving linearity on the right is equivalent to prove that for every $\alpha \in M$, the map λ^*_α is an R-module morphism but this is true by construction.

- *Linearity on the left.* Proving linearity on the left means proving that for every $\alpha, \beta \in M$ and for every $r, s \in R$, $\lambda^*_{r\alpha+s\beta} = r\lambda^*_\alpha + s\lambda^*_\beta$ holds componentwise. By the universal property of free modules, we only have to prove that for every $x \in G$, $\lambda^*_{r\alpha+s\beta}(x) = r\lambda^*_\alpha(x) + s\lambda^*_\beta(x)$ holds, i.e. that
$$\rho^*_x(r\alpha + s\beta) = r\rho^*_x(\alpha) + s\rho^*_x(\beta)$$
holds. Since ρ^*_x is an R-module morphism, we're done.

- *Identity.* Let 1_G be the identity of G and take $\alpha \in M$, then
$$\alpha \cdot 1_G = \lambda^*_\alpha(1_G) = \lambda_\alpha(1_G) = \rho^*_{1_G}(\alpha)$$
and
$$1_G \cdot \alpha = \lambda^*_{1_G}(\alpha).$$
Therefore, we have to prove that both $\rho^*_{1_G}$ and $\lambda^*_{1_G}$ are the identity morphism $M \to M$. By the universal property of free generated modules, it suffices to prove that for every $x \in G$
$$\rho^*_{1_G}(x) = x = \lambda^*_{1_G}(x)$$
holds. This follows immediately by the construction of the maps and by the fact that 1_G is the identity of G.

We have just proved that M endowed with the product $\cdot$ is both a ring and an R-algebra. The fact that the product over M restricted to G yields the same product we have over G is easy to show (and we leave it to the reader). Eventually, it remains to prove third point of the statement. Let $\cdot' : M \times M \to M$ be a product that turns M into an R-algebra and such that for every $x, y \in G$
$$x \cdot' y = x \cdot_G y$$
holds. For every $\alpha \in M$ we set the following maps:
$$\begin{aligned} \phi_\alpha : M &\longrightarrow M \\ \beta &\longmapsto \alpha \cdot' \beta \end{aligned}$$
and
$$\begin{aligned} \psi_\alpha : M &\longrightarrow M \\ \beta &\longmapsto \beta \cdot' \alpha. \end{aligned}$$
All these maps are R-module morphisms. To conclude the proof, it suffices to prove that for every $\alpha \in M$, $\lambda^*_\alpha = \phi_\alpha$ holds. By the universal property of

free modules, it suffices to prove that for every $\alpha \in M$ ad for every $x \in G$, $\lambda_\alpha^*(x) = \phi_\alpha(x)$ holds, i.e. that

$$\rho_x^*(\alpha) = \psi_x(\alpha)$$

holds. Again by the universal property of free modules, it suffices to prove that for every $x, y \in G$, $\rho_x^*(y) = \psi_x(y)$ holds; this follows immediately from the definitions of the maps. □

Corollary 1.1.4. *Let G be a group and R be a commutative ring. There exists a unique (up to isomorphism) R-algebra such that it is freely generated by G as an R-module and the ring product restricted to G coincides with the product that gives G the group structure.*

Proof. Existence. Let M be the free R-module generated by G; by Proposition 1.1.3 we can define an operation $\cdot : M \times M \to M$ which endows M with an R-algebra structure and such that its restriction to $G \times G$ coincides with the product constituting the group structure of G.

Uniqueness. Let M' be an other R-algebra freely generated by G as an R-module and such that the ring product of M' restricted to G coincides with the product that gives G the group structure. By uniqueness of free generated modules, there exists an isomorphism $\phi : M \to M'$ of R-modules such that for every $x \in G$, $\phi(x) = x$ holds. To conclude the proof, we have to prove that ϕ is an isomorphism of algebras, i.e. that ϕ preserves the inner product of M. Because of the bijectivity of ϕ, this is equivalent to prove that for every α and β in M

$$\alpha \cdot_M \beta = \phi^{-1}(\phi(\alpha) \cdot_{M'} \phi(\beta)).$$

Consider the operation

$$\begin{aligned} \cdot' : M \times M &\longrightarrow M \\ (\alpha, \beta) &\longmapsto \phi^{-1}(\phi(\alpha) \cdot_{M'} \phi(\beta)). \end{aligned}$$

The set M together with its R-module structure and the operation $\cdot'$ is an R-algebra (we leave to the reader the computations to prove this[2]) and for every $x, y \in G$

$$x \cdot' y = \phi^{-1}(\phi(x) \cdot_{M'} \phi(y)) = \phi^{-1}(x \cdot_G y) = x \cdot_G y.$$

By Proposition 1.1.3, we conclude that the operation $\cdot' : M \times M \to M$ and the inner product of M as a ring are actually the same, as desired. □

Definition 1.1.5 (Group ring)**.** Let G be a multiplicative group and R be a commutative ring. The *group ring of G over R*, that we will always denote with $R[G]$, is the associative R-algebra freely generated as an R-module by the set G and such that the ring product of $R[G]$ restricted to G coincides with the product of G ($R[G]$ exists and is unique by Corollary 1.1.4).

Every group ring can be described more precisely. Let G be a multiplicative group and R be a commutative ring. Since the set G is an R-basis of $R[G]$, every element $\alpha \in R[G]$ can be written as

$$\alpha = \sum_{x \in G} a_x \cdot x,$$

[2]It could be useful to know that ϕ^{-1} is an R-module morphism.

where, for all $x \in G$, the element α_x belongs to R (product and sum in the equality above are meant as product and sum of the R-algebra $R[G]$), only finitely many coefficients a_x are non zero and the choice of the coefficients a_x is unique (by Lemma A.1.3). The ring operations in $R[G]$ can be explicitly described. Given $\alpha,\ \beta \in R[G]$, we may write

$$\alpha = \sum_{x \in G} a_x \cdot x, \quad \beta = \sum_{x \in G} b_x \cdot x$$

where $a_x,\ b_x \in R$ for all $x \in G$; thanks to the properties that define an algebra (commutativity of the sum and distributivity of the scalar product) sum and product are, respectively,

$$\begin{aligned} \alpha + \beta &= \sum_{x \in G} (a_x + b_x) \cdot x, \\ \alpha \cdot \beta &= \sum_{x, y \in G} (a_x \cdot b_y) \cdot xy = \sum_{x \in G} \left(\sum_{y \in G} a_{xy^{-1}} \cdot b_y \right) \cdot x. \end{aligned}$$

Eventually, for every $a \in R$ we must have

$$a \cdot \alpha = \sum_{x \in G} (a \cdot a_x) \cdot x.$$

Remark 1.1.6. Let's remember that in a left (or right) module over a commutative ring R, the zero element coincides with the product of the zero element of R with any element of the module. Moreover, if the module is free generated by a multiplicative group G, then it's a ring with identity where the identity is given by the product of the identity of R with the identity of G. Summing up, denoting with $0_R,\ 1_R,\ 1_G$, respectively, the zero of R, the identity of R and the identity of G, we have that the identity and the zero element of $R[G]$ are, respectively,

$$\begin{aligned} 1_{R[G]} &= 1_R \cdot 1_G, \\ 0_{R[G]} &= \sum_{x \in G} 0_R \cdot x = 0_R \cdot 1_G. \end{aligned}$$

Notations. Until now, whenever a product appeared, we denoted it with a dot; from now on, we'll omit the dot whenever it will be clear that there's a multiplication. Second, until now, given a set X, if X was equipped with an operation (i.e. if X was an algebraic structure) and in X there was an identity relative to this operation, we denoted such identity with 1_X (if the operation was a product) or with 0_X (if the operation was a sum). From now on, we'll denote these identities with 1 or 0, depending on whether the operation is a product or a sum, omitting the subscript whenever it will be clear which algebraic structure X the identity belongs to.

Definition 1.1.7 (Support in group rings)**.** Let G be a group and R be a commutative ring. Given an element $\alpha \in R[G]$, there exists a set $\{ a_x \in R \mid x \in G \}$ such that $\alpha = \sum_{x \in G} a_x \cdot x$. The *support* of α is defined as the (finite) set

$$\mathrm{Supp}(\alpha) := \{ x \mid x \in G \ \wedge a_x \neq 0_R \}$$

(the support is-well defined since G is a basis for $R[G]$).

Definition 1.1.8 (Trivial units in group rings)**.** Let G be a group and R be a commutative ring. A non zero element $\alpha \in R[G]$ is said a *trivial unit* of the group ring if it is a unit and its support contains exactly one element.

Remark 1.1.9 (Equivalent definition of trivial units)**.** Let G be a group and R be a commutative ring. The trivial units of $R[G]$ are exactly the elements of the form

$$\alpha = a \cdot x$$

with $x \in G$, $a \in R$ and a unit. Indeed, for every choice of $x \in G$ together with a unit $a \in R$, the element $a \cdot x$ is a unit of $R[G]$, whose inverse is $a^{-1} \cdot x^{-1}$, since

$$(a \cdot x) \cdot (a^{-1} \cdot x^{-1}) = (a \cdot a^{-1}) \cdot (x \cdot x^{-1}) = 1_G \cdot 1_R$$
$$(a^{-1} \cdot x^{-1}) \cdot (a \cdot x) = (a^{-1} \cdot a) \cdot (x^{-1} \cdot x) = 1_G \cdot 1_R.$$

Conversely, if α is a trivial unit then, according to the definition above, there exist $a \in R$ and $x \in G$ such that $\alpha = a \cdot x$; we need to prove that a is a unit in R. Thanks to previous lines, $1_R \cdot x^{-1}$ is a unit in $R[G]$; therefore

$$\alpha \cdot (1_R \cdot x^{-1}) = a \cdot 1_G$$

is a unit in $R[G]$ (products of units give units); let $\beta \in R[G]$ be its inverse. We may assume that

$$\beta = \sum_{i=1}^{n} a_i \cdot x_i$$

with $n \in \mathbb{N}$ and, for all $i \in \mathbb{N}$, $a_i \in R$ and $x_i \in G$. Hence,

$$(a \cdot 1_G) \cdot \beta = \sum_{i=1}^{n} (a \cdot a_i) \cdot x_i = 1_R \cdot 1_G.$$

Without lost of generality, we may assume that the elements x_i, $i \in \mathbb{N}$, are pairwise distinct. Therefore, being G a basis for $R[G]$, last equality holds if and only if, up to reordering,

$$a \cdot a_1 = 1_R \ \wedge \ \forall_{1<i\leq n} \ a \cdot a_i = 0.$$

In particular, a_1 is a right inverse of a in R. Moreover, since unit in a ring are never zero divisors, we can conclude that for all $i \in \mathbb{N}$ with $1 < i \leq n$, $a_i = 0_R$ and therefore

$$\beta = a_1 \cdot 1_G.$$

At this point, using that β is a left inverse of α, we deduce that $a_1 \cdot a = 1_R$. Summing up, a_1 is both left and right inverse of a and so a is a unit in R.

Remark 1.1.10. Given a commutative ring R and a group G, we have the following canonical embeddings:

$$\begin{aligned} R &\longrightarrow R[G] \\ r &\longmapsto r \cdot 1_G \end{aligned} \qquad\qquad \begin{aligned} G &\longrightarrow R[G] \\ g &\longmapsto 1_R \cdot g \end{aligned}$$

These two maps are both injective ring homomorphisms, since $R[G]$ is an R-module with G as an R-basis. Therefore, from now on we will identify R and G with their images through their respective canonical embeddings in $R[G]$. In other words, for every $r \in R$ and $g \in G$ we can denote with r the element $r \cdot 1_G$ in $R[G]$ and with g the element $1_R \cdot g$ in $R[G]$.

Remark 1.1.11. Given a commutative ring R, a subring $S \subseteq R$ and a group G, we have the following canonical embedding:

$$S[G] \longrightarrow R[G] \tag{1.1}$$
$$\sum_{x\in G} s_x \cdot x \longmapsto \sum_{x\in G} s_x \cdot x \tag{1.2}$$

This is an injective ring homomorphism, since $S[G]$ is an S-module with G as an S-basis.

Lemma 1.1.12. *Let R be a commutative ring, G be a group and M be an R-algebra. Let $f : R[G] \to M$ be an R-module morphism. If the restriction of f to G preserves products, then f is an R-algebra homomorphism.*

Proof. Let R be a commutative ring, G be a group and M be an R-algebra. Let $f : R[G] \to M$ be an R-module morphism such that the restriction of f to G preserves product. To prove that f is an R-algebra homomorphism, we only have to prove that f preserves products. Take α and β in G, then for every $x \in G$ there exists $a_x, b_x \in R$ such that

$$\alpha = \sum_{x\in G} a_x \cdot x, \qquad \beta = \sum_{x\in G} b_x \cdot x,$$

where only finitely many coefficients a_x and b_x are non-zero. Therefore

$$\begin{aligned} f(\alpha\cdot\beta) &= f\Bigg(\sum_{x,y\in G} (a_x b_y)\cdot(xy)\Bigg) \\ &\overset{*}{=} \sum_{x,y\in G} (a_x b_y)\cdot f(xy) \\ &\overset{**}{=} \sum_{x,y\in G} (a_x b_y)\cdot f(x)f(y) \\ &= \sum_{x,y\in G} a_x \cdot f(x) \cdot \sum_{x,y\in G} b_y \cdot f(y) \overset{*}{=} f(\alpha)\cdot f(\beta) \end{aligned}$$

where equalities $*$ hold because f is an R-module morphism and equality $**$ holds because the restriction of f to G preserves products. ☐

Lemma 1.1.13. *Let $f : G \to H$ be a group homomorphism and R be an integral domain. There exists a unique R-algebra homomorphism $f^* : R[G] \to R[H]$ such that the following diagram commutes (where the vertical arrows are the canonical inclusions):*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & H \\ \big\downarrow & & \big\downarrow \\ R[G] & \xrightarrow{\ f^*\ } & R[H] \end{array}$$

Therefore, we can defined the injective map

$$\begin{aligned} \phi : \mathrm{Hom}_{\mathsf{Grp}}(G,H) &\longrightarrow \mathrm{Hom}_{R-\mathsf{Alg}}(R[G],R[H]) \\ f &\longmapsto f^* \end{aligned}$$

where Grp *and* $R - \mathsf{Alg}$ *are the categories of groups and R-algebras. Moreover, if $G = H$, ϕ restricts to a monomorphism of groups*

$$\begin{aligned} \psi : \mathrm{Aut}_{\mathsf{Grp}}(G) &\longrightarrow \mathrm{Aut}_{R-\mathsf{Alg}}(R[G]) \\ f &\longmapsto f^* \end{aligned}$$

Proof. Let $f : G \to H$ be a group homomorphism and R be an integral domain. We first prove the existence of $f^* : R[G] \to R[H]$. By definition, G freely generates $R[G]$ as a R-module therefore, by the universal property of free modules (Proposition A.1.4), there exists a unique R-module morphism $f^* : R[G] \to R[H]$ making the diagram

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ \downarrow & & \downarrow \\ R[G] & \xrightarrow{\quad f^* \quad} & R[H] \end{array}$$

commutative. Moreover, the restriction of f^* to G preserves the product, because f is a group homomorphism and the canonical inclusion $H \to R[H]$ is a ring homomorphism. Thanks to Lemma 1.1.12, f^* is an R-algebra homomorphism.

The map ϕ constructed in the statement is well-defined since we just proved that f^* exists and is unique. Moreover, if $f : G \to H$ and $g : G \to H$ are group homomorphism such that $f^* = g^*$ holds then, naming $i : H \to R[H]$ the canonical inclusion, we get that

$$i \circ f = f^*_{|G} = g^*_{|G} = i \circ g$$

holds but i is a monomorphism (i being injective) therefore last chain of equalities implies that $f = g$, that is ϕ is injective.

Let G be a fixed group. It remains to prove that the image of the map ψ defined in the statement actually lies in $\mathrm{Aut}_{R-\mathsf{Alg}}(R[G])$ and that ψ preserves compositions. Let $f : G \to G$ and $h : G \to G$ be automorphisms, then the following is a commutative diagram in the category of R-modules

$$\begin{array}{ccccc} G & \xrightarrow{\quad f \quad} & G & \xrightarrow{\quad h \quad} & G \\ \downarrow & & \downarrow & & \downarrow \\ R[G] & \xrightarrow{\quad f^* \quad} & K[G] & \xrightarrow{\quad h^* \quad} & R[G] \end{array}$$

Since, by definition, $(h \circ f)^*$ is the unique R-module morphism such that

$$\begin{array}{ccccc} G & \xrightarrow{\quad f \quad} & G & \xrightarrow{\quad h \quad} & G \\ \downarrow & & & & \downarrow \\ R[G] & & \xrightarrow{\qquad (h \circ f)^* \qquad} & & R[G] \end{array}$$

commutes we deduce that

$$(h \circ f)^* = h^* \circ f^* \tag{1.3}$$

holds. In particular,

$$\mathrm{id}_{R[G]} = (\mathrm{id}_G)^* = (f \circ f^{-1})^* = f^* \circ (f^{-1})^*,$$
$$\mathrm{id}_{R[G]} = (\mathrm{id}_G)^* = (f^{-1} \circ f)^* = (f^{-1})^* \circ f^*.$$

Thus f^* is an automorphism, that is ψ is well-defined. Eventually, the equality 1.3 implies that ψ preserves products, as desired. □

An important property of group rings is that all group rings of torsion free groups over fields are prime rings (Definition 1.1.14 and Corollary 1.1.16). This result was proved by Passman ([12], [13]); the proof provided by Passman needs some non-trivial facts regarding group theory and that abelian group rings have no non-trivial zero divisors (Theorem 2.2.5).

Definition 1.1.14 (Prime ring)**.** A ring R is said to be *prime* if $\alpha R \beta = 0$ for $\alpha,\ \beta \in R$ implies $\alpha = 0$ or $\beta = 0$.

Proposition 1.1.15. *Given a group G and a field K, the group ring $K[G]$ is prime if and only if G has no non-trivial finite normal subgroups.*

Proof of "$\Rightarrow$". Let K be a field and G be a group. Let's prove that if G has a non-trivial finite normal subgroup, then $K[G]$ is not prime. Let us assume that G has a non-trivial finite normal subgroup H. The idea is to find two non zero elements in $K[G]$ such that their product is zero and one of them is in the center of $K[G]$; this would imply, denoting with α and β these elements, with α in the center of $K[G]$, that

$$\alpha K[G] \beta = K[G] \alpha \beta = \{\, 0_{K[G]} \,\}.$$

The non zero element α will be chosen such that $\mathrm{Supp}(\alpha) = H$ (this is a non-absurd request since H is assumed to be finite): the fact that H is a non-trivial subgroup will be used to prove that α^2 is a scalar multiple of α and through this we will construct β; the fact that H is normal will be used to prove that α is in the center of $K[G]$. Set

$$\alpha := \sum_{h \in H} h.$$

This is a well-defined non zero element in $K[G]$ (H being finite). Since H is a subgroup, for every $h \in H$ the map $H \to H$ given by the left multiplication by h is well-defined and a bijection, thus

$$\alpha^2 = \sum_{h \in H} \left(\sum_{k \in H} hk \right) = \sum_{h \in H} \left(\sum_{g \in H} g \right) = |H| \alpha.$$

Set $\beta := \alpha - |H| \cdot 1_G$; then β isn't zero because $|\mathrm{Supp}(\alpha)| > 1$ (H being non-trivial), so $\mathrm{Supp}(\beta)$ contains at least two elements. Moreover $\alpha\beta = 0_{K[G]}$ holds. On the other hand, H being a normal subgroup, we have that for every $x \in G$

$$x \cdot \alpha = \sum_{h \in H} xh = \sum_{k \in xH} k = \sum_{k \in Hx} k = \sum_{h \in H} hx = \alpha \cdot x.$$

Thus, α commutes with all the elements in a basis of $K[G]$ as a K-module (G being such a basis) and, therefore, α is in the center of $K[G]$. Summing up, we have proved that

$$\alpha K[G] \beta = K[G] \alpha \beta = \{\, 0_{K[G]} \,\}.$$

Both α and β being non zero, we just proved that $K[G]$ is not a prime ring.

Proof of " $\Leftarrow$ " (idea). Let K be a field and let G be a group such that the identity group is its only finite normal subgroup. *Assume* for a contradiction that $K[G]$ is not a prime ring. Since $K[G]$ is assumed not to be a prime ring, there exist non-zero elements $\alpha,\ \beta \in K[G]$ such that $\alpha K[G]\beta$ is the zero ring. The idea is to consider a suitable subgroup of G, to use the assumption over G to prove that this subgroup is torsion free abelian and to use α and β to construct a non-trivial zero divisor in the group ring of this subgroup over the field K; this will contradict Theorem 2.2.5. Set

$$\Delta(G) := \{\, x \in G \mid x \text{ has only finitely many conjugates in } G \,\}\,.$$

This is a subgroup of G and the assumption that the only finite normal subgroup of G is the identity group implies that $\Delta(G)$ is an abelian torsion free group (this is an immediate consequence of [10, Lemma 19.3]).
Without lost of generality, we may assume that 1_G belongs to both the supports of α and β; indeed, taking $x \in \mathrm{Supp}(\alpha)$ and $y \in \mathrm{Supp}(\beta)$ (these supports are both non-empty since α and β are both non zero), one can replace α and β with, respectively, $x^{-1}\alpha$ and βy^{-1} because, certainly, $(x^{-1}\alpha)K[G](\beta y^{-1}) = 0$. The elements α and β can be written as

$$\alpha = \alpha_0 + \alpha_1 \text{ with } \mathrm{Supp}(\alpha_0) \subseteq \Delta(G) \text{ and } \mathrm{Supp}(\alpha_1) \subseteq (G \smallsetminus \Delta(G));$$
$$\beta = \beta_0 + \beta_1 \text{ with } \mathrm{Supp}(\beta_0) \subseteq \Delta(G) \text{ and } \mathrm{Supp}(\beta_1) \subseteq (G \smallsetminus \Delta(G)).$$

First, α_0 and β_0 are both non zero since 1_G belongs to $\Delta(G) \cap \mathrm{Supp}(\alpha) \cap \mathrm{Supp}(\beta)$. Second, $\alpha_0\beta_0 = 0_{K[\Delta(G)]}$ and this can be proved using that $\alpha K[G]\beta$ is the zero ring (the proof is not easy and requires some algebra facts; details can be found in the proof of [13, Theorem 1]). Summing up, α_0 is a zero divisor in $K[\Delta(G)]$. This gives the contradiction: since $\Delta(G)$ is torsion free abelian, $K[\Delta(G)]$ has no zero divisors different from zero (Theorem 2.2.5). □

Corollary 1.1.16. *If G is a torsion free group and K is a field, the group ring $K[G]$ is a prime ring.*

Proof. Since G is a torsion free group, no element in G different from the identity has finite order thus G cannot contain finite nontrivial subgroups. Hence, it follows from Proposition 1.1.15 that $K[G]$ is a prime ring. □

1.2 Kaplansky Conjectures and Their Relations

If K is a field and G is a torsion free group, exhibiting (or just proving the existence of) non-trivial units, non-zero zero divisors and non-trivial (under the usual meaning) idempotents in $K[G]$ becomes a very difficult problem, so difficult to think that in $K[G]$ (A) the only units are trivial, that (B) the zero is the only zero divisor and that (C) the identity and the zero are the only idempotents. These claims (A), (B) and (C) have been for many years just conjectures commonly known as, respectively, the *Kaplansky unit, zero divisor and idempotent conjectures.* Historically, the unit conjecture was first stated by Graham Higman in 1940 in his D.Phil thesis and then has been been revived by Kaplansky [5] in 1970. In the meanwhile, Kaplansky formulated the zero divisor conjecture as an open problem in 1957 [6, Problem 6]. The purpose of this section, is to formally formulate the Kaplansky conjectures (Definition 1.2.2) and to prove that the unit conjecture is stronger then the zero divisor conjecture (Theorem 1.2.9) and that the zero divisor conjecture, in turn, is stronger then the idempotent conjecture (Theorem 1.2.7).

1.2.1 Statements of the Kaplansky Conjectures

Remark 1.2.1. Let G be torsion free group and let K be a field. Let $\alpha \in K[G]$ be a trivial unit; the element α is idempotent if and only if $\alpha = 1_{K[G]}$ holds: being it a trivial unit, $\alpha = a \cdot x$ with $a \in K^\times$ (where $K^\times$ denotes the group of units of K) and $x \in G$ (Remark 1.1.9); thus $\alpha^2 = a^2 \cdot x^2$. Since G is a basis of $K[G]$ as a K-module, α is an idempotent if and only if both $a^2 = a$ and $x^2 = x$ hold, that is if and only if both a and x are idempotents[3]. This happens if and only if a is the identity of K (a can't be 0_K since α is non-zero) and x is the identity of G (the group G being torsion free). Summing up, α is idempotent if and only if $\alpha = 1_K \cdot 1_G$.

Definition 1.2.2 (Kaplansky conjectures)**.** Let G be a torsion free group and let K be a field. Under these assumptions, the statements of the three Kaplansky conjectures about group rings are the following.

Idempotent conjecture. The group ring $K[G]$ has no non-trivial idempotents. Equivalently, the idempotents of $K[G]$ are exactly $0_{K[G]}$ and $1_{K[G]}$.

Zero-divisor conjecture. The group ring $K[G]$ has no non-trivial zero divisors. Equivalently, the unique zero divisor of $K[G]$ is zero.

Unit conjecture. The group ring $K[G]$ has no non-trivial units.

Remark 1.2.3. The equivalence inside the formulation of first conjecture is proved in Remark 1.2.1.

Remark 1.2.4. The three Kaplansky conjectures are formulated for group rings over fields; this assumption is not too restrictive, according to what follows. Consider any of the three Kaplansky conjectures written above, then we claim that:

Claim. Given a group G, the thesis of the Kaplansky conjecture is true for every group ring $K[G]$, where K is a field, if and only if the same thesis is true for every group ring $R[G]$, where R is an integral domain.

Obviously, if for every ring R the group ring $R[G]$ satisfies a property, then for every field K the group ring $K[G]$ satisfies the same property. Conversely, if for every field K the group ring $K[G]$ realizes the thesis of a Kaplansky conjecture then for every integral domain R the group ring $R[G]$ realizes the same thesis because, given an integral domain R, the group ring $R[G]$ can be embedded in a group ring $K[G]$ over a field K (by Remark 1.1.11, because every integral domain embeds in a field) and every property stated in the Kaplansky conjectures is preserved when passing to subrings.

Remark 1.2.5. In the formulation of the zero divisor conjecture over a group ring $R[G]$, the assumptions that G is a torsion free group and R is an integral

[3]Remember that a field never contains idempotents different from zero and the identity (Theorem 1.2.7)

domain or the zero ring are necessary; equivalently, if G is a group with torsion or if R is a commutative ring with zero divisors different from 0_R, then the group ring $R[G]$ has at least one non-trivial zero divisor.

(i) Let R be a non-zero commutative ring but not a domain; let $a, b \in R$ be such that $ab = 0_R$ and let A, B be finite non-empty subsets of G. Set $\alpha := \sum_{x \in A} a \cdot x$ and $\beta := \sum_{x \in B} b \cdot x$; then $\alpha \cdot \beta = 0_{R[G]}$ holds. Thus, if a and b are non-zero, then α and β are non-trivial zero divisors for every choice of the finite non-empty subsets $A, B \subseteq G$.

(ii) Let G be a group with torsion; let $x \in G$ be a torsion element different from the identity of G. Let $n \in \mathbb{N}$ be a non zero number such that x^n is the identity of G. In $R[G]$ take

$$\alpha := x - 1_G, \quad \beta := 1 + x + x^2 + \cdots + x^{n-1}.$$

Then $\alpha \cdot \beta = 0_{R[G]}$ holds and α is non-trivial.

Remark 1.2.6. A last remark regarding the assumptions that G is a torsion free group and K is a field in the formulations of the Kaplansky conjectures: these assumptions are both used in the proofs of the connections between the three conjectures. More precisely, in the proof of Theorem 1.2.7 one uses that K is a field; in the proof of Theorem 1.2.9 one uses both that K is a field (when using Lemma 1.2.8 and Remark 1.2.1) and that G is torsion free. Anyway, both Theorems 1.2.7 and 1.2.9 are still true under the weaker assumption that K is a domain, since also Proposition 1.1.15, Corollary 1.1.16 and Lemma 1.2.8 are still true under this weaker assumption (and these three results are, explicitly or implicitly, used to prove Theorems 1.2.7 and 1.2.9).

1.2.2 Connections between the Kaplansky Conjectures

The three Kaplansky conjectures are closely connected to each other: given a group ring $K[G]$ where K is a field and G is a torsion free group, if $K[G]$ satisfies the unit conjecture then it satisfies the zero divisor conjecture (Theorem 1.2.9) and if it satisfies the zero divisor conjecture then it satisfies the idempotent conjecture (Theorem 1.2.7). These connections are briefly summarized by the following diagram:

$$\text{Unit conjecture} \implies \text{Zero divisor conjecture} \implies \text{Idempotent conjecture.}$$

Our aim in this subsection is to state and prove both these implications. The proof of the second implication is well-known; the idea is to prove that, in every ring, idempotent elements different from the identity are always zero divisors. The proof of the first implication is a bit more complicated; the idea is taken from Passman ([12, Lemma 1.2]) and uses the fact that a group ring over a field of a torsion free group is always a prime ring (Theorem 1.1.16).

