Explicit free groups in division rings

Gabriel de Arêa Leão Souza

Thesis presented to the
Institute of Mathematics and Statistics
of the University of São Paulo
in partial fulfillment
of the requirements
for the degree of
Master of Science

Program: Mathematics
Advisor: Prof. Dr. Jairo Zacarias Gonçalves

During the development of this work, the author has received financial support from CNPq – grant 131804/2023-5

São Paulo
December, 2023

Explicit free groups in division rings

Gabriel de Arêa Leão Souza

This version of the thesis includes the corrections and modifications suggested by the Examining Committee during the defense of the original version of the work, which took place on December 13, 2023.

A copy of the original version is available at the Institute of Mathematics and Statistics of the University of São Paulo.

Examining Committee:

Prof. Dr. Jairo Zacarias Gonçalves (advisor) – IME-USP
Prof. Dr. Arnaldo Mandel – IME-USP
Prof. Dr. Érica Zancanella Fornaroli – UEM

À minha família.

Agradecimentos

> *Mathematics, rightly viewed, possesses not only truth, but supreme beauty - a beauty cold and austere, like that of sculpture, [...] capable of a stern perfection such as only the greatest art can show.*
>
> — Bertrand Russell

Ao meu pai Rogério, por ser meu exemplo e por toda a ajuda nos momentos de insegurança, à minha mãe Sílvia, por todo o amor, por todo o carinho e por todo o incentivo à vida matemática, e especialmente ao meu irmão Guilherme, por tornar cada dia e cada descoberta ainda mais interessantes.

À Carol, por todo o amor, companhia e paciência ao longo destes mais de cinco anos, sem a qual eu certamente não teria chegado até aqui.

Aos meus avós, Ana Maria e Tertuliano Miguel, cujas carreiras matemáticas serviram de grande inspiração, juntamente aos muitos conselhos e histórias, e à minha avó Mírian, pelas muitas orações e desejos de sucesso.

Aos diversos professores que marcaram toda a minha trajetória, com especial destaque ao professor Carlos N. C. Oliveira, cujas aulas foram um marco no meu interesse pela matemática; ao professor Manuel Garcia, que por completo acidente foi responsável pelo meu interesse pela álgebra, ao professor Yoshiharu Kohayakawa, por ter me ajudado com diversas inseguranças, à professora Lucia Murakami, por toda a mentoria, ajuda e apoio quanto à minha trajetória e ao futuro, e ao professor Vitor Ferreira pela tremenda assistência, especialmente neste último ano.

Ao meu professor e orientador Jairo Zacarias Gonçalves, por todas as conversas, matemáticas ou não, por todo o carinho durante o meu processo de formação, e por uma orientação sem igual, e sem a qual este trabalho não existiria.

Por fim, aos meus amigos, com especiais agradecimentos a Gabriel Mazzante, Georges Kallás e Anna Drewanz, que sempre estiveram comigo nos momentos de maior dificuldade.

Resumo

Gabriel de Arêa Leão Souza. **Grupos livres explícitos em anéis com divisão**. Dissertação (Mestrado). Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2023.

Seja K um corpo. Obteremos condições para elementos da forma $\{1 + \alpha\mathbf{i}, 1 + \beta\mathbf{j}\}$ gerarem um grupo livre de posto 2 em uma álgebra de quatérnios sobre K, inclusive em característica 2, baseado em um artigo dos professores Jairo Gonçalves, Arnaldo Mandel e Mazi Shirvani [GMS99]. Estes resultados serão, então, utilizados para encontrar pares de elementos que gerem um grupo livre em diversas classes de anéis com divisão, como corpos totais de frações de domínios de Ore e anéis de séries de Malcev-Neumann. Com isso, procura-se responder parcialmente uma conjectura de Lichtman ([Lic77]), a respeito da existência de grupos livres não-abelianos no grupo multiplicativo de anéis com divisão não-comutativos.

Palavras-chave: grupos livres. anéis com divisão. quatérnios.

Abstract

Gabriel de Arêa Leão Souza. **Explicit free groups in division rings**. Thesis (Master's).
Institute of Mathematics and Statistics, University of São Paulo, São Paulo, 2023.

Let K be a field. We will obtain conditions for elements of the form $\{1 + \alpha\mathbf{i}, 1 + \beta\mathbf{j}\}$ to generate a free group of rank 2 in a quaternion algebra over K, including the case where the characteristic of the field K is 2, based on an article by Professors Jairo Gonçalves, Arnaldo Mandel and Mazi Shirvani [GMS99]. These results will then be applied to obtain pairs of elements that freely generate a free group in many other classes of division rings, such as total fields of fractions of Ore domains and Malcev-Neumann series rings. With these results, we plan to partially answer a conjecture by Lichtman ([Lic77]), regarding the existence of non-abelian free groups in the multiplicative group of non-commutative division rings.

Keywords: free groups. division rings. quaternions.

Symbols and Acronyms

PID	Principal ideal domain
f.g.	Finitely generated
Ring R	Associative ring R with unity 1
Ring homomorphism	Ring homomorphism preserving the unity
Domain R	Possibly noncommutative ring R with no zero divisors
Integral domain	Commutative domain
$\mathbb{N}$	Natural numbers (including 0)
$\mathbb{N}^{\dagger}$	Natural numbers without 0
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Integers, rationals, reals, complex numbers
$\mathbb{F}_q$	The unique (up to isomorphism) field of order q
$\cong$	Is isomorphic to
$\subset$	Inclusion
$\underset{\neq}{\subset}$	Strict inclusion
$\lhd$	Proper normal subgroup
$\unlhd$	Not-necessarily proper normal subgroup
$H \leq G$	H is a subgroup of G
$M_n(R)$	Ring of "$n \times n$" matrices over the ring R
$Gl_n(F)$	Multiplicative group of "$n \times n$" invertible matrices over the field F
$\mathfrak{U}(R)$	Group of units of the ring R
$R^{\dagger}$	$R \setminus \{0\}$
id_X	Identity function of the set X
$\mathscr{A}(X)$	Group of bijections of the set X
$\mathscr{F}(X, Y)$	Set of functions from X to Y
$[x, y]$	$= x^{-1}y^{-1}xy$
x^y	$= y^{-1}xy$
$\sqcup$	Disjoint union
$\partial p(x)$	Degree of the polynomial $p(x)$

Contents

Appendixes

Introduction

In 1927, extending a result previously established by J. Wedderburn in 1907, E. Artin proved the following theorem, which completely classifies semisimple (artinian) rings and is today known as the "Wedderburn-Artin Theorem" ([Art27]):

Theorem (Wedderburn-Artin)**.** *Let R be a semisimple ring. Then, there exists a natural number k and pairs (n_i, D_i), $i = 1, ..., k$, uniquely determined up to permutations, where the D_i are division rings and $n_i \in \mathbb{N}^\dagger$, such that*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

This result, due to its completeness, paved way to a whole method of studying non-commutative rings; namely, one could search for properties that allow for a regression to the semisimple case, and later try to lift the results thus obtained to the original ring (look, for instance, at the Jacobson radical theory, [Lam01]).

Simultaneously, the previous theorem sheds light onto the importance of studying the structure of division rings. These objects, even though they present some good properties derived from the equality $\mathfrak{U}(D) = D^\dagger$, have very particular difficulties, such as the fact that they don't have any non-trivial quotients.

Some of the main results on non-commutative division rings are evidence to some of the more pathological behavior they display. Theorems such as those of J. Wedderburn [Wed05], C. Stuth [Stu64] and I. Kaplansky [Kap51], as well as the famous result by H. Cartan [Car47], extended by R. Brauer [Bra49], and proven independently in almost trivial fashion by L. Hua [Hua49], known today as the "Brauer-Cartan-Hua Theorem", show us how relatively mild hypothesis over some subgroup of the multiplicative group of a non-commutative division ring necessarily imply its centrality or commutativity. This strongly suggests that the multiplicative group of a non-commutative division ring has a very "wild" structure, and doesn't generally display good properties such as chain conditions.

Some years later, in 1972, Belgian mathematician J. Tits proved the so-called "Tits Alternative" [Tit72], presented below:

Theorem (Tits Alternative)**.** *Let G be a f.g. subgroup of $Gl_n(F)$, where F is a field. Then, one of the following is true:*

- *Either G is a solvable-by-locally finite group;*
- *Or G contains a free group of rank 2;*

Soon after, the question appeared on whether the same would be true if the field F were replaced by a non-commutative division ring [SY74]. Even though he gave a negative answer to the conjecture when he found a division ring D and a multiplicative subgroup $G \leq D^*$ which is neither solvable-by-locally finite nor does it contain a free group of rank 2, A. Lichtman proposed the following conjecture ([Lic77]):

Conjecture. *If D is a non-commutative division ring, then $D^\dagger$ contains a free subgroup of rank* 2.

This conjecture has stood the test of time and is still open to this day, in spite of many special cases having been established, such as that in which D is finite-dimensional over its center [Gon84]. An important observation is that, even in this case, the proof used isn't constructive, due to its close proximity to the proof of the Tits Alternative. This opens yet another can of worms: *what are the generators* of the free group of rank 2, should it exist?

It is that question upon which we focus the bulk of our work, whose objective is to collect different results that explicitly obtain free pairs in division rings. We have structured it in 3 chapters. The first discusses the required group-theoretic preliminaries, such as central series and ordered groups. The second discusses some classes of rings which allow us to construct the studied division rings. And the last one is where the actual free groups are obtained by using results previously established in the other two chapters. We have also included a couple small appendices, versing on variants of the main conjecture.

Chapter 1

Group-theoretic preliminaries

When it comes to choosing the starting-point of a dissertation, there are many possibilities. For what follows, we have opted for assuming only the contents of an undergraduate degree in mathematics and the corresponding courses in group, ring and Galois theories. Other than that, most concepts will be defined and constructed as needed.

We should emphasize that we have no intent of being encyclopedic - indeed, the theorems, lemmas, corollaries, definitions and so on will always be presented with a goal in mind, which are the main results of the third chapter. Thus, we will sometimes omit important results, whose proofs are not out of reach. When deemed convenient, we will briefly mention such results, but without necessarily providing a proof.

1.1 Free groups

We begin with one of the fundamental notions to be used throughout: that of a free group. Roughly speaking, free groups are those groups which do not satisfy any algebraic relations between their elements besides those imposed by the three axioms which define a group. Loosely following the exposition of J. Rotman [Rot99], we begin with the ensuing definition:

Definition. A group F is said to be **free of basis** $X \subset F$ if, for every group H and for every function $f : X \longrightarrow H$, there exists a unique group homomorphism $\varphi : F \longrightarrow H$ such that $\varphi|_X = f$. If $|X| < \infty$, $|X|$ is said to be the **rank** of F. Otherwise, F is said to be **of infinite rank**.

One can (rightfully) wonder the validity of using the definite article when talking about the rank of a free group. We settle this issue in what follows.

Proposition 1.1.1. *The rank of a free group is unique.*

Proof. Suppose F is a free group of basis X. For every function $f : X \longrightarrow \mathbb{Z}_2$, the definition of a free group yields a unique group homomorphism $\varphi_f : F \longrightarrow \mathbb{Z}_2$ which restricts to f on X. At the same time, any homomorphism $\varphi : F \longrightarrow \mathbb{Z}_2$ defines a function $\varphi|_X : X \longrightarrow \mathbb{Z}_2$.

This allows us to construct a one-to-one correspondence between functions from X to $\mathbb{Z}_2$ and homomorphisms from F to $\mathbb{Z}_2$. Indeed, if $\text{Hom}(F, \mathbb{Z}_2)$ denotes the set of group homomorphisms from F to $\mathbb{Z}_2$, we define

$$\begin{aligned} \Phi\colon \text{Hom}(F, \mathbb{Z}_2) &\longrightarrow \mathscr{F}(X, \mathbb{Z}_2) \qquad & \Psi\colon \mathscr{F}(X, \mathbb{Z}_2) &\longrightarrow \text{Hom}(F, \mathbb{Z}_2) \\ \varphi &\longmapsto \varphi|_X & f &\longmapsto \varphi_f \end{aligned}$$

It's straightforward to see that Φ and Ψ are mutual inverses, meaning there are exactly $2^{|X|}$ homomorphisms from F to $\mathbb{Z}_2$. If F is also free of basis Y, then the same reasoning yields $2^{|Y|}$ homomorphisms and, since this number should only depend on F itself, $|X| = |Y|$. ■

Proposition 1.1.2. [1] *Let X be a non-empty set. Then, there exists (up to isomorphism) a unique free group of basis Y, with $|Y| = |X|$.*

Proof. Existence: Consider a set X^{-1} with the same cardinality of X, such that $X \cap X^{-1} = \emptyset$ and, given a bijection $f : X \longrightarrow X^{-1}$, write $f(x) =: x^{-1}$. Let, then, $\mathcal{X} = X \cup X^{-1} \cup \{1\}$ and define

$$\mathcal{P}(X) = \left\{ (a_i) \in \prod_{i \in \mathbb{N}} \mathcal{X} \mid \exists N \in \mathbb{N} \text{ such that } a_i = 1, \forall i > N \right\}$$

called the *set of words* in X. If $(a_i) \in \mathcal{P}(X)$ and $a_i = 1$ for all i bigger than some N, we denote $(a_i) = (a_0, a_1, ..., a_N)$. The word $(1, 1, 1, ...)$ is called the *empty word*, and will be denoted by 1.

A word (a_i) is said to be *reduced* if it's empty or if it satisfies the following condition: "if $N \in \mathbb{N}$ is the biggest natural number such that $a_N \neq 1$, then $a_i \neq 1$ for all $i \leq N$ and, for all $x \in X$, x and x^{-1} aren't adjacent in (a_i)".

Now let F be the set of reduced words in X and, for each $x \in X$, define the maps $|x| : F \longrightarrow F$ and $|x^{-1}| : F \longrightarrow F$ as follows:[2]

$$|x^\varepsilon|((a_i)) = \begin{cases} (x^\varepsilon, a_0, a_1, ...) & \text{if } a_0 \neq x^{-\varepsilon} \\ (a_1, a_2, ...) & \text{if } a_0 = x^{-\varepsilon} \end{cases}, \varepsilon = \pm 1$$

They are trivially well-defined and both are bijections for all $x \in X$, since $|x| \circ |x^{-1}| = |x^{-1}| \circ |x| = \text{id}_F$.

Thus, consider the subset $[X] = \{|x| \mid x \in X\} \subset \mathscr{A}(F)$ and the group it generates, $\mathscr{F}$. If $g \in \mathscr{F}$, then $g = |x_1^{\varepsilon_1}| \circ \cdots \circ |x_n^{\varepsilon_n}|$ where $n \in \mathbb{N}$ and $\varepsilon_i = \pm 1, \forall i$, such that $|x|$ and $|x^{-1}|$ are never adjacent. We also refer to this description of g as a reduced word in the $|x_i^{\varepsilon_i}|$. This factorization is unique: $g(1) = (x_1^{\varepsilon_1}, ..., x_n^{\varepsilon_n})$ meaning, if $g = |x_1'^{\delta_1}| \circ \cdots \circ |x_m'^{\delta_m}|$ is another reduced expression for g, $(x_1^{\varepsilon_1}, ..., x_n^{\varepsilon_n}) = (x_1'^{\delta_1}, ..., x_m'^{\delta_m})$. Ergo, $n = 0$ forces $m = 0$ and, if $n \neq 0$, we obtain $n = m$ and $x_i^{\varepsilon_i} = x_i'^{\delta_i}$.

Let G be an arbitrary group and let $f : [X] \longrightarrow G$ be a function. Due to the uniqueness

[1] For what follows, it will always be implicit that $\varepsilon_i = \pm 1$, unless written otherwise.

[2] The set F is a free group of basis X with juxtaposition as its operation, but verifying associativity is not trivial.

of the previous factorization, the function $\varphi : \mathscr{F} \longrightarrow G$ defined by

$$\varphi(|x_1^{\varepsilon_1}| \circ \cdots \circ |x_n^{\varepsilon_n}|) = f(|x_1|)^{\varepsilon_1} \cdots f(|x_n|)^{\varepsilon_n}$$

is well-defined. If $w, v \in \mathscr{F}$, we write $w = |x_1^{\varepsilon_1}| \circ \cdots \circ |x_n^{\varepsilon_n}|$ and $v = |x_1'^{\delta_1}| \circ \cdots \circ |x_m'^{\delta_m}|$ as reduced words. There are two possibilities:

1. $|x_n^{\varepsilon_n}| \neq |x_1'^{-\delta_1}|$. In this case, $w \circ v = |x_1^{\varepsilon_1}| \circ \cdots \circ |x_n^{\varepsilon_n}| \circ |x_1'^{\delta_1}| \circ \cdots \circ |x_m'^{\delta_m}|$ is reduced, hence it's trivial that $\varphi(w \circ v) = \varphi(w)\varphi(v)$.

2. $|x_n^{\varepsilon_n}| = |x_1'^{-\delta_1}|$. Take $j = \max\{k \in \mathbb{N}^\dagger \mid |x_{n-k+1}^{\varepsilon_{n-k+1}}| = |x_k'^{-\delta_k}|\}$. We can write $w \circ v = |x_1^{\varepsilon_1}| \circ \cdots \circ |x_{n-j}^{\varepsilon_{n-j}}| \circ |x_{j+1}'^{\delta_{j+1}}| \circ \cdots \circ |x_m'^{\delta_m}|$ as a reduced word. Notice that

$$\begin{aligned}\varphi(w \circ v) &= f(|x_1|)^{\varepsilon_1} \cdots f(|x_{n-j}|)^{\varepsilon_{n-j}} f(|x_{j+1}'|)^{\delta_{j+1}} \cdots f(|x_m'|)^{\delta_m} \\ &= f(|x_1|)^{\varepsilon_1} \cdots f(|x_{n-j}|)^{\varepsilon_{n-j}} \left(f(|x_{n-j+1}|)^{\varepsilon_{n-j+1}} f(|x_{n-j+1}|)^{-\varepsilon_{n-j+1}}\right) f(|x_{j+1}'|)^{\delta_{j+1}} \cdots f(|x_m'|)^{\delta_m} \\ &= f(|x_1|)^{\varepsilon_1} \cdots f(|x_{n-j}|)^{\varepsilon_{n-j}} f(|x_{n-j+1}|)^{\varepsilon_{n-j+1}} f(|x_j'|)^{\delta_j} f(|x_{j+1}'|)^{\delta_{j+1}} \cdots f(|x_m'|)^{\delta_m}\end{aligned}$$

   by the definition of j. We proceed inductively to obtain $\varphi(w \circ v) = \varphi(w)\varphi(v)$.

Therefore, φ is a group homomorphism and, by definition, $\mathscr{F}$ is a free group of basis $[X]$. Since $x \longmapsto |x|$ is a bijection from X to $[X]$, existence is established.

Uniqueness: Let X and Y be non-empty sets, F free of basis X, G free of basis Y and $f : X \longrightarrow Y$ a bijection. Composing f with the standard inclusion map, we get a function $\tilde{f} : X \longrightarrow G$, such that there is a unique homomorphism $\varphi : F \longrightarrow G$ extending it. Doing the same to the function $f^{-1} : Y \longrightarrow X$, we obtain a homomorphism $\psi : G \longrightarrow F$.

Notice, then, that $\varphi \circ \psi : G \longrightarrow G$ is a group homomorphism such that $(\varphi \circ \psi)(y) = \varphi(f^{-1}(y)) = f(f^{-1}(y)) = y$, if $y \in Y$. Since $\mathrm{id}_G : G \longrightarrow G$ is another group homomorphism such that $\mathrm{id}_G|_Y = \mathrm{id}_Y$, we get, using uniqueness, that $\varphi \circ \psi = \mathrm{id}_G$. Analogously, $\psi \circ \varphi = \mathrm{id}_F$ and $F \cong G$. ■

Corollary 1.1.2.1. *Let G be an arbitrary group. Then, there exists a free group F and a surjective homomorphism $\psi : F \longrightarrow G$. In particular, $G \cong F/N$ for some $N \trianglelefteq F$.*

Proof. Let $X = G$. By Proposition 1.1.2, there exists a free group F of basis Y, with a bijection $f : Y \longrightarrow X$. By definition, there is a group homomorphism $\psi : F \longrightarrow X = G$ such that $\psi|_Y = f$. Since f is surjective, the same is true of ψ. ■

This corollary allows us to make the following construction:

Definition. Let G be a group and write $G \cong F/N$, where F is free of basis X and $N \trianglelefteq F$. Let R be a set of generators for N as a normal subgroup. Then, we write $G = \langle X \mid R \rangle$, which is called a **presentation** of G.

This way of expressing a group G as a quotient of a free group is really helpful, since it really facilitates defining homomorphisms with domain G.[3]

[3] This follows from the definition of a free group and from the First Isomorphism Theorem.

While the proof of Proposition 1.1.2 is very technical, it has one major advantage in that it gives us a way of expressing the elements of a free group in terms of the basis. This will be of major importance in what comes; so much so that we make it into the two following corollaries, which will be used without reference for the remainder of our work.

Corollary 1.1.2.2. *Let F be a group generated by $X \neq \emptyset$. Then, F is free of basis X if, and only if, every element of F can be uniquely written as a reduced word in X.*

Proof. We saw the "only if" part in the construction of a free group - indeed, every element of $\mathscr{F}$ had a unique expression as a reduced word in $[X]$. On the other hand, if every element of F can be uniquely written as a reduced word in X, the extension φ obtained in Proposition 1.1.2 remains well-defined, and the proof can be continued unchanged, proving the freedom of F. ■

Definition. The **length** of a reduced word $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ in a free group F is $l(w) = n$. By definition, $l(1) = 0$.

Corollary 1.1.2.3. *Let F be a group generated by $X \neq \emptyset$. Then, F is free of basis X if, and only if, every reduced word of length greater than* 0 *is different from the identity.*

Proof. The first part is trivial using the previous corollary. For the other implication, suppose an element can be written in more than one way as a reduced word; that is, suppose $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = y_1^{\delta_1} \cdots y_m^{\delta_m}$, where $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ and $y_1^{\delta_1} \cdots y_m^{\delta_m}$ are reduced.

Then, we obtain $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_m^{-\delta_m} \cdots y_1^{-\delta_1} = 1$. By hypothesis, the word on the left can't be reduced, and it's easy to see that $m = n$ and $y_i^{\delta_i} = x_i^{\varepsilon_i}$ (if any of these equalities failed, we could cancel out as much as possible and get a non-trivial reduced word equal to the empty word). ■

One important observation is that free groups can be lifted through homomorphisms; this will become extremely relevant in Chapter 3.

Proposition 1.1.3. *Let G and H be groups and let $\theta : G \longrightarrow H$ be a homomorphism. Suppose $g_1, g_2 \in G$ are such that $\theta(g_1), \theta(g_2)$ freely generate a free group (that is, the group they generate is free of basis $X = \{\theta(g_1), \theta(g_2)\}$). Then, g_1, g_2 freely generate a free group in G.*

Proof. Let $w_1 \cdots w_n = 1$ be a reduced word in G, with $w_i \in \{g_1, g_2, g_1^{-1}, g_2^{-1}\}, \forall i$. Then, $\theta(w_1) \cdots \theta(w_n) = 1$. By hypothesis, this implies $n = 0$. ■

Let F be a free group of basis X, where $|X| = n$. If $Y \subsetneq X$, it's clear, by the characterizations obtained before, that the subgroup of F generated by Y is free of basis Y. This means any free group of rank n contains free groups of any rank less than n as subgroups. Surprisingly, the converse is also true, as we prove below.

Proposition 1.1.4. *Let F be a free group of rank* 2*. Then, F contains a free subgroup of (countably) infinite rank.*

Proof. Let $X = \{x, y\}$ be a basis for F, consider the set $Y = \{y^{-1}xy, y^{-2}xy^2, \ldots\}$ and let H be the subgroup of F generated by Y. Let $w = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ be a reduced word with $a_i \in Y$. Using induction, we will show that, when w is written as a reduced word in X, it ends in $x^{\varepsilon_n}y^m$, with $a_n = y^{-m}x^{\varepsilon_n}y^m$. If $n = 1$, $w = a_1^{\varepsilon_1} = y^{-m}x^{\varepsilon_1}y^m$.

Suppose that the result is true for $l(w) = n - 1$ and let $w = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ be reduced in Y. Ergo, $w = w'a_n^{\varepsilon_n}$, with w' reduced in Y, with length $n - 1$. Moreover, w' is such that $w' = zx^{\varepsilon_{n-1}}y^m$, with $a_{n-1} = y^{-m}x^{\varepsilon_{n-1}}y^m$, when reduced in X, by the induction hypothesis (in particular, z is a reduced word in X which does not end in $x^{-\varepsilon_{n-1}}$).

$w = zx^{\varepsilon_{n-1}}y^m a_n^{\varepsilon_n}$. There are two possibilities for a_n:

- $a_n = y^{-m}xy^m$. This means $w = zx^{\varepsilon_{n-1}}x^{\varepsilon_n}y^m$. As w is reduced in Y, $\varepsilon_n \neq -\varepsilon_{n-1}$, and so the preceding expression is reduced in X.

- $a_n = y^{-k}xy^k$, $k \neq m$. This means $w = zx^{\varepsilon_{n-1}}y^{m-k}x^{\varepsilon_n}y^k$ as a reduced word in X.

In any case, we establish the induction result and, as a consequence, $w \neq 1$ when reduced in X. Thus, H is free of basis Y. ■

Before moving on to the next section, it is worth noting the following result, known as the “Nielsen-Schreier Theorem”, which establishes the fact that every subgroup of a free group is itself free. There exists an algebraic proof not too distant from the contents here exposed, which can be found in [BC68], but to show it would be to wander away from the goals of our work.

We also take this opportunity to note that many results on free groups, including the Nielsen-Schreier Theorem below, can be proven using geometry and algebraic topology. For a sample of how this can be done, we refer the reader to [Rot99].

Theorem (Nielsen-Schreier). *Let H be a subgroup of a free group F. Then, H is free of basis Y, for some subset $Y \subset F$. Furthermore, if F has rank r and H has index n in F, then H has rank $n(r - 1) + 1$.*

1.2 Free products

Similarly to how free groups capture the notion of “independence” between its basis elements, free products are a way to obtain new groups from some that were previously given, in such a way that elements from distinct factors are “independent” in the resulting group. As was done before, we begin with a fairly abstract definition.

Definition. Let A_i, $i \in I$ be groups. A **free product** of the A_i is a group P and a family of homomorphisms $\iota_j : A_j \longrightarrow P$ such that, given any group G and any family of homomorphisms $f_j : A_j \longrightarrow G$, there exists a unique group homomorphism $\varphi : P \longrightarrow G$ such that $\varphi \circ \iota_j = f_j$ for all j.

It’s worth pointing out, for readers with a background in category theory, that just as the definition of a free group was that of a free object in the category of groups, the free product is just the coproduct in the same category.

For what follows, we'll study free products in a similar manner to what was done for free groups. In so doing, we'll constantly alternate between the expositions in [Rot99], [MKS75] and [LS01].

Proposition 1.2.1. *Given a free product (P, ι_i) of the groups A_i, the functions $\iota_j : A_j \longrightarrow P$ are injections.*

Proof. Just consider the group $G = A_j$ and the family of homomorphisms $f_j = \mathrm{id}_{A_j}$. Thus, $\varphi : P \longrightarrow A_j$ is such that $\varphi \circ \iota_j = \mathrm{id}_{A_j}$. As ι_j has a left inverse, it's an injection. ■

Proposition 1.2.2. *Let $\{A_i \mid i \in I\}$ be groups. Then there exists a unique (up to isomorphism) free product of the A_i.*

Proof. Existence: Write $A_i = \langle X_i \mid R_i \rangle$, where the X_i and R_i are each pairwise disjoint. Define $P = \langle \bigcup X_i \mid \bigcup R_i \rangle$. If F_i is a free group of basis X_i, and F, a free group of basis $\bigcup X_i$, we have the following:

$$\begin{tikzcd}
F_i & & P \\
X_i \arrow[u, hook] \arrow[r, hook] \arrow[urr, dotted] & \bigcup_{i\in I} X_i \arrow[r, hook] & F \arrow[u, hook]
\end{tikzcd}$$

Thus, for each i, there exists a homomorphism $\varphi_i : F_i \longrightarrow P$. But also note, using the diagram, that $R_i \subset \ker \varphi_i$. Therefore, there is an induced homomorphism $\iota_i : A_i \longrightarrow P$.

Let $f_j : A_j \longrightarrow G$ be a family of homomorphisms, where G is an arbitrary group. By considering the projections $\pi_j : F_j \longrightarrow A_j$, the f_j induce functions $(f_j \circ \pi_j) \mid_{X_j} : X_j \longrightarrow G$. As the X_j are pairwise disjoint, this in turn induces $f : \bigcup X_j \longrightarrow G$ such that $f \mid_{X_j} = (f_j \circ \pi_j) \mid_{X_j}$. Therefore, there exists a unique homomorphism $\Phi : F \longrightarrow G$ which restricts to f. In particular, $\Phi \mid_{X_j} = (f_j \circ \pi_j) \mid_{X_j}, \forall j$.

There are also unique homomorphisms $\phi_j : F_j \longrightarrow G$ extending $(f_j \circ \pi_j) \mid_{X_j}$. Looking at F_j as a subset of F, it is clear that $\Phi \mid_{F_j} = \phi_j$. Moreover, it is evident that, since $\ker \pi_j = \langle R_j \rangle$, then $R_j \subset \ker \phi_j$. Ergo, $R_j \subset \ker \Phi, \forall j$ and the universal property of the quotient gives us a unique homomorphism induced by Φ from P to G. The uniqueness of all the constructed objects finishes the proof.

Uniqueness: Let P_1, P_2 be two free products of the groups A_i. Consider the following diagram:

$$\begin{tikzcd}
P_1 \\
A_j \arrow[u, hook, "\iota_j^1"] \arrow[r, hook, "\iota_j^2"] & P_2
\end{tikzcd}$$

By definition, there are unique homomorphisms $\phi : P_1 \longrightarrow P_2$ and $\psi : P_2 \longrightarrow P_1$ which restrict to ι_j^1 and ι_j^2, respectively. Then, an argument similar to that of Proposition 1.1.2 proves they are both isomorphisms. ■

We will denote the free product of A_j, $j \in J$ by $\mathop{\ast}_{j\in J} A_j$. Similarly to what we did for free groups, it will be convenient to describe an arbitrary element of a free product. This is done next, loosely following the exposition of [LS01, Theorem IV.1.2] and [MKS75, Corollary 4.1.1]. Beforehand, though, we remark that a free group of basis X has presentation $F = \langle X \mid \rangle$. Hence, the free product of free groups F_i of basis X_i is a free group of basis $\bigcup X_i$.

Definition. Let P be a group containing $A_j, \forall j \in J$. A sequence $g_1 \cdots g_n \in P$, $n \in \mathbb{N}$ is said to be **reduced** in the A_j if either $n = 0$, or the following is true: "each $g_i \neq 1$ belongs to one of the A_j, such that no two elements of the same A_j are ever adjacent".

Proposition 1.2.3 (Normal form). *For a group G generated by subgroups $A_j \subset G$, where $A_i \cap A_j = 1$ if $i \neq j$, the following are equivalent:*

i) $G \cong \mathop{\ast}_{j\in J} A_j$;

ii) Every element of G can be uniquely written as a reduced sequence in the A_j;

iii) Every non-empty reduced sequence in the A_j is different from the identity;

Proof. Up to some small adaptations, the proof of the first two implications is identical to that of Proposition 1.1.2 and its subsequent corollaries. Now let $A_j = \left\langle X_j \mid R_j \right\rangle$. We may view the X_j as being subsets of A_j. If F_j is a free group of basis X_j, for each j, we know F_j projects onto A_j, with the kernel being the normal subgroup generated by R_j (we call this the **normal closure** of R_j in F_j). Hence, we obtain a group homomorphism $\varphi_j : F_j \longrightarrow G$ with $R_j \subset \ker \varphi_j$.

At the same time, if F is the free group of basis $X = \bigcup X_j$, then it's the free product of the F_j. This yields a group homomorphism $\psi : F \longrightarrow G$ which restricts to φ_j on each F_j. In particular, its kernel contains the union $\bigcup R_j$. This shows that there is a group homomorphism $\Psi : \mathop{\ast}_{j\in J} A_j \longrightarrow G$. Moreover, since the X_j generate G, both ψ and Ψ are surjective.

Suppose $g_1 \cdots g_m \in \ker \Psi$, where $g_1 \cdots g_m$ is reduced (we know every element of the free product can be uniquely written in this form, from the first implication). We claim $g_1 \cdots g_m$ is in the normal closure of R in F, where $R = \bigcup R_j$. We prove this by induction on m, with the base case ($m = 1$) being trivial, since, in that case, $\varphi_1(g_1) = 1$, meaning g_1 is in the normal closure of $R_1 = R$.

For the inductive step, $\Psi(g_1 \cdots g_m) = 1$ means $\varphi_{j_1}(g_1) \cdots \varphi_{j_n}(g_n) = 1$, where $g_i \in A_{j_i}$. The image of φ_j is A_j, from the definition, which means, by hypothesis, the sequence above can't be reduced. The only way this can happen (since $A_i \cap A_j = 1$ if $i \neq j$) is if $\varphi_{j_i}(g_i) = 1$ for some i, meaning g_i is in the normal closure of R_{j_i} in F_{j_i}. Then, one of two things may happen:

- $j_{i-1} \neq j_{i+1}$. In this case, $g_1 \cdots g_{i-1} g_{i+1} \cdots g_m$ is reduced and in the kernel of Ψ. By the induction hypothesis, $g_1 \cdots g_{i-1} g_{i+1} \cdots g_m$ is in the normal closure of R in F. Thus, $g_{i+1}^{-1} \cdots g_m^{-1} g_1 \cdots g_{i-1}$ is in that same subgroup. Since $R_j \subset R$, $g_{i+1}^{-1} \cdots g_m^{-1} g_1 \cdots g_{i-1} g_i$ is also in the normal closure of R and thus, the same is true for $g_1 \cdots g_m$.

- $j_{i-1} = j_{i+1}$. Now, if $g_{i-1} \neq g_{i+1}^{-1}$, then $g_1 \cdots (g_{i-1}g_{i+1}) \cdots g_m$ is reduced an the preceding case applies. Otherwise, $g_{i-1}g_ig_{i-1}^{-1}$ is in the normal closure of R in F. Looking at the sequence $g_1 \cdots g_{i-2}g_{i+2} \cdots g_m$, we may repeat the process. If, at any point, $g_{i-k} \neq g_{i+k}^{-1}$, we may apply induction as before. Otherwise, the original sequence was of the form wg_iw^{-1}, which is in the normal closure of R in F.