Theorem 1.2.7. *In a ring with no non-zero zero divisors there are no idempotent elements different from the identity and zero. In particular, if a group ring over a field satisfies the zero divisor conjecture, then it also satisfies the idempotent conjecture.*

Proof. The second part of the statement follows immediately from the first part. To prove the first part, let R be a ring such that zero is the only zero divisor and let $a \in R$ be an idempotent element, that is $a^2 = a$ holds. Thus a satisfies $a(a-1_R) = 0_R$. Therefore, since the only zero divisor in R is 0_R by assumption, it follows that a can only be zero or the identity. □

Lemma 1.2.8. *Let G be a torsion free group and K be a field. The group ring $K[G]$ has a proper zero divisor (i.e., a zero divisor different from $0_{K[G]}$) if and only if it has a non-zero element of square zero.*

Proof. Let $K[G]$ be a group ring with a proper zero divisor $\alpha \neq 0_{K[G]}$. Hence, there exists a non-zero element $\beta \in K[G]$ such that $\alpha\beta = 0_{K[G]}$. This implies that $(\beta K[G]\alpha)(\beta K[G]\alpha)$ is the zero ring, hence the ring $\beta K[G]\alpha$ is formed only by elements of square zero. To conclude, it suffices to prove that $\beta K[G]\alpha$ is different from the zero ring. This follows directly from the fact that $K[G]$ is a prime ring (Corollary 1.1.16), G being torsion free by assumption.
Conversely, if $\alpha \in K[G]$ is a non-zero element of square zero then α is a zero divisor. □

Theorem 1.2.9. *Let G be a torsion free group and K be a field. If the group ring $K[G]$ has a proper zero divisor (i.e., a zero divisor different from $0_{K[G]}$), then it also has a non-trivial unit. Equivalently, if $K[G]$ satisfies the unit conjecture, then it also satisfies the zero divisor conjecture.*

Proof. Let G be a torsion free group, let K be a field and suppose that $K[G]$ has a proper zero divisor. By the previous lemma (Lemma 1.2.8), in the group ring $K[G]$ there exists a non zero element α of square zero. Therefore,

$$(1+\alpha)(1-\alpha) = 1,$$
$$(1-\alpha)(1+\alpha) = 1.$$

hold. These equalities imply that $\beta := 1+\alpha$ is a unit; to conclude it suffices to prove that β is a non-trivial unit. By contradiction, *assume* that there exist $r \in K$ and $g \in G$ such that $\beta = r \cdot g$; in particular, r is non-zero because β is non-zero (β being a unit). We have that

$$\begin{aligned} r^2 \cdot g^2 = \beta^2 = (1+\alpha)^2 &= 1 + 2\cdot\alpha \\ &= 1 + 2\cdot(\beta - 1) = 1 + 2\cdot(r\cdot g - 1) = 2r\cdot g - 1. \end{aligned}$$

Summing up,

$$1 - 2r\cdot g + r^2\cdot g^2 = 0.$$

The coefficients $2r$ and r^2 are not zero, because we're assuming r to be non-zero. It follows that at least one of the following equalities must be true:

$$g = 1_G, \qquad g = g^2, \qquad g^2 = 1_G.$$

The third one is possible if and only if $g = 1_G$ (since G is torsion free by assumption); the second one implies the first one; so, let us assume that $g = 1_G$. This implies that

$$\alpha = \beta - 1 = r\cdot g - 1 = r\cdot 1_G - 1 = (r - 1_R)\cdot 1_G.$$

This means, in particular, that α is a trivial unit (by Remark 1.1.9, α being non-zero by assumption). This is impossible because α is a zero divisor (since, by assumption, $\alpha^2 = 0$ holds) and a zero divisor can't be a unit. □

Chapter 2

Positive Results on the Kaplansky Conjectures

The search of proofs of the Kaplansky conjectures has been very intense in the world of mathematics in last half a century. Literature is full of articles which prove that a group ring $K[G]$ satisfies a certain Kaplansky conjecture under more or less restrictive assumptions on the group G or the field K. We present in this chapter some of these results: the basic ones that, in our opinion, everyone who approaches to the study of the Kaplansky conjectures should know. The classes of group rings $K[G]$ we're referring to are distinguished only by the properties satisfied by the group G, more precisely we will consider group rings $K[G]$ where K is any field and G is a unique product group, ordered group or an abelian group.

2.1 Preliminary Results of Group Theory

2.1.1 Unique Product Property

This subsection is dedicate to define and characterize unique product groups. Alongside the unique product property, we will define the two unique products property which, a priory, seems to be stronger than the unique product property. In 1980 Andrzej Strojnwski proved that these properties are actually equivalent; we provide here statement and proof by Strojnwski [16] (Proposition 2.1.3). The equivalence between the unique product property and the two unique products property is very useful to prove a central result in next section: every group ring of a unique product group has no non-trivial units (Theorem 2.2.2).

Definition 2.1.1 (U.p. group and t.u.p. group)**.** Let G be a multiplicative group. The group G satisfies the *unique product property* (briefly, G is a *u.p. group*) if for every pair of finite non empty subsets A, B of G there exists at least one element in $AB = \{ ab \mid a \in A,\ b \in B \}$ that can be uniquely represented as ab with $a \in A$ and $b \in B$. The group G satisfies the *two unique products property* (briefly, G is a *t.u.p. group*) if for every pair of finite non empty subsets A, B of G with $|A| + |B| > 2$ there exist in AB at least two elements such that each one of them can be uniquely represented as ab with $(a, b) \in A \times B$.

Lemma 2.1.2 (Unique product groups are torsion free)**.** *Let G be a unique product group; then G is torsion free.*

Proof. Let G be a unique product group. By contradiction, *assume* that $x \in G$ is a torsion element and let $n \in \mathbb{N}$ be a positive integer such that $x^n = 1_G$ holds. Set $A := \{ 1_G, x^{n-1} \}$ and $B := \{ 1_G, x \}$. Then $1_G = 1_G \cdot 1_G = x \cdot x^{n-1}$ where the pairs $(1_G, 1_G)$ and $(x^{n.1}, x)$ are distinct and both belong to $A \times B$ but this contradicts the assumption that G is a u.p. group. □

Proposition 2.1.3. *Let G be a group. The following conditions are equivalent:*

(i) G is a t.u.p. group;

(ii) For any nonempty finite subset A of the group G there exists at least one element in $AA = \{ xy : x, y \in A \}$ which has a unique representation in the form xy with $(x, y) \in A \times A$;

(iii) G is a u.p. group.

Proof. "(i) $\implies$ (ii)". Let G be a t.u.p group and $A \subseteq G$ be non-empty finite subset. If $|A| = 1$ then A obviously realizes condition (ii). If $|A| > 1$ then A realizes condition (ii) thanks to the two unique products property.

"(ii) $\implies$ (iii)". Let G be a group but not a unique product group; we'll prove that G doesn't satisfy condition (ii). Since the group G is not a u.p. group, there exists two finite non-empty subsets A, B of G such that any element in AB has at least two different representations as ab with $(a, b) \in A \times B$. Set $C := BA$; our aim is to prove that C is a subset of G thanks to which G can't satisfy condition (ii). The set C is non-empty and finite (both A and B being non-empty and finite). Let $x \in CC$ be arbitrary; this element can be written as $x = b_1a_1b_2a_2$ with $a_1,\ a_2 \in A$ and $b_1,\ b_2 \in B$. Consider the element $a_1b_2 \in AB$: our assumption over A and B implies that there exists a pair $(a_3, b_3) \in A \times B$ distinct from (a_1, b_2) such that $a_1b_2 = a_3b_3$ holds. Thus

$$x = (b_1a_1)(b_2a_2) = b_1(a_1b_2)a_2 = b_1(a_3b_3)a_2 = (b_1a_3)(b_3a_2)$$

holds and the inequality $(a_1, b_2) \neq (a_3, b_3)$ implies that

$$(b_1a_1, b_2a_2) \neq (b_1a_3, b_3a_2).$$

Therefore $x \in CC$ has two representations as c_1c_2 with $c_1,\ c_2 \in C$. Since $x \in C$ was arbitrary, it follows that the existence of the non-empty finite subset C of G denies the possibility that G satisfies condition (ii).

"(iii) $\implies$ (i)". Let G be a group but not a two unique products group; we'll prove that G is not a unique product group. Since the group G is not a two unique products group, there exists two finite subsets A, B of G with $|A| + |B| > 2$ such that in AB there exists exactly one element that admits a unique representation as product of an element in A and an element in B; let ab be such an element, where $(a, b) \in A \times B$. The idea is to construct two non-empty finite subsets E and F of G that deny the possibility that G satisfies the unique product property. We set $C := a^{-1}A$ and $D := Bb^{-1}$. Inside CD the element $1_G = a^{-1}abb^{-1} = 1_G1_G$ is the only element that admits a unique representation as a product of an element in C and an element in D. Indeed, in $A \times B$ and in $C \times D$ we can define the following equivalence relations:

$$\forall_{(x,y),(x',y') \in A \times B}\ (x,y) \sim_{A,B} (x',y') \text{ if } xy = x'y';$$
$$\forall_{(x,y),(x',y') \in C \times D}\ (x,y) \sim_{C,D} (x',y') \text{ if } xy = x'y'.$$

The fact that these are equivalence relations is easy to show. Moreover, the bijection

$$\begin{aligned} f : A \times B &\longrightarrow C \times D \\ (x,y) &\longmapsto (a^{-1}x, yb^{-1}) \end{aligned}$$

translates the equivalence relation defined in $A \times B$ in the equivalence relation defined in $C \times D$, i.e.

$$\begin{aligned} \forall_{(x,y),(x',y') \in A \times B}\ & (x,y) \sim_{A,B} (x',y') \\ & \iff (a^{-1}x, yb^{-1}) \sim_{C,D} (a^{-1}x', y'b^{-1}) \\ & \iff f(x,y) \sim_{C,D} f(x',y'). \end{aligned} \tag{2.1}$$

In particular, thanks to our assumption over the subsets A and B, exactly one equivalence class of the equivalence relation $\sim_{A,B}$ has cardinality equal to 1; therefore, since f is a bijection that satisfies the equivalences in 2.1, exactly one equivalence class of the equivalence relation $\sim_{C,D}$ has cardinality equal to 1 and this is the equivalence class containing

$$f(a,b) = a^{-1}abb^{-1} = 1_G.$$

We set $E := D^{-1}C$ and $F := DC^{-1}$; let $(x,y) \in E \times F$ be an arbitrary element. We will prove that there exists an element $(x',y') \in E \times F$ distinct from (x,y) such that $xy = x'y'$. First, by definition of E and F, there exist $c_1,\ c_2 \in C$ and $d_1,\ d_2 \in D$ such that $x = d_1^{-1}c_1$ and $y = d_2c_2^{-1}$. We distinguish three cases.

(a) If $(c_1, d_2) \neq (1_G, 1_G)$, then, there exists a pair $(c,d) \in C \times D$ distinct from (c_1, d_2) such that $c_1d_2 = cd$ holds. Thus, the pair $(x',y') := (d_1^{-1}c, dc_2^{-1}) \in E \times F$ is distinct from (x,y) and $xy = x'y'$.

(b) If $(c_1, d_2) = (1_G, 1_G)$ and $(c_2, d_1) \neq (1_G, 1_G)$, then, there exists a pair $(c,d) \in C \times D$ distinct from (c_2, d_1) such that $c_2d_1 = cd$ holds true; equivalently, we have the equality $d_1^{-1}c_2^{-1} = d^{-1}c^{-1}$. Thus, the pair $(x',y') := (d^{-1}1_G, 1_Gc^{-1})$ is distinct from (x,y) and $xy = x'y'$.

(c) In the last case, $(c_1, c_2, d_1, d_2) = (1_G, 1_G, 1_G, 1_G)$ holds. By assumption, one set between A and B contains at least two distinct elements; up to rename the subsets, we may assume that A has at least two elements. Therefore, C has at least one element distinct from $1_G \in C$; let c be such an element and set $(x',y') := (1_Gc, 1_Gc^{-1}) \in E \times F$. The pair (x',y') is distinct from (x,y) and $xy = x'y'$.

In each case, we exhibited an element $(x',y') \in E \times F$ distinct from (x,y) and such that $xy = x'y'$ holds. Thus, being the pair (x,y) arbitrary in $E \times F$, it follows that the two non empty finite subsets E and F of G defined above are such that any element in EF admits at least two representations as a product of an element in E and an element in F. We conclude that G can't satisfy the unique product property. □

Remark 2.1.4. An important question is if there exists an explicit example of a torsion free non-unique product group. Answering this question has been a non-trivial problem in the history of mathematics. The first example of a torsion free, non-unique product group was published in 1987 by Rips and Segev [15] and one year later Promislow [14] proved that the *Promislow group* is a torsion free non-unique product group. The problem of finding one example of a torsion free non-unique product group could be posed alongside the problem of finding a counterexample to the Kaplansky unit conjecture: indeed, every group ring over a unique product group always satisfies the Kaplansky unit conjecture (Theorem 2.2.2).

2.1.2 Ordered Groups

Definition 2.1.5. A group G is said to be a *right-ordered group* (*left-ordered group*) or, briefly, a *RO-group* (*LO-group*) if there exists a relation $\prec$ on G such that for all $x,\ y,\ z \in G$ the following properties are satisfied:

(i) *Transitivity.* If $x \prec y$ and $y \prec z$, then $x \prec z$ holds.

(ii) *Totality.* If $x \neq y$, then either $x \prec y$ or $y \prec x$ holds, but not both.

(iii) *Right (left) multiplication preserves order.* If $x \prec y$ then $xz \prec yz$ ($xz \prec yz$) holds.

Definition 2.1.6. A group G is said to be an *ordered group* if there exists a relation $\prec$ on G such that for all $x,\ y,\ z \in G$ the following properties are satisfied:

(i) *Transitivity.* If $x \prec y$ and $y \prec z$, then $x \prec z$ holds

(ii) *Totality.* If $x \neq y$, then either $x \prec y$ or $y \prec x$ holds, but not both.

(iii) *Left and right multiplications preserve order.* If $x \prec y$ then both $zx \prec zy$ and $xz \prec yz$ hold.

Remark 2.1.7. Let $(G, \prec)$ be a right-ordered group or a left-ordered group. There could be an element $x \in G$ such that $x \prec x$ holds. In particular, this fact together with property (iii) in the definition 2.1.5 applied to $z = x^{-1}$ and $y = x$ implies that $1_G \prec 1_G$ and so, thanks to the same property, for all $y \in G$, $y \prec y$ holds. As an example of this, consider the additive group $(\mathbb{Z}, \prec)$ where, describing the relation $\prec$ as a subset R of $\mathbb{Z} \times \mathbb{Z}$, we set $R := \{\, (a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b \,\}$. It's easy to check that this relation satisfies all the conditions in the definition 2.1.6, thus $(\mathbb{Z}, \prec)$ is an ordered group (in particular, a right-ordered and left-ordered group) and, for all $z \in Z$, (z, z) belongs to R, that is $z \prec z$ holds.

Remark 2.1.8. Let $(G, \prec)$ be a right-ordered (left-ordered) group. As observed in remark 2.1.7, there could be $x \in G$ such that $x \prec x$ holds. However, one can construct a new order relation $\prec'$ over the same group G such that $(G, \prec')$ is a right-ordered (left-ordered) group and for all $x \in G$ it never happens that $x \prec' x$ holds. Indeed, let $\prec'$ be the order relation on G defined as follows: for all $x,\ y \in G$,

$$x \prec' y \iff x \prec y \ \wedge \ x \neq y.$$

We prove that $(G, \prec')$ is a right-ordered (left-ordered) group.

(i) *Transitivity.* Let $x,\ y,\ z \in G$ be such that $x \prec' y \prec' z$; this means that

$$x \prec y \prec z \ \wedge \ x \neq y \ \wedge \ y \neq z.$$

By the transitivity of $\prec$ we have that $x \prec z$ holds true; to prove that $x \prec' z$ it remains to prove that x and z are distinct. By contradiction, *assume* that $x = z$. Then

$$x \prec y \ \wedge y \prec z = x.$$

Therefore, x and y need to be the same element, otherwise, if they were different to each other, last relations would contradict the fact that $\prec$ satisfies property (ii) in the definition 2.1.5. But we assumed x and y to be distinct, contradiction.

(ii) *Totality.* Immediate.

(iii) *Left and right multiplications preserve order.* Let $x,\ y \in G$ be such that $x \prec' y$; this means that $x \prec y$ and $x \neq y$. Let $z \in G$, we have to prove that $xz \prec' yz$ ($zx \prec' zy$). This is quite easy to show; indeed, thanks to the fact that $\prec$ satisfies property (iii) in the definition 2.1.5, we have that

$$x \prec y \ \wedge \ x \neq y \implies xz \prec yz \ \wedge \ xz \neq yz.$$

(analogously, if $(G, \prec')$ is a left-ordered group, then $x \prec' y$ implies $zx \prec zy$ and $zx \neq zy$).

Lemma 2.1.9. *Let $(G, \prec')$ be a left-ordered group (right-ordered group). Then there exists a relation $\prec$ in G such that $(G, \prec)$ is a right-ordered group (left-ordered group). Explicitly, $\prec$ is defined as follows: for every $x, y \in G$ we set $x \prec y$ if $y^{-1} \prec' x^{-1}$ holds.*

Proof. We prove just that a left-order relation generates a right-order relation; the other case is analogous. Let $(G, \prec)$ be a left-ordered group and let "$\prec'$" be a new relation over G defined as in the statement. We prove that "$\prec'$" satisfies the three condition defining a right-order relation. Let $x, y, z \in G$.

(i) *Transitivity.* If $x \prec' y \prec' z$, this means that $z^{-1} \prec y^{-1} \prec x^{-1}$ holds. Hence, by the transitivity of "$\prec$" it follows that $z^{-1} \prec x^{-1}$ holds, that is $x \prec' z$.

(ii) *Totality.* Immediate, because "$\prec$" is a total relation.

(iii) (*Right multiplication preserves order.* If $x \prec' y$, this means that $y^{-1} \prec x^{-1}$ holds. Since "$\prec$" is preserved by left multiplication, we obtain that $(yz)^{-1} = z^{-1}y^{-1} \prec z^{-1}x^{-1} = (xz)^{-1}$. Therefore, $xz \prec' yz$ holds. □

Through next lemmas, we will formulate some important properties regarding right-ordered and left-ordered groups, up to arrive to the most important result of this subsection: all right-ordered groups and all left-ordered groups are unique product groups. The reference for lemma 2.1.11 is [12, Lemma 13.1.4]. First, we need to define the *positive cone* associated to a right-order relation (left-order relation).

Definition 2.1.10. Let $(G, \prec)$ be a right-ordered (left-ordered) group. The *positive cone* of G is denoted with $P(G)$ (or with $P(G, \prec)$ if we need to specify the order relation that we're considering) and is defined as

$$P(G) := \{ x \in G \mid 1_G \prec x \wedge x \neq 1_G \} .$$

The positive cone characterizes the order relation, as expressed in next lemma.

Lemma 2.1.11. *Let $(G, \prec)$ be a right-ordered (left-ordered) group with positive cone $P = P(G)$, then*

(i) P is multiplicatively closed (that is, P is a subsemigroup of G);

(ii) $G = P \cup P^{-1} \cup \{ 1_G \}$ is a disjoint union.

Conversely, let G be a group and let $P \subseteq G$ be a subset satisfying conditions (i) and (ii), then G becomes both a right-ordered group and a left-ordered group:

- *for every $x, y \in G$ we set $x \prec y$ if $yx^{-1} \in P$, then $(G, \prec)$ is a RO-group;*
- *for every $x, y \in G$ we set $x \prec' y$ if $x^{-1}y \in P$, then $(G, \prec')$ is a LO-group.*

Moreover, both "$\prec$" and "$\prec'$" have P as positive cone.

Proof. We prove the first part of the statement just in the case of a right-ordered group; the case of a left-ordered group is analogous. Let G be a right-ordered group with positive cone $P = P(G)$. The set P is multiplicatively closed, indeed: let $x, y \in P$, then both $1 \prec x$ and $1 \prec y$ hold; from property (iii) in the definition of right-ordered group we get

$$1 \prec y = 1 \cdot y \prec x \cdot y;$$

hence xy belongs to P. About point (ii), by condition (ii) in the definition of right-ordered group we get that for every $x \in G$ with $x \neq 1_G$ then exactly one between $1_G \prec x$ and $x \prec 1_G$ holds. By property (iii) in the definition of right-ordered group we have that

$$x \prec 1_G \iff x \cdot x^{-1} \prec 1_G \cdot x^{-1} \iff 1 \prec x^{-1}.$$

Summing up, we just proved that for every $x \in G$ with $x \neq 1_G$, then exactly one element between x and x^{-1} belongs to P, that is x belongs to either P or P^{-1} but not both. Therefore, since by definition of positive cone 1_G doesn't belong to P, we get that $G = P \cup P^{-1} \cup \{ 1_G \}$ is a disjoint union.

Conversely, let G be a group, let $P \subseteq G$ be a subset satisfying conditions (i) and (ii) in the statement and let $\prec$ and $\prec'$ be relations over G defined as in the statement. To prove that both $\prec$ and $\prec'$ are transitive, let $x, y, z \in G$, then

$$x \prec y \prec z \Longrightarrow (yx^{-1} \in P \wedge zy^{-1} \in P) \overset{*}{\Longrightarrow} zx^{-1} = zy^{-1}yx^{-1} \in P \Longrightarrow x \prec z$$

and

$$x \prec' y \prec' z \Longrightarrow (x^{-1}y \in P \wedge y^{-1}z \in P) \overset{*}{\Longrightarrow} x^{-1}z = x^{-1}yy^{-1}z \in P \Longrightarrow x \prec' z,$$

where in the implication $*$ we used that P is multiplicatively closed. Now we prove that $\prec$ is a total relation. Let $x, y \in G$ be distinct elements, then by definition $x \prec y$ if $yx^{-1} \in P$ and

$$y \prec x \Longleftrightarrow xy^{-1} \in P \Longleftrightarrow yx^{-1} \in P^{-1}.$$

Since $yx^{-1} \neq 1_G$ holds (x and y being distinct) and since $G = P \cup P^{-1} \cup \{ 1_G \}$ is a disjoint union by assumption, it follows that yx^{-1} belongs to either P or P^{-1} but not both, that is at least one between $x \prec y$ or $y \prec x$ holds, but not both. The proof that $\prec'$ is total is analogous. Eventually, we prove that right-product and left-product preserve, respectively, the relation $\prec$ and the relation $\prec'$. Let $x, y, z \in G$, then

$$x \prec y \Longrightarrow yx^{-1} \in P \overset{*}{\Longrightarrow} (yz)(xz)^{-1} = yx^{-1} \in P \Longrightarrow xz \prec yz$$

and

$$x \prec' y \Longrightarrow x^{-1}y \in P \overset{*}{\Longrightarrow} (zx)^{-1}(zy) = x^{-1}y \in P \Longrightarrow zx \prec' zy,$$

where in the implication $*$ we used that P is multiplicatively closed. The last sentence of the statement of the lemma is immediate. □

Lemma 2.1.12. *Let $(G, \prec)$ be a right-ordered group and let P be the associated positive cone. Then $(G, \prec)$ is an ordered group if and only if P satisfies the following condition:*

$$\forall_{x \in G}\ xPx^{-1} \subseteq P.$$

Proof. Let $(G, \prec)$ be a right-ordered group and let P be its positive cone. Then $(G, \prec)$ is an ordered group if and only if left multiplication preserves the order. Let $x, y, z \in G$; by the fact that right product preserves order, we have that $x \prec y$ holds if and only if $1 \prec yx^{-1}$ holds and $zx \prec zy$ holds if and only if $1 \prec zy(zx)^{-1}$ holds. Therefore, by the definition of positive cone, the condition

$$\forall_{x,y,z \in G}\ x \prec y \Longrightarrow zx \prec zy$$

is equivalent to

$$\forall_{x,y,z \in G}\ yx^{-1} \in P \Longrightarrow zyx^{-1}z^{-1} \in P. \tag{2.2}$$

Last condition is equivalent to require that for all $z \in G$, $zPz^{-1} \subseteq P$ holds. Indeed:

- if P satisfies condition 2.2, applying it to $x = 1_G$ we get that for all $z \in G$ and $y \in P$, the element zyz^{-1} belongs to P, that is: for all $z \in G$, zPz^{-1} is a subset of P;

- conversely, if for all $z \in G$, $zPz^{-1} \subseteq P$ holds then it immediately follows that condition 2.2 holds. □

Next lemma gives two useful properties of finite non-empty subsets of right-ordered (left-ordered) groups.

Lemma 2.1.13. *Let $(G, \prec)$ be a right-ordered (left-ordered) group. Let A be a finite non-empty subset of G and let $n \in \mathbb{N}$ be the cardinality of A.*

1. There exists $x_A \in A$ *such that*

$$\forall_{y \in A \smallsetminus \{ x_A \}} \; y \prec x_A.$$

2. There exists a bijection $f : \{ i \in \mathbb{N} \mid 1 \leq i \leq n \} \longrightarrow A$ *such that*

$$\forall_{i,j \in \mathbb{N},\, 1 \leq i,j \leq n} \; i < j \Longrightarrow f(i) \prec f(j).$$

Proof. 1. Let $(G, \prec)$ be a right-ordered (left-ordered) group and $A \subseteq G$ be a finite non-empty subset. If $|A| = 1$ the claim is trivial. For the case $|A| = 2$ we prove the claim by contradiction. *Assume* that the claim is false; this means that for every $x \in A$ there exists $y \in A \smallsetminus \{ x \}$ such that $x \prec y$ holds. We fix $x \in A$ (it exists since A is non-empty). We inductively define a sequence of elements in A as follows: we set $x_1 := x$ and, for every $n \geq 2$, $n \in \mathbb{N}$, we fix $x_n \in A \smallsetminus \{ x_{n-1} \}$ such that $x_{n-1} \prec x_n$ holds (x_n is well-defined by our assumption over A). Being A finite, there exists two distinct indices $i, j \in \mathbb{N}$ such that $x_i = x_j$; we may assume $i < j$. More precisely, $i+1 < j$ holds because, by construction, x_i and x_{i+1} are distinct. We have the chain

$$x_i \prec x_{i+1} \prec \cdots \prec x_j$$

and so, thanks to transitivity property,

$$x_i \prec x_{i+1} \;\wedge x_{i+1} \prec x_j = x_i.$$

It follows that $x_i = x_{i+1}$ holds because of property (ii) in the definition of right-ordered group, but this is impossible since x_{i+1} belongs to $A \smallsetminus \{ x_i \}$.

2. Let $(G, \prec)$ be a right-ordered (left-ordered) group and $A \subseteq G$ be a finite non-empty subset. We prove the claim by induction on $n = |A| \in \mathbb{N}_{>0}$. If $|A| = 1$ the claim is trivial. We now assume that $n \geq 2$ and that the claim holds for all finite non-empty subsets $B \subseteq G$ with $|B| < n$. By the first claim of the Lemma we're proving, there exists $x_A \in A$ such that

$$\forall_{y \in A \smallsetminus \{ x_A \}} \; y \prec x_A$$

holds. We set $B := A \smallsetminus \{ x_A \}$. The set B is non-empty since $|A| \geq 2$ by assumption; in particular, $|B| = n - 1$. Thus, by induction, there exists a bijection $f : \{ i \in \mathbb{N} \mid 1 \leq i \leq n - 1 \} \longrightarrow B$ such that

$$\forall_{i,j \in \mathbb{N},\, 1 \leq i,j \leq n-1} \; i < j \Longrightarrow f(i) \prec f(j).$$

Now we set

$$\begin{aligned} f' : \{ i \in \mathbb{N} \mid 1 \leq i \leq n \} &\longrightarrow A \\ i &\longmapsto \begin{cases} f(i) & \text{if } i < n \\ x_A & \text{if } i = n. \end{cases} \end{aligned}$$

The map f' is bijective (easy to show) and for every $i, j \in \mathbb{N}$ with $1 \leq i < j \leq n$,

- if $j \neq n$ then $f'(i) = f(i) \prec f(j) = f'(j)$, by assumption over f;
- if $j = n$ then $f'(i) = f(i) \prec x_A = f'(j)$, by assumption over x_A. □

Theorem 2.1.14. *Let $(G, \prec)$ be a right-ordered (left-ordered) group. Then G is a unique product group.*

Proof. It suffices to give the proof for right-ordered groups; indeed, if G is a group endowed with a left-order relation then, by Lemma 2.1.9, it can also be endowed with a right-order relation; hence, if all right-ordered groups are u.p. groups, G is a u.p. group. Let $(G, \prec)$ be a right-ordered group and let A and B be finite non-empty subsets of G. Without lost of generality, we may assume that the following condition holds:

$$\forall_{x,y\in G}\ x \prec y \Longrightarrow x \neq y. \tag{2.3}$$

Indeed, if this condition is not satisfied, by Remark 2.1.8 we can replace the order relation in G with a new order relation that satisfies this condition. Our aim is to find $(a^*, b^*) \in A \times B$ such that for every $(a, b) \in A \times B \setminus \{ (a^*, b^*) \}$, the relation $a^*b^* \prec ab$ holds. The conclusion will follow from condition 2.3. Let $n = |A|$ and $m = |B|$; by point 2 of Lemma 2.1.13 we can write

$$A = \{ x_i \mid i \in \mathbb{N} \wedge 1 \leq i \leq n \} \text{ with } x_1 \prec x_2 \prec \cdots \prec x_n \tag{2.4}$$

and

$$B = \{ y_j \mid j \in \mathbb{N} \wedge 1 \leq j \leq m \} \text{ with } y_1 \prec y_2 \prec \cdots \prec y_m.$$

To figure out how to exhibit the element (a^*, b^*), we consider an $n \times m$ matrix where the entry indexed by $(i, j) \in \{ 1, \dots, n \} \times \{ 1, \dots, m \}$ is given by x_iy_j:

$$\begin{pmatrix} x_1y_1 & x_1y_2 & \dots & x_1y_m \\ x_2y_1 & x_2y_2 & \dots & x_2y_m \\ \dots & \dots & \dots & \dots \\ x_ny_1 & x_ny_2 & \dots & x_ny_m \end{pmatrix}.$$

For every $j \in \mathbb{N}$ with $1 \leq j \leq m$, the elements in the j-th column are related as follows:

$$x_1y_j \prec x_2y_j \prec \cdots \prec x_ny_j \tag{2.5}$$

(because of property (iii) in the definition of right-ordered group applied to the chain of relations in 2.4). Hence, the idea is to search a^*b^* between the elements in the first line of the matrix. We set

$$C := \{ x_1y_j \mid j \in \mathbb{N} \wedge 1 \leq j \leq m \} \subseteq AB.$$

From point 2 of Lemma 2.1.13, it follows that there exists $j^* \in \mathbb{N}$ with $1 \leq j^* \leq m$ such that

$$\forall_{j\in\mathbb{N}\wedge 1\leq j\leq m}\ j \neq j^* \Longrightarrow x_1y_{j^*} \prec x_1y_j. \tag{2.6}$$

Our aim now is to prove that for every pair $(x_i, y_j) \in A \times B$ distinct from (x_1, y_{j^*}), $x_1y_{j^*} \prec x_iy_j$ holds. Let $(x_i, x_j) \in (A \times B) \setminus \{ (x_1, y_{j^*}) \}$.

- If $i = 1$ then $j \neq j^*$ holds. Hence, by the implication in 2.6, the relation $x_1y_{j^*} \prec x_1y_j = x_iy_j$ holds.
- If $j = j^*$ then $i \neq 1$. Applying the transitivity property to the chain of relations in 2.5, we get $x_iy_{j^*} = x_1y_j \prec x_iy_j$.

- If $i \neq 1$ and $j \neq j^*$ then $x_1 y_{j^*} \prec x_1 y_j \prec x_i y_j$, where the first relation follows from the first point and the second relation follows from the transitivity property applied to the chain of relations in 2.5. Hence, $x_1 y_{j^*} \prec x_i y_j$ holds.

In conclusion, we can set $(a^*, b^*) := (x_1, x_{j^*})$. We just showed that for every $(a, b) \in A \times B \setminus \{ (a, b) \}$, $a^* b^* \prec ab$ holds and, by condition 2.3, this implies that $a^* b^* \neq ab$ holds, as desired. □

Corollary 2.1.15. *Let G be a right-ordered (left-ordered) group. Then G is torsion free.*

Proof. Let G be a right-ordered (left-ordered) group. By Theorem 2.1.14, G is a unique product group thus, by Lemma 2.1.2, G is torsion free. □

Last two results we are going to present in this subsection will be applied, respectively, in the next section and in the first section of next chapter. Precisely, Lemma 2.1.16 will be used to prove that the central group inside a suitable short exact sequence of groups is a right ordered group (Theorem 2.1.25); Lemma 2.1.17 will be used to prove that the *Promislow group* (a group we will present in next chapter) is not a right-ordered group (Lemma 3.1.7). These two facts together will allow us to deduce that the Promislow group is, in some sense (as we will explain), the "smallest" group that gives a counterexample to the unit conjecture.

Lemma 2.1.16. *Let G be a group and $N \lhd G$ be a normal subgroup. If N and G/N are both right-ordered groups, then so is G.*

Proof. Let G be a group and $N \lhd G$ be a normal subgroup such that both N and G/N are right-ordered groups. Our aim is to prove that G is right-ordered applying second part of Lemma 2.1.11: we will construct a positive cone for G using the positive cones of N and G/N. Let $P(N)$ and $P(G/N)$ be the positive cones associated to the right-order relations over, respectively, N and G/N. Let $\pi : G \to G/N$ be the canonical projection and $Q \subseteq G$ be a family of coset representatives of the elements in $P(G/N) \subseteq G/N$; that is, π restricted to Q is injective and $\pi(Q) = P(G/N)$. Applying condition (ii) in Lemma 2.1.11 we get the disjoint union

$$G/N = P(G/N) \cup P(G/N)^{-1} \cup \{ 1_{G/N} \} = \pi(Q) \cup \pi(Q^{-1}) \cup \pi(\{ 1_G \}).$$

Hence $Q \cup Q^{-1} \cup \{ 1_G \}$ is a disjoint union (the union above being disjoint) and, since $\pi_{|Q}$ is injective, $Q \cup Q^{-1} \cup \{ 1_G \}$ is a transversal for N in G. Therefore, we get the following disjoint union

$$G = \Big(\bigcup_{x \in Q} xN \Big) \cup \Big(\bigcup_{x \in Q^{-1}} xN \Big) \cup 1_G N. \tag{2.7}$$

By definition of Q and by point (ii) in Lemma 2.1.11 applied to $P(N)$ we get

$$\bigcup_{x \in Q} xN = \{ x \in G \mid \pi(x) \in P(G/N) \},$$

$$\bigcup_{x \in Q^{-1}} xN = \{ x \in G \mid \pi(x) \in P(G/N)^{-1} \} = \{ x \in G \mid \pi(x) \in P(G/N) \}^{-1},$$

$$N = P(N) \cup P(N)^{-1} \cup \{ 1_G \}.$$

We define

$$P := \{ x \in G \mid \pi(x) \in P(G/N) \} \cup P(N).$$

Summing up, the disjoint union in 2.7 becomes

$$G = P \cup P^{-1} \cup \{ 1_G \}$$

Since this last union is disjoint, thanks to Lemma 2.1.11 to prove that G is a right-ordered group it suffices to prove that P is multiplicatively closed. Remembering that $P(N)$ and $P(G/N)$ are both multiplicatively closed, we can deduce that P is union of multiplicatively closed sets. Moreover, let $y \in P(N)$ and $x \in \{ x \in G \mid \pi(x) \in P(G/N) \}$; we have that (because of y belongs to N)

$$\pi(xy) = \pi(x)\pi(y) = \pi(x) \in P(G/N)$$
$$\pi(yx) = \pi(y)\pi(x) = \pi(x) \in P(G/N),$$

where we used that x belongs to $\{ x \in G \mid \pi(x) \in P(G/N) \}$. It follows that both xy and yx belongs to $\{ x \in G \mid \pi(x) \in P(G/N) \} \subseteq P$ and this concludes the proof that P is multiplicatively closed. □

Lemma 2.1.17. *Let G be a right-ordered group. Let A be a finite non-empty subset of G such that the identity of G doesn't belong to it. Then, for every $x \in A$ there exists $\epsilon_x \in \{ 1, -1 \}$ such that the identity of G doesn't belong to the subsemigroup of G generated*[1] *by $\{ x^{\epsilon_x} \mid x \in G \}$.*

Proof. Let G be a right-ordered group and $A \subseteq G$ be a finite non-empty subset such that the identity of G doesn't belong to it. Let "$\prec$" be a right-order relation over G and let $P \subset G$ be the positive cone associated to the fixed order relation. We know that P is multiplicatively closed (Lemma 2.1.11) and that $1_G \notin P$ (by definition of positive cone) hence every subsemigorup of G generated by elements belonging P is contained in P and, therefore, is such that the identity of G doesn't belong to it. Knowing this, to conclude the proof it suffices to prove that for every $x \in A$ there exists one element inside $\{ x, x^{-1} \}$ that belongs to P. Let $x \in A$ because. Then, by definition of right-order relation, one between the following relations holds:

$$1 \prec x \qquad\qquad \text{or} \qquad\qquad x \prec 1$$

(x is not the identity by assumption over A). Again by definition of right-order relation, $x \prec 1$ is equivalent to $1 \prec x^{-1}$. We can deduce that one element in $\{ x, x^{-1} \}$ belongs to P, as desired. □

Remark 2.1.18. The converse of Lemma 2.1.17 is also true, that is: if G is a group such that for every finite non-empty subset $A \subseteq G$ the claim of Lemma 2.1.17 is satisfied, then G is a right-ordered group. We don't formally formulate and prove here this implication because it's not necessary for our purposes; a reference for it is [12, Lemma 13.2.1].

[1] The subsemigroup $S(X)$ of a group G generated by a subset $X \subseteq G$ is, set-theoretically, the subset of G that contains, for every $n \in \mathbb{N} \setminus \{ 0 \}$, all the products of n elements belonging to A. Then $S(X)$ is a semigroup where the product is inherited from the product in G.

2.1.3 Examples of Unique Product Groups

In this subsection we will see classes of groups that are *RO*-groups, *O*-groups and u.p. groups. We will start constructing explicitly an order relation over $\mathbb{Z}^n$ for every $n \in \mathbb{N}$ (Example 2.1.19). Next, we'll prove that all torsion free abelian groups are ordered groups and so unique product groups (Proposition 2.1.20); about this result, the proof we will provide is taken from Passmann's proof of [12, Lemma 13.1.6], which uses Zorn's Lemma. As a consequence, we'll deduce that special solvable groups are *RO*-groups and so unique product groups (Proposition 2.1.22, whose reference is [12, Lemma 13.1.6]). Eventually, we will prove that every group extension of an abelian group by a finite cyclic group is a *poly-infinite-cyclic group* (Definition 2.1.23) and so both a right-ordered group and a u.p. group (Theorem 2.1.25, whose reference is [12, Lemma 13.3.1]).

Example 2.1.19. , The additive group $\mathbb{Z}^n$ is an ordered group for every $n \in \mathbb{N}$. Let $n \in \mathbb{N}$ fixed. We define a relation "$\prec$" on $\mathbb{Z}^n$ as follows: given two distinct elements $(a_1, \dots, a_n),\ (b_1, \dots, b_n) \in \mathbb{Z}^n$ we set

$$(a_1, \dots, a_n) \prec (b_1, \dots, b_n) \text{ if } a_s < b_s \text{ for } s := \min \{ i \in \mathbb{N} : 1 \le i \le n \wedge a_i \neq b_i \} .$$

We want to prove that this relation is an order relations satisfying the three conditions in the Definition 2.1.6.

(i) *Transitivity.* Let $(a_1, \dots, a_n),\ (b_1, \dots, b_n), (c_1, \dots, c_n) \in \mathbb{Z}^n$ be such that

$$(a_1, \dots, a_n) \prec (b_1, \dots, b_n) \prec (c_1, \dots, c_n).$$

By definition, there exist $h, k \in \mathbb{N}$ such that

$$\forall_{i \in \mathbb{N} \text{ with } 1 \le i < h}\ a_i = b_i \ \wedge \ a_h < b_h,$$

$$\forall_{i \in \mathbb{N} \text{ with } 1 \le i < k}\ b_i = c_i \ \wedge \ b_k < c_k.$$

Set $s := \min\{ h, k \}$. For every $i \in \mathbb{N}$ with $1 \le i < s$ we have that $a_i = b_i = c_i$ holds true. Moreover the inequality $a_s < c_s$ holds because

- if $s = h \le k$ then $a_s < b_s \le c_s$;
- if $s = k \le h$ then $a_s \le b_s < c_s$.

We can conclude that $(a_1, \dots, a_n) \prec (c_1, \dots, c_n)$, as desired.

(ii) *Totality.* Immediate.

(iii) *Sum preserves the order.* Let $(a_1, \dots, a_n),\ (b_1, \dots, b_n), (c_1, \dots, c_n) \in \mathbb{Z}^n$ be such that

$$(a_1, \dots, a_n) \prec (b_1, \dots, b_n).$$

By definition, there exists $h \in \mathbb{N}$ such that

$$\forall_{i \in \mathbb{N} \text{ with } 1 \le i < h}\ a_i = b_i \ \wedge \ a_h < b_h.$$

Thus, for every $i \in \mathbb{N}$ with $1 \le i < h$ we have that $a_i + c_i = b_i + c_i$ and $a_h + c_h < b_h + c_h$ hold. We can conclude that

$$(a_1 + c_1, \dots, a_n + c_n) \prec (b_1 + c_1, \dots, b_n + c_n).$$

Proposition 2.1.20. *Let G be a group. If G is abelian torsion free, then G is an ordered group and so a unique product group.*

Proof. The claim is immediate when the group is the trivial group. Therefore, we consider the case of non-trivial groups. Let G be a non-trivial abelian torsion free group. If G is a right-ordered group then G an ordered group because left and right multiplication in G are actually the same, G being abelian; moreover, G is a unique product group by theorem 2.1.14. Hence, we only have to prove that G is a right-ordered group. The proof we provide here uses Zorn's Lemma. The idea is to prove that G admits a multiplicatively closed subset P maximal with respect to the "inclusion relation" and that doesn't contain 1_G; then we want to apply Lemma 2.1.11 to prove that P is a positive cone associated to a right-order relation "$\prec$". Set

$$\mathcal{P} = \{\, A \subseteq G \mid A \text{ is multiplicatively closed, non-empty and } 1_G \notin A \,\}\,.$$

The set $\mathcal{P}$ is non-empty because we can take $x \in G$ with $x \neq 1_G$ (G not being the trivial group) and the set

$$X = \{\, x^n \mid n \in \mathbb{N} \ \wedge\ n \neq 0 \,\}$$

is multiplicatively closed, non-empty and 1_G doesn't belong to X because G is torsion free; hence X belongs to $\mathcal{P}$. We endow $\mathcal{P}$ with the order relation given by the inclusion between sets:

$$\forall_{A,B\in\mathcal{P}}\ A \leq B \text{ if } A \subseteq B.$$

Given an ascendant chain $(A_n)_{n\in\mathbb{N}}$ in $\mathcal{P}$, it has a majority element given by

$$A := \bigcup_{n\in\mathbb{N}} A_n.$$

Indeed, A is non-empty and $1_G \notin A$ because A is union of non-empty sets not containing 1_G; A is multiplicatively closed because given a pair of elements in A, there exists $n \in \mathbb{N}$ such that both the elements are in A_n (the chain being ascendant) and A_n is multiplicatively closed. Hence, A belongs to $\mathcal{P}$ and, for every $n \in \mathbb{N}$, $A_n \leq A$ holds. We can apply Zorn's Lemma: $\mathcal{P}$ has a maximal element; let P be such a maximal element. To conclude it remains to prove that P satisfies both conditions (i) and (ii) in Lemma 2.1.11.

- P is multiplicatively closed because P belongs to $\mathcal{P}$.
- $P \cup P^{-1} \cup \{\, 1_G \,\}$ is a disjoint union because $1_G \notin P$ and if, by contradiction, there exists $x \in P \cap P^{-1}$ then, since $x \in P^{-1}$, there exists $y \in P$ such that $y = x^{-1}$ holds and so, since $x \in P$ and P is multiplicatively closed, $1_G = xy \in P$ but this is impossible, P belonging to $\mathcal{P}$.
- $G = P \cup P^{-1} \cup \{\, 1_G \,\}$ holds. *Assume*, by contradiction, that there exists $x \in G$ with $x \notin P \cup P^{-1} \cup \{\, 1_G \,\}$ and set

$$M := P \cup \{\, x^n \cdot p \mid n \in \mathbb{N} \ \wedge\ n \neq 0 \ \wedge\ p \in P \,\}\,,$$
$$M' := P \cup \{\, x^{-n} \cdot p \mid n \in \mathbb{N} \ \wedge\ n \neq 0 \ \wedge\ p \in P \,\}\,,$$

Both M and M' are non-empty and multiplicatively closed because G is abelian and P is multiplicatively closed. Since P is a subset of both M and M' and P is maximal in $\mathcal{P}$, then necessarily M and M' don't belong to $\mathcal{P}$ and this means that $1_G \in M \cap M'$. Since P doesn't contain 1_G we get that

$$\exists n \in \mathbb{N}_{>0},\ \exists p \in P \text{ such that } x^n p = 1_G$$

and

$$\exists m \in \mathbb{N}_{>0},\ \exists q \in P \text{ such that } x^{-m} q = 1_G.$$

Therefore

$$1_G = (x^n)^m \cdot (x^{-m})^{-n} = p^{-m} \cdot q^n$$

and last product belongs to P because P is multiplicatively closed (we used that $m \neq 0 \neq n$). Thus $1_G \in P$ but this contradicts that $P \in \mathcal{P}$. □

Remark 2.1.21. A special case of Proposition 2.1.20 is given by torsion free finitely generated abelian groups. In this case, proving that these groups are ordered groups (so, unique product groups) is easier. Indeed, let G be a finitely generated torsion free abelian group. By the fundamental theorem of finitely generated abelian groups, there exists $n \in \mathbb{N}$ such that G is isomorphic to $\mathbb{Z}^n$ (because G is torsion free). In Example 2.1.19 we proved that $\mathbb{Z}^n$ is an ordered group and this property is stable under isomorphism (easy to check), hence G is an ordered group.

Proposition 2.1.22. *Let G be a group. If G has a finite subnormal series*

$$\langle 1_G \rangle = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

with, for all $i = 1, \dots, n$, quotient G_i/G_{i-1} which is a torsion free abelian group, then G is a right-ordered group and a unique product group.

Proof. Let G be a group and let $\langle 1_G \rangle = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ as in the statement. If G is a right-ordered group then G is a unique product group by Theorem 2.1.14. Thus, we only have to prove that G is a right-ordered group. We prove it by induction over the length $n \in \mathbb{N}$ of the subnormal series.

- If $n = 0$ then G is the trivial group, hence it's a right-ordered group.
- We now suppose that $n \geq 1$ and that the claim holds for every group that admits a subnormal series that satisfies the assumptions in the statement and whose length is $n - 1$. In particular, this inductive assumption implies that G_{n-1} is a right-ordered group. On the other hand, $G/G_{n-1} = G_n/G_{n-1}$ is torsion free abelian by assumption, hence G/G_{n-1} is a right-ordered group by Proposition 2.1.20. Therefore, since both G_{n-1} and G_{n-1} are *RO*-groups, by Lemma 2.1.16 we can conclude that G is a right-ordered group. □

Definition 2.1.23 (Poly-infinite-cyclic groups)**.** A group G is said to be a *poly-infinite-cyclic group* if it admits a finite subnormal series

$$\langle 1_G \rangle = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

with, for all $i = 1, \dots, n$, quotients G_i/G_{i-1} infinite cyclic groups.

Remark 2.1.24. Every poly-infinite-cyclic group is a right-ordered group and a unique product group because a poly-infinite-cyclic group always satisfies assumptions of proposition 2.1.22. To prove this just use that a cyclic group is always abelian and that every infinite cyclic group is necessarily torsion free.

Theorem 2.1.25. *Let G be a finitely generated torsion free group. Suppose that G has a normal abelian subgroup A such that G/A is finite and cyclic. Then G is a poly-infinite-cyclic group and hence it is both a right-ordered group and a unique product group.*

Proof. Let G be a finitely generated torsion free group. Let A be a normal abelian subgroup of G and suppose that G/A is finite and cyclic. If G is poly-infinite-cyclic, then G is both a right-ordered group and a unique product group by Remark 2.1.24. Therefore, to prove the theorem we only have to prove that G is poly-infinite-cyclic. This proof needs the concept of *rank* of finitely generated abelian groups together with two lemmas; we report here everything we need (some details can be found in the Appendix A.2)

Definition A (Definition A.2.1 in the Appendix)**.** Let G be a finitely generated abelian group. The *rank* of G is the dimension of $G \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space and is denoted with $\operatorname{rank}(G)$.

Lemma B (from [12, Lemma 4.1.7])**.** *Let G be a finitely generated group and let H be a subgroup of finite index. Then H is finitely generated.*

Lemma C (Lemma A.2.2 in the Appendix)**.** *Let $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$ be a short exact sequence of groups. Suppose that X is a finitely generated abelian group. Then the following equality holds:*

$$\operatorname{rank}(Y) = \operatorname{rank}(X) + \operatorname{rank}(Z).$$

The proof proceeds by induction over $n = \operatorname{rank}(A) \in \mathbb{N}$; indeed, A is a subgroup of finite index of a finitely generated group hence, by Lemma B, the group A is finitely generated abelian and, therefore, its rank is a well-defined natural number. If $n = 0$, then A is the trivial group; this implies that $G \cong G/A$ is torsion free, finite and cyclic by assumption. Thus, we must have $G = \langle 1_G \rangle$ and so G is poly-infinite-cyclic. Suppose now that $n \geq 1$. The idea is to prove that there exists a normal subgroup $H \triangleleft G$ such that, setting $B := A \cap H$,

1. G/H is infinite cyclic;

2. $\operatorname{rank}(B) < \operatorname{rank}(A)$ holds;

3. H/B is finite cyclic.

Suppose we have proved the existence of the subgroup H satisfying these three points. Points 2 and 3 allow us to apply the inductive hypothesis to the short exact sequence $0 \to B \to H \to H/B \to 0$ and deduce that the group H is poly-infinite-cyclic. This fact together with point 1 implies that G is poly-infinite-cyclic. We prove now the existence of the group H that satisfies points 1, 2 and 3 above.

Existence of H satisfying condition 1. We introduce here a new notation:

$$\forall_{a,x\in G}\ a^x := x^{-1}ax.$$

The group G/A is cyclic by assumption hence we can fix $x \in G$ such that the projection of x in G/A generates G/A. In particular, $G = \langle A, x\rangle$ holds. We define a group homomorphism:

$$\begin{aligned} f : A &\longrightarrow A \\ a &\longmapsto a^{-1}a^x. \end{aligned}$$

If we prove that $f(A)$ is a normal subgroup of G and that $G/f(A)$ is finitely generated, infinite and abelian, then this would imply that we can choose a normal subgroup $H \subseteq G$ such that G/H is infinite cyclic.

- Since $G = \langle A, x\rangle$, to prove that $f(A)$ is a normal subgroup of G it suffices to prove that $f(A)$ is normalized by both A and x. First, $f(A)$ is normalized by A because $f(A) \subseteq A$ and A is abelian by assumption. Second, $f(A)$ is normalized by x because for every $a \in A$

  $$x^{-1}f(a)x = x^{-1}a^{-1}x^{-1}axx = (x^{-1}ax)^{-1}(x^{-1}ax)^x = f(x^{-1}ax) \in f(A)$$

  and this implies that $x^{-1}f(A)x \subseteq f(A)$. For the other inclusion, we observe that for every $a \in A$

  $$xf(a)x^{-1} = xa^{-1}x^{-1}axx^{-1} = (xax^{-1})^{-1}(xax^{-1})^x = f(xax^{-1}) \in f(A).$$

  Hence, $xf(A)x^{-1} \subseteq f(A)$, which means that $f(A) \subseteq x^{-1}f(A)x$.
- Since G is finitely generated, then $G/f(A)$ is finitely generated.
- Since $G = \langle A, x\rangle$, to prove that $G/f(A)$ is abelian it suffices to prove that for every $a \in A$, the element $(xa)^{-1}(ax)$ belongs to $f(A)$. Let $a \in A$, then $(xa)^{-1}(ax) = a^{-1}a^x = f(a) \in f(A)$, as desired.
- To prove that $G/f(A)$ is infinite, we want to prove that its subgroup $A/f(A)$ is infinite. To prove this, it suffices to prove that its rank is at least 1 (it makes sense to compute the rank, $A/f(A)$ being abelian and finitely generated). In order to compute the rank, consider the following short exact sequences

  $$0 \longrightarrow \ker(f) \longrightarrow A \stackrel{f}{\longrightarrow} f(A) \longrightarrow 0$$
  $$0 \longrightarrow f(A) \longrightarrow A \longrightarrow A/f(A) \longrightarrow 0.$$

  Applying Lemma C on the previous page, we can estimate the rank of all the groups involved in these shorts exact sequences. Before of this, we need to get some information concerning $\ker(f)$. We have that

  $$\ker(f) = \{\, a \in A \mid ax = xa \,\} = \mathrm{C}_A(x)$$

  is the centralizer of x in A. This subgroup of G is non-trivial, indeed the projection of x in G/A generates G/A (by the choice of x) but G/A is finite by assumption, thus there exists $n \in \mathbb{N}$ such that x^n belongs to A Hence x^n belongs to $\ker(f) = \mathrm{C}_A(x)$ and $x^n \neq 1_G$ because G is torsion free. The fact that $\ker(f)$ is non-trivial implies that $\operatorname{rank}(\ker(f))$ is at least 1, because $\ker(f)$ is torsion free (subgroup of a torsion free group). Considering now the first short exact sequence above, we get that

$$\operatorname{rank}(A) = n \ \wedge \ \operatorname{rank}(\ker(f)) \geq 1 \Longrightarrow \operatorname{rank}(f(A)) \leq n - 1.$$

Applying this to the second short exact sequence we get

$$\operatorname{rank}(A) = n \ \wedge \ \operatorname{rank}(f(A)) \leq n - 1 \Longrightarrow \operatorname{rank}(A/f(A)) \geq 1.$$

Proof that condition 2 is satisfied. Let H be a normal subgroup of G such that G/H is infinite cyclic (we just proved that H exists) and set $B := A \cap H$. To estimate the rank of B, we consider the following short exact sequence:

$$0 \longrightarrow B \longrightarrow A \longrightarrow A/B \longrightarrow 0.$$

Applying Lemma C, we get that

$$\operatorname{rank}(B) = \operatorname{rank}(A) - \operatorname{rank}(A/B).$$

Therefore, to prove that $\operatorname{rank}(B) < \operatorname{rank}(A)$ holds it suffices to prove that $\operatorname{rank}(A/B)$ is at least 1. First, A/B is non-trivial, otherwise A would be fully contained in H and so G/H would be a subgroup of G/A but G/H is infinite by the choice of H and G/A is finite by assumption, contradiction. Second,

$$A/B = A/(A \cap H) \cong AH/H \leq G/H.$$

Summing up, A/B is a non trivial subgroup of G/H which is an infinite cyclic group; this implies that A/B is infinite cyclic, hence $\operatorname{rank}(A/B) = 1$ holds.

Proof that condition 3 is satisfied. Let H an B as above. We have that

$$H/B = H/(H \cap A) \cong AH/A \leq G/A.$$

This means that H/B is isomorphic to a subgroup of G/A and so H/B is finite cyclic because G/A is finite cyclic by assumption. □

2.2 Group Rings Satisfying Kaplansky Conjectures

In this section, we will prove that group rings over unique product groups, (right- or left-)ordered groups and abelian torsion free groups satisfy both the Kaplansky zero divisor conjecture and the Kaplansky unit conjecture. A small remark: we already proved that the unit conjecture is stronger than the zero divisor conjecture (Theorem 1.2.9) but the proof we gave uses (in the last sentence) that group rings over torsion free abelian groups satisfy the zero divisor conjecture. This causes the necessity of writing a direct proof of the fact that group rings over torsion free abelian groups satisfy the zero divisor conjecture (as we will do). There are different methods to develop this direct proof; the one we choose is just to apply the analogous result for group rings over unique product group (since in this thesis we studied unique product groups and we proved that torsion free abelian groups are unique product groups); this motivates the choice of proving directly also that group rings over unique product groups satisfy the zero divisor conjecture.

2.2.1 Group Rings of Unique Product Groups

Lemma 2.2.1. *Let G be a unique product group and let R be a an integral domain. Let $\alpha \in R[G]$ be such that $|Supp(\alpha)| > 1$ holds and let $\beta \in R[G]$ be non-zero. Then $Supp(\alpha\beta)$ contains at least two distinct elements.*

Proof. Let G be a unique product group and R be an integral domain. Let $\alpha, \beta \in R[G]$ be such that $|\mathrm{Supp}(\alpha)| > 1$ and β is non-zero. In particular, $\mathrm{Supp}(\beta)$ is non-empty (the unique element in $R[G]$ with empty support is $0_{R[G]}$). Hence $|\mathrm{Supp}(\alpha)| + |\mathrm{Supp}(\beta)| > 2$ holds. The group G is a u.p. group by assumption and so it satisfies the two unique products property (Lemma 2.1.3). Applying this property to $\mathrm{Supp}(\alpha)$ and $\mathrm{Supp}(\beta)$, it follows that there exists two distinct elements x and y in $\mathrm{Supp}(\alpha)\mathrm{Supp}(\beta) \subseteq G$ such that

$$\exists!(a,b) \in \mathrm{Supp}(\alpha) \times \mathrm{Supp}(\beta) \text{ with } x = ab$$

and

$$\exists!(a',b') \in \mathrm{Supp}(\alpha) \times \mathrm{Supp}(\beta) \text{ with } y = a'b'.$$

Thus, writing α and β as

$$\alpha = \sum_{g \in \mathrm{Supp}(\alpha)} r_g \cdot g$$

and

$$\beta = \sum_{g \in \mathrm{Supp}(\beta)} s_g \cdot g,$$

we get that

$$\alpha\beta = (r_a s_b)x + (r_{a'} s_{b'})y + \sum_{g \in G \smallsetminus \{x,y\}} t_g \cdot g$$

for some coefficients $t_g \in R$. Since R is assumed to be an integral domain, we get that $\mathrm{Supp}(\alpha\beta)$ contains two distinct elements, x and y being distinct; thus $\alpha\beta$ can't be the identity. □

Theorem 2.2.2. *Let G be a unique product group and let R be a an integral domain. The group ring $R[G]$ has neither non-trivial units nor non-trivial zero divisors. In particular, if K is a field, the group ring $K[G]$ satisfies both the unit conjecture and the zero divisor conjecture.*

Proof. By Lemma 2.1.2, a unique product group is always torsion free; therefore, the second part of the claim to prove follows directly from the first part. We now prove the first part. Let G be a unique product group and R be an integral domain. To prove the claim it suffices to prove that for every pair of elements $\alpha, \beta \in R[G]$ with β non-zero, if $\alpha\beta \in \{1_{R[G]}, 0_{R[G]}\}$ then α is zero or a trivial unit. This in turn is equivalent to prove that for every pair of elements $\alpha, \beta \in R[G]$ with β non-zero the following implication holds:

$$|\mathrm{Supp}(\alpha)| > 1 \Longrightarrow \alpha\beta \notin \{1_{R[G]}, 0_{R[G]}\}.$$

This is a direct application of Lemma 2.2.1. □

Corollary 2.2.3. *Let G be an ordered group or, more generally, a right-ordered group and let R be a an integral domain. The group ring $R[G]$ has neither non-trivial units nor non-trivial zero divisors. In particular, if K is a field, the group ring $K[G]$ satisfies both the unit conjecture and the zero divisor conjecture.*

Proof. Every ordered group is a right-ordered group and every right-ordered group is a unique product group (Theorem 2.1.14). Thanks to this, the claim follows directly from Theorem 2.2.2 on the facing page. □

2.2.2 Abelian Group Rings

The aim of this subsection is to prove that the unit conjecture and the zero divisor conjecture hold when the group ring is abelian (equivalently, when the group ring is constructed taking an abelian group, by Lemma 2.2.4). There are several ways to prove this result; the proof we provide here uses that a group ring of an ordered group over an integral domain have neither non-trivial zero-divisors nor non-trivial units (Corollary 2.2.3).

Lemma 2.2.4. *Let G be a group and R be a commutative ring. The group ring $R[G]$ is abelian if and only if G is an abelian group.*

Proof. One direction follows from the fact that given a group ring $R[G]$, the group G is isomorphic to a subgroup of the multiplicative group of $R[G]$ (Remark 1.1.11), hence if $R[G]$ is abelian, so is G. The other direction follows directly from the definition of group ring: given a group ring $R[G]$, the group G is a basis of $R[G]$ as an R-module and the product in $R[G]$ is defined distributively. □

Theorem 2.2.5. *Let G be a torsion free abelian group and let R be an integral domain. The group ring $R[G]$ has neither non-trivial units nor non-trivial zero divisors. In particular, if K is a field, the group ring $K[G]$ satisfies both the unit conjecture and the zero divisor conjecture.*

Proof. Every torsion free abelian group is an ordered group (Proposition 2.1.20). Thanks to this, the claim follows directly from Corollary 2.2.3. □

To conclude this section, we propose an alternative proof of the fact that group rings $R[G]$ over torsion free abelian groups with R integral domain have no non-trivial zero divisors. The alternative proof we provide is taken from [13] and doesn't use theory of unique product groups; the key idea is that, if G is finitely generated, then $R[G]$ can be embedded in the field of fractions of a suitable polynomial ring.