Thus, in any case, the element $g_1 \cdots g_m$ is in the normal closure of R in F, showing this contains the kernel of Ψ. The reverse inclusion was already established, implying Ψ is injective, by Proposition 1.2.2, and thus finishing the proof. ■

In general, just as with free groups, identifying whether two (or more) subgroups have any relations between them is not an easy task. The following result gives us a pivotal tool in this regard, which will be our main way of proving many of the theorems of Chapter 3.

Theorem 1.2.4 (Ping-Pong Lemma). *Let G be a group generated by two non-trivial subgroups H and K, with $|H| > 2$, and suppose G acts on a non-empty set X. Denoting $H^\dagger = H \setminus \{1\}$ (the same for K), suppose there are two non-empty subsets $P \neq Q$ of X such that $PH^\dagger \subset Q$ and $QK^\dagger \subset P$. Then, $G \cong H * K$.*

Proof. Consider a non-trivial reduced sequence $w = w_1w_2 \cdots w_n$ in G (that is, the w_i alternate between H and K), and suppose $w = 1$.

If w_1 and w_n are both in K, we can conjugate by a non-identity element of H and obtain a relation of the same form that both begins and ends in H. If $w_1 \in H$ and $w_n \in K$, then, as $|H| > 2$, we can pick an element $x \in H$ different from w_1^{-1} and, therefore, xwx^{-1} begins and ends in H. The same argument deals with the case in which $w_1 \in K$ and $w_n \in H$.

Thus, we can assume, without losing generality, that both w_1 and w_n are in H. Using an inductive argument and the hypotheses, it's easy to show that $Pw \subset Q$. If $y \in K$, ywy^{-1} begins and ends in K. The same reasoning now shows $Qywy^{-1} \subset P$.

But, since $w = 1$, $P = Pw$, whence $P \subset Q$. At the same time, $Q = Qywy^{-1}$, implying $Q \subset P$. We thus obtain $P = Q$, a contradiction. Therefore, such a relation cannot exist, proving the result, by Proposition 1.2.3. ■

Before moving on, we remark that, similarly to how every subgroup of a free group is free, there's a generalization of this result, due to Kurosh, that shows that every subgroup of a free product is a free product. For a precise statement and proof (which makes heavy use of algebraic topology), see [Rot99].

1.3 Nilpotent groups

We now change gears a bit to discuss chain conditions in groups and properties derived from them. We'll mainly continue to follow some of the exposition in [LS01], [MKS75] and [Rot99], whenever convenient. We begin with the following definition.

Definition. A **subnormal series** for a group G is a finite sequence $1 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_k = G$. It is called a **normal series** if $N_j \trianglelefteq G$, for all j.

An important example of a normal series is the derived series of a solvable group G. That said, there are many others, such as those defined below.

Definition. A normal series $1 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_k \trianglelefteq \ldots \trianglelefteq G$ is called a **central series** if $H_j/H_{j-1} \leq Z(G/H_{j-1})$ for all j.

There are two extremely important examples of sequences of subgroups which might be central series in certain contexts. In order to define them, it's worth recalling the following construction.

Definition. Let G be a group and let H, K be subgroups of G. We define the **commutator subgroup** of H and K by $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle$; i.e., it's the subgroup of G generated by the commutators of the elements of H and those of K.

Definition. Let G be a group. The **upper central series** $1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \ldots$ is inductively defined by $Z_1(G) = Z(G)$ and $Z_n(G)$ is the unique normal subgroup of G containing $Z_{n-1}(G)$ such that $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$.

Definition. Let G be a group. The **lower central series** $G = \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \gamma_3(G) \trianglerighteq \ldots$ is inductively defined by $\gamma_1(G) = G$ and $\gamma_n(G) = [\gamma_{n-1}(G), G]$.

When the group G is clear from context, the terms of these sequences will be simply denoted Z_n and γ_n respectively. It's worth noting that, in spite of the name, both may fail to be central series, by failing to reach G or 1, respectively (an example is the group S_5).

The following result will be pivotal in establishing the relationship between the upper and lower central series.

Proposition 1.3.1. *Let G be a group.*

1. *If $H, K \leq G$ and $f : G \longrightarrow L$ is a homomorphism, then $f([H,K]) = [f(H), f(K)]$;*
2. *If $K \trianglelefteq G$ and $K \leq H \leq G$, then $[H,G] \leq K \iff H/K \leq Z(G/K)$;*

Proof.

1. Let $[h,k]$ be a commutator in the subgroup $[H,K]$. Then, $f([h,k]) = f(h^{-1}k^{-1}hk) = f(h)^{-1}f(k)^{-1}f(h)f(k) = [f(h), f(k)] \in [f(H), f(K)]$. Similarly, $[f(h), f(k)] = f(h)^{-1}f(k)^{-1}f(h)f(k) = f([h,k])$, completing the proof.
2. Suppose $[H,G] \leq K$. Then, if $\pi : G \longrightarrow G/K$ is the natural projection, $\pi([H,G]) = 1$. By the preceding item, $\pi([H,G]) = [\pi(H), \pi(G)] = [H/K, G/K]$. Thus, $[H/K, G/K] = 1$, and therefore, $H/K \leq Z(G/K)$. On the other hand, if $H/K \leq Z(G/K)$, then $[H/K, G/K] = 1$. As such, $\pi([H,G]) = 1$. Therefore, if $[h,g] \in [H,G]$, $\pi([h,g]) = 1$ which implies $[h,g] \in K$, meaning $[H,G] \leq K$.

■

Definition. A group is said to be **nilpotent** if it admits a central series.

Proposition 1.3.2. *Let $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{n+1} = 1$ be a central series for a group G. Then, $\gamma_{i+1} \leq G_{i+1} \leq Z_{n-i}$. In particular, if G is nilpotent, there exists $n \in \mathbb{N}$ such that $\gamma_{n+1} = 1$ and $Z_n = G$.*

Proof. For the first inclusion, we induct on i. The base case is trivial. Suppose, then, $\gamma_i \leq G_i$. By Proposition 1.3.1, since $G_i/G_{i+1} \leq Z(G/G_{i+1})$, we get $[G_i, G] \leq G_{i+1}$. By the induction hypothesis, we then obtain $\gamma_{i+1} = [\gamma_i, G] \leq [G_i, G] \leq G_{i+1}$.

For the second inclusion, we induct on $n - i$. When $i = n$, the result is clear. Suppose it is valid for $n-i = j$; i.e., that $G_{n-(j-1)} \leq Z_j$. We wish to check $G_{n-j} \leq Z_{j+1}$. Using the induction hypothesis, there is a surjective group homomorphism $\psi : G/G_{n-(j-1)} \longrightarrow G/Z_j$ given by $\psi(gG_{n-(j-1)}) = gZ_j$. In particular, $\psi(Z(G/G_{n-(j-1)})) \leq Z(G/Z_j)$. Thus, $\psi(G_{n-j}/G_{n-(j-1)}) \leq Z(G/Z_j) = Z_{j+1}/Z_j$. But $\psi(G_{n-j}/G_{n-(j-1)}) = (G_{n-j}Z_j)/Z_j$. The Correspondence Theorem then implies $G_{n-j} \leq G_{n-j}Z_j \leq Z_{j+1}$, finishing the proof. ■

As an immediate consequence of Proposition 1.3.2, we can characterize nilpotent groups as follows:

Theorem 1.3.3. *Let G be a group. Then, the following are equivalent:*

1. *G is nilpotent;*
2. *The lower central series is a normal series;*
3. *The upper central series is a normal series;*

Proof. Trivial from the preceding remarks. ■

Definition. Let G be a nilpotent group. The length n of the upper and lower central series of G (which is the smallest length of a central series of G, by Proposition 1.3.2) is called the **nilpotency class** of G.

Thus, the only nilpotent group of class 0 is the trivial group, those of class 1 are the abelian groups and those of class 2 are the groups whose commutators are central. The next couple of results, despite having simple proofs, show some of the good properties of nilpotent groups.

Proposition 1.3.4. *Let G be a nilpotent group and let $1 \neq N \trianglelefteq G$. Then, $N \cap Z(G) \neq 1$. In particular, $Z(G) \neq 1$.*

Proof. Let c be the nilpotency class of G and consider its upper central series, $1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \ldots \trianglelefteq Z_c = G$. Since $N \neq 1$, the set $\{n \in \mathbb{N} \mid N \cap Z_n \neq 1\}$ is non-empty, meaning it has a minimum. Let, then, $n \in \mathbb{N}$ be such that $N \cap Z_n = 1$, but $N \cap Z_{n+1} \neq 1$.

As $[G, N \cap Z_{n+1}] \leq [G, N] \leq N$, since $N \cap Z_{n+1} \leq N$, $N \trianglelefteq G$, and $[G, N \cap Z_{n+1}] \leq [G, Z_{n+1}] \leq Z_n$, by Proposition 1.3.1, we get $[G, N \cap Z_{n+1}] = 1$. Thus, $N \cap Z_{n+1} \subset Z(G) = Z_1$, meaning $N \cap Z_1 \neq 1$. So $n = 0$ and the result is proved. ■

Recall that a group is deemed **solvable** if there exists an $n \in \mathbb{N}$ such that $G^{(n)} = 1$, where the subgroups $G^{(k)}$ are defined inductively as $G^{(0)} = G$ and $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$ ($G^{(1)}$ is usually denoted G', and, from the definition of the lower central series, $G' = \gamma_2(G)$).

While the following fact won't be used, it is an interesting remark with a simple proof, using an equivalent characterization of solvable groups (see, for instance, [Isa11, Lemma 3.9])

Proposition 1.3.5. *Let G be a nilpotent group. Then, G is solvable.*

Proof. Indeed, the factors of a central series for G are all central and, in particular, abelian. ■

Proposition 1.3.6. *Let G be a nilpotent group of class c and let $N \trianglelefteq G$ and $H \leq G$. Then, H and G/N are both nilpotent, and their nilpotency classes are bounded from above by c.*

Proof. Using induction, we will show that $\gamma_i(H) \leq \gamma_i(G)$. The base case is clear. Now suppose $\gamma_i(H) \leq \gamma_i(G)$. We obtain: $\gamma_{i+1}(H) = [\gamma_i(H), H] \leq [\gamma_i(G), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G)$, finishing the induction. Ergo, if $\gamma_{c+1}(G) = 1$, then $\gamma_{c+1}(H) = 1$.

Now let $\pi : G \longrightarrow G/N$ be the canonical projection. We'll prove that $\gamma_i(G/N) = \pi(\gamma_i(G))$. Again, the base case is trivial. Using the induction hypothesis, $\gamma_{i+1}(G/N) = [\gamma_i(G/N), G/N] = [\pi(\gamma_i(G)), \pi(G)]$, and, using Proposition 1.3.1, $[\pi(\gamma_i(G)), \pi(G)] = \pi([\gamma_i(G), G]) = \pi(\gamma_{i+1}(G))$, whence the result. In particular, $\gamma_{c+1}(G) = 1 \implies \gamma_{c+1}(G/N) = 1$. ■

We can separate out a piece of the above proof, and obtain the following:

Proposition 1.3.7. *Let G be a group and $N \trianglelefteq G$. Then, G/N is nilpotent of class c if, and only if, c is the smallest natural number such that $\gamma_{c+1} \subset N$.*

It's worth noting that, contrary to what happens for solvable groups, the converse to Proposition 1.3.6 is false (an easy example is D_3, whose center is trivial, and yet has a normal subgroup isomorphic to C_3). What is true is that, if both $N \trianglelefteq G$ and G/N' (where $N' = [N, N]$) are nilpotent, then G is nilpotent, but the proof is outside the scope of this work; for reference, see [Isa11, Exercise 1D.17], or [Rot99, page 116].

In what follows, we'll explore some properties of the lower central series - and of commutators, more generally - to obtain some results about nilpotent groups which will be frequently used in the subsequent sections. This exploration will follow some of the exposition in [MKS75] and [Pas14].

We begin by extending the notion of commutators to more than two elements. Since the commutator bracket is non-associative, it becomes important to set-up a convention on the order of performing the brackets. We do so in the following definition, opting for bracketing always from the left:

Definition. Let G be a group and $x_1, ..., x_n \in G$. The **commutator of weight n** of the x_i is defined as follows:

$$[x_1, ..., x_n] = \begin{cases} x_1 & \text{if } \text{n} = 1 \\ [x_1, x_2] & \text{if } \text{n} = 2 \\ [[x_1, ..., x_{n-1}], x_n] & \text{if } \text{n} > 2 \end{cases}$$

Analogously, if $X_1, ..., X_n$ are subgroups of G, then $[X_1, ..., X_n] := [[X_1, ..., X_{n-1}], X_n]$.

Proposition 1.3.8 (Witt-Hall identity). [4] *Let G be a group and let $x, y, z \in G$. Then, the following identity holds:*

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$$

Proof. First, note that $[a, b]^{-1} = [b, a]$. Therefore,

$$\begin{aligned} [x, y^{-1}, z]^y &= y^{-1}[y^{-1}, x]z^{-1}[x, y^{-1}]zy \\ &= x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy \end{aligned}$$

Similarly, the same process yields

$$\begin{aligned} [y, z^{-1}, x]^z &= y^{-1}z^{-1}yx^{-1}y^{-1}zyz^{-1}xz \\ [z, x^{-1}, y]^x &= z^{-1}x^{-1}zy^{-1}z^{-1}xzx^{-1}yx \end{aligned}$$

Thus, we obtain

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z = x^{-1}y^{-1}xz^{-1}x^{-1}zyz^{-1}xz$$

and, finally,

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$$

■

Proposition 1.3.9 (Three subgroup lemma). *Let G be a group, $N \trianglelefteq G$ and X, Y, Z be subgroups of G. If $[X, Y, Z] \subset N$ and $[Y, Z, X] \subset N$, then $[Z, X, Y] \subset N$.*

Proof. Let $x \in X$, $y \in Y$ and $z \in Z$. Since $[X, Y, Z] \subset N$, with N normal in G, $[x, y^{-1}, z]^y \in N$. Similarly, $[y, z^{-1}, x]^z \in N$. Due to the Witt-Hall identity, we get $[z, x^{-1}, y]^x \in N$, and thus $[z, x^{-1}, y] \in N$, again using normality. But it's clear that these elements generate $[Z, X, Y]$. Since x, y, z were arbitrary, we get the result. ■

We may now use the preceding lemma to show a beautiful property of the lower central series, allowing us to descend it multiple steps at once by taking appropriate commutators.

Proposition 1.3.10. *Let G be a group and $\gamma_n(G)$, $n \in \mathbb{N}^\dagger$ be the terms of its lower central series. Then:*

$$[\gamma_m(G), \gamma_n(G)] \leq \gamma_{m+n}(G)$$

Proof. We use induction on n. If $n = 1$, $[\gamma_m(G), \gamma_1(G)] = [\gamma_m(G), G] = \gamma_{m+1}(G)$ by definition. Suppose, then, that $[\gamma_m(G), \gamma_n(G)] \leq \gamma_{m+n}(G), \forall m \in \mathbb{N}^\dagger$. In particular, $[\gamma_m(G), G, \gamma_n(G)] = [\gamma_{m+1}(G), \gamma_n(G)] \leq \gamma_{m+n+1}(G)$ and $[\gamma_n(G), \gamma_m(G), G] \leq [\gamma_{m+n}(G), G] = \gamma_{m+n+1}(G)$. By Proposition 1.3.9, this forces $[G, \gamma_n(G), \gamma_m(G)] \leq \gamma_{m+n+1}(G)$. But $[G, \gamma_n(G), \gamma_m(G)] = [\gamma_{n+1}(G), \gamma_m(G)] = [\gamma_m(G), \gamma_{n+1}(G)]$. This establishes the result. ■

[4] Notice how this is a group-theoretic analogue of the Jacobi identity of Lie algebras. In fact, [Rot99] refers to this proposition as the Jacobi identity.

Proposition 1.3.11. *Let G be a group and let $a \in \gamma_m(G), b \in \gamma_n(G), c \in \gamma_p(G)$. Then, the following are true:*

a) $[ab, c] \equiv [a, c][b, c] \pmod{\gamma_{m+n+p}(G)}$;

b) $[a, bc] \equiv [a, b][a, c] \pmod{\gamma_{m+n+p}(G)}$;

Proof. a) $[ab, c] = b^{-1}a^{-1}c^{-1}abc = [a, c]^b[b, c] = [a, c][a, c]^{-1}[a, c]^b[b, c] = [a, c][a, c, b][b, c]$. By Proposition 1.3.10, $[a, c, b] \in \gamma_{m+n+p}(G)$, whence the identity.

b) $[a, bc] = a^{-1}c^{-1}b^{-1}abc = [a, c][a, b]^c = [a, c][a, b][a, b]^{-1}[a, b]^c = [a, c][a, b][a, b, c] = [a, b][a, c][[a, c], [a, b]][a, b, c]$. But notice that, repeatedly using Proposition 1.3.10, $[a, c] \in \gamma_{m+p}(G), [a, b] \in \gamma_{m+n}(G)$ and $[[a, c], [a, b]] \in \gamma_{2m+n+p}(G) \leq \gamma_{m+n+p}(G)$. This shows the identity.

■

One particular consequence of this proposition is that it shows nilpotent groups of class 2 possess a very special property.

Corollary 1.3.11.1. *If G is a nilpotent group of class 2 and $x \in G$, then the mappings $[\cdot, x] : G \longrightarrow G$ and $[x, \cdot] : G \longrightarrow G$ defined by $y \longmapsto [y, x]$ and $y \longmapsto [x, y]$, respectively, are both homomorphisms.*

Proposition 1.3.12. *Let G be a group, $k \geq 1$, $g_1, ..., g_k \in \gamma_m(G)$, $g \in \gamma_n(G)$ and $\epsilon_i \in \{1, -1\}$. Then:*

a) $\left[\prod_{i=1}^k g_i^{\epsilon_i}, g\right] \equiv \prod_{i=1}^k [g_i, g]^{\epsilon_i} \pmod{\gamma_{2m+n}(G)}$;

b) $\left[g, \prod_{i=1}^k g_i^{\epsilon_i}\right] \equiv \prod_{i=1}^k [g, g_i]^{\epsilon_i} \pmod{\gamma_{2m+n}(G)}$;

Proof. a) We will proceed by induction on k. If $k = 1$, there are two possibilities: $\epsilon_1 = 1$, so that the identity is trivial, or $\epsilon_1 = -1$, and so, by Proposition 1.3.11, $[g_1^{-1}, g][g_1, g] \equiv [g_1^{-1}g_1, g] = 1 \pmod{\gamma_{2m+n}(G)}$, meaning $[g_1^{-1}, g] \equiv [g_1, g]^{-1} \pmod{\gamma_{2m+n}(G)}$.

Now, for the inductive step, suppose the result is true for $k - 1$. Using Proposition 1.3.11, we obtain the following:

$$\left[\prod_{i=1}^{k} g_i^{\epsilon_i}, g\right] = \left[\prod_{i=1}^{k-1} g_i^{\epsilon_i} g_k^{\epsilon_k}, g\right] \equiv \left[\prod_{i=1}^{k-1} g_i^{\epsilon_i}, g\right] [g_k^{\epsilon_k}, g] \pmod{\gamma_{2m+n}(G)}$$

Now, using both the inductive hypothesis and the base case, the congruence becomes:

$$\left[\prod_{i=1}^{k} g_i^{\epsilon_i}, g\right] \equiv \prod_{i=1}^{k-1} [g_i, g]^{\epsilon_i} [g_k, g]^{\epsilon_k} = \prod_{i=1}^{k} [g_i, g]^{\epsilon_i} \pmod{\gamma_{2m+n}(G)}$$

finishing the proof.

b) The proof of this item is the same as that of the first one, now using the second item of Proposition 1.3.11 instead of the first.

■

Having established all these commutator identities and related properties, we can now obtain a set of generators for the factor groups of the lower central series, γ_n/γ_{n+1}. These results will become important later on.

Proposition 1.3.13. *Let G be a group generated by a set $X \subset G$. Then, $\gamma_n(G)/\gamma_{n+1}(G)$ is generated by the cosets of the commutators of weight n in the generators G. In particular, if G is finitely generated, then the quotient is finitely generated for all $n \in \mathbb{N}^{\dagger}$.*

Proof. We'll proceed by induction on n. The base case is trivial; indeed, the set of commutators of weight 1 in X is X itself, and of course the cosets of elements of X generate the quotient group G/G'. Thus, all that is left is to consider the inductive case.

Suppose the result to be true for $\gamma_n(G)/\gamma_{n+1}(G)$. As $\gamma_{n+1}(G) = [\gamma_n(G), G]$, $\gamma_{n+1}(G)$ is generated by the commutators of the form $[h, g]$, with $h \in \gamma_n(G)$. Since $h \in \gamma_n(G)$, then, by the inductive hypothesis, $h = \prod_i h_i^{\epsilon_i} \cdot h'$, where each h_i is a commutator of weight n in X, $\epsilon_i \in \{1, -1\}$ and $h' \in \gamma_{n+1}(G) \subset \gamma_n(G)$. But then

$$[h, g] = \left[\prod_i h_i^{\epsilon_i} \cdot h', g\right] \equiv \prod_i [h_i, g]^{\epsilon_i} \cdot [h', g] \pmod{\gamma_{2n+1}(G)}$$

by Proposition 1.3.11 and Proposition 1.3.12. And $h' \in \gamma_{n+1}$, so that $[h', g] \in \gamma_{n+2}$. We now obtain

$$[h, g] \equiv \prod_i [h_i, g]^{\epsilon_i} \pmod{\gamma_{n+2}(G)}$$

since $\gamma_{2n+1} \subset \gamma_{n+2}$.

If X generates G, then $g = \prod_j a_j^{\eta_j}$, where $a_j \in X$ and $\eta_j \in \{1, -1\}$ for all j. Thus:

$$[h_i, g] = \left[h_i, \prod_j a_j^{\eta_j}\right] \equiv \prod_j [h_i, a_j]^{\eta_j} \pmod{\gamma_{n+2}(G)}$$

again using Proposition 1.3.12.

Putting both of the congruences together:

$$[h, g] \equiv \prod_i \left(\prod_j [h_i, a_j]^{\eta_j}\right)^{\epsilon_i} \pmod{\gamma_{n+2}(G)},$$

which is a product of commutators of weight $n + 1$ in the generators of G. This establishes the result. ■

It's well-known that, if both $N \trianglelefteq G$ and G/N are finitely generated, then the same is true of G (indeed, if $\{g_1, ..., g_n\}$ generate N and $\{h_1N, ..., h_mN\}$ generates G/N, then $\{g_ih_j \mid 1 \le i \le n, 1 \le j \le m\}$ generates G). Putting this fact together with the previous proposition, we get the following corollary:

Corollary 1.3.13.1. *Let G be a finitely generated nilpotent group. Then, the terms of its lower central series are finitely generated.*

For what follows, we must briefly digress to discuss torsion. An element $1 \neq x$ in a group G is said to be **torsion** or **a torsion element** if it has finite order in G. Otherwise, we call it **torsion-free**. The group G itself is said to be **torsion** if every non-identity element of G is a torsion element. Otherwise, G is said to be **torsion-free**.

Of course, any finite group is a torsion group. Later on, when we discuss group algebras, torsion is going to be a major issue in embedding it in a division ring. For now, though, we study how it relates to the central series of a nilpotent group, starting with the following property of the lower central series.

Proposition 1.3.14. *Let G be a group generated by torsion elements. Then, $\gamma_n(G)/\gamma_{n+1}(G)$ is a torsion group for all $n \in \mathbb{N}^\dagger$.*

Proof. We proceed by induction on n. If $n = 1$, $\gamma_1(G)/\gamma_2(G) = G/G'$. Since all the cosets of the generators are torsion elements and G/G' is abelian, G/G' is torsion.

Now suppose $\gamma_n(G)/\gamma_{n+1}(G)$ is torsion. The abelian group $\gamma_{n+1}(G)/\gamma_{n+2}(G)$ is generated by the cosets of the commutators of weight $n + 1$ on the commutators of G, due to Proposition 1.3.13. As such, all we have to do is show that these cosets are torsion elements.

Let $[x_1, ..., x_{n+1}]$ be one such commutator. We have $[x_1, ..., x_{n+1}] = [[x_1, ..., x_n], x_{n+1}]$. As $[x_1, ..., x_n] \in \gamma_n(G)$, by the inductive hypothesis, there exists $k \in \mathbb{N}^\dagger$ such that $[x_1, ..., x_n]^k \in \gamma_{n+1}$. Ergo, $[[x_1, ..., x_n]^k, x_{n+1}] \in \gamma_{n+2}(G)$. But, using Proposition 1.3.12, we get:

$$[[x_1, ..., x_n]^k, x_{n+1}] \equiv [x_1, ..., x_n, x_{n+1}]^k \pmod{\gamma_{2n+1}(G)}$$

Furthermore, $\gamma_{2n+1}(G) \subset \gamma_{n+2}(G)$, since $n \geq 1$. We now have $[x_1, ..., x_n, x_{n+1}]^k \in \gamma_{n+2}(G)$, finishing the proof. ∎

We now study the relationship between torsion and the upper central series.

Proposition 1.3.15. *Let G be a group whose center is torsion-free, and let $1 = Z_0 \trianglelefteq Z_1 \trianglelefteq ...$ be its upper central series. Then, Z_{n+1}/Z_n is torsion-free abelian for all $n \in \mathbb{N}$.*

Proof. We use induction on n. The base case is trivial, by hypothesis. If $n = 1$, let $x \in Z_2$ and suppose $x^r \in Z_1 = Z(G)$. By Proposition 1.3.1, given $y \in G$, $[x, y] \in Z_1$. Therefore, $[x, y]^r = [x^r, y]$, as can be seen from the proof of Proposition 1.3.11, so that $[x, y]^r = 1$. This, in turn, means $[x, y] = 1$, implying $x \in Z_1$. Ergo, it's also true that Z_2/Z_1 is torsion-free.

For the inductive step, suppose Z_{n+1}/Z_n is torsion-free. Let $\overline{G} = G/Z_n$. Its center is Z_{n+1}/Z_n, which is torsion-free by hypothesis. Using the case $n = 1$, $Z_2(\overline{G})/Z_1(\overline{G})$ is torsion-free. But

$$\frac{Z_2(\overline{G})}{Z_1(\overline{G})} = Z\left(\frac{\overline{G}}{Z_1(\overline{G})}\right) = Z\left(\frac{G/Z_n}{Z_{n+1}/Z_n}\right) \cong Z\left(\frac{G}{Z_{n+1}}\right) = \frac{Z_{n+2}}{Z_{n+1}}$$

Therefore, Z_{n+2}/Z_{n+1} is torsion-free, which completes the proof. ∎

Corollary 1.3.15.1. *If G is a nilpotent group whose center is torsion-free, then G/Z_n is torsion-free for all $n \in \mathbb{N}$. In particular, G is torsion-free.*

Proof. Let c be the nilpotency class of G. For $n = c, c-1$, the result follows immediately from Proposition 1.3.15. Otherwise, let $x \in G$ and suppose $x^r \in Z_n$. Since $Z_n \subset Z_{c-2} \subset Z_{c-1}$, $x^r \in Z_{c-1}$. Thus, by Proposition 1.3.15, $x \in Z_{c-1}$. Now, all we have to do is apply the same proposition inductively (indeed, $x^r \in Z_{c-2}$ and $x \in Z_{c-1}$ means $x \in Z_{c-2}$, and so on). After a finite number of steps, $x \in Z_n$. ∎

Proposition 1.3.16. *Let G be a nilpotent group and let $\operatorname{tor}(G)$ be the subset of torsion elements of G. Then, $\operatorname{tor}(G) \trianglelefteq G$.*

Proof. It's evident that $1 \in \operatorname{tor}(G)$, $x^{-1}\operatorname{tor}(G)x \subset \operatorname{tor}(G)$ and that $x \in \operatorname{tor}(G)$ implies $x^{-1} \in \operatorname{tor}(G)$. Thus, we only need to verify that $x, y \in \operatorname{tor}(G)$ implies $xy \in \operatorname{tor}(G)$. For this, we'll induct on the nilpotency class c of $\langle x, y\rangle \leq G$. If $c = 1$, this subgroup is abelian and the result is clear. All that's left is the inductive step.

We have $1 = \gamma_{c+1} \triangleleft \gamma_c \triangleleft \ldots \triangleleft \gamma_1 = \langle x, y\rangle$ and, by Proposition 1.3.7, $\gamma_c(\langle x, y\rangle/\gamma_c) = 1$. Therefore, $\langle x, y\rangle/\gamma_c$ has nilpotency class less than c. Using the inductive hypothesis, as $x, y \in \operatorname{tor}(\langle x, y\rangle/\gamma_c)$, the same happens to xy. Then, there exists $m \in \mathbb{N}^\dagger$ such that $(xy)^m \in \gamma_c$. But, using Proposition 1.3.14, γ_c is torsion, meaning $xy \in \operatorname{tor}(\langle x, y\rangle) \subset \operatorname{tor}(G)$. ∎

We can then conclude the following corollary, which allows us to obtain torsion-free nilpotent groups from torsion ones:

Corollary 1.3.16.1. *Let G be a nilpotent group. Then, $G/\operatorname{tor}(G)$ is torsion-free nilpotent.*

Proposition 1.3.17. *Let G be a nilpotent group and let $x, y \in G$ be such that there exist $r, s \in \mathbb{N}^\dagger$ with $[x^r, y^s] = 1$. Then, $[x, y] \in \operatorname{tor}(G)$.*

Proof. We can divide the proof in two cases:

- Case 1: G is torsion-free.

  Let $H_x = \langle x, y^s\rangle$. By hypothesis, $x^r \in Z(H_x)$. By Corollary 1.3.15.1, $H_x/Z(H_x)$ is torsion-free, meaning $x \in Z(H_x)$. Thus, $[x, y^s] = 1$. Similarly, if $K_y = \langle x, y\rangle$, we see that $y \in Z(K_y)$. Ergo, $[x, y] = 1 \in \operatorname{tor}(G)$.

- General case:

  By the previous corollary, $G/\operatorname{tor}(G)$ is torsion-free nilpotent. So, using Case 1, since $[\overline{x}^r, \overline{y}^s] = 1$, we get $\overline{[x, y]} = [\overline{x}, \overline{y}] = \overline{1}$, meaning $[x, y] \in \operatorname{tor}(G)$.

∎

1.4 Residual properties

Definition. Let $\mathscr{P}$ be a group property. A group G is said to be **residually $\mathscr{P}$** if, for all $1 \neq g \in G$, there exists a normal subgroup $N_g \trianglelefteq G$ such that $g \notin N_g$ and G/N_g is $\mathscr{P}$.

Even though we have given quite a general definition, for the purposes of this work, we'll only deal with **residually (torsion-free nilpotent)** groups (we'll omit the parentheses from now on). In order to characterize these groups, it will be important to introduce some notation.

Let G be an arbitrary group. By Proposition 1.3.7, $\overline{G} = G/\gamma_n$ is a nilpotent group (of nilpotency class less than or equal to $n-1$). And, by Proposition 1.3.16, $\operatorname{tor}(\overline{G})$ is a normal subgroup of $\overline{G}$. By the Correspondence Theorem, there exists a unique normal subgroup H of G, containing γ_n, such that $\pi(H) = \operatorname{tor}(\overline{G})$, where $\pi : G \longrightarrow \overline{G}$ is the canonical projection. Thus, from the same theorem:

$$\begin{aligned} H &= \{g \in G \mid \pi(g) \in \operatorname{tor}(\overline{G})\} \\ &= \{g \in G \mid \exists m \in \mathbb{N}^\dagger \text{ such that } \pi(g)^m = \overline{1}\} \\ &= \{g \in G \mid \exists m \in \mathbb{N}^\dagger \text{ such that } g^m \in \gamma_n\} \end{aligned}$$

The normal subgroup H defined above will be denoted by $\sqrt{\gamma_n(G)}$ or simply $\sqrt{\gamma_n}$ when the group G is clear from context (notice the clear analogy with the radical of an ideal of a commutative ring). It's trivial to check that, in a similar vein to what happened with the terms of the lower central series, we have:

$$G = \sqrt{\gamma_1} \trianglerighteq \sqrt{\gamma_2} \trianglerighteq \ldots \text{ and also } \gamma_n \subset \sqrt{\gamma_n}, \forall n \in \mathbb{N}^\dagger$$

We may characterize residually torsion-free nilpotent using these "radicals" of the lower central series. We do this in what follows (many of these ideas were adapted from [GFS19]).

Proposition 1.4.1. *For a group G, the following are equivalent:*

1. *G is residually torsion-free nilpotent;*
2. *$\bigcap_{n=1}^{\infty} \sqrt{\gamma_n(G)} = 1$;*
3. *There exists a (possibly infinite) sequence $G = N_1 \supset N_2 \supset \ldots$ such that $N_i \trianglelefteq G, \forall i$, $\bigcap_i N_i = 1$ and G/N_i is torsion-free nilpotent for all i;*

Proof. (1) $\Longrightarrow$ (2): Let $1 \neq g \in G$ and consider N_g such that G/N_g is torsion-free nilpotent, $g \notin N_g$. By Proposition 1.3.7, there is some c_g with $\gamma_{c_g} \subset N_g$.

Let $x \in \sqrt{\gamma_{c_g}}$ be arbitrary. By definition, $x^m \in \gamma_{c_g} \subset N_g$ for some $m \in \mathbb{N}^\dagger$. Since G/N_g is torsion-free, $x \in N_g$. Thus, we conclude that $\sqrt{\gamma_{c_g}} \subset N_g$. As g is arbitrary, we get

$$\bigcap_{i=1}^{\infty} \sqrt{\gamma_i} \subset \bigcap_{g \in G} \sqrt{\gamma_{c_g}} \subset \bigcap_{g \in G} N_g = 1$$

(2) $\Longrightarrow$ (3): The group $\frac{G}{\sqrt{\gamma_n}}$ is nilpotent (since $\gamma_n \subset \sqrt{\gamma_n}$), torsion-free, by construction, and, by hypothesis, their intersection is trivial.