Different proof of the part of Theorem 2.2.5 concerning zero divisors. Let G be a torsion free abelian group and R be an integral domain. We first suppose that G is finitely generated. The idea is to embed $R[G]$ in a field. From the classification theorem of abelian finitely generated groups it follows that there exists $n \in \mathbb{N}$ such that G is isomorphic to the additive group $\mathbb{Z}^n$ (since G is torsion free), thus the group ring $R[G]$ is isomorphic to $R[\mathbb{Z}^n]$. Consider the polynomial ring $R[x_1, \dots, x_n]$ and its field of fractions $K(x_1, \dots, x_n)$ (where K is the field of fractions of R). We can construct a ring homomorphism that behaves as follows:

$$\begin{aligned} f : R[\mathbb{Z}^n] &\longrightarrow K(x_1, \dots, x_n) \\ (m_1, \dots, m_n) &\longmapsto x_1^{m_1} \cdot \dots \cdot x_n^{m_n} \end{aligned}$$

Indeed, the definition above is given just for the basis of $R[\mathbb{Z}^n]$ and this definition induces an R-module morphism $f : R[\mathbb{Z}^n] \to K(x_1, \dots, x_n)$ because of the universal property of free R-modules (Proposition A.1.4). To check that f is a ring homomorphism it suffices to check that it preserves the identity and the product. For this purpose, it's useful to remember that we're looking at $\mathbb{Z}^n$ as an additive group, that is for every $r, s \in R$ and for every $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{Z}^n$ the product in $R[\mathbb{Z}^n]$ is defined with

$$(r(a_1, \ldots, a_n)) \cdot (s(b_1, \ldots, b_n)) := rs(a_1 + b_1, \ldots, a_n + b_n).$$

Eventually, the ring homomorphism f is an injection and this can be proved directly checking that the image of any non-zero element in $R[\mathbb{Z}^n]$ is a non-zero polynomial. Summing up, we just proved that $R[\mathbb{Z}^n]$ is a subring of a field, hence $R[\mathbb{Z}^n]$ is a domain.

We now consider the general case: let G be a torsion free abelian group (finitely generated or not) and R be an integral domain. Let $\alpha, \beta \in R[G]$ be such that $\alpha\beta = 0_{R[G]}$. Let H be the subgroup of G generated by $\mathrm{Supp}(\alpha) \cup \mathrm{Supp}(\beta)$; thus H is finitely generated. Moreover, H is abelian and torsion free, because G is abelian and torsion free by assumption. Thus, we can apply to $R[H]$ what we just proved for finitely generated abelian group: the group ring $R[H]$ has no non-trivial zero divisors. In particular, since α is a zero divisor in $R[H]$, it follows that α is zero. □

Chapter 3

Counterexamples to the Unit Conjecture

The purpose of this chapter is to prove that every group ring $K[P]$, where K is a field of finite characteristic and P is the *Promislow group*, doesn't satisfy the Kaplansky unit conjecture. We will reach our purpose by explicitly exhibiting non-trivial units in the group rings $\mathbb{F}_d[P]$ where d is a prime number and $\mathbb{F}_d$ denotes the finite field with d-elements (Lemma 3.3.1 and Theorem 3.3.9). The non-trivial units we will exhibit have been recently found out by Gardam [3], Murray [9] and Passman [11] (details are in the second and third section).

The reader may be wondering why searching a proof or a disproof of the unit conjecture for group rings over the Promislow group. The motivation could be the following. We already know that group rings of torsion free abelian groups satisfy the Kaplansky conjecture (Theorem 2.2.5); thus, the next step in the study of Kaplansky conjectures may be focusing on group rings of torsion free virtually abelian groups, that is torsion free groups G for which there exists a short exact sequence

$$0 \longrightarrow H \longrightarrow G \longrightarrow L \longrightarrow 0$$

of groups where H is abelian and L is finite. We already know that given such a short exact sequence, if G is finitely generated torsion free and L is cyclic and finite, then G is a unique product group (Theorem 2.1.25) and this implies that, for every field K, the group ring $K[G]$ satisfies the unit conjecture (Theorem 2.2.2). We conclude that, given a field K and a torsion free finitely generated group G for which there exists a short exact sequence as above, the minimal case (minimal with respect to the cardinality of L) in which we don't know yet if $K[G]$ satisfies the unit conjecture is when L is non-cyclic and contains exactly 4 elements[1]. At this point, the Promislow group P comes into play: P is finitely generated, torsion free and has an abelian subgroup H such that P/H has cardinality 4 and is not cyclic.

Eventually, it's interesting to know that the Promislow group is, historically, one of the first examples of torsion free non-unique product group: in 1988 Promislow [14] proved that the group that takes his name is not a unique product group (the first example of a torsion free, non-unique product group was constructed on year before by Rips and Segev [15]).

[1]Groups that are formed by exactly 1, 2 or 3 elements are cyclic.

Notations. Let G be a group and let $a, b \in G$; with the words *conjugation of a by b* we mean the element $b^{-1}ab$ and we set the following notation:

$$a^b := b^{-1}ab.$$

3.1 The Promislow Group

The *Promislow group* P is a finitely presented group whose main properties are being torsion free and virtually abelian where it has an abelian subgroup H such that H is isomorphic to $\mathbb{Z}^3$ and P/H is a non-cyclic finite abelian group of 4 elements. In other words, there exists a short exact sequence that looks as follows:

$$0 \longrightarrow \mathbb{Z}^3 \longrightarrow P \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

In the literature is also known as the *Fibonacci group* $F(2, 6)$ and one motivation to its importance is that it is an example of torsion free, non-unique product group (proved by Promislow in 1988 [14]).

The only properties of the Promislow group P that we need to build the counterexamples to the unit conjecture are that P is torsion free and can be insert in a shorts exact sequence that looks like the short exact sequence written above. To prove these properties, we will need some intermediate results concerning the Promislow group; we will motivate step by step these intermediate results, explaining in which direction we're moving.

Definition 3.1.1. The *Promislow group* P is the group defined via the following presentation:

$$P := \langle a, b \mid (a^2)^b = a^{-2}, (b^2)^a = b^{-2} \rangle.$$

Notations. In this chapter, when saying *Promislow group* we always refer to the presentation given in Definition 3.1.1 and, unless otherwise specified, with $a \in P$ and $b \in P$ we'll always denote the generators of P that appears in the presentation given in Definition 3.1.1.

Lemma 3.1.2. *Let P be the Promislow group and let N be the subgroup of P generated by a^2 and b^2; then N is normal in P.*

Proof. Let P and N be as in the statement. To prove that N i normal is suffices to prove that the conjugates of the generators of N by the generators of P belong to N. The presentation of P forces $(a^2)^b$ and $(b^2)^a$ to coincide, respectively, with a^{-2} and b^{-2} and both of these elements belong to N, as desired. □

The subgroup N of the Promislow group P introduced in previous lemma turns out to be important because, as we will prove, the quotient P/N is isomorphic to the *infinite dihedral group* (Definition A.5.1) and this fact will allow us to exhibit a normal subgroup H of P such that H is abelian and P/H is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. The idea to proceed in this direction to find the subgroup H comes from Gardam's article [3].

Lemma 3.1.3. *Let P be the Promislow group. Set $x := a^2$ and $y := b^2$ and denote with A, B and N the subgroups of P generated by, respectively, $\{ a, y \}$, $\{ b, x \}$ and $\{ x, y \}$ (in particular, N is a subgroup of both A and B). Then P is the amalgamated free product $A *_N B$ of A and B over N.*

Proof. Let P, A, B and N as in the statement. To prove the claim we have to prove that the following diagram is a pushout diagram, where all the arrows are canonical inclusions.

$$\begin{array}{ccc} N & \rightarrowtail & A \\ \downarrow & & \downarrow \\ B & \rightarrowtail & P \end{array}$$

The commutativity of the diagram is trivial, all the arrows being canonical inclusions. Let now G be a group and $f : A \to G$ and $g : B \to G$ be a pair of group homomorphism such that $f_{|N} = g_{|N}$ holds. To conclude the proof, we need to prove that there exists a unique group homomorphism $h : P \to G$ such that both $h_{|A} = f$ and $h_{|B} = g$ hold.

[Uniqueness] Let $h : P \to G$ and $k : P \to G$ be group homomorphisms such that $h_{|A} = f = k_{|A}$ and $h_{|B} = g = k_{|A}$ hold. Then, since a and b belong, respectively, to A and B, we get that both $h(a) = k(a)$ ans $h(b) = k(b)$ holds. This implies that h and k are necessarily the same group homomorphism because the set $\{ a, b \}$ generates P.

[Existence] We prove the existence applying the universal property of finitely presented groups. First, we observe that, if there exists a group homomorphism $h : P \to G$ satisfying both $h_{|A} = f$ and $h_{|B} = g$, then both $h(a) = f(a)$ and $h(b) = g(b)$ holds. Let F_2 be the free (non-abelian) group of rank 2 generated by $\{ a, b \}$ and let $h^* : F_2 \to G$ be the group homomorphism such that $h^*(a) = f(a)$ and $h^*(b) = g(b)$ (h^* exists by definition of free group). The homomorphism h^* preserves the relations of P indeed, applying the equality $f_{|N} = g_{|N}$, we get

$$\begin{aligned} h^*((a^2)^b) &= h^*(b)^{-1}h^*(a)^2h^*(b) = g(b)^{-1}f(a)^2g(b) = g(b)^{-1}f(x)g(b) \\ &= g(b)^{-1}g(x)g(b) = g(b^{-1}xb) = g(x^{-1}) = f(x^{-1}) = f(a^{-2}) \\ &= f(a)^{-2} = h^*(a^{-2}); \\ h^*((b^2)^a) &= h^*(a)^{-1}h^*(b)^2h^*(a) = f(a)^{-1}g(b)^2f(a) = f(a)^{-1}g(y)f(a) \\ &= f(a)^{-1}f(y)f(a) = f(a^{-1}ya) = f(y^{-1}) = g(y^{-1}) = g(b^{-2}) \\ &= g(b)^{-2} = h^*(b^{-2}). \end{aligned}$$

Therefore, by the universal property of finitely presented groups, there exists a group homomorphism $h : P \to G$ such that both $h(a) = f(a)$ and $h(b) = g(b)$ hold. It remains to prove that h satisfies both $h_{|A} = f$ and $h_{|B} = g$. Remembering that A is generated by $\{ a, y \}$ and B is generated by $\{ b, x \}$, it suffices to prove that h and f coincides if applied to the generators of A and, analogously, that h and g coincides if applied to the generators of B. First, $h(a) = f(a)$ and $h(b) = g(b)$ hold by definition. Second,

$$\begin{aligned} h(y) &= h(b^2) = h(b)^2 = g(b)^2 = g(y) = f(y), \\ h(x) &= h(a^2) = h(a)^2 = f(a)^2 = f(x) = g(x) \end{aligned}$$

and this concludes the proof. □

Corollary 3.1.4. *Let P be the Promislow group and let N be the subgroup of P generated by a^2 and b^2; then P/N is isomorphic to the infinite dihedral group.*

Explicitly, there exists an isomorphism behaving in the following way:

$$\begin{aligned} P/N &\longrightarrow D_\infty = \langle s, t \mid t^2, s^t = s^{-1} \rangle \\ [a] &\longmapsto t \\ [b] &\longmapsto ts \\ [ab] &\longmapsto s. \end{aligned}$$

Proof. Let P be the Promislow group. Set $x := a^2$ and $y := b^2$ and denote with A, B and N the subgroups of P generated by, respectively, $\{ a, y \}$, $\{ b, x \}$ and $\{ x, y \}$. Lemma 3.1.3 tells us that the following is a pushout diagram, where all the arrows are the canonical inclusions.

$$\begin{array}{ccc} N & \rightarrowtail & A \\ \downarrow & & \downarrow \\ B & \rightarrowtail & P \end{array}$$

Since N is a normal subgroup of A, B and P (because N is normal in P by Lemma 3.1.2), we can pass to the quotient over N obtaining a new pushout diagram (in Appendix A.3 is explained how to prove this), that appears as follows.

$$\begin{array}{ccc} 1 & \longrightarrow & A/N \\ \downarrow & & \downarrow \\ B/N & \longrightarrow & P/N \end{array}$$

Observe that both A/N and B/N are isomorphic to the group $\mathbb{Z}/2$, indeed

- the subgroup A is generated by $\{ a, y \}$ and both a^2 and y belong to N;
- the subgroup B is generated by $\{ b, x \}$ and both b^2 and x belong to N.

Summing up, we just proved that P/N is isomorphic to $\mathbb{Z}/2 * \mathbb{Z}/2$ (the free product being unique up to isomorphism). Hence by Remark A.5.3 P/N is isomorphic to the finitely presented group $G := \langle a, b \mid a^2, b^2 \rangle$ where the equivalence class $[a] \in P/N$ corresponds to $a \in G$ and the equivalence class $[b] \in P/N$ corresponds to $b \in G$ (because $[a], [b] \in P/N$ generate, respectively, A/N and B/N). Eventually, applying Remarmk A.5.2 we can conclude that P/N is isomorphic to the infinite dihedral group; the same Remark gives us the desired correspondence. □

Remark 3.1.5. Let P be the Promislow group. Set $x := a^2$, $y := b^2$ and $z := (ab)^2$ in P. Since it will be very useful in many parts of this chapter, we list the images of x, y and z through the conjugation homomorphisms by a, b and ab. First, observe that the conjugation by ab can be obtained conjugating first by a and then by b (easy to check). Second, we compute the conjugates of z. We have

$$z^a z = a^{-1}(abab)a(abab) = bab^2(b^{-1}a^2b)ab = b(ab^2a^{-1})b = bb^{-2}b = 1.$$

Hence $z^a = z^{-1}$ holds. On the other hand

$$z = z^{ab} = (z^a)^b = (z^{-1})^b = (z^b)^{-1},$$

so $z^b = z^{-1}$ holds. Now, we can record all the conjugates of x, y and z by a, b and ab in the following list.

$$\begin{aligned} x^a &= x & y^a &= y^{-1} & z^a &= z^{-1} \\ x^b &= x^{-1} & y^b &= y & z^b &= z^{-1} \\ x^{ab} &= x^{-1} & y^{ab} &= y^{-1} & z^{ab} &= z \end{aligned}$$

Eventually, we could deduce that the conjugation by a or b or ab gives an automorphism of H whose square is the identity automorphism (i.e., it is its own inverse). Therefore, for every $w \in \{a, b, ab\}$, the automorphisms of H given by conjugating by w and by w^{-1} coincide to each other.

Lemma 3.1.6. *Let P be the Promislow group. Set $x := a^2$, $y := b^2$ and $z := (ab)^2$ in P and let H be the subgroup of P generated by $\{x, y, z\}$. Then*

1. *H is abelian;*
2. *H is normal in P;*
3. *P/H is isomorphic to the product of two groups of order 2 and the equivalence classes of a, b and ab are the non-identity elements of P/H.*
4. *H is isomorphic to the additive group $\mathbb{Z}^3$, in particular, H is torsion free.*

Proof. Let P be the Promislow group and let H and $x, y, z \in P$ as in the statement. Proving points 1 and 2 is immediate thanks to Remark 3.1.5. Indeed we have that

$$\begin{aligned} xy = yx &\iff y^{-1}xy = x \iff (x^b)^b = x; \\ xz = zx &\iff z^{-1}xz = x \iff (x^{ab})^{ab} = x; \\ zy = yz &\iff y^{-1}zy = z \iff (z^b)^b = z. \end{aligned}$$

Last equality in each line holds by Remark 3.1.5, hence H is an abelian group because its generators commute. On the other hand, Remark 3.1.5 shows us that when we conjugate the generators of H by the generators of P, the elements we obtain are contained in H and this proves that H is a normal subgroup.

We now prove the third point. The idea is to use the isomorphism between P and the infinite dihedral group stated in Corollary 3.1.4 and to use that the quotient of the infinite dihedral D_∞ group over a suitable subgroup is isomorphic to a product of two cyclic groups of order 2 (Lemma A.5.4). First, by Corollary 3.1.4 there exists an isomorphism $P/N \to D_\infty$ such that $\phi([ab]) = s$ where $D_\infty = \langle s, t \mid t^2, s^t = s^{-1} \rangle$. In particular, since $[ab]^2$ is a generator of H/N, the subgroup H/N corresponds through ϕ to the subgroup of D_∞ generated by s^2 (we denote it with $\langle s^2 \rangle_{D_\infty}$). Therefore,

$$P/H \cong \frac{P/N}{H/N} \cong \frac{D_\infty}{\langle s^2 \rangle_{D_\infty}} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

where last congruence holds by Lemma A.5.4. Eventually, the equivalence classes $[1]$, $[a]$, $[b]$ and $[ab]$ in P/H are pairwise distinct. Indeed, since P is generated by $\{ a, b \}$, then $\{ [a], [b] \} \subseteq P/N$ is a generating set for P/N; the fact that P/N is not cyclic implies that $[1]$, $[a]$, $[b]$ are pairwise distinct; therefore, P/N being isomorphic to a product of two cyclic groups, the fourth element of P/N is given by the product $[a][b] = [ab] \in P/N$.

The proof of the fourth point we provide here comes from the one given by Passman inside its proof of [12, Lemma 13.3.3]. The idea is to construct two group homomorphisms

$$\mathbb{Z}^3 \xrightarrow{\phi} P \xrightarrow{\psi} \mathrm{GL}_4(\mathbb{Q}),$$

where $\mathrm{GL}_4(\mathbb{Q})$ denotes the multiplicative group consisting of all 4×4 invertible matrices with coefficients in $\mathbb{Q}$, such that

(a) the image of ϕ is exactly the subgroup H of P;

(b) the composition $\psi \circ \phi$ is injective.

The existence of such group homomorphisms allows us to conclude, because the group homomorphism $\mathbb{Z}^3 \to H$ obtained restricting the target set of ϕ is well-defined and surjective by point (a) and it is injective by point (b); hence, it is an isomorphism. It remains to prove the existence of ϕ and ψ satisfying points (a) and (b). We set

$$\begin{aligned} \phi : \mathbb{Z}^3 &\longrightarrow P \\ (i,j,k) &\longmapsto x^i y^j z^k. \end{aligned}$$

This map ϕ is a group homomorphism because H is abelian by point 1. Moreover, since $\mathbb{Z}^3$ is generated by $\{ (1,0,0), (0,1,0), (0,0,1) \}$, the image of ϕ is the group generated by $\phi(\{ (1,0,0), (0,1,0), (0,0,1) \}) = \{ x, y, z \}$ and this group is H, by definition. We just exhibited a group homomorphism satisfying (a). Now we prove that there exists a group homomorphism

$$\begin{aligned} \psi : P &\longrightarrow \mathrm{GL}_4(\mathbb{Q}) \\ a &\longmapsto A \\ b &\longmapsto B. \end{aligned}$$

where

$$A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad B := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \end{pmatrix}.$$

The existence of ψ can be proved applying the universal property of finitely presented group, since the following relations hold:

$$A^{-1}B^2A = B^{-1} \qquad \text{and} \qquad B^{-1}A^2B = A^{-2}.$$

It remains to prove that the composition $\psi \circ \phi$ is injective; we do this proving that the kernel of this composition is trivial. Let $(i,j,k) \in \ker(\psi \circ \phi)$; then

$$1_{\mathrm{GL}_4(\mathbb{Q})} = \psi(\phi(i,j,k)) = \psi(x^i y^j z^k) = A^{2i} B^{2j} (AB)^{2k}.$$

We have that

$$A^2 = \operatorname{diag}(2, 2, 1/2, 1/2),$$
$$B^2 = \operatorname{diag}(2, 1/2, 2, 1/2),$$
$$(AB)^2 = \operatorname{diag}(2, 1/2, 1/2, 2).$$

Hence, $1_{\mathrm{GL}_4(\mathbb{Q})} = A^{2i}B^{2j}(AB)^{2k}$ holds if and only if the three-uple (i, j, k) satisfies the following system

$$\begin{cases} 2^i 2^j 2^k = 1 \\ 2^i 2^{-j} 2^{-k} = 1 \\ 2^{-i} 2^j 2^{-k} = 1 \\ 2^{-i} 2^{-j} 2^k = 1, \end{cases}$$

that is if and only if $(i, j, k) = (0, 0, 0)$ holds and this proves that the kernel of $\psi \circ \phi$ is trivial. □

The goal of the remaining part of this section is to prove that the Promislow group P is torsion free and not a right-ordered group. Once again, the proof we provide here comes from the one given by Passman inside its proof of [12, Lemma 13.3.3]

Lemma 3.1.7. *Let P be the Promislow group. Then P is torsion free and not right-orderable.*

Proof. Let P be the Promislow group and let H be the subgroup of P generated by $\{ x, y, z \}$ where $x := a^2$, $y := b^2$ and $z := (ab)^2$. We prove that P is torsion free and we prove this by contradiction. Let $g \in P$ be a torsion element and *assume* that g is a non-identity element. The proof consists of the following two steps:

- proving that g has order 2;
- proving that one element in $\{ x, y, z \}$ has finite order.

The second point gives the contradiction. Indeed, $\{ x, y, z \}$ is a generating set of H and H is isomorphic to $\mathbb{Z}^3$ by Lemma 3.1.6, hence the generating set $\{ x, y, z \}$ of H must consists of elements of infinite order, against the second point above. We prove now the two points above.

Proof of the first point. The equivalence class of g in P/H is a torsion element of P/H. The group P/H is, by Lemma 3.1.6, a product of two cyclic groups of order 2 hence all the elements in P/H has order at most 2; this implies that $[g]^2 = 1_{P/H}$ holds, that is g^2 belongs to H. On the other hand, the group H is torsion free because by Lemma 3.1.6 it is isomorphic to $\mathbb{Z}^3$, and g^2 is a torsion element inside H. Therefore, the following equality holds

$$g^2 = 1_P.$$

Proof of the second point. By Lemma 3.1.6 the group P can be written as the following disjoint union

$$P = H \cup aH \cup bH \cup abH.$$

Hence, remembering that H is abelian, there exist $c \in \{ a, b, ab \}$ and $(i, j, k) \in \mathbb{Z}^3$ such that

$$g = cx^i y^j z^k$$

(the element g can't belong to H because H is torsion free). Summing up, we have that

$$1_P = g^2 = cx^i y^j z^k cx^i y^j z^k = c^2 (x^i y^j z^k)^c x^i y^j z^k.$$

Now, applying Remark 3.1.5, we can observe that

$$(x^i y^j z^k)^c x^i y^j z^k = (c^2)^{2n}$$

for some $n \in \{ i, j, k \}$, because the conjugation by $c \in \{ a, b, ab \}$ fixes c^2 and inverts the elements of $\{ x, y, z \}$ distinct from c^2. Therefore we have that

$$1_P = c^2 (c^2)^{2n} = (c^2)^{2n+1}.$$

This means that c^2 is a torsion element and this proves the second point, because c^2 belongs to $\{ a^2, b^2, (ab)^2 \}$.

We now prove that P is not a right-ordered group. The idea is to apply Lemma 2.1.17 considering the subset $\{ a, b \} \subseteq P$. First, we need to list some relations holding in P. The presentation of P has as relations $a^{-1}b^2a = b^{-2}$ and $b^{-1}a^2b = b^{-2}$, hence all the equalities in the following chain of equivalences hold:

$$\begin{aligned} a^{-1}b^2a = b^{-2} &\iff b^2 = ab^{-2}a^{-1} \\ &\iff b^{-2} = ab^2a^{-1} \iff a^{-1}b^{-2}a = b^2 \end{aligned}$$

and

$$\begin{aligned} b^{-1}a^2b = b^{-2} &\iff a^2 = ba^{-2}b^{-1} \\ &\iff a^{-2} = ba^2b^{-1} \iff b^{-1}a^{-2}b = a^2. \end{aligned}$$

All these relations are summarized by

$$\begin{aligned} &\forall_{\epsilon,\delta\in\{ -1,1 \}} \; a^\epsilon b^{2\delta} a^{-\epsilon} = b^{-2\delta}, \\ &\forall_{\epsilon,\delta\in\{ -1,1 \}} \; b^\delta a^{2\epsilon} b^{-\delta} = a^{-2\epsilon}. \end{aligned}$$

Let $\epsilon, \delta \in \{ -1, 1 \}$. Then

$$1_P = a^\epsilon b^{2\delta} a^{-\epsilon} b^{2\delta} = a^\epsilon b^{2\delta} a^{-2\epsilon} a^\epsilon b^{2\delta} = a^\epsilon b^\delta (b^\delta a^{-2\epsilon} b^{-\delta}) b^\delta a^\epsilon b^{2\delta} = a^\epsilon b^\delta a^{2\epsilon} b^\delta a^\epsilon b^{2\delta}.$$

This means that for every $\epsilon, \delta \in \{ -1, 1 \}$ the semigroup generated by $\{ a^\epsilon, b^\delta \}$ contains the identity of P; therefore, by Lemma 2.1.17, the group P is not a right-ordered group. □

Insights on the Promislow Group

We present here some results concerning the Promislow group that are not essential to build our counterexamples to the unit conjecture we will describe (main purpose of this chapter) but that can be useful to understand more deeply the Promislow group.

Lemma 3.1.8. *Let P be the Promislow group and let σ be a permutation of the set $\{a, b, ab\}$. Then there exists an automorphism ϕ_σ of P that behaves as follows:*

$$\begin{aligned}\phi_\sigma : P &\longrightarrow P\\ a &\longmapsto \sigma(a)\\ b &\longmapsto \sigma(b)\end{aligned}$$

Proof. Let P be the Promislow group and let σ be a permutation of the set $\{a, b, ab\}$. We first prove the existence of the group homorphism $\phi_\sigma : P \to P$ such that $\phi_\sigma(a) = \sigma(a)$ and $\phi_\sigma(b) = \sigma(b)$; second we prove that for every σ in the group of permutations of $\{a, b, ab\}$, the homomorphism ϕ_σ is an isomorphism.

[Existence] We prove the existence applying the universal property of finitely presented group. Let $f : \{a, b\} \to P$ the map such that $f(a) = \sigma(a)$ and $f(b) = \sigma(b)$. This map induces a group homomorphism $f^* : F(\{a, b\}) \to P$, where with $F(\{a, b\})$ we denote the free group generated by $\{a, b\}$: the homomorphism f^* preserves the relation that generates P, indeed:

$$\begin{aligned}f^*(a^b) &= \sigma(b)^{-1}(\sigma(a))^2\sigma(b) = (\sigma(a))^{-2} = (f^*(a))^{-2} = f^*(a^{-2}),\\ f^*(b^a) &= \sigma(a)^{-1}(\sigma(b))^2\sigma(a) = (\sigma(b))^{-2} = (f^*(b))^{-2} = f^*(b^{-2})\end{aligned}$$

where the central equality in both lines holds by Remark 3.1.5. Therefore, by the universal property of finitely presented group, there exists a group homomorphism $\phi_\sigma : P \to P$ such that $\phi_\sigma(a) = f(a)$ and $\phi_\sigma(b) = f(b)$, as desired.

[Invertibility] To prove that for every permutation σ in the symmetric group $\mathrm{Sym}(\{a, b, ab\})$, the group homomorphism ϕ_σ is an isomorphimsm, it suffices to prove that ϕ_σ is an isomorphism if σ is a transposition[2]. Indeed, given a permutation $\sigma \in \mathrm{Sym}(\{a, b, ab\})$, there exists a transposition ρ such that $\sigma = \rho \circ (b\ a)$ holds[3], hence

$$\begin{aligned}\phi_\sigma(a) &= \sigma(a) = \rho(b) = \phi_\rho(b) = \phi_\rho \circ \phi_{(a\ b)}(a),\\ \phi_\sigma(b) &= \sigma(b) = \rho(a) = \phi_\rho(a) = \phi_\rho \circ \phi_{(a\ b)}(b),\end{aligned}$$

Therefore, since every group homomorphism whose domain is P is uniquely identified by the images of a and b, we get that $\phi_\sigma = \phi_\rho \circ \phi_{(a\ b)}$ and it follows that, if both ϕ_ρ and $\phi_{(a\ b)}$ are isomorphisms, also ϕ_σ is an isomorphism. It remain to prove that, if σ is a transposition, then ϕ_σ is an isomorphism. The idea is to exhibit an inverse. There are exactly three transposition and we consider them separately.

- First case: $\sigma = (a\ b)$ holds. It follows immediately that $\phi_\sigma \circ \phi_\sigma$ is the identity morphism of P, that is ϕ_σ is invertible and it is its own inverse.
- Second case: $\sigma = (b\ ab)$ holds. Hence, $\phi_\sigma(a) = a$ and $\phi_\sigma(b) = ab$. From this we deduce that the inverse homomorphism $\psi : P \to P$ (if it exists) needs to fix a and send b to $a^{-1}b$. This group homomorphism $\psi : P \to P$ exists by the universal property of finitely presented group. Indeed, let

[2]A transposition is a permutation that exchanges just 2 elements and keeps all others fixed

[3]The notation $(a\ b)$ indicates the transposition which exchanges a and b; more in general, if X is a non-empty set and $n \in \mathbb{N} \setminus 0$, given $x_1, x_2, \ldots, x_n \in X$ we denote with $(x_1\ x_2\ \ldots\ x_n)$ the permutation of X that, for every $1 \le i < n$, sends x_i to x_{i+1} and x_n to x_1.

$f : \{ a, b \} \to P$ be the map such that $f(a) = a$ and $f(b) = a^{-1}b$ and let $f^* : F(\{ a, b \}) \to P$ be the group homomorphism that f induces, then

$$\begin{aligned} f^*(a^b) &= f(b)^{-1}f(a)^2 f(b) = (a^{-1}b)^{-1}a^2a^{-1}b = a^{-2} = f^*(a^{-2}), \\ f^*(b^a) &= f(a)^{-1}f(b)^2 f(a) = a^{-1}a^{-1}ba^{-1}ba \\ &= b(b^{-1}a^{-2}b)a^{-1}ba \\ &= baba \overset{*}{=} (a^{-1}b)^{-2} = f^*(b^{-2}) \end{aligned}$$

where the equality $*$ holds because

$$babaa^{-1}ba^{-1}b = bab^2a^{-1}b = bb^{-2}b = 1_P.$$

We conclude that we can apply the universal property of finitely presented group to the map f, hence the desired group homomorphism $\psi : P \to P$ exists.

- Third case: $\sigma = (a\ ab)$ holds. Hence, $\phi_\sigma(a) = ab$ and $\phi_\sigma(b) = b$. From this we deduce that the inverse homomorphism $\psi : P \to P$ (if it exists) needs to fix b and send a to ab^{-1}. This group homomorphism $\psi : P \to P$ exists by the universal property of finitely presented group. Indeed, let $f : \{ a, b \} \to P$ be the map such that $f(a) = ab^{-1}$ and $f(b) = b$ and let $f^* : F(\{ a, b \}) \to P$ be the group homomorphism that f induces, then

$$\begin{aligned} f^*(b^a) &= f(a)^{-1}f(b)^2 f(a) = (ab^{-1})^{-1}b^2ab^{-1} = b^{-2} = f^*(b^{-2}) \\ f^*(a^b) &= f(b)^{-1}f(a)^2 f(b) = b^{-1}ab^{-1}ab^{-1}b = \\ &= b^{-1}ab^{-1}a \overset{*}{=} (ab^{-1})^{-2} = f^*(a^{-2}) \end{aligned}$$

where the equality $*$ holds because

$$\begin{aligned} b^{-1}ab^{-1}aab^{-1}ab^{-1} &= b^{-1}ab^{-1}a^2bb^{-2}ab^{-1} \\ &= b^{-1}a^{-1}b^{-2}ab^{-1} = b^{-1}b^2b^{-1} = 1_P. \end{aligned}$$

We conclude that we can apply the universal property of finitely presented group to the map f, hence the desired group homomorphism $\psi : P \to P$ exists. □

Remark 3.1.9. Let P be the Promislow group and let σ be a permutation of the set $\{ a, b, ab \}$ distinct from the identity permutation. Then

$$\sigma(a)\sigma(b) \neq \sigma(ab)$$

holds. For each of the five possible non-identity permutations σ, this can be checked by contradiction: the equality $\sigma(a)\sigma(b) = \sigma(ab)$ would imply the existence of a non-identity torsion element, but P is torsion free by Lemma 3.1.7 (the details to exhibit the non-identity torsion element are left to the reader). In particular, if ϕ_σ denotes the automorphism of P constructed in Lemma 3.1.8, then $\phi_\sigma(ab) \neq \sigma(ab)$ holds. It follows that

$$\phi_{\sigma^{-1}} \neq (\phi_\sigma)^{-1}$$

holds, except when $\sigma = (a\ b)$; indeed, if $\sigma \neq (a\ b)$, let $x \in \{ a, b \}$ be such that $\sigma(ab) = x$, then

$$\phi_\sigma(\phi_{\sigma^{-1}}(x)) \stackrel{*}{=} \phi_\sigma(\sigma^{-1}(x)) = \phi_\sigma(ab) \neq \sigma(ab) = x,$$

where in $*$ we used that x belongs to $\{ a, b \}$. Explicit examples of the inverse automorphisms are described inside the proof of Lemma 3.1.8.

Lemma 3.1.10. *Let P be the Promislow group. Set $x := a^2$ and $y := b^2$ and denote with A and B the subgroups of P generated by, respectively, $\{ a, y \}$ and $\{ b, x \}$. Then the following isomorphisms of groups hold:*

$$A \cong \langle s, t \mid s^t = s^{-1} \rangle \cong B$$

where the middle group $\langle s, t \mid s^t = s^{-1} \rangle$ is called Klein bottle group[4].

Proof. It suffices to prove the existence of the first isomorphism; indeed, B is isomorphic to B where the isomorphism is given by a restriction of a suitable automorphism among those constructed in Lemma 3.1.8. The idea is to construct a monomorphism ϕ from the Klein bottle group to the Promislow group whose image is exactly A. The Klein bottle group being a finitely presented group, we construct ϕ applying the universal property of finitely presented groups. Consider the following set-theoretic map

$$\begin{aligned} \{ s, t \} &\longrightarrow P \\ t &\longmapsto a \\ s &\longmapsto b^2. \end{aligned}$$

This maps induces a group homomorphism $f^* : F(\{ s, t \}) \to P$, where with $F(\{ s, t \})$ we denote the free group generated by $\{ s, t \}$; the homomorphism f^* preserves the relation that generates the Klein bottle group, indeed:

$$\begin{aligned} f^*(s^t) &= f^*(t)^{-1} f^*(s) f^*(t) = f(t)^{-1} f(s) f(t) \\ &= a^{-1} b^2 a = b^{-2} = f(s)^{-1} = f^*(s^{-1}). \end{aligned}$$

Therefore, by the universal property of finitely presented group, f induces a group homomorphism $\phi : \langle s, t \mid s^t = s^{-1} \rangle \to P$ such that, set-theoretically, $\phi_{|\{ s,t \}} = f$ holds. It remains to prove that ϕ induces an isomorphism between the Klein bottle group and the subgroup A of P, that is both $\mathrm{Im}(\phi) = A$ and $\ker(\phi) = \{ 1_P \}$ hold.

The image of ϕ is A because the image is generated by the images of the generators of the domain, that this $\mathrm{Im}(\phi)$ is generated by $\phi(\{ s, t \}) = \{ a, b^2 \}$; this set generates A, by definition.

It remains to prove that $\ker(\phi) = \{ 1_P \}$ holds. In order to do this, it's useful to find a compact way to represent the elements in the Klein bottle group. We claim that for every element w in the Klein bottle group $\langle s, t \mid s^t = s^{-1} \rangle$, there exist $i, n \in \mathbb{Z}$ such that $w = t^i s^n$ holds (we will prove this claim after we finish the proof of the injectivity of ϕ). Let $w \in \langle s, t \mid s^t = s^{-1} \rangle$ be such that $\phi(w) = 1_P$ holds. By the claim, there exist $i, n \in \mathbb{Z}$ such $z = t^i s^n$ holds; to conclude, we prove that $i = 0 = j$. Since w belongs to $\ker(\phi)$, we have

$$1_P = \phi(w) = \phi(t^i s^n) = a^i b^{2n}.$$

[4]The Klein bottle group is the fundamental group of the Klein bottle.

Hence $a^{-i} = b^{2n}$ holds and this implies that

$$a^i = b^{-2n} = a^{-1}b^{2n}a = a^{-1}a^{-i}a = a^{-i}.$$

As a consequence, $a^{2i} = 1_P$ holds but a^2 is not a torsion element, because the subgroup of P generated by $\{ a^2, b^2, (ab)^2 \}$ is isomorphic to $\mathbb{Z}^3$ by Lemma 3.1.6 (if a^2 were the identity, then $\{ a^2, b^2, (ab)^2 \}$ couldn't generate a free abelian group of rank 3), hence $i = 0$ holds[5]. Since, as written some lines above, $a^{-i} = b^{2n}$, we get that b^{2n} holds but b^2 is not a torsion element (for the same reason that a^2 is not a torsion element), hence $n = 0$ holds. We conclude that $w = t^0 s^0 = 1$, as desired. □

Proof of the claim. The set $\{ s, t \}$ is a generating set for the Klein bottle group thus every element in this group is of the form

$$t^{j_0} s^{k_0} t^{j_1} s^{k_1} \cdots t^{j_m} s^{k_m} \text{ with } m \in \mathbb{N},\ j_0, \dots, j_m, k_0, \dots, k_m \in \mathbb{Z}, \tag{3.1}$$

We prove that every such an element can be written as $t^i s^n$ for some $i, n \in \mathbb{Z}$ by induction on $m \in \mathbb{N}$ (where m is the parameter appearing in 3.1)

- If $m = 0$, the claim is immediate.
- Suppose $m \geq 1$ and that the claim is true for $m - 1$. Fix an element $t^{j_0} s^{k_0} t^{j_1} s^{k_1} \cdots t^{j_m} s^{k_m}$, with $j_0, \dots, j_m, k_0, \dots, k_m \in \mathbb{Z}$. By the inductive hypothesis there exist $j, k \in \mathbb{Z}$ such that $t^{j_0} s^{k_0} t^{j_1} s^{k_1} \cdots t^{j_{m-1}} s^{k_{m-1}} = t^j s^k$ holds. Thus

$$\begin{aligned} t^{j_0} s^{k_0} t^{j_1} s^{k_1} \cdots t^{j_m} s^{k_m} &= t^j s^k t^{j_m} s^{k_m} \\ &= t^{j+j_m} t^{-j_m} s^k t^{j_m} s^{k_m} \\ &\overset{(*)}{=} t^{j+j_m} s^h s^{k_m} = t^{j+j_m} s^{h+k_m} \end{aligned}$$

  where equality $(*)$ is true for a suitable $h \in \{ k, -k \}$ and it is obtained iterating $|j_m|$-times one relation among $t^{-1}st = s^{-1}$ and $tst^{-1} = s^{-1}$. □

Remark 3.1.11. Let P be the Promislow group. Then, by Lemma 3.1.3 together with Lemma 3.1.10, the Promislow group P is the amalgamated free product of two Klein bottle groups.

Remark 3.1.12. An alternative solution to the problem of proving that the Promislow group is torsion free is suggested by Gardam [3]. Gardam's approach requires the following (non-trivial) results:

- the Klein bottle group is torsion free;
- the amalgamated free product of torsion free groups is torsion free.

If these claims are true (as they are), we can deduce directly from Remark 3.1.11 that the Promislow group is torsion free. We suggest here an idea to prove that the Klein bottle group is torsion free.

[5] Even if we already proved that P is torsion free (Lemma 3.1.7), we prefer not to apply this result here. Indeed, we will see in Remark 3.1.12 that the property that P is torsion free can also be seen as a consequence of the Lemma we're proving now.

Idea to prove that the Klein bottle group is torsion free. The Klein bottle group is the fundamental group of the Klein bottle. The universal covering of the Klein bottle is $\mathbb{R}^2$, therefore the Klein bottle is a $K(G, 1)$ (according to definition at page 87 in [4]). On the other hand, the Klein bottle is also a finite dimensional CW complex. Eventually, one can conclude using that if a finite dimensional CW complex X is a $K(G, 1)$ then the group $G = \pi_1(X)$ is torsion free [4, Proposition 2.45].

3.2 Units in Group Rings of the Promislow Group

Let K be a field and P be the Promislow group. The search of units in the group ring $K[P]$ starts from the search for sufficient conditions for units in $K[P]$ (that is, conditions such that if they're satisfied by an element in $K[P]$, then the element is a unit in $K[P]$). This is what we're going to do in this section: we will reason deductively to exhibit some of these sufficient conditions and we will find different ways to transform units into new elements that are still units.

If not differently specified, all the results we provide here haven't been taken from the literature. For example, Gardam proposes sufficient conditions for units in $K[P]$ ([3, Lemma 1]) different from the conditions we propose here (Lemma 3.2.8); it is possible to prove that Gardam's conditions are stronger then the one we provide here (this motivate our choice not to insert in this work sufficient condition proved by Gardam in [3, Lemma 1]).

3.2.1 Properties of Group Rings of the Promislow Group

Lemma 3.2.1. *Let P be the Promislow group and K be a field. The group ring $K[P]$ satisfies the zero divisor conjecture, that is the only zero divisor in $K[P]$ is zero.*

Proof. The lemma we have to prove is a direct consequence of the following more general result.

Lemma D. *Let K be a field and G be a torsion free group. If G has a normal subgroup H such that H is abelian, H is finitely generated and G/H is finite, then $K[G]$ satisfies the zero divisor conjecture.*

Suppose this lemma true. Let P be the Promislow group and K be a field. By Lemma 3.1.7 and Lemma 3.1.6, the group P satisfies all assumptions of Lemma D and this implies that $K[P]$ satisfies the zero divisor conjecture. □

Proof of Lemma D. Bartosz Malman in [8, Theorem 3.28] proved that given a group G, the zero divisor conjecture is satisfied by every group ring $K[G]$, where K is any field, if and only if it is satisfied by every group ring $K[G]$, where K is a finite field. Therefore, it suffices to prove Lemma D under the assumption that K is a finite field. Let K be a finite field and G be a torsion free group such that G has a normal abelian finitely generated subgroup H with G/H finite. These assumptions over G imply that G is a polycyclic-by-finite group[6], indeed

[6] A *polycyclic-by-finite group* is a virtually polycyclic group. A *polycyclic group* is a group that admits a subnormal series with cyclic factors.

H is a polycyclic group[7]. At this point, the conclusion follows from the more general result stating that every group ring over a field of prime characteristic and of a tosion free polycyclic-by-finite group satisfies the Kaplansky zero divisor conjecture ([1, Theorem 2]). □

Corollary 3.2.2. *Let P be the Promislow group and K be a field. Let $\alpha, \alpha' \in K[P]$ be elements such that $\alpha'\alpha = 1_{K[P]}$. Then $\alpha\alpha' = 1_{K[P]}$ holds and, in particular, α is a unit in $K[P]$.*

Proof. Let P be the Promislow group and K be a field. Let $\alpha, \alpha' \in K[P]$ be elements such that $\alpha'\alpha = 1_{K[P]}$. Then

$$\alpha\alpha' = \alpha(\alpha'\alpha)\alpha'$$

holds and this implies

$$\alpha\alpha'(1 - \alpha\alpha') = 0_{K[P]}.$$

By Lemma 3.2.1, the group ring $K[P]$ has no non-zero zero-divisors; hence, either $\alpha\alpha' = 0$ or $\alpha\alpha' = 1$ holds. First possibility can't happen, because by assumption $\alpha'\alpha = 1$ (and $K[P]$ is not the trivial ring). We conclude that $\alpha\alpha' = 1$ holds. □

Notations. At the beginning of the previous section, we established that with a and b we always denote the two generators of the Promislow group P that appear in the presentation given to define it. Set

$$x := a^2,\ y := b^2,\ z := (ab)^2.$$

From now on, when talking about x, y or z we will always refer to this setting.

Remark 3.2.3. Let K be a field, P be the Promislow group and H be its normal subgroup generated by $\{x, y, z\}$. The group P acts over H by conjugation, that is there exists the group homomorphism

$$\begin{aligned} P &\longrightarrow \mathrm{Aut}(H) \\ w &\longmapsto \phi^*_w : p \mapsto \phi^*_w(p) := wpw^{-1}. \end{aligned}$$

On the other hand, there exists a monomorphism $\mathrm{Aut}(H) \to \mathrm{Aut}(K[H])$ in the category of groups (Lemma 1.1.13, where $\mathrm{Aut}(K[H])$ denotes the group of automorphisms of the group ring $K[H]$ as a K-algebra). Therefore, we get an action of G over $K[H]$ (in the category of K-algebras):

$$\begin{aligned} \phi : P &\longrightarrow \mathrm{Aut}(K[H]) \\ w &\longmapsto \phi_w : p \mapsto \phi_w(p) := wpw^{-1}. \end{aligned}$$

Let $w \in P$. According to the notation introduced at the beginning of this chapter, we have $(-)^w = \phi^*_{w^{-1}}(-) : H \to H$. We extend this notation to all $K[H]$, setting for every $p \in K[H]$

$$p^w := \phi_{w^{-1}}(p).$$

[7] An abelian finitely generated group is always a polycyclic group. Indeed, let A be a finitely generated abelian group. By the fundamental theorem of finitely generated abelian groups, A is isomorphic to a finite product of cyclic groups $C_1 \times \cdots \times C_n$. Up to isomorphism, A admits the following normal subseries: $1 \trianglelefteq C_1 \trianglelefteq C_1 \times C_2 \trianglelefteq \cdots \trianglelefteq C_1 \times \cdots \times C_n$ and the quotient of each group in such a series with the previous one in the series is a cyclic group.

Suppose now $w, w' \in \{1, a, b, ab\}$ and let $p \in K[H]$. Then following formulas hold:

$$p^{ww'} = (p^w)^{w'} = (p^{w'})^w, \tag{3.2}$$
$$p^{w^2} = p, \tag{3.3}$$
$$p^{w^{-1}} = p^w. \tag{3.4}$$

First equality follows from the fact that ϕ is a group homomorphism:

$$\begin{aligned}(-)^{ww'} &= \phi((ww')^{-1})(-) = \phi(w'^{-1}) \circ \phi(w^{-1})(-) \\ &= \phi(w'^{-1})((-)^w) = ((-)^w)^{w'}.\end{aligned}$$

To check second equality it suffices to check that the $(-)^w, (-)^{w'} : K[H] \to K[H]$ commute if restricted to H (H being a basis of $K[H]$ as a K-module), equivalently that they commute when restricted to $\{x, y, z\}$, because $\{x, y, z\}$ is a generating set of H as a group and the restrictions of $(-)^w$ and $(-)^{w'}$ are group homomorphisms. By Remark 3.1.5, both $(-)^w$ and $(-)^{w'}$ send each element in $\{x, y, z\}$ to a power of the element itself and all maps behaving in such a way always commute. By the same argument used for the second equality, to check third and fourth equality we may suppose, without lost of generality, that p belongs to $\{x, y, z\}$. Let $p \in \{x, y, z\}$, then:

- $p^{w^2} = (p^w)^w = p$ because of formulas in Remark 3.1.5;
- $p^{w^{-1}} = p^w$ thanks to last sentence of Remark 3.1.5.

Lemma 3.2.4. *Let K be a field and P be the Promislow group. Let H be the subgroup of P generated by $\{x, y, z\}$. Then $K[P]$ is a free $K[H]$-module generated by $\{1, a, b, ab\}$.*

Proof. Let K be a field, P be the Promislow group and H be the subgroup of P generated by $\{x, y, z\}$. The group ring $K[H]$ is abelian, H being abelian (Lemma 3.1.6). We first prove that

$$K[P] = \{p + qa + rb + sab \mid p, q, r, s \in K[H]\}.$$

Indeed, let $\alpha \in K[P]$ be any element, then we can write

$$\alpha = a_0x_0 + a_2x_2 + \cdots + a_nx_n \in K[P],$$

where $n \in \mathbb{N}$ and, for every $0 \leq i \leq n$, the coefficient a_i belongs to K and the element x_i belongs to P. The subgroup H has index 4 in P and the projections of 1_P, a, b and ab in the quotient P/H are pairwise distinct (Lemma 3.1.6). Therefore, the group P can be decomposed as a disjoint union:

$$P = H \cup Ha \cup Hb \cup Hab. \tag{3.5}$$

We deduce that for every $0 \leq i \leq n$ there exists $p_i,\ q_i,\ r_i,\ s_i \in H$ such that

$$x_i = p_i + q_ia + r_ib + s_iab.$$

So, the sum in $K[P]$ being commutative,

$$\alpha = \left(\sum_{i=1}^{n} a_i p_i\right) + \left(\sum_{i=1}^{n} a_i q_i\right) a + \left(\sum_{i=1}^{n} a_i r_i\right) b + \left(\sum_{i=1}^{n} a_i s_i\right) ab$$

and

$$\sum_{i=1}^{n} a_i p_i,\ \sum_{i=1}^{n} a_i q_i,\ \sum_{i=1}^{n} a_i r_i,\ \sum_{i=1}^{n} a_i s_i \in K[H].$$

Eventually, since the union in 3.5 is disjoint, it follows that all the elements $p + qa + rb + sab$, with $p, q, r, s \in K[H]$ are pairwise distinct. □

Remark 3.2.5. Previous lemma can be generalised to any group ring $K[G]$ over a group G that admits a finite index subgroup H. That is, if H is a finite index subgroup of a group G, then $K[G]$ is freely-generated as a $K[H]$-module by a set of representatives in G of the right cosets of H in G.

Notations. Let P be the Promislow group and H be the abelian subgroup of P generated by $\{x, y, z\}$. Let $w \in \{1, a, b, ab\}$. We set this notation: for every $\alpha \in K[P]$,

$$\alpha_w := \text{coefficient of } w \text{ when writing } \alpha \text{ as a } K[H]\text{-linear combination of } 1,\ a,\ b,\ ab.$$

The element α_w is well-defined by Lemma 3.2.4 and belongs to $K[H]$.

Remember that the main purpose of this subsection is to exhibit sufficient conditions for elements in $K[P]$ to be units, where K is any field and P is the Promislow group. We will do this trying to determine conditions that make the product $\alpha \cdot \beta$ be the identity, where $\alpha, \beta \in K[P]$. In order to do this, we need to easily compute the product of elements in $K[P]$ and this motivates next Remark.

Remark 3.2.6. Let P be the Promislow group and H be the abelian subgroup of P generated by $\{x, y, z\}$. By Lemma 3.2.4, the group ring $K[P]$ is a free module over $K[H]$ generated by $\{1, a, b, ab\} \in K[P]$. Therefore, to study how the product between elements of $K[P]$ behaves, it suffices to compute the products of scalar multiples with coefficients in $K[H]$ of the elements in the basis $\{1, a, b, ab\}$. Let $p, p' \in K[H]$ and $w, w' \in \{1, a, b, ab\}$. Then

$$pwp'w' = pwp'w^{-1}ww' = pp'^{w}(ww'). \tag{3.6}$$

We want to write $pwp'w'$ as a $K[H]$-linear combination of $1,\ a,\ b,\ ab$ hence we need to rewrite ww' as a product of an element in H and an element in $\{1, a, b, ab\}$. The following table summarizes these factorizations (the 4×4 inner sub-matrix is the product of the first column with the first row, in this order).

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	x	ab	xb
b	b	$x^{-1}yz^{-1}ab$	y	$x^{-1}z^{-1}a$
ab	ab	$zy^{-1}b$	$y^{-1}a$	z

(3.7)

Some entries of this table are immediate to compute; for the others, we did these computations (applying formulas in Remark 3.1.5, last sentence in the same Remark and that H is abelian by Lemma 3.1.6):

$$\begin{aligned} ba &= a^{-1}(abab)aa^{-1}b^{-1} = z^{-1}a^{-1}b^{-2}aa^{-1}b = z^{-1}ya^{-2}ab = x^{-1}yz^{-1}ab;\\ bab &= a^{-1}(abab)aa^{-1} = z^{-1}a^{-2}a = x^{-1}z^{-1}a;\\ aba &= ababb^{-1} = zb^{-2}b = zy^{-1}b;\\ abb &= aya^{-1}a = y^{-1}a. \end{aligned}$$

Let $\alpha = p + qa + rb + sab$ and $\alpha' = p' + q'a + r'b + s'ab$ be elements in $K[P]$ with $p, q, r, s, p', q', r', s' \in K[H]$. Thanks to equation 3.6 considered together with last table, we get that

$$\begin{aligned} (\alpha'\alpha)_1 &= p'p + q'q^a x + r'r^b y + s's^{ab} z\\ (\alpha'\alpha)_a &= p'q + q'p^a + r's^b x^{-1}z^{-1} + s'r^{ab}y^{-1}\\ (\alpha'\alpha)_b &= p'r + q's^a x + r'p^b + s'q^{ab}y^{-1}z\\ (\alpha'\alpha)_{ab} &= p's + q'r^a + r'q^b x^{-1}yz^{-1} + s'p^{ab}. \end{aligned}$$

We conclude this subsection giving a family of ring endomorphisms of $K[P]$ where P is the Promislow group and K is any field. The knowledge of endomorphisms of a ring can be useful when studying the group of units of the ring itself, since the endomorphisms of a ring transform units into units. We will use the family of ring endomorphisms of $K[P]$ we're going to present at the end of next section (Remark 3.3.13).

Lemma 3.2.7. *Let P be the Promislow group and K be a field. For every pair of integers $i, j \in \mathbb{Z}$ there exists an homomorphism of R-algebras $\sigma_{i,j} : K[P] \to K[P]$ such that*

$$\begin{aligned} \sigma_{i,j} : K[P] &\longrightarrow K[P]\\ a &\longmapsto z^i a\\ b &\longmapsto z^j b \end{aligned}$$

Moreover

1. *$\sigma_{i,j}$ fixes $x = a^2$ and $y = b^2$ and on $z = abab$ we have $\sigma_{i,j}(z) = z^{2i-2j+1}$.*
2. *for every $i, j \in \mathbb{Z}$, the equality $\sigma_{i+j,j} = \sigma_{j,j} \circ \sigma_{i,0}$ holds.*

Proof. Let P be the Promislow group and K be a field. Fix $i, j \in \mathbb{Z}$. We prove the existence of the homomorphism $\sigma_{i,j}$ by applying Lemma 1.1.13: we define a group homomorphism $f : P \to P$ that extends to an isomorphism of $K[P]$. Since P is a finitely presented group, we define the desired isomorphism f applying the universal property of finitely presented group. Precisely, consider the set theoretic map

$$\begin{aligned} h : \{\, a, b \,\} &\longrightarrow P\\ a &\longmapsto z^i a\\ b &\longmapsto z^j b. \end{aligned}$$

This map preserves the relations that define P as a presented group, that is

$$h(a)^{-2} = h(b)^{-1}h(a)^2h(b),$$
$$h(b)^{-2} = h(a)^{-1}h(b)^2h(a)$$

hold (it's a straightforward computation that can be done applying the formulas for the conjugates of z written in Remark 3.1.5). Therefore, h induces a group homomorphism $f : P \to P$ which in turn induces a homomorphism of R-algebras $\sigma_{i,j} : K[P] \to K[P]$ by Lemma 1.1.13, as desired.

We prove points 1 and 2. We have

$$\begin{aligned}
\sigma_{i,j}(x) &= \sigma_{i,j}(a^2) = z^iaz^ia = a(a^{-1}z^ia)z^ia = az^{-i}z^ia = x,\\
\sigma_{i,j}(y) &= \sigma_{i,j}(b^2) = z^jbz^jb = b(b^{-1}z^jb)z^jb = bz^{-j}z^jb = y,\\
\sigma_{i,j}(z) &= \sigma_{i,j}(abab) = z^iaz^jbz^iaz^jb = a(a^{-1}z^ia)z^jbz^iaz^jb = az^{-i+j}bz^iaz^jb\\
&= ab(b^{-1}z^{-i+j}b)z^iaz^jb = abz^{i-j+i}az^jb = aba(a^{-1}z^{i-j+i}a)z^jb\\
&= abaz^{-2i+j+j}b = abab(b^{-1}z^{-2i+j+j}b) = zz^{2i-2j} = z^{2i-2j+1}
\end{aligned}$$

and this proves point 1. To prove point 2 it suffices to check that $\sigma_{i,j}$ and $\sigma_{j,j} \circ \sigma_{i,0}$ behave in the same way over a and b, indeed this implies that their restrictions to P coincides, hence by Lemma 1.1.13, $\sigma_{i,j}$ and $\sigma_{j,j} \circ \sigma_{i,0}$ must be equal to each other. Computing the images of a and b through $\sigma_{i,j}$ and $\sigma_{j,j} \circ \sigma_{i,0}$ is not difficult, since by point 1 we already know that $\sigma_{j,j}(z) = z$. □

3.2.2 Sufficient Conditions for (non-trivial) Units

Let K be a field and P be the Promislow group. An element $\alpha \in K[P]$ is a unit if and only if there exists $\alpha' \in K[P]$ such that $\alpha'\alpha = 1_{K[P]}$ holds; indeed, if such an element α' exist, then $\alpha\alpha' = 1_{K[P]}$ also holds (Corollary 3.2.2).

Remember that $K[P]$ is a $K[H]$-free module generated by $\{ 1, a, b, ab \}$, where H is the subgroup of P generated by $\{ x, y, z \}$ (Lemma 3.2.4). Let $\alpha = p + qa + rb + sab \in K[P]$ with $p, q, r, s \in K[H]$. The goals of following discussion are:

- finding conditions over p, q, r, s such that there exist $p', q', r', s' \in K[H]$ such that $(p' + q'a + r'b + s'ab)(p + qa + rb + sab) = 1_{K[P]}$ holds;
- if there exist $p', q', r', s' \in K[H]$ such that $(p' + q'a + r'b + s'ab)(p + qa + rb + sab) = 1_{K[P]}$ holds, determining $p', q', r', s' \in K[H]$ as functions of p, q, r, s.

By Remark 3.2.6, given $p', q', r', s' \in K[H]$, the equality $(p' + q'a + r'b + s'ab)(p + qa + rb + sab) = 1_{K[P]}$ holds if and only if following system is satisfied:

$$\begin{cases}
p'p + q'q^ax + r'r^by + s's^{ab}z = 1\\
p'q + q'p^a + r's^bx^{-1}z^{-1} + s'r^{ab}y^{-1} = 0\\
p'r + q's^ax + r'p^b + s'q^{ab}y^{-1}z = 0\\
p's + q'r^a + r'q^bx^{-1}yz^{-1} + s'p^{ab} = 0.
\end{cases} \tag{3.8}$$

We focus on second and third equations: we split summaries in the first sides so that second and third equations of system 3.8 are satisfied if the following system is satisfied:

$$\begin{cases} p'q + q'p^a = 0 \\ r's^b x^{-1}z^{-1} + s'r^{ab}y^{-1} = 0 \\ p'r + r'p^b = 0 \\ q's^a x + s'q^{ab}y^{-1}z = 0. \end{cases} \tag{3.9}$$

This new system is a linear system in the unknowns p', q', r' s' and coefficient in the domain $K[H]$, whose associated matrix is

$$\begin{pmatrix} q & p^a & 0 & 0 \\ 0 & 0 & ys^b & xzr^{ab} \\ r & 0 & p^b & 0 \\ 0 & yxs^a & 0 & zq^{ab} \end{pmatrix}.$$

System 3.9 admits a non-trivial solution $(p', q', r', s') \in K[H]^4$ if and only if the determinant of last matrix is zero[8], that is if and only if

$$qp^b r^{ab} s^a x^2 - p^a q^{ab} r s^b = 0$$

(we multiplied the determinant by $y^{-1}z^{-1} \in K[H]$). Last equation is satisfied if following system is satisfied:

$$\begin{cases} p^a q^{ab} = xqp^b \\ s^a r^{ab} = x^{-1} r s^b. \end{cases} \tag{3.10}$$

We now suppose that $p,\ q,\ r,\ s$ satisfies system 3.10 and we look for a non-trivial solution $(p', q', r', s') \in K[H]^4$ of system 3.9. We are going to determine p' as a function of only p, q' as a function of only q, r' as a function of only r and s' as a function of only s. We start setting

$$\boxed{s' := z^{-1}s^a}.$$

With such a definition, fourth equation of system 3.9 becomes $q'xy + q^{ab} = 0$ and it is satisfied setting q' as follows:

$$\boxed{q' := -x^{-1}y^{-1}q^{ab}}.$$

With such a definition, first equation of system 3.9 becomes equivalent to $xyp'q + q^{ab}p^a = 0$ and, since system 3.10 is satisfied,

$$xyp'q - q^{ab}p^a = 0 \Longleftrightarrow yp'q - qp^b = 0.$$

[8]Pay attention that in linear algebra theory is stated that, given a square matrix A with coefficients in a field F, the linear homogeneous system with associated matrix A admits a non-trivial solution with coefficient in F if and only if $\det A$ is zero. This result generalizes to matrices with coefficients in any domain. Indeed, let R be a domain, F be the field of fractions of R and A be a square matrix with coefficients in R. If the linear homogeneous system with associated matrix A admits a non-trivial solution with coefficient in R, then this is also a solution when we work inside the field F, hence $\det A$ is zero. Conversely, if $\det A$ is zero, then the linear homogeneous system with associated matrix A admits a non-trivial solution $\overline{x}$ with coefficient in F. All the scalar multiples of $\overline{x}$ are solutions of the system; in particular, being F the field of fractions of R, it's possible to find $\lambda \in F$ such that all the coefficients $\lambda\overline{x}$ belong to R and $\lambda\overline{x}$ solves the system.