(3) $\implies$ (1): Let $1 \neq g$ be an arbitrary element of G. As $\bigcap_i N_i = 1$, there is some N_{i_0} such that $g \notin N_{i_0}$. Furthermore G/N_{i_0} is torsion-free nilpotent, by hypothesis. Thus, G is residually torsion-free nilpotent.

■

We may also prove a version of Proposition 1.3.10 to the "radicals" of the lower central series, as we do below.

Proposition 1.4.2. *Let G be a group. The following are true:*

1. $[\sqrt{\gamma_i}, \sqrt{\gamma_j}] \subset \sqrt{\gamma_{i+j}}$;
2. $\sqrt{\gamma_n}/\sqrt{\gamma_{n+1}}$ *is torsion-free abelian for all* $n \in \mathbb{N}^\dagger$;

Proof. 1. If $x \in \sqrt{\gamma_i}$ and $y \in \sqrt{\gamma_j}$, then there exist $r, s \in \mathbb{N}^\dagger$ such that $x^r \in \gamma_i$ and $y^s \in \gamma_j$. Thus, by Proposition 1.3.10, $[x^r, y^s] \in \gamma_{i+j}$. Now using Proposition 1.3.17, $\pi([x, y]) \in \operatorname{tor}(G/\gamma_{i+j})$, which means $[x, y] \in \sqrt{\gamma_{i+j}}$, by definition.

2. The quotient is torsion-free, by construction. Furthermore, by the previous item, $[\sqrt{\gamma_i}, \sqrt{\gamma_i}] \subset \gamma_{2i} \subset \gamma_{i+1}$, since $i \geq 1$. Thus, it's also abelian.

■

1.5 Polycyclic groups

Having dealt with nilpotent groups, there exists a chain condition, similar to solubility, which will also be important for some arguments to be employed further on, in order to find free groups within certain types of division rings. We mostly follow [Rot99], with occasional references to [Rob96].

Definition. A group G is said to be **polycyclic** if there exists a subnormal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ such that G_{i+1}/G_i is cyclic for all i. This is called a **polycyclic series** for G.

It's trivial, from the definition, that every polycyclic group is solvable. And, continuing this analogy with solubility, we present the following result, whose proof is identical to that of the solvable case:

Proposition 1.5.1. *Let G be a group. If G is polycyclic, then, all subgroups and quotients of G are polycyclic. And, if $N \trianglelefteq G$ and G/N are both polycyclic, then G is itself polycyclic.*

Proof. Suppose, first, that G is polycyclic and let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ be a polycyclic series for G (i.e., the subsequent quotients are cyclic). Let H be a subgroup of G and consider $1 = H_0 \trianglelefteq \ldots \trianglelefteq H_n = H$, where $H_k = G_k \cap H$ (each is normal in the next by a simple argument). We have

$$\frac{H_{k+1}}{H_k} = \frac{H \cap G_{k+1}}{H \cap G_k} = \frac{H \cap G_{k+1}}{H \cap G_{k+1} \cap G_k} \cong \frac{(H \cap G_{k+1})G_k}{G_k} \leq \frac{G_{k+1}}{G_k}$$

by the Second Isomorphism Theorem and the fact that $(H \cap G_{k+1})G_k \leq G_{k+1}$. Hence, this quotient is a subgroup of a cyclic group, meaning it's itself cyclic.

Now take $N \trianglelefteq G$ and consider $N = N_0 \trianglelefteq \ldots \trianglelefteq N_n = G$, where $N_k = NG_k$ (again, since N is normal, each of these is normal in the next by a simple argument). We have:

$$\frac{N_{k+1}}{N_k} = \frac{NG_{k+1}}{NG_k} = \frac{NG_kG_{k+1}}{NG_k} \cong \frac{G_{k+1}}{(NG_k) \cap G_k} \cong \frac{G_{k+1}/G_k}{((NG_k) \cap G_k)/G_k}$$

by the Second and Third Isomorphism Theorems and the fact that $G_k \trianglelefteq (NG_k) \cap G_k$. Hence, this quotient is a quotient of a cyclic group, meaning it's itself cyclic. By the Correspondence Theorem, this yields a polycyclic series for the quotient group G/N.

For the converse, if $N \trianglelefteq G$ and G/N are both polycyclic, we get a polycyclic series for G by "gluing" the two series together. More precisely, if $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_m = N$ is a polycyclic series for N and $1 = \overline{H_0} \trianglelefteq \ldots \trianglelefteq \overline{H_n} = \overline{G} = G/N$ is one for G/N, the following series is polycyclic:

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_m = N = H_0 \trianglelefteq \ldots \trianglelefteq H_n = G$$

where we used the Correspondence Theorem to lift the subgroups $\overline{H_k}$ to subgroups of G containing N. ■

What is interesting for our purposes is that f.g. nilpotent groups are polycyclic. We break the proof down into two propositions:

Proposition 1.5.2. *Let G be a finitely generated abelian group. Then, G is polycyclic.*

Proof. By the Fundamental Theorem of Finitely Generated Abelian Groups (see, for instance, [Rot99, Theorem 10.20]), $G \cong \mathbb{Z}^k \times \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_l^{n_l}}$, where $k \in \mathbb{N}$, $n_i \in \mathbb{N}$ for all i and each p_i is a prime (we allow $p_i = p_j$ even when $i \neq j$). This allows us to construct the series

$$1 \triangleleft \mathbb{Z} \triangleleft \ldots \triangleleft \mathbb{Z}^k \triangleleft \mathbb{Z}^k \times \mathbb{Z}_{p_1^{n_1}} \triangleleft \ldots \triangleleft G$$

whose quotients are all cyclic by construction. ■

Proposition 1.5.3. *Let G be a finitely generated nilpotent group. Then, G is polycyclic.*

Proof. We induct on the nilpotency class c of the group G. The base case $c = 1$ is Proposition 1.5.2. By Proposition 1.3.10, $G' = \gamma_2$ has nilpotency class less than or equal to $c - 1$. Furthermore, Corollary 1.3.13.1 tells us that G' is finitely generated. Using the inductive hypothesis, G' is polycyclic. But G/G' is finitely generated abelian by Proposition 1.3.13. Thus, by Proposition 1.5.2, it's polycyclic and, by Proposition 1.5.1, the same is true of G. ■

Therefore, the study of polycyclic groups gives us tools to further study f.g. nilpotent groups. This sheds even more light on the importance of studying polycyclic series and their properties. We'll soon see they give us a helpful invariant of the group. For now, we define the following:

Definition. Let $S_1 : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ and $S_2 : 1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m = G$ be two subnormal series for the same group G. The series S_2 is said to be a **refinement** of S_1 if, for all $i \in \{1, \ldots, n\}$, there exists a $j \in \{1, \ldots, m\}$ such that $H_j = G_i$. The refinement is deemed **proper** if there exists j_0 such that $H_{j_0} \neq G_i, \forall i$.

Definition. Two subnormal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ and $1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$ are deemed **equivalent** if $m = n$ and there exists $\sigma \in S_n$ such that $G_{i+1}/G_i \cong H_{\sigma(i)+1}/H_{\sigma(i)}$, for all i.

A relatively surprising fact is that any two subnormal series of a group may be refined down to equivalent series. In order to prove this result due to O. Schreier, we first establish a lemma, one that is known for its pictorial representation. The results below are all from [Rot99].

Proposition 1.5.4 (Butterfly/Zassenhaus' Lemma)**.** *Let $A \trianglelefteq G$ and $B \trianglelefteq H$, where G, H are subgroups of a given group K. Then, the following are true:*

- $A(G \cap B) \trianglelefteq A(G \cap H)$;
- $B(H \cap A) \trianglelefteq B(G \cap H)$;
- $\dfrac{A(G \cap H)}{A(G \cap B)} \cong \dfrac{B(G \cap H)}{B(H \cap A)}$;

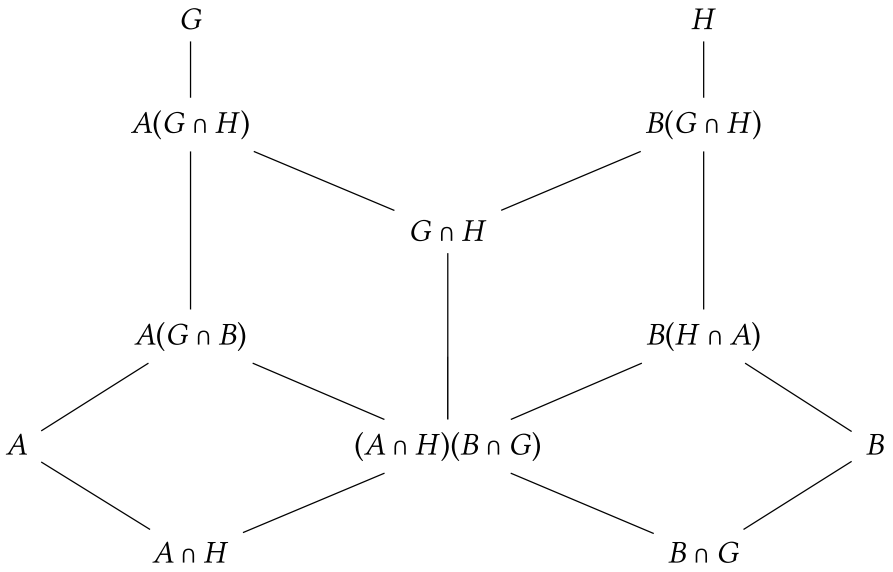
Proof. Since $A \trianglelefteq G$, by the Second Isomorphism Theorem, $A \cap H = (A \cap G) \cap H = A \cap (G \cap H) \trianglelefteq G \cap H$. Doing the same to $B \trianglelefteq G$, we get $B \cap G \trianglelefteq G \cap H$. Therefore:

$$M = (A \cap H)(B \cap G) \trianglelefteq (G \cap H)$$

Now consider $\varphi : A(G \cap H) \longrightarrow (G \cap H)/M$ given by $\varphi(gh) = hM$. It's straightforward to check that φ is a surjective homomorphism with $\ker(\varphi) = A(G \cap B)$. This now yields the following isomorphism:

$$\frac{A(G \cap H)}{A(G \cap B)} \cong \frac{G \cap H}{M}$$

The same argument may now be repeated, by considering $\psi : B(G \cap H) \longrightarrow (G \cap H)/M$ instead, whence the result.



Above, we present the diagram representation of the subgroups considered, where moving up a line signals inclusion. ■

Theorem 1.5.5 (Schreier's Refinement Theorem)**.** *Let G be a group and let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ and $1 = H_0 \trianglelefteq \ldots \trianglelefteq H_m = G$ be two subnormal series. Then, both admit equivalent refinements.*

Proof. Define $G_{i,j} = G_{i-1}(G_i \cap H_j)$ and $H_{i,j} = H_{i-1}(H_i \cap G_j)$. It's easy to see that $G_{i,0} = G_{i-1}$, $G_{i,m} = G_i$, $H_{i,0} = H_{i-1}$ and $H_{i,n} = H_i$. Furthermore, $G_{i,j-1} \leq G_{i,j}$. Defining $G = G_i, H = H_j, A = G_{i-1}, B = H_{j-1}$, as in Proposition 1.5.4, we get

$$1 = G_{1,0} \trianglelefteq G_{1,1} \trianglelefteq \ldots \trianglelefteq G_{1,m} = G_1 = G_{2,0} \trianglelefteq \ldots \trianglelefteq G_{i,j-1} \trianglelefteq G_{i,j} \trianglelefteq \ldots \trianglelefteq G_{n,m} = G$$

Doing the same to H, we also get

$$1 = H_{1,0} \trianglelefteq H_{1,1} \trianglelefteq \ldots \trianglelefteq H_{1,n} = H_1 = H_{2,0} \trianglelefteq \ldots \trianglelefteq H_{i,j-1} \trianglelefteq H_{i,j} \trianglelefteq \ldots \trianglelefteq H_{m,n} = G$$

Both series have $nm + 1$ terms. Moreover, it also follows from Proposition 1.5.4 that

$$\frac{G_{i,j}}{G_{i,j-1}} = \frac{G_{i-1}(G_i \cap H_j)}{G_{i-1}(G_i \cap H_{j-1})} \cong \frac{H_{j-1}(H_j \cap G_i)}{H_{j-1}(H_j \cap G_{i-1})} = \frac{H_{j,i}}{H_{j,i-1}}$$

Thus, both of the refinements are equivalent. ■

Even though this result won't be used for this work, it's worth noting the following straightforward consequence of the preceding theorem, which is a very famous result and a huge motivator to many developments in the theory of finite groups: the Jordan-Hölder Theorem.

In order to do this, we establish another bit of terminology. A subnormal series for a group G is said to be a **composition series** if it doesn't admit any proper refinements. It's relatively simple to see that a subnormal series is a composition series if and only if all factor groups (that is, the quotient groups of successive terms) are either simple or trivial.[5]

All finite groups admit a composition series, by an induction argument, but the same needn't be true for infinite groups. As an example, the infinite cyclic group doesn't have a composition series, since, if $0 = m_0\mathbb{Z} \triangleleft \ldots \triangleleft m_k\mathbb{Z} = \mathbb{Z}$ is a composition series, then $m_{i+1}\mathbb{Z}/m_i\mathbb{Z}$ is isomorphic to C_p for some prime p. In particular, $m_1\mathbb{Z}$ should be finite, meaning $m_1 = 0$, a contradiction, since we assumed strict inclusions.

Theorem (Jordan-Hölder)**.** *Let G be a group admitting a composition series. Then, any two such series are equivalent.*

Another consequence of the Schreier Refinement Theorem is that the number of infinite-cyclic factors in a polycyclic series for a polycyclic group G is an invariant of the group, meaning it doesn't depend on the chosen series. We prove this next, following the ideas from [Rob96].

[5] We may instead require that all inclusions are proper for a series to be a composition series, in which case the factor groups can't be trivial.

Proposition 1.5.6. *Let G be a polycyclic group and let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ be a polycyclic series for G. Then, the number of infinite cyclic factors (G_{i+1}/G_i) is refinement-invariant.*

Proof. Evidently, we need only consider proper refinements. Thus, we only have to analyze a refinement $G_i = N_0 \triangleleft \ldots \triangleleft N_k = G_{i+1}$. There are two possible cases:

- Case 1: G_{i+1}/G_i is finite. Then, since

  $$\frac{N_{j+1}}{N_j} \cong \frac{N_{j+1}/G_i}{N_j/G_i} \leq \frac{G_{i+1}/G_i}{N_j/G_i}$$

  it's clear that every one of the introduced factors is finite.

- Case 2: G_{i+1}/G_i is infinite. In this case, N_j/G_i is infinite cyclic for all $j \neq 0$, since they are all isomorphic to proper subgroups of an infinite cyclic group. In particular, N_1/G_i is infinite cyclic. But, from the preceding argument, if $j \neq 0$, we get:

  $$\frac{N_{j+1}}{N_j} \cong \frac{N_{j+1}/G_i}{N_j/G_i} \leq \frac{G_{i+1}/G_i}{N_j/G_i}$$

  and this last term is a non-trivial quotient of an infinite cyclic group. Thus, it's finite. Therefore, if $j \neq 0$, N_{j+1}/N_j is finite, whence the number of infinite cyclic factors remains constant.

■

Proposition 1.5.7. *Let G be a polycyclic group. Then, the number of infinite cyclic factors of a polycyclic series for G is independent of the series.*

Proof. Let S_1 and S_2 be two polycyclic series for G. By Theorem 1.5.5, both admit equivalent refinements (that is, with isomorphic factors up to permutation). Since, by Proposition 1.5.6, the number of infinite cyclic factors is refinement-invariant, the result follows. ■

The invariant thus defined merits a special name.

Definition. Let G be a polycyclic group. Its **Hirsch number**, denoted $h(G)$, is the number of infinite cyclic factors of a polycyclic series for G.

The following additive property of Hirsch numbers follows from the proof of Proposition 1.5.1:

Proposition 1.5.8. *Let G be a polycyclic group and let $N \trianglelefteq G$. Then:*

$$h(G) = h(N) + h(G/N)$$

We'll return to the Hirsch number of a polycyclic group in Chapter 3, where it will be used in an inductive argument.

1.6 Ordered groups

We end the chapter on group theory with the class of groups which admit a total ordering compatible with the group structure. They'll be a key component to constructing the so-called "Malcev-Neumann Series Rings", which will be done further on. Right now, it's of our interest to prove a technical lemma (which will, in fact, be the crucial piece for the aforementioned construction) and the fact that residually torsion-free nilpotent groups are ordered. For this, we'll mostly follow [Fuc63] and [Lam01].

Definition. Let G be a group and assume that G admits (as a set) total ordering. Then, G is said to be an **ordered group** if, for all $a, b, c \in G$

$$a < b \implies ca < cb \text{ and } ac < bc$$

If G is an ordered group, there is a subset of G, which merits particular attention, due to the fact that it completely determines the ordering. It will be quite clear from the terminology that it is analogous to the positive numbers in the canonical ordering of the real numbers.

Definition. Let G be an ordered group. The subset $P = \{x \in G \mid x > 1\}$ is called the **positive cone** of G.

The following proposition highlights some of the main properties of the positive cone of an ordered group, which are fairly simple to verify:

Proposition 1.6.1. *Let G be an ordered group and let P be its positive cone. Then:*

- $x, y \in P \implies xy \in P$;
- $G = P \sqcup \{1\} \sqcup P^{-1}$;
- $x^{-1}Px = P$;
- $x < y \iff yx^{-1} \in P$;

It's less immediately apparent, however, that a subset with the properties above actually completely determines an ordered group structure, as we see below:

Proposition 1.6.2. *Let G be a group and let P be a subset of G with the following three properties:*

1. $x, y \in P \implies xy \in P$;
2. $G = P \sqcup \{1\} \sqcup P^{-1}$;
3. $x^{-1}Px = P$;

Then, the relation $x < y \iff yx^{-1} \in P$ induces an ordered group structure in G.

Proof. From item 2., $x < x$ is false, since $1 \notin P$. If $a < b$ and $b < c$, then $ba^{-1}, cb^{-1} \in P$, which implies, using item 1., $cb^{-1}ba^{-1} = ca^{-1} \in P$, which, in turn, is equivalent to saying $a < c$. Also, if $x < y$, then $yx^{-1} \in P$. Thus, $xy^{-1} \in P^{-1}$, meaning $xy^{-1} \notin P$, by item 1., and

$y < x$ is false. Finally, $x \neq y$ implies $yx^{-1} \in P$ or $yx^{-1} \in P^{-1}$, from item 2., meaning either $x < y$ or $y < x$. It is, therefore, a total order relation in G.

Furthermore, from item 3., we have, assuming $a < b$, that $ba^{-1} \in P$ and, therefore, both $cba^{-1}c^{-1} \in P$, which is equivalent to saying $ca < cb$ and $bcc^{-1}a^{-1} \in P$, which is equivalent to $ac < bc$. Thus, G has an ordered group structure induced by P. ∎

This characterization of ordered groups makes it much easier to prove that a given group is ordered. Indeed, instead of searching for relations compatible with the group structure, all we have to do is find a subset of G with the preceding properties. In particular, as will become clear, this makes it easier to construct ordered groups from other ordered groups.

We illustrate this approach by proving that torsion-free abelian groups are ordered. We first note that every ordered group has to be torsion-free. Indeed, if $x \neq 1$ is a torsion element, either x or x^{-1} is greater than 1. Without loss of generality, suppose $x > 1$. Then, we'd have $1 < x < x^2 < \cdots < x^n = 1$, which is absurd.

Proposition 1.6.3. *Let G be an abelian group. Then, G is ordered if, and only if, G is torsion-free.*

Proof. From the preceding comment, we only have to check the "if" part. We follow the argument presented in [Fuc63]. Let $\mathscr{S} = \{S \subset G \mid S \text{ is multiplicatively closed and } 1 \notin S\}$. This set is non-empty if G is torsion-free, as, given $x \neq 1$, $S = \{x^n \mid n \in \mathbb{N}^\dagger\} \in \mathscr{S}$. Let $\{S_i\}$ be a chain in $\mathscr{S}$ (ordered by inclusion) and take $S = \bigcup_i S_i$. Since $1 \notin S_i, \forall i$, then $1 \notin S$. At the same time, if $x, y \in S$, there is some n such that $x, y \in S_n$. Therefore, $xy \in S_n \subset S$, which is to say $S \in \mathscr{S}$ is an upper bound for the chain.

Using Zorn's Lemma, take some maximal element $\mathfrak{P} \in \mathscr{S}$. By construction, it's multiplicatively closed. Let $1 \neq x \in G$, and suppose that $x \notin \mathfrak{P}, \mathfrak{P}^{-1}$. Then, the set $T_x = \mathfrak{P} \cup \{sx^n \mid s \in \mathfrak{P}, n \in \mathbb{N}^\dagger\} \cup \{x^n \mid n \in \mathbb{N}^\dagger\}$ properly contains $\mathfrak{P}$. Moreover, it's easy to check, using the fact that G is abelian, that it's multiplicatively closed. Using the maximality of $\mathfrak{P}$, this implies $1 \in T$. Since x is torsion-free and $1 \notin \mathfrak{P}$, then $1 = sx^n$, for some n, and $s \in \mathfrak{P}$. Therefore, $x^{-n} \in \mathfrak{P}$.

We can repeat the preceding paragraph using $x^{-1} \notin \mathfrak{P}$ instead of x, and we'd obtain some $m \in \mathbb{N}^\dagger$ such that $x^m \in \mathfrak{P}$. This implies $1 = (x^{-n})^m(x^m)^n \in \mathfrak{P}$, which is a contradiction. Ergo, if $x \neq 1$, then either $x \in \mathfrak{P}$, or $x \in \mathfrak{P}^{-1}$, and they're easily seen to be pairwise disjoint. Finally, G is abelian, so that $x^{-1}\mathfrak{P}x = \mathfrak{P}$. Using Proposition 1.6.2, G is ordered. ∎

Proposition 1.6.4. *Let G be a group and let $N \trianglelefteq G$ be central in G. If N and G/N are both ordered, then so is G.*

Proof. Let P_N and $P_{G/N}$ be the positive cones of N and G/N, respectively, and consider the set $P = \{x \in G \mid x \in P_N \text{ or } xN = \overline{x} \in P_{G/N}\}$. All we have to do is show that P satisfies the properties of a positive cone.

If $x, y \in P$, then there are three possibilities: either $x, y \in P_N$, in which case $xy \in P_N$ and, therefore, $xy \in P$; or $\overline{x}, \overline{y} \in P_{G/N}$, meaning $\overline{xy} \in P_{G/N}$ and, here too, $xy \in P$;

finally, without loss of generality, $x \in P_N$ and $\overline{y} \in P_{G/N}$. Since $P_N \subset N$, we get $\overline{x} = 1$, meaning $\overline{xy} = \overline{y} \in P_{G/N}$. Thus, in any case, $xy \in P$;

First, suppose $x \in N$. If $x \notin P$, then $x \notin P_N$. So either $x = 1$ or $x \in P_N^{-1}$. But it's easy to check that $P^{-1} = \{x \in G \mid x \in P_N^{-1}$ or $\overline{x} \in P_{G/N}^{-1}\}$. We thus obtain that $N = (P \cup \{1\} \cup P^{-1}) \cap N$. Furthermore, their union is disjoint, as can also be easily seen. Now suppose $x \notin N$. If $x \notin P$, then $\overline{x} \in P_{G/N}^{-1}$, so that $x \in P^{-1}$. Therefore, $G \setminus N = (P \cup \{1\} \cup P^{-1}) \cap (G \setminus N)$. Putting both of the results together, we prove the statement;

If $x \in P$, then either $x \in P_N$ or $\overline{x} \in P_{G/N}$. In the first case, $t^{-1}xt = x \in P_N \subset P$, since N is central. In the second case, $\overline{t^{-1}xt} = \overline{t}^{-1}\overline{x}\overline{t} \in P_{G/N}$. Thus, in any case, $t^{-1}xt \in P$, for all $t \in G$.

■

Proposition 1.6.5. *Let G be a residually torsion-free nilpotent group. Then, G is an ordered group.*

Proof. By Proposition 1.4.2, $\sqrt{\gamma_n}/\sqrt{\gamma_{n+1}}$ is a torsion-free abelian group for all n. Thus, by Proposition 1.6.3, it's an ordered group, and we can consider its positive cone P_n.

Consider the set $P = \{x \in G \setminus \{1\} \mid x \in \sqrt{\gamma_n} \setminus \sqrt{\gamma_{n+1}} \implies x\sqrt{\gamma_{n+1}} \in P_n\}$. Since G is residually torsion-free nilpotent, given $x \in G \setminus \{1\}$, there exists some $n_x \in \mathbb{N}^\dagger$ such that $x \in \sqrt{\gamma_{n_x}} \setminus \sqrt{\gamma_{n_x+1}}$. Let, then, $x, y \in P$ and $i, j \in \mathbb{N}^\dagger$ be such that $x \in \sqrt{\gamma_i} \setminus \sqrt{\gamma_{i+1}}$ and $y \in \sqrt{\gamma_j} \setminus \sqrt{\gamma_{j+1}}$. Without loss of generality, we can assume $i \leq j$.

If $i = j$, then $x\sqrt{\gamma_{i+1}}, y\sqrt{\gamma_{i+1}} \in P_i$, meaning $xy\sqrt{\gamma_{i+1}} \in P_i$, and it's then trivial that $xy \in P$. Now, if $i < j$, then $y \in \sqrt{\gamma_{i+1}}$, so that $xy\sqrt{\gamma_{i+1}} = x\sqrt{\gamma_{i+1}} \in P_i$. So, in any case, we have $xy \in P$, meaning P is multiplicatively closed.

By definition, $1 \notin P$. If $g \neq 1$ isn't in P, assume $g \in \sqrt{\gamma_i} \setminus \sqrt{\gamma_{i+1}}$, so that $g\sqrt{\gamma_{i+1}} \notin P_i$. Since $g \notin \sqrt{\gamma_{i+1}}$, then $g\sqrt{\gamma_{i+1}} \neq 1$. Therefore, by hypothesis, $g\sqrt{\gamma_{i+1}} \in P_i^{-1}$; that is, $g^{-1}\sqrt{\gamma_{i+1}} \in P_i$. It's trivial then that $g^{-1} \in \sqrt{\gamma_i} \setminus \sqrt{\gamma_{i+1}}$, and thus, $g^{-1} \in P$. This means $G = P \cup \{1\} \cup P^{-1}$. We can easily see that the unions are pairwise disjoint.

Finally, if $g \in P$ with $g \in \sqrt{\gamma_i} \setminus \sqrt{\gamma_{i+1}}$ and $x \in G$, then $x^{-1}gx = g[g, x]$. By Proposition 1.4.2, $[g, x] \in \sqrt{\gamma_{i+1}}$. Thus, $x^{-1}gx\sqrt{\gamma_{i+1}} = g\sqrt{\gamma_{i+1}} \in P_i$ and $x^{-1}Px \subset P$, concluding the proof. ■

In order to construct the Malcev-Neumann series rings, it will be necessary to establish the concept of a well-ordered set. Similarly to what is done for the natural numbers, we have the following definition:

Definition. Let G be an ordered group. A non-empty subset $S \subset G$ is said to be **well-ordered** if every non-empty $A \subset S$ contains a minimum element (i.e., an element y such that $y \leq x, \forall x \in A$).

Of course, G doesn't have to be a group for well-ordered subsets to be defined, or even to prove the ensuing couple of propositions. That said, our main interest is to use the group structure to construct some specific well-ordered subsets of G.

We first state the following important characterization, which will be freely used throughout the rest of the section.

Proposition 1.6.6. *Let G be an ordered group and let $S \subset G$ be non-empty. The following are equivalent:*

1. *S is well-ordered;*
2. *Every decreasing sequence in S is eventually constant;*
3. *Every sequence in S has an increasing subsequence;*

Proof. $\underline{(1) \implies (2)}$: Let (s_n) be a decreasing sequence in S and consider $A = \{s_n \mid n \in \mathbb{N}\}$ (A is the set of values attained by the sequence). Since S is well-ordered, there exists $\mu = \min A$. Let n_0 be the smallest natural number such that $s_{n_0} = \mu$. Then, since the sequence is decreasing, $s_{n_0} \geq s_n$, for all $n \geq n_0$. On the other hand, the minimality of μ yields $s_{n_0} = \mu \leq s_n$ for all $n \in \mathbb{N}$. Thus, $s_{n_0} = s_n$ for all $n \geq n_0$.

$\underline{(2) \implies (3)}$: Let (s_n) be an arbitrary sequence in S and suppose it doesn't have an increasing subsequence. Thus, for any given $n_0 \in \mathbb{N}$, there are only finitely many terms such that $s_{n_0} \leq s_n$; in particular, there are infinitely many terms such that $s_{n_0} > s_n$. So we can construct a strictly decreasing subsequence by taking the smallest n_1 such that $s_1 > s_{n_1}$ and, given n_k, we take n_{k+1} to be the smallest number such that $s_{n_k} > s_{n_{k+1}}$.

$\underline{(3) \implies (1)}$: Let $A \subset S$ be non-empty. If there's no minimum element in A, given $a \in A$, there exists $b \in A$ such that $b < a$. So, choosing an arbitrary $s_0 \in A$ to start with, we can construct a strictly decreasing sequence (s_n) of elements of A. Consider an increasing subsequence (s_{n_k}). On the one hand, $s_{n_0} \leq s_{n_k}$ for all $k \in \mathbb{N}$, and $n_k \geq n_0$ (with equality only if $k = 0$). On the other hand, $s_{n_0} > s_n$, for all $n > n_0$. By combining both inequalities, $s_{n_0} \leq s_{n_1}$ and $s_{n_0} > s_{n_1}$, a contradiction.

■

We now relate the group structure of G to its ordering and, most importantly, to its well-ordered subsets.

Proposition 1.6.7. *Let G be an ordered group and let $S, T \subset G$ be well-ordered subsets. Then, both $S \cup T$ and ST are well-ordered. Furthermore, given $u \in ST$, there exist a finite number of pairs $(s, t) \in S \times T$ such that $u = st$.*

Proof. First, let $A \subset S \cup T$ be non-empty. We can write $A = (A \cap S) \cup (A \cap T)$. If either of these is empty, then A is contained in either S or T, in which case the result follows from hypothesis. Otherwise, both $A \cap S$ and $A \cap T$ contain minimum elements x and y respectively. Without losing generality, we may assume $x \leq y$. Let $z \in A$. If $z \in S$, $x \leq z$. And, if $z \in T$, $x \leq y \leq z$. In any case, $x \leq z$, meaning x is a minimum element for A.

For the second statement, let $(s_i t_i)$ be a sequence in ST. Since S is well-ordered, there is an increasing subsequence (s_{n_i}) of (s_i); that is, $s_{n_i} \leq s_{n_{i+1}}$ for all i. Since T is well-ordered, we may find an increasing subsequence $(t_{n_{j_i}})$ of (t_{n_i}). Thus, $(s_{n_{j_i}} t_{n_{j_i}})$ is an increasing subsequence of $(s_i t_i)$, meaning ST is well-ordered.

Now suppose there exists $u \in ST$ such that $u = s_i t_i$, $s_i \neq s_j$ if $i \neq j$ (i.e., that there are (countably) infinitely many elements $s \in S$ such that $u = st$ for some t in T). Then, there exists a strictly increasing subsequence (s_{n_i}) of (s_i), using the fact that the original sequence is injective.

If $t_{n_i} < t_{n_{i+1}}$, then $u = s_{n_i} t_{n_i} < s_{n_{i+1}} t_{n_{i+1}} = u$, which is absurd. Hence, $t_{n_i} \geq t_{n_{i+1}}$ for all i. As T is also well-ordered, there exists some j such that $t_{n_i} = t_{n_j}$ for all $i \geq j$. This means $u = s_{n_j} t_{n_j} = s_{n_j} t_{n_i} < s_{n_i} t_{n_i} = u$, which is also a contradiction. Ergo, the set of $s \in S$ such that $u = st$ for some $t \in T$ must be finite. The same argument applied to T finishes the proof. ■

The following is the most important proposition in this section, and will be the crucial piece in proving that Malcev-Neumann series rings are division rings. Its proof is quite technical, as will soon become apparent, but there is a way around it, using the ideas of [Hig52].

The biggest issue with this alternative approach (which is why we've opted against it) is that it requires a lot of background knowledge, meaning we could either develop the relevant material here, detracting from our goal with a relatively small pay-off, or simply refer to [Hig52] for all the needed material, making the exposition very "top-down" and unclear.

That said, the reader who possesses the relevant background in universal algebra and on quasi-orderings will surely find the alternative proof a lot simpler.

Proposition 1.6.8. *Let G be an ordered group, P its positive cone and $S \subset P$ a well-ordered subset of P. Let $S^\infty = \bigcup_{n=1}^{\infty} S^n$. Then:*

1. *S^∞ is well-ordered;*
2. *If $u \in S^\infty$, then u belongs to a finite number of S^n;*

In order to prove this proposition, it'll be important to define an equivalence relation on P, the positive cone of G, and an order relation on the quotient set $\overline{P} = P/\sim$. We begin with the first one:

Definition. Let G be an ordered group and let P be its positive cone. The elements $x, y \in P$ are said to be **relatively archimedian** (notation: $x \sim y$) if there exist $m, n \in \mathbb{N}$ such that $x \leq y^m$ and $y \leq x^n$.

Proposition 1.6.9. *Let G be an ordered group and let P be its positive cone. Then, the relation $x \sim y$ is an equivalence relation and $\overline{x_1 \cdots x_n} = \overline{\max\{x_1, \dots, x_n\}}$. Moreover, in the quotient set $\overline{P}$, $\overline{x} < \overline{y} \iff x^n < y, \forall n \in \mathbb{N}$ defines a total order relation such that $x \leq y$ implies $\overline{x} \leq \overline{y}$.*

Proof. See [Lam01, Chapter 14]. ■

Proof of Proposition 1.6.8. **Part (1):** We'll proceed by contradiction. Suppose S^∞ isn't well ordered. Then, there exists a strictly decreasing sequence $u_1 > u_2 > \dots$ in S^∞, such that $u_i \in S^{n_i}$. In particular, in $\overline{P}$, $\overline{u_1} \geq \overline{u_2} \geq \dots$ and, by Proposition 1.6.9, $\overline{u_i} = \overline{s_i}$ for some $s_i \in S$.

Let $\mathfrak{S} = \{s_i\} \subset S$. Since S is well-ordered, $\mathfrak{S}$ has a minimum element s_k. Therefore, as $\overline{u_k} = \overline{s_k}$, then $\overline{u_k} \leq \overline{u_i}$ for all i, so that $\overline{u_k}$ is a minimum element in the decreasing sequence in $\overline{P}$.