Thus, we set

$$\boxed{p' := y^{-1}p^b}$$

so that first equation is also satisfied. With these settings, third equation of system 3.9 becomes equivalent to $p^b r + yr'p^b = 0$ and it is satisfied setting r' as follows:

$$\boxed{r' := -y^{-1}r}.$$

It remains to check that our setting for (p', q', r', s') solves the second equation of system 3.9: replacing p' , q', r', s' with their definitions just given, we get

$$\begin{aligned} r's^b x^{-1}z^{-1} + s'r^{ab}y^{-1} = 0 &\iff -y^{-1}rs^b x^{-1}z^{-1} + z^{-1}s^a r^{ab}y^{-1} = 0 \\ &\iff rs^b x^{-1} - s^a r^{ab} = 0 \end{aligned}$$

and this last equation is satisfied since r and s are assumed to satisfy system 3.10. We summarize what we did until now: we were looking for sufficient conditions over $p,\ q,\ r,\ s$ such that there exist $p',\ q',\ r',\ s' \in K[H]$ that satisfy system 3.8; we proved that if $p,\ q,\ r,\ s$ satisfy system 3.10 and if $p',\ q',\ r',\ s'$ are as set in the boxes, then second and third equations of system 3.8 are satisfied. Eventually, if $p,\ q,\ r,\ s$ satisfy system 3.10 and if $p',\ q',\ r',\ s'$ are as set in the boxes, first and fourth equations of system 3.8 can be reformulated:

$$\begin{aligned} & p'p + q'q^a x + r'r^b y + s's^{ab}z = 1 \\ \iff & y^{-1}p^b p - y^{-1}q^{ab}q^a - y^{-1}rr^b y + s^a s^{ab} = 1 \\ \iff & p^b p - q^a q^{ab} - rr^b y + ys^a s^{ab} = y \end{aligned}$$

and

$$\begin{aligned} & p's + q'r^a + r'q^b x^{-1}yz^{-1} + s'p^{ab} = 0 \\ \iff & y^{-1}p^b s - x^{-1}y^{-1}q^{ab}r^a - y^{-1}rq^b x^{-1}yz^{-1} + z^{-1}s^a p^{ab} = 0 \\ \iff & xzp^b s - zq^{ab}r^a - yrq^b + xys^a p^{ab} = 0. \end{aligned}$$

We can summarize what has been deduced so far in the following lemma, which therefore turns out to be proved.

Lemma 3.2.8. *Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{ x, y, z \}$ and let K be a field. Let $\alpha = p + qa + rb + sab \in K[P]$, with $p, q, r, s \in K[H]$. If the system*

$$\begin{cases} p^a q^{ab} = xqp^b \\ s^a r^{ab} = x^{-1}rs^b \\ xzp^b s - zq^{ab}r^a - yrq^b + xys^a p^{ab} = 0 \\ p^b p - q^a q^{ab} - rr^b y + ys^a s^{ab} = y \end{cases} \tag{3.11}$$

is satisfied, then α is a unit and its inverse is $\alpha' = p' + q'a + r'b + s'ab$ with

$$\begin{aligned} p' &= y^{-1}p^b \\ q' &= -x^{-1}y^{-1}q^{ab} \\ r' &= -y^{-1}r \\ s' &= z^{-1}s^a. \end{aligned}$$

From last sufficient conditions for units, we can exhibit new conditions: on one hand, new ones are more restrictive (that is, if a unit satisfies new conditions then it also satisfies old conditions); on the other hand, it could be easier to control that the candidate unit satisfies new conditions then controlling that it verifies old conditions. The way to produce these new condition is suggested by Murray in [9]: the idea is, starting from the first two equations in the system 3.11, to construct four equations, where one depends only by p, one depends only by q, one depends only by r and one depends only by s.

Corollary 3.2.9. *Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let $\alpha = p + qa + rb + sab \in K[P]$, with $p, q, r, s \in K[H]$. If the following system is satisfied, then α is a unit.*

$$\begin{cases} p^{ab} = x^{-1}y^{-1}p \\ q^{ab} = yq \\ r^{ab} = x^{-1}r \\ s^{ab} = s \\ zyp^a s + s^a p = zyqr^a + rq^a \\ p^a p + xs^a s = x + xqq^a + rr^a \end{cases} \tag{3.12}$$

Proof. Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let $\alpha = p+qa+rb+sab \in K[P]$, with $p, q, r, s \in K[H]$ and suppose that $p,\ q,\ r,\ s$ satisfy system 3.12. By Lemma 3.2.8, to prove that α is a unit it suffices to prove that $p,\ q,\ r,\ s$ satisfy system 3.11. Inside next computations, we will indicate with (A) equalities for which we apply our assumptions over $p,\ q,\ r,\ s$ and with (B) equalities for which we apply formulas stated in Remark 3.2.3 together with formulas stated in Remark 3.1.5. We have

$$\begin{aligned} p^a q^{ab} &\overset{(B)}{=} (p^{ab})^b q^{ab} \overset{(A)}{=} (x^{-1}y^{-1}p)^b yq = xp^b q; \\ s^a r^{ab} &\overset{(B)}{=} (s^{ab})^b r^{ab} \overset{(A)}{=} x^{-1} r s^b; \\ xzp^b s + xys^a p^{ab} &\overset{(B)}{=} xz(p^{ab})^a s + xys^a p^{ab} \overset{(A)}{=} yzp^a s + s^a p \overset{(A)}{=} zyqr^a + rq^a \\ &\overset{(B)}{=} zy(q^{ab})^{ab} r^a + r(q^{ab})^b \overset{(A)}{=} zqr^a + yrq^b; \\ p^b p + ys^a s^{ab} &\overset{(B)}{=} (p^{ab})^a p + ys^a s^{ab} \overset{(A)}{=} x^{-1}yp^a p + ys^a s = x^{-1}y(p^a p + xs^a s) \\ &\overset{(A)}{=} x^{-1}y(x + xqq^a + rr^a) = y + yqq^a + x^{-1}yrr^a \\ &\overset{(B)}{=} y + yqq^a + x^{-1}yr(r^{ab})^b \overset{(A)}{=} y + q^{ab}q^a + yrr^b. \end{aligned}$$

□

Corollary 3.2.10. *Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let $\alpha = p + qa + rb + sab$, with $p, q, r, s \in K[H]$, be a unit of $K[P]$ such that (p, q, r, s) satisfies system 3.11. Then $\alpha' := p' + q'a + r'b + s'ab$ is a unit for all the nine tuples (p', q', r', s') constructed matching any of the following possibilities for (p', s') with any of the following possibilities for (q', r').*

$$\begin{aligned} (p', s') :&\quad (p, s),\ (zp, zs),\ (z^{-1}p, z^{-1}s) \\ (q', r') :&\quad (q, r),\ (zq, zr),\ (z^{-1}q, z^{-1}r) \end{aligned}$$

Proof. Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let $\alpha = p + qa + rb + sab$, with $p, q, r, s \in K[H]$, be a unit of $K[P]$ such that (p, q, r, s) satisfies system 3.11. We prove that $\alpha' := p + zqa + zrb + sab$ and $\alpha'' := zp + qa + rb + zsab$ are units. Proof for all the other possibilities are analogous. By Lemma 3.2.8, it suffices to prove that both $(\alpha'_1, \alpha'_a, \alpha'_b, \alpha'_{ab})$ and $(\alpha''_1, \alpha''_a, \alpha''_b, \alpha''_{ab})$ solve system 3.11. In the following lines, chains of equalities in [1.1], [2.1], [3.1], [4.1] imply that (zp, q, r, zs) satisfies system 3.11 and chains of equalities in [1.2], [2.2], [3.2], [4.2] imply that (p, zq, zr, s) is a unit. Inside the computations, we denote with

(A) equalities for which we apply that (p, q, r, s) satisfies system 3.11;

(B) equalities for which we use Remark 3.1.5.

We have:

$$[1.1] \quad (zp)^a q^{ab} \overset{(B)}{=} z^{-1} p^a q^{ab} \overset{(A)}{=} z^{-1} xqp^b \overset{(B)}{=} xq(zp)^b;$$

$$[1.2] \quad p^a (zq)^{ab} \overset{(B)}{=} zp^a q^{ab} \overset{(A)}{=} zxqp^b = x(zq)p^b;$$

$$[2.1] \quad (zs)^a r^{ab} \overset{(B)}{=} z^{-1} s^a r^{ab} \overset{(A)}{=} z^{-1} x^{-1} rs^b \overset{(B)}{=} x^{-1} r(zs)^b;$$

$$[2.2] \quad s^a (zr)^{ab} \overset{(B)}{=} zs^a r^{ab} \overset{(A)}{=} zx^{-1} rs^b = x^{-1}(zr)s^b;$$

$$[3.1] \quad xz(zp)^b zs - zq^{ab} r^a - yrq^b + xy(zs)^a (zp)^{ab} \overset{(B)}{=} xzp^b s - zq^{ab} r^a - yrq^b + xys^a p^{ab} \overset{(A)}{=} 0$$

$$[3.2] \quad xp^b s - z(zq)^{ab} (zr)^a - y(zr)(zq)^b + xys^a p^{ab} \overset{(B)}{=} xzp^b s - zq^{ab} r^a - yrq^b + xys^a p^{ab} \overset{(A)}{=} 0$$

$$[4.1] \quad (zp)^b zp - q^a q^{ab} - rr^b y + y(zs)^a (zs)^{ab} \overset{(B)}{=} p^b p - q^q a^{ab} - rr^b y + ys^a s^{ab} \overset{(A)}{=} y$$

$$[4.2] \quad p^b p - (zq)^a (zq)^{ab} - (zr)(zr)^b y + ys^a s^{ab} \overset{(B)}{=} p^b p - q^q a^{ab} - rr^b y + ys^a s^{ab} \overset{(A)}{=} y.$$

□

Lemma 3.2.11. *Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let $\alpha \in K[H]$. If α is a unit in $K[P]$, then α is a unit in $K[H]$ and, in particular, it's a trivial unit.*

Proof. Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{x, y, z\}$ and let K be a field. Let α be a unit of $K[P]$ such that α belongs to $K[H]$. We first prove that α is also a unit in $K[H]$, i.e. that the inverse of α in $K[P]$ actually belongs to $K[H]$. Let β be the inverse of α in $K[P]$; by Lemma 3.2.4, there exist $p, q, r, s \in K[H]$ such that $\beta = p + qa + rb + sab$. Since β is the inverse of α, we have

$$1 = \alpha\beta = \alpha p + \alpha qa + \alpha rb + \alpha sab.$$

The supports $\mathrm{Supp}(\alpha p)$, $\mathrm{Supp}(\alpha qa)$, $\mathrm{Supp}(\alpha rb)$ and $\mathrm{Supp}(\alpha sab)$ are pairwise disjoint because, α belonging to H, following inclusions hold

$$\begin{aligned} &\mathrm{Supp}(\alpha p) \subseteq H, && \mathrm{Supp}(\alpha qa) \subseteq Ha \\ &\mathrm{Supp}(\alpha rb) \subseteq Hb, && \mathrm{Supp}(\alpha sab) \subseteq Hab \end{aligned} \qquad (3.13)$$

and $H \cup Ha \cup Hb \cup Hab$ is a disjoint union (consequence of third point of Lemma 3.1.6). Therefore, $\mathrm{Supp}(\alpha\beta)$ can be written as a disjoint union:

$$\mathrm{Supp}(\alpha\beta) = \mathrm{Supp}(\alpha p) \cup \mathrm{Supp}(\alpha qa) \cup \mathrm{Supp}(\alpha rb) \cup \mathrm{Supp}(\alpha sab).$$

Remembering that $1 = \alpha\beta$ holds, we get the disjoint union

$$\{ 1 \} = \mathrm{Supp}(\alpha p) \cup \mathrm{Supp}(\alpha qa) \cup \mathrm{Supp}(\alpha rb) \cup \mathrm{Supp}(\alpha sab).$$

This last equality of sets together with inclusions in 3.13 implies that $\mathrm{Supp}(\alpha qa)$, $\mathrm{Supp}(\alpha rb)$ and $\mathrm{Supp}(\alpha sab)$ are all empty, that is $\alpha qa = \alpha rb = \alpha sab = 0$ holds; since α, a and b are units, this is equivalent to

$$q = r = s = 0.$$

We just proved that

$$\beta = p \in K[H]$$

holds, as desired.

On the other hand, H is an abelian torsion free group by Lemma 3.1.6, thus $K[H]$ satisfies the unit conjecture by Theorem 2.2.5. Thus, α must be a trivial unit in $K[H]$ and, by definition of trivial units, this means that α is a trivial unit even in $K[P]$. □

Lemma 3.2.12. *Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{ x, y, z \}$ and let K be a field. Let $\alpha = p + qa + rb + sab$ be a unit of $K[P]$ with $p, q, r, s \in K[H]$.*

(a) If exactly one element between p, q, r and s is non-zero, then this element is a trivial unit in $K[H]$ and α is a trivial unit in $K[P]$.

(b) If at least two elements between p, q, r and s are non-zero, then α is a non-trivial unit in $K[P]$.

Proof. Let P be the Promislow group, let $H \subseteq P$ be the subgroup generated by $\{ x, y, z \}$ and let K be a field. Let $\alpha = p + qa + rb + sab$ be a unit of $K[P]$ with $p, q, r, s \in K[H]$. We first prove point (a): suppose that exactly one element between p, q, r and s is non-zero and let $w \in \{ 1, a, b, ab \}$ be such that α_w is non-zero. By assumption, $\alpha = \alpha_w w$ is a unit, hence

$$\alpha_w = \alpha_w \cdot w \cdot w^{-1} = \alpha \cdot w^{-1}$$

is also a unit in $K[P]$. By Lemma 3.2.11, this implies that α_w is both a trivial unit in $K[H]$ and in $K[P]$. By definition of trivial units, this means that there exists $v \in H$ such that $\mathrm{Supp}(\alpha_w) = \{ v \}$ holds. Therefore

$$\mathrm{Supp}(\alpha) = \mathrm{Supp}(\alpha_w w) = \{ vw \}$$

which is a singleton, i.e. α is a trivial unit.

We now prove point (b): suppose that at least two elements between p, q, r and s are non-zero. We have that $\mathrm{Supp}(p)$, $\mathrm{Supp}(qa)$, $\mathrm{Supp}(rb)$ and $\mathrm{Supp}(sab)$ are pairwise disjoint, because following inclusions hold

$$\mathrm{Supp}(p) \subseteq H, \quad \mathrm{Supp}(qa) \subseteq Ha, \quad \mathrm{Supp}(rb) \subseteq Hb, \quad \mathrm{Supp}(sab) \subseteq Hab$$

and $H \cup Ha \cup Hb \cup Hab$ is a disjoint union (consequence of third point of Lemma 3.1.6). Therefore, $\mathrm{Supp}(\alpha)$ can be written as a disjoint union:

$$\mathrm{Supp}(\alpha) = \mathrm{Supp}(p) \cup \mathrm{Supp}(qa) \cup \mathrm{Supp}(rb) \cup \mathrm{Supp}(sab). \tag{3.14}$$

On the other hand, if $w \in \{1, a, b, ab\}$ is such that α_w is non-zero then $\alpha_w w$ is also non-zero, (w is a unit, thus it can't be a zero divisor). Therefore, our assumption that at least two of the elements p, q, r and s are non-zero implies that at least two of the sets $\mathrm{Supp}(p)$, $\mathrm{Supp}(qa)$, $\mathrm{Supp}(rb)$ and $\mathrm{Supp}(sab)$ are non-empty. This last fact together with the fact that union in 3.14 is disjoint implies that α is a non-trivial unit. □

3.3 Explicit Counterexamples to the Unit Conjecture

The purpose of this section is to prove that every group ring $K[P]$ of the Promislow group P over a field K of prime characteristic doesn't satisfy the Kaplansky unit conjecture. We will reach this result as a corollary of the fact that every group ring $K[P]$ of the Promislow group P over a finite field K has a non-trivial unit. To do this, we will explicitly provide non-trivial units in such group rings; precisely, we will provide explicit solutions of the system in Corollary 3.2.9.

The non-trivial unit in $\mathbb{F}_2[P]$, where $\mathbb{F}_2$ is the finite field with only two elements, we are going to exhibit is the one provided by Gardam [3, Theorem A]. It seems far to be an intuitive example of solution of the system 3.12. The only information that Gardam gave on how he found the long-sought-after counterexample is that it involved a computer search[9].

The family of non-trivial units in $\mathbb{F}_p[P]$, where p is a prime number and $\mathbb{F}_p$ is the finite field with p elements, we are going to exhibit is an extension of the family provided by Murray [9, Theorem 3], where the additional units extending Murray's family of units have been provided by Passman [11].

Notations. Let $p \in \mathbb{N}$ be a prime number. We denote with $\mathbb{F}_p$ the finite field with p elements.

3.3.1 Non-trivial Units over Fields of Characteristic 2

Lemma 3.3.1. *Let P be the Promislow group and $\mathbb{F}_2$ be the field with two elements. In the group ring $\mathbb{F}_2[P]$ set*[10]

$$\begin{aligned}
p &:= (1+x)(1+y)(1+z^{-1}),\\
q &:= x^{-1}y^{-1} + x + y^{-1}z + z,\\
r &:= 1 + x + y^{-1}z + xyz,\\
s &:= 1 + (x + x^{-1} + y + y^{-1})z^{-1}.
\end{aligned}$$

Then (p,q,r,s) satisfies system 3.12, hence $\alpha := p + qa + rb + sab$ is a non-trivial unit in the group ring $\mathbb{F}_2[P]$.

[9] Even if this is not written in his article [3], Gardam communicated it during the online talk he gave on February 22, 2021.

[10] These choices arises from a computer search.

Proof. Let P be the Promislow group and $\alpha \in \mathbb{F}_2[P]$ defined as in the statement. Let H be the subgroup of P generated by $\{x, y, z\}$. We first suppose that α is a unit. The property of α to be a non-trivial unit (referring to Definition 1.1.7) follows from Lemma 3.2.12. We now prove that α satisfies system 3.12; supposing this true then, by Corollary 3.2.9, α is a unit. Equations from first to fourth in the system are easily verified, indeed:

$$\begin{aligned}
p^{ab} &= (1 + x^{-1})(1 + y^{-1})(1 + z^{-1}) = x^{-1}y^{-1}p \\
q^{ab} &= xy + x^{-1} + yz + z = y(x + x^{-1}y^{-1} + z + y^{-1}z) = yq \\
r^{ab} &= 1 + x^{-1} + yz + x^{-1}y^{-1}z = x^{-1}(x + 1 + xyz + y^{-1}z) = x^{-1}r \\
s^{ab} &= 1 + (x^{-1} + x + y^{-1} + y)z^{-1} = s
\end{aligned}$$

For fifth equation in the system we first compute the products involved. On one side we have:

$$\begin{aligned}
s^a p &= (1 + x)(1 + y)(1 + z^{-1})[1 + (x + x^{-1} + y + y^{-1})z] \\
&= (1 + x)(1 + y)(1 + z)[z^{-1} + x + x^{-1} + y + y^{-1}]
\end{aligned}$$

and

$$\begin{aligned}
zyp^a s &= zy(ps^a)^a \\
&= (1 + x)(1 + y)(1 + z)[z + x + x^{-1} + y + y^{-1}].
\end{aligned}$$

To compute the right hand side the idea is: since $zyqr^a = zy(rq^a)^a$ holds, we write rq^a "separating" the elements that are fixed for the map $zy(-)^a$, so that these elements will disappear in the sum $rq^a + zy(rq^a)^a$ because we're working over a field of characteristic 2. We have:

$$\begin{aligned}
rq^a =&(1 + x + y^{-1}z + xyz)(x^{-1}y + x + yz^{-1} + z^{-1}) \\
&= x^{-1}y + x + yz^{-1} + z^{-1} + y + x^2 + xyz^{-1} + xz^{-1} \\
&\quad + x^{-1}z + x + 1 + y^{-1} + y^2z + x^2yz + xy^2 + xy \\
&= (1 + x)(1 + y)(1 + z^{-1}) \\
&\quad + x^{-1}(y + z) + x(y^{-1}z + y^2) + x^2(1 + yz) + (y^2z + y^{-1})
\end{aligned}$$

and

$$\begin{aligned}
zyqr^a &= zy(q^a r)^a \\
&= (1 + x)(1 + y)(1 + z)z \\
&\quad + x^{-1}(y + z) + x(y^{-1}z + y^2) + x^2(1 + yz) + (y^2z + y^{-1}).
\end{aligned}$$

Since the group ring we're working in is over a field of characteristic 2, we get

$$\begin{aligned}
s^a p + zyp^a s &= (1 + x)(1 + y)(1 + z)(z + z^{-1}); \\
rq^a + zyqr^a &= (1 + x)(1 + y)(1 + z^{-1}) + (1 + x)(1 + y)(1 + z)z \\
&= (1 + x)(1 + y)(1 + z)(z^{-1} + z).
\end{aligned}$$

Hence fifth equation is verified. For sixth equation in the system we first compute the products involved. We'll try to "separate" the terms that are multiples of z or z^{-1} with coefficients in the ring of Laurent polynomials $\mathbb{F}_2[x^{\pm 1}, y^{\pm 1}]$ from all the other terms. On one side we have:

$$\begin{aligned} p^a p &= (1+x)^2(1+y)(1+y^{-1})(1+z)(1+z^{-1}) \\ &= (1+x^2)(1+y)(1+y^{-1})(1+z)(1+z^{-1}) \\ &= (1+x^2)(y+y^{-1})(z+z^{-1}) \end{aligned}$$

and

$$\begin{aligned} xs^a s &= x[1+(x+x^{-1}+y+y^{-1})z][1+(x+x^{-1}+y+y^{-1})z^{-1}] \\ &= x+(x^2+1+xy+xy^{-1})(z+z^{-1})+x(x+x^{-1}+y+y^{-1})^2 \\ &= x+(x^2+1+xy+xy^{-1})(z+z^{-1})+x(x^2+x^{-2}+y^2+y^{-2}). \end{aligned}$$

On the other side we have:

$$\begin{aligned} xqq^a &= x(x^{-1}y^{-1}+x+y^{-1}z+z)(x^{-1}y+x+yz^{-1}+z^{-1}) \\ &= x(x^{-1}y^{-1}+x)(x^{-1}y+x)+x(y^{-1}z+z)(x^{-1}y+x) \\ &\quad + x(x^{-1}y^{-1}+x)(yz^{-1}+z^{-1})+x(y^{-1}z+z)(yz^{-1}+z^{-1}) \\ &= x(x^{-2}+y^{-1}+y+x^2)+z(1+y+x^2y^{-1}+x^2) \\ &\quad + z^{-1}(1+y^{-1}+x^2y+x^2)+x(y^{-1}+y) \\ &= x(x^{-2}+x^2)+z(1+y+x^2y^{-1}+x^2)+z^{-1}(1+y^{-1}+x^2y+x^2) \end{aligned}$$

and

$$\begin{aligned} rr^a &= (1+x+y^{-1}z+xyz)(1+x+yz^{-1}+xy^{-1}z^{-1}) \\ &= (1+x)^2+z^{-1}(1+x)(y+xy^{-1}) \\ &\quad + z(y^{-1}+xy)(1+x)+(y^{-1}+xy)(y+xy^{-1}) \\ &= 1+x^2+z^{-1}(y+xy+xy^{-1}+x^2y^{-1}) \\ &\quad + z(y^{-1}+xy+xy^{-1}+x^2y)+(1+xy^2+xy^{-2}+x^2) \\ &= x(y^2+y^{-2})+z(y^{-1}+xy+xy^{-1}+x^2y)+z^{-1}(y+xy+xy^{-1}+x^2y^{-1}) \end{aligned}$$

Putting together these computations, we get:

$$\begin{aligned} p^a p + xs^a s - x &= (z+z^{-1})(y+y^{-1}+x^2y+x^2y^{-1}+x^2+1+xy+xy^{-1}) \\ &\quad + x(x^2+x^{-2}+y^2+y^{-2}); \\ xqq^a + rr^a &= x(x^2+x^{-2}+y^2+y^{-2}) \\ &\quad + (z+z^{-1})(1+x^2)+zy+x^2y^{-1}z+y^{-1}z^{-1}+x^2yz^{-1} \\ &\quad + (z+z^{-1})(xy+xy^{-1})+y^{-1}z+x^2yz+yz^{-1}+x^2y^{-1}z^{-1} \\ &= x(x^2+x^{-2}+y^2+y^{-2}) \\ &\quad + (z+z^{-1})(1+x^2)+(z+z^{-1})(xy+xy^{-1}) \\ &\quad + (z+z^{-1})y+(z+z^{-1})x^2y^{-1}+(z+z^{-1})y^{-1}+(z+z^{-1})x^2y \\ &= x(x^2+x^{-2}+y^2+y^{-2}) \\ &\quad + (z+z^{-1})(y+y^{-1}+x^2y+x^2y^{-1}+x^2+1+xy+xy^{-1}). \end{aligned}$$

We can conclude that last equation of system 3.12 is also satisfied. □

Corollary 3.3.2. *Let P be the Promislow group and K be a field with characteristic 2. The group ring $K[P]$ doesn't satisfy the Kaplansky unit conjecture.*

Proof. Let P be the Promislow group and K be a field with characteristic 2. The field K contains a subfield, named *prime subfield*[11], isomorphic to the field with two elements $\mathbb{F}_2$, therefore $\mathbb{F}_2[P]$ is isomorphic to a subring of $K[P]$ (Remark 1.1.11). On the other hand, isomorphisms of group rings preserve the cardinality of the supports, that is: if $\phi : M \to N$ is an isomorphism of group rings, then for every $\alpha \in M$ we have

$$|\mathrm{Supp}(\phi(\alpha))| = |\mathrm{Supp}(\alpha)|.$$

Indeed, the injectivity of ϕ implies both the following equalities:

$$|\mathrm{Supp}(\phi(\alpha))| = |\phi(\mathrm{Supp}(\alpha))| = |\mathrm{Supp}(\alpha)|.$$

Since $\mathbb{F}_2[P]$ has a non-trivial unit (Lemma 3.3.1) and since isomorphisms of group rings preserve the cardinality of the supports, we obtain that $K[P]$ has a subring that admits a non-trivial units. Eventually, since non-trivial units in a subring stay non-trivial units in the whole ring $K[P]$, we conclude that $K[P]$ doesn't satisfy the unit conjecture. □

Remark 3.3.3. Let P be the Promislow group and K be a field. Let H be the subgroup of P generated by $\{ x, y, z \}$ and fix $w \in \{ x, y, z \}$. Since H is a free abelian group (Lemma 3.1.6), the set theoretic map $\{ x, y, z \} \to \{ x, y, z \}$ that maps w to w^{-1} and fixes the other elements induces a group homomorphism $H \to H$ and, by Lemma 1.1.13 this group homomorphism extends to a ring homomrphism $(-)_w : K[H] \to K[H]$ that behaves as follows:

$$\begin{aligned} (-)_w : K[H] &\longrightarrow K[H] \\ w &\longmapsto w_w := w^{-1} \\ (\{ x, y, z \} \smallsetminus \{ w \}) \ni v &\longmapsto v_w := v. \end{aligned}$$

Our notation coincides with the one introduced by Murray in [9]. Ring homomorphism just defined satisfies the following properties: for every $w, w' \in \{ x, y, z \}$, $v \in \{ a, b, ab \}$ and $p \in K[H]$,

$$(p_w)_{w'} = (p_{w'})_w, \tag{3.15}$$
$$(p_w)^v = (p^v)_w. \tag{3.16}$$

To check both the equalities it suffices to check that the maps $(-)_w, (-)_{w'}, (-)^v : K[H] \to K[H]$ commute if restricted to H (H being a basis of $K[H]$ as a K-module); equivalently, that they commute when restricted to $\{ x, y, z \}$, because $\{ x, y, z \}$ is a generating set of H as a group and the restrictions of $(-)_w$, $(-)_{w'}$ and $(-)^v$ are group homomorphisms. By definition, $(-)_w$, $(-)_{w'}$ and $(-)^v$ send each element in $\{ x, y, z \}$ to a power of the element itself and all maps behaving in such a way always commute.

[11] The *prime subfield* of a field is the field generated by the identity of the field itself. The prime field of a field F is isomorphic to $\mathbb{Q}$ if the characteristic of F is infinite, otherwise it is isomorphic to the field with p elements, where p is the characteristic of F.

Remark 3.3.4. Let P be the Promislow group, let $\mathbb{F}_2$ be the field with two elements and let $\alpha = p+qa+rb+sab$ be the non-trivial unit of $\mathbb{F}_2[P]$ constructed in the statement of Lemma 3.3.1. There exists new non-trivial units of $\mathbb{F}_2[P]$ of the form $\alpha' = p' + q'a + r'b + s'ab$ where p', q', r' and s' are obtained transforming, respectively, the elements p, q, r and s that form the fixed α. To find which transformations generate units, we look for transformations that create solutions of system 3.12, because a solution (p', q', r', s') of that system generates a unit in $\mathbb{F}_2[P]$ (Corollary 3.2.9). We restrict the search to transformations belonging to the set A defined as the union of

$$\{ (-)_w, z(-)_w, z^{-1}(-)_w, (-)^v, z(-)^v, z^{-1}(-)^v \}$$

for all the possible $w \in \{ x, y, z \}$ and $v \{ 1, a, b, ab \}$ and we proceed by steps.

- We first focus on the equations from one to four in the system. We individuate which transformations $\psi \in A$ realizes following implication:

  $$\begin{aligned} &p \text{ solves first equation in system 3.12} \\ &\quad \Longrightarrow p' := \psi(p) \text{ solves first equation in system 3.12.} \end{aligned}$$

  We proceed in an analogous way for q, r and s, trying to create elements q', r', s' that solve, respectively, second, third and fourth equation in the system 3.12 (under the assumption that q, r and s solve the system).

- Second, we focus on last two equations of the system. Left sides only depend on p and s and right sides only depend on q and r. The idea is to create (p', q', s', r') such that

  $$\begin{cases} zyp^a s + s^a p = zyp'^a s' + s'^a p' \\ zyqr^a + rq^a = zyq'r'^a + r'q'^a \end{cases} \tag{3.17}$$

  holds and

  $$\begin{cases} p^a p + xs^a s = p'^a p' + xs'^a s' \\ x + xqq^a + rr^a = x + xq'q'^a + r'r'^a \end{cases} \tag{3.18}$$

  holds. Therefore, we get that

  - if (p, q, r, s) satisfies fifth condition to be a unit, then, by system 3.17, (p', q', r', s') also satisfies fifth equation of system 3.12;
  - if (p, q, r, s) satisfies sixth condition to be a unit, then, by system 3.18, (p', q', r', s') also satisfies sixth equation of system 3.12.

It's clear that this procedure can create new units when starting from a unit that satisfies system 3.12. Although in the first step to produce (p', q', r', s') we can start to any tuple (p, q, r, s) that solves system 3.12, second step actually depends on the explicit form of the elements p, q, r and s appearing in the statement of Lemma 3.3.1. Eventually, we can affirm that units produced with such a procedure are all non-trivial unit, as a consequence of Lemma 3.2.12.

Example 3.3.5. Murray in [9] suggests some examples of non-trivial units $\alpha' = p' + q'a + r'b + s'ab$ where the tuples (p', q', r', s') are produced through the method explained in Remark 3.3.4. He proposes twelve tuples[12] that arise matching any of the following possibilities for (p', s') with any of the following possibilities for (q', r'):

$$\begin{aligned} (p', s'):&\quad (p, s),\ (p_z, zs),\ (p_z, z^{-1}s_z) \\ (q', r'):&\quad (q, r),\ (q, zr_x),\ (q_x, r_y),\ (q_x, zr_{yz}) \end{aligned}$$

We will not prove for each possible choice of (p', q', r', s') that it generates a unit, since the proof just consists of computations of Laurent polynomials in $\mathbb{F}_2[x^{\pm1}, y^{\pm1}, z^{\pm1}]$ and such computations can be done by a calculator. We will only prove in Example 3.3.6 that the tuple $(p', q', r', s') = (p, q_x, r_y, z)$ generates a unit because on one hand we want to give an explicit example of the reasoning methods explained in Remark 3.3.4, on the other hand we will need this tuple, in some way, to produce counterexamples to the unit conjecture in $\mathbb{F}_p[P]$ for every prime number $p \in \mathbb{N}$.

Example 3.3.6. We give here an explicit example of a unit produced through the method explained in Remark 3.3.4. Let $\alpha = p + qa + rb + sab$ be the non-trivial unit exhibited by Gardam (Lemma 3.3.1); explicitly we have

$$\begin{aligned} p &:= (1+x)(1+y)(1+z^{-1}), \\ q &:= x^{-1}y^{-1} + x + y^{-1}z + z, \\ r &:= 1 + x + y^{-1}z + xyz, \\ s &:= 1 + (x + x^{-1} + y + y^{-1})z^{-1}. \end{aligned}$$

We now prove that

$$\alpha' := p + q_x a + r_y b + sab$$

is a non-trivial unit. Suppose that α' is a unit; then it's a non-trivial unit by Lemma 3.2.12. We now prove that α' is a unit. By Corollary 3.2.9, it suffices to prove that (p, q_x, r_y, s) satisfies system 3.12. By Lemma 3.3.1, (p, q, r, s) satisfies system 3.12. Therefore (p, q_x, r_y, s) obviously satisfies first and fourth equation of the system. Inside following computations, we denote with

(A) equalities for which we apply that (p, q, r, s) satisfies system 3.12;

(B) equalities for which we use computations that have already been written inside the proof of Lemma 3.3.1;

(C) equalities for which we use formulas stated in Remark 3.3.3.

Second and third equations are easily verified, indeed

$$\begin{aligned} (q_x)^{ab} &\overset{(C)}{=} (q^{ab})_x \overset{(A)}{=} (yq)_x = yq_x, \\ (r_y)^{ab} &\overset{(C)}{=} (r^{ab})_y \overset{(A)}{=} (x^{-1}r)_y = x^{-1}r_y. \end{aligned}$$

[12] More precisely, Murray proposes eighteen tuples, exhibiting two more possibilities for the pair (q', r'). The possibilities we omitted here can be obtained just applying Corollary 3.2.10.

For fifth equation, we compute right sides on the pair (q_x, r_y):

$$\begin{aligned}
r_y q_x^a &= (1+x+yz+xy^{-1}z)(xy+x^{-1}+yz^{-1}+z^{-1}) \\
&= xy+x^{-1}+yz^{-1}+z^{-1}+x^2y+1+xyz^{-1}+xz^{-1} \\
&\quad + xy^2z+x^{-1}yz+y^2+y+x^2z+y^{-1}z+x+xy^{-1} \\
&= (1+x)(1+y)(1+z^{-1}) \\
&\quad + x^2(y+z)+(y^{-1}z+y^2)+x^{-1}(1+yz)+x(y^2z+y^{-1}); \\
zyq_x r_y^a &= zy(r_y q_x^a)^a \\
&= (1+x)(1+y)(1+z)z \\
&\quad + x^2(y+z)+(y^{-1}z+y^2)+x^{-1}(1+yz)+x(y^2z+y^{-1}).
\end{aligned}$$

Remembering that we're working in $\mathbb{F}_2[P]$ and comparing these computations with ones in the proof of Lemma 3.3.1, we get

$$\begin{aligned}
r_y q_x^a + zyq_x r_y^a &= (1+x)(1+y)(1+z)(z^{-1}+z) \\
&\overset{(B)}{=} rq^a + zyqr^a \overset{(A)}{=} s^a p + zyps^a
\end{aligned}$$

and this proves that $(p.q_x, r_y, s)$ satisfies fifth equation of the system 3.12. Eventually, for sixth equation, we compute right side on the pair (q_x, r_y):

$$\begin{aligned}
xq_x q_x^a &\overset{(C)}{=} x(qq^a)_x = x^2(xqq^a)_x \\
&= x^2[x(x^{-2}+x^2)+z(1+y+x^2y^{-1}+x^2)+z^{-1}(1+y^{-1}+x^2y+x^2)]_x \\
&= x(x^{-2}+x^2)+z(x^2+x^2y+y^{-1}+1)+z^{-1}(x^2+x^2y^{-1}+y+1); \\
r_y r_y^a &\overset{(C)}{=} (rr^a)_y \\
&= [x(y^2+y^{-2})+z(y^{-1}+xy+xy^{-1}+x^2y) \\
&\quad + z^{-1}(y+xy+xy^{-1}+x^2y^{-1})]_y \\
&= x(y^2+y^{-2})+z(y+xy^{-1}+xy+x^2y^{-1}) \\
&\quad + z^{-1}(y^{-1}+xy^{-1}+xy+x^2y).
\end{aligned}$$

Comparing these computations with ones in the proof of Lemma 3.3.1, we get

$$xq_x q_x^a + r_y r_y^a \overset{(B)}{=} xqq^a + rr^a \overset{(A)}{=} p^a p + xs^a s - x$$

and this proves that $(p.q_x, r_y, s)$ satisfies sixth equation of the system 3.12.

3.3.2 Non-trivial Units over Fields of Prime Characteristic

To find out non-trivial units in $\mathbb{F}_d[P]$ for every prime number $d \in \mathbb{N}$, where P is the Promislow group and $\mathbb{F}_d$ is the field with d elements, we will mix Murray and Passman's ideas. Murray's argumentation in [9] arises from an analogy between a fixed non-trivial unit in $\mathbb{F}_2[P]$ and a fixed non-trivial unit in $\mathbb{F}_3[P]$. The first one is the non-trivial unit showed in Example 3.3.6. The second one is the non-trivial unit stated in Lemma 3.3.7 (taken from [9, Theorem 2]). The analogy between these units is explained in Remark 3.3.8. Ingeniously exploiting this analogy, Murray comes to a double (that is, depending on two parameters) family of units in $\mathbb{F}_d[P]$ for every prime $d \in \mathbb{N}$. Passman [11] goes deeper into the research introduced by Murray, extending the family found by Murray to a triple family of non-trivial units.

Lemma 3.3.7. *Let P be the Promislow group and $\mathbb{F}_3$ be the field with two elements. In the group ring $\mathbb{F}_3[P]$ set*

$$\begin{aligned} p &:= (1+x)(1+y)(z^{-1}-z), \\ q &:= (1+x)(x^{-1}+y^{-1})(1-z^{-1}) + (1+y^{-1})(z-z^{-1}), \\ r &:= (1+y^{-1})(x+y)(z-1) + (1+x)(z-z^{-1}), \\ s &:= -z + (1+x+x^{-1}+y+y^{-1})(z^{-1}-1). \end{aligned}$$

Then $\alpha := p + qa + rb + sab$ is a non-trivial unit in the group ring $\mathbb{F}_3[P]$.

Proof. The tuple (p, q, r, s) in the statement satisfies system 3.12 in the group ring $\mathbb{F}_3[P]$, therefore α is a unit (it's a straightforward computation). Eventually, α is a non-trivial unit by Lemma 3.2.12. □

Remark 3.3.8. Let P be the Promislow group and $\mathbb{F}_2$ and $\mathbb{F}_3$ be, respectively, the fields with two and three elements. The unit of $\mathbb{F}_2[P]$ stated in Example 3.3.6 and the unit of $\mathbb{F}_3[P]$ stated in Lemma 3.3.7 are similar to each other. Precisely, if $\alpha = p + qa + rb + sab$ is one between these units in $\mathbb{F}_d[P]$, where $d \in \{2, 3\}$, then there exist seven Laurent polynomials $f_1, f_2, f_3, f_4, f_5, f_6, f_7 \in \mathbb{F}_p[z^{\pm 1}]$ such that following equalities hold:

$$\begin{aligned} p &= (1+x)(1+y)f_1, \\ q &= (1+x)(x^{-1}+y^{-1})f_2 + (1+y^{-1})f_3, \\ r &= (1+y^{-1})(x+y)f_4 + (1+x)f_5, \\ s &= (x+x^{-1}+y+y^{-1}+4)f_6 + f_7. \end{aligned}$$

For the unit exhibited in the statement of Lemma 3.3.7, it's quite immediate to individuate these seven Laurent polynomials in $\mathbb{F}_3[z^{\pm 1}]$. We prove now that the seven Laurent polynomials $f_1, \dots, f_7$ exist also for the unit exhibited in Example 3.3.6. This unit is $\alpha = p + qa + rb + sab$ with

$$\begin{aligned} p &:= (1+x)(1+y)(1+z^{-1}), \\ q &:= xy^{-1} + x^{-1} + y^{-1}z + z = (x^{-1}+y^{-1}+1+xy^{-1}) + (1+y^{-1})(z-1), \\ r &:= 1 + x + yz + xy^{-1}z = (x + xy^{-1} + y + 1)z + (1+x)(1-z), \\ s &:= 1 + (x + x^{-1} + y + y^{-1})z^{-1}. \end{aligned}$$

Hence, in this case,

$$\begin{aligned} f_1 &= 1 + z^{-1}, & f_2 &= 1 = f_7, & f_3 &= z - 1 \\ f_4 &= z, & f_5 &= 1 - z, & f_6 &= z^{-1} \end{aligned}$$

(to determine f_6 remember that the group ring we are working in is over a field of characteristic 2).

We now follow Murray and Passman's ideas in [9] and [11] to find units in every group ring of the Promislow group over finite fields.

Let P be the Promislow group, $d \in \mathbb{N}$ be a prime number and $f_1, \dots, f_7 \in \mathbb{F}_p[z^{\pm 1}]$ be Laurent polynomials. In $F_d[H]$, where H is the subgroup of P generated by $\{ x, y, z \}$, we set

$$\begin{aligned} p &:= (1+x)(1+y)f_1, \\ q &:= (1+x)(x^{-1}+y^{-1})f_2 + (1+y^{-1})f_3, \\ r &:= (1+y^{-1})(x+y)f_4 + (1+x)f_5, \\ s &:= (x+x^{-1}+y+y^{-1}+4)f_6 + f_7. \end{aligned} \tag{3.19}$$

We look for $f_1, \dots, f_7$ such that $\alpha := p + qa + rb + sab$ is a unit of $\mathbb{F}_d[P]$. By Corollary 3.2.9, a sufficient condition for α to be a unit is that α satisfies system 3.12; therefore, we look for $f_1, \dots, f_7$ such that α satisfies this system. First, for every Laurent polynomial $f \in \mathbb{F}_p[P]$, we set

$$f^* := f(z^{-1}) = f^a = f^b.$$

Equations from one to four in the system 3.12 are verified for any choice of $f_1, \dots, f_7$. Indeed, inserting in first equation our definitions of p, q, r, s we get

$$x^{-1}y^{-1}p = (1+x^{-1})(1+y^{-1})f_1 = p^{ab}.$$

Inserting in second equation our definitions of p, q, r, s we get

$$\begin{aligned} yq &= (1+x)(yx^{-1}+1)f_2 + (1+y)f_3 \\ &= (1+x^{-1})(y+x)f_2 + (1+y)f_3 = q^{ab}. \end{aligned}$$

Inserting in third equation our definitions of p, q, r, s we get

$$\begin{aligned} x^{-1}r &= (1+y^{-1})(1+x^{-1}y)f_4 + (1+x^{-1})f_5 \\ &= (1+y)(y^{-1}+x^{-1})f_4 + (1+x^{-1})f_5 = r^{ab}. \end{aligned}$$

The fact that fourth equation is verified is immediate. Therefore, we can restrict to consider just fifth and sixth equations of the system 3.12. When we insert our definitions of p, q, r and s, each side of these equations becomes a "long" Laurent polynomial in $\mathbb{F}_d[z^{\pm 1}][x^{\pm 1}, y^{\pm 1}]$. An equality of Laurent polynomials in $\mathbb{F}_d[z^{\pm 1}][x^{\pm 1}, y^{\pm 1}]$ is verified if and only if for every $i, j \in \mathbb{Z}$ the coefficient of $x^i y^j$ of the Laurent polynomial on the left side coincides with the coefficient of $x^i y^j$ of the Laurent polynomial on the right side. Because of this, fifth and sixth equations of the system 3.12 are satisfied by the elements p, q, r, s that we defined above if and only if the following system is satisfied in $\mathbb{F}_d[z^{\pm 1}]$:

$$\begin{cases} f_7^* f_7 = 1 \\ f_3^* f_3 = f_5^* f_5 = f_7^* f_6 + f_6^* f_7 + 4 f_6^* f_6 \\ f_2^* f_2 = f_4^* f_4 = f_6^* f_6 \\ f_1^* f_1 = f_2^* f_3 + f_4^* f_5 \\ f_2^* f_5 = z f_5^* f_2 = f_3^* f_4 = z f_4^* f_3 = f_6^* f_1 + z f_1^* f_6 - f_2^* f_4 - z f_4^* f_2 \\ f_3^* f_5 + z f_5^* f_3 = f_7^* f_1 + z f_1^* f_7 + 4(f_2^* f_4 + z f_4^* f_2) \end{cases} \tag{3.20}$$

First of all, we prove the following claim.

Claim. If $(f_1, \ldots, f_7)$ solves system 3.20 and there exists $i = 1, \ldots, 6$ such that $f_i = 0$ then for all $i = 1, \ldots, 6$, $f_i = 0$.

Proof of the claim. Suppose that $(f_1, \ldots, f_7)$ solves system 3.20. First, observe that for every Laurent polynomial in $\mathbb{F}_d[z^{\pm 1}]$ we have that

$$f = 0 \Leftrightarrow f^* = 0.$$

We get the following chains of implications (tags "n.m" over implications denote that to get the implication we're using m-th equality inside n-th equation in the system 3.20) and all these chains of implication turn out to prove the claim:

$$\begin{aligned} f_3 = 0 &\overset{2.1}{\Longleftrightarrow} f_5 = 0, \\ f_3 = 0 \ \wedge \ f_5 = 0 &\overset{4.1}{\Longrightarrow} f_1 = 0, \\ f_1 = 0 &\overset{*}{\Longrightarrow} f_3 = 0 \ \vee \ (f_2 = 0 \ \wedge \ f_4 = 0), \\ f_1 = 0 \ \wedge \ f_3 = 0 &\overset{**}{\Longrightarrow} f_2 = 0 \ \wedge \ f_4 = 0, \\ f_2 = 0 &\overset{3.1}{\Longleftrightarrow} f_4 = 0 \overset{3.2}{\Longleftrightarrow} f_6 = 0 \overset{2.1+2.2}{\Longrightarrow} f_3 = 0. \end{aligned}$$

It remains to check implication "$*$" and "$**$". For the first one, suppose $f_1 = 0$ holds. From fourth and fifth lines in the system 3.20 we get

$$\begin{cases} f_2^* f_3 = -f_4^* f_5 \\ f_2^* f_5 = z f_4^* f_3. \end{cases}$$

Hence

$$(f_2^*)^2 f_3 = -f_2^* f_5 f_4^* = -z(f_4^*)^2 f_3$$

holds. Therefore, since the ring $\mathbb{F}_d[z^{\pm 1}]$ is an integral domain, we get that at least one between $f_3 = 0$ and $(f_2^*)^2 = -z(f_4^*)^2$ holds. This last equality is equivalent to $f_2 = 0 = f_4$. Indeed, if f_2 and f_4 were not zero, then the module of the degree of $(f_2^*)^2$ would be even and the module of the degree of $-z(f_4^*)^2$ would be odd, thus they couldn't be the same.

Suppose now that both $f_1 = 0$ and $f_3 = 0$ hold. From third and sixth lines in the system 3.20 we get

$$\begin{cases} f_2^* f_2 = f_4^* f_4 \\ f_2^* f_4 = -z f_4^* f_2. \end{cases}$$

Hence

$$f_4^*(f_4)^2 = f_2 f_2^* f_4 = -z f_4^* (f_2)^2$$

holds. Arguing in the same way as done to prove $*$, we get that at least one between $f_2 = 0$ and $f_4 = 0$ holds but, by third line of the system, $f_2 = 0$ holds if and only if $f_4 = 0$ holds. □

If $f_1 = f_2 = \cdots = f_6 = 0$ holds, then, by our definitions of p, q, r and s we have $p + qa + rb + sab = f_7 ab$; by Lemma 3.2.12, such an element is a unit if and only if it is a trivial unit. Since we're interested in non-trivial units, from now on we will suppose that for every $i = 1, 2 \ldots, 6$, the Laurent polynomial f_i

is non-zero. Our purpose is to find at least one tuple $(f_1, \dots, f_7)$ which solves system 3.20. As above, we will use the tag "n.m", for appropriate $n, m \in \mathbb{N}_{>0}$, to label the m-th equality within the n-th equation.

First, we focus on equalities 2.1, 3.1 and 5.2:

$$\begin{cases} f_3 f_3^* = f_5 f_5^* & (2.1) \\ f_2 f_2^* = f_4 f_4^* & (3.1) \\ z f_5^* f_2 = f_3^* f_4 & (5.2) \end{cases}$$

Let $t \in \mathbb{Z}$. We start setting

$$\boxed{f_4 := z^t f_2}.$$

Under this setting, equation 3.1 is verified and equation (5.2) becomes

$$z f_5^* f_2 = z^t f_3^* f_2.$$

By assumption, f_2 is non-zero hence, the ring $\mathbb{F}_d[z^{\pm 1}]$ being an integral domain, this last equation is satisfied if and only if we set[13]

$$\boxed{f_5 := z^{1-t} f_3}.$$

Under this setting, system 3.20 becomes

$$\begin{cases} f_7^* f_7 = 1 \\ f_3^* f_3 = f_7^* f_6 + f_6^* f_7 + 4 f_6^* f_6 \\ f_2^* f_2 = f_6^* f_6 \\ f_1^* f_1 = (1 + z^{1-2t}) f_2^* f_3 \\ z^{1-t} f_2^* f_3 = z^t f_3^* f_2 \\ z^{1-t} f_2^* f_3 = f_6^* f_1 + z f_1^* f_6 - (z^t + z^{1-t}) f_2^* f_2 \\ (z^{1-t} + z^t) f_3^* f_3 = f_7^* f_1 + z f_1^* f_7 + 4(z^t + z^{1-t}) f_2^* f_2. \end{cases} \tag{3.21}$$

We now proceed with the following steps.

- We first try to solve the subsystem of system 3.21 given by

$$\begin{cases} f_6^* f_1 + z f_1^* f_6 - (z^t + z^{1-t}) f_6^* f_6 = z^{1-t} f_2^* f_3 & (A) \\ f_1^* f_1 = (1 + z^{1-2t}) f_2^* f_3 & (B) \\ z^{1-t} f_2^* f_3 = z^t f_3^* f_2 & (C) \end{cases}.$$

  We will determine f_1 and f_3 as multiples of f_6.

- Second, we replace, within first, second and seventh equation of system 3.21, f_1 and f_3 with the definitions set in previous step and we try to find at least one solution (it will depend only by f_2, f_6, f_7). We will determine Laurent polynomials f_6 and f_7 that satisfy this system. In this step the finite characteristic of the field $\mathbb{F}_d$ is needed.

- Third, we choice f_2 depending on f_6 in such a way to satisfy third equation of the system (the only equation not yet solved).

[13] Equivalently, we might have started by setting $f_5 := z^{1-t} f_3$; indeed it implies $f_4 = z^t f_2$.

[Step 1]. We focus on fourth (B), fifth (C) and sixth (A) equations of system 3.21. Replacing $f_2 f_2^*$ with $f_6 f_6^*$ (by third equation) and combining equations A and B, we can obtain an equation that only depends on f_1 and f_6. More precisely, the equation "$B - (1 + z^{1-2t})z^{t-1}A$" turns out to be

$$f_1^* f_1 - (z^{t-1} + z^{-t}) f_6^* f_1 - (z^t + z^{1-t}) f_1^* f_6 + (z^t + z^{1-t})(z^{t-1} + z^{-t}) f_6^* f_6 = 0.$$

This last equation is equivalent to

$$\Big(f_1 - (z^t + z^{1-t}) f_6\Big)\Big(f_1 - (z^t + z^{1-t}\Big)^* = 0.$$

Since the ring $\mathbb{F}_d[z^{\pm 1}]$ is an integral domain, last equation is satisfied by f_1 and f_6 if and only if we set

$$\boxed{f_1 := (z^t + z^{1-t}) f_6}.$$

The system consisting only of equations A, B ad C is equivalent to the system

$$\begin{cases} f_6^* f_1 + z f_1^* f_6 - (z^t + z^{1-t}) f_6^* f_6 = z^{1-t} f_2^* f_3 & (A) \\ B - (1 + z^{1-2t}) z^{t-1} A & \\ z^{1-t} f_2^* f_3 = z^t f_3^* f_2 & (C) \end{cases}$$

(one can check that combining equations of the second system one can get the equations of the first one). In this last system, second equation is satisfied by our definition of f_1. We now focus on equation A: we replace f_1 with the definition we just set:

$$(z^t + z^{1-t}) f_6^* f_6 + (z^{1-t} + z^{t-1}) f_6^* f_6 - (z^t + z^{1-t}) f_6^* f_6 = z^{1-t} f_2^* f_3.$$

Simplifying and replacing $f_6 f_6^*$ by $f_2 f_2^*$ (third equation of system 3.21), we get

$$(z^{1-t} + z^t) f_2^* f_2 = z^{1-t} f_2^* f_3.$$

Equivalently,

$$\Big((1 + z^{2t-1}) f_2 - f_3\Big) f_2^* = 0.$$

By assumption, f_2^* is non-zero and the ring of Laurent polynomial $\mathbb{F}_d[z^{\pm 1}]$ is an integral domain, therefore last equation is satisfied if and only if we set

$$\boxed{f_3 := (1 + z^{2t-1}) f_2}.$$

With such a definition of f_3, equation C is also verified, indeed replacing f_3 in it with the definition we just set, we get:

$$z^{1-t}(1 + z^{2t-1}) f_2^* f_2 = z^t (1 + z^{1-2t}) f_2^* f_2$$

which holds for every choice of $f_2 \in \mathbb{F}_d[z^{\pm 1}]$.

[Step 2]. Our new settings solve fourth, fifth and sixth equation of system 3.21; we now try to solve first, second and seventh equation of this system. Second equation becomes

$$(1 + z^{2t-1})(1 + z^{1-2t}) f_2^* f_2 = f_7^* f_6 + f_6^* f_7 + 4 f_6^* f_6$$

Which is equivalent to

$$z^{2t-1}(1-z^{1-2t})^2 f_2^* f_2 = f_7^* f_6 + f_6^* f_7. \tag{3.22}$$

Last equation of system 3.21 becomes

$$\begin{aligned}(z^{1-t}+z^t)(1+z^{2t-1})(1+z^{1-2t})f_2^* f_2 - 4(z^t+z^{1-t})f_2^* f_2 =& \\ = (z^{1-t}+z^t)f_7^* f_6 + z(z^{t-1}+z^{-t})f_6^* f_7.&\end{aligned}$$

Which is equivalent to

$$(z^{1-t}+z^t)\Big(z^{2t-1}(1-z^{1-2t})^2\Big)f_2^* f_2 = (z^{1-t}+z^t)(f_7^* f_6 + f_6^* f_7).$$

This last equation is a multiple of equation 3.22, thus we can ignore it. Therefore, by our computations and under our settings, the subsystem of 3.21 consisting of first, second and seventh equation turns out to be equivalent to

$$\begin{cases} f_7^* f_7 = 1 & (D) \\ z^{2t-1}(1-z^{1-2t})^2 f_6^* f_6 = f_7^* f_6 + f_6^* f_7 & (E). \end{cases} \tag{3.23}$$

We can notice that combining these two equations, we can get an equation such that, "moving" almost everything to the left side, the left side becomes factorizable: renaming with k the factor that multiplies of $f_6 f_6^*$ in second equation, the equation "$kE + D$" turns out to be

$$k^2 f_6 f_6^* - k f_6 f_7^* - k f_6^* f_7 + f_7 f_7^* = 1$$

and the left side factorizes into $(kf_6 - f_7)(kf_6^* - f_7^*)$. We focus on the coefficient k: the equality $k = k^*$ holds, indeed

$$k^* = z^{1-2t}(1-z^{2t-1})^2 = z^{1-2t}\Big(z^{2t-1}(z^{1-2t}-1)\Big)^2 = z^{2t-1}(1-z^{1-2t})^2 = k$$

Last system is equivalent to the system consisting of equations "$kE + D$" and "E", i.e. it is equivalent to

$$\begin{cases} k f_6^* f_6 = f_7^* f_6 + f_6^* f_7 & (E) \\ (kf_6 - f_7)(kf_6 - f_7)^* = 1 & (F) \end{cases}$$

Easiest Laurent polynomials $f \in \mathbb{F}_d[z^{\pm 1}]$ satisfying $ff^* = 1$ are all powers (with coefficients ± 1) of $z \in \mathbb{F}_d[z^{\pm 1}]$ with integer exponents; we therefore try to fix f_7 and f_6 such that $kf_6 - f_7 = \pm z^n$ holds for some $n \in \mathbb{Z}$ and this assures that equation "F" is satisfied. Here Passman's idea [11] gets in the game (deepening the search started by Murray [9]). Keeping in mind that $k = z^{2t-1}(1-z^{1-2t})^2$ holds (by definition) and that f_6 multiplies k, we set $w := z^{1-2t}$ and we do following computations in the field of fractions of the ring of Laurent polynomials $\mathbb{F}_d[z^{\pm 1}]$. Let $n \in \mathbb{N}$ be a non-zero natural number, then:

$$(1-w)^2 \frac{1-w^{nd}}{(1-w)^2} = 1 - w^{nd}$$

and

$$\begin{aligned}\frac{1-w^{nd}}{(1-w)^2} &= \frac{(1-w^d)(1+w^d+w^{2d}+\cdots+w^{(n-1)d})}{(1-w)^2}\\ &\overset{*}{=} \frac{(1-w)^d}{(1-w)^2}(1+w^d+w^{2d}+\cdots+w^{(n-1)d})\\ &= (1-w)^{d-2}(1+w^d+w^{2d}+\cdots+w^{(n-1)d}) \in \mathbb{F}_d[z^{\pm 1}]\end{aligned}$$

where in $*$ we used that d is the characteristic of the ring[14] we're working in. Therefore, we set

$$\boxed{f_6 := \frac{1-w^{nd}}{(1-w)^2}},$$

which belongs to $\mathbb{F}_d[z^{\pm 1}]$ thanks to last computations. Applying such a definition, we get that

$$\begin{aligned}kf_6 - f_7 &= w^{-1}(1-w)^2\frac{1-w^{nd}}{(1-w)^2} - f_7\\ &= w^{-1}(1-w^{nd}) - f_7 = w^{-1} - w^{nd-1} - f_7.\end{aligned}$$

Therefore, we set

$$\boxed{f_7 := w^{-1} = z^{2t-1}}$$

and this assures us that $kf_6 - f_7 = -w^{nd-1} = -z^{(1-2t)(nd-1)}$, as desired to have equation "F" satisfied. It remains to check that our definitions of f_6 and f_7 give a solution of equation "E". Replacing f_6 and f_7 with Laurent polynomials we assigned them, equation "E" becomes

$$w^{-1}(1-w)^2\frac{1-w^{nd}}{(1-w)^2}\frac{1-w^{-nd}}{(1-w^{-1})^2} = w\frac{1-w^{nd}}{(1-w)^2} + w^{-1}\frac{1-w^{-nd}}{(1-w^{-1})^2}.$$

We first simplify right side (applying computation rules of field of fractions of $\mathbb{F}_d[z^{\pm 1}]$):

$$\begin{aligned}w\frac{1-w^{nd}}{(1-w)^2} + w^{-1}\frac{1-w^{-nd}}{(1-w^{-1})^2} &= \frac{w}{w^2}\frac{1-w^{nd}}{(1-w^{-1})^2} + w^{-1}\frac{1-w^{-nd}}{(1-w^{-1})^2}\\ &= \frac{w^{-1}(1-w^{nd}+1-w^{-nd})}{(1-w^{-1})^2}\\ &= \frac{w^{-1}(1-w^{nd})(1-w^{-nd})}{(1-w^{-1})^2}\end{aligned}$$

and this is exactly the left side, as desired.

[Step 3]. It remains to solve equation $f_2 f_2^* = f_6 f_6^*$. If $f_2 = z^m f_6$, for any $s \in \mathbb{Z}$, then the equation is satisfied. Let $m \in \mathbb{Z}$, we can set

$$\boxed{f_2 := z^m f_6}.$$

[14] If $d \in \mathbb{N}$ is a prime characteristic of a ring R, for every $r \in R$ we have that $(1+r)^d = 1+r^d$. Thus, $(1-r)^d = 1+(-r)^d = 1-r^d$ holds, because

- if $d = 2$ then $(-r)^d = r^d = -r^d$ since R has characteristic $d = 2$;
- if $d \neq 2$ then d is odd (d being prime), hence $(-r)^d = -r^d$ holds.