<u>Statement 1</u>: There exists some strictly decreasing sequence in S^∞ whose minimal element in the sequence of equivalence classes in $\overline{P}$ is less than or equal to that of every other strictly decreasing sequence in S.

□ *Proof of Statement 1*: Let $(u_n)^\lambda, \lambda \in \Lambda$ be some strictly decreasing sequence in S^∞. Here, Λ denotes an indexing set of strictly decreasing sequences in S^∞. From the preceding argument, there is some $s_\lambda \in S$ such that $\overline{s_\lambda} = \min\{\overline{u_n}\}$. Consider the set $\{s_\lambda \mid \lambda \in \Lambda\} \subset S$. Since S is well-ordered, there exists a minimum element s_{λ_0} relative to this set. As $s_{\lambda_0} \leq s_\lambda$, then $\overline{s_{\lambda_0}} \leq \overline{s_\lambda}$, for all $\lambda \in \Lambda$. This finishes the proof of this statement. □

For the remainder of the proof, we'll denote the minimal equivalence class given by Statement 1 (that is, minimal relative to all the minimal classes of all the decreasing sequences of S^∞) by μ. We know that $\{s \in S \mid \overline{s} = \mu\}$ is non-empty. By the well-ordering of S, there is some minimal element, s_μ, in this set. By definition, for each $u \in S^\infty$ with $\overline{u} = \overline{s_\mu} = \mu$, there's some $m_u \in \mathbb{N}$ such that $u \leq s_\mu^{m_u}$.

<u>Statement 2</u>: There's a strictly decreasing sequence (u_n) in S^∞, whose induced sequence of equivalence classes is constant and equal to μ, such that the smallest $m \in \mathbb{N}$ with $u_1 \leq s_\mu^m$ is smaller than that of all other strictly decreasing sequences in S with constant class sequence μ.

□ *Proof of Statement 2*: Let $(u_n)^\lambda, \lambda \in \Lambda$ be a strictly decreasing sequence in S^∞ with minimal class μ and $\overline{u_1} = \mu$.

For those sequences, $\overline{u_1} = \overline{s_\mu}$, meaning there is $m_\lambda \in \mathbb{N}$ such that $u_1 \leq s_\mu^{m_\lambda}$. Consider the set $\{m_\lambda \mid \lambda \in \Lambda\} \subset \mathbb{N}$. The well-ordering of the natural numbers gives us some minimum element $m = m_{\lambda_0}$. The sequence $(u_n)^{\lambda_0}$ satisfies the hypotheses of Statement 2. □

For the remainder of the proof, we fix a strictly decreasing sequence (u_n) in S^∞ such that $\overline{u_1} = \overline{u_2} = ... = \mu$ and such that the value m so $u_1 \leq s_\mu^m$ is as small as possible. This can be done by Statement 2. Notice that, since S is well-ordered and (u_n) is strictly decreasing, it can't contain a subsequence in S. Thus, save for a finite number of terms, we have:

$$u_n = \begin{cases} v_n s_n & v_n \in S^\infty, s_n \in S \\ s_n w_n & w_n \in S^\infty, s_n \in S \\ v_n s_n w_n & v_n, w_n \in S^\infty, s_n \in S \end{cases}$$

where, if $u_n = s_1 \cdots s_{i_n}$, we define $s_n = \max\{s_1, ..., s_{i_n}\}$ (i.e, we have decomposed the word defining u_n into its maximum letter and (potentially empty) sub-words on each side. In particular, $\mu = \overline{u_n} = \overline{s_n}$). At least one of the above three cases must occur an infinite number of times. Without loss of generality, we'll assume its the third one (the others follow similar lines).

Consider a subsequence (u_{n_i}) of (u_n) such that $u_{n_i} = v_{n_i} s_{n_i} w_{n_i}$ for all $i \in \mathbb{N}^\dagger$. For convenience, we'll denote $v_{n_i} = v_i$ and the same for the other two sub-words. Let $B = \{v_i \mid i \in \mathbb{N}^\dagger\}, C = \{w_i \mid i \in \mathbb{N}^\dagger\}, D = \{s_i \mid i \in \mathbb{N}^\dagger\}$. Since every term of (u_{n_i}) belongs to BDC, this can't be well-ordered (since the sequence is strictly decreasing). Given that $D \subset S$, it has to be well-ordered, meaning either B or C isn't. Let's assume its B (again, the other case is identical).

Let, then, $v_{k_1} > v_{k_2} > \dots$ be a strictly decreasing subsequence in B. As $S^\infty \subset P$, $v_{k_i} < u_{n_{k_i}}$ for all i. In particular, $\overline{v_{k_i}} = \mu$ for all i, by the minimality of μ. By the minimality of s_μ, we have $v_{k_i} s_\mu \leq v_{k_i} s_{k_i}$ and, therefore, $v_{k_1} s_\mu < u_{k_1} \leq s_\mu^m$. Thus, $v_{k_1} < s_\mu^{m-1}$, which contradicts the minimality of m, given that the sequence (v_{k_i}) satisfies the hypotheses of Statement 2. This concludes the first part of the proof.

Part 2: Suppose $u \in S^\infty$ belongs to an infinite number of S^n. By the first part, S^∞ is well-ordered, meaning there exists a smallest u with this property. Then, we can write $u = s_{i1} s_{i2} \cdots s_{in_i}$, where $2 \leq n_1 < n_2 < \dots$.

By Proposition 1.6.7, u can only be written as a product of elements of S and S^∞ in a finite number of ways. Thus, some of the s_{i1} repeats infinitely many times. But, then, we'd get some i such that $(s_{i2} \dots s_{in_i})$ belongs to infinitely many S^n (we only have to consider the smallest i such that s_{i1} appears infinitely many times). And, since $S \subset P$, this element is smaller than u, contradicting its minimality. ■

Chapter 2

Some classes of rings

With most of the group theoretic results out of the way, we now turn our attention to the construction of some classes of rings, focusing on those that will give rise to important division ring constructions further on.

2.1 Ore rings

Constructing fields from integral domains is a relatively simple task - indeed, we can associate every integral domain to its field of fractions, which is, in some sense, the smallest field containing it. Unfortunately, when it comes to noncommutative rings, the same construction can't always be replicated. The rings for which we can construct a sort of "noncommutative field of fractions" which behaves in a similar manner to their commutative counterparts deserve special attention, and will be the focus of our efforts for this section, which roughly follows [Lam99] and [Coh03].

Definition. Let R be a ring and let $S \subset R^\dagger$ be a *multiplicative submonoid* (i.e., a subset of $R^\dagger$ which is closed for multiplication and contains 1). A ring R' is called a **right ring of fractions** (relative to S) for R if there exists a homomorphism $\varphi : R \longrightarrow R'$ such that:

- $\varphi(S) \subset \mathfrak{U}(R')$;
- Every element of R' can be written as $\varphi(r)\varphi(s)^{-1}$, for $r \in R, s \in S$;
- $\ker(\varphi) = \{r \in R \mid \exists s \in S \text{ such that } rs = 0\}$;

Definition. A **right denominator set** for a ring R is a multiplicative submonoid S satisfying:

- For all $a \in R$ and $s \in S$, $aS \cap sR \neq \emptyset$;
- If $a \in R$ and $s \in S$ are such that $sa = 0$, then $\exists s' \in S$ such that $as' = 0$;

A set satisfying the first of the two conditions above is called **right permutable** and a set satisfying the second one is called **right reversible**. It turns out, as can be inferred by the name, that those are exactly the two conditions required of S for a right ring of fractions to exist, essentially copying the proof of the existence of commutative localization.

Proposition 2.1.1. *A ring R admits a right ring of fractions relative to the submonoid $S \subset R$ if, and only if, S is a right denominator set for R.*

Proof. Let S be a right denominator set for a ring R. Define, on the set $R \times S$, the following relation:

$$(a, s) \sim (b, t) \iff \text{there exist } u_1, u_2 \in R \text{ such that } su_1 = tu_2 \in S \text{ and } au_1 = bu_2$$

It's trivial that the relation defined thus is both reflexive and symmetric. As for transitivity, suppose that $(a, s) \sim (b, t)$ and that $(b, t) \sim (c, r)$. Then, there are $u_1, u_2, v_1, v_2 \in R$ such that $su_1 = tu_2 \in S$, $tv_1 = rv_2 \in S$, $au_1 = bu_2$, and $bv_1 = cv_2$, .

Since S is right permutable, $(tu_2)S \cap (tv_1)R \neq \emptyset$. Thus, there exist $w \in S$ and $d \in R$ such that $tu_2w = tv_1d$; that is, $t(u_2w - v_1d) = 0$. Now, S is right reversible and $t \in S$, meaning there exists $t' \in S$ such that $(u_2w - v_1d)t' = 0$. From the preceding equalities, this then implies:

$$su_1w = tu_2w = tv_1d = rv_2d$$

and, in turn, we get

$$s(u_1wt') = r(v_2dt'), \text{ with } u_1wt' = v_2dt' \in S$$

At the same time, the previous equalities also yield

$$a(u_1wt') = bu_2wt' = bv_1dt' = c(v_2dt')$$

This finishes the proof of transitivity. We can now consider the quotient set $RS^{-1} := (R \times S)/\sim$, where we'll denote the class of the element (a, s) by either a/s or as^{-1}. We now need to show that this set is indeed a right ring of fractions for R relative to S.

We define the operations in RS^{-1} as follows:

- Addition: If $a_1/s_1, a_2/s_2 \in RS^{-1}$, since S is right permutable, $s_1S \cap s_2R \neq \emptyset$. Thus, there exist $t \in S$, $b \in R$ such that $s_1t = s_2b \in S$. We now define the sum of a_1/s_1 and a_2/s_2 as follows:
$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1t + a_2b}{s_2b}$$

- Multiplication: If $a_1/s_1, a_2/s_2 \in RS^{-1}$, since S is right permutable, $a_2S \cap s_1R \neq \emptyset$. Therefore, there exist $t \in S$, $b \in R$ such that $a_2t = s_1b$. We now define the product of a_1/s_1 and a_2/s_2 as follows:
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1b}{s_2t}$$

Verifying that both are well-defined is tedious, but straightforward. It's also worth emphasizing that the definition of the product of two elements was the first time thus far in which we used right permutability where one of the elements wasn't necessarily in S.

Checking that the operations defined above indeed endow RS^{-1} with the structure of a ring is very tedious, and will be omitted. The most important is to highlight that 0/1 is its zero element and that $1/1$ is its unity. All that's left is to check that it's a right ring of fractions for R relative to S.

- Let $\varphi : R \longrightarrow RS^{-1}$ be the function defined by $\varphi(a) = a/1$. Since $1 \in S$, we can take $t = b = 1$ in the definition of the sum of two fractions. We then have that, if $a_1, a_2 \in R$, $\varphi(a_1 + a_2) = (a_1 + a_2)/1 = a_1/1 + a_2/1 = \varphi(a_1) + \varphi(a_2)$.

  Furthermore, now taking $t = 1$ and $b = a_1$, then $\varphi(a_1a_2) = (a_1a_2)/1 = a_1/1 \cdot a_2/1 = \varphi(a_1)\varphi(a_2)$. Thus, the function φ is a ring homomorphism. Moreover, if $s \in S$, $\varphi(s) = s/1$, and $s/1 \cdot 1/s = s/s = 1/1$, by taking $t = s$ and $b = 1$. This means $\varphi(S) \subset \mathfrak{U}\left(RS^{-1}\right)$.

- This item is immediate by a simple computation: if $s \in S$, then $(s/1)^{-1} = 1/s$, meaning $a/s = a/1 \cdot (s/1)^{-1} = \varphi(a)\varphi(s)^{-1}$, performing the computations as before.

- Notice that $a/1 = 0/1$ if and only if there exists $s \in S$ such that $as = 0$. Thus, the kernel of φ is the set $\{a \in R \mid \exists s \in S \text{ such that } as = 0\}$, as was desired.

Therefore, RS^{-1} is a right ring of fractions for R relative to S.

For the converse, suppose R' is a right ring of fractions for R relative to S and let $\varphi : R \longrightarrow R'$ be the associated ring homomorphism. Then:

- Given $a \in R$ and $s \in S$, there exist $r \in R$ and $s' \in S$ such that $\varphi(s)^{-1}\varphi(a) = \varphi(r)\varphi(s')^{-1}$ (by the first two properties of a right ring of fractions). We now get that $\varphi(as') = \varphi(sr)$, meaning $as' - sr \in \ker(\varphi)$. By the third property, there exists some $s'' \in S$ with $(as' - sr)s'' = 0$, meaning $as's'' = srs'' \in aS \cap sR$.

- Finally, if $sa = 0$, for $a \in R$, $s \in S$, then $\varphi(sa) = 0$, meaning $\varphi(a) = 0$, since $\varphi(s) \in \mathfrak{U}(R')$. Ergo, there exists $s' \in S$ such that $as' = 0$.

■

Corollary 2.1.1.1. *Let R be a ring and let RS^{-1} be a right ring of fractions of R relative to S. Consider $\varphi : R \longrightarrow RS^{-1}$ the homomorphism $a \mapsto a/1$. Then, for all rings T and for all homomorphisms $f : R \longrightarrow T$ with $f(S) \subset \mathfrak{U}(T)$, there's a unique ring homomorphism $\Phi : RS^{-1} \longrightarrow T$ such that $\Phi \circ \varphi = f$. In particular, any two right rings of fractions of R relative to S are isomorphic.*

Proof. Let $\Phi : RS^{-1} \longrightarrow T$ be given by $\Phi(a/s) = f(a)f(s)^{-1}$. This mapping is well-defined, since $a/s = b/t$ if and only if there exist $u, v \in R$ such that $au = bv$ and $su = tv \in S$. Then, $f(s), f(su) \in \mathfrak{U}(T)$, meaning $f(u) \in \mathfrak{U}(T)$. Thus:

$$\Phi(a/s) = f(a)(f(u)f(u)^{-1})f(s)^{-1} = f(au)f(su)^{-1} = f(bv)f(tv)^{-1} = \Phi(b/t)$$

It's straightforward to verify that Φ is a ring homomorphism. Moreover, $\Phi(a/1) = f(a)f(1)^{-1} = f(a)$, meaning $\Phi \circ \varphi = f$. And it's unique, as can be easily seen. ■

Evidently, there are leftward analogues for the constructions we have described above, whose result would be a **left ring of fractions** $S^{-1}R$, for which $ta/ts = a/s$ for all $t \in S$. Should both exist (that is, should S be both a left and right denominator set), then the left/right distinction becomes irrelevant, as we see below.

Corollary 2.1.1.2. *Let S be both a left and right denominator set for a ring R. Then, $S^{-1}R \cong RS^{-1}$.*

Corollary 2.1.1.3. *Let R be a domain and let $S = R^{\dagger}$. Then, there exists a right ring of fractions of R relative to S if and only if $aR \cap bR \neq \{0\}$, for all $a, b \in S$.*

Proof. Evidently, S is always right (and left) reversible, since R doesn't contain any zero-divisors. Thus, first suppose that S is right permutable and let $r, s \in S$. Then, $rt = sa$ for some $a \in R, t \in S$. And, since R is a domain, $rt \neq 0$. This means $rR \cap sR \neq \{0\}$.

On the other hand, if $sR \cap tR \neq \{0\}$, where $s, t \in S$, let $a \in R$. If $a = 0$, $aS \cap sR = \{0\} \neq \emptyset$. And, if $a \neq 0$, then $a \in S$. Thus, by hypothesis, there exist b, t such that $ab = st \neq 0$. As $ab \neq 0$, $b \neq 0$. Ergo, $b \in S$ and, as such, $aS \cap sR \neq \emptyset$. ∎

Recall that an element of a ring is said to be **regular** if it's not a zero divisor.

Definition. A ring R is said to be a **right Ore ring** if the set of all regular elements of R is a right denominator set for R (that is, if this set is right permutable, since reversibility is automatic in this case).

The condition described in Corollary 2.1.1.3 is known as the **right Ore condition**. Thus, the corollary may be rephrased as "a domain is right Ore if and only if it satisfies the right Ore condition". Moreover, in this case, its right ring of fractions relative to $S = R^{\dagger}$ is a division ring, called its **total classical field of fractions**. Corollary 2.1.1.3 also allows us to prove the following:

Corollary 2.1.1.4. *Let R be a domain. Then, R is either right Ore, or it contains a right ideal which is a free right R-module of infinite rank. In particular, every right Noetherian domain is right Ore.*

Proof. Suppose R isn't right Ore and let $a, b \in R^{\dagger}$ be such that $aR \cap bR = \{0\}$. We shall show that $\{a^j b \mid j \in \mathbb{N}\}$ is R-linearly independent. Suppose $\sum a^j br_j = 0$. Then, $br_0 + a(\sum_{j\geq 1} a^{j-1} br_j) = 0$. By hypothesis, since $br_0 = -a(\sum_{j\geq 1} a^{j-1} br_j)$, $br_0 = 0$ and, therefore, $r_0 = 0$.

But, then, $a(\sum_{j\geq 1} a^{j-1} br_j) = 0$. Since R is a domain and $a \neq 0$, $\sum_{j\geq 1} a^{j-1} br_j = 0$. We can now use an inductive argument to obtain that $r_j = 0$ for all j. Thus, R contains the right ideal $\bigoplus_{j\geq 0} a^j bR$, which is a free R-module of infinite rank. ∎

2.2 Skew polynomial rings

A pretty general construction which allows us to obtain many different division rings through Ore localization is that of the so-called "skew polynomial rings" (see [Lam01] and [Coh03]). In order to define them, we first need the following concept:

Definition. Let R be a ring and let $\alpha : R \longrightarrow R$ be a ring homomorphism. A (left) α-**derivation** is an additive function $\delta : R \longrightarrow R$ such that $\delta(ab) = \delta(a)b + \alpha(a)\delta(b)$. If $\alpha = \mathrm{id}_R$, then δ is simply called a **derivation**.

Definition. Let R be a ring, let $\alpha : R \longrightarrow R$ be a ring homomorphism and let $\delta : R \longrightarrow R$ be an α-derivation. A **skew polynomial ring** defined by α and δ over R, $S = R[x; \alpha, \delta]$, is a ring such that:

1. R is a subring of S;
2. There exists $x \in S$ such that S is a free left R-module, with basis $\{1, x, x^2, ...\}$;
3. $xr = \alpha(r)x + \delta(r)$, for all $r \in R$;

As usual, it is important for us to verify that skew polynomial rings actually exist. This could be done "from the ground up", by explicitly defining operations on a set and verifying the ring axioms (this is done in [Lam01], albeit without the tedious computations), but checking associativity is far from easy. Alternatively, we can look at known rings and find a subring which agrees with the definition we've laid out. This is done, for instance, in [Coh03], and is the approach we follow here.

Proposition 2.2.1. *Let R be a ring, let $\alpha : R \longrightarrow R$ be a ring homomorphism and let $\delta : R \longrightarrow R$ be an α-derivation. Then, there exists a skew polynomial ring defined by α and δ over R.*

Proof. Let $E = \operatorname{End}_{\mathbb{Z}} R[t]$ be the ring of endomorphisms of the (standard) polynomial ring $R[t]$ as an abelian group. We can define a faithful representation of R via:

$$\begin{aligned} \lambda : R &\longrightarrow E \\ r &\longmapsto \lambda_r : R[t] \longrightarrow R[t] \\ &\qquad\qquad p(t) \longmapsto rp(t) \end{aligned}$$

Since α and δ are both additive, we define $x \in E$ such that:

$$x\left(\sum_j r_j t^j\right) = \sum_j \alpha(r_j)t^{j+1} + \delta(r_j)t^j$$

Let, then, S be the subring of E generated by $\lambda(R)$ and x. From now on, we'll identify a and λ_a. If $a \in R$ and $p(t) = \sum_j r_j t^j$, we get:

$$\begin{aligned} (xa)(p(t)) &= \sum_j \alpha(ar_j)t^{j+1} + \delta(ar_j)t^j \\ &= \alpha(a)\left(\sum_j \alpha(r_j)t^{j+1} + \delta(r_j)t^j\right) + \sum_j \delta(a)r_j t^j \\ &= \alpha(a)(x(p(t))) + \delta(a)(p(t)) \\ &= (\alpha(a)x + \delta(a))(p(t)) \end{aligned}$$

In other words, $xa = \alpha(a)x + \delta(a)$ for all $a \in R$. In particular, $xR \subset Rx + R$. Using induction, we can easily check that $x^j R \subset Rx^j + Rx^{j-1} + \cdots + R$. This implies

$$\left(\sum_i Rx^i\right)\left(\sum_j Rx^j\right) = \sum_{i,j} Rx^i Rx^j \subset \sum_{i,j}\left(Rx^{i+j} + \cdots + Rx^j\right) \subset \sum_i Rx^i$$

and, in particular, $\sum_i Rx^i$ is a subring of E containing S (as it contains R and x). At the same time, it's also clear that S contains every element of $\sum_i Rx^i$, meaning the inclusion is, in fact, an equality. Thus, S is a R-submodule of E generated by $\{1, x, x^2, \ldots\}$. All that's left is to check that these elements are R-LI.

From the definition of x, $x(t^i) = t^{i+1}$ for all $i \in \mathbb{N}$. In particular, $x^j(1) = t^j$. Ergo, if $\sum a_i x^i = 0$, where $a_i \in R$, then:

$$0 = \left(\sum_i a_i x^i\right)(1) = \sum_i a_i t^i \implies a_i = 0, \forall i$$

which concludes the proof. ■

Similarly to what happens to the standard polynomial rings over a ring R, their skew analogues also satisfy a universal property.

Proposition 2.2.2. *Let R be a ring, $\alpha : R \longrightarrow R$ be a ring homomorphism and let $\delta : R \longrightarrow R$ be an α-derivation. Let T be a ring and let $\phi : R \longrightarrow T$ be a ring homomorphism such that $y\phi(a) = \phi(\alpha(a))y + \phi(\delta(a))$ for some $y \in T$. Then, there exists a unique ring homomorphism $\psi : R[x; \alpha, \delta] \longrightarrow T$ such that $\psi|_R = \phi$ and $\psi(x) = y$.*

Proof. Let $\psi\left(\sum_i r_i x^i\right) = \sum_i \phi(r_i) y^i$. It's trivial to check that ψ is well-defined, additive and that $\psi(1) = 1$. Let $q(x) = \sum b_j x^j$. We get:

$$\begin{aligned} \psi(xq(x)) &= \psi\left(\sum_j \alpha(b_j)x^{j+1} + \delta(b_j)x^j\right) \\ &= \sum_j \phi(\alpha(b_j))y^{j+1} + \phi(\delta(b_j))y^j \\ &= y\left(\sum_j \phi(b_j)y^j\right) \\ &= \psi(x)\psi(q(x)) \end{aligned}$$

Using induction, we can extend the result to $\psi(x^i)\psi(q(x)) = \psi(x^i q(x))$. Thus, it's immediate that, for all $p(x) \in R[x; \alpha, \delta]$, $\psi(p(x)q(x)) = \psi(p(x))\psi(q(x))$. The uniqueness of ψ is clear. ■

If the underlying ring of a skew polynomial ring happens to be a division ring, we have a noncommutative analogue of the Euclidean algorithm for standard polynomials.

Proposition 2.2.3. *Let D be a division ring, let $\alpha : D \longrightarrow D$ be a ring homomorphism and let $\delta : D \longrightarrow D$ be an α-derivation. Then, given $p(x), q(x) \in D[x; \alpha, \delta]$, $q(x) \neq 0$, there exist unique $d(x), r(x) \in D[x; \alpha, \delta]$, with either $r(x) = 0$ or $\partial r(x) < \partial q(x)$, such that $p = dq + r$. Furthermore, if α is surjective, then there exist unique $d'(x), r'(x) \in D[x; \alpha, \delta]$ such that $p = qd' + r'$ and either $r'(x) = 0$ or $\partial r'(x) < \partial q(x)$.*

Proof. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{j=0}^{m} b_j x^j$, with $b_m \neq 0$. If $n < m$, we need only take $r = p$ and $d = 0$. Otherwise, a straightforward computation yields $a_n x^n = a_n \alpha^{n-m}(b_m^{-1}) x^{n-m} b_m x^m + k(x)$, in which $k(x)$ is either 0 or has degree strictly less than n. Thus, if $f(x) = p(x) - a_n \alpha^{n-m}(b_m^{-1}) x^{n-m} q(x)$, then either $f = 0$ or $\partial f(x) < n$. Applying an inductive argument, we obtain the desired d, r.

If $p = dq + r = d'q + r'$, then $(d - d')q + (r - r') = 0$. As D is a domain and α is injective, the degree of the first term (if it's nonzero) is at least that of q, while the second term (also, if it's nonzero) has degree strictly less than that of q This forces $d = d'$ and $r = r'$.

If α is surjective, then so is α^j, for all j. In particular, there exists some $c \in D$ such that $\alpha^m(c) = b_m^{-1} a_n$. We then get $a_n x^n = b_m x^m c x^{n-m} + k(x)$, where $k(x)$ is either 0 or has degree strictly less than n. Again, using induction and the previous uniqueness argument, we get the result. ∎

Corollary 2.2.3.1. *In the conditions of Proposition 2.2.3, every left ideal of $D[x; \alpha, \delta]$ is principal. If α is surjective, then every right ideal of $D[x; \alpha, \delta]$ is also principal. In particular, $D[x; \alpha, \delta]$ is left Noetherian (and right Noetherian if α is surjective).*

Even though $R[x; \alpha, \delta]$ isn't generally a principal left ideal ring, the last part of Corollary 2.2.3.1 is still valid if R is left Noetherian (or right Noetherian, depending on the case) and the endomorphism α is bijective. These are the contents of the following result:

Theorem 2.2.4 (Hilbert's Basis Theorem for skew polynomial rings)**.** *Let R be a ring, let $\alpha : R \longrightarrow R$ be an automorphism and let $\delta : R \longrightarrow R$ be an α-derivation. If R is right (respectively, left) Noetherian, then so is $R[x; \alpha, \delta]$.*

Proof. First, we note that it's sufficient to prove only the right Noetherian case (for the left analogue, we only have to use the fact that $R[x; \alpha, \delta]^{op} = R^{op}[x; \alpha^{-1}, -\delta\alpha^{-1}]$ and the result becomes an immediate corollary). Let I be a right ideal of $R[x; \alpha, \delta]$ and define $J = \{r \in R \mid rx^d + \cdots + r_0 \in I \text{ for some } d \text{ and } r_{d-1}, ..., d_0 \in R\}$ (i.e., J is the set of the leading coefficients of the polynomials in I).

Since I is a right ideal of $R[x; \alpha, \delta]$, if $rx^d + \cdots + r_0 \in I$, then $rx^{d+k} + \cdots + r_0 x^k \in I$. Thus, it's easy to see that J is an additive subgroup of R. Furthermore, as α is an automorphism, given $a \in R$, $rx^d \alpha^{-d}(a) + \cdots + r_0 \alpha^{-d}(a) \in I$. The leading term of this polynomial, when we shift the coefficients from right to left, is rax^d, meaning that $ra \in J$ for all $r \in J, a \in R$. Therefore, J is a right ideal of R.

As R is right Noetherian, J is finitely generated. This means we can write $J = r_1 R + \cdots + r_k R$ for some $r_i \in R$. Let $p_i(x) \in I$ be polynomials with leading coefficients r_i (which exist, from the definition of J). Consider $n = \max\{\partial p_i\}$. Thus, $q_i(x) = p_i(x) x^{n - \partial p_i}$ are elements of I of degree n and leading coefficient r_i.

In the proof of Proposition 2.2.1, we saw that $\sum_{i=0}^{n-1} Rx^i = \sum_{i=0}^{n-1} x^i R$ (indeed, we only saw one inclusion, but the other one follows from the fact that α is bijective). Thus, if we define $N = \sum_{i=0}^{n-1} Rx^i$, then N is a right R-module and, therefore, as R is right Noetherian, so is N. This means $N \cap I$ is a finitely generated right R-module. Suppose, then, that it's generated by $f_1, ..., f_t$.

Let $I_0 = \sum_{i=1}^{k} q_k R + \sum_{j=1}^{t} f_t R$. If $p \in I$ has degree less then n, then $p \in N \cap I$, meaning $p \in I_0$. And if p has degree $m \geq n$, we can assume, inductively, that every polynomial in I with degree less then m is in I_0. Using the definition of J, we write:

$$p(x) = rx^m + \cdots + a_0, \text{ where } r = r_1 b_1 + \cdots + r_k b_k, \text{ for some} b_1, ..., b_k \in R$$

As q_i has leading coefficient r_i, it's easy to see that $q_i \alpha^{-n}(b_i)$ has leading coefficient $r_i b_i$. Now defining $q(x) = \sum_i q_i(x)\alpha^{-n}(b_i)x^{m-n}$, we obtain $\partial(p - q) < m$ and $p - q \in I$. By hypothesis, then, $p - q \in I_0$. But $q \in I_0$ by construction, implying $p \in I_0$. This yields $I = I_0$, which is finitely generated, finishing the proof. ■

Corollary 2.2.4.1. *If R is a right (resp. left) Noetherian domain, $\alpha : R \longrightarrow R$ is an automorphism and $\delta : R \longrightarrow R$ is an α-derivation, then $R[x; \alpha, \delta]$ is a right (resp. left) Ore domain.*

Proof. All that's left is to prove that $R[x; \alpha, \delta]$ is a domain, due to Theorem 2.2.4 and Corollary 2.1.1.4. But, if $p(x) = a_m x^m + \cdots + a_0$ and $q(x) = b_n x^n + \cdots + b_0$ are two nonzero polynomials, we get $p(x)q(x) = a_m \alpha^m(b_m)x^{m+n} + k(x)$, where $k(x)$ is either 0 or has degree strictly less than $m + n$. Since α is injective and R is a domain, we get the result. ■

Actually, the Corollary 2.2.4.1 is still valid under the hypothesis that R is a right Ore domain. That said, for the purposes of this work, the version we have presented will be sufficient. Another important corollary is the following result taken from [Pas14]:

Corollary 2.2.4.2. *Let S be a ring, let R be a right Noetherian subring of S and let $x \in S$ be invertible. Suppose $x^{-1}Rx = R$ and $S = R[x, x^{-1}]$. Then, S is right Noetherian.*

Proof. It's trivial to check, using $x^{-1}Rx = R$ and the logic of Proposition 2.2.1, that $S = \left\{ \sum_{i=-m}^{n} r_i x^i \mid m, n \in \mathbb{N} \right\}$. Let S^+ be the subring of S generated by R and x. If $r \in R$, then $xr = (xrx^{-1})x$. And of course $\sigma : R \longrightarrow R$ defined by $\sigma(r) = xrx^{-1}$ is an automorphism of R. Ergo, $S^+ = R[t; \sigma]/J$, where J is some ideal, using the universal property of the skew polynomial ring[1]. In particular, S^+ is right Noetherian.

If I is a right ideal of S, $I^+ = I \cap S^+$ is a right ideal of S^+ and, therefore, $I^+ = s_1 S^+ + \cdots + s_k S^+$. If $s \in S$, there's some $m \in \mathbb{N}$ such that $sx^m \in S^+$. In particular, the same is true if $s \in I$, so that $sx^m = \sum_i s_i b_i$ for some $b_i \in S^+$. This yields $s = \sum_i s_i(b_i x^{-m}) \in s_1 S + \cdots + s_k S$. Thus, $I = s_1 S + \cdots + s_k S$ is finitely generated, concluding the proof. ■

2.3 Group rings

Roughly speaking, a group ring over a ring R is a free R-module that admits a group as a basis, hence inducing a multiplication and ring structure in the underlying module. Even though they're subjected to intense study in their own right, we'll focus on the group rings which may be embedded in division rings, mostly following the ideas laid out in [Pas14], [Lam01] and [MS02].

[1] Here, we took the derivation to be the "zero derivation"; the function $\delta(a) = 0$ for all a.

Before giving a more precise definition of group rings, we establish a bit of notation. If G and H are abelian groups (written additively) and $f : G \longrightarrow H$ is a function, the **support** of f, denoted supp(f), is the set $\operatorname{supp}(f) = \{x \in G \mid f(x) \neq 0\}$.

Definition. Let R be a ring and let G be a group. The **group ring**[2] of G over R is the set $RG = \{\alpha : G \longrightarrow R \mid \operatorname{supp}(\alpha) \text{ is finite}\}$, where we denote an element $\alpha \in RG$ by $\alpha = \sum \alpha(g)g = \sum \alpha_g g$, together with the operations

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} \alpha_g \beta_h gh = \sum_{k\in G} \gamma_k k, \text{ where } \gamma_k = \sum_{gh=k} \alpha_g \beta_h = \sum_{g\in G} \alpha_g \beta_{g^{-1}k}$$

We remark that, in the definition of the product of two elements of RG we've written a few equalities. It's straightforward to check that $\sum_{g,h\in G} \alpha_g\beta_h gh = \sum_{k\in G} \gamma_k k$ (for the γ_k as in the definition), meaning either one can be taken as the definition.

Notice that the mapping $\iota : R \longrightarrow RG$ such that $\iota(x) = x1$ is an injective ring homomorphism and the mapping $j : G \longrightarrow \mathfrak{U}(RG)$ such that $j(g) = 1g$ is an injective group homomorphism. So, we can view R as a subring of RG and G, as a subgroup of $\mathfrak{U}(RG)$. Using these identifications, group rings satisfy the following universal property:

Proposition 2.3.1. *Let R be a ring and G be a group. Then, given a ring S, a ring homomorphism $\varphi : R \longrightarrow S$ and a group homomorphism $\psi : G \longrightarrow \mathfrak{U}(S)$, there exists a unique ring homomorphism $\Psi : RG \longrightarrow S$ such that $\Psi|_R = \varphi$ and $\Psi|_G = \psi$.*

Proof. Suppose $\Psi : RG \longrightarrow S$ satisfies the conditions outlined in the statement of the proposition. Then, we get

$$\Psi\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \Psi(\alpha_g g) = \sum_{g\in G} \Psi(\alpha_g 1)\Psi(1g) = \sum_{g\in G} \varphi(\alpha_g)\psi(g)$$

showing that, if such a homomorphism exists, it is unique.

Now take that to be the definition of a function $\Psi : RG \longrightarrow S$. It is well-defined, as each element of RG can be expressed uniquely in the form $\sum_{g\in G} \alpha_g g$ (this follows from the usual definition of equality of functions). Furthermore, it is clear that $\Psi(1) = 1$ and that Ψ restricts to φ on R and to ψ on G. Finally

$$\begin{aligned}\Psi\left(\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g\right) &= \sum_{g\in G} \varphi(\alpha_g + \beta_g)\psi(g) \\ &= \sum_{g\in G} \varphi(\alpha_g)\psi(g) + \varphi(\beta_g)\psi(g) = \Psi\left(\sum_{g\in G} \alpha_g g\right) + \Psi\left(\sum_{g\in G} \beta_g g\right)\end{aligned}$$

[2] Whenever R is commutative, we may use the terms "group ring" and "group algebra" interchangeably.

and

$$\begin{aligned}\Psi\left(\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right)\right) &= \sum_{k\in G}\varphi(\gamma_k)\psi(k)\\ &= \sum_{k\in G}\varphi\left(\sum_{gh=k}\alpha_g\beta_h\right)\psi(k)\\ &= \sum_{k\in G}\sum_{gh=k}\varphi(\alpha_g)\varphi(\beta_h)\psi(k)\\ &= \left(\sum_{g\in G}\varphi(\alpha_g)\psi(g)\right)\left(\sum_{h\in G}\varphi(\beta_h)\psi(h)\right)\\ &= \Psi\left(\sum_{g\in G}\alpha_g g\right)\Psi\left(\sum_{h\in G}\beta_h h\right)\end{aligned}$$

meaning Ψ is a well-defined ring homomorphism, finishing the proof. ■

It will be important to relate the group ring RG with $R[G/N]$, where N is a normal subgroup of G. The main tool in this relationship is a special ideal of RG, which we define next.

Definition. Let G be a group, let R be a ring and let $N \trianglelefteq G$. The **augmentation ideal** Δ**(G, N) of G relative to N** is the kernel of the homomorphism:

$$\begin{aligned}\omega_N\ :\ RG &\longrightarrow R[G/N]\\ \sum\alpha_g g &\mapsto \sum\alpha_g\overline{g}\end{aligned}$$

where $\overline{g}$ denotes the natural projection of g in the quotient group. If $N = G$, we write $\Delta(G, G) = \Delta(G)$ and identify $R[G/G]$ and R. This last one is simply called the **augmentation ideal** of RG.

We can actually obtain a set of generators for $\Delta(G, N)$, which make practical applications a lot simpler.

Proposition 2.3.2. *Let R be a ring, let G be a group and let $N \trianglelefteq G$. We have:*

$$\Delta(G,N) = \left\{\sum_{h\in N}X_h(h-1)\mid X_h\in RG,\ \textit{where}\ \sum_{h\in N}X_h(h-1)\ \textit{is finite}\right\}$$

Proof. Let X be a *transversal* for N in G (that is, X is a complete set of representatives of the cosets of N in G). If $g \in G$, then $g \in x_gN$ for some $x_g \in X$, meaning $g = x_gn_g$, with $n_g \in N$. Thus, given an arbitrary element $\alpha \in RG$, we can write:

$$\alpha = \sum_{g\in G}\alpha_g g = \sum_{g\in G}\alpha_g x_g n_g$$

In particular, with the notation above, we have:

$$\omega_N(\alpha) = \sum_{g\in G} \alpha_g \overline{x_g} = \sum_{x\in X}\left(\sum_{g\in xN} \alpha_g\right)\overline{x}$$

Therefore, $\omega_N(\alpha) = 0$ if and only if $\sum_{g\in xN}\alpha_g = 0$ for all $x \in X$. On the one hand, if $\sum_{g\in xN}\alpha_g = 0$, then

$$\alpha = \sum_{g\in G}\alpha_g x_g n_g = \sum_{g\in G}\alpha_g x_g n_g - \sum_{x\in X}\left(\sum_{g\in xN}\alpha_g\right)x = \sum_{g\in G}\alpha_g x_g n_g - \sum_{g\in G}\alpha_g x_g = \sum_{g\in G}\alpha_g x_g(n_g - 1)$$

since we've only subtracted 0. This gives us one inclusion. The other one is trivial: indeed, if $\alpha = \sum_{h\in N} X_h(h-1)$, then

$$\omega_N(\alpha) = \sum_{h\in N}\omega_N(X_h)(1-1) = 0$$

■

There are two very well-know problems in the theory of group-rings which are relevant to our goals. The first, known as the "zero-divisor problem", asks when a group ring is a domain. The second asks when a group ring is Noetherian. Both are still open to this day, but certain results are known. We present a few of these results in what follows, starting with those on the latter problem.

Theorem 2.3.3 (P. Hall)**.** *Let R be a right Noetherian ring and G be a polycyclic-by-finite group (that is, there exists some polycyclic $N \trianglelefteq G$ such that G/N is finite). Then, RG is right Noetherian.*

Proof. Let $1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_k = N$ be a polycyclic series for $N \trianglelefteq G$ with $[G : N]$ finite. This yields a subnormal series for G, $N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N \trianglelefteq G$. Let's define $S_i = RN_i$. Then, $S_0 = R$ is right Noetherian, by hypothesis. Suppose, as an inductive hypothesis, that S_i is right Noetherian.

If $i \neq k$, then N_{i+1}/N_i is cyclic, by hypothesis, and therefore, there exists $x \in N_{i+1}$ such that, if $g \in N_{i+1}$, then $g = x^k h$ for some $h \in N_i$. In particular, $N_{i+1} = \langle N_i, x\rangle$ and thus, $S_{i+1} = S_i[x, x^{-1}]$. By Corollary 2.2.4.2, S_{i+1} is right Noetherian. Thus, by induction, RN is right Noetherian.

Let $X = \{x_1, \ldots, x_t\}$ be a transversal for N in G. Thus, if $g \in G$, $g = x_i h$, for some i and for some $h \in N$. This shows us $RG \subset x_1RN + \cdots + x_tRN$, from which we get the equality $RG = x_1RN + \cdots + x_tRN$. That is to say, RG is a f.g. right RN-module. By the preceding case, RN is right Noetherian and, therefore, RG is a right Noetherian RN-module. In particular, it's a right Noetherian RG-module (since every RG-submodule of RG is also a RN-submodule), which finishes the proof. ■

Corollary 2.3.3.1. *Let G be a finitely generated nilpotent group and let K be a field. Then, KG is right Noetherian.*

Proof. This is a direct corollary of Proposition 1.5.3 and the preceding theorem. ■

We now present a result relative to the zero-divisor problem. We'll actually do a bit more, and show that, for certain classes of groups and rings, their group ring can be embedded in a division ring.

Definition. Let R be a ring and let G be an ordered group. The **Malcev-Neumann series ring** of R and G is the set $R((G)) = \{\alpha : G \longrightarrow R \mid \operatorname{supp}(\alpha) \text{ is well-ordered}\}$, with the operations:

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} \alpha_g \beta_h gh = \sum_{k\in G} \gamma_k k, \text{ where } \gamma_k = \sum_{gh=k} \alpha_g \beta_h = \sum_{g\in G} \alpha_g \beta_{g^{-1}k}$$

Proposition 2.3.4. *The preceding operations are well-defined and with them, $R((G))$ is a ring.*

Proof. First, note that $\operatorname{supp}(\alpha + \beta) \subset \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$. Indeed, if $g \notin \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$, then $\alpha_g = \beta_g = 0$, in which case $(\alpha_g + \beta_g) = 0$. By Proposition 1.6.7, therefore, addition is well-defined.

For multiplication, suppose $g \in \operatorname{supp}(\alpha\beta)$. Then, $\gamma_g \neq 0$, where $\gamma_g = \sum_{h\in G} \alpha_h \beta_{h^{-1}g}$. This means at least one term $\alpha_h \beta_{h^{-1}k}$ is nonzero, meaning there exists some $h \in G$ for which both $\alpha_h \neq 0$ and $\beta_{h^{-1}g} \neq 0$. Thus, $h \in \operatorname{supp}(\alpha)$ and $h^{-1}g \in \operatorname{supp}(\beta)$, implying $g \in \operatorname{supp}(\alpha)\operatorname{supp}(\beta)$. Therefore, we have proved $\operatorname{supp}(\alpha\beta) \subset \operatorname{supp}(\alpha)\operatorname{supp}(\beta)$. By Proposition 1.6.7, multiplication is also well-defined (since said proposition also ensures the sum appearing in γ_g is finite).

All that's left is to verify that these operations satisfy the axioms defining a ring. For the reader's sake, we omit this relatively straightforward verification. ■

Proposition 2.3.5. *Let G be an ordered group with positive element cone P, and let $\alpha \in R((G))$ with $S := \operatorname{supp}(\alpha) \subset P$. Then, for all $a_n \in R$, the sum $\sum_{n\in\mathbb{N}} \alpha^n$ is well-defined in $R((G))$.*

Proof. Let $\beta = \sum_{n\in\mathbb{N}} \alpha^n$. We know, from the previous verification that $R((G))$ is a ring, that $\operatorname{supp}(\zeta\xi) \subset \operatorname{supp}(\zeta)\operatorname{supp}(\xi)$, for $\zeta, \xi \in R((G))$. In particular, $\operatorname{supp}(\alpha^2) \subset S^2$. Inductively, we can extend this result to show that $\operatorname{supp}(\alpha^n) \subset S^n$. In particular, $\operatorname{supp}(\beta) \subset \{1\} \cup S^\infty$. By Proposition 1.6.8, this set is well-ordered. Moreover, each g belongs to a finite number of S^n, meaning the sums that determine their coefficients in β are finite. Hence, β is a well-defined element of $R((G))$. ■

Proposition 2.3.6. *Let R be a division ring and let G be an ordered group. Then, $R((G))$ is a division ring.*

Proof. Let $\beta \neq 0$ in $R((G))$ and take $g_0 = \min \operatorname{supp}(\beta)$. We have:

$$\beta_{g_0}^{-1}\beta g_0^{-1} = \beta_{g_0}^{-1}\left(\sum_{g\in G}\beta_g g\right)g_0^{-1} = \beta_{g_0}^{-1}\left(\sum_{g\in G}\beta_{gg_0} g\right) = 1 + \sum_{g\in G\setminus\{1\}}\beta_{gg_0} g$$

Let's define $\alpha = -\sum_{g\in G\setminus\{1\}}\beta_{gg_0} g$. If $g \in \operatorname{supp}(\alpha)$, then $gg_0 \in \operatorname{supp}(\beta)$. From the definition of g_0, this then implies $gg_0 \geq g_0$; in particular, $g \geq 1$ and, as $g \neq 1$, $g > 1$. Hence, $\operatorname{supp}(\alpha) \subset P$. From Proposition 2.3.5:

$$(\beta_{g_0}^{-1}\beta g_0^{-1})\left(\sum_{n\in\mathbb{N}}\alpha^n\right) = (1-\alpha)\left(\sum_{n\in\mathbb{N}}\alpha^n\right) = 1 = \left(\sum_{n\in\mathbb{N}}\alpha^n\right)(\beta_{g_0}^{-1}\beta g_0^{-1})$$

Thus

$$(\beta g_0^{-1})\left(\sum_{n\in\mathbb{N}}\alpha^n\right) = \beta_{g_0} \implies \beta\left(g_0^{-1}\sum_{n\in\mathbb{N}}\alpha^n\beta_{g_0}^{-1}\right) = 1 = \left(g_0^{-1}\sum_{n\in\mathbb{N}}\alpha^n\beta_{g_0}^{-1}\right)\beta$$

This means β is invertible, and since it was an arbitrary element of $R((G))$, this finishes the proof. ■

Corollary 2.3.6.1. *If R is a division ring and G is an ordered group, then RG is a domain.*

Proof. Just note that finite subsets of an ordered group are well-ordered, meaning RG naturally embeds in $R((G))$. ■

Corollary 2.3.6.2. *If R is a division ring and G is a residually torsion-free nilpotent group, then RG is a domain which can be embedded in a division ring.*

Proof. It's a consequence of Proposition 1.6.5. ■

Chapter 3

Free groups in division rings

With all these constructions and properties out of the way, we are now able to establish results about free groups in the multiplicative groups of division rings. In fact, in some cases, we're also able to find free groups in groups of units of algebras which are not necessarily division algebras. Most of what is done here (except for the first section) will come from the main paper upon which the dissertation is based; namely, [GMS99].

Moreover, we want to find free pairs *explicitly*. By this, we mean one of two things: firstly, some division rings (and other algebras) naturally come with a basis. In this case, we want to express the free pairs in that basis. Secondly, if there isn't a "special" basis, we want to find conditions for a couple of elements to generate a free group. This second case will become more clear as we obtain some results.

In order to achieve our goal, it will sometimes be convenient to restrict our attention to a special kind of pair of elements, defined as follows:

Definition. Let G be a group and let $H \trianglelefteq G$. Then, the pair g_1, g_2 is said to be **semi-free modulo H** if it satisfies the following conditions:

- In G/H, $\langle \overline{g_1}, \overline{g_2} \rangle \cong \langle \overline{g_1} \rangle * \langle \overline{g_2} \rangle$;
- $\overline{g_1}$ has order greater than or equal to 3 and $\overline{g_2}$ has order 2;

If $H = Z(G)$, we say the pair is **semi-free modulo center** and, if $H = 1$, the pair is said to be **semi-free**, for short.

Similar to what happens to free pairs, we can lift semi-free pairs modulo H via homomorphisms, as shows the following proposition.

Proposition 3.0.1. *Let $K \trianglelefteq G$ and suppose a pair $\{\pi(x), \pi(y)\}$ is semi-free modulo some normal subgroup $\overline{H} = H/K$ in $\overline{G} = G/K$, where $\pi : G \longrightarrow G/K$ is the canonical projection. Then, $\{x, y\}$ is semi-free modulo H in G.*

Proof. We know, from the First and Third Isomorphism Theorems that the function $\Phi : G/H \longrightarrow \dfrac{G/K}{H/K}$ such that $\Phi(zH) = \pi(y)H/K$ is a group isomorphism. Since the pair $\{\pi(x), \pi(y)\}$ is semi-free modulo H/K, we know $\pi(y)$ has order 2 and $\pi(x)$ has order at least 3 in the quotient, which is the image of Φ. As isomorphisms preserve order, the same is true in the domain, which is G/H.

At the same time, any non-trivial reduced work in $\{xH, yH\}$ in G/H would translate (via Φ) into a non-trivial reduced word in $\{\pi(x)H/K, \pi(y)H/K\}$ in the image of Φ, which can't happen, by hypothesis. Hence, the pair $\{x, y\}$ is semi-free modulo H, finishing the proof. ■

Corollary 3.0.1.1. *Let $\varphi : G \longrightarrow H$ be a group homomorphism and suppose $\{\varphi(x), \varphi(y)\}$ is semi-free modulo $N \trianglelefteq H$. Then, $\{x, y\}$ is semi-free modulo $\varphi^{-1}(N \cap \varphi(G))$ in G.*

Proof. Of course, $\{\varphi(x), \varphi(y)\}$ is semi-free modulo N in $\varphi(G)N \leq H$. Since $\varphi(G)N/N \cong \varphi(G)/(N \cap \varphi(G))$, by the Second Isomorphism Theorem, $\{\varphi(x), \varphi(y)\}$ is semi-free modulo $N \cap \varphi(G)$ in $\varphi(G)$. We can now use Proposition 3.0.1 to obtain the result, using the First Isomorphism Theorem and the Correspondence Theorem. ■

While one might think semi-free pairs modulo some normal subgroup H might be too restrictive, the following proposition shows us how to recover free pairs from semi-free pairs modulo H:

Proposition 3.0.2. *Let G be a group, let $H \trianglelefteq G$ and let $\{g_1, g_2\}$ be a semi-free pair modulo H. Then, the following pairs are free in G:*

- *$\{g_1 g_2, g_1^2 g_2\}$;*
- *$\{g_1, g_2 g_1 g_2\}$, if $\overline{g_1}$ has infinite order in G/H;*

Proof. For the sake of simplicity, we'll only prove the second item; the first one follows from a similar argument.

Let w be a non-trivial reduced word in G/H in $\{x_1, x_2\}$, where $x_1 = \overline{g_1}$ and $x_2 = \overline{g_2 g_1 g_2}$. Write $w = x_{i_1}^{\epsilon_1} \cdots x_{i_k}^{\epsilon_k}$, where $i_j \in \{1, 2\}$ and $\epsilon_j \in \{-1, 1\}$. We will show, using induction on k, that if $i_k = 1$, then w ends in $\overline{g_1}^{l\epsilon_k}$ when reduced in $\{\overline{g_1}, \overline{g_2}\}$, for some $l \in \mathbb{N}$, and, if $i_k = 2$, it ends in $\overline{g_2 g_1}^{l\epsilon_k}\overline{g_2}$ when reduced, for some $l \in \mathbb{N}$.

If $k = 1$, there's nothing to prove (in this case, $l = 1$). Now write $w = w' x_{i_k}^{\epsilon_k}$. Suppose, first, $i_{k-1} = 1$. When reduced in $\{\overline{g_1}, \overline{g_2}\}$, then, $w' = w''\overline{g_1}^{l\epsilon_{k-1}}$ by induction hypothesis, where w'' is reduced in $\{\overline{g_1}, \overline{g_2}\}$ and so is w'. If $i_k = 1$, we get $w = w''\overline{g_1}^{(l+1)\epsilon_k}$, since ϵ_{k-1} can't be different from ϵ_k (since w was reduced in $\{x_1, x_2\}$). And, if $i_k = 2$, then $w = w''\overline{g_1}^{l\epsilon_{k-1}}\overline{g_2 g_1}^{\epsilon_k}\overline{g_2}$, which is reduced in $\{\overline{g_1}, \overline{g_2}\}$.

Now, suppose $i_{k-1} = 2$. Then, the roles are reversed: $w' = w''\overline{g_2 g_1}^{l\epsilon_{k-1}}\overline{g_2}$ for some $l \in \mathbb{N}$ as a reduced word in $\{\overline{g_1}, \overline{g_2}\}$. If $i_k = 1$, w ends in $\overline{g_1}$ as a reduced word in $\{\overline{g_1}, \overline{g_2}\}$ and, if $i_k = 2$, it ends in $\overline{g_2 g_1}^{(l+1)\epsilon_k}\overline{g_2}$, since it was reduced in $\{x_1, x_2\}$ to begin with.

Thus, the result is established and, since $\overline{g_1}$ has infinite order, both $\overline{g_1}^{l\epsilon_k}\overline{g_2}$ and $\overline{g_1}^{l\epsilon_k}$ are non-trivial. In particular, w itself is non-trivial when reduced in $\overline{g_1}, \overline{g_2}$. Then, $w \neq 1$, meaning the pair $\{x_1, x_2\}$ is free, by Proposition 1.2.3. By Proposition 1.1.3, the required pair is also free in G, lifting via the canonical projection. ■

This means that, when we determine a pair of elements in a group G which are semi-free modulo some normal subgroup H, we can use them to explicitly obtain a free pair in G.

3.1 Valuations

In order to obtain free pairs in division rings, we'll usually need to construct suitable sets to apply the Ping-Pong Lemma (Theorem 1.2.4). This will mostly be done through valuations (more specifically, non-archimedean valuations), and so we take the time to define them and briefly study some of their properties, mostly following [Jan96] and [Rib99]. As usual, we begin with a definition.

Definition. Let R be a ring and let G be an ordered abelian group (written with additive notation). Consider an element ∞ such that $x + \infty = \infty = \infty + \infty$ and $x < \infty$ for all $x \in G$, by definition. A **non-archimedean valuation** is a function $v : R \longrightarrow G \sqcup \{\infty\}$ such that:

- $v(x) = \infty \iff x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min\{v(x), v(y)\}$;

The valuation is called a **discrete valuation** if $G = \mathbb{Z}$. Given two discrete valuations $v : R \longrightarrow \mathbb{Z}$ and $w : R \longrightarrow \mathbb{Z}$, they are said to be **equivalent** if there exists some $a \in \mathbb{N}$ such that $v(x) = aw(x)$ for all $x \in R$.

We will mostly restrict ourselves to valuations defined over fields, but valuations defined over noncommutative rings will appear in some instances (usually, over division rings).

While this fact won't actually be used, it's interesting to note that valuations are intrinsically related to metric spaces. Indeed, suppose we have a discrete valuation v on a field K and let $c > 1$ in $\mathbb{R}$. Define $||x|| = c^{-v(x)}$, with the convention that $||0|| = 0$. Then, the following properties hold:

- $||x|| \geq 0$, with equality if and only if $x = 0$;
- $||xy|| = ||x|| \cdot ||y||$;
- $||x + y|| \leq \max\{||x||, ||y||\}$ and, in particular, $||x + y|| \leq ||x|| + ||y||$;

Any function $|| \cdot || : K \longrightarrow \mathbb{R}$ satisfying these properties is called an **absolute value**. If it satisfies (like our case here) $||x + y|| \leq \max\{||x||, ||y||\}$, it's called **non-archimedean**. It's easy to see that an absolute value endows K with a metric $d(x, y) = ||x - y||$, meaning one can then use topological arguments for the study of K (some things are done to this end in [McC76], [Rib99] and [Jan96]).

Returning to valuations themselves, we begin with a few basic properties that will be freely used from now on.

Proposition 3.1.1. *Let R be a ring and let $v : R \longrightarrow G \sqcup \{\infty\}$ be a valuation. Then, the following are true:*

- *$v(1) = 0$;*
- *$v(x^{-1}) = -v(x)$, for all $x \in \mathfrak{U}(R)$;*
- *$v(-x) = v(x)$ for all $x \in R$;*
- *If $v(x) \neq v(y)$, then $v(x + y) = \min\{v(x), v(y)\}$;*

Proof.

- $v(1) = v(1 \cdot 1) = v(1) + v(1)$, from which the statement follows.
- $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, by the preceding item.
- $-1 = (-1)^{-1}$, from which $v(-1) = 0$, using the preceding two statements. Now, $v(-x) = v((-1)x) = v(-1) + v(x) = v(x)$.
- Suppose, without losing generality, that $v(x) < v(y)$. Then, $v(x + y) \geq v(x)$. At the same time, $v(x) = v((x + y) - y) \geq \min\{v(x + y), v(-y)\}$. Since $v(x) < v(y)$, this minimum has to be $v(x + y)$, from which $v(x) \geq v(x + y)$. Combining with the previous inequality, the result follows.

■

When considering a valuation v over a field K, a special subring of K merits attention - the so called **valuation ring** associated with the valuation, defined as $R = \{x \in K \mid v(x) \geq 0\}$; it's called a **discrete valuation ring** if the valuation v is discrete. We study below some of the main properties of these rings:

Proposition 3.1.2. *Let K be a field and let $v : K \longrightarrow G \sqcup \{\infty\}$ be a valuation on K. Let $R = \{x \in K \mid v(x) \geq 0\}$ be the valuation ring associated with v. Then:*

- *If $x \in K$, then either $x \in R$ or $x^{-1} \in R$. In particular, K is the field of fractions of R;*
- *$\mathfrak{U}(R) = \{x \in R \mid v(x) = 0\}$;*
- *R is a local ring with maximal ideal $\mathfrak{p} = \{x \in R \mid v(x) > 0\}$;*
- *If R is a discrete valuation ring, then it's a PID;*

Proof.

- Since G is an ordered group, either $v(x) \geq 0$, in which case $x \in R$, or $v(x) < 0$, in which case $v(x^{-1}) = -v(x) > 0$ and $x^{-1} \in R$.
- An element x of R is invertible if and only if $x^{-1} \in R$, which means $v(x^{-1}) = -v(x) \geq 0$. But since $x \in R$, $v(x) \geq 0$. Combining both yields the result.
- If $x, y \notin \mathfrak{U}(R)$, then $v(x), v(y) > 0$. Thus, $v(x + y) \geq \min\{v(x), v(y)\} > 0$ and $x + y$ isn't invertible. This means R is local (it's one of many characterizations of local rings) and its maximal ideal is $\mathfrak{p} = R \setminus \mathfrak{U}(R) = \{x \in R \mid v(x) > 0\}$.
- Let $\pi \in R$ be some element such that $v(\pi) = n$, $n \in \mathbb{N}$ and consider the ideal $R\pi$. If $x \in R$ is such that $v(x) \geq n$, then $x = (x\pi^{-1})\pi$ in the field K. Moreover, $v(x\pi^{-1}) \geq 0$, meaning this is an element of R. Thus, $x \in R\pi$, and therefore $R\pi = \{x \in R \mid v(x) \geq n\}$.

  Now let I be a nonzero ideal of R and take $\alpha \in I$ such that $v(\alpha) = \min\{v(x) \mid x \in I\}$. Then, I contains the ideal $R\alpha = \{x \in R \mid v(x) \geq v(\alpha)\}$. At the same time, by our choice of α, I is contained in this set. Hence, $I = R\alpha$, meaning every ideal of R is principal.

■

We now work towards constructing what is perhaps the most important example of a valuation: the so-called **$\mathfrak{p}$-adic valuations**. In order to do so, there's yet another class of rings which has to be defined.

Definition. Let R be an integral domain. Then, R is said to be a **Dedekind domain** if it's integrally closed[1], Noetherian and every one of its prime ideals is maximal.

While this definition may seem out of the blue at first, there is another characterization of Dedekind domains which quickly relates them to what has been done so far.

Theorem 3.1.3. *Let R be an integral domain. Then, the following are equivalent:*

- *R is a Dedekind domain;*
- *R is Noetherian and the localization[2] of R at any nonzero prime ideal $\mathfrak{p}$, $R_\mathfrak{p}$, is a discrete valuation ring;*

Proof. Since the proof is rather long and delves deep into commutative algebra, we refer the reader to [Jan96, Theorem 3.16] to avoid developing all the details here. ■

This allows us to prove the following basic fact:

Proposition 3.1.4. *Let R be a Dedekind domain and let $S \subset R$ be a multiplicative submonoid not containing* 0*. Then the localization R_S is also a Dedekind domain.*

Proof. It is well-known that the ideals of R_S are of the form I_S, where I is an ideal of R, and that the prime ideals of R_S are of the form $\mathfrak{p}_S$, where $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$ (for a proof, see [AM94], for instance). Thus, it's straightforward that R_S is Noetherian and that

$$R_\mathfrak{p} = (R_S)_{\mathfrak{p}_S}$$

when viewed as subsets of the field of fractions K of R. From this, $(R_S)_{\mathfrak{p}_S}$ is a discrete valuation ring. As every prime ideal of R_S is of this form, the localization at any prime ideal is a discrete valuation ring, meaning R_S is a Dedekind domain, by Theorem 3.1.3. ■

Perhaps the most important property of Dedekind domains is that they satisfy a version of the Fundamental Theorem of Arithmetic. In order to state the precise result, we first define another concept.

Definition. Let R be an integral domain with field of fractions K. A **fractional ideal** of R is a nonzero f.g. R-submodule of K.

[1] For a basic reference on commutative algebra, see [Sam08].

[2] Again, we refer to [Jan96] and [Sam08] for concepts in commutative algebra.

Note that, if $\mathfrak{M}$ is a fractional ideal of R, then we can write $\mathfrak{M} = \frac{p_1}{q_1}R + \cdots + \frac{p_k}{q_k}R$, where $p_i, q_i \in R$ and $q_i \neq 0$ for all i. Taking some common multiple d of $q_1, ..., q_k$, we then get $d\mathfrak{M} \subset R$. We call the set $\mathfrak{M}^{-1} = \{x \in K \mid x\mathfrak{M} \subset R\}$ the **inverse** of the fractional ideal $\mathfrak{M}$.

If R is a Noetherian integral domain and $\mathfrak{N}$ is a nonzero R-submodule of K such that there exists $d \in R \setminus \{0\}$ with $d\mathfrak{N} \subset R$, then $d\mathfrak{N}$ is a f.g. submodule of R, meaning $d\mathfrak{N} = p_1R + \cdots + p_kR$. Then, $\mathfrak{N}$ is a f.g. submodule of K (multiplying by the inverse of d). Thus, in this case, this property characterizes fractional ideals.

Let $\mathfrak{M}$ and $\mathfrak{N}$ be fractional ideals of an integral domain R. Their product $\mathfrak{M}\mathfrak{N}$ is defined by $\mathfrak{M}\mathfrak{N} = \{\sum m_i n_j \mid m_i \in \mathfrak{M}, n_j \in \mathfrak{N}\}$, where the sums are finite and the product is in the field of fractions K of R.

Proposition 3.1.5. *Let R be a Dedekind domain with field of fractions K and let $\mathfrak{M}, \mathfrak{N}$ be fractional ideals of R. Then, both $\mathfrak{M}^{-1}$ and $\mathfrak{M}\mathfrak{N}$ are fractional ideals. Moreover:*

- *$R\mathfrak{M} = \mathfrak{M}$;*
- *$(yR)^{-1} = y^{-1}R$ for all $0 \neq y \in K$;*
- *If I is an ideal of R, then, viewing it as a fractional ideal, $II^{-1} = R$;*

Proof. Consider $\{x_i \mid 1 \leq i \leq m\}$ and $\{y_j \mid 1 \leq j \leq n\}$ generating sets for $\mathfrak{M}$ and $\mathfrak{N}$, respectively. It's easy to see that $\{x_i y_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a generating set for $\mathfrak{M}\mathfrak{N}$, meaning it's also a fractional ideal.

For the inverse, it is simple to verify that $\mathfrak{M}$ is a submodule of K. Moreover, let $0 \neq m \in \mathfrak{M}$. By definition, $\mathfrak{M}^{-1}m \subset R$, meaning $\mathfrak{M}^{-1} \subset Rm^{-1}$. This is, of course, finitely generated and, since R is Noetherian, the same is true of $\mathfrak{M}^{-1}$. It is also nonzero, by our previous characterization of fractional ideals (which implies the existence of some $d \neq 0$ such that $d\mathfrak{M} \subset R$).

We now prove the three remaining bullet points.

- Trivial (since rings contain 1);
- Let $d \in K$ be such that $dyR \subset R$. Then, $dR \subset y^{-1}R$, meaning $d \in y^{-1}R$. For the converse inclusion, if $r \in R$, then $y^{-1}r(yR) = rR \subset R$;
- We'll freely use many facts regarding localization. Consider the ideal $J = II^{-1}$ of R and let $\mathfrak{q}$ be a maximal ideal of R. Then, $I_\mathfrak{q}$ is a principal ideal of $R_\mathfrak{q}$ (since it's a discrete valuation ring), meaning $I_\mathfrak{q} = yR_\mathfrak{q}$ for some $y \in R_\mathfrak{q}$. Thus

$$J_\mathfrak{q} = (II^{-1})_\mathfrak{q} = I_\mathfrak{q} I_\mathfrak{q}^{-1} = yR_\mathfrak{q} y^{-1} R_\mathfrak{q} = R_\mathfrak{q}$$

meaning $J = R$, since the maximal ideal was arbitrary.[3]

■

[3] In the sequence of equalities, we used some properties of localization and the fact that localization and inversion in the sense previously defined commute. See [Jan96, Exercise I.4.1].

We may now state the main result we need for our goals - the "Fundamental Theorem of Arithmetic" for Dedekind domains.

Theorem 3.1.6. *Let R be a Dedekind domain with field of fractions K.*

- *If I is a nonzero ideal of R, then there exist distinct prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_k$ uniquely determined by I such that $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$, for some $a_i \in \mathbb{N}$. Moreover, these are the only prime ideals containing I.*
- *If $\mathfrak{M}$ is a fractional ideal of R, then there exist distinct prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_k$ uniquely determined by $\mathfrak{M}$ such that $\mathfrak{M} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$, for some $a_i \in \mathbb{Z}$.*

Proof. Just as Theorem 3.1.3, the proof is very long and would detract a lot from our goals at this point. Thus, we refer to [Jan96, Theorems 3.14 and 4.2]. ■

Remark. With the theorem above, using the fact that prime ideals are invertible (in the sense that $\mathfrak{p}\mathfrak{p}^{-1} = R$), one can prove that every fractional ideal is invertible, meaning $\mathfrak{M}\mathfrak{M}^{-1} = R$. Thus, the set of fractional ideals of R forms a group (called the *ideal group* of R). Also note that we define $\mathfrak{p}^{-a} = (\mathfrak{p}^{-1})^a$, where $a \in \mathbb{N}$.

An easy consequence we will need later is the following:

Proposition 3.1.7. *Let R be a Dedekind domain with a finite number of prime ideals. Then, R is a PID.*

Proof. Let $\mathfrak{p}_1, ..., \mathfrak{p}_k$ be the pairwise distinct nonzero prime ideals of R. Since all of them are maximal, the ideals $\mathfrak{p}_1^2, ..., \mathfrak{p}_k$ are also pairwise coprime (meaning the sum of any two of them is equal to R) - notice that $\mathfrak{p}_1^2$ can't be contained in any of the other due to their primality.

By the Chinese Remainder Theorem, there exists a surjective ring homomorphism φ from R to the direct sum $R/\mathfrak{p}_1^2 \oplus \cdots \oplus R/\mathfrak{p}_k$. Also, $R_{\mathfrak{p}_1}$ is local, with maximal ideal $\mathfrak{p}_{1_{\mathfrak{p}_1}}$. By Nakayama's Lemma (see [Jan96]), $0 \neq (\mathfrak{p}_{1_{\mathfrak{p}_1}})^2 \neq \mathfrak{p}_{1_{\mathfrak{p}_1}}$. This implies $\mathfrak{p}_1^2 \neq \mathfrak{p}_1$. Taking some element $y \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$, there exists $x \in R$ such that x maps to $(y, 1, ..., 1)$ via φ. This means xR is contained in $\mathfrak{p}_1$, but not in any of the other prime ideals or $\mathfrak{p}_1^2$. Using Theorem 3.1.6, the only possible factorization for xR is thus $xR = \mathfrak{p}_1$. Doing the same to all the others means all prime ideals are principal. Theorem 3.1.6 yields the result. ■

Now we can construct the $\mathfrak{p}$-adic valuations. So, for the remainder of this section, R will denote a Dedekind domain, $\mathfrak{p}$, one of its prime ideals and K, its field of fractions.

Let $x \in K$ be an arbitrary nonzero element. Since R is a Dedekind domain, so is $R_{\mathfrak{p}}$. Thus, $xR_{\mathfrak{p}}$ can be uniquely written as a product of prime ideals of $R_{\mathfrak{p}}$ and their inverses. But this is a local ring such that every prime ideal is maximal, meaning its only prime ideal is $\mathfrak{p}_{\mathfrak{p}}$ (recall that these are the fractions such that the numerator is in $\mathfrak{p}$ and the denominator is *not* in $\mathfrak{p}$). This means

$$xR_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}^{v_{\mathfrak{p}}(x)}$$

where $v_{\mathfrak{p}}(x) \in \mathbb{Z}$ is a well-defined integer. We can now use the fact that $R_{\mathfrak{p}}$ is a discrete valuation ring to write $\mathfrak{p}_{\mathfrak{p}} = \pi R_{\mathfrak{p}}$, for some $\pi \in R_{\mathfrak{p}}$. Then, $\mathfrak{p}_{\mathfrak{p}}^{v_{\mathfrak{p}}(x)} = \pi^{v_{\mathfrak{p}}(x)} R_{\mathfrak{p}}$, by Proposition 3.1.5. Thus, $x = \pi^{v_{\mathfrak{p}}(x)}u$, for some $u \in R_{\mathfrak{p}}$. Also, $\pi^{v_{\mathfrak{p}}(x)} = xu'$, meaning $uu' = 1$. This means $u \in \mathfrak{U}\left(R_{\mathfrak{p}}\right)$.

We may then consider the function $v_{\mathfrak{p}} : K \longrightarrow \mathbb{Z} \sqcup \{\infty\}$, with the convention that $v_{\mathfrak{p}}(0) = \infty$. We will prove that this is a valuation of the field K. Indeed, let $y \in K$ be another nonzero element. From the preceding paragraph, we can write $x = u\pi^{v_{\mathfrak{p}}(x)}$ and $y = u'\pi^{v_{\mathfrak{p}}(y)}$, where u, u' are invertible elements of the ring $R_{\mathfrak{p}}$. Assuming, without losing generality, that $v_{\mathfrak{p}}(x) \leq v_{\mathfrak{p}}(y)$, we get

$$x + y = \pi^{v_{\mathfrak{p}}(x)}(u + u'\pi^{v_{\mathfrak{p}}(y)-v_{\mathfrak{p}}(x)})$$

where the term in parenthesis is an element of $R_{\mathfrak{p}}$, as $\pi \in R_{\mathfrak{p}}$. Thus, it follows that $v_{\mathfrak{p}}(x+y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$. Also

$$xy = uu'\pi^{v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y)}$$

meaning $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$, since $uu' \in \mathfrak{U}\left(R_{\mathfrak{p}}\right)$.

Definition. The valuation $v_{\mathfrak{p}}$ constructed above is called the **$\mathfrak{p}$-adic valuation** of K.

Notice, from the construction, that the valuation ring associated with $v_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$, that it's discrete, and that its maximal ideal is $\mathfrak{p}_{\mathfrak{p}}$. These valuations are very good to work with, as we will soon see, because they can easily be computed.

We will now deal with the problem of extending valuations. Suppose K is a field, v is a valuation of K and $L : K$ is a field extension. We want to construct a valuation of L which restricts to v when considered as a valuation of K. A very general result in this direction is the following:

Theorem 3.1.8. *Let R be a subring of a field K and let $\mathfrak{P}$ be a prime ideal of R. Then, there exists a valuation ring $A \subset K$ such that $R \subset A$ and, denoting the maximal ideal of A by $\mathfrak{A}$, $\mathfrak{P} = \mathfrak{A} \cap R$.*

Proof. See [End72, Corollary 9.7]. ∎

For some applications, however, it will be convenient to have an explicit construction for the extension. In order to do that, we need a general result, which will also be left without proof, since it's also quite long.

Proposition 3.1.9. *Let R be a Dedekind domain with field of fractions K and let L be a finite field extension[4] of K. Consider the integral closure S of R in L of the extension - i.e., S is the set of elements of L which are roots of monic polynomials with coefficients in R. Then, S is also a Dedekind domain.*

Proof. See [Jan96, Theorem 6.1]. ∎

Now we can deal with the extensions in the particular case of $\mathfrak{p}$-adic valuations extended to finite dimensional extension fields. Let R be a Dedekind domain, K its field of fractions,

[4] We will use the term "finite field extension" of a field K to denote a field L containing K which is a finite dimensional vector space over K.

$\mathfrak{p}$ a prime ideal of R, and consider the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of K. Let $L : K$ be a finite dimensional extension field and let S be the integral closure in L of $R_\mathfrak{p}$.

By Proposition 3.1.9, we can decompose the ideal $\mathfrak{p}_\mathfrak{p}S$ as a product of nonzero prime ideals of S. Thus, we write:

$$\mathfrak{p}_\mathfrak{p}S = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_k^{a_k}$$

In fact, these are all the nonzero prime ideals of S. To see this, note that any prime ideal $\mathfrak{P}$ of S intersects with $R_\mathfrak{p}$ at a prime ideal, meaning it's either at $\mathfrak{p}_\mathfrak{p}$ or at 0. If $\mathfrak{P} \cap R_\mathfrak{p} = 0$, then take some $x \in \mathfrak{P}$ and write $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, with minimal n, where $a_i \in R_\mathfrak{p}$. Thus, $x(x^{n-1} + a_{n_1}x^{n-2} + \cdots a_1) = -a_0 \in \mathfrak{P} \cap R_\mathfrak{p}$. This means $a_0 = 0$ and, since we are working on a domain, the minimality of n implies $x = 0$.

We've thus established that S is a Dedekind domain with a finite number of prime ideals, meaning, by Proposition 3.1.7, it's a PID. So we can consider $\mathfrak{P}_i = \tau_i S$ for each i. Let $v_{\mathfrak{P}_i}$ be the $\mathfrak{P}_i$-adic valuation on S. We know, from our construction of these valuations, that $v_{\mathfrak{P}_i}(\tau_i) = 1$ and that its valuation ring is $S_{\mathfrak{P}_i}$. If π is a generator of $\mathfrak{p}_\mathfrak{p}$, we have

$$\pi S_{\mathfrak{P}_i} = \mathfrak{p}_\mathfrak{p} S_{\mathfrak{P}_i} = \mathfrak{P}_{i\mathfrak{P}_i}^{a_i}$$

meaning $\pi = \tau_i^{a_i} w$, where w is some unit of $S_{\mathfrak{P}_i}$. Then, $v_{\mathfrak{P}_i}(\pi) = a_i = a_i v_\mathfrak{p}(\pi)$. One easily sees that this relation extends to $v_{\mathfrak{P}_i}(x) = a_i = a_i v_\mathfrak{p}(x)$ for all $x \in K$ (since every element of K could be expressed as a product of a power of π and an element of valuation 0). This means $v_{\mathfrak{P}_i}$ is equivalent to $v_\mathfrak{p}$ as valuations of K. In particular, if $a_i = 1$, they are equal on K.

This discussion proves the part we will need of the following, more general, result.

Theorem 3.1.10. *Let R be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and quotient field K, and let S be its integral closure in a finite separable extension $L : K$. Suppose*

$$\mathfrak{p}S = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_k^{a_k}$$

in S. Then, the $\mathfrak{P}_i$-adic valuations of L are equivalent to the $\mathfrak{p}$-adic valuation on K, with the relation $v_{\mathfrak{P}_i}(x) = a_i v_\mathfrak{p}(x)$ for $x \in K$. Moreover, these are pairwise nonequivalent and are the only valuations (up to equivalence) which restrict to a valuation equivalent to $v_\mathfrak{p}$ on K.

Proof. For the remainder of the proof (i.e., the bits that weren't shown in our previous discussion), see [Jan96, Theorem II.3.1]. ■

Finally, we briefly mention extensions of valuations to transcendental extension fields, as in the following result, whose proof will be omitted due to its simplicity.

Proposition 3.1.11. *Let K be a field and let v be a valuation on K. Let $K(x)$ be a simple transcendental extension of K. Then, the function defined by*

$$V\left(\sum_i a_i x^i\right) = \min\{v(a_i)\}$$

is a valuation on $K(x)$.

3.2 Quaternion algebras

In 1843, Irish mathematician Sir William Rowan Hamilton discovered the so-called hamiltonian quaternions, the only noncommutative division algebra algebraic over the real numbers (as evidenced by a theorem of Frobenius; see [Her75, Theorem 7.3.1]).

In fact, the algebra constructed by Hamilton can easily be generalized to a whole family of algebras over an arbitrary field of characteristic different from two. This is the construction we will analyze next.

Definition. Let K be a field of characteristic different from 2 and let $a, b \in K^\dagger$. The **quaternion algebra** $\left(\frac{a,b}{K}\right)$ is the K-algebra defined by:

$$\left(\frac{a,b}{K}\right) = \frac{K\langle \mathbf{i}, \mathbf{j}\rangle}{\langle \mathbf{i}^2 - a, \mathbf{j}^2 - b, \mathbf{ji} + \mathbf{ij}\rangle}$$

One very important property of these algebras is as follows.

Proposition 3.2.1. *Quaternion algebras are central-simple algebras of dimension* 4 *over the base field.*

Proof. Let F be the algebraic closure of K and let α, β be elements of F such that $\alpha^2 = -a, \beta^2 = b$. It's trivial to verify, by definition, that there exists a K-algebra homomorphism defined as follows:

$$\begin{aligned} \psi : \left(\frac{a,b}{K}\right) &\longrightarrow M_2(F) \\ \mathbf{i} &\longmapsto \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} \\ \mathbf{j} &\longmapsto \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix} \end{aligned}$$

It's also clear that the images of $\{1, \mathbf{i}, \mathbf{j}, \mathbf{ij}\}$ are LI in $M_2(F)$, meaning the original set is also LI. In particular, since it's a generator set, it forms a basis for the algebra $\left(\frac{a,b}{K}\right)$.

Now, let $0 \neq I$ be an ideal of the quaternion algebra. Consider a nonzero element $q = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{ij}$ in I. Then, $\mathbf{i}q = a\alpha_1 + \alpha_0\mathbf{i} + a\alpha_3\mathbf{j} + \alpha_2\mathbf{ij}$ and $q\mathbf{i} = a\alpha_1 + \alpha_0\mathbf{i} - a\alpha_3\mathbf{j} - \alpha_2\mathbf{ij}$, whence:

$$\frac{\mathbf{i}q + q\mathbf{i}}{2} = a\alpha_1 + \alpha_0\mathbf{i} \quad \text{and} \quad \frac{\mathbf{i}q - q\mathbf{i}}{2} = (a\alpha_3 + \alpha_2\mathbf{i})\mathbf{j}$$

It's clear that at least one of the two elements is nonzero. Furthermore, $\mathbf{j}$ is an invertible element, from which we conclude that I contains a nonzero element of the form $z = \alpha + \beta\mathbf{i}$. Thus, $z\mathbf{j} = \alpha\mathbf{j} + \beta\mathbf{ij}$ and $\mathbf{j}z = \alpha\mathbf{j} - \beta\mathbf{ij}$.

Repeating the same argument as before, we conclude that either I contains a nonzero element of the form $\alpha\mathbf{j}$, or I contains a nonzero element of the form $\beta\mathbf{ij}$. In any case, since both of the elements are invertible, we obtain $I = \left(\frac{a,b}{K}\right)$, meaning it is a simple algebra. Moreover, the above calculations show that, if q is central, then q belongs to the base field K, meaning it is also a central algebra. This concludes the proof. ■

It's worth noting that these algebras may be categorized into two types: either $\left(\frac{a,b}{K}\right)$ is a division ring, such as the case of the real hamiltonian quaternions, or $\left(\frac{a,b}{K}\right) \cong M_2(K)$ ([Lam04, Chapter 2], for instance). In the latter case, we say the algebra is **split**. The **Hamiltonian quaternions** $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ are an example of a quaternion algebra which is not split.

In order to tell the two cases apart, we may analyze the **norm function** associated to the quaternion algebra, $N(\alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{ij}) = \alpha_0^2 - \alpha_1^2 a - \alpha_2^2 b + \alpha_3^2 ab$. A simple computation shows that, if $q = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{ij}$ and we denote $\overline{q} = \alpha_0 - \alpha_1\mathbf{i} - \alpha_2\mathbf{j} - \alpha_3\mathbf{ij}$, then $q\overline{q} = N(q)$.

In particular, this shows that q is invertible if and only if $N(q) \neq 0$, since $N(q)$ is an element of the base field K (this criterion will be relevant later). Moreover, the quaternion algebra $\left(\frac{a,b}{K}\right)$ is a division ring if and only if the associated norm form is anisotropic (meaning $N(q)$ is 0 if and only if q is 0), since this is equivalent to saying every element is a unit.

In order to construct free pairs in quaternion algebras, no matter the case, we first need a couple of technical results (from now on, all the propositions in this section are from [GMS99], except when explicitly stated otherwise).

Proposition 3.2.2. *Let $x, y, \alpha, \beta \in K$ and $m \in \mathbb{Z}$, where K is a field of characteristic different from 2 and $\alpha + \beta\mathbf{i}$ is invertible in $\left(\frac{a,b}{K}\right)$. Then, $(x + y\mathbf{j})(\alpha + \beta\mathbf{i})^m = x(\alpha + \beta\mathbf{i})^m + y(\alpha - \beta\mathbf{i})^m\mathbf{j}$.*

Proof. We'll first deal with the case where $m \geq 0$, proceeding by induction on m. If $m = 0, 1$, the result is trivial (using the quaternion relations). For the inductive step, if the result is valid for $m - 1$, we get:

$$\begin{aligned}(x + y\mathbf{j})(\alpha + \beta\mathbf{i})^m &= (x(\alpha + \beta\mathbf{i})^{m-1} + y(\alpha - \beta\mathbf{i})^{m-1}\mathbf{j})(\alpha + \beta\mathbf{i}) \\ &= x(\alpha + \beta\mathbf{i})^m + y(\alpha - \beta\mathbf{i})^m\mathbf{j}\end{aligned}$$

For the case where $m < 0$, all we have to do is use the identities

$$(\alpha + \beta\mathbf{i})^{-1} = \frac{\alpha - \beta\mathbf{i}}{\alpha^2 - \beta^2 a} \quad \text{and} \quad (\alpha - \beta\mathbf{i})^{-1} = \frac{\alpha + \beta\mathbf{i}}{\alpha^2 - \beta^2 a}$$

and the preceding case (note that these identities follow by computing the norm of the quaternions involved). ■

Proposition 3.2.3. *Let K be a field of characteristic different from 2, with $a, b, \beta \in K^\dagger$, $\beta^2 \neq b^{-1}$, and let $F = K(\sqrt{a}, \sqrt{b})$. Let's define*

$$\theta = \frac{1+\beta\sqrt{b}}{1-\beta\sqrt{b}} \quad \text{and} \quad r_n = \frac{1}{\sqrt{b}}\left[\frac{\theta^n - 1}{\theta^n + 1}\right], n \in \mathbb{Z}$$

Then, in the quaternion algebra $\left(\frac{a,b}{F}\right)$, for all $n \in \mathbb{Z}$, there exists some $0 \neq d_n \in F$ such that $(1+\beta\mathbf{j})^n = d_n(1 + r_n\mathbf{j})$.

Proof. Just as in Proposition 3.2.2, we'll proceed by induction on n, beginning with $n \geq 0$. If $n = 0$, just take $d_n = 1$, since $r_0 = 0$. Suppose, then, that $n \geq 1$ and that the result is valid for $n-1$; that is, that there exists some $0 \neq d_{n-1} \in F$ such that $(1+\beta\mathbf{j})^{n-1} = d_{n-1}(1 + r_{n-1}\mathbf{j})$. Hence:

$$\begin{aligned}(1+\beta\mathbf{j})^n &= d_{n-1}(1 + r_{n-1}\mathbf{j})(1+\beta\mathbf{j}) \\ &= d_{n-1}(1 + r_{n-1}\beta b + (r_{n-1}+\beta)\mathbf{j}) \\ &= (d_{n-1}(1 + r_{n-1}\beta b))\left(1 + \left(\frac{r_{n-1}+\beta}{1+r_{n-1}\beta b}\right)\mathbf{j}\right)\end{aligned}$$

Using the definition of r_n, one can directly compute that $r_n = \left(\frac{r_{n-1}+\beta}{1+r_{n-1}\beta b}\right)$. Also, since $\beta^2 \neq b^{-1}$, the quaternion $1+\beta\mathbf{j}$ has nonzero norm, and is, therefore, invertible. In particular, if we take $d_n = d_{n-1}(1 + r_{n-1}\beta b)$, d_n is nonzero. By induction, the result follows.

Now, if $n < 0$, we can use the fact that $r_{-n} = -r_n$ (which may also be verified directly), and see, using the previous case, that

$$(1+\beta\mathbf{j})^{-n} = d_{-n}(1 - r_n\mathbf{j})$$

This now means that

$$(1+\beta\mathbf{j})^n = \frac{1}{d_{-n}(1 - r_n^2 b)}(1 + r_n\mathbf{j})$$

since $1+\beta\mathbf{j}$ is invertible, meaning $d_{-n}(1 - r_n^2 b) \neq 0$.

Then, we can just take $d_n = (d_{-n}(1 - r_n^2 b))^{-1}$. ■

We may now use these results, together with non-archimedean valuations, to obtain results on free pairs in quaternion algebras. The main difficulty in these theorems is determining the sets we will use to apply the Ping-Pong Lemma, as will become clear.

Theorem 3.2.4. *Let R be an integral domain of characteristic distinct from 2 with field of fractions $Q(R) = Q$, and let $a, b, \alpha, \beta \in R^\dagger$, $\alpha^2 \neq a^{-1}$, $\beta^2 \neq -ab^{-1}$. Suppose there exists some non-archimedian valuation v over the field $Q(\mathbf{i})$ such that $v(a) = v(b) = v(\beta) = 0$ and $v(1+\alpha\mathbf{i}) \neq v(1-\alpha\mathbf{i})$. Then, $\{1+\alpha\mathbf{i}, \mathbf{i}+\beta\mathbf{j}\}$ is semi-free modulo center in $\mathfrak{U}\left(\frac{a,b}{Q}\right)$.*

Proof. We can decompose $\left(\frac{a,b}{Q}\right)$ as a free module of rank 2, with $\{1, \mathbf{j}\}$ as a basis, over the field $Q(\mathbf{i})$, essentially breaking this 4-dimensional space into two 2-dimensional "steps". This observation will be the key for finding the appropriate sets upon which the desired pair of elements acts.

Let $H = \mathfrak{U}\left(\frac{a,b}{Q}\right)/Q^{\dagger}$. Notice that, if we take $\overline{x + y\mathbf{j}} \in H$, with $x, y \in Q(\mathbf{i})$, then any element in the same class is of the form $(x + y\mathbf{j})z$, with $0 \neq z \in Q$. Thus, $v(x) = v(y)$ if and only if the same is true with any other representative of the same class.

Let's define, then, $X_1 = \{\overline{x + y\mathbf{j}} \mid x, y \in Q(\mathbf{i}), v(x) = v(y)\}$ and $X_2 = \{\overline{x + y\mathbf{j}} \mid x, y \in Q(\mathbf{i}) v(x) \neq v(y)\}$. Then, H acts on both by right multiplication. Consider $\overline{x + y\mathbf{j}} \in X_1$ and let $0 \neq n \in \mathbb{Z}$. By Proposition 3.2.2, $\overline{(x + y\mathbf{j})(1 + \alpha\mathbf{i})^n} = \overline{x(1 + \alpha\mathbf{i})^n + y(1 - \alpha\mathbf{i})^n\mathbf{j}}$. Then, we compute the valuations of the terms, and obtain

$$\begin{aligned} v(x(1+\alpha\mathbf{i})^n) &= v(x) + nv(1 + \alpha\mathbf{i}) \\ &= v(y) + nv(1 + \alpha\mathbf{i}) \\ &\neq v(y) + nv(1 - \alpha\mathbf{i}) = v(y(1 - \alpha\mathbf{i})^n) \end{aligned}$$

meaning $\overline{(x + y\mathbf{j})(1 + \alpha\mathbf{i})^n} \in X_2$.

Now let $\overline{x + y\mathbf{j}} \in X_2$. Then, $\overline{(x + y\mathbf{j})(\mathbf{i} + \beta\mathbf{j})} = \overline{(x\mathbf{i} + y\beta b) + (x\beta - y\mathbf{i})\mathbf{j}}$. Since $v(a) = 0$, it's also true that $v(i) = 0$, as $2v(\mathbf{i}) = v(a)$ and the field doesn't have characteristic 2. Thus, $v(x\mathbf{i}) = v(x)$ and $v(y\beta b) = v(y)$, by hypothesis. We conclude

$$v(x\mathbf{i} + y\beta b) = \min\{v(x), v(y)\} = v(x\beta - y\mathbf{i})$$

using Proposition 3.1.1. This means $\overline{(x + y\mathbf{j})(\mathbf{i} + \beta\mathbf{j})} \in X_2$.

Finally, $\overline{(\mathbf{i} + \beta\mathbf{j})}^2 = 1$ (as scalars are central) and $\overline{1 + \alpha\mathbf{i}}$ has order greater than 2 (since its square still contains a $\mathbf{i}$ term and quaternion algebras are central). Therefore, the pair $\{1 + \alpha\mathbf{i}, \mathbf{i} + \beta\mathbf{j}\}$ is semi-free modulo center, by Theorem 1.2.4. ∎

As an example of an application of Theorem 3.2.4, the authors highlight, in [GMS99], the following result.

Proposition 3.2.5. *Suppose that $\zeta = \cos\theta + \sin\theta\mathbf{i}$ is a primitive n-th root of unity, where $n \neq 2$ and $4 \nmid n$. Then, the pair $\{\zeta, \mathbf{i} + \mathbf{j}\}$ is semi-free modulo center.*

The proof uses a bit more of commutative algebra and valuation theory than we have developed up to this point, but what's interesting is that nothing is said regarding the cases in which $\cos\theta + \sin\theta\mathbf{i}$ has infinite order, and finding a valuation to use Theorem 3.2.4 directly is particularly hard. We have partially answered this case in the following proposition from [GSed].

Proposition 3.2.6. *Let (a, b, c) be a primitive Pythagorean triple (i.e., such that the three integers are coprime) and let $0 < \theta < \frac{\pi}{2}$ be an angle such that $\cos 2\theta = \frac{b}{c}$. Then, $\{\cos\theta + \sin\theta\mathbf{i}, \mathbf{i} + \mathbf{j}\}$ is semi-free modulo center in $\mathbb{H}$.*

We may also use valuations to find free pairs directly.

Theorem 3.2.7. *Let R be an integral domain of characteristic different from 2 and with field of fractions Q. Let $a, b, \alpha, \beta \in R^{\dagger}$, $\alpha^2 \neq a^{-1}, \beta^2 \neq b^{-1}$. Suppose there exists a non-archimedian valuation v on $Q(\sqrt{b}, \mathbf{i})$ such that $v(a) = v(b) = v(\alpha) = v(\beta) = 0$ and $v(1+\alpha\mathbf{i}) \neq v(1-\alpha\mathbf{i})$, $v(1+\beta\sqrt{b}) \neq v(1-\beta\sqrt{b})$. Then, $\{1+\alpha\mathbf{i}, 1+\beta\mathbf{j}\}$ is a free pair in $\mathfrak{U}\left(\frac{a,b}{Q}\right)$.*

Proof. We can essentially copy the proof of Theorem 3.2.4, but ignoring the "modulo center restriction". So we define $X_1 = \{x + y\mathbf{j} \mid x, y \in Q(\mathbf{i}), v(x) = v(y)\}$ and $X_2 = \{x + y\mathbf{j} \mid x, y \in Q(\mathbf{i}) v(x) \neq v(y)\}$. We have $X_1(1+\alpha\mathbf{i})^n \subset X_2$ for all $n \neq 0$, by a computation similar to what had been done. Now, by Proposition 3.2.3, we have $(1+\beta\mathbf{j})^m = d_m(1 + r_m\mathbf{j})$, where

$$\theta = \frac{1+\beta\sqrt{b}}{1-\beta\sqrt{b}} \text{ and } r_n = \frac{1}{\sqrt{b}}\left[\frac{\theta^n - 1}{\theta^n + 1}\right]$$

By hypothesis, $v(\theta) \neq 0$. Hence, if $m \neq 0$, then $v(\theta^m + 1) = v(\theta^m - 1)$ and, in particular, $v(r_m) = 0$. Thus, from $(x + y\mathbf{j})(1+\beta\mathbf{j})^m = d_m((x + r_m yb) + (xr_m + y)\mathbf{j})$ and $v(x) \neq v(y)$, we get $X_2(1+\beta\mathbf{j})^m \subset X_1$. Also, both of these elements have infinite order. To see this, note that the inverse of $1+\alpha\mathbf{i}$ is $(1-\alpha\mathbf{i})(1-\alpha^2 a)^{-1}$. If it had finite order, then there would be some $m \in \mathbb{N}$ such that $(1+\alpha\mathbf{i})^m = (1-\alpha\mathbf{i})(1-\alpha^2 a)^{-1}$. This would mean

$$mv(1+\alpha\mathbf{i}) = v(1-\alpha\mathbf{i}) - v(1-\alpha^2 a)$$

Since $v(1-\alpha^2 a) = v(1+\alpha\mathbf{i}) + v(1-\alpha\mathbf{i})$, we can substitute to obtain $v(1+\alpha\mathbf{i}) = 0$. There would be some $n \in \mathbb{N}$ such that $(1-\alpha\mathbf{i})^n = (1+\alpha\mathbf{i})(1-\alpha^2 a)^{-1}$. The same reasoning as before yields $v(1-\alpha\mathbf{i}) = 0$, which is a contradiction. Of course, everything we have just done also applies to $1+\beta\mathbf{i}$, meaning it also has infinite order. The Ping-Pong Lemma (Theorem 1.2.4) yields the result. ■

There's a limitation to these theorems in that finding the appropriate valuations may be difficult, and thus checking whether a specific pair of elements is free or not can involve quite a lot of work. In the case of the Hamiltonian quaternions $\mathbb{H}$, we can dodge valuations altogether in many situations, as shown by this proposition from [GSed].

Proposition 3.2.8. *Let α be either a rational number other than 0 and ±1, or a transcendental number. Then, the pair $\{1+\alpha\mathbf{i}, 1+\alpha\mathbf{j}\}$ is free in $\mathbb{H}^{\dagger}$.*

This result is actually more general (a will be seen in Theorem B.0.1). In order to get such generality, we use the matricial representation of quaternions acting on the pure quaternions (those of the form $\beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{ij}$) by conjugation, and obtain properties of the matrices that appear. An example of this type of reasoning appears in Proposition 3.2.10 below.

For algebraic (and not rational) α, we can't get this level of generality, and there can be a lot of variation on the specific α. For example, $1+\sqrt{3}\mathbf{i}$ is twice a root of unity, which immediately prevents it from being an element freely generating a free group. That said, we were able to obtain a result by imposing some conditions on α (see [GSed]).

Proposition 3.2.9. *Let α be an algebraic number with minimal polynomial $f(x)$. Consider $K = \mathbb{Q}(\alpha)$ and let R be the integral closure of $\mathbb{Z}$ in K. Suppose that $f(x)$ is irreducible modulo 2, and that $\Delta(\alpha) \notin 2\mathbb{Z}$, where $\Delta(\alpha)$ denotes the discriminant of the extension*[5]*. Suppose further that $1 + \alpha^2 \notin \mathfrak{U}(R)$ and that $\frac{1+\alpha^2}{2} \notin R$. Then, $\langle 1 + \alpha\mathbf{i}, 1 + \alpha\mathbf{j}, 1 + \alpha\mathbf{ij}\rangle \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z}$ in $\mathfrak{U}\left(\frac{-1,-1}{K}\right)$.*

One example of an α that satisfies all the conditions of the previous proposition is a root of the irreducible polynomial $x^3 - 3x + 1$.

Another case of algebraic α we were able to prove is the following, which didn't appear in [GSed].

Proposition 3.2.10. *Let $\alpha = \sqrt{a}$, where a is an even, square-free natural number. Then, $\langle 1 + \alpha\mathbf{i}, 1 + \alpha\mathbf{j}, 1 + \alpha\mathbf{ij}\rangle \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z}$ in $\mathfrak{U}\left(\frac{-1,-1}{\mathbb{Q}(\alpha)}\right)$.*

Proof. First, notice that $a + 1$ is not a unit in the integral closure R of $\mathbb{Z}$ in the extension $\mathbb{Q}(\alpha)$ - this is done computing its norm (see, for instance, [Jan96, Chapter I.5]), which is $(a + 1)^2$. Since this isn't invertible in $\mathbb{Z}$, $a + 1$ can't be invertible in R.

Now notice that $a + 1$ and $a - 1$ are coprime integers. This is because, if $a + 1 \equiv 0 \pmod{p}$ and $a - 1 \equiv 0 \pmod{p}$, then $2 \equiv 0 \pmod{p}$, meaning $p = 2$. Since a is even, however, this can't be the case. Also, $a + 1$ and $2a$ are coprime, since any prime factor dividing $2a$ is either 2, which doesn't divide $a + 1$, or a prime factor of a, which also can't divide $a + 1$.

Let $m, n \in \mathbb{Z}$ be such that $(1 + a)m + 2an = 1$. Then, $2\alpha \cdot n\alpha = 1 - (1 + a)m$. This means, in the quotient ring $R/(1 + a)R$, both 2α and $1 - a$ are invertible. Also, $2(na) = 1 - (1 + a)m$, meaning 2 is also invertible in this quotient. As such, $2(1 - a)$ is invertible.

Denoting by ρ the unit quaternions' representation by conjugation on the set of pure quaternions (i.e., $\rho(q)(\mathbf{i}) = q\mathbf{i}q^{-1}$, for instance, where q is a unit in $\left(\frac{-1,-1}{\mathbb{Q}(\alpha)}\right)$), we get

$$\rho(1 + \alpha\mathbf{i}) = \frac{1}{1+a}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-a & -2\alpha \\ 0 & 2\alpha & 1-a \end{bmatrix};$$

$$\rho(1 - \alpha\mathbf{j}) = \frac{1}{1+a}\begin{bmatrix} 1-a & 0 & -2\alpha \\ 0 & 1 & 0 \\ 2\alpha & 0 & 1-a \end{bmatrix};$$

$$\rho(1 + \alpha\mathbf{ij}) = \frac{1}{1+a}\begin{bmatrix} 1-a & -2\alpha & 0 \\ 2\alpha & 1-a & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

from which [GSed, Theorem 5] finishes the proof (since, if $\{x, y, z\}$ is a basis for a free group, the same is trivially true for $\{x, y^{-1}, z\}$). ∎

The reason this previous result is singled out is that the discriminant of quadratic extensions is always even, and so this is never in the conditions of our previous result on

[5] If $f(x)$ has degree m, $\Delta(\alpha) = \Delta(1, \alpha, \ldots, \alpha^{m-1}) = \det[T(\alpha^i\alpha^j)]_{i,j}$, where $T(x) = \mathrm{tr}[x]$ using the regular representation (see [Jan96]).

algebraic extensions.

We now move on to a different setting. If K is a field of characteristic 2, quaternion algebras have to be defined differently (indeed, the definition we've used thus far would give us a commutative algebra). We do this next.

Definition. Let K be a field of characteristic 2 and let $a, b \in K^{\dagger}$. The **quaternion algebra** $\left(\frac{a,b}{K}\right]$ is the K-algebra defined by:

$$\left(\frac{a,b}{K}\right] = \frac{K\langle \mathbf{i}, \mathbf{j}\rangle}{\langle \mathbf{i}^2 + \mathbf{i} + a, \mathbf{j}^2 + b, \mathbf{ji} + \mathbf{ij} + \mathbf{j}\rangle}$$

Proposition 3.2.11. *$\left(\frac{a,b}{K}\right]$ is a central simple 4 dimensional K-algebra.*

Proof. Let F be the algebraic closure of K and let $\alpha^2 = a, \beta^2 = b$ in F. Consider the homomorphism

$$\begin{aligned}\psi : \left(\frac{a,b}{K}\right] &\longrightarrow M_2(F) \\ \mathbf{i} &\longmapsto \begin{bmatrix} 0 & \alpha \\ \alpha & 1 \end{bmatrix} \\ \mathbf{j} &\longmapsto \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix}\end{aligned}$$

It's trivial to verify that the image of the set $\{1, \mathbf{i}, \mathbf{j}, \mathbf{ij}\}$ is LI, meaning the original set is also LI. This immediately implies it's a basis for $\left(\frac{a,b}{K}\right]$ as a K-vector space.

We now check that it's a central algebra. Let $q = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{ij}$ be central. Notice that

$$\begin{aligned}\mathbf{i}q &= \alpha_1 a + (\alpha_0 + \alpha_1)\mathbf{i} + \alpha_3 a\mathbf{j} + (\alpha_2 + \alpha_3)\mathbf{ij} \\ q\mathbf{i} &= \alpha_1 a + (\alpha_0 + \alpha_1)\mathbf{i} + (\alpha_2 + \alpha_3 a)\mathbf{j} + \alpha_2\mathbf{ij}\end{aligned}$$

meaning $\alpha_2 = \alpha_3 = 0$. We also have

$$\begin{aligned}\mathbf{j}q &= (\alpha_0 + \alpha_1)\mathbf{j} + \alpha_1\mathbf{ij} \\ q\mathbf{j} &= \alpha_0\mathbf{j} + \alpha_1\mathbf{ij}\end{aligned}$$

and, therefore, $\alpha_1 = 0$. Thus, $q = \alpha_0 \in K$, which finishes this part of the proof.

Finally, let $q = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{ij}$ be a nonzero element of an ideal $0 \neq I$ of $\left(\frac{a,b}{K}\right]$. From the previous calculations, since $\mathbf{i}q, q\mathbf{i} \in I$, $\alpha_2\mathbf{j} + \alpha_3\mathbf{ij} \in I$. Moreover:

$$(\alpha_2\mathbf{j} + \alpha_3\mathbf{ij})\mathbf{j} = \alpha_2 b + \alpha_3 b\mathbf{i}$$

Thus, I contains a nonzero element of the form $p = \alpha + \beta\mathbf{i}$. Now:

$$p\mathbf{j} = \alpha\mathbf{j} + \beta\mathbf{ij}$$

and also

$$\mathbf{j}p = (\alpha + \beta)\mathbf{j} + \beta\mathbf{ij}$$

In particular, I contains a nonzero element of the form $\gamma\mathbf{j}$. But $\mathbf{j}$ and $\gamma \neq 0$ are invertible, meaning $I = \left(\frac{a,b}{K}\right]$. Since the ideal I was arbitrary, this concludes the proof. ■

As before, we will need a more technical result.

Proposition 3.2.12. *Let $x, y, \alpha \in K$ and $m \in \mathbb{Z}$, where K is a field of characteristic 2 and $1 + \alpha\mathbf{i}$ is invertible in $\left(\frac{a,b}{K}\right]$. Then, $(x + y\mathbf{j})(1 + \alpha\mathbf{i})^m = x(1 + \alpha\mathbf{i})^m + y(1 + \alpha + \alpha\mathbf{i})^m\mathbf{j}$.*

Proof. We'll first deal with the case where $m \geq 0$, proceeding by induction on m. If $m = 0, 1$, the result is trivial (using the quaternion relations). For the inductive step, if the result is valid for $m - 1$, we get:

$$\begin{aligned}(x + y\mathbf{j})(1 + \alpha\mathbf{i})^m &= (x(1 + \alpha\mathbf{i})^{m-1} + y(1 + \alpha + \alpha\mathbf{i})^{m-1}\mathbf{j})(1 + \alpha\mathbf{i}) \\ &= x(1 + \alpha\mathbf{i})^m + y(1 + \alpha + \alpha\mathbf{i})^m\mathbf{j}\end{aligned}$$

For the case where $m < 0$, we use the identities

$$(1 + \alpha\mathbf{i})^{-1} = \frac{1 + \alpha + \alpha\mathbf{i}}{1 + \alpha + \alpha^2 a} \quad \text{and} \quad (1 + \alpha + \alpha\mathbf{i})^{-1} = \frac{1 + \alpha\mathbf{i}}{1 + \alpha + \alpha^2}$$

to obtain

$$\begin{aligned}(x + y\mathbf{j})(1 + \alpha\mathbf{i})^{-1} &= (x + y\mathbf{j})(1 + \alpha + \alpha\mathbf{i})(1 + \alpha + \alpha^2)^{-1} \\ &= (x(1 + \alpha + \alpha^2\mathbf{i}) + y(1 + \alpha\mathbf{i})\mathbf{j})(1 + \alpha + \alpha^2)^{-1} \\ &= x(1 + \alpha\mathbf{i})^{-1} + y(1 + \alpha + \alpha\mathbf{i})^{-1}\mathbf{j}\end{aligned}$$

The rest is done by induction as before. ■

About these algebras, our main result for obtaining free pairs is the following:

Theorem 3.2.13. *Let K be a field of characteristic 2 and let $a, b, \alpha \in K^\dagger, b \neq 1$. Suppose there exists a valuation of $\mathbb{F}_2(a, b, \alpha, \mathbf{i}) \subset K(\mathbf{i})$ such that $v(b) = 0$ and $v(a + \alpha^{-1} + \alpha^{-2}) \neq 0, \infty$. Then, $\{1 + \alpha\mathbf{i}, 1 + \mathbf{j}\}$ is semi-free modulo center in $\mathfrak{U}\left(\frac{a,b}{F}\right]$.*

Proof. Using the same notations as in Theorem 3.2.4, let $X_1 = \{\overline{x + y\mathbf{j}} \mid x, y \in K(\mathbf{i}), v(x) = v(y)\}$ and $X_2 = \{\overline{x + y\mathbf{j}} \mid x, y \in K(\mathbf{i}) v(x) \neq v(y)\}$. We can do this since quaternion algebras are also central in characteristic 2.

First, notice that $(1 + \mathbf{j})^2 = 1 + b \neq 0$, meaning it's an invertible element of order 2 modulo center. Now let $\overline{x + y\mathbf{j}} \in X_2$. We have $\overline{(x + y\mathbf{j})(1 + \mathbf{j})} = \overline{(x + by) + (x + y)\mathbf{j}}$. Since $v(b) = 0$, $v(by) = v(y)$, from which it follows that $v(x + by) = v(x + y)$ (as $v(x) \neq v(y)$, meaning $v(x + y) = \min\{v(x), v(y)\}$).

For the other inclusion, let's define $f = (1 + \alpha\mathbf{i})(1 + \alpha(1 + \mathbf{i}))$. It's easy to see that $f = a\alpha^2 + \alpha + 1 \in K$. Ergo, $v(f) = 2v(\alpha) + v(a + \alpha^{-1} + \alpha^{-2})$ and, since $\alpha \neq 0$, we get by hypothesis that $v(f) \neq \infty$; in particular, f is invertible and the same happens to $1+\alpha\mathbf{i}$, $1+\alpha(1+\mathbf{i})$.

Let $t = \frac{1+\alpha(1+\mathbf{i})}{1+\alpha\mathbf{i}}$. Simple computation gives $t+t^{-1} = \frac{\alpha^2}{f}$. Thus, $v(t+t^{-1}) = -v(a+\alpha^{-1}+\alpha^{-2}) \neq 0$, meaning $v(t) \neq 0$. Equivalently, $v(1+\alpha\mathbf{i}) \neq v(1+\alpha(1+\mathbf{i}))$.

Now take $\overline{x+y\mathbf{j}} \in X_1$. By Proposition 3.2.12, $\overline{(x+y\mathbf{j})(1+\alpha\mathbf{i})^m} = \overline{x(1+\alpha\mathbf{i})^m + y(1+\alpha+\alpha\mathbf{i})^m\mathbf{j}}$ for all $m \in \mathbb{Z}$. Since $v(x) = v(y)$, our previous computation shows

$$v(x) + mv(1+\alpha\mathbf{i}) \neq v(y) + mv(1+\alpha(1+\mathbf{i}))$$

implying $X_1\overline{(1+\alpha\mathbf{i})^m} \subset X_2$ for all $m \in \mathbb{Z}$. Also, $(1+\alpha\mathbf{i})^2 = (1+\alpha^2 a) + \alpha^2\mathbf{i}$, meaning it's not in the center (again using the centrality of quaternion algebras in any characteristic). Thus, Theorem 1.2.4 finishes the proof. ■

3.3 The first Weyl Algebra

Using the previous results on quaternions, we can obtain free pairs in other classes of algebras. In order to do so, we begin with the construction of the first Weyl Algebra, gathering some assorted results from [Lam01]. While this construction can be carried out inductively, allowing us to get a whole family of Weyl algebras, we'll focus our attention on the first one, due to its greater simplicity.

Definition. The **first Weyl algebra** over a field K is the K-algebra given by generators and relations as follows:

$$A_1(K) = \frac{K\langle s,t\rangle}{\langle ts-st-1\rangle}$$

We identify, for simplicity, $\bar{s} = s + \langle ts-st-1\rangle$ with s and $\bar{t} = t + \langle ts-st-1\rangle$ with t.

Proposition 3.3.1. *The set $\{s^i t^j \mid i,j \in \mathbb{N}\}$ is a basis for $A_1(K)$ over the field K.*

Proof. First, to prove this set generates $A_1(K)$, let $m \in \mathbb{N}$. We will show $t^m s$ is a linear combination of the terms of $\{s^i t^j \mid i,j \in \mathbb{N}\}$. If $m = 1$, this is trivially true, as $ts = st+1$. By induction, $t^m s = t^{m-1}(ts) = t^{m-1}(st+1) = (\sum \lambda_{i,j} s^i t^j)t + t^{m-1}$, for some $\lambda_{i,j} \in K$ almost all zero, which is of the form we wanted.

Next, let w be a word on s, t. We'll do induction on the length of w to show it can be written as a K-linear combination of the elements of $\{s^i t^j \mid i,j \in \mathbb{N}\}$. If w has length 1, then there's nothing to show, since either $w = s$ or $w = t$.

Now, for the inductive step, write $w = w' x_n$, where $x_n \in \{s,t\}$. Since w' has smaller length, $w' = \sum \alpha_{i,j} s^i t^j$ for some $\alpha_{i,j} \in K$, by the inductive hypothesis (where almost all of the $\alpha_{i,j}$ are zero). If $x_n = t$, $w = \sum \alpha_{i,j} s^i t^{j+1}$ and we are done. If $x_n = s$, on the other hand, then $w = \sum \alpha_{i,j} s^i t^j s$. By the first paragraph, we can write $t^j s = \sum_{k,l} \beta_{k,l} s^k t^l$. Thus, $w = \sum_{i,j,k,l} \alpha_{i,j}\beta_{k,l} s^{i+k} t^l$, and once again, we are done.

For linear independence, consider the standard polynomial ring $K[x,y]$. We may define unique linear operators $\varphi, \psi : K[x,y] \longrightarrow K[x,y]$ such that $\varphi(x^i y^j) = x^{i+1} y^j$ and

$\psi(x^i y^j) = ix^{i-1}y^j + x^i y^{j+1}$ (if $i = 0$, we interpret the first term as 0). Then, we have

$$\begin{aligned}(\psi\varphi - \varphi\psi)(x^i y^j) &= \psi(x^{i+1}y^j) - \varphi(ix^{i-1}y^j + x^i y^{j+1})\\ &= (i+1)x^i y^j + x^{i+1}y^{j+1} - ix^i y^j - x^{i+1}y^{j+1}\\ &= 1\end{aligned}$$

Therefore, there exists a K-algebra homomorphism $\rho : A_1(K) \longrightarrow \mathrm{L}(K[x,y])$ such that $\rho(s) = \varphi$ and $\rho(t) = \psi$ (here, $\mathrm{L}(K[x,y])$ denotes the ring of linear operators on $K[x,y]$), by the universal property of the free K-algebra and the First Isomorphism Theorem.

Suppose $\sum_{i,j} \alpha_{i,j} s^i t^j = 0$. Then, $\rho\left(\sum_{i,j} \alpha_{i,j} s^i t^j\right) = 0$. In particular, computing the effect of this element on 1, we get

$$\begin{aligned}\left(\sum_{i,j} \alpha_{i,j}\varphi^i\psi^j\right)(1) &= 0\\ \sum_{i,j} \alpha_{i,j}\varphi^i(y^j) &= 0\\ \sum_{i,j} \alpha_{i,j}x^i y^j &= 0\end{aligned}$$

meaning $\alpha_{i,j} = 0$ for all i, j. Thus, the set $\{s^i t^j \mid i, j \in \mathbb{N}\}$ is linearly independent, finishing the proof. ■

This means arbitrary elements of $A_1(K)$ may be written as polynomials on s, t. This will be made even more precise soon. For a bit of historical context, the first Weyl algebra has its origins in quantum mechanics, where it appears as the algebra generated by certain operators. We'll see a version of this interpretation in the following basic properties, where it becomes clear that s, t act as the standard derivative via commutators. When there's no ambiguity, we will use $[x, y] = xy - yx$ for the additive commutators as well.

Proposition 3.3.2. *In the K-algebra $A_1(K)$, the following identities hold for all $n \in \mathbb{N}$ and all $p(s,t) \in A_1(K)$:*

- $[t^n, s] = \frac{\partial}{\partial t}(t^n)$;
- $[t, s^n] = \frac{\partial}{\partial s}(s^n)$;
- $[p(s,t), s] = \frac{\partial}{\partial t}p(s,t)$;
- $[t, p(s,t)] = \frac{\partial}{\partial s}p(s,t)$;

Proof. Direct computation using induction and linearity. ■

Proposition 3.3.3. *The first Weyl algebra over a field K is simple.*

Proof. Let $I \neq 0$ be an ideal of $A_1(K)$ and let $p(s,t) \in I$ be nonzero and of minimal degree[6]. Since I is an ideal, we know that $[t, p(s,t)] \in I$ and $[p(s,t), s] \in I$. By Proposition 3.3.2, this

[6] We define the degree as with polynomials in two variables

implies $\frac{\partial}{\partial t}p(s,t), \frac{\partial}{\partial s}p(s,t) \in I$. Due to the minimality of the degree of $p(s,t)$, this yields, in turn, that $p(s,t) = k \in K$, $k \neq 0$. Ergo, $I = A_1(K)$. ■

Proposition 3.3.4. $A_1(K) \cong K[x][y; \frac{d}{dx}]$.[7]

Proof. Let $\phi : K\langle s,t\rangle \longrightarrow K[x][y; \frac{d}{dx}]$ be the K-algebra homomorphism given by $\phi(s) = x$, $\phi(t) = y$. Since $yx = xy + 1$, this induces a K-algebra homomorphism $\psi : A_1(K) \longrightarrow K[x][y; \frac{d}{dx}]$. It is surjective, as x, y generate the skew polynomial ring, and injective, by Proposition 3.3.3, meaning it is a K-algebra isomorphism. ■

In particular, the proposition above shows $A_1(K)$ is an Ore domain, by Corollary 2.2.4.1, meaning it admits a total field of fractions. In order to investigate the presence of free pairs in the multiplicative group of that division ring, we'll need some results on free pairs in multiplicative groups of fields of fractions of skew polynomial rings, which can be obtained using our previous results on quaternions. We begin with the following:

Proposition 3.3.5. *Let $K(x,y)$ be the field of fractions of the standard polynomial ring in x and y over the field K of characteristic different than 2 (resp. characteristic 2). Then, given $\alpha, \beta \in K^\dagger$, the pair $\{1+\alpha\mathbf{i}, 1+\beta\mathbf{j}\}$ is free (resp. semi-free modulo center if $\beta = 1$) in $\mathfrak{U}\left(\frac{x,y}{K(x,y)}\right)$ (resp. in $\mathfrak{U}\left(\frac{x,y}{K(x,y)}\right]$).*

We will present two proofs of this results. The first will use valuations and the theorems on quaternions. The second will also do this to some extent, but will also be a good demonstration of another technique for obtaining free pairs, using the so called *specializations*, defined as follows.

Definition. Let D and Δ be division rings. A **specialization** $\alpha : D \longrightarrow \Delta$ is a surjective ring homomorphism $\alpha : R \subset D \longrightarrow \Delta$, where R is a local subring of D, such that $\ker \alpha = \mathfrak{m}$, with $\mathfrak{m}$ the maximal ideal of R ([Coh08]).

There is a weaker variant of specializations that lifts the requirements of the subring being local.

Definition. Let D and Δ be division rings. A **proto-specialization** $\alpha : D \longrightarrow \Delta$ is a ring homomorphism $\alpha : R \subset D \longrightarrow \Delta$, where R is a subring of D, such that $\alpha(\mathfrak{U}(R)) = \Delta^\dagger$ ([GP20]).

First proof of Proposition 3.3.5. Let $\mathfrak{p} = \langle 1 - \alpha^2 x\rangle$ in the ring $K[x]$. It is easy to see that this is a prime ideal (the quotient ring is isomorphic to K, via the evaluation of x at α^{-2}). Consider the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of $K(x)$ and take $L = K(\sqrt{x})$ and S the integral closure of $K[x]_\mathfrak{p}$ in L. In S, $1-\alpha^2 x = (1-\alpha\sqrt{x})(1+\alpha\sqrt{x})$, meaning $(1-\alpha^2 x)S = (1-\alpha\sqrt{x})S \cdot (1+\alpha\sqrt{x})S$.

By [Jan96, Corollary 6.7], $(1-\alpha^2 x)S$ can have at most two prime ideal factors, meaning each of the ideals $(1-\alpha\sqrt{x})S$ and $(1+\alpha\sqrt{x})S$ is prime. They are also distinct, since $S/(1+\alpha\sqrt{x})S$ is not of characteristic 2 (it contains an isomorphic copy of K, which is $K[x]/\mathfrak{p}$; see [Jan96, Lemma 6.5]) and $1-\alpha\sqrt{x} = 2$ in the quotient.

[7] Here, the automorphism is the identity.

Thus, we can extend $v_\mathfrak{p}$ to a valuation v of $K(\sqrt{x})$ such that $v(1+\alpha\sqrt{x}) = 1$ and $v(1-\alpha\sqrt{x}) = 0$, by Theorem 3.1.10. Of course, the same exact process can be done to construct a valuation w of $K(\sqrt{y})$ such that $w(1+\beta\sqrt{y}) = 1$ and $w(1-\beta\sqrt{y}) = 0$.

Now consider the subring $K[\sqrt{x}, \sqrt{y}]$ of $K(\sqrt{x}, \sqrt{y})$ and the ideal $\mathfrak{P} = (1 + \alpha\sqrt{x})K[\sqrt{x}, \sqrt{y}] + (1+\beta\sqrt{y})K[\sqrt{x}, \sqrt{y}]$. Since $K[\sqrt{x}, \sqrt{y}]$ is isomorphic to a polynomial ring on two variables, it's easy to see that $\mathfrak{P}$ is a maximal ideal, since the quotient is isomorphic to K; in particular, it's a prime ideal.

Take a valuation V associated to a valuation ring $A \subset K(\sqrt{x}, \sqrt{y})$ given by Theorem 3.1.8. We know that $\mathfrak{P}$ is the set of elements of $K[\sqrt{x}, \sqrt{y}]$ with positive valuation. Thus, the set of elements of $K[\sqrt{x}]$ with positive valuation is $\mathfrak{P} \cap K[\sqrt{x}] = (1+\alpha\sqrt{x})K[\sqrt{x}]$. In particular, $V(1-\alpha\sqrt{x}) = 0$ and $V(1+\alpha\sqrt{x}) > 0$. The same can be done for the intersection with $K[\sqrt{y}]$, meaning V satisfies all of the conditions of Theorem 3.2.7 (we may use $\mathbf{i}$ and $\sqrt{x}$ interchangeably), finishing the proof.

For the characteristic 2 case, we can simply consider the valuation of $K(x)$ associated to the prime ideal $\langle x + \alpha^{-1} + \alpha^{-2} \rangle$ and extend it, via the minimum valuation (see Section 1) to the field $K(x, y)$. ■

Second proof of Proposition 3.3.5. We now present a second proof using specializations. First, we use the same arguments as in the first proof. Consider a valuation v of $K(\sqrt{t})$ such that $v(1+\alpha\sqrt{t}) = 1$ and $v(1-\alpha\sqrt{t}) = 0$ (we have constructed such a valuation in the first proof). It shows that $\{1+\alpha\mathbf{i}, \mathbf{i}+\mathbf{j}\}$ is semi-free modulo center in $\mathfrak{U}\left(\frac{t,t}{K(t)}\right)$. If $(1+\alpha\mathbf{i})$ had finite order modulo center, there would exist some $m \in \mathbb{N}$ such that $(1+\alpha\mathbf{i})^m \in K$, meaning $mv(1+\alpha\mathbf{i}) = 0$, which is absurd. By Proposition 3.0.2, since $(\mathbf{i}+\mathbf{j})^{-1}(1+\alpha\mathbf{i})(\mathbf{i}+\mathbf{j}) = 1+\alpha\mathbf{j}$, the pair $\{1+\alpha\mathbf{i}, 1+\alpha\mathbf{j}\}$ is free.

Consider the K-algebra homomorphism $\psi : K[x, y] \longrightarrow K(t)$ given by $\psi(x) = \psi(y) = t$, constructed using the universal property of polynomial rings. Its kernel is a prime ideal (as $K(t)$ is a domain), and $K(t)$ is a field, meaning ψ inverts $K[x, y] \setminus \ker\psi$. Thus, by the universal property of localization, there exists a unique extension $\tilde{\psi} : K[x, y]_\mathfrak{p} \longrightarrow K(t)$, where $\mathfrak{p} = \ker\psi$. Furthermore, $\tilde{\psi}$ is trivially surjective.

Take $S = \{\gamma_0 + \gamma_1\mathbf{i} + \gamma_2\mathbf{j} + \gamma_3\mathbf{ij} \mid \gamma_i \in K[x, y]_\mathfrak{p}, \forall i\}$. As $x, y \in K[x, y]_\mathfrak{p}$, a simple calculation proves that S is a subring of $\left(\frac{x,y}{K(x,y)}\right)$, and we can define $\alpha : S \longrightarrow \left(\frac{t,t}{K(t)}\right)$ by

$$\alpha(\gamma_0 + \gamma_1\mathbf{i} + \gamma_2\mathbf{j} + \gamma_3\mathbf{ij}) = \tilde{\psi}(\gamma_0) + \tilde{\psi}(\gamma_1)\mathbf{i} + \tilde{\psi}(\gamma_2)\mathbf{j} + \tilde{\psi}(\gamma_3)\mathbf{ij}$$

It's straightforward to check that this α is a surjective homomorphism, meaning it defines a proto-specialization from $\left(\frac{x,y}{K(x,y)}\right)$ to $\left(\frac{t,t}{K(t)}\right)$. From the first paragraph, the pair $\{1+\mathbf{i}, 1+\mathbf{j}\}$ is free in $\left(\frac{x,y}{K(x,y)}\right)$.

Now define a K-algebra homomorphism $\varphi : K\langle\mathbf{i},\mathbf{j}\rangle \longrightarrow \left(\frac{\alpha^2 x, \beta^2 y}{K(x,y)}\right)$ with $\varphi(\mathbf{i}) = \alpha^{-1}\tilde{\mathbf{i}}$ and $\varphi(\mathbf{j}) = \beta^{-1}\tilde{\mathbf{j}}$, where the "~" is used to differentiate between the elements of the domain and those of the image. Notice that

$$\varphi(\mathbf{i})^2 = x, \varphi(\mathbf{j})^2 = y \text{ and } \varphi(\mathbf{j})\varphi(\mathbf{i}) = -\varphi(\mathbf{i})\varphi(\mathbf{j})$$

meaning φ uniquely extends to a K algebra homomorphism $\Phi : \left(\frac{x,y}{K(x,y)}\right) \longrightarrow \left(\frac{\alpha^2 x, \beta^2 y}{K(x,y)}\right)$, which is evidently an isomorphism (using the simplicity of quaternion algebras and the definition of Φ). Also, $\alpha^2 x$ and $\beta^2 y$ are two algebraically independent variables over $K(x, y)$. Thus, the pair $\{1 + \mathbf{i}, 1 + \mathbf{j}\}$ is free in $\left(\frac{\alpha^2 x, \beta^2 y}{K(x,y)}\right)$, by the proto-specialization we had build, and this pair lifts via Φ to $\{1 + \alpha\mathbf{i}, 1 + \beta\mathbf{j}\}$ in $\left(\frac{x,y}{K(x,y)}\right)$, finishing the proof. The characteristic 2 case is done as before. ■

Proposition 3.3.6. *Let K be a field and let Q be the total classical field of fractions of the skew polynomial ring $K(x)[y; \sigma]$ (the derivation is the "zero" derivation). Then, the following are true:*

1. *If $\sigma(x) = x + 1$ and K is of characteristic 2, then $\{1 + x, 1 + y\}$ is semi-free modulo center in Q;*
2. *If $\sigma = \lambda x$, where λ is a primitive $2n^{th}$-root of unity, and K is of characteristic not 2, then $\{1 + \alpha x^n, 1 + \beta y\}$ is free in Q, for all $\alpha, \beta \in K^\dagger$;*

Proof. We will contend ourselves to the proof of item 2.; the first one is analogous, using the appropriate results over characteristic 2. Let $u = x^{2n}$ and $v = y^2$. It's trivial to check that both are central in Q, meaning $K(u, v) \subset Z$, where Z is the center of the division ring Q.

Let's consider $H = \left(\frac{u,v}{K(u,v)}\right)$. By the definitions of λ and σ, $yx^n = -x^n y$. Therefore, if F is the subdivision ring of Q generated by $\{x^n, y\}$, we will get a homomorphism $\phi : H \longrightarrow F$ with $\phi(\mathbf{i}) = x^n$, $\phi(\mathbf{j}) = y$. This is, in fact, an isomorphism, since H is simple and ϕ surjective. Thus, we just need to use Proposition 3.3.5. ■

In order to proceed, we will need the following important result due to Lichtman ([Lic78]), that translates known results in commutative rings to the noncommutative case.

Proposition 3.3.7. *Let R be an integral domain with field of fractions F and let A be a prime ideal of R. Suppose there exists a discrete valuation v of F such that $A = \{r \in R \mid v(r) > 0\}$. Let $a, b \in R$, with $a \in \mathfrak{U}(R)$, and consider the automorphism $\theta : R[x] \longrightarrow R[x]$, such that $\theta(x) = ax + b$. Let $S = R[x][y; \theta]$, which is a right Ore domain. Under these conditions, the following are true:*

1. *AS is a completely prime ideal of S;*[8]
2. *The complement M of the prime ideal AS is a right denominator set for S;*

[8] A *completely prime ideal* of a noncommutative ring is an ideal I such that $ab \in I$ implies either $a \in I$ or $b \in I$.

3. *The ring of fractions SM^{-1} of S relative to M is a local ring whose maximal ideal B satisfies $B \cap S = AS$*

Proof. 1. It is relatively simple to see that AS is the set consisting of the elements of S with all of its coefficients in A. Suppose $pq \in AS$, with $p, q \notin AS$. Write, then, $p = p' + r_1$ and $q = q' + r_2$, where all the coefficients of the monomials in p', q' are in A, but those of r_1, r_2 are not, and no monomial in p' appears in r_1 (analogously with q' and r_2). Take the leading coefficients $\omega_1 x^k y^l$ and $\omega_2 x^m y^n$ of r_1 and r_2, respectively. Then, we get

$$\omega_1 x^k y^l \omega_2 x^m y^n = \omega_1 \omega_2 a^{ml} x^{k+m} y^{l+n} + \epsilon$$

where ϵ consists of terms of smaller degree. By hypothesis, $pq \in AS$, meaning we must have $\omega_1 \omega_2 a^{ml} \in A$. As a is invertible in R, $a \notin A$, since it's a prime ideal, meaning $a^{ml} \notin A$. But A this implies either ω_1 or ω_2 is in A, a contradiction.

2. Let $m \in M, r \in S$. Since S is a right Ore domain, there exist $m_1, r_1 \in S$ such that $mr_1 = rm_1 \neq 0$. Thus, all we need to show is that such a relation exists with $m_1 \in M$.

   Suppose $m_1 \notin M$, which is equivalent to $m_1 \in AS$. It's therefore true that $m_1 = \sum a_{ij} x^i y^j$, where $a_{ij} \in A$ for all i, j. Furthermore, $mr_1 = rm_1 \in AS$ and, as $m \notin AS$ and the latter is a completely prime ideal, we get $r_1 \in AS$; in particular, $r_1 = \sum b_{ij} x^i y^j$, where $b_{ij} \in A$ for all i, j.

   Take $\pi \in A$ such that $v(\pi) = 1$ (i.e., a generator of the ideal). Since $v(a_{ij}) > 0, \forall i, j$, there exists some maximal $n \in \mathbb{N}$ such that $\pi^n \mid a_{ij}$ for all i, j. Thus, $m_1 = \pi^n m'$, where $m' \in M$, using the maximality of the chosen n. As $\pi \nmid m$, then $\pi^n \mid r_1$. Canceling both sides, we get the equality $mr' = rm'$, $m' \in M$.

3. Every element of SM^{-1} is of the form sm^{-1}. This element fails to be invertible if, and only if, $s \in AS$. Thus, the set of non-units is a two-sided ideal, $B = ASM^{-1}$, meaning AM^{-1} is a local ring. Moreover, $ASM^{-1} \cap S = AS$.

■

With this tool at hand, we can get a very interesting result regarding the field of fractions of $A_1(\mathbb{Q})$ ([GMS99, Theorem 4]).

Theorem 3.3.8. *The pair $\{1 + ts, 1 + s\}$ is semi-free modulo some normal subgroup of the multiplicative group of the total field of fractions of $A_1(\mathbb{Q})$.*

Proof. Let $\theta : \mathbb{Q}(x) \longrightarrow \mathbb{Q}(x)$ be the ring automorphism given by $\theta(x) = x + 1$. It's easy to see that, defining $s \longmapsto y^{-1}x$ and $t \longmapsto y$, we get an isomorphism from the total field of fractions of $A_1(\mathbb{Q})$ onto the division ring $\mathbb{Q}(x)(y; \theta)$. The latter is also the total field of fractions of $\mathbb{Z}[x][y; \theta]$ (where we identify θ with its restriction).

Take, then, $R = \mathbb{Z}$, $A = 2\mathbb{Z}$, $S = \mathbb{Z}[x][y; \theta]$ and v the rational valuation associated to the prime ideal A of R. We're now in the conditions of Proposition 3.3.7. Hence, defining $M = S \setminus AS$, this is a right denominator set for S, and SM^{-1} is a local ring with maximal ideal ASM^{-1}. It's straightforward to see that

$$\frac{SM^{-1}}{ASM^{-1}} \cong \mathbb{Z}_2(x)(y;\theta)$$

through simple computation.

We now obtain, using Proposition 3.3.6, that the pair $\{1+x, 1+y\}$ is semi-free modulo center in $\mathbb{Z}_2(x)(y;\theta)^{\dagger}$. We can now lift the required pairs using the following diagram and Corollary 3.0.1.1

$$\begin{tikzcd}
 & \mathbb{Q}\langle s,t\rangle \arrow[dl] \arrow[dr] & & \\
A_1(\mathbb{Q}) \arrow[r, hook] & Q(A_1(\mathbb{Q})) \arrow[r, shift left] & \mathbb{Q}(x)(y;\theta) \arrow[l, shift left] & \\
 & & SM^{-1} \arrow[u, hook] \arrow[r] & \mathbb{Z}_2(x)(y;\theta)
\end{tikzcd}$$

■

Using Proposition 3.0.2, the following corollary is immediate:

Corollary 3.3.8.1. *There exists a free pair in the total classical field of fractions of $A_1(\mathbb{Q})$.*

3.4 Malcev-Neumann series rings

The final class of division rings in which we'll construct free pairs is that of the Malcev-Neumann series rings, as constructed in Section 2.3. In order to do so, we'll need the following categorical construction:

Definition. Let R_n be rings and let $\psi_n : R_{n+1} \longrightarrow R_n$ be ring homomorphisms, $n \in \mathbb{N}$. An **inverse limit** of this system is a ring R together with a sequence of homomorphisms $\alpha_n : R \longrightarrow R_n$ such that:

- $\psi_n \circ \alpha_{n+1} = \alpha_n$;
- If R' is another ring with another sequence of homomorphisms $\beta_n : R' \longrightarrow R_n$ such that $\psi_n \circ \beta_{n+1} = \beta_n$, then there exists a unique homomorphism $\Phi : R' \longrightarrow R$ such that the following commutes:

$$\begin{tikzcd}
R' \arrow[rr, dashed, "\exists!\Phi"] \arrow[dr, "\beta_n"] \arrow[ddr, "\beta_{n+1}"'] & & R \arrow[dl, "\alpha_n"'] \arrow[ddl, "\alpha_{n+1}"] \\
 & R_n & \\
 & R_{n+1} \arrow[u, "\psi_n"] &
\end{tikzcd}$$

Proposition 3.4.1. *Given a sequence of rings R_n and a sequence of homomorphisms $\psi_n : R_{n+1} \longrightarrow R_n$, there exists, up to isomorphism, a unique inverse limit of the system.*

Proof. Uniqueness, as tends to be the case with universal property definitions, is rather simple. Given two such inverse limits R and R', together with their homomorphisms α_n, β_n, consider the diagram:

$$\begin{tikzcd}
R' \arrow[rr, dashed, "\exists!\Phi"] \arrow[dr, "\beta_n"] \arrow[ddr, "\beta_{n+1}"'] & & R \arrow[rr, dashed, "\exists!\Psi"] \arrow[dl, "\alpha_n"'] \arrow[ddl, "\alpha_{n+1}"] \arrow[dr, "\alpha_n"] \arrow[ddr, "\alpha_{n+1}"'] & & R' \arrow[rr, dashed, "\exists!\Phi"] \arrow[dl, "\beta_n"'] \arrow[ddl, "\beta_{n+1}"] \arrow[dr, "\beta_n"] \arrow[ddr, "\beta_{n+1}"'] & & R \arrow[dl, "\alpha_n"'] \arrow[ddl, "\alpha_{n+1}"] \\
& R_n & & R_n & & R_n & \\
& R_{n+1} \arrow[u, "\psi_n"] & & R_{n+1} \arrow[u, "\psi_n"] & & R_{n+1} \arrow[u, "\psi_n"] &
\end{tikzcd}$$

From the uniqueness of the constructed homomorphisms, both compositions yield their respective identities. In particular, $R \cong R'$. Hence, all that's left is to show existence.

Let, then, $\mathscr{R} = \prod_{i=0}^{\infty} R_i$ and define $L = \{(m_i) \in \mathscr{R} \mid m_i = \psi_i(m_{i+1})\}$. Since ring homomorphisms preserve both additive and multiplicative identities and $a_i + b_i = \psi_i(a_{i+1} + b_{i+1})$, $a_i b_i = \psi_i(a_{i+1} b_{i+1})$, we get that L is a subring of $\mathscr{R}$. Let's define $\alpha_n = \pi_n|_L$, where $\pi_n : \mathscr{R} \longrightarrow R_n$ is the canonical projection. We'll show that the pair $(L, \{\alpha_n\})$ is an inverse limit to the given system.

Let $(a_i) \in L$. We get $(\psi_n \circ \alpha_{n+1})((a_i)) = \psi_n(a_{n+1}) = a_n = \alpha_n((a_i))$. Hence, $\psi_n \circ \alpha_{n+1} = \alpha_n$. Now let $(R', \{\beta_n\})$ be another ring with homomorphisms such that $\psi_n \circ \beta_{n+1} = \beta_n$. Let $\Phi : R' \longrightarrow L$ be defined by $x \longmapsto (\beta_i(x))$. As $\psi_n \circ \beta_{n+1} = \beta_n$, this function is well-defined, and is trivially a ring homomorphism.

Moreover, $(\alpha_n \circ \Phi)(x) = \beta_n(x)$ for all x, meaning $\alpha_n \circ \Phi = \beta_n$. Finally, if $\theta : R' \longrightarrow L$ is a homomorphism such that $\alpha_n \circ \theta = \beta_n$ for all n, then, writing $\theta(x) = (m_i)$, we get $m_n = \alpha_n(\theta(x)) = \beta_n(x)$. Ergo, $\theta = \Phi$, finishing the proof. ∎

In view of the preceding proposition, we may refer to "the" inverse limit, and will denote it by $\varprojlim R_n$. As a consequence of our explicit construction, we have the following:

Corollary 3.4.1.1. *If the functions $\psi_n : R_{n+1} \longrightarrow R_n$ are surjective, then the same is true of the mappings $\alpha_n : \varprojlim R_i \longrightarrow R_n$.*

Proof. Let $x \in R_n$. We need to find a sequence $(y_i) \in L$ (returning to the notations of the preceding proposition) such that $y_n = x$. Since all ψ_i are surjective, there exists $z_{n+1} \in R_{n+1}$ such that $\psi_n(z_{n+1}) = x$ and, inductively, having obtained z_i, $i > n$, we may obtain $z_{i+1} \in R_{i+1}$ such that $\psi_i(z_{i+1}) = z_i$. Thus, we may define the sequence:

$$y_i = \begin{cases} (\psi_i \circ \cdots \circ \psi_{n-1})(x) & \text{if } 0 \leq i < n; \\ x & \text{if } i = n; \\ z_i & \text{if } i > n; \end{cases}$$

■

We may now prove some other, fairly technical results due to Lichtman (they are parts of proofs from [Lic95]). We begin as follows:

Proposition 3.4.2. *Let R be a domain and let $t \in R$ be central. Suppose $\bigcap_{i=0}^{\infty} t^i R = (0)$ and denote $R_n = R/t^n R$, $\mathfrak{t}_n = \pi_n(t)$, where $\pi_n : R \longrightarrow R_n$ is the canonical projection. Then, if R_1 is a right Ore domain, $R_n \setminus \mathfrak{t}_n R_n$ is a right denominator set for R_n.*

Proof. Let's denote $S_n = R_n \setminus \mathfrak{t}_n R_n$. By hypothesis, we may define a function $v : R \longrightarrow \mathbb{Z} \sqcup \{\infty\}$ as $v(x) = \max\{n \in \mathbb{N} \mid x \in t^n R\}, x \neq 0$ and $v(0) = \infty$. It is simple to check that it is a valuation of R. Let $x \in R$ be such that $\pi_n(x) = \overline{x} \in S_n$. Of course, $x \notin (t)$; otherwise, $\pi_n(x) = \mathfrak{t}_n \pi_n(r)$ for some $r \in R$, meaning, $v(x) = 0$.[9]

Suppose $\overline{xr} = 0$ for some $r \in R$; i.e., $xr \in (t)^n$. Then $n \leq v(xr) = v(x) + v(r) = v(r)$, and thus, $\overline{r} = 0$. The same argument also works for $\overline{rx}$, meaning S_n is a right reversible subset of R_n. All that's left is to check permutability.

By hypothesis, R_1 is a right Ore domain, which is equivalent to saying that $R_1^\dagger = S_1$ is a right denominator set. Suppose, then, as an inductive hypothesis, that S_{n-1} is right permutable and let $\overline{s} \in S_n, \overline{a} \in R_n$. By hypothesis, $(s + (t)^{n-1})R_{n-1} \cap (a + (t)^{n-1})S_{n-1} \neq \emptyset$. It's clear that $\pi_n((t)) = \pi_n(tR) = \mathfrak{t}_n R_n$, meaning $\pi_n(R \setminus (t)) = S_n$. Hence, there are $b \in R$, $u \in R \setminus (t)$ such that $z = sb - au \in (t)^{n-1}$.

If $z \in (t)^n$, the result is immediate. We may then assume $z = z_0 t^{n-1}$, $z_0 \in R \setminus (t)$. We get $sb - au - z_0 t^{n-1} = 0$. As R_1 is a right Ore domain, there exist $b_1 \in R$, $u_1 \in R \setminus (t)$ such that $sb_1 - z_0 u_1 \in (t)$. Hence:

$$\begin{cases} sb_1 t^{n-1} - z_0 u_1 t^{n-1} \in (t)^n \\ -sbu_1 + auu_1 + z_0 u_1 t^{n-1} \in (t)^n \end{cases} \implies s(-b_1 t^{n-1} + bu_1) + a(uu_1) \in (t)^n$$

As R_1 is a domain and $u, u_1 \in R \setminus (t)$, then $uu_1 \in R \setminus (t)$, meaning $\pi_n(uu_1) \in S_n$. Ergo, in R_n, we have $\overline{s}\overline{(bu_1 - b_1 t^{n-1})} = \overline{a}\overline{(uu_1)} \in \overline{s}R_n \cap \overline{a}S_n$. Therefore, S_n is a right denominator set for R_n, as we wished to show. ■

Proposition 3.4.3. *Under the conditions of Proposition 3.4.2, denote by Q_n the ring of fractions of R_n with respect to S_n. Then, the following are true:*

1. $(\mathfrak{t}_n Q_n)^n = 0$;
2. $Q_n/\mathfrak{t}_n Q_n \cong Q_1$;
3. *The surjective homomorphism $\phi_n : R_{n+1} \longrightarrow R_n$ given by $r + (t)^{n+1} \longmapsto r + (t)^n$ can be extended to a surjective homomorphism $\Phi_n : Q_{n+1} \longrightarrow Q_n$.*

Proof. 1. Follows from the fact that $\mathfrak{t}_n$ is central in Q_n and $\mathfrak{t}_n^n = \pi_n(t^n) = 0$;

[9] We will use (t) to denote the ideal generated by t. In particular, $(t) = tR$, since t is central. By convention, $(t)^0 = R$.

2. Let $\lambda_i : R_i \longrightarrow Q_i$ be the localization map $\lambda_i(r) = r/1$. We have an induced map $\psi : R \longrightarrow Q_1$, $\psi = \lambda_1 \circ \pi_1$. Since $(t)^n \subset (t)$, there exist homomorphisms $\psi_n : R_n \longrightarrow Q_1$, induced by the quotient. Furthermore, these are homomorphisms inverting S_n, as Q_1 is a division ring. Hence, Corollary 2.1.1.1 yields a homomorphism $\Psi_n : Q_n \longrightarrow Q_1$ extending ψ_n. It's trivial to check that it's surjective with kernel $\mathfrak{t}_n Q_n$.

3. The homomorphism $\varphi_n = \lambda_n \circ \phi_n$ inverts S_{n+1}, meaning it induces a homomorphism $\Phi_n : S_{n+1} \longrightarrow S_n$, which is surjective by definition.

■

Proposition 3.4.4. *Under the conditions of Proposition 3.4.3, let $Q = \varprojlim Q_i$ and $\mathfrak{t} = (\mathfrak{t}_n)_{n\in\mathbb{N}^\dagger}$. Then, Q is a local domain with maximal ideal $\mathfrak{t}Q$. Furthermore, $Q/\mathfrak{t}Q \cong Q_1$ and $\mathfrak{t}Q$ defines a valuation $\rho : Q \longrightarrow \mathbb{Z} \sqcup \{\infty\}$ in Q which extends the valuation v of R.*

Proof. By Corollary 3.4.1.1 and Proposition 3.4.3 item (3), the mappings α_n associated to the inverse limit Q are surjective, . Ergo for all $n \in \mathbb{N}^\dagger$, there exists an ideal I_n of Q such that $Q/I_n \cong Q_n$. Moreover, as $Q_n/\mathfrak{t}_n Q_n \cong Q_1$, there's a unique ideal J_n containing I_n such that $Q/J_n \cong Q_1$. In particular, each J_n is a maximal ideal.

Let $J = \bigcap J_n$. If $x \in Q \setminus J$, then $\alpha_n(x) \in Q_n \setminus \mathfrak{t}_n Q_n$, from the definition of J_n. In particular, $\alpha_n(x)$ is invertible. As this is true for all n, the definition of Q immediately yields that x is invertible in Q, meaning it is a local ring. In particular, $J_n = J$, for all n.

Now suppose, $x \in Q \setminus \mathfrak{t}Q$. Writing $x = (x_i)$, there's some i such that $x_i \notin \mathfrak{t}_i Q_i$. This, in turn, implies $x_i \in S_i$. Hence, there exists $\tilde{x} \in R \setminus (t)$ such that $\pi_i(\tilde{x}) = x_i$. In particular, $\pi_j(\tilde{x}) \in S_j$ for all $j < i$. By the definition of the inverse limit, $x_j \in S_j$ if $j > i$ (since $\Phi_k(\mathfrak{t}_{k+1}Q_{k+1}) \subset \mathfrak{t}_k Q_k$). Therefore, $x_i \in S_i$ for all i. In particular, x is invertible in Q. Thus, $J = \mathfrak{t}Q$. Moreover

$$\alpha_i\left(\bigcap_{n=1}^{\infty}(\mathfrak{t}Q)^n\right) \subset \bigcap_{n=1}^{\infty}(\alpha_i(\mathfrak{t}Q))^n = \bigcap_{n=1}^{\infty}(\mathfrak{t}_i Q_i)^n = (0)$$

using Proposition 3.4.3, item (1). It follows that $\bigcap_{n\in\mathbb{N}^\dagger}(\mathfrak{t}Q)^n = (0)$.

Define $\rho(x) = \max\{n \in \mathbb{N} \mid x \in (\mathfrak{t}Q)^n\}, x \neq 0$. Suppose $x, y \in Q$ are nonzero, with $xy = 0$. Of course $x, y \in \mathfrak{t}Q$. Ergo, $\rho(x) = n \geq 1, \rho(y) = m \geq 1$. This means $x = \mathfrak{t}^n s_1$, $y = \mathfrak{t}^m s_2$, where s_1, s_2 are invertible. Then, $\mathfrak{t}^{m+n} = 0$. But this is absurd, as $\mathfrak{t}^{m+n}_{m+n+1} \neq 0$. Therefore, Q is a domain.

Using the same reasoning as the preceding paragraph, we may show that ρ is a valuation, in a very similar fashion to what is done with v. Furthermore, R is naturally embedded in Q via $x \longmapsto (x + (t)^i)$, as $\bigcap(t)^i = (0)$. If $\rho(x) = k, x \in R^\dagger$, it's easy to see that $\alpha_n(x) \in \mathfrak{t}_n^k R_n \setminus \mathfrak{t}_n^{k+1} R_n$ if $n \geq k + 1$ and, therefore, $x \in t^k R \setminus t^{k+1} R$, which is equivalent to $v(x) = k$. Thus, ρ extends v, finishing the proof. ■

All of the preceding propositions may be summarized in the following theorem:

Theorem 3.4.5. *Let R be a domain and let $t \in R$ be central. Suppose $\bigcap (t)^i = (0)$ and $R/(t)$ is a right Ore domain. Then:*

1. *There exists a discrete valuation $v : R \longrightarrow \mathbb{Z} \sqcup \{\infty\}$ given by $v(x) = \max\{n \in \mathbb{N} \mid x \in (t)^n\}$ if $x \neq 0$ and $v(0) = \infty$;*
2. *R may be embedded in a division ring D and v may be extended to D;*
3. *The set $Q = \{x \in D \mid v(x) \geq 0\}$ is a local subring of D, with maximal ideal tQ satisfying $Q/tQ \cong \Delta$, where Δ is the total field of fractions of $R/(t)$;*

Proof. The theorem follows from Proposition 3.4.4, after constructing the ring of fractions of Q with respect to the (central) subset $\{\mathrm{t}, \mathrm{t}^2, \ldots\}$ and extending the function ρ to the resulting division ring, by $\rho(as^{-1}) = \rho(a) - \rho(s)$. Notice that t may be identified with $t \in R$, via the embedding seen in the previous proof, and that Q consists entirely of the elements x with $\rho(x) \geq 0$. ■

We may reinterpret the preceding theorem using the language of specializations. With this interpretation, the third item in the preceding theorem may be rewritten by saying there is a surjective specialization from D to Δ, where Δ is the total classical field of fractions of $R/(t)$. This is the actual result we will need for the last theorem we will prove. The following proposition by Fuchs ([Rei95]) will also be very useful.

Proposition 3.4.6. *Let R be a right Noetherian domain and let $t \in R$ be a central non-unit. Then, $\bigcap_{i=0}^{\infty} (t)^i = 0$.*

Proof. Evidently, we may assume $t \neq 0$. Suppose there exists $0 \neq a \in \bigcap_{i=1}^{\infty} Rt^i$. As $a \in Rt$, we get $a = a't$, implying $aR \subset a'R$. If $a'R \subset aR$, then $a' = ab$, for some b, meaning $abt = a$, and so, $a(bt - 1) = 0$. Since $a \neq 0$, we would get $bt = 1$. Since t is central, $tb = 1$, implying t is invertible, which goes against our hypothesis. Thus, $aR \subsetneq a'R$.

Now $a \in Rt^2$, and therefore $a = a''t^2$. Thus, $a't = a''t^2$, meaning $(a' - a''t)t = 0$. As $t \neq 0$, we have $a' = a''t$, and therefore, $a'R \subset a''R$. If $a''R \subset a'R$, then there exists b' such that $a'' = a'b' = a''tb'$. Thus, $tb' = 1$, and we arrive at the same contradiction as before. Thus, $aR \subsetneq a'R \subsetneq a''R$.

Proceeding inductively, we'll obtain an infinite ascending sequence of right ideals of R, which goes against the hypothesis that R is right Noetherian, a contradiction. ■

In the original paper which serves as the main reference for our work ([GMS99]), the authors rely on the following result of Lichtman and Eizenbud ([LE87]):

Theorem. *Let K be a field, G an ordered group and $N \trianglelefteq G$. Let X be a transversal for N in G and define $S = \left\{ \sum_{i \in I} \lambda_i x_i \mid \lambda_i \in KN, \{x_i \in X \mid i \in I\} \text{ well-ordered} \right\} \subset K((G))$. Then, S is a local ring, and the ideal $\Delta(G, N)S$ is such that:*

$$\frac{S}{\Delta(G,N)S} \cong K((G/N))$$

In the language of specializations, we can translate the result by saying that there is a specialization from $K((G))$ to $K((G/N))$. Unfortunately, this result is incorrect, at least in the way it is stated above ([Lic00, Remark, p. 674]). It is, however, true that there exists a proto-specialization from $K((G))$ to $K((G/N))$, as shown by the following result from J. Sánchez ([Sán14]).

Proposition 3.4.7. *Let K be a field, G an ordered group, $N \trianglelefteq G$ and suppose G/N is also an ordered group. Let X be a transversal for N in G and, given $\alpha \in G/N$, let $\hat{\alpha}$ be the unique element x_α of X such that $x_\alpha N = \alpha$. Write $K(G)$ for the division subring of $K((G))$ generated by KG. Then, there exist a subring S of $K(G)$ and a ring homomorphism $\Phi : S \longrightarrow K((G/N))$ such that, given $0 \neq \mathcal{L} = \sum_{\alpha\in G/N} r_\alpha \alpha \in K((G/N))$, the element $\sum_{\alpha\in G/N} r_\alpha \hat{\alpha}$ is a unit in S and maps to $\mathcal{L}$ via Φ.*

Proof. As the construction of the subring requires many results on so-called "cross products", we refer to [Sán14, Example 8 and Proposition 9] for the appropriate details. ■

Before presenting the main result in this section, we'll need a final proposition.

Proposition 3.4.8. *Let K be a field of characteristic not 2 and let $\theta : K[x] \longrightarrow K[x]$ be the homomorphism given by $\theta(x) = \lambda x$, with $\lambda \in K^\dagger$ transcendental over the prime field P of K. Then, $\langle 1 + \alpha x, 1 + \beta y\rangle$ is free in the multiplicative group of $K(x)(y; \theta)$, for all $\alpha, \beta \in K^\dagger$.*

Proof. Let $R = P[\lambda]$. Since λ is transcendental over P, the ideal $\mathfrak{p}$ generated by $(1 + \lambda)$ is prime. It thus induces a valuation in R, with valuation ring $R_\mathfrak{p}$ and maximal ideal $A = \mathfrak{p}_\mathfrak{p}$. By Proposition 3.3.7, the set $M = S \setminus AS$ is a right denominator set for the ring $S = R_\mathfrak{p}[x][y; \theta]$.

The maximal ideal of the local ring SM^{-1} may be identified with ASM^{-1}. In particular it's clear that $1 + \alpha x, 1 + \beta y \notin ASM^{-1}$ and are hence invertible in this localization. In the quotient, $yx + AM^{-1} = \lambda xy + AM^{-1} = -xy + AM^{-1}$. This is thus isomorphic to the division ring $P(x)(y; x \mapsto -x)$, using the same reasoning as in Theorem 3.3.8. This yields the result, by Proposition 3.3.6. ■

With all these results out of the way, we conclude our work with what is perhaps the biggest confluence of all the ideas presented in all three sections: the proof of Theorem 5 from [GMS99], which answers a question due to J. Lewin.

Theorem 3.4.9. *Let K be a field of characteristic not 2, G a residually torsion-free nilpotent group, $a, b \in K^\dagger$ and $x, y \in G$ two non-commuting elements of G. Then, $\langle 1 + ax, 1 + by\rangle$ is free in the multiplicative group of the division subring $K(G)$ of the Malcev-Neumann series ring $K((G))$ generated by KG.*

Proof. Let M be the subgroup of G generated by x, y. The proof can be divided in two cases:

- Case 1 - G is nilpotent

  Suppose there exists some G for which the result is false. We can thus take a counterexample such that M has minimal Hirsch number. Let's first suppose M nilpotent of class 2. In this case, $M = \langle x, y \mid \lambda = [x, y], [x, \lambda] = [y, \lambda] = 1\rangle$ is the so-called

Heisenberg group. Indeed, M has to satisfy the stated relations to be nilpotent of class 2.

Also, any other relation between x, y could be expressed as $\lambda^k x^m y^n = 1$, meaning $y^{-n} = \lambda^k x^m$. Then, $1 = [\lambda^k x^m, y] = [x^m, y]$, as commutators are central. Furthermore, by Corollary 1.3.11.1, $1 = [x^m, y] = [x, y]^m$. Thus, $m = 0$, since M is torsion-free. Then, y^{-n} is a power of λ, which is central, meaning $1 = [x, y^{-n}] = [x, y]^{-n}$, which implies $n = 0$. The relation now becomes $\lambda^k = 1$, which means $k = 0$ and proves the equality. In particular, if $\lambda^{k_1} x^{m_1} y^{n_1} = \lambda^{k_2} x^{m_2} y^{n_2}$, then $\lambda^{k_1 - k_2} x^{m_1 - m_2} y^{n_1 - n_2} = 1$. By the above, $k_1 = k_2$, $m_1 = m_2$ and $n_1 = n_2$. Therefore, every element of M can be uniquely expressed in this way.

Then, writing $\lambda = [x, y]$ and $L = K(\lambda)$, we can get a ring homomorphism from KM to $Q = L(x)(y; x \mapsto \lambda^{-1}x)$, by taking $\varphi : K \longrightarrow L$ to be the natural inclusion of K in L and $\psi : M \longrightarrow \mathfrak{U}(Q)$ such that $\psi(x) = x$ and $\psi(y) = y$. The presentation for M means that this indeed gives a group homomorphism. By Proposition 2.3.1, these combine to yield a ring homomorphism $\Psi : KM \longrightarrow Q$. We can write the evaluation of an element through Ψ as

$$\Psi\left(\sum_{g \in M} \alpha_g g\right) = \sum_{k,m,n \in \mathbb{Z}} \alpha_{\lambda^k x^m y^n} \lambda^k x^m y^n$$

from which we easily see that Ψ is injective.

It thus induces a homomorphism from the field of fractions of KM to Q (recall that KM is Noetherian by Corollary 2.3.3.1 and, in particular, right Ore rings by Corollary 2.1.1.4). By Proposition 3.4.8, $\langle 1 + ax, 1 + by \rangle$ is free in $\mathfrak{U}(Q)$ and, hence, in $\mathfrak{U}(Q(KM))$ (which goes against the choice of M). Ergo, M can't be nilpotent of class 2.

Let $c \in Z(M)$ be non-trivial and let $t = c - 1$. Since M is torsion-free, $\langle c \rangle \cong \mathbb{Z}$. In particular, the Hirsch number of $\overline{M} = M/\langle c \rangle$ is strictly less than that of M, by Proposition 1.5.8. Using Proposition 2.3.2,

$$\frac{KM}{(t)} \cong K\overline{M}$$

Since M and $\overline{M}$ are both finitely generated and nilpotent, just like in the case where M had nilpotent class 2, their respective group rings KM and $K\overline{M}$ are Noetherian and, therefore, right Ore rings. Moreover, both are domains (Corollary 2.3.6.2). Let, then, $Q(KM)$ and $Q(K\overline{M})$ be their respective total classical fields of fractions.

Since t is non-invertible, central, and KM is Noetherian, Proposition 3.4.6 yields $\bigcap_{i \in \mathbb{N}^\dagger} (t)^i = (0)$. By Theorem 3.4.5, there exists a surjective specialization from $Q(KM)$ to $Q(K\overline{M})$. Since M isn't of class 2, the images of x, y don't commute in $\overline{M}$. The minimality of M gives us that $\langle 1 + a\overline{x}, 1 + b\overline{y} \rangle$ is a free pair in $Q(K\overline{M})$. This is a contradiction, since the pair can then be lifted to $Q(KM)$.

- Case 2 - General case

  By Proposition 1.4.1, there exists a sequence $G = N_0 \supset N_1 \supset N_2 \supset \ldots$ of normal subgroups of G such that $G_i = G/N_i$ is torsion-free nilpotent for all i and $\bigcap_{i\in\mathbb{N}} N_i = 1$. Write D and D_i for the subdivision rings of the Malcev-Neumann series rings generated by KG and KG_i. Choose some i such that $[x, y] \notin N_i$ (i.e., such that the images of x and y don't commute in G_i). In particular, $x, y \notin N_i$ (if either were in N_i, so would $[x, y]$).

  Also, x and y don't lie on the same coset of N_i. If that were the case, then both $y^{-1}x$ and $x^{-1}y$ are in N_i, meaning $[x, y] = x^{-1}(y^{-1}x)x(x^{-1}y) \in N_i$, since it is a normal subgroup. Thus, we can choose a transversal X for N_i in G such that both $x \in X$ and $y \in X$.

  Consider the elements $1 + a\overline{x}$ and $1 + b\overline{y}$ in D_i. Since the group G/N is torsion-free nilpotent, the first case shows that this pair is free. Now, by Proposition 3.4.7, there exist a subring S of $K(G) = D$ and a homomorphism $\Phi : S \longrightarrow K((G/N_i))$ such that $1 + ax = 1 + a\hat{\overline{x}}$ and $1 + by = 1 + b\hat{\overline{y}}$ are units in S and map to $1 + a\overline{x}$ and $1 + b\overline{y}$ respectively. By Proposition 1.1.3, they are a free pair in S and hence, in D, finishing the proof.

■

Appendix A

Division rings with involution

Even though this isn't the goal of our work, it's worth singling out a variant of Lichtman's Conjecture that was the focus of the other sections. Indeed, multiple families of division rings come endowed with an **involution**; that is, an antimorphism of order 2.

There are two natural examples where this occurs. First of all, if G is a finitely generated torsion-free nilpotent group and K is a field, then $\sum \alpha_g g \longmapsto \sum \alpha_g g^{-1}$ is an involution of KG which induces an involution in its total classical field of fractions. And second, when $\left(\frac{a,b}{K}\right)$ is a division ring, it admits the **symplectic involution** $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \longmapsto a - b\mathbf{i} - c\mathbf{j} - d\mathbf{ij}$ and the **orthogonal involution** $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \longmapsto a + b\mathbf{i} + c\mathbf{j} - d\mathbf{ij}$.

If D is a division ring with involution $*$, it's natural to ask if there's a free pair in the multiplicative group $D^\dagger$ which interacts nicely with the involution in some way. There are two natural candidates: elements which are left fixed by the involution (i.e., such that $x^* = x$) and elements upon which the involution acts as the natural group antimorphism $^{-1}$ (i.e., such that $x^* = x^{-1}$). The former is the set of **symmetric** elements and the latter, that of the **unitary** elements. The following conjecture then arose:

Conjecture 1. *If D is a division ring with an involution *, then $D^\dagger$ contains free symmetric and unitary pairs.*

The way this is formulated, the conjecture is known to be false. Indeed, if K is a field of characteristic not 2 and $a, b \in K^\dagger$, then the symmetric elements of $\left(\frac{a,b}{K}\right)$ with the symplectic involution are central, and the unitary elements with the orthogonal involution form an abelian group. Hence, in any case, they can't contain free pairs (it's worth noting that, in the first case, the unitary elements contain a free pair and, in the second case, the same is true of the symmetric elements). Adapting the conjecture results in:

Conjecture 2. *Let D be a division ring with involution * and center Z, such that $[D : Z] > 4$. Then, $D^\dagger$ contains free symmetric and unitary pairs.*

This conjecture has received quite a bit of attention in the last few years (see, for instance, [GP20], [GFS19], [Gon17]) and is also still unanswered, in part due to the same difficulties presented by Lichtman's original conjecture, with the extra difficulty of restricting what are deemed "good" free pairs.

Appendix B

Free groups of higher rank

Finally, as we've noted before, whenever a free pair is obtained in the multiplicative group of a division ring, one can explicitly find free groups of arbitrary countable rank (Proposition 1.1.4). However, some division rings contain a higher level of symmetry.

As an example, the quaternion algebras contain three analogous elements (namely $\mathbf{i}, \mathbf{j}, \mathbf{ij} = \mathbf{k}$) and we've seen that, under suitable conditions, $1 + \alpha\mathbf{i}, 1 + \beta\mathbf{j}$ form a free pair. Would it perhaps be true, under certain conditions, that $1 + \alpha\mathbf{i}, 1 + \beta\mathbf{j}, 1 + \gamma\mathbf{k}$ freely generate a free group of rank three?

Remarkably, the answer, at least over the rational numbers, is that, in a considerable number of cases, the above triple indeed freely generates a free group, as we present in the following theorem ([GSed]), which is the more general form of Proposition 3.2.8.

Theorem B.0.1. *Let $0, \pm 1 \neq \alpha \in \mathbb{Q}$ and let $H = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Then: $\langle 1 + \alpha\mathbf{i}, 1 + \alpha\mathbf{j}, 1 + \alpha\mathbf{k}\rangle \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z}$.*

Other examples of results of this kind were already shown in Chapter 3, Section 1, both in Proposition 3.2.9 and in Proposition 3.2.10.

The same question can be posed for group algebras over torsion-free nilpotent groups: can we generalize Theorem 3.4.9 for three or more non-commuting elements? In general, the answer doesn't appear to be known, but, at least in the special case of a free nilpotent group of class 2 and rank 3, the answer is affirmative:

Theorem B.0.2. *Let Γ_3 be the free nilpotent group of class 2 and rank 3, generated by elements x_1, x_2, x_3 and let D be the total classical field of fractions of the group algebra $\mathbb{Q}\Gamma_3$. Then, for all $0, \pm 1 \neq \alpha \in \mathbb{Q}$, $\langle 1 + \alpha x_1, 1 + \alpha x_2, 1 + \alpha x_3\rangle \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z}$.*

The list is far from exhaustive, and suggests taking advantage of natural symmetries in division rings may provide hints towards explicitly obtaining "natural" free groups of higher rank.

References

[AM94] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra.* Ed. by CRC Press. 1994 (cit. on p. 51).

[Art27] E. Artin. “Zur Theorie der hyperkomplexen Zahlen”. In: *Abh.Math.Semin.Univ.Hambg.* 5 (1927), pp. 261–270 (cit. on p. 1).

[BC68] B. Baumslag and B. Chandler. *Schaum’s outlines: Group theory.* Ed. by McGraw Hill. 1968 (cit. on p. 7).

[Bra49] R. Brauer. “On a theorem of H. Cartan”. In: *Bull. Amer. Math. Soc.* 55 (1949), pp. 619–620 (cit. on p. 1).

[Car47] H. Cartan. “Théorie de Galois pour les corps non commutatifs”. In: *Ann. Sci. Ecole Norm. Sup.* 64 (1947), pp. 59–77 (cit. on p. 1).

[Coh03] P. M. Cohn. *Further Algebra and Applications.* Ed. by Springer. 2003 (cit. on pp. 33, 36, 37).

[Coh08] P. M. Cohn. *Skew Fields.* Ed. by Cambridge University Press. 2008 (cit. on p. 66).

[End72] O. Endler. *Valuation Theory.* Ed. by Berlin-Heidelberg-New York Springer-Verlag. 1972 (cit. on p. 54).

[Fuc63] L. Fuchs. *Partially Ordered Algebraic Number Systems.* Ed. by Dover. 1963, pp. 36–37 (cit. on pp. 25, 26).

[GFS19] J. Z. Gonçalves, V. O. Ferreira, and J. S. Serdà. “Free Symmetric and Unitary Pairs in the Field of Fractions of Torsion-Free Nilpotent Group Algebras”. In: *Algebras and Representation Theory* 2019 (2019), pp. 1–15 (cit. on pp. 19, 79).

[GMS99] J. Z. Gonçalves, A. Mandel, and M. Shirvani. “Free products of units in algebras I. Quaternion algebras”. In: *J. Algebra* 214 (1999), pp. 301–316 (cit. on pp. iii, v, 47, 57, 59, 69, 74, 75).

[Gon17] J. Z. Gonçalves. “Free pairs of symmetric and unitary units in normal subgroups of a division ring”. In: *J. Algebra and its Applications* 16 (2017) (cit. on p. 79).

[Gon84] J. Z. Gonçalves. “Free groups in subnormal subgroups and the residual nilpotence of the group of units of groups rings”. In: *Canad. Math. Bull.* 27 (1984), pp. 365–370 (cit. on p. 2).

[GP20] J. Z. Gonçalves and D. S. Passman. “Free pairs of symmetric elements in normal subgroups of division rings”. In: *J. Algebra* 550 (2020), pp. 154–185 (cit. on pp. 66, 79).

[GSed] J. Z. Gonçalves and G. A. L. Souza. “Elements generating a rank three subgroup in the multiplicative group of a division ring”. In: *J. Algebra and its Applications* (submitted) (cit. on pp. 59–61, 81).

[Her75] I. N. Herstein. *Topics in Algebra, Second Edition.* Ed. by John Wiley and Sons. 1975 (cit. on p. 56).

[Hig52] G. Higman. “Ordering by Divisibility in Abstract Algebras”. In: *Proceedings of the London Mathematical Society* s3-2 (1952), pp. 326–336 (cit. on p. 29).

[Hua49] L. Hua. “Some properties of a sfield”. In: *Proc. Nat. Acad. Sci. USA* 35 (1949), pp. 533–537 (cit. on p. 1).

[Isa11] I. M. Isaacs. *Finite Group Theory*. Ed. by AMS Graduate Studies in Mathematics. 2011 (cit. on pp. 12, 13).

[Jan96] G. J. Janusz. *Algebraic Number Fields, Second Edition*. Ed. by American Mathematical Society. 1996, p. 86. ISBN: 0-8218-0429-4 (cit. on pp. 49, 51–55, 61, 66).

[Kap51] I. Kaplansky. “A Theorem on Division Rings”. In: *Canadian Journal of Mathematics* 3 (1951), pp. 290–292 (cit. on p. 1).

[Lam01] T. Y. Lam. *A First Course in Noncommutative Rings, Second Edition*. Ed. by Springer. 2001 (cit. on pp. 1, 25, 29, 36, 37, 40, 64).

[Lam04] T. Y. Lam. *Quadratic Forms Over Fields*. Ed. by AMS Graduate Studies in Mathematics. 2004 (cit. on p. 57).

[Lam99] T. Y. Lam. *Lectures on Modules and Rings*. Ed. by Springer. 1999 (cit. on p. 33).

[LE87] A. I. Lichtman and A. Eizenbud. “On embedding of group rings of residually torsion free nilpotent groups into skew fields”. In: *Trans. Amer. Math. Soc* 299 (1987), pp. 373–386 (cit. on p. 74).

[Lic00] A. I. Lichtman. “On Universal Fields of Fractions for Free Algebras”. In: *Journal of Algebra* 231 (2000), pp. 652–676 (cit. on p. 75).

[Lic77] A. I. Lichtman. “On the subgroups of the multiplicative group of skew-fields”. In: *Proc. Amer. Math. Soc* 63 (1977), pp. 15–16 (cit. on pp. iii, v, 2).

[Lic78] A. I. Lichtman. “Free subgroups of normal subgroups of the multiplicative group of skew fields”. In: *Proc. Amer. Math. Soc* 71 (1978), pp. 174–178 (cit. on p. 68).

[Lic95] A. I. Lichtman. “Valuation methods in division rings”. In: *J. Algebra* 177 (1995), pp. 870–898 (cit. on p. 72).

[LS01] R. Lyndon and P. Schupp. *Combinatorial Group Theory - Reprint of the 1977 ed.* Ed. by Springer. 2001, p. 177. ISBN: 3-540-41158-5 (cit. on pp. 8–10).

[McC76] P. J. McCarthy. *Algebraic Extensions of Fields*. Ed. by Dover. 1976 (cit. on p. 49).

[MKS75] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*. Ed. by Dover. 1975 (cit. on pp. 8–10, 13).

[MS02] C. P. Milies and S. K. Sehgal. *An Introduction to Group Rings*. Ed. by Kluwer Academic Publishers. 2002 (cit. on p. 40).

[Pas14] D. S. Passman. *The Algebraic Structure of Group Rings*. Ed. by Dover. 2014 (cit. on pp. 13, 40).

[Rei95] M. Reid. *Undergraduate Commutative Algebra*. Ed. by Cambridge. 1995 (cit. on p. 74).

[Rib99] P. Ribenboim. *The Theory of Classical Valuations*. Ed. by Springer. 1999 (cit. on p. 49).

[Rob96] D. J. S Robinson. *A Course in the Theory of Groups, Second Edition*. Ed. by Springer. 1996 (cit. on pp. 20, 23).

[Rot99] J. J. Rotman. *An Introduction to the Theory of Groups, Fourth Edition*. Ed. by Springer. 1999 (cit. on pp. 3, 7, 8, 10, 13, 14, 20–22).

[Sam08] P. Samuel. *Algebraic Theory of Numbers*. Ed. by Dover. 2008 (cit. on p. 51).

[Sán14] J. Sánchez. “Free Group Algebras in Malcev-Neumann Skew Fields of Fractions”. In: *Forum Mathematicum* 26.2 (2014), pp. 443–466 (cit. on p. 75).

[Stu64] C. Stuth. “A Generalization of the Cartan-Brauer-Hua Theorem”. In: *Proc. Amer. Math. Soc* 15.2 (1964), pp. 211–217 (cit. on p. 1).

[SY74] Berlin Springer-Verlag and New York, eds. *Proceedings of the Second International Conference on the Theory of Groups, (Canberra. Australia, 1973)*. Vol. 372. Lecture Notes in Math. 1974 (cit. on p. 2).

[Tit72] J. Tits. “Free groups in linear groups”. In: *J. Algebra* 20 (1972), pp. 250–270 (cit. on p. 1).

[Wed05] J. Wedderburn. “A theorem on finite algebras”. In: *Transactions of the American Mathematical Society* 6 (1905), pp. 349–352 (cit. on p. 1).

Index