Backsolving, choices we set for the seven polynomials $f_1, \dots, f_7$ becomes

$$\begin{aligned}
f_1 &:= (z^t + z^{1-t}) f_6 \\
f_2 &:= z^m f_6 \\
f_3 &:= z^m (1 + z^{2t-1}) f_6 \\
f_4 &:= z^{t+m} f_6 \\
f_5 &:= z^{m+1-t} (1 + z^{2t-1}) f_6 \\
f_6 &:= \frac{1 - z^{nd(1-2t)}}{(1 - z^{1-2t})^2} \\
f_7 &:= z^{2t-1}.
\end{aligned}$$

Next theorem summarizes what we discussed until now.

Theorem 3.3.9. *Let P be the Promislow group. Let $d \in \mathbb{N}$ be a prime number, let $t, m \in \mathbb{Z}$ and $n \in \mathbb{N}_{>0}$. Set*

$$\begin{aligned}
h &= (1 - z^{1-2t})^{d-2} (1 + z^{d(1-2t)} + z^{2d(1-2t)} + \dots + z^{(n-1)d(1-2t)}) \\
p &= (1 + x)(1 + y)(z^t + z^{1-t}) h \\
q &= z^m [(1 + x)(x^{-1} + y^{-1}) + (1 + y^{-1})(1 + z^{2t-1})] h \\
r &= z^m [(1 + y^{-1})(x + y) z^t + (1 + x)(z^t + z^{1-t})] h \\
s &= z^{2t-1} + (4 + x + x^{-1} + y + y^{-1}) h.
\end{aligned}$$

Then $p+qa+rb+sab$ is a non-trivial unit in the group ring $\mathbb{F}_d[P]$ (in particular, (p, q, r, s) satisfies system 3.12).

Proof. Let everything as in the statement. Our previous discussion is a proof of the fact that $p + qa + rb + sab$ is a unit and that (p, q, r, s) satisfies system 3.12. Eventually, this is a non-trivial unit by Lemma 3.2.12. □

Corollary 3.3.10. *Let P be the Promislow group and K be a field with finite characteristic. The group ring $K[P]$ doesn't satisfy the Kaplansky unit conjecture.*

Proof. Let P be the Promislow group and K be a field with finite characteristic; let p be its characteristic. The field K contains a subfield, named the *prime subfield*[15] isomorphic to the field with p elements $\mathbb{F}_p$, therefore $\mathbb{F}_p[P]$ is isomorphic to a subring of $K[P]$ (Remark 1.1.11). Since $\mathbb{F}_p[P]$ has non-trivial units (Theorem 3.3.9) and since isomorphisms of group rings preserve the cardinality of the supports (as proved in the proof of Corollary 3.3.2), we obtain that $K[P]$ has a subring that admits a non-trivial units. Eventually, since non-trivial units in a subring stay non-trivial units in the whole ring $K[P]$, we conclude that $K[P]$ doesn't satisfy the unit conjecture. □

Remark 3.3.11. One might ask if is it possible to and how recover from Theorem 3.3.9 the non-trivial units of $\mathbb{F}_2[P]$ and $\mathbb{F}_3[P]$ from which the argument to construct Theorem 3.3.9 arose (we're referring to Remark 3.3.8). The answer is that these units cannot be recovered directly from Theorem 3.3.9.

[15] See footnote 11 on page 63.

- The unit α of $\mathbb{F}_2[P]$ considered in Remark 3.3.8 can't be obtained directly from the theorem since it has $f_7 = 1$ but the units constructed in the theorem have $f_7 = z^{2t-1}$ for some $t \in \mathbb{Z}$. Anyway, let $\tilde{\alpha}$ be the unit given by the theorem associated to the parameters $t = m = n = 1$. Through a straightforward computation it's possible to check that

$$\alpha = z^{-1}\tilde{\alpha}$$

holds.

- The unit α of $\mathbb{F}_3[P]$ considered in Remark 3.3.8 can't be obtained directly from the theorem since it has $f_7 = -z$ but the units constructed in the theorem have $f_7 = z^{2t-1}$ for some $t \in \mathbb{Z}$. Anyway, let $\tilde{\alpha}$ be the unit given by the theorem associated to the parameters $t = n = 1$ and $m = 0$. Through a straightforward computation it's possible to check that

$$\alpha_1 = -\tilde{\alpha}_1, \qquad \alpha_a = \tilde{\alpha}_a, \qquad \alpha_b = \tilde{\alpha}_b, \qquad \alpha_{ab} = -\tilde{\alpha}_{ab}$$

hold.

We conclude that to recover the units considered in Remark 3.3.8 we need to change a bit our choices for the polynomials $f_1, \dots, f_7$: for the unit in $\mathbb{F}_2[P]$ we need to multiply all the Laurent polynomials $f_1, \dots, f_7$ for z^{-1}; for the unit in $\mathbb{F}_3[P]$ we need to replace f_1, f_6 and f_7 by their respective opposite. In both cases, we still get a solution of system 3.20, independently on the explicit form of the Laurent polynomials $f_1, \dots, f_7$. In other words, we need to enlarge the family A of units in Theorem 3.3.9 to the family of units

$$A \cup \{\, z^i\tilde{\alpha} \mid i \in \mathbb{Z}, \tilde{\alpha} \in A \,\} \cup \{\, -\tilde{\alpha}_1 + \tilde{\alpha}_a a + \tilde{\alpha}_b b + -\tilde{\alpha}_{ab} ab \mid \tilde{\alpha} \in A \,\}.$$

Remark 3.3.12. In Theorem 3.3.9. it is exhibited a triple family of non-trivial units of $\mathbb{F}_d[P]$, where P is the Promislow group and d is a prime number, where the family depends on parameters $t, m, n \in \mathbb{Z}$. However, by varying the parameter $m \in \mathbb{Z}$, we get new solutions that we were already able to construct. Precisely, suppose t and n fixed and let $p_0+q_0a+r_0b+s_0ab$ be the non-trivial unit constructed in the statement of Theorem 3.3.9 and associated to the parameters t, n and $m = 0$. If $p_m + q_m a + r_m b + s_m ab$ is the non-trivial unit constructed in the statement of Theorem 3.3.9 and associated to the parameters t, n and $m \in \mathbb{Z}$, then

$$p_m = p_0 \qquad q_m = z^m q_0 \qquad r_m = z^m r_0 \qquad s_m = s_0$$

hold. Therefore, the fact that, for every $m \in \mathbb{Z}$, $p_m + q_m a + r_m b + s_m ab$ is a non trivial unit can be deduced by the fact $p_0 + q_0 a + r_0 b + s_0 ab$ is a non-trivial unit, by Corollary 3.2.10.

Remark 3.3.13. Let everything as in the statement of Theorem 3.3.9. The truly interesting parameter definying the family of non-trivial units is n (the parameter introduced by Passman [11]), in the sense that varying the other parameters m and t the units we get are just transformations of other units in the family via maps that always send units into units. We anticipated this fact in previous remark for the parameter $m \in \mathbb{Z}$; we now generalize it to the pair of parameters $m, t \in \mathbb{Z}$. For every choice of parameters $m, t \in \mathbb{Z}$ consider the ring homomorphism $\sigma_{m-t,m} : K[P] \to K[P]$ defined in Lemma 3.2.7; it behaves as follows

$$\begin{aligned} \sigma_{m-t,m} : K[P] &\longrightarrow K[P] \\ a &\longmapsto z^{m-t}a \\ b &\longmapsto z^t b. \end{aligned}$$

Fix $n \in \mathbb{N} \smallsetminus \{0\}$. For every choice of the parameters $m, t \in \mathbb{Z}$ let

$$h_{m,t}, \qquad p_{m,t}, \qquad q_{m,t}, \qquad r_{m,t}, \qquad s_{m.t}$$

be the Laurent polynomials $h,\ p,\ q,\ r,\ s$ defined in Theorem 3.3.9 and associated to the parameters m, t, n. Set

$$\alpha_{m,t} := p_{m,t} + q_{m,t}a + r_{m,t}b + s_{m.t}ab$$

Then

$$\alpha_{m,t} = z^t \sigma_{m-t,m}(\alpha_{0,0}).$$

This equality can be computed looking at the explicit form of each Laurent polynomial involved, as defined in the statement of Theorem 3.3.9, and using that $\sigma_{m-t,m}$ fixes x and y and $\sigma_{m-t,m}(z) = z^{1-2t}$ (asserted in Lemma 3.2.7). The map $\sigma_{m-t,m}$ transforms units into units (it is a ring homomorphism) and the multiplication by any power of z also transforms units into units (any power of z is a unit and the product of units is still a unit), therefore we could have constructed the unit $\alpha_{m,t}$ only knowing that $\alpha_{0,0}$ is a unit.

Appendix A

Appendix

A.1 Free Modules

We first recall the definition of submodule generated by a subset (second part of this definition requires a proof and we leave it to the reader)

Definition A.1.1. Sub-module generated by a subset Let R be a commutative ring and M be an R-module. If $S \subseteq M$ is a non-empty subset, the sub-module of M generated by S is the smallest submodule of M that contains S. In particular, if S is empty, the submodule generated by S is the zero module; if S is non-empty, for every non-zero element x in the submodule generated by S, there exist $n \in \mathbb{N} \smallsetminus \{ 0 \}$, $r_1, \dots, r_n \in R$ and $x_1, \dots, x_n \in S$ such that

$$x = r_1 x_1 + \cdots + r_n x_n$$

holds.

Definition A.1.2. Let R be a commutative ring and M be an R-module. We say that M is *freely generated* by $S \subseteq M$ (equivalently, that S *freely generates* M or that S is a *free set of generators* for M) as an R-module if the submodule generated by S coincides with M and if for every $n \in \mathbb{N} \smallsetminus \{ 0 \}$ and for every choice of $x_1, \dots, x_n \in S$ pairwise distinct and $r_1, \dots, r_n \in R$, the equality

$$r_1 x_1 + \cdots + r_n x_n = 0_M$$

implies that at least one coefficient between $r_1, \dots, r_n$ is zero. We say that an R-module is free if it has a free set of generators.

Lemma A.1.3. *Let R be a commutative ring and M be an R-module freely generated by a subset $S \subseteq M$. If $x \in M$ is a non zero element, then there exists $n \in \mathbb{N} \smallsetminus \{ 0 \}$, $x_1, \dots, x_n \in S$ pairwise distinct and $r_1, \dots, r_n \in R$ such that*

$$x = r_1 x_1 + \cdots + r_n x_n$$

holds and the choice of $n, r_1, \dots, r_n, x_1, \dots, x_n$ is unique (up to reordering).

Proof (idea). First part of the statement follows by the definition of generating set. Uniqueness can be proved applying the definition of free set of generators. Suppose there exist $n, m \in \mathbb{N} \smallsetminus \{ 0 \}$, $r_1, \dots, r_n, s_1, \dots, s_m \in R$ and

$x_1, \ldots, x_n, y_1, \ldots, y_m \in S$ with $x_1, \ldots, x_n$ pairwise distinct and $y_1, \ldots, y_m$ pairwise distinct such that

$$r_1 x_1 + \cdots + r_n x_n = s_1 y_1 + \cdots + s_m y_m.$$

Without lost of generalities (up to adding elements with coefficient $0 \in R$ and up to reordering), we may assume that $m = n$ and that for every $1 \leq i \leq n$, $x_i = y_i$ holds. Applying iteratively the definition of free set of generators, we deduce that for every $1 \leq i \leq n$, $r_i = s_i$ holds. □

Proposition A.1.4 (Universal property of free modules)**.** *Let R be a commutative ring and M be an R-module freely generated by a non-empty subset $S \subseteq M$. For every module N and every map $\phi : S \to N$ there is a unique R-module morphism $\phi^* : M \to N$ extending ϕ.*

Proof. A reference for the proof is [2, Proposition 12.5] (the idea is to apply A.1.3 to prove the existence). □

Proposition A.1.5. *Let S be a set and R be a commutative ring. There exists an R-module $R^{(S)}$ such that S is a subset of $R^{(S)}$ and $R^{(S)}$ is freely generated by S. Such a module is unique up to a unique isomorphism, that is: if M and M' are R-modules freely generated by S, then there exists a unique R-module isomorphism $M \to M'$ such that its restriction to S behaves like the identity.*

Proof (idea). Existence. Let M be the set of all maps $S \to R$ whose support (i.e., the set of elements with non-zero image) is a finite set. R being a ring, we can endow M with a sum and a scalar product by element of M defining these operations component-wise. The set M together with these operations becomes an R-module. For every $x \in S$, we denote with $\delta_x \in M$ the map such that $\delta_x(x) = 1_R$ and for every $y \in S \setminus \{ x \}$, $\delta_x(y) = 0_R$. We set $\Delta := \{ \delta_x \mid x \in S \}$. It's possible to prove that Δ is a free set of generators for M.

Uniqueness. The proof of uniqueness of an algebraic set endowed with a universal property is standard. Let M and M' be R-modules freely generated by S. The canonical inclusions $S \hookrightarrow M$ and $S \hookrightarrow M'$ can be extended, respectively, by R-modules homomorphisms $\phi' : M' \to M$ and $\phi : M \to M'$ by the universal property and these extensions are unique. The compositions $\phi \circ \phi'$ and $\phi' \circ \phi$ have to coincide with the identities over, respectively, M' and M, as a consequence of *uniqueness* stated in the universal property. □

A.2 Rank of Finitely Generated Abelian Groups

Let G be an abelian group; in particular G is a $\mathbb{Z}$-module, thus we can construct the tensor product $G \otimes_{\mathbb{Z}} \mathbb{Q}$ in the category of $\mathbb{Z}$-modules. This tensor product can be endowed with a $\mathbb{Q}$-module structure, that is $G \otimes_{\mathbb{Z}} \mathbb{Q}$ can be seen an a $\mathbb{Q}$-vector space. If G is also finitely generated and S is a finite set of generators of G, then the subset $\{ s \otimes 1_{\mathbb{Q}} \mid s \in S \}$ of $G \otimes_{\mathbb{Z}} \mathbb{Q}$ generates $G \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$ vector space. Therefore, the dimension of $G \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$ vector space is finite and this motivates following definition.

Definition A.2.1. Let G be a finitely generated abelian group. The *rank* of G is the dimension of $G \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space and it's denoted with $\operatorname{rank}(G)$.

Lemma A.2.2. *Let $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$ be a short exact sequence of groups. Suppose that X is a finitely generated abelian group. Then the following equality holds*[1]*:*

$$\operatorname{rank}(Y) = \operatorname{rank}(X) + \operatorname{rank}(Z).$$

Proof. Let X, Y, Z as in the statement. The $\mathbb{Z}$-module $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, therefore the sequence

$$0 \longrightarrow X \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow Y \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow Z \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow 0$$

is exact in the category of $\mathbb{Z}$-modules; in particular, it is also exact in the category of $\mathbb{Q}$-vector spaces. A well-known result of linear algebra asserts that if $\phi : V \to W$ is a morphism of vector spaces over a field K, then

$$\dim_K(V) = \dim_K(\operatorname{Im}(\phi)) + \dim_K(\ker(\phi)).$$

Applying this formula to the short exact sequence above, we get that

$$\dim_{\mathbb{Q}}(Y \otimes_{\mathbb{Z}} \mathbb{Q}) = \dim_{\mathbb{Q}}(X \otimes_{\mathbb{Z}} \mathbb{Q}) + \dim_{\mathbb{Q}}(Z \otimes_{\mathbb{Z}} \mathbb{Q}),$$

as desired. □

A.3 Pushouts and Quotients of Groups

Lemma A.3.1. *Let $f : X \to Y$ be a morphism of groups and let N be a normal subgroup of X such that $f(N)$ is normal in Y. Then the following diagram is a pushout diagram in the cateogry of groups:*

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X/N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ Y & \xrightarrow{\pi'} & Y/f(N) \end{array}$$

where the arrow $X/N \to Y/f(N)$ is induced by the composition of $f : X \to Y$ with the projection $Y \to Y/f(N)$ (N belonging to the kernel of this composition).

Proof. Let everything as in the statement. We prove that the diagram verifies the universal property of pushouts. Let Z be a group and $k : Y \to Z$ and $h : X/N \to Z$ be group homomorphisms such that

$$k \circ f = h \circ \pi$$

holds. This implies that

$$k(f(N)) = h(\phi(N)) = \{ 1_Z \}.$$

This means that $f(N)$ is contained in the kernel of k, therefore there exists a unique group homomorphism $k' : Y/f(N) \to Z$ such that

$$k' \circ \pi' = k$$

[1]It makes sense to compute the rank of both X and Z, indeed: Z is a homomorphic image of Y, hence Z is a finitely generated abelian group; X is a subgroup of a finitely generated abelian group hence, by the fundamental theorem of finitely generated abelian groups applied to Y, the group X is finitely generated abelian.

It remains to check that $k' \circ f' = h$. The morphism π is an epimorphism (with respect to the categorical definition of epimorphism) because it is surjective (every surjective group homomorphism is always an epimorphism), it suffices to prove that $k' \circ f' \circ \pi = h \circ \pi$ holds; this can be easily verified, indeed

$$k' \circ f' \circ \pi = k' \circ \pi' \circ f = k \circ f = h \circ \pi,$$

as desired. $\square$

Let $i : N \to A$ and $j : N \to B$ be group monomorphisms; without lost of generaity we may assume that N is a subgroup of both A and B and that i and j are the canonical inclusions. Suppose that N is a normal subgroup of both A and B and set $P := A *_N B$ be the *amalgamated free product* of A and B over N, that is the following is a pushout diagram in the category of groups:

$$\begin{array}{ccc} N & \rightarrowtail & A \\ \downarrow & & \downarrow f \\ B & \xrightarrow{f'} & P \end{array}$$

Such a pushout diagram always exists and is unique up to canonical isomorphism ([7, Theorem 2.3.9]). Under this setting, we formulate the following lemma, whose proof can be seen as an exercise and can be developed in many different ways. For example, one can prove the second point of the lemma by directly verifying that the diagram satisfies the universal property of pushouts; however, in the proof we provide here we propose an alternative idea.

Lemma A.3.2. *Let N, A, B and P be groups as in last settings. Then*

1. *$f(N)$ is a normal subgroup of P;*
2. *the following diagram is a pushout diagram in the category of groups:*

$$\begin{array}{ccc} 1 & \longrightarrow & A/N \\ \downarrow & & \downarrow \\ B/N & \longrightarrow & P/f(N) \end{array}$$

where the group homomorphisms $A/N \to P/f(N)$ and $B/N \to P/f(N)$ have been induced by, respectively, the compositions $A \to P \to P/f(N)$ and $B \to P \to P/f(N)$ (since N belongs to the kernel of both of them).

Proof (idea). Let everything as in the statement. The fact that $f(N)$ is a normal subgroup of P can be proved through the explicit construction of the amalgamated free product P (for details, see the proof of [7, Theorem 2.3.9]). The group P is constructed as the presented group generated by the set $\{ x_g \mid g \in A \sqcup B \}$ and whose relations are those that arise from the group relations of A, those that arise from the group relations of B and those that constitute the set

$$\{ x_a = x_b \mid a \in A \cap N,\ b \in B \cap N,\ a = b \}.$$

To not overloading the notation, for every $g \in A \sqcup B$, we denote with x_g also the equivalence class of x_g in P. Under such a construction, the map $f : A \to P$ becomes

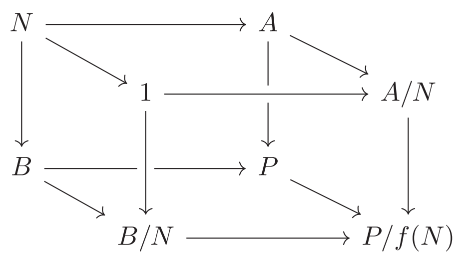
$$\begin{aligned} f : A &\longrightarrow P \\ a &\longmapsto x_a \end{aligned}$$

and f' is defined analogously (by the symmetry of the diagram). One can prove that for every $g \in A \sqcup B$, $(x_g)^{-1} = x_{g^{-1}}$ holds. Therefore, for every $a \in A$ and $b \in B$ we get

$$x_a f(N)(x_a)^{-1} = x_a f(N) x_{a^{-1}} = f(aNa^{-1}) = f(N),$$
$$x_b f(N)(b_a)^{-1} = x_b f'(N) x_{b^{-1}} = f'(bNb^{-1}) = f'(N) = f(N),$$

Since we proved that for every x in a generating set of P the equality $xf(N)x^{-1}$ holds, we deduce that $f(N)$ is a normal subgroup of P.

We now prove the second point. Consider the following diagram.



(A.1)

Every face of this diagram is commutative (easy to verify). Each square in the sub-diagram

$$\begin{array}{ccccc} N & \longrightarrow & A & \longrightarrow & A/N \\ \downarrow & & \downarrow & & \downarrow \\ B & \longrightarrow & P & \longrightarrow & P/f(N) \end{array}$$

is a pushout: the left square is a pushut by assumption, the right square is a pushout by Lemma A.3.1. Therefore the outer square is also a pushout. By the commutativity of the full diagram A.1, this implies that the outer square of the diagram

$$\begin{array}{ccccc} N & \longrightarrow & 1 & \longrightarrow & A/N \\ \downarrow & & \downarrow & & \downarrow \\ B & \longrightarrow & B/N & \longrightarrow & P/f(N) \end{array}$$

is a pushout diagram. The left square in this last diagram is also a pushout (by Lemma A.3.1) therefore, by a property of pushouts[2], we obtain that also the right square in last diagram is a pushout, as desired. □

[2] In a diagram composed by two squares with a common arrow, as the diagram represented above, if the outer square and the left square are both pushouts, then the right square is also a pushout.

A.4 Commutator Subgroup

Definition A.4.1. Let G be a group. Let $g, h \in G$, the *commutator* of g and h is defined as $[g, h] := ghg^{-1}h^{-1}$. The *commutator subgroup* of G, denoted with $[G, G]$, is the subgroup of G generated by all the commutators of elements of G.

Lemma A.4.2. *Let G be a group. The commutator subgroup of G is a normal subgroup of G and it is the smallest normal subgroup such that the quotient group of G over this subgroup is abelian.*

Proof. Let G be a group and $[G, G]$ be its commutator subgroup. First we prove that $[G, G]$ is a normal subgroup. The conjugation being a group homomorphism, it suffices to prove that the conjugate of every generator of $[G, G]$ by any element of G belongs to $[G, G]$. Let $x, y, z \in G$, then

$$\begin{aligned} x[y,z]x^{-1} &= xyzy^{-1}z^{-1}x^{-1} \\ &= (xyx^{-1})(xzx^{-1})(xy^{-1}x^{-1})(xz^{-1}x^{-1}) \\ &= (xyx^{-1})(xzx^{-1})(xyx^{-1})^{-1}(xzx^{-1})^{-1} \in [G,G]. \end{aligned}$$

Second we prove that the quotient group $G/[G, G]$ is abelian. Let $x, y \in G$, then $xyx^{-1}y^{-1}$ belongs to $[G, G]$. This means that the projection of $xyx^{-1}y^{-1}$ in $G/[G, G]$ is the identity element, that is the projections of xy and yx in $G/[G, G]$ coincide and this proves that the product in $G/[G, G]$ is commutative. We prove now the remaining part of the statement. Let N be a normal subgroup of G such that G/N is abelian; to conclude it suffices to prove that all the commutators of G belong to N, because the commutators of G generate $[G, G]$. Let $x, y \in G$. The projection of $[x, y] = xyx^{-1}y^{-1}$ in G/N is the identity element, since G/N is abelian. This means that $[x.y]$ belongs to N, as desired. □

A.5 The Infinite Dihedral Group

Definition A.5.1. The *infinite dihedral group* is defined as the group

$$D_\infty := \langle s, t \mid t^2, t^{-1}st = s^{-1} \rangle.$$

Remark A.5.2. The infinite dihedral group is isomorphic to the finitely presented group $\langle a, b \mid a^2, b^2 \rangle$. Possible isomorphisms, one the inverse of the other, between these groups behaves as follows

$$\begin{aligned} f : D_\infty = \langle s, t \mid t^2, t^{-1}st = s^{-1} \rangle &\longrightarrow \langle a, b \mid a^2, b^2 \rangle \\ t &\longmapsto a \\ s &\longmapsto ab \\ g : \langle a, b \mid a^2, b^2 \rangle &\longrightarrow D_\infty = \langle s, t \mid t^2, t^{-1}st = s^{-1} \rangle \\ a &\longmapsto t \\ b &\longmapsto ts. \end{aligned}$$

The existence of group homomorphisms that behaves in this way can be proved thanks to the universal property of finitely presented groups. Moreover, these group homomorphism are inverse to each other because their compositions behaves as the identity homomorphism when applied to the generators of the domain (thanks to the relations in the presentations of each group)

$$\begin{aligned} g(f(t)) &= g(a) = t \\ g(f(s)) &= g(ab) = g(a)g(b) = t^2 s = s \\ f(g(a)) &= f(t) = a \\ f(g(b)) &= f(ts) = a^2 b = b. \end{aligned}$$

Remark A.5.3. The finitely presented group $\langle a, b \mid a^2, b^2 \rangle$ is isomorphic to the free product $\mathbb{Z}/2 * \mathbb{Z}/2$ (the free product being unique up to isomorphism), that is the following diagram is a pushout diagram

$$\begin{array}{ccc} 1 & \longrightarrow & \mathbb{Z}/2 \\ \downarrow & \ulcorner & \downarrow \\ \mathbb{Z}/2 & \longrightarrow & \langle a, b \mid a^2, b^2 \rangle \end{array}$$

where the vertical and horizontal arrows $\mathbb{Z}/2 \to \langle a, b \mid a^2, b^2 \rangle$ send $[1] \in \mathbb{Z}/2$ to, respectively, a and b in $\langle a, b \mid a^2, b^2 \rangle$.

Lemma A.5.4. *The commutator subgroup of the infinite dihedral group $D_\infty = \langle s, t \mid t^2, t^{-1}st = s^{-1} \rangle$ is the subgroup generated by $s^2 \in D_\infty$. Moreover, the quotient $D_\infty/[D_\infty, D_\infty]$ is isomorphic to the finite abelian group $C_2 \times C_2$ of four elements, where C_2 denotes the group of order 2.*

Proof. Let $D_\infty = \langle s, t \mid t^2, t^{-1}st = s^{-1} \rangle$ be the infinite dihedral group. Let N be the subgroup of D_∞ generated by s^2; by Lemma A.4.2, to prove that N is the commutator subgroup of D_∞ it suffices to prove that N is the smallest normal subgroup such that the quotient of D_∞ by N is abelian. First, N is normal in D_∞. Indeed, the conjugate of the generator of N by any generator of D_∞ belongs to N, because

$$t^{-1}s^2t = (t^{-1}st)^2 = s^{-2} \in N,$$

and this is sufficient to prove that N is a normal subgroup. Second, let H be a normal subgroup of D_∞ such that D_∞/H is normal; we prove that N is a subgroup of H. To prove this, it suffices to prove that the element s^2 that generates N belongs to H. Let $\pi : D_\infty \to D_\infty/N$ be the canonical projection. Since D_∞/N is abelian we get

$$\pi(s)^{-1} = \pi(s^{-1}) = \pi(t^{-1}st) = \pi(s)$$

and this implies $\pi(s^2) = 1$, which means that s^2 belongs to N. Eventually, since D_∞/N is finitely generated (D_∞ being finitely generated) and abelian (by Lemma A.4.2), we deduce, by the classification theorem of finitely generated abelian groups, that D_∞/N is isomorphic to a product of cyclic groups. In detail, consider the projections of s and t in D_∞/N as generators of this quotient; these projections have order 2 thus every element in D_∞/N has order 2, this quotient being abelian. We can deduce that D_∞/N is isomorphic to a product of cyclic groups of order 2 but D_∞/N can't be cyclic of order 2 because its generators considered above are distinct. We can conclude that D_∞/N is isomorphic to a product of two cyclic groups of order 2. □

Bibliography

[1] Gerald H. Cliff. “Zero Divisors and Idempotents in Group Rings”. In: *Canadian Journal of Mathematics* 32.3 (1980), pp. 596–602.

[2] Alberto Facchini. *Introduction to Ring and Module Theory*. 6. ed. Padova: Libreria Progetto, Oct. 2020.

[3] Giles Gardam. “A counterexample to the unit conjecture for group rings”. In: *Annals of Mathematics* 194.3 (2021), pp. 967–979.

[4] Allen Hatcher. *Algebraic topology*. Cambridge: Cambridge University Press, 2002.

[5] Irving Kaplansky. ““Problems in the Theory of Rings” Revisited”. In: *The American Mathematical Monthly* 77.5 (1970), pp. 445–454.

[6] Irving Kaplansky. “Problems in the theory of rings”. In: *Report of a conference on linear algebras*. Ed. by A. A. Albert. National Academy of Sciences-National Research Council Publications 502. Washington: National Research Council, 1957, pp. v+60.

[7] Clara Löh. *Geometric Group Theory: An Introduction*. 1. ed. Universitext. Springer International Publishing, 2018.

[8] Bartosz Malman. *Zero-divisors and idempotents in group rings*. eng. Student Paper. 2014.

[9] Alan G. Murray. *More Counterexamples to the Unit Conjecture for Group Rings*. 2021. arXiv: `2106.02147 [math.RA]`.

[10] Donald S. Passman. *Infinite group rings*. Pure and applied mathematics. Marccel Dekker, New York, 1971.

[11] Donald S. Passman. *On the counterexamples to the unit conjecture for group rings*. 2021. arXiv: `2108.06570 [math.RA]`.

[12] Donald S. Passman. *The algebraic structure of group rings*. John Wiley & Sons, New York, 1977.

[13] Donald S. Passman. “What is a Group Ring?” In: *The American Mathematical Monthly* 83.3 (1976), pp. 173–176.

[14] S. David Promislow. “A Simple Example of a Torsion-Free, Non Unique Product Group”. In: *Bulletin of the London Mathematical Society* 20.4 (July 1988), pp. 302–304.

[15] Eliyahu Rips and Yoav Segev. “Torsion-free group without unique product property”. In: *Journal of Algebra* 108.1 (Jan. 1987), pp. 116–126.

[16] Andrzej Strojnowski. “A note on u.p. groups”. In: *Communications in Algebra* 8.3 (1980), pp. 231–234.

Ich habe die Arbeit selbständig verfasst, keine anderen als die angegebenen Quellen unf Hilfsmittel benutzt und bisher keiner anderen Prüfungsbehörde vorgelegt. Außerdem bestätige ich hiermit, dass die vorgelegten Druckexemplare und die vorgelegte elektronische Version der Arbeit identisch sind und dass ich von den in §26 Abs. 6 vorgesehenen Rechtsfolgen Kenntnis habe.

Unterschrift: