Around the Jacobian Conjecture

The Jacobian Conjecture for free groups, a generalization of Duistermaat-Van der Kallen in dimension one, and classifying Mathieu-Zhao spaces of finite rings

J. J. P. Schoone, s0815217

August, 2018

Master's Thesis in Mathematics
Department of Mathematics
Radboud University, Nijmegen
Supervisor: Dr. A. R. P. van den Essen
Second reader: Dr. W. Bosma

Abstract

This thesis contains various results surrounding the Jacobian Conjecture. The first chapter is concerned with the Jacobian Conjecture for free groups, which is essentially a worked-out proof of [2].

Then we fast-forward in time by about 35 years and discuss the notion of Mathieu-Zhao spaces, first introduced by Zhao after noticing similarities between various conjectures implying the Jacobian Conjecture, including the Mathieu Conjecture. For the history about this, see [7].

On this subject a proof of a generalized version of Duistermaat and Van der Kallen's theorem (which in itself is the abelian version of the Mathieu Conjecture) in one dimension is given, based on joint work with Van den Essen.

The last subject in this thesis are the first steps in classifying all MZ-spaces of finite commutative rings with identity.

Preface

Back in 2015 I followed a course called *Polynomial Mappings*. This followed [6] as its main text. During this course I learned many new ways of proving theorems. These lectures, in combination with the lectures on *Commutative Algebra* a year earlier, convinced me that I wanted to write a thesis with Arno.

Arno introduced me to the notion of Mathieu spaces. At the time I was not interested in them, as all writing I found about them contained only very difficult theorems and proofs. Instead, I asked for another subject surrounding the Jacobian Conjecture. Recently, he found out about [2], and asked me to read that article and study it until I completely understood it. This took about two weeks of non-stop mathematics (literally). Then two years later I really needed to work hard again to actually put down the proofs in writing. The result is chapter 1. I am greatly indebted to prof. Van Rooij for helping me understand the Functional Analysis needed here, a subject I was never very familiar with.

Then the subject of writing a thesis remained dormant for a while. At a certain point in time, Arno approached me with another subject: Kernels that are Mathieu-Zhao spaces. This can be found in chapter 3. Even though I found Mathieu-Zhao spaces no longer as frightening as I did before, since I now understood at least one difficult proof, I was still not sure I wanted my thesis to go in that direction.

In May of 2017, prof. Zhao visited Nijmegen. During his talk he mentioned that even for *finite* rings, nothing was known about the MZ-spaces. This sparked my interest, as my Bachelor's thesis was about the subject of classifying finite rings. Two weeks later I started to think about the example he mentioned in his talk ($\mathbf{Z}/100\mathbf{Z}$) and solved the more general case $\mathbf{Z}/n\mathbf{Z}$ in fifteen minutes.

That point was the real start of my interest in MZ-spaces. The results of this venture can be found in the last chapter, while chapter 2 deals with general results about MZ-spaces. My interest has actually grown so much that right now all I want to do is continue the research into this subject – who would have thought?

What remains is to explain the logical dependencies of the various chapters in a simple diagram:

$$\begin{tikzcd}
1 & 2 \arrow[r] \arrow[d] & 3 \\
 & 4 &
\end{tikzcd}$$

When finishing this thesis, many friends offered to proofread the final version of this thesis. I am already grateful for this offer, even though some of them were unable to proofread this due to time constraints, solely caused by myself. I specifically want to thank Alex, Ton and Wouter for their time.

For his help in understanding the Functional Analysis needed in the first chapter and communicating some theorems to me, I am indebted to prof. Van Rooij.

Many thanks go out to dr. Bosma for careful reading of this thesis and suggesting many edits for better reading that will also help in my future writing.

To prof. Zhao I am very grateful for visiting Nijmegen, introducing this notion of MZ-spaces and sparking my interest in researching the subject.

Next, although this may seem to come 'out of the blue', is my profound thanks to dr. Kortram, who was always there for me when I had a course in Analysis or Applied Mathematics that I could not pass. Many of these courses I still would not have passed if it were not for him.

In a similar way, I want to thank my study advisor, Ina, for her continued support and help during my studies, right until the end (and back).

I am most indebted to my supervisor, Arno, for his many years of guidance through the field of mathematics. Just as outside of mathematics he has been, and continues to be, an inspiration for me. I hope that we will be able to continue discussing the many aspects of life for a long time, my friend.

But most of all, I am thankful to my parents, who, even though the level of mathematics that I work on is difficult for them to grasp, were always supportive of my studies. Without this support I would have quit mathematics a long time ago.

Thank you, to all teachers in Nijmegen, all students I have met during my ten years here, and all my friends who have made my life as a student worthwhile.

Contents

Chapter 1

Inverse Function Theorem for Free Groups

The Inverse Function Theorem from Analysis is well-known. When we write down the equivalent for Polynomial Rings, we get the Jacobian Conjecture. This conjecture is yet unsolved. In 1973, Joan Birman [2] proved a similar result for Free Groups. We discuss her proof in this chapter. It uses free differential calculus, as defined by Ralph H. Fox in [8]. This has later been named Fox Calculus. We will discuss this in section 1.3.

In [6], one can read about the Jacobian Conjecture. For completeness, we shall state the most essential.

We write $\mathrm{J}\,F$ for the Jacobian matrix

$$\mathrm{J}\,F = \left(\frac{dF_i(X)}{dX_j}\right)_{1\leq i,j\leq n}.$$

Conjecture. (Jacobian Conjecture) *Let k be a field of characteristic zero. Let $F\colon k^n \to k^n$ be a polynomial map such that $\det \mathrm{J}\,F \in k^*$. Then F is invertible.*

The converse of this conjecture is clearly true:

Suppose F is invertible with inverse G, then

$$(G_1(F_1(X_1,\dots,X_n),\dots,F_n(X_1,\dots,X_n)),\dots,G_n(F_1(X_1,\dots,X_n),\dots,F_n(X_1,\dots,X_n)))$$
$$= (X_1,\dots,X_n).$$

For brevity, we write $X = (X_1,\dots,X_n)$, $G = (G_1,\dots,G_n)$ and $F = (F_1,\dots,F_n)$, so

$$G(F(X)) = X.$$

By the chain rule of differential calculus we get

$$(\mathrm{J}\,G)(F(X)) \cdot \mathrm{J}\,F(X) = I.$$

Then by taking determinants, we find $\det(\mathrm{J}\,G)(F(X)) \cdot \det \mathrm{J}\,F(X) = 1$. Hence, since $k[X]^* = k^*$, we find that $\det \mathrm{J}\,F \in k^*$.

It is known that the Jacobian Conjecture is false in characteristic > 0 and true for $n = 1$ in characteristic 0 :

Example 1.0.1. *Consider k a field of characteristic $p > 0$ and $F(X) = X - X^p$. Then clearly $\det \mathrm{J}\,F = 1 - pX^{p-1} = 1$. But we have $F(0) = F(1) = 0$, hence F is not injective and hence not invertible.*

The above example can be easily generalized for arbitrary n :

$$F = (F_1, \dots, F_n) = (X_1 - X_1^p, \dots, X_n - X_n^p)$$

has $\mathrm{J}\, F = I_n$, while $X_1 = \dots = X_n = 0$ and $X_1 = \dots = X_n = 1$ both yield 0 again.

Example 1.0.2. *Let k be a field of characteristic zero and consider $F\colon k \to k$ a polynomial map. Then, if $\det \mathrm{J}\, F \in k^*$, we have $F' \in k^*$. Hence F is of the form $\alpha X + \beta$, where $\alpha \in k^*$ and $\beta \in k$. Then the inverse is given by $G = \alpha^{-1}X - \alpha^{-1}\beta$:*

$$F \circ G = \alpha(\alpha^{-1}X - \alpha^{-1}\beta) + \beta = X - \beta + \beta = X.$$

By the following lemma, we have a different formulation of the Jacobian Conjecture:

Lemma 1.0.3. *Let $F\colon k^n \to k^n$ be a polynomial map. Then F is invertible iff $k[X_1, \dots, X_n] = k[F_1, \dots, F_n]$.*

Proof. $\Rightarrow$:) If F is invertible with inverse G, then $X_i = G_i(F_1, \dots, F_n)$ for each $i = 1, \dots, n$. Hence $k[X_1, \dots, X_n] = k[F_1, \dots, F_n]$, as $k[F_1, \dots, F_n] \subset k[X_1, \dots, X_n]$ is trivial.
$\Leftarrow$:) If $k[X_1, \dots, X_n] = k[F_1, \dots, F_n]$, then $X_i \in k[F_1, \dots, F_n]$, i.e., $X_i = G_i(F_1 \dots, F_n)$ for some G_i. Hence F is invertible with inverse $G = (G_1, \dots, G_n)$. △

Using this, we can formulate the Jacobian Conjecture as follows:

Conjecture. (Jacobian Conjecture) *Let k be a field of characteristic zero. Let $F\colon k^n \to k^n$ be a polynomial map such that* $\det \mathrm{J}\, F \in k^*$. *Then $k[X_1, \dots, X_n] = k[F_1, \dots, F_n]$.*

We now invite the reader to skip ahead compare this result to Theorem 1.2.13 and observe the similarity.

1.1 Prerequisites on group rings

In this section we shall discuss results on group rings necessary for the rest of this chapter. Some results will be used in other chapters as well.

Definition 1.1.1. *Given a group G and a ring R, we can define the* group ring *$R[G]$ as the set of formal expressions*

$$\sum_{g \in G} \alpha_g g,$$

where $\alpha_g \in R$ and $\alpha_g = 0$ for all but a finite number of $g \in G$.
Addition is defined by

$$\sum_g \alpha_g g + \sum_g \beta_g g = \sum_g (\alpha_g + \beta_g) g$$

and multiplication by

$$\sum_g \alpha_g g \cdot \sum_h \beta_h h = \sum_{g,h} (\alpha_g \beta_h) gh = \sum_g \left(\sum_h \alpha_{gh^{-1}} \beta_h \right) g$$

We can also define a multiplication by scalars from R by setting

$$r\sum_g \alpha_g g = \sum_g (r\alpha_g)g$$

This makes $R[G]$ into an R-module.

When R is a commutative ring, we will also speak of a *group algebra* and when R is a field, we can also regard $R[G]$ as an R-vector space.

It is clear that for $R[G]$ to be commutative, we need R commutative and G abelian. Also note that the set of elements of G forms a basis for $R[G]$ as a free R-module (or R-vector space).

Before we give some examples of group rings, we state and prove a lemma.

Lemma 1.1.2. *Let R be a ring and C_n the cyclic group of order n. Then $R[C_n] \cong R[X]/(X^n - 1)$.*

Proof. Consider $\varphi\colon R[X] \to R[C_n]$ with $\varphi_{|R} = \mathrm{id}_R$ and $\varphi(X) = g$, where $\langle g\rangle = C_n$. In the usual fashion φ can be extended to a ring homomorphism:

$$\sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} a_i g^i.$$

This φ is then surjective. Its kernel clearly contains $(X^n - 1)$. Suppose $f \in \operatorname{Ker}\varphi$, then $\varphi(f) = 0$.

If $m < n$, then $a_0 + a_1 g + \ldots a_m g^m = 0$ implies that $a_0 = a_1 = \ldots = a_m = 0$ since $R[G]$ is a free R-module with basis $\{1, \ldots, g^{n-1}\}$.

Now suppose that $m \geq n$. Write $f = q(X^n - 1) + r$, with $q, r \in R[X]$ and $\deg r < n$ by Euclidean division. We find that

$$0 = \varphi(f) = \varphi(q)\varphi(X^n - 1) + \varphi(r) = \varphi(r).$$

Since $\deg r < n$, we find by the above that $r = 0$. Hence $f \in (X^n - 1)$. The result follows by the First Isomorphism Theorem. △

Example 1.1.3. $(\mathbf{Q}^2)$: *Consider the field of rational numbers $\mathbf{Q}$ and the cyclic group of order 2, C_2. Then by the above we have*

$$\mathbf{Q}[C_2] \cong \mathbf{Q}[X]/(X^2 - 1).$$

Since $(X^2 - 1) = (X - 1)(X + 1)$ and $\frac{1}{2}(X + 1) - \frac{1}{2}(X - 1) = 1$ we find by the Chinese Remainder Theorem that

$$\mathbf{Q}[C_2] \cong \mathbf{Q}[X]/(X - 1) \times \mathbf{Q}[X]/(X + 1) \cong \mathbf{Q}^2.$$

The preceding example holds for any field $\mathbb{F}$ of characteristic $\neq 2$:

$$\mathbb{F}[C_2] \cong \mathbb{F}^2.$$

For a field $\mathbb{F}$ of characteristic 2, we instead have

$$\mathbb{F}[C_2] \cong \mathbb{F}[X]/(X^2) \cong \mathbb{F}[\varepsilon],$$

with $\varepsilon^2 = 0$.

Example 1.1.4. $(\mathbf{Q} \times \mathbf{Q}(\sqrt{-3}))$: *Let C_3 be the cyclic group of order 3. Then we have*

$$\mathbf{Q}[C_3] \cong \mathbf{Q}[X]/(X^3 - 1).$$

Since $\frac{1}{3}(X^2+X+1) - \frac{1}{3}(X+2)(X-1) = \frac{1}{3}(X^2+X+1-X^2+X-2X+2) = 1$, *we find by the Chinese Remainder Theorem that*

$$\mathbf{Q}[C_3] \cong \mathbf{Q}[X]/(X-1) \times \mathbf{Q}[X]/(X^2+X+1) \cong \mathbf{Q} \times \mathbf{Q}(\zeta_3) = \mathbf{Q} \times \mathbf{Q}(\sqrt{-3}).$$

Proposition 1.1.5. *Given a (commutative) ring R and groups G and H, then we have*

$$\mathrm{Mat}_n(R[G]) \cong \mathrm{Mat}_n(R)[G]$$

and

$$R[G \times H] \cong R[G][H].$$

Proof. The maps $\phi\colon \mathrm{Mat}_n(R[G]) \to \mathrm{Mat}_n(R)[G]$ defined by

$$\left(\sum_g \alpha_{ij,g} g\right)_{\substack{1\le i\le n\\1\le j\le n}} \mapsto \sum_g \left(\alpha_{ij,g}\right)_{\substack{1\le i\le n\\1\le j\le n}} g$$

and $\psi\colon R[G \times H] \to R[G][H]$ defined by

$$\sum_{(g,h)\in G\times H} \alpha_{(g,h)}(g,h) \mapsto \sum_{h\in H}\left(\sum_{g\in G}\alpha_{(g,h)} g\right) h$$

are isomorphisms in both **Ring** and R-**Mod**. □

As seen in the examples above, group rings aren't necessarily fields. Since they aren't commutative, left inverses might not even be right inverses. We study when left inverses are indeed right inverses. It is clear that for all $\alpha_g \in R^*$ and $g \neq e$, the element $\alpha_g g$ is invertible, its inverse being $\alpha_g^{-1} g^{-1}$. For these kind of units it is trivial that $xy = 1$ implies $yx = 1$. We now show some results of group rings where this holds in general.

Lemma 1.1.6. *Let R be a ring and G a* finite *group. If $x, y \in R[G]$ and $xy = 1$, then $yx = 1$.*

Proof. Let $x, y \in R[G]$ with $xy = 1$. Consider the following maps:

$$x\cdot\colon R[G] \to R[G],\ \alpha \mapsto x\alpha,$$

$$y\cdot\colon R[G] \to R[G],\ \alpha \mapsto y\alpha,$$

then $x \cdot \circ y \cdot = \mathrm{id}$. Hence $y\cdot$ is an injective map and $x\cdot$ is surjective.
Since $R[G]$ is finitely generated as an R-module, we find that $x\cdot$ is also injective by Poposition 1.1.7.
Hence $yx\cdot = y \cdot \circ x\cdot$ is injective.
Now consider $yxyx = yx$, hence $yx(yx-1) = 0$. Since $yx\cdot$ is an injective map, we get $yx - 1 = 0$, hence $yx = 1$. △

We have used

Proposition 1.1.7. *Let M be a finitely generated R-module and let $\varphi\colon M \to M$ be a surjective R-module homomorphism. Then φ is also injective, hence an R-module automorphism.*

Proof. Consider M as an $R[X]$-module via the multiplication $f(X) \cdot m = f(\varphi)(m)$. Then surjectivity of φ translates to $M = XM$. Hence for the ideal $I = XR[X]$ of $R[X]$ we have $M = IM$. Then by Nakayama's Lemma (see Proposition 1.1.8) there exists an element $Xg(X) \in I$ such that $m = Xg(X)m$ for all m. I.e., $m = \varphi(g(\varphi)(m))$. Hence the inverse for φ is $g(\varphi)$. □

The above proof is based on Nakayama's Lemma, an important result in Commutative Algebra:

Proposition 1.1.8. *(Nakayama's Lemma) Let R be a commutative ring with identity and let I be an ideal of R. If M is a finitely generated R-module such that $M = IM$, then there exists an $i \in I$ such that for all $m \in M$ we have $m = im$.*

The following generalisation of Proposition 1.1.6 holds:

Lemma 1.1.9. *Let R be a ring and G a* finite *group. If $X, Y \in \mathrm{Mat}_n(R[G])$ and $XY = I_n$, then $YX = I_n$.*

Proof. By Proposition 1.1.5 we have $\phi(X)\phi(Y) = \phi(I_n) = 1 \in \mathrm{Mat}_n(R)[G]$, hence by Lemma 1.1.6 we have $\phi(Y)\phi(X) = 1 = \phi(I_n)$. Since ϕ is an isomorphism, we have $YX = I_n$, as required. △

1.1.1 Main Theorem

The main result of section 1.1 is the following theorem:

Theorem. *Let G be a group and X, Y elements of $\mathrm{Mat}_n(\mathbf{C}[G])$ such that $XY = I_n$, then $YX = I_n$.*

This theorem is essential for the proof of the Inverse Function Theorem for Free Groups, but its proof is rather lengthy (we adopt the proof of Susan Montgomery [12]). It can be skipped if the reader is not familiar with the concepts of Functional Analysis used here. Before we can start with proving this theorem, we discuss a few notions of Functional Analysis.

1.1.2 C^*-algebras and other prerequisites

In this section we assume a certain familiarity with Hilbert spaces and (linear) operators. The most important results are stated and proved.

Definition 1.1.10. *Let $\mathfrak{A}$ be an associative $\mathbf{C}$-algebra, let $\| - \|$ be a norm on the $\mathbf{C}$-vector space $\mathfrak{A}$, and let $*\colon \mathfrak{A} \to \mathfrak{A}, L \mapsto L^*$ be a $\mathbf{C}$-antilinear map. Then $(\mathfrak{A}, \| - \|, *)$ is called a C^*-algebra if $(\mathfrak{A}, \| - \|)$ is complete and for all $x, y \in \mathfrak{A}$ we have:*

1. $x^{**} = x$;
2. $(xy)^* = y^*x^*$;
3. $\|xy\| \leq \|x\|\|y\|$;
4. $\|x^*\| = \|x\|$;

5. $\|x^*x\| = \|x\|^2$.

Example 1.1.11. *Let $(\mathcal{H}, \langle -,-\rangle)$ be a complex Hilbert space, let $\| - \|_0$ be the norm induced by $\langle -,-\rangle$, let $\mathfrak{A} = B(\mathcal{H})$ be the algebra of bounded linear operators on $\mathcal{H}$. Let $\| - \|$ be the operator norm, i.e.*

$$\|L\| := \sup_{x\in\mathcal{H}; \|x\|_0=1} \|Lx\|_0.$$

Let L^* be the operator adjoint to L, i.e., $\langle Lx, y\rangle = \langle x, L^*y\rangle$ for all $x, y \in \mathcal{H}$. Then $\mathfrak{A}$ is a C^*-algebra.

Proof. We check the axioms 1-5. That $(\mathfrak{A}, \| - \|)$ is complete is standard.

1. We have $\langle Lx, y\rangle = \langle x, L^*y\rangle$ and $\langle L^*x, y\rangle = \langle x, L^{**}y\rangle$. Then

$$\langle Lx, y\rangle = \langle x, L^*y\rangle = \langle L^{**}x, y\rangle$$

Hence $Lx = L^{**}x$ for all x and $L^{**} = L$, as required.

2. We have

$$\langle LMx, y\rangle = \langle Mx, L^*y\rangle = \langle x, M^*L^*y\rangle.$$

3. We use here that $\sup_{x\in\mathcal{H};\|x\|_0=1} \|Lx\|_0 = \sup_{x\in\mathcal{H};x\neq 0} \frac{\|Lx\|_0}{\|x\|_0}$. Then

$$\begin{aligned}\|LM\| &= \sup_{x\in\mathcal{H};x\neq0} \frac{\|LMx\|_0}{\|x\|_0} \\ &= \sup_{x\in\mathcal{H};Mx\neq0} \frac{\|LMx\|_0}{\|x\|_0} \\ &= \sup_{x\in\mathcal{H};Mx\neq0} \frac{\|LMx\|_0}{\|Mx\|_0} \cdot \frac{\|Mx\|_0}{\|x\|_0} \\ &\leq \sup_{y\in\mathcal{H};y\neq0} \frac{\|Ly\|_0}{\|y\|_0} \cdot \sup_{x\in\mathcal{H};x\neq0} \frac{\|Mx\|_0}{\|x\|_0} \\ &= \|L\|\|M\|\end{aligned}$$

4. We prove $\|L^*\| \leq \|L\|$ and note that the other inequality is found by substituting L^* for L and using that $L^{**} = L$.

$$\begin{aligned}\|L^*x\|_0^2 &= \langle L^*x, L^*x\rangle \\ &= \langle LL^*x, x\rangle \\ &\leq \|LL^*x\|_0 \cdot \|x\|_0 \\ &\leq \|L\| \cdot \|L^*x\|_0 \cdot \|x\|_0\end{aligned}$$

Hence $\|L^*x\|_0 \leq \|L\|\|x\|_0$ so L^* is bounded by $\|L^*\| \leq \|L\|$. (We have used the Cauchy-Schwarz inequality as the first inequality.)

5. Note that we have

$$\|L^*L\| \leq \|L^*\| \cdot \|L\| = \|L\|^2.$$

For the converse:

$$\|Lx\|_0^2 = \langle Lx, Lx\rangle$$

$$\begin{aligned}&= \langle L^*Lx, x\rangle \\ &\leq \|L^*Lx\|_0 \cdot \|x\|_0 \\ &\leq \|L^*L\| \cdot \|x\|_0^2\end{aligned}$$

Hence $\|L\|^2 \leq \|L^*L\|$. (Again, we have used the Cauchy-Schwarz inequality.)

△

Definition 1.1.12. *An operator L is called* idempotent *if $L^2 = L$, a* projection *if it is idempotent and $L^* = L$, furthermore an operator L is called* unitary *if $L^*L = I$ and $LL^* = I$.*

Theorem 1.1.13. *In the C^*-algebra $\mathfrak{A}$ from Example 1.1.11, every operator of the form $1 + AA^*$ for some $A \in \mathfrak{A}$ is invertible.*

This theorem is valid in any C^*-algebra, but we only need it for this specific case. To prove this theorem, we first need the following theorem:

Theorem 1.1.14. *Let $\mathcal{H}$ be a Hilbert space and let $A \in B(\mathcal{H})$ be arbitrary. Then $I + A^*A$ is invertible in $B(\mathcal{H})$.*

Proof. Write $C = I + A^*A$. Then for every $x \in \mathcal{H}$ we have

$$\begin{aligned}\|Cx\|_0 \cdot \|x\|_0 &\geq |\langle Cx, x\rangle| \\ &= |\langle x + A^*Ax, x\rangle| \\ &= |\langle x, x\rangle| + |\langle A^*Ax, x\rangle| \\ &= |\langle x, x\rangle| + \langle Ax, Ax\rangle| \\ &= \|x\|_0^2 + \|Ax\|_0^2\end{aligned}$$

Hence $Cx = 0$ implies $x = 0$, so C is injective. Furthermore

$$\|Cx\|_0 \geq \|x\|_0. \tag{1.1}$$

We now show that $\operatorname{Im} C$ is dense in $\mathcal{H}$ and that $\operatorname{Im} C$ is closed.

Let $x \in \mathcal{H}$ be arbitrary such that $x \perp \operatorname{Im} C$. Then $x \perp Cx$, i.e., $\langle x, Cx\rangle = 0$. Hence $\|x\|^2 + \|Ax\|^2 = 0$ and therefore $x = 0$. So, indeed, $\operatorname{Im} C$ lies dense in $\mathcal{H}$.

To show that $\operatorname{Im} C$ is closed, let $(x_n)_{n\in\mathbf{N}}$ be a sequence in $\operatorname{Im} C$ that converges in $\mathcal{H}$ to some $x \in \mathcal{H}$. We need to show that $x \in \operatorname{Im} C$.

Therefore choose $y_n \in \mathcal{H}$ with $x_n = Cy_n$. Then $\|y_n - y_m\|_0 \leq \|x_n - x_m\|_0$, so $(y_n)_{n\in\mathbf{N}}$ is a Cauchy sequence. Hence (y_n) converges to some y in $\mathcal{H}$. But then (Cy_n) converges to Cy, hence (x_n) converges to Cy. Since limits are unique, we find $x = Cy$.

Hence $\operatorname{Im} C$ is complete, hence closed.

Therefore C is surjective. By (1.1) we find that C^{-1} is continuous. □

We now only need to prove that $(I + A^*A)^{-1} \in \mathfrak{A}$. This follows from two lemmas, which use the same notations as above in Theorems 1.1.13 and 1.1.14

Lemma 1.1.15. *The operator $C + iI$ has an inverse in $\mathfrak{A}$.*

Proof. Let $s \in (0, \infty)$ be such that $s > \|C\|^2$. Then

$$\begin{aligned} C - iI &= (C + siI) - (s+1)iI \\ &= -(s+1)i(I - ((s+1)i)^{-1}(C + siI)) \\ &= -(s+1)i(I - T) \end{aligned}$$

with $T = \frac{1}{(s+1)i}(C + siI)$.

Now, if $\|T\| < 1$, then $I + T + T^2 + \ldots$ is the inverse of $I - T$. Note that $\|T\| = \frac{1}{s+1}\|C + siI\| < 1$ if $\|C + siI\| < s + 1$.

Claim. *We have* $\|C + siI\| \leq \sqrt{\|C\|^2 + s^2}$.

Proof. We have

$$\begin{aligned} \|(C + siI)x\|^2 = \langle (C + siI)x, (C + siI)x\rangle \\ &= \langle Cx + six, Cx + six\rangle \\ &\leq \|Cx\|^2 + 2\operatorname{Re}\langle Cx, six\rangle + \|sx\|^2 \\ &= (\|C\|^2 + s^2)\|x\|^2 \end{aligned}$$

Where we have seen that $2\operatorname{Re}\langle Cx, six\rangle = 2\operatorname{Re} i\langle Cx, sx\rangle = 0$ since $\langle Cx, sx\rangle \in \mathbb{R}$. △

By the claim, we find that $\|C + siI\|^2 \leq \|C\|^2 + s^2 < s^2 + 2s + 1 = (s+1)^2$ since $\|C\|^2 < s$. △

We have the following immediate corollary:

Corollary 1.1.16. *For every $t > 0$, the operator $C + tiI$ has an inverse in $\mathfrak{A}$.*

Lemma 1.1.17. *We have*

$$\lim_{\varepsilon \downarrow 0}(C + \varepsilon iI)^{-1} = C^{-1}.$$

Proof. Consider for every $\varepsilon > 0$ the operator $C^{-1} - (C + \varepsilon iI)^{-1}$. Then for small ε

$$\begin{aligned} C(C^{-1} - (C + \varepsilon iI)^{-1}) &= I - (C^{-1}(C + \varepsilon iI))^{-1} \\ &= I - (I + \varepsilon iC^{-1})^{-1} \\ &= \sum_{n=1}^{\infty}(-1)^{n-1}(\varepsilon iC^{-1})^n \\ &= \varepsilon iC^{-1}\sum_{m=0}^{\infty}(-1)^m(\varepsilon iC^{-1})^m \end{aligned}$$

Then

$$\|C(C^{-1} - (C + \varepsilon iI)^{-1})\| \leq \varepsilon\|C^{-1}\|\sum_{m=0}^{\infty}(\varepsilon\|C^{-1}\|)^n$$

If we take $\varepsilon < \frac{1}{\|C^{-1}\|}$, then the right-hand-side is $\leq 2\varepsilon\|C^{-1}\|$.

Therefore,

$$\lim_{\varepsilon \downarrow 0}\|C(C^{-1} - (C + \varepsilon iI)^{-1})\| = 0,$$

and hence:

$$\lim_{\varepsilon\downarrow 0} C(C^{-1} - (C + \varepsilon i I)^{-1}) = 0.$$

Lastly then,

$$\lim_{\varepsilon\downarrow 0} C^{-1} - (C + \varepsilon i I)^{-1} = C^{-1}0 = 0.$$

△

Proof. (of Theorem 1.1.13) The theorem follows directly from Theorem 1.1.14, Corollary 1.1.16 and Lemma 1.1.17 □

The above theorems and their proofs were communicated to the author by A. van Rooij.

Lemma 1.1.18. *For a projection P we have $P = PP^*$ and $1 - P$ is a projection.*

Proof. Note that $P = P^* = P^2$ by definition. So $P = P^2 = P \cdot P = P \cdot P^*$. Furthermore, we have $(1-P)^* = 1 - P^* = 1 - P$ and $(1-P)^2 = 1 - 2P + P^2 = 1 - 2P + P = 1 - P$, so indeed $1 - P$ is a projection. △

The following theorem will be used in the proof of our main result. It is found in [10]. Note that the results 1.1.19 - 1.1.22 are stated there in terms of rings of operators, but they go verbatim for arbitrary (non-commutative) rings if we use the following definitions:

> An *involution* is a ring anti-homomorphism which is its own inverse, i.e., $f(xy) = f(y)f(x)$, $f(x+y) = f(x) + f(y)$ and $f(f(x)) = x$.
>
> A *projection* is an element in the ring for which we have $e^* = e$ and $e^2 = e$, given a certain involution $*$.

Theorem 1.1.19. *Let A be a ring with involution $*$ and suppose that for every $x \in A$, $1 + xx^*$ is invertible in A. Then for any idempotent f in A, there exists a projection e such that $fA = eA$.*

Proof. Write $z = 1 + (f - f^*)(f^* - f)$ such that z is invertible by assumption. Furthermore $z = 1 + ff^* - ff - f^*f^* + f^*f$ and $z^* = z$. By the very easy lemma below (Lemma 1.1.23), we find that $z = 1 + ff^* - f - f^* + f^*f$.

> **Claim.** $z^{-1} = (z^{-1})^*$
>
> *Proof.* We have $zz^{-1} = 1 = 1^* = (z^{-1}z)^* = z^*(z^{-1})^* = z(z^{-1})^*$ △

Now we have

$$\begin{aligned} fz &= f + fff^* - ff - ff^* + ff^*f \\ &= f - f + ff^* - ff^* + ff^*f = ff^*f \\ zf &= f + ff^*f - ff - f^*f + f^*ff \\ &= f - f + f^*f - f^*f + ff^*f = ff^*f \end{aligned}$$

Then z^{-1} commutes with f and f^* :

> **Claim.** - $z^{-1}f = fz^{-1}$

- $z^{-1}f^* = f^*z^{-1}$

Proof.

- $z^{-1}fz = z^{-1}ff^*f = z^{-1}zf = f$
- $z^{-1}f^*z = z^{-1}f^*z^* = z^{-1}(zf)^* = z^{-1}(fz)^* = z^{-1}z^*f^* = z^{-1}zf^* = f^*$

In both above equations multiply from the right with z^{-1}. △

Now we define $e = ff^*z^{-1}$.

Claim. *e is a projection.*

Proof.

- $e^* = (ff^*z^{-1})^* = (z^{-1})^*ff^* = z^{-1}ff^* = fz^{-1}f^* = ff^*z^{-1} = e$
- $e^2 = ff^*z^{-1}ff^*z^{-1} = z^{-1}ff^*ff^*z^{-1} = z^{-1}zff^*z^{-1} = ff^*z^{-1} = e$

Indeed e is a projection. Note that we have used $zf = ff^*f$ in the third equality from $e^2 = e$. △

Since $fe = fff^*z^{-1} = ff^*z^{-1} = e$, we have $eA \subset fA$. Also, since $ef = ff^*z^{-1}f = ff^*fz^{-1} = fzz^{-1}f = f$, we have $fA \subset eA$. Hence $fA = eA$ as required. □

Lemma 1.1.20. *Let e, f be idempotents in a ring A. If $fA = eA$, then $e - f$ is nilpotent.*

Proof. Using that $fA = eA$, determine $a, b \in A$ such that $e = fa$ and $f = eb$. Then $fe = f(fa) = fa = e$ and $ef = e(eb) = eb = f$. Now

$$(e-f)^2 = e^2 - ef - fe + f^2 = e - f - e + f = 0.$$

△

Proposition 1.1.21. *Let e, f be idempotents in a ring A. If $fA = eA$, then there exists some invertible $x \in A$ for which $f = xex^{-1}$.*

Proof. Define $x = 1 + (e - f)$. As above $fe = e$ and $ef = f$. Then

$$xe = e + (e-f)e = e + e^2 - fe = e + e - e = e$$

and

$$fx = f + f(e-f) = f + fe - f^2 = f + e - f = e$$

Hence $xe = fx$. Now, since $(e-f)^2 = 0$, we find

$$\begin{aligned} x(1-(e-f)) &= (1+(e-f))(1-(e-f)) \\ &= 1 - (e-f) + (e-f) - (e-f)^2 \\ &= 1 - (e-f)^2 \\ &= 1 \end{aligned}$$

and

$$\begin{aligned}(1-(e-f))x &= (1-(e-f))(1+(e-f)) \\ &= 1+(e-f)-(e-f)-(e-f)^2 \\ &= 1\end{aligned}$$

Hence x is invertible and we have $xex^{-1} = f$. □

If there exists an invertible $x \in A$ such that $f = xex^{-1}$, we call e and f *similar.*

Corollary 1.1.22. *Let A be a ring with involution $*$ and suppose that $\{1 + xx^* \mid x \in A\} \subset A^*$. Then every idempotent $f \in A$ is similar to a projection.*

Proof. This is a direct corollary of Theorem 1.1.19 and Proposition 1.1.21. △

Lemma 1.1.23. *Let A, B be rings and $f\colon A \to B$ be a ring (anti-)homomorphism. Let e be an idempotent in A, then $f(e)$ is an idempotent in B.*

Proof. We have $f(e) = f(e^2) = f(e)f(e) = f(e)^2$. △

1.1.3 Proof of the Main Theorem

We start with proving our main result for $n = 1$:

Theorem 1.1.24. *Let G be a group and x, y elements of $\mathbf{C}[G]$ such that $xy = 1$. Then $yx = 1$.*

Proof. On $\mathbf{C}[G]$ we have two maps:

$$*\colon \mathbf{C}[G] \to \mathbf{C}[G],\ \sum_{g\in G} \alpha_g g \mapsto \sum_{g \in G} \overline{\alpha_g} g^{-1}$$

and

$$\operatorname{tr}\colon \mathbf{C}[G] \to \mathbf{C},\ \sum_{g\in G} \alpha_g g \mapsto \alpha_1.$$

The first is an involution, we write $x^* := *(x)$. Then

Claim. *This* tr *is a* $\mathbf{C}$*-linear map with*

i) $\operatorname{tr}(1) = 1$;

ii) $\operatorname{tr}(xy) = \operatorname{tr}(yx)$ *for all* $x, y \in \mathbf{C}[G]$;

iii) $\operatorname{tr}(xx^*) \geq 0$ *for all* $x \in \mathbf{C}[G]$ *and* $\operatorname{tr}(xx^*) = 0 \implies x = 0$.

Proof.

) Let $x, y \in \mathbf{C}[G]$ and $\lambda \in \mathbf{C}$ be arbitrary. Write $x = \sum_{g\in G} \alpha_g g$ and $y = \sum_{g \in G} \beta_g g$. Then we have

$$\operatorname{tr}(x+y) = \operatorname{tr}\left(\sum_{g\in G}(\alpha_g + \beta_g) g\right) = \alpha_1 + \beta_1 = \operatorname{tr}(x) + \operatorname{tr}(y)$$

and

$$\operatorname{tr}(\lambda x) = \operatorname{tr}\left(\sum_{g\in G}(\lambda\alpha_g) g\right) = \lambda\alpha_1 = \lambda \operatorname{tr}(x).$$

Thus tr is indeed a $\mathbf{C}$-linear map.

i) Since $1 \in \mathbf{C}[G]$ is just $1 \cdot 1$ where the first $1 \in \mathbf{C}$ and the second $1 \in G$ we find that $\operatorname{tr}(1) = 1$.

ii) Let $x, y \in \mathbf{C}[G]$ be arbitrary. Write $x = \sum_{g\in G} \alpha_g g$ and $y = \sum_{g\in G} \beta_g g$. Then

$$\operatorname{tr}(xy) = \operatorname{tr}\left(\sum_{g\in G, h \in G} (\alpha_g \beta_h) gh\right) = \sum_{g\in G} \alpha_g \beta_{g^{-1}}$$

and

$$\operatorname{tr}(yx) = \operatorname{tr}\left(\sum_{h\in G, g \in G} (\beta_h \alpha_g) hg\right) = \sum_{h\in G} \beta_h \alpha_{h^{-1}}$$

which agree.

iii) We have

$$\operatorname{tr}(xx^*) = \operatorname{tr}\left(\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{g\in G}\overline{\alpha_g} g^{-1}\right)\right) = \sum_{g\in G} |\alpha_g|^2.$$

Therefore $\operatorname{tr}(xx^*) = \sum_{g\in G} |\alpha_g|^2 \geq 0$, since $|\alpha_g| \geq 0$. Lastly, if $\operatorname{tr}(xx^*) = 0$, then $|\alpha_g| = 0$ for all $g \in G$, hence $\alpha_g = 0$ for all $g \in G$. Thus $x = 0$.

△

We can bestow upon $\mathbf{C}[G]$ an inner product given by $\langle \sum_{g\in G} \alpha_g g, \sum_{g \in G} \beta_g g\rangle = \sum_{g\in G} \alpha_g \overline{\beta_g}$.

Claim. *This indeed defines an inner product on* $\mathbf{C}[G]$.

Proof. Let $\lambda \in \mathbf{C}$ and $x, y, z \in \mathbf{C}[G]$ be arbitrary. Write $x = \sum_{g\in G}\alpha_g g$, $y = \sum_{g\in G} \beta_g g$ and $z = \sum_{g\in G} \gamma_g g$. Then we have

$$\begin{aligned}
\langle \lambda x, y\rangle &= \langle \lambda \sum \alpha_g g, \sum \beta_g g\rangle \\
&= \langle \sum \lambda\alpha_g g, \sum \beta_g g\rangle \\
&= \sum \lambda \alpha_g \overline{\beta_g} \\
&= \lambda \sum \alpha_g \overline{\beta_g} \\
&= \lambda \langle \sum \alpha_g g, \sum \beta_g g\rangle \\
&= \lambda\langle x, y\rangle
\end{aligned}$$

and

$$\begin{aligned}\langle x+y,z\rangle &= \langle \sum \alpha_g g + \sum \beta_g g, \sum \gamma_g g\rangle \\ &= \langle \sum (\alpha_g+\beta_g)g, \sum \gamma_g g\rangle \\ &= \sum (\alpha_g+\beta_g)\overline{\gamma_g} \\ &= \sum \alpha_g \overline{\gamma_g} + \sum \beta_g \overline{\gamma_g} \\ &= \langle \sum \alpha_g g, \sum \gamma_g g\rangle + \langle \sum \beta_g g, \sum \gamma_g g\rangle \\ &= \langle x,z\rangle + \langle y,z\rangle\end{aligned}$$

Hence $\langle -,-\rangle$ is linear in its first component. Furthermore

$$\begin{aligned}\overline{\langle y,x\rangle} &= \overline{\langle \sum \beta_g g, \sum \alpha_g g\rangle} \\ &= \overline{\sum \beta_g \overline{\alpha_g}} \\ &= \sum \overline{\beta_g}\alpha_g \\ &= \langle \sum \alpha_g g, \sum \beta_g g\rangle \\ &= \langle x,y\rangle\end{aligned}$$

and

$$\langle x,x\rangle = \sum \alpha_g \overline{\alpha_g} = \sum |\alpha_g|^2$$

hence $\langle x,x\rangle \geq 0$ and $\langle x,x\rangle = 0 \iff x = 0$. So indeed this defines an inner product on $\mathbf{C}[G]$. $\triangle$

We write $\| \sum_{g\in G} \alpha_g g\|_0 = \left(\sum_{g\in G} |\alpha_g|^2\right)^{\frac{1}{2}}$ for the norm induced by this inner product and we complete $\mathbf{C}[G]$ to a Hilbert space $\mathcal{H}$ with respect to this norm. In particular note that $\|x\|_0 = \mathrm{tr}(xx^*)^{\frac{1}{2}}$. Now for any $x \in \mathbf{C}[G]$, left multiplication by x is an element of $B(\mathcal{H})$, the bounded linear operators on $\mathcal{H}$.

Claim. *For all $x \in \mathbf{C}[G]$, left multiplication by x is a bounded linear operator on $\mathcal{H}$.*

Proof. Write L_x for the map defined by left multiplication by x.

- Let $\lambda, \mu \in \mathbf{C}$ and $v, w \in \mathbf{C}[G]$. We will show $L_x(\lambda v + \mu w) = \lambda L_x(v) + \mu L_x(w)$ for linearity.

$$\begin{aligned}L_x(\lambda v + \mu w) &= x(\lambda v + \mu w) \\ &= x\lambda v + x\mu w \\ &= \lambda x v + \mu x w \\ &= \lambda L_x(v) + \mu L_x(w)\end{aligned}$$

  We have used the distributivity of multiplication over addition in $\mathbf{C}[G]$.

- Note that

$$\|L_x(y)\|_0 = \|xy\|_0 = \|\sum_{g\in G} \alpha_g g y\|_0 \leq \sum_{g\in G} |\alpha_g| \|gy\|_0 = \left(\sum_{g\in G} |\alpha_g|\right) \|y\|_0$$

  where we have used the claim below, that $\|gx\|_0 = \|x\|_0$ for all $g \in G$.

Claim. *For all $g \in G$ we have $\|gx\|_0 = \|x\|_0$.*

Proof. Note that $h \mapsto gh$ is a permutation of G. Hence

$$\|gx\|_0 = \|\sum_{h \in G} \beta_h gh\|_0 = \sqrt{\sum_{h \in G} |\beta_h|^2} = \|x\|_0.$$

$\triangle$

Now we have seen that $L_x \colon \mathbf{C}[G] \to \mathbf{C}[G]$ is a bounded linear operator, which we can extend to $\mathcal{H}$ since $\mathbf{C}[G]$ is dense in $\mathcal{H}$. $\triangle$

If we write $\| - \|$ for the operator norm on $B(\mathcal{H})$, then $\|L_x\| = \sup\{\|L_x(v)\|_0 \mid v \in \mathcal{H}, \|v\|_0 = 1\} \geq \|L_x(1)\|_0 = \|x\|_0$ and $L_x^* = L_{x*}$. Therefore L_g is a unitary operator.

Claim. *For all $x \in \mathbf{C}[G]$ we have $L_x^* = L_{x^*}$, while L_g is a unitary operator for all $g \in G$.*

Proof.

- In order to prove $L_x^* = L_{x^*}$ we need to show that for every $y, z \in \mathcal{H}$ we have $\langle L_x(y), z\rangle = \langle y, L_{x^*}(z)\rangle$. Since inner products are continuous in either argument and $\mathbf{C}[G]$ is dense in $\mathcal{H}$, we may assume $y, z \in \mathbf{C}[G]$. Since $y, z \in \mathbf{C}[G]$ are linear combinations of $g \in G$, we can suffice by showing $\langle L_x(h), h'\rangle = \langle h, L_{x^*}(h')\rangle$ for all $h, h' \in G$. Write $x = \sum_{g \in G} \alpha_g g$. Then

$$\begin{aligned}\langle L_x(h), h'\rangle &= \langle \sum_g \alpha_g gh, h'\rangle \\ &= \sum_g \alpha_g \\ &= \langle h, \sum_g \overline{\alpha_g} g^{-1} h'\rangle \\ &= \langle h, L_{x^*}(h')\rangle\end{aligned}$$

- We have

$$L_g L_g^* = L_g L_{g^*} = L_g L_{g^{-1}} = L_{gg^{-1}} = L_1 = I$$

  and

$$L_g^* L_g = L_{g^*} L_g = L_{g^{-1}} L_g = L_{g^{-1}g} = L_1 = I$$

  So L_g is unitary.

$\triangle$

Now we write $\mathfrak{A}$ for the closure of $\{L_x\}_{x \in \mathbf{C}[G]}$ in $B(\mathcal{H})$ with respect to the operator norm. Then by Example 1.1.11 $\mathfrak{A}$ is a C^*-algebra and for all $A \in \mathfrak{A}$ we find that $1 + AA^*$ is invertible in $\mathfrak{A}$ by Theorem 1.1.13.

Then by Corollary 1.1.22, we find that every idempotent in $\mathfrak{A}$ is similar to a projection. We now wish to define our trace map on $\mathfrak{A}$. Write $\operatorname{tr}(L_x) = \operatorname{tr}(x)$. Note that tr is continuous on $\{L_x\}_{x \in \mathbf{C}[G]}$:

Proof. Note that we have $\|L_x\| \geq \|x\|_0$. Also,

$$\|x\|_0 = \sqrt{\sum_{g \in G} |\alpha_g|^2} \geq |\alpha_1| = |\operatorname{tr}(x)|,$$

hence $\|L_x\| \geq |\operatorname{tr}(x)|$.

Then $|\operatorname{tr}(x) - \operatorname{tr}(y)| = |\operatorname{tr}(x-y)| \leq \|L_{x-y}\| = \|L_x - L_y\|$, so we find that tr is continuous on $\{L_x\}_{x \in \mathbf{C}[G]}$. △

Now we can extend tr to the whole of $\mathfrak{A}$. Then this extended tr has the same properties as our original $\operatorname{tr}\colon \mathbf{C}[G] \to \mathbf{C}$:

Claim. tr *is a* $\mathbf{C}$*-linear map with*

i) $\operatorname{tr}(I) = 1$;

ii) $\operatorname{tr}(XY) = \operatorname{tr}(YX)$ *for all* $X, Y \in \mathfrak{A}$;

iii) $\operatorname{tr}(XX^*) \geq 0$ *for all* $X \in \mathfrak{A}$ *and* $\operatorname{tr}(XX^*) = 0 \implies X = 0$.

Proof. Let $X, Y \in \mathfrak{A}$ be arbitrary and $\lambda \in \mathbf{C}$. Choose $(x_n)_{n=0}^{\infty} \in \mathbf{C}[G]$ such that

$$\lim_{n \to \infty} \|L_{x_n} - X\| = 0,$$

and likewise some $(y_n)_{n=0}^{\infty} \in \mathbf{C}[G]$ such that

$$\lim_{n \to \infty} \|L_{y_n} - Y\| = 0.$$

) Note that

$$\begin{aligned}
\operatorname{tr}(\lambda X) &= \operatorname{tr}\left(\lambda \lim_{n \to \infty} L_{x_n}\right) \\
&= \operatorname{tr}\left(\lim_{n \to \infty} \lambda L_{x_n}\right) \\
&= \lim_{n \to \infty} \operatorname{tr}(\lambda L_{x_n}) \\
&= \lim_{n \to \infty} \operatorname{tr}(L_{\lambda x_n}) \\
&= \lim_{n \to \infty} \operatorname{tr}(\lambda x_n) \\
&= \lim_{n \to \infty} \lambda \operatorname{tr}(x_n) \\
&= \lambda \lim_{n \to \infty} \operatorname{tr}(x_n) \\
&= \lambda \lim_{n \to \infty} \operatorname{tr}(L_{x_n}) \\
&= \lambda \operatorname{tr}\left(\lim_{n \to \infty} L_{x_n}\right) \\
&= \lambda \operatorname{tr}(X)
\end{aligned}$$

Also

$$\operatorname{tr}(X + Y) = \operatorname{tr}\left(\lim_{n \to \infty} L_{x_n} + \lim_{n \to \infty} L_{y_n}\right)$$

$$\begin{aligned}
&= \operatorname{tr}\left(\lim_{n\to\infty} L_{x_n} + L_{y_n}\right) \\
&= \lim_{n\to\infty} \operatorname{tr}(L_{x_n} + L_{y_n}) \\
&= \lim_{n\to\infty} \operatorname{tr}(x_n + y_n) \\
&= \lim_{n\to\infty} \operatorname{tr}(x_n) + \operatorname{tr}(y_n) \\
&= \lim_{n\to\infty} \operatorname{tr}(L_{x_n}) + \operatorname{tr}(L_{y_n}) \\
&= \lim_{n\to\infty} \operatorname{tr}(L_{x_n}) + \lim_{n\to\infty} \operatorname{tr}(L_{y_n}) \\
&= \operatorname{tr}\left(\lim_{n\to\infty} L_{x_n}\right) + \operatorname{tr}\left(\lim_{n\to\infty} L_{y_n}\right) \\
&= \operatorname{tr}(X) + \operatorname{tr}(Y)
\end{aligned}$$

so tr is indeed a $\mathbf{C}$-linear map.

i) We have $\operatorname{tr}(I) = \operatorname{tr}(L_1) = \operatorname{tr}(1) = 1$.

ii) Note that

$$\begin{aligned}
\lim_{n\to\infty} \|L_{x_n y_n} - XY\| &= \lim_{n\to\infty} \|L_{x_n} L_{y_n} - XY\| \\
&= \lim_{n\to\infty} \|(L_{x_n} - X)L_{y_n} + X(L_{y_n} - Y)\| \\
&\leq \lim_{n\to\infty} \|(L_{x_n} - X)L_{y_n}\| + \|X(L_{y_n} - Y)\| \\
&\leq \lim_{n\to\infty} \|L_{x_n} - X\|\|L_{y_n}\| + \|X\|\|L_{y_n} - Y\| \\
&= \lim_{n\to\infty} \|L_{x_n} - X\|\|L_{y_n}\| + \lim_{n\to\infty} \|X\|\|L_{y_n} - Y\| \\
&= 0
\end{aligned}$$

since L_{y_n} converges to Y. Similarly

$$\lim_{n\to\infty} \|L_{y_n x_n} - YX\| = 0.$$

Then we have

$$\begin{aligned}
\operatorname{tr}(XY) &= \operatorname{tr}\left(\lim_{n\to\infty} L_{x_n y_n}\right) \\
&= \lim_{n\to\infty} \operatorname{tr}(L_{x_n y_n}) \\
&= \lim_{n\to\infty} \operatorname{tr}(x_n y_n) \\
&= \lim_{n\to\infty} \operatorname{tr}(y_n x_n) \\
&= \lim_{n\to\infty} \operatorname{tr}(L_{y_n x_n}) \\
&= \operatorname{tr}\left(\lim_{n\to\infty} L_{y_n x_n}\right) \\
&= \operatorname{tr}(YX)
\end{aligned}$$

iii) Note that

$$\lim_{n\to\infty} \|L_{x_n}^* - X^*\| = 0$$

hence

$$\lim_{n\to\infty} \|L_{x_n x_n^*} - XX^*\| = 0.$$

Then

$$\begin{aligned}\operatorname{tr}(XX^*) &= \operatorname{tr}\left(\lim_{n\to\infty} L_{x_n x_n^*}\right)\\ &= \lim_{n\to\infty} \operatorname{tr}(L_{x_n x_n^*})\\ &= \lim_{n\to\infty} \operatorname{tr}(x_n x_n^*) \geq 0\end{aligned}$$

Now suppose that $\operatorname{tr}(XX^*) = 0$, i.e., $\lim_{n\to\infty} \|x_n\|_0^2 = 0$. Then $\lim_{n\to\infty} \|x_n\|_0 = 0$.

If we show that $Xg = 0$ for all $g \in G$, then since any element of $\mathbf{C}[G]$ is a finite linear combination of $g \in G$, and $\mathbf{C}[G]$ is dense in $\mathcal{H}$, then $X = 0$.

Let $g \in G$ be arbitrary. We have

$$\begin{aligned}\|Xg\|_0 &= \|(\lim_{n\to\infty} L_{x_n})g\|_0\\ &= \|\lim_{n\to\infty} L_{x_n} g\|_0\\ &= \|\lim_{n\to\infty} x_n g\|_0\\ &= \lim_{n\to\infty} \|x_n g\|_0\\ &= \lim_{n\to\infty} \|x_n\|_0 \|g\|_0\\ &= \|g\|_0 \cdot \lim_{n\to\infty} \|x_n\|_0\\ &= 0\end{aligned}$$

Hence $Xg = 0$ for all $g \in G$.

△

Now, if e is an idempotent in $\mathbf{C}[G]$, then we have the following:

Claim. - $\operatorname{tr}(e) = 0 \implies e = 0$;

- $\operatorname{tr}(e) = 1 \implies e = 1$;

- $0 \leq \operatorname{tr}(e) \leq 1$.

Proof. Since e is an idempotent in $\mathbf{C}[G]$, we find that L_e is an idempotent in $\mathfrak{A}$. Therefore, $L_e = A^{-1}PA$ with P a projection. Then $\operatorname{tr}(P) = \operatorname{tr}(L_e) = \operatorname{tr}(e)$. Since P is a projection, we have $P = PP^*$ (see Lemma 1.1.18).

- Now if $\operatorname{tr}(e) = \operatorname{tr}(P) = 0$, then $\operatorname{tr}(PP^*) = 0$ and hence (by iii) of the previous claim) $P = 0$, i.e. $L_e = 0$ and $e = 0$.

- If $\operatorname{tr}(e) = 1$, then $\operatorname{tr}(1 - e) = 0$, hence $\operatorname{tr}(1 - P) = 0$. Then

$$\operatorname{tr}((1-P)(1-P^*)) = \operatorname{tr}(1 - P - P^* + PP^*) = \operatorname{tr}(1-P) = 0$$

Now by part iii) of the previous claim, $1 - P = 0$, hence $1 - L_e = 0$ and $e = 1$.

- If $\mathrm{tr}(P) \neq 0$, then $\mathrm{tr}(PP^*) \neq 0$, hence $\mathrm{tr}(P) > 0$. If $P \neq 1$, then since $1 - P$ is also a projection (see Lemma 1.1.18), we have $\mathrm{tr}((1-P)(1-P^*)) \neq 0$, hence $1-\mathrm{tr}(P) = \mathrm{tr}(1-P) = \mathrm{tr}((1-P)(1-P^*)) > 0$. Therefore $0 < \mathrm{tr}(P) < 1$. Together with $P = 0$ and $P = 1$, we find $0 \leq \mathrm{tr}(P) \leq 1$.

△

Now suppose that $x, y \in \mathbf{C}[G]$ are such that $xy = 1$. Then since yx is an idempotent, we find that $\mathrm{tr}(yx) = \mathrm{tr}(xy) = 1$, hence $yx = 1$, by the previous claim. This completes the proof. □

Then the essential theorem of this section will be a direct corollary of the following theorem:

Theorem 1.1.25. *Let G be a group and x, y elements of $\mathrm{Mat}_n(\mathbf{C})[G]$ such that $xy = 1$, then $yx = 1$.*

Proof. This proof is similar to the proof for $n = 1$, where the maps on $\mathrm{Mat}_n(\mathbf{C})[G]$ are:

$$*\colon\ \mathrm{Mat}_n(\mathbf{C})[G] \to \mathrm{Mat}_n(\mathbf{C})[G],\ \sum_{g\in G} A_g g \mapsto \sum_{g\in G} \overline{A_g^t} g^{-1}$$

and

$$\mathrm{tr}\colon\ \mathrm{Mat}_n(\mathbf{C})[G] \to \mathbf{C},\ \sum_{g\in G} A_g g \mapsto \mathrm{Tr}(A_1).$$

□

Corollary 1.1.26. *Let G be a group and X, Y elements of $\mathrm{Mat}_n(\mathbf{C}[G])$ such that $XY = I_n$, then $YX = I_n$.*

Proof. This is a direct corollary of Theorem 1.1.25 and Proposition 1.1.5. △

1.2 Fox-calculus

Fox-calculus is essentially just calculus on free group rings. We start by defining what a derivation on a group ring is and apply this to free group rings. We will ultimately arrive at the chain rule for Fox-calculus, which is needed in the proof of the Inverse Function Theorem for Free Groups.

1.2.1 Derivations on group rings

Let G, H be groups and $\phi\colon G \to H$ be a group homomorphism. Then this ϕ extends to a ring homomorphism $\phi\colon R[G] \to R[H]$ by

$$\sum_g \alpha_g g \mapsto \sum_g \alpha_g \phi(g).$$

For example, let $\varepsilon\colon G \to 1$ be the trivial group homomorphism. Then $\varepsilon\colon R[G] \to R$

$$\sum_g \alpha_g g \mapsto \sum_g \alpha_g \varepsilon(g) = \sum_g \alpha_g.$$

Definition 1.2.1. *We define a* derivation *D on $R[G]$ as an R-linear map $D\colon R[G] \to R[G]$ that satisfies:*

$$D(uv) = D(u)\varepsilon(v) + uD(v) \quad \textit{for all } u, v \in R[G]. \tag{1.2}$$

Remark. *The last equation simplifies for group elements as*

$$D(gh) = D(g) + gD(h) \quad \textit{for all } g, h \in G. \tag{1.3}$$

Since $D(0) = D(0+0) = D(0) + D(0)$ *we have* $D(0) = 0$ *and* $D(1) = D(1 \cdot 1) = D(1) \cdot 1 + 1 \cdot D(1) = D(1) + D(1)$*, hence* $D(1) = 0$*. By* R*-linearity we then have* $D(r) = rD(1) = 0$ *for all* $r \in R$*.*

We list some properties:

Lemma 1.2.2. *Let* R *be a ring and* G *a group. We have*

$$D\left(\sum_g \alpha_g g\right) = \sum_g \alpha_g D(g). \tag{1.4}$$

$$D(u_1 u_2 \cdots u_n) = \sum_{i=1}^{n} u_1 \cdots u_{i-1} \cdot Du_i \cdot \varepsilon(u_{i+1}) \cdots \varepsilon(u_n) \tag{1.5}$$

$$D(g^{-1}) = -g^{-1}D(g) \tag{1.6}$$

Proof. (1.4) is just another way of stating the R-linearity of D.
(1.5) follows inductively from (1.2). For $n = 1$, we have nothing to prove. For $n = 2$ it is precisely (1.2). Assume it holds for $n - 1$. Then

$$\begin{aligned} D(u_1 u_2 \cdots u_n) &= D((u_1 \cdots u_{n-1})u_n) \\ &= D(u_1 \cdots u_{n-1})\varepsilon(u_n) + u_1 \cdots u_{n-1} D(u_n) \\ &= D(u_1 \cdots u_{n-1}) + u_1 \cdots u_{n-1} D(u_n) \\ &= u_1 \cdots u_{n-1} D(u_n) + \sum_{i=1}^{n-1} u_1 \cdots u_{i-1} D(u_i)\varepsilon(u_{i+1}) \cdots \varepsilon(u_{n-1}) \\ &= \sum_{i=1}^{n} u_1 \cdots u_{i-1} D(u_i)\varepsilon(u_{i+1}) \cdots \varepsilon(u_n) \end{aligned}$$

(1.6) then follows from $0 = D(1) = D(gg^{-1}) = D(g)\varepsilon(g^{-1}) + gD(g^{-1}) = D(g) + gD(g^{-1})$. △

Proposition 1.2.3. *Let* $\mathrm{Der}_R(G)$ *be the set of derivations on* $R[G]$*. Then* $\mathrm{Der}_R(G)$ *is a right* $R[G]$*-module, with operations defined as:*

$$(D_1 + D_2)(v) = D_1(v) + D_2(v);$$
$$(Dv)(u) = D(u)v.$$

Proof. We have

$$\begin{aligned} (D_1 + D_2)(u + v) &= D_1(u + v) + D_2(u + v) \\ &= D_1(u) + D_1(v) + D_2(u) + D_2(v) \\ &= (D_1 + D_2)(u) + (D_1 + D_2)(v) \end{aligned}$$

and

$$(D_1 + D_2)(uv) = D_1(uv) + D_2(uv)$$

$$\begin{aligned} &= D_1(u)\varepsilon(v) + uD_1(v) + D_2(u)\varepsilon(v) + uD_2(v) \\ &= D_1(u)\varepsilon(v) + D_2(u)\varepsilon(v) + uD_1(v) + uD_2(v) \\ &= (D_1(u) + D_2(u))\varepsilon(v) + u(D_1(v) + D_2(v)) \\ &= (D_1 + D_2)(u)\varepsilon(v) + u(D_1 + D_2)(v) \end{aligned}$$

Hence $D_1 + D_2$ is a derivation.
Since

$$\begin{aligned} (Dv)(u_1 + u_2) &= D(u_1 + u_2)v \\ &= D(u_1)v + D(u_2)v \\ &= (Dv)(u_1) + (Dv)(u_2) \end{aligned}$$

and

$$\begin{aligned} (Dv)(u_1u_2) &= D(u_1u_2)v \\ &= D(u_1)\varepsilon(u_2)v + u_1D(u_2)v \\ &= (Dv)(u_1)\varepsilon(u_2) + u_1(Dv)(u_2) \end{aligned}$$

we find that Dv is a derivation.
Then $\mathrm{Der}_R(G)$ is a right $R[G]$-module, with operations defined as above. □

Remark. *We cannot bestow upon* $\mathrm{Der}_R(G)$ *the structure of a left* $R[G]$*-module by setting* $(vD)(u) = vD(u)$*, for we have*

$$\begin{aligned} (vD)(u_1u_2) &= vD(u_1u_2) \\ &= v(D(u_1)\varepsilon(u_2) + u_1D(u_2)) \\ &= vD(u_1)\varepsilon(u_2) + vu_1D(u_2) \\ &= (vD)(u_1)\varepsilon(u_2) + vu_1D(u_2) \end{aligned}$$

Since v *does not necessarily commute with* u_1*, we see that* vD *is not necessarily a derivation.*

1.2.2 Derivations on free group rings

We begin with an example of a free group, that should explain the terminology and the properties of the free group.

Example 1.2.4. *Let* $A = \{a, b\}$*, then* A^* *is the set of all finite sequences consisting of* a*'s and* b*'s, e.g.,*

$$1 \quad a \quad b \quad ba \quad aa \quad abb \quad babb \quad abababbabab \quad abababaaa$$

Here we write 1 *for the empty sequence, this is clearly finite and only contains* a*'s and* b*'s (even though it doesn't contain any of those).*
We can add a binary operation of concatenation to this set A^**. We write that here (in this example only) as* $\diamondsuit$*, e.g.,*

$$a\diamondsuit b = ab \quad a\diamondsuit 1 = a \quad a\diamondsuit a = aa$$

If we add the relations $ab-1$ and $ba-1$, i.e., construct

$$A^*/ < ab-1, ba-1 >$$

while still using $\diamondsuit$ as multiplication, we find e.g.,

$$ababba\diamondsuit baabaaa = 1\diamondsuit aaa = aaa \qquad aaaabb\diamondsuit aab = aaaabbaab = aaa$$

One may easily verify that this structure $A^*/ < ab-1, ba-1 >$ yields a group with multiplication $\diamondsuit$ and unit 1. We call this group the free group on one variable *or* free group on one generator*. The elements of a free group are called* words*.*

Let X be a free group with a set $(x_i)_{i\in I}$ of generators. Every $u \in X$ is an equivalence class of elements in X, represented by a unique *reduced* word

$$x_{j_1}^{e_1}x_{j_2}^{e_2}\cdots x_{j_r}^{e_r}, \text{ where } e_i = \pm 1 \text{ and } e_i + e_{i+1} \neq 0 \text{ when } j_i = j_{i+1}$$

The length of u is the number r.
The inverse of a (reduced) word is represented by

$$x_{j_r}^{-e_r}\cdots x_{j_2}^{-e_2}x_{j_1}^{-e_1}$$

and the unit element 1 is represented by the empty word of length 0.
The following example is to clarify these notations on the free group with two elements.

Example 1.2.5. *Now, let $A = \{a, b, x, y\}$ and consider*

$$A^*/ < ab-1, ba-1, xy-1, yx-1 >$$

i.e. the free group on two generators. The following words aren't reduced

$$axbay \qquad abxaayabx \qquad aaaaab$$

Their reduced forms are respectively

$$a \qquad xaa \qquad aaaa$$

For the following word, we list its inverse word

$$aaxxaybxb \to ayaxbyybb.$$

If we want, we can write a^{-1} for b and x^{-1} for y to obtain

$$aaxxax^{-1}a^{-1}xa^{-1} \to ax^{-1}axa^{-1}x^{-1}x^{-1}a^{-1}a^{-1}.$$

If $w = x_1x_2^{-1}x_3x_1^{-1}$ is a word in the free group X with generators $(x_i)_{i\in\mathbf{N}}$, then we can speak of *initial segments* of w. Here, the initial segments are

$$1, \quad x_1, \quad x_1x_2^{-1}, \quad x_1x_2^{-1}x_3, \quad w.$$

A word w of length 1 has only two initial segments: $1, w$. A word of length r has exactly $r+1$ initial segments.

Let R be a ring, then elements of $R[X]$ can be considered as $\sum_{u\in X} a_u u$, with at most finitely many $a_u \in R$ nonzero. With $\overline{x}$ as the double sequence $((x_i)_{i\in I}, (x_i^{-1})_{i\in I})$, we write $f(\overline{x})$ for such an expression to indicate that we can consider $f(\overline{x}) := \sum_{u\in X} a_u u$ as a "polynomial" in the variables $(x_i)_{i\in I}$ and $(x_i^{-1})_{i\in I}$.
As before, the homomorphism $\varepsilon\colon R[X] \to R$ gives $f(\bar{x}) \mapsto f(1)$, i.e.

$$\sum_{u\in X} a_u u \mapsto \sum_{u\in X} a_u.$$

Example 1.2.6. *Let U be the free group on three variables: x, y, z. Let $R = \mathbf{Z}$ be the ring of integers. Then*

$$f(\overline{x}) = xy + 2xxz + xzxxz^{-1} - 4yx^{-1} + x^{-1}x^{-1}y$$

is an element of $\mathbf{Z}[U]$ and $\epsilon(f(\overline{x})) = 1 + 2 + 1 - 4 + 1 = 1$.

We now can characterize all derivations on $R[X]$ for an arbitrary ring R and free group X:

Theorem 1.2.7. *There exists a derivation $\frac{\partial}{\partial x_j}$ for each generator x_j of X with the property that*

$$\frac{\partial x_k}{\partial x_j} = \delta_{j,k}.$$

Furthermore, there exists only one derivation D that maps $(x_j)_{j\in I}$ to given elements $(h_j(\bar{x}))_{j\in I}$ of $R[X]$, $x_j \mapsto h_j(\bar{x})$.
This is given by

$$D(f(\bar{x})) = \sum_{j\in I} \frac{\partial f(\bar{x})}{\partial x_j} h_j(\bar{x}). \tag{1.7}$$

Proof. For each $j \in I$ and every element $u \in X$ we define

$$\langle j, u\rangle = \begin{cases} 1 & \text{if } u \text{ starts with } x_j \\ 0 & \text{else} \end{cases}$$

For instance $\langle 1, x_1x_2\rangle = 1$, $\langle 2, x_1x_2\rangle = 0$ and $\langle 1, x_1^{-1}x_2\rangle = 0$.
We extend this definition linearly in the second component for elements of $R[X]$:

$$\langle j, f(\bar{x})\rangle = \langle j, \sum_{u\in X} a_u u\rangle = \sum_{u\in X} a_u \langle j, u\rangle.$$

We then define for each $j \in I$ and $w \in X$

$$\langle j, w, f(\bar{x})\rangle = \langle j, w^{-1} f(\bar{x})\rangle - \langle j, w^{-1}\rangle f(1).$$

Remark that for $f(\bar{x}) = u \in X$ we have

$$\langle j, w, u\rangle = \langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle \cdot 1$$

which equals 0 if w is not an initial segment of u.
For if it is, then x_j is the first letter of $w^{-1}u$ if and only if x_j is the first letter of w^{-1}.

The first letter of w^{-1} only disappears in $w^{-1}u$ if w^{-1} disappears entirely in $w^{-1}u$, which happens only if w is an initial segment of u.

Given j and $f(\bar{x})$ we have

$$\begin{aligned} \langle j, w, f(\bar{x})\rangle &= \langle j, w^{-1}f(\bar{x})\rangle - \langle j, w^{-1}\rangle f(1) \\ &= \langle j, w^{-1}\sum_{u\in X} a_u u\rangle - \langle j, w^{-1}\rangle f(1) \\ &= \sum_{u\in X} a_u\langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle f(1) \\ &= \sum_{u\in X} a_u\left(\langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle\right) \\ &= \sum_{u\in X} a_u\langle j, w, u\rangle \end{aligned}$$

Obviously, $\langle j, w, f(\bar{x})\rangle$ is nonzero for only finitely many $w \in X$, for w has to be an initial segment of all $u \in X$ for which $a_u \neq 0$ in $f(\bar{x}) = \sum a_u u$.

Define

$$\frac{\partial f(\bar{x})}{\partial x_j} = \sum_{w\in X}\langle j, w, f(\bar{x})\rangle w.$$

This is a finite sum.

We check that it is a derivation:

$$\begin{aligned} \frac{\partial f(\bar{x}) + g(\bar{x})}{\partial x_j} &= \sum_{w\in X}\langle j, w, f(\bar{x}) + g(\bar{x})\rangle w \\ &= \sum_{w\in X}\langle j, w, \sum_{u\in X} a_u u + \sum_{u\in X} b_u u\rangle w \\ &= \sum_{w\in X}\langle j, w, \sum_{u\in X}(a_u + b_u)u\rangle w \\ &= \sum_{w\in X}\sum_{u\in X}(a_u + b_u)\langle j, w, u\rangle w \\ &= \sum_{w\in X}\sum_{u\in X} a_u\langle j, w, u\rangle w + \sum_{u\in X} b_u\langle j, w, u\rangle w \\ &= \sum_{w\in X}\langle j, w, f(\bar{x})\rangle w + \langle j, w, g(\bar{x})\rangle w \\ &= \sum_{w\in X}\langle j, w, f(\bar{x})\rangle w + \sum_{w\in X}\langle j, w, g(\bar{x})\rangle w \\ &= \frac{\partial f(\bar{x})}{\partial x_j} + \frac{\partial g(\bar{x})}{\partial x_j} \end{aligned}$$

and

$$\begin{aligned} \frac{\partial \lambda f(\bar{x})}{\partial x_j} &= \sum_{w\in X}\langle j, w, \lambda f(\bar{x})\rangle w \\ &= \sum_{w\in X}\lambda\langle j, w, f(\bar{x})\rangle w \end{aligned}$$

$$
\begin{aligned}
&= \lambda \sum_{w \in X} \langle j, w, f(\bar{x}) \rangle w \\
&= \lambda \frac{\partial f(\bar{x})}{\partial x_j}
\end{aligned}
$$

hence $\frac{\partial}{\partial x_j}$ is R-linear.

For the other property of derivations (see (1.2)), we first prove it for elements $u, v \in X$:

$$
\begin{aligned}
\frac{\partial uv}{\partial x_j} &= \sum_{w \in X} \langle j, w, uv \rangle w \\
&= \sum_{w \in X} \left(\langle j, w^{-1}uv \rangle - \langle j, w^{-1} \rangle \right) w \\
&= \sum_{w \in X} \left(\langle j, w^{-1}uv \rangle - \langle j, w^{-1}u \rangle + \langle j, w^{-1}u \rangle - \langle j, w^{-1} \rangle \right) w \\
&= \sum_{w \in X} \left(\langle j, w^{-1}u \rangle - \langle j, w^{-1} \rangle \right) w + \sum_{w \in X} \left(\langle j, w^{-1}uv \rangle - \langle j, w^{-1}u \rangle \right) w \\
&= \frac{\partial u}{\partial x_j} + \sum_{t \in X} \left(\langle j, t^{-1}v \rangle - \langle j, t^{-1} \rangle \right) ut \\
&= \frac{\partial u}{\partial x_j} + u \sum_{t \in X} \left(\langle j, t^{-1}v \rangle - \langle j, t^{-1} \rangle \right) t \\
&= \frac{\partial u}{\partial x_j} + u \frac{\partial v}{\partial x_j}
\end{aligned}
$$

Now, let $f(\bar{x}) = \sum a_u u$ and $g(\bar{x}) = \sum b_v v$. Then since $\frac{\partial}{\partial x_j}$ is linear and we have the above, we get:

$$
\begin{aligned}
\frac{\partial}{\partial x_j}(f(\bar{x})g(\bar{x})) &= \frac{\partial}{\partial x_j} \left(\sum a_u b_v uv \right) \\
&= \sum a_u b_v \frac{\partial}{\partial x_j}(uv) \\
&= \sum a_u b_v \left(\frac{\partial}{\partial x_j}(u)\varepsilon(v) + u \frac{\partial}{\partial x_j}(v) \right) \\
&= \sum \frac{\partial}{\partial x_j}(a_u u)\varepsilon(b_v v) + \sum a_u u \frac{\partial}{\partial x_j}(b_v v) \\
&= \frac{\partial}{\partial x_j} \left(\sum a_u u \right) \varepsilon \left(\sum b_v v \right) + \sum a_u u \frac{\partial}{\partial x_j} \left(\sum b_v v \right) \\
&= \frac{\partial}{\partial x_j}(f(\bar{x}))\varepsilon(g(\bar{x})) + f(\bar{x}) \frac{\partial}{\partial x_j}(g(\bar{x}))
\end{aligned}
$$

Indeed, $\frac{\partial}{\partial x_j}$ is a derivation. Now we show that $\frac{\partial x_k}{\partial x_j} = \delta_{j,k}$:

$$
\begin{aligned}
\frac{\partial x_k}{\partial x_j} &= \sum_{w \in X} \langle j, w, f(\bar{x}) \rangle w \\
&\overset{*}{=} \langle j, 1, x_k \rangle + \langle j, x_k, x_k \rangle x_k
\end{aligned}
$$

$$\begin{aligned} &= \langle j, x_k\rangle - \langle j, 1\rangle + (\langle j, 1\rangle - \langle j, x_k^{-1}\rangle)x_k \\ &= \delta_{j,k} - 0 + (0-0)x_k \\ &= \delta_{j,k} \end{aligned}$$

Note that in (*) we have used that only 1 and x_k are initial segments of x_k.
We have $\frac{\partial}{\partial x_j} f(\bar{x}) \neq 0$ for only finitely many j. This is due to the fact that $f(\bar{x}) = \sum_{u\in X} a_u u$, where there at most finitely many $a_u \neq 0$ and where each u has only finitely many different x_j's (and x_j^{-1}'s). If u does not contain an x_j or an x_j^{-1} we have $\frac{\partial u}{\partial x_j} = 0$, by (1.5) and the fact that

$$\frac{\partial x_k^{-1}}{\partial x_j} = -x_k^{-1}\frac{\partial x_k}{\partial x_j} = 0$$

for $j \neq k$.
Hence the sum

$$\sum_{j\in I} \frac{\partial f(\bar{x})}{\partial x_j}$$

is a finite sum. Since $\mathrm{Der}_R(G)$ is a right $R[G]$-module, we find that

$$D_0(f(\bar{x})) = \sum_{j\in I} \frac{\partial f(\bar{x})}{\partial x_j} h_j(\bar{x})$$

is a derivation for any given $(h_j(\bar{x}))_{i\in I}$.
Note that $D_0(x_k) = \sum_{j\in I} \frac{\partial x_k}{\partial x_j} h_j(x) = h_k(x)$ as required.
Suppose lastly that D is a derivation of $R[X]$ for which we also have $x_j \mapsto h_j(\bar{x})$.
Consider the derivation $\widehat{D} = D - D_0$. This is a derivation for which $x_k \mapsto 0$ for each k and hence $x_k^{-1} \mapsto 0$ as well. Hence we have

$$\begin{aligned} \widehat{D}(f(\bar{x})) &= \widehat{D}\left(\sum_{u\in X} a_u u\right) \\ &= \sum_{u\in X} a_u \widehat{D}(u) \\ &= \sum_{u\in X} a_u \cdot 0 \\ &= 0 \end{aligned}$$

Therefore, $D = D_0$ and we have uniqueness. □

Corollary 1.2.8. *We can obtain $f(\bar{x})$ from the information $f(1)$ and $\frac{\partial}{\partial x_j} f(\bar{x})$, as in the following (fundamental) formula*

$$f(\bar{x}) = f(1) + \sum_{j\in I} \frac{\partial f(\bar{x})}{\partial x_j}(x_j - 1).$$

Proof. The linear map D given by $D(f(\bar{x})) = f(\bar{x}) - f(1)$ is a derivation.

$$D(f(\bar{x})g(\bar{x})) = f(\bar{x})g(\bar{x}) - f(1)g(1)$$

$$\begin{aligned} &= f(\bar{x})g(\bar{x}) + f(\bar{x})g(1) - f(\bar{x})g(1) - f(1)g(1) \\ &= (f(\bar{x}) - f(1))g(1) + f(\bar{x})(g(\bar{x}) - g(1)) \\ &= D(f(\bar{x}))g(1) + f(\bar{x})D(g(\bar{x})) \end{aligned}$$

as required. As we have $D(x_j) = x_j - 1$ for every $j \in I$, we obtain by Theorem 1.2.7

$$f(\bar{x}) - f(1) = \sum_{j \in I} \frac{\partial f(\bar{x})}{\partial x_j}(x_j - 1)$$

as required. △

Example 1.2.9. *Let $f(\bar{x}) = x_j^p$ for some p. By the fundamental formula we obtain*

$$x_j^p = 1 + \sum_{j \in I} \frac{\partial x_j^p}{\partial x_j}(x_j - 1).$$

Since $\frac{\partial x_j^p}{\partial x_i} = 0$ for all $i \neq j$, we have

$$x_j^p - 1 = \frac{\partial x_j^p}{\partial x_j}(x_j - 1).$$

Hence

$$\frac{\partial x_j^p}{\partial x_j} = \frac{x_j^p - 1}{x_j - 1} = \begin{cases} 1 + x_j + \ldots + x_j^{p-1} & \text{if } p \geq 1; \\ 0 & \text{if } p = 0; \\ -x_j^p - x_j^{p+1} - \ldots - x_j^{-1} & \text{if } p \leq -1. \end{cases}$$

We already know that given a homomorphism $\varphi\colon Y \to X$ where X and Y are free groups, that φ induces a ring homomorphism between the free group rings $R[Y]$ and $R[X]$ given by

$$\varphi\left(\sum_{u \in Y} a_u u\right) = \sum_{u \in Y} a_u \varphi(u).$$

Theorem 1.2.10. *For free groups X generated by $(x_i)_{i \in I_X}$ and Y generated by $(y_j)_{j \in I_Y}$ and a homomorphism $\varphi\colon Y \to X$ we have the* chain rule *of Fox calculus:*

$$\frac{\partial \varphi(f(\bar{y}))}{\partial x_j} = \sum_{k \in I_Y} \varphi\left(\frac{\partial f(\bar{y})}{\partial y_k}\right) \frac{\partial \varphi(y_k)}{\partial x_j}.$$

Proof. We apply Corollary 1.2.8 to $f(\bar{y})$:

$$\begin{aligned} \frac{\partial \varphi(f(\bar{y}))}{\partial x_j} &= \frac{\partial \varphi\left((f(1) + \sum_{k \in I_Y} \frac{\partial f(\bar{y})}{\partial y_k}(y_k - 1)\right)}{\partial x_j} \\ &= \frac{\partial \varphi(f(1))}{\partial x_j} + \frac{\partial \varphi\left(\sum_{k \in I_Y} \frac{\partial f(\bar{y})}{\partial y_k}(y_k - 1)\right)}{\partial x_j} \\ &= \sum_{k \in I_Y} \frac{\partial \varphi\left(\left(\frac{\partial f(\bar{y})}{\partial y_k}\right)(y_k - 1)\right)}{\partial x_j} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k\in I_Y} \frac{\partial\varphi\left(\frac{\partial f(\bar{y})}{\partial y_k}\right)\varphi(y_k-1)}{\partial x_j} \\
&= \sum_{k\in I_Y} \frac{\partial\varphi\left(\frac{\partial f(\bar{y})}{\partial y_k}\right)(\varphi(y_k)-1)}{\partial x_j} \\
&= \sum_{k\in I_Y} \frac{\partial\varphi\left(\frac{\partial f(\bar{y})}{\partial y_k}\right)}{\partial x_j}\varepsilon(\varphi(y_k-1)) + \sum_{k\in I_Y}\varphi\left(\frac{\partial f(\bar{y})}{\partial y_k}\right)\cdot\frac{\partial\varphi(y_k)}{\partial x_j}
\end{aligned}
$$

Since $\varphi(y_k)\in X$ we have $\varepsilon(\varphi(y_k)-1)=\varepsilon(\varphi(y_k))-\varepsilon(1)=1-1=0$, hence the result. □

1.2.3 Inverse Function Theorem for free groups

In this section, we repeat the proof of Birman in [2] of the Inverse Function Theorem for free groups. Therefore, our answer to the Jacobian Conjecture in this context is affirmative.

The following definition and lemma are from elementary group theory (see [3]), we will use it in the proof for the Inverse Function Theorem.

Definition 1.2.11. *Let G be a group and R a ring. The* augmentation ideal *I_G of G is the kernel of the homomorphism $\varepsilon\colon R[G]\to R$. Note that I_G is a free R-module with set of generators $\{g-e \mid e\neq g\in G\}$. If $H<G$, then we write J_H for the right ideal I_H of $R[G]$.*

Lemma 1.2.12. *Let G be a group and R a ring. Let $H,K<G$ and $g\in G$. Then*

i. $g-e\in J_H$ if and only if $g\in H$;

ii. $J_H\subset J_K$ iff $H\subset K$;

iii. $J_H=J_K$ iff $H=K$.

Proof.

i. If $g\in H$, then clearly $g-e\in J_H$. Conversely, since J_H is generated by $\{h-e \mid e\neq h\in H\}$, if $g-e\in J_H$ we can write $g-e=\sum n_h(h-e)$ with the $n_h\in\mathbf{Z}$. Since $h-e\in H$, we find that indeed $g-e\in H$, and hence $g\in H$.

ii. It is clear that if $H\subset K$, that $J_H\subset J_K$. Now suppose that $J_H\subset J_K$ and let $h\in H$. Then by (i), we have $h-e\in J_H$, hence $h-e\in J_K$. By (i) again, we have $h\in K$. Hence $H\subset K$.

iii. This follows immediately from (ii).

△

Theorem 1.2.13. (Inverse Function Theorem for Free Groups) *Let $\{y_1,\dots,y_k\}$ be a set of $k\leq n$ elements of the free group on n generators F_n. We write J_{kn} for the $k\times n$ matrix*

$$
\begin{pmatrix}
\frac{\partial y_1}{\partial x_1} & \cdots & \frac{\partial y_1}{\partial x_n} \\
\vdots & & \vdots \\
\frac{\partial y_k}{\partial x_1} & \cdots & \frac{\partial y_k}{\partial x_n}
\end{pmatrix}
$$

with elements in $\mathbf{Z}[F_n]$.

i. If $k = n$, then $\{y_1, \dots, y_n\}$ is a generating set for F_n if and only if J_{nn} has a right inverse.

ii. If $k < n$ and $\{y_1, \dots, y_k\}$ extends to a generating set $\{y_1, \dots, y_n\}$, then J_{kn} has a right inverse.

Proof. i. ($\Leftarrow$): Suppose that $B = (\beta_{ij})$ is a right inverse of J_{nn}. Then by Corollary 1.1.26 we see that it is also a left inverse of J_{nn}. Hence we have

$$\sum_{s=1}^{n} \beta_{is} \left(\frac{\partial y_s}{\partial x_j} \right) = \delta_{i,j} \text{ for all } i, j \in \{1, \dots, n\}.$$

If we multiply both sides by $x_j - 1$ and then summing over j, we get

$$\sum_{j=1}^{n} \sum_{s=1}^{n} \beta_{is} \left(\frac{\partial y_s}{\partial x_j} \right) (x_j - 1) = \sum_{j=1}^{n} \delta_{i,j} (x_j - 1)$$

i.e.

$$\sum_{s=1}^{n} \beta_{is} \sum_{j=1}^{n} \frac{\partial y_s}{\partial x_j} (x_j - 1) = x_i - 1.$$

By the fundamental formula of Fox calculus (Corollary 1.2.8) we have (setting $f(\bar{x}) = y_s$)

$$\sum_{j=1}^{n} \frac{\partial y_s}{\partial x_j} (x_j - 1) = y_s - 1 \text{ for all } s = 1, \dots, n.$$

Hence

$$\sum_{s=1}^{n} \beta_{is} (y_s - 1) = x_i - 1 \text{ for all } i = 1, \dots, n.$$

Now write $\langle y_1, \dots, y_n \rangle = H < F_n$. Then I_H is the two-sided ideal of $\mathbf{Z}[F_n]$ generated by $y_1 - 1, \dots, y_n - 1$.

We have shown that for each $i = 1, \dots, n$ we have $x_i - 1 \in I_H$. Then by Lemma 1.2.12 we have $x_i \in H$. Hence $H = F_n$.

($\Rightarrow$): Suppose that $\{y_1, \dots, y_n\}$ is a generating set for F_n. Then we have $x_i = X_i(y_1, \dots, y_n)$ and $y_i = Y_i(x_1, \dots, x_n)$ (we can write x_i as a word in the y_j and each y_i as a word in the x_j).

Combining these, we find

$$Y_i(X_1(y_1, \dots, y_n), \dots, X_n(y_1, \dots, y_n)) = y_i \text{ for all } i = 1, \dots, n.$$

We then get

$$\frac{\partial Y_i(X_1(y_1, \dots, y_n), \dots, X_n(y_1, \dots, y_n))}{\partial y_j} = \frac{\partial y_i}{\partial y_j} \text{ for all } i, j = 1, \dots, n.$$

Or, using the chain rule (Theorem 1.2.10) we get

$$\sum_{s=1}^{n} \left(\frac{\partial Y_i(x_1, \dots, x_n)}{\partial x_s} \right) \left(\frac{\partial X_s(y_1, \dots, y_n)}{\partial y_j} \right) = \delta_{i,j} \text{ for all } i, j = 1, \dots, n,$$

i.e.,

$$\sum_{s=1}^{n} \left(\frac{\partial y_i}{\partial x_s}\right) \left(\frac{\partial x_s}{\partial y_j}\right) = \delta_{i,j} \text{ for all } i, j = 1, \ldots, n.$$

Hence $J_{nn} = \left(\frac{\partial y_i}{\partial x_j}\right)_{i,j}$ has a right inverse, namely $\left(\frac{\partial x_i}{\partial y_j}\right)_{i,j}$.

ii. Suppose that $\{y_1, \ldots, y_k\}$ extends to a generating set $\{y_1, \ldots, y_n\}$. Then J_{kn} is the $k \times n$ submatrix of J_{nn} formed by taking the first k rows of J_{nn}.

A right inverse is then given by the $n \times k$ submatrix of J_{nn}^{-1} formed by taking the first k columns of J_{nn}^{-1}.

□

Chapter 2

Mathieu-Zhao spaces

In this section we will talk about the general notion of Mathieu-Zhao spaces that Zhao introduced from the various conjectures regarding the Jacobian Conjecture.

As discussed in the introduction, we have various Conjectures which imply the Jacobian Conjecture. Particular examples are

Conjecture. (Mathieu Conjecture) *Let G be a compact connected real Lie group with Haar measure σ. Let f be a complex valued G-finite function on G such that $\int_G f^m d\sigma = 0$ for all $m \geq 1$. Then for every G-finite function g on G, also $\int_G gf^m d\sigma = 0$ for all large m.*

See [11] for discussion about the Mathieu Conjecture and the proof that it implies the Jacobian Conjecture.

Conjecture. (Vanishing Conjecture) *If $f \in k[X_1, \dots, X_n]$ is homogeneous and such that $\Delta^m f^m = 0$ for all $m \geq 1$, then for every $g \in k[X_1, \dots, X_n]$ we have $\Delta^m(gf^m) = 0$ for all large m.*

These conjectures imply the Jacobian Conjecture, and can be formulated in terms of MZ-spaces, we will do so in Section 2.1 after we have defined MZ-spaces. In this text we do not discuss the above two conjectures, but only note that just one special case of (MC) is proven by the theorem of Duistermaat and Van der Kallen in [5], which we will discuss in Chapter 3. For more about these conjectures see [7].

2.1 Definition and Examples

Let R be a commutative ring with identity (all rings will be as such from now on) and A an associative unital R-algebra (all algebras in this chapter will be as such). Recall that a (left) ideal I of A is a subalgebra of A such that for all $a, b \in A$ we have

$$a \in I \implies ba \in I.$$

Hence in particular, if $a^m \in I$ for all $m \geq 1$, then $ba^m \in I$ for all $m \geq 1$.

For (left) Mathieu-Zhao spaces we relax this criterion to:

If $a^m \in M$ for all $m \geq 1$, then $ba^m \in M$ for all $m \gg 0$.

That is, there exists some $N > 0$ (depending on b) such that $ba^m \in M$ for all $m \geq N$.

Below, we define Mathieu-Zhao spaces a little more rigorous and give some examples.

Definition 2.1.1. *Let R be any commutative ring and A an associative (unital) R-algebra. For any subset M of A we define the* radical of M *by*

$$r(M) := \{a \in A \mid \forall m \gg 0 : a^m \in M\}$$

with $m \gg 0$ meaning all $m \geq N$ for some $N \geq 1$.

Remark. *For an ideal I of R, this coincides with the usual definition of the radical of I, being:*

$$\sqrt{I} := \{a \in R \mid \exists n : a^n \in I\}.$$

It is well-known that the radical of an ideal is an ideal itself, and hence all a^{n+i} are elements of I for $i \geq 0$.

Definition 2.1.2. *Let R be any commutative ring and A an associative (unital) R-algebra. For any subset M of A we define the* (left) strong radical of M *by*

$$sr(M) := \{a \in A \mid \forall b \in A \, \forall m \gg 0 : ba^m \in M\}.$$

Remark. *Note that if $a \in sr(M)$, then $1 \cdot a^m \in M$ for all $m \gg 0$, hence $a \in r(M)$. So we always have $sr(M) \subset r(M)$.*

Definition 2.1.3. *Let R be any commutative ring and A an associative (unital) R-algebra. We say that an R-submodule M of A is a Mathieu-Zhao space of A if and only if $sr(M) = r(M)$.*

A little less is needed in practice. Define $r'(M) = \{a \in A \mid \forall m \geq 1 : a^m \in M\}$. It is clear that $r'(M) \subset r(M)$. We now show that if $r'(M) \subset sr(M)$, then $r(M) = sr(M)$.

Proposition 2.1.4. *If $r'(M) \subset sr(M)$, then $r(M) \subset sr(M)$ and M is an MZ-space.*

Proof. Let $a \in r(M)$ be arbitrary. Then there exists some $N \geq 1$ such that $a^m \in M$ for all $m \geq N$. In particular we find $(a^N)^m \in M$ for all $m \geq 1$. Let $b \in A$ be arbitrary. Then since $a^N \in r'(M)$ we know that $a^N \in sr(M)$. Hence for every $0 \leq i \leq N-1$ there exists some N_i such that $(ba^i)(a^N)^m \in M$ for all $m \geq N_i$. Write $N' = \max_i N_i$. It follows that $ba^{Nm+i} \in M$ for all $m \geq N'$ and all $0 \leq i \leq N-1$. Now note that every $n \geq NN'$ can be written as $Nm + i$ for some $m \geq N'$ and $0 \leq i \leq N-1$ by division with remainder. Hence $ba^n \in M$ for all $n \geq NN'$, and $a \in sr(M)$. □

The above proposition shows that the introductory definition of Mathieu-Zhao spaces is correct. It is immediate that ideals are Mathieu-Zhao spaces.

Example 2.1.5. *Let R be a commutative ring and A an associative (unital) R-algebra. Let I be an ideal of A. Then I is an MZ-space.*

Proof. By Proposition 2.1.4, we only need to prove $r'(I) \subset sr(I)$. Therefore, let $a \in r'(I)$ be arbitrary, that is, $a^m \in I$ for all $m \geq 1$, in particular $a \in I$. Since I is an ideal, we have for all $c \in A$ that $ca \in I$. In particular, for any $b \in A$ and any $n \geq 0$ we have $ba^n a \in I$. Hence indeed, $a \in sr(I)$. △

The converse is not true:

Counterexample 2.1.6. *The finite field $\mathbb{F}_4$ has only two (trivial) ideals, while it has much more Mathieu-Zhao spaces, for example the set $\{0, x\}$ is one. For a proof of this result, see Example 4.1.3.*

For non-commutative rings we have distinctions for left- and right- Mathieu-Zhao spaces and we reserve the notion of Mathieu-Zhao space for the (two-sided) Mathieu-Zhao space for which $a \in r(M)$ implies that $ba^m c \in M$ for all $b, c \in A$ and $m \gg 0$. We have stated above the definition of a left- Mathieu-Zhao space and leave the definition for a right- Mathieu-Zhao space to the reader. For commutative rings there is no such distinction necessary.

Now that we have defined MZ-spaces, we can write the Mathieu Conjecture in terms of MZ-spaces:

Conjecture. (Mathieu Conjecture) *Let G be a compact connected real Lie group with Haar measure σ and let A be the set of $\mathbf{C}$-complex G-finite functions on G. Then*

$$\left\{ f \in A \mid \int_G f d\sigma = 0 \right\}$$

is an MZ-space of A.

This reformulation of the Mathieu Conjecture and further generalizations of the Vanishing Conjecture made by Zhao, motivated Zhao to define and investigate what he called Mathieu subspaces. See also [16]. Later Van den Essen renamed Mathieu subspaces to Mathieu-Zhao spaces, to honor him for his founding of this field of study and his many great contributions to it.

2.1.1 Non-trivial Example

For the first (highly) non-trivial example we note that the following theorem is of high importance.

Theorem 2.1.7. (Zero-Traces Theorem) *Let M be an $n \times n$ matrix with coefficients $\mathbf{C}$. If $\mathrm{Tr}(M^m) = 0$ for all $m \geq 1$, then M is nilpotent.*

We have two different versions of this theorem, each with an interesting proof. Note that they are all a little bit stronger than the above theorem, so either proof is a proof of the above, verbatim.

Theorem 2.1.8. *Let M be an $n \times n$ matrix with coefficients in $\mathbf{C}$. If there exists an N such that $\mathrm{Tr}(M^m) = 0$ for all $m \geq N$, then M is nilpotent.*

Proof. (1. Generating series) It is well-known that $\mathrm{Tr}(M^m) = \lambda_1^m + \ldots + \lambda_n^m$, where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of M. Suppose that M is not nilpotent, that is, there is some eigenvalue of M that is nonzero. Choose any such eigenvalue λ_{j_0}. Define $\ell = \#\{i \in \{1, \ldots, n\} \mid \lambda_i = \lambda_{j_0}\}$. Order the eigenvalues such that $\lambda_{j_0} = \lambda_1$ and $\lambda_1 = \ldots = \lambda_\ell$.

Define

$$W(z) = \sum_{m=0}^{\infty} \mathrm{Tr}(M^m) z^m.$$

By our hypothesis $W(z)$ is a polynomial and we find

$$\begin{aligned} W(z) &= \sum_{m=0}^{\infty} (\lambda_1^m + \ldots + \lambda_n^m) z^m \\ &= \sum_{j=1}^{n} \sum_{m=0}^{\infty} (\lambda_j z)^m \end{aligned}$$

$$= \sum_{j=1}^{n} \frac{1}{1-\lambda_j z}$$

Consider multiplying $W(z)$ by the other polynomial $1-\lambda_1 z$. We find $(1-\lambda_1 z)W(z) = \ell + \sum_{i=\ell+1}^{n} \frac{1-\lambda_1 z}{1-\lambda_i z}$. If we evaluate at $z = \frac{1}{\lambda_1}$, we get 0 on the left-hand side, while the right-hand side equals $\ell > 0$. This is a contradiction. Hence there is no nonzero eigenvalue, hence M is nilpotent. □

Theorem 2.1.9. *Let M be an $n \times n$ matrix with complex coefficients. If $\mathrm{Tr}(M^k) = 0$ for all $1 \leq k \leq n$, then M is nilpotent.*

Proof. (2: Vandermonde-determinant) Suppose that M is not nilpotent, then M has some non-zero eigenvalues $\lambda_1, \ldots, \lambda_r$. Suppose they are all distinct and have multiplicities n_i. Then by a well-known fact we have $\mathrm{Tr}(M^k) = n_1\lambda_1^k + \ldots + n_r\lambda_r^k$. Hence we have the following system of equations:

$$\begin{cases} n_1\lambda_1 & +\ldots & +n_r\lambda_r & = 0 \\ n_1\lambda_1^2 & +\ldots & +n_r\lambda_r^2 & = 0 \\ \vdots & & \vdots & \vdots \\ n_1\lambda_1^n & +\ldots & +n_r\lambda_r^n & = 0 \end{cases}$$

which we can write as

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^n & \lambda_2^n & \ldots & \lambda_r^n \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

By Vandermonde's identity for determinants we find

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^n & \lambda_2^n & \ldots & \lambda_r^n \end{vmatrix} = \lambda_1\lambda_2\cdots\lambda_r \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_r \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_r^{n-1} \end{vmatrix} \neq 0.$$

Therefore, the system as a unique solution in the n_i. Hence $n_i = 0$ for all i, a contradiction. Hence M is indeed nilpotent. □

We now consider the aforementioned non-trivial example of Mathieu-Zhao spaces.

Example 2.1.10. *Let G be a finite group. Then the following subset of $\mathbf{C}[G]$ is a Mathieu-Zhao space:*

$$\{f \in \mathbf{C}[G] \mid f_e = 0\}.$$

Proof. For $f \in \mathbf{C}[G]$ define $\lambda(f)\colon \mathbf{C}[G] \to \mathbf{C}[G]$ as $\lambda(f)(h) = fh$. This a $\mathbf{C}$-linear map:

Let $h_1, h_2 \in \mathbf{C}[G]$ and $\mu \in \mathbf{C}$ be arbitrary. Then

$$\lambda(f)(h_1 + h_2) = f(h_1 + h_2) = fh_1 + fh_2 = \lambda(f)(h_1) + \lambda(f)(h_2)$$

and

$$\lambda(f)(\mu h) = f \cdot \mu h \overset{(*)}{=} \mu f h = \mu\lambda(f)(h)$$

where we have used that $\mathbf{C}[G]$ is an $\mathbf{C}$-module in (*).

Note further that $\dim_{\mathbf{C}} \mathbf{C}[G] = \#G = n < \infty$.
Since $\lambda(f)$ is linear, we can compute the trace of this map. Note that $\mathrm{Tr}(\lambda(g)) = 0$ when $g \neq e$:
Write $G = \{e, g_2, \ldots, g_n\}$ and suppose that $g \neq e$. Then

$$\lambda(g)_{ij} = \begin{cases} 1 & \text{if } gg_i = g_j; \\ 0 & \text{otherwise} \end{cases}.$$

Since $g \neq e$ we have $gg_i \neq g_j$ when $i = j$. So $\lambda(g)_{ii} = 0$ for all i, hence $\mathrm{Tr}(\lambda(g)) = 0$.

Then $\mathrm{Tr}(\lambda(f)) = \mathrm{Tr}(\lambda(\sum f_g g)) = \mathrm{Tr}(\sum f_g \lambda(g)) = \sum f_g \,\mathrm{Tr}(\lambda(g)) = n \cdot f_e$.
Now if $(f^m)_e = 0$ for all $m \geq 1$, then we have

$$\mathrm{Tr}(\lambda(f)^m) = \mathrm{Tr}(\lambda(f^m)) = n(f^m)_e = 0 \text{ for all } m \geq 1.$$

Then $\lambda(f)$ satisfies the condition of the Zero-Traces Theorem (2.1.7), hence $\lambda(f)$ is nilpotent.
Hence $\lambda(f)^n = 0$ for some $n \geq 1$ and hence $\lambda(f^n) = 0$ for some $n \geq 1$. So $f^n = 0$. In particular, for all $h \in \mathbf{C}[G]$ we have $f^n h = 0$. Thus $\{f \in \mathbf{C}[G] \mid f_e = 0\}$ is a Mathieu Zhao space. △

The last lines of this proof can be generalized to the following important but easy result:

Lemma 2.1.11. *Let R be a commutative ring with identity and A an R-algebra. Let M be an R-linear subspace of A such that $r(M)$ is contained in the set of nilpotent elements, then M is an MZ-space of A.*

Proof. Let $a \in r(M)$. Then there exists some $N \in \mathbf{N}$ such that $a^N = 0$. Then $ba^m = (ba^{m-N})a^N = 0$ for all $m \geq N$. Hence $a \in sr(M)$ and M is an MZ-space. △

Corollary 2.1.12. *Let R be a commutative ring with identity and A an A-algebra. Let M be an R-linear subspace of A. Then*

$$r(M) \subset \mathfrak{n}(R) \iff r'(M) \subset \mathfrak{n}(R).$$

Proof. Since $r'(M) \subset r(M)$, the implication $\Longrightarrow$ is clear. Conversely, let $a \in r(M)$ be arbitrary. Then there exists some $N \geq 1$ such that $a^k \in M$ for all $k \geq N$. Hence in particular $(a^N)^i \in M$ for all $i \geq 1$. Therefore $a^N \in r'(M) \subset \mathfrak{n}(R)$, hence a^N is nilpotent. But then a is nilpotent, as required. △

Another highly non-trivial example is the one-dimensional theorem of Duistermaat and Van der Kallen, see Theorem 3.2.4. We end this section with another non-trivial example due to Mitya Boyarchenko, his proof can be found in [9].

Example 2.1.13. *Let V be the set*

$$\left\{ f \in \mathbf{C}[X] \mid \int_0^1 f(x)dx = 0 \right\}.$$

Then V is an MZ-space of $\mathbf{C}[X]$.

2.2 General Results

In this section we discuss results on MZ-spaces that we need for this thesis. Further reading can be done in [4], [16].

Lemma 2.2.1. *Let R be a commutative ring and A an associative (unital) R-algebra. Let M be a Mathieu-Zhao space of A and $e \in M$ an idempotent. Then $Ae \subset M$. In particular, if $1 \in M$, then $M = A$.*

Proof. Since $e^m = e$ for all $m \geq 1$, we find that $e \in r(M)$. Then for all $b \in A$ we have $be^m \in M$ for all $m \gg 0$, hence $be \in M$ for all $b \in A$ and $Ae \subset M$. △

Proposition 2.2.2. *Let R be a ring and A, B be R-algebras. Let $f\colon A \to B$ be a ring homomorphism. Let $M \subset A$ and $N \subset B$ be arbitrary subsets. Then*

(i) $r(f^{-1}(N)) = f^{-1}(r(N))$;

(ii) $f^{-1}(sr(N)) \subset sr(f^{-1}(N))$;

(iii) $f(r(M)) \subset r(f(M))$;

If f is surjective, we have

(iv) $f^{-1}(sr(N)) = sr(f^{-1}(N))$;

(v) $f(sr(M)) \subset sr(f(M))$;

If M is additive and $\operatorname{Ker}(f) \subset M$, then (without f necessarily being surjective):

(vi) $f^{-1}(r(f(M))) \subset r(M)$;

(vii) $f^{-1}(sr(f(M))) \subset sr(M)$;

Now assume that f is surjective and M is an additive subset of A such that $\operatorname{Ker}(f) \subset M$:

(viii) $f(r(M)) = r(f(M))$;

(ix) $f(sr(M)) = sr(f(M))$.

Proof. (i) Note that the following are equivalent for $a \in A$:

$$\begin{array}{ll} & a \in r(f^{-1}(N)) \\ \forall m \gg 0 & a^m \in f^{-1}(N) \\ \forall m \gg 0 & f(a^m) \in N \\ \forall m \gg 0 & f(a)^m \in N \\ & f(a) \in r(N) \\ & a \in f^{-1}(r(N)) \end{array}$$

Hence indeed, $r(f^{-1}(N)) = f^{-1}(r(N))$.

(ii) Note that the following are all equivalent for $a \in A$:

$$\begin{array}{lll} & & a \in f^{-1}(sr(N)) \\ & & f(a) \in sr(N) \\ \forall b \in B & \forall m \gg 0 & bf(a)^m \in N \\ \forall b \in B & \forall m \gg 0 & bf(a^m) \in N \end{array}$$

This last expression trivially implies (but is not equivalent to) the first of the following equivalent expressions for $a \in A$:

$$\begin{array}{lll} \forall b \in f(A) & \forall m \gg 0 & bf(a^m) \in N \\ \forall c \in A & \forall m \gg 0 & f(c)f(a^m) \in N \\ \forall c \in A & \forall m \gg 0 & f(ca^m) \in N \\ \forall c \in A & \forall m \gg 0 & ca^m \in f^{-1}(N) \\ & & a \in sr(f^{-1}(N)) \end{array}$$

(iii) Let $b \in f(r(M))$ be arbitrary. Then there exists some $a \in r(M)$ with $f(a) = b$. Let N be such that $a^n \in M$ for all $n \geq N$. Since $f(a) = b$ and f is a ring homomorphism, we have $f(a^n) = f(a)^n = b^n$ for all $n \geq N$. Then for all $n \geq N$ we have $b^n = f(a^n) \in f(M)$, hence $b \in r(f(M))$.

(iv) Here the implication mentioned in (ii) is in fact an equivalence, since $f(A) = B$.

(v) Let $b \in f(sr(M))$ be arbitrary. That is, there exists some $a \in sr(M)$ with $f(a) = b$. Furthermore let $b' \in B$ be arbitrary. Since f is surjective, we know that there exists some $c \in A$ with $f(c) = b'$. Since $a \in sr(M)$ we find that $ca^m \in M$ for all $m \gg 0$. Hence $f(ca^m) \in f(M)$ for all $m \gg 0$. Note that $b'b^m = f(c)f(a)^m = f(ca^m) \in f(M)$ for all $m \gg 0$, hence $b \in sr(f(M))$ as required.

(vi) Let $a \in f^{-1}(r(f(M)))$ be arbitrary. Then $f(a) \in r(f(M))$. Hence $f(a)^m \in f(M)$ for all $m \gg 0$. Since $f(a^m) = f(a)^m \in f(M)$ for all $m \gg 0$, there exists a $\mu_m \in M$ such that $f(a^m) = f(\mu_m)$ for all $m \gg 0$. Hence for all $m \gg 0$ we have $a^m - \mu_m \in \operatorname{Ker} f \subset M$. Hence $a^m \in M$ for all $m \gg 0$. Therefore $a \in r(M)$.

(vii) Let $a \in f^{-1}(sr(f(M)))$ and $c \in A$ be arbitrary. Since $a \in f^{-1}(sr(f(M)))$ we have $f(a) \in sr(f(M))$. That is, $bf(a)^m \in f(M)$ for all $b \in B$ and all $m \gg 0$. Hence in particular $f(c)f(a)^m \in f(M)$ for all $m \gg 0$. Then $f(ca^m) \in f(M)$ for all $m \gg 0$. Therefore, for every $m \gg 0$ there exists some $\mu_m \in M$ such that $f(ca^m) = f(\mu_m)$, hence $ca^m - \mu_m \in \operatorname{Ker} f \subset M$ for all $m \gg 0$. Therefore $ca^m \in M$ for all $m \gg 0$. Since $c \in A$ was arbitrary, we find $a \in sr(M)$.

(viii) Due to (iii) we only have to prove the converse inclusion. Note that by (vi) we already have $f^{-1}(r(f(M))) \subset r(M)$. Hence we obtain $f(f^{-1}(r(f(M)))) \subset f(r(M))$. Since f is surjective we have $f(f^{-1}(N)) = N$ for every subset N of B, hence $r(f(M)) \subset f(r(M))$ as required.

(ix) Due to (v) we only have to prove the converse inclusion. For that, let $b \in sr(f(M))$ be arbitrary. Since f is surjective, we may write $b = f(a)$ for some $a \in A$. If we show that $a \in sr(M)$, then $b = f(a) \in f(sr(M))$, as required.

Therefore let $c \in A$ be arbitrary. Since $f(a) \in sr(f(M))$ we know that $b'f(a)^m \in f(M)$ for all $m \gg 0$ and all $b' \in B$. Therefore, in particular it holds for $b' = f(c)$. Hence $f(ca^m) \in f(M)$ for all $m \gg 0$. Therefore, for every $m \gg 0$ there exists some $\mu_m \in M$ such that $f(ca^m) = f(\mu_m)$. So $ca^m - \mu_m \in \operatorname{Ker} f \subset M$ for all $m \gg 0$. Thus $ca^m \in M$ for all $m \gg 0$. Since $c \in A$ was arbitrary, we find $a \in sr(M)$.

□

Corollary 2.2.3. *Let R be a commutative ring and A, B be R-algebras. Let $f\colon A \to B$ be surjective and let M be an additive subset of A such that $\operatorname{Ker}(f) \subset M$. Then M is an MZ-space of A if and only if $f(M)$ is an MZ-space of B. In particular, isomorphisms preserve MZ-spaces.*

Proof. If M is an MZ-space of A, then $sr(M) = r(M)$. Hence $f(sr(M)) = f(r(M))$. By (viii) and (ix) of Proposition 2.2.2 we find that $sr(f(M)) = f(sr(M)) = f(r(M)) = r(f(M))$ and $f(M)$ is an MZ-space of B.

Conversely, if $f(M)$ is an MZ-space of B, we need to show that $r(M) \subset sr(M)$. Therefore let $a \in r(M)$ be arbitrary. Then $f(a) \in f(r(M)) = r(f(M)) \subset sr(f(M))$ since $f(M)$ is an MZ-space. Then $a \in f^{-1}(sr(f(M))) \subset sr(M)$ by (vii) of Proposition 2.2.2. △

Corollary 2.2.4. *Let R be a commutative ring and A an associative (unital) R-algebra. Let M be an additive subset of A and $I \subset A$ an ideal of A such that $I \subset M$. Then M is an MZ-space of A if and only if M/I is an MZ-space of A/I.*

Proof. Apply Corollary 2.2.3 with $B := A/I$ and $f\colon A \to A/I$ the canonical map. Then $\operatorname{Ker} f = I \subset M$ and f is surjective by definition. △

2.2.1 Zhao's Theorem

One of the most important theorems regarding MZ-spaces is Zhao's Theorem about idempotent elements:

Theorem 2.2.5. (Zhao's Theorem) *Let k be a field and A an associative k-algebra. Let M be a k-linear subspace of A such that all elements of $r(M)$ are algebraic over k. Then M is an MZ-space of A if and only if $Ae \subset M$ for all idempotents e which belong to M.*

Proof. $(\Rightarrow)$: This is already proven earlier in Lemma 2.2.1.

$(\Leftarrow)$: Let $a \in r(M)$ be arbitrary.

Claim: There exists $e \in M$ with $e^2 = e$ and $n \geq 1$ such that $a^m \in M$ for all $m \geq n$ with $a^n e = a^n$:

Proof. Since $a \in r(M)$ we find that for some N we have $a^m \in M$ for all $m \geq N$. Since a is algebraic over k, there exists some $0 \neq f(X) \in k[X]$ with $f(a) = 0$. Define $g(X) = X^N f(X)$ and write $g(X) = X^n h(X)$ with $n \geq N$ and $h(0) \neq 0$. Since $k[X]$ is a Euclidean domain we can find $u(X), v(X) \in k[X]$ with

$$u(X)X^n + v(X)h(X) = 1. \tag{2.1}$$

Set $e = e(a)$ where $e(X) = u(X)X^n$. If we multiply (2.1) by X^n and subsitute a for X we get

$$u(a)a^{2n} + v(a)h(a)a^n = a^n.$$

Since $h(a)a^n = 0$ we find $e(a)a^n = u(a)a^{2n} = a^n$ as required.

If we multiply (2.1) by $e(X)$ and substitute a for X we get

$$u(a)a^n e(a) + v(a)h(a)e(a) = e(a).$$

Since $h(a)e(a) = h(a)u(a)a^n = 0$ we get $e(a)^2 = e(a)$, hence $e^2 = e$.
Lastly, since $n \geq N$ we find that $e = u(a)a^n \in M$. $\triangle$

So we choose e and n accordingly. If $b \in A$ and $m \geq n$, then $ba^m = ba^{m-n}a^n = ba^{m-n}a^n e \in Ae \subset M$ and M is an MZ-space of A. $\square$

We have two corollaries from this theorem that are worth mentioning explicitly.

Corollary 2.2.6. *With notations as in Zhao's Theorem, if every element of $r(M)$ is algebraic over k, then M is an MZ-space of A if and only if for every $a \in r(M)$ there exists some $n \geq 1$ such that $Aa^n \in M$.*

Proof. The implication $\Leftarrow$: is clear, while the implication $\Rightarrow$: follows as in the last line of the proof of Zhao's Theorem. $\triangle$

Corollary 2.2.7. *Let A be commutative and suppose that all elements of $r(M)$ are algebraic over k. Then M is an MZ-space of A if and only if $r(M)$ is an ideal of A.*

Proof. $\Rightarrow$:) Let $a, b \in r(M)$. Then by Corollary 2.2.6 there exists n, m such that $Aa^n \subset M$ and $Ab^m \subset M$. Hence $A(a+b)^{n+m} \subset M$. It is also clear that for every $c \in A$ we have $A(ca)^n \subset Aa^n \subset M$. Hence $r(M)$ is an ideal.
$\Leftarrow$:) Let $e \in M$ be an idempotent. By Zhao's Theorem we need to show $Ae \subset M$. Write M_e for the set $\{a \in A \mid ae \in M\}$. Then we need to show that $A = M_e$. We only need to show $r(M_e) = A$ by the following claim.

> **Claim.** *Let M be an additive subset of A such that $1 \in M$. If $r(M)$ is additive, then $r(M) \subset M$. In particular if $r(M) = A$, then $M = A$.*
>
> *Proof.* Suppose that there exists some $a \in r(M)$ with $a \notin M$. Choose $r \geq 1$ such that $a^r \notin M$. and $a^{r+1}, a^{r+2}, \ldots \in M$. Then in particular $a^r \in r(M)$. Since $1 \in M$, we find $1 \in r(M)$. Hence $1 + a^r \in r(M)$. Hence there exists some N such that $(1 + a^r)^N \in M$ and $(1 + a^r)^{N+1} \in M$. Therefore $1 + Na^r \in M$ and $1 + (N+1)a^r \in M$. Then $a^r \in M$ by substracting these elements, a contradiction. Hence $r(M) \subset M$. $\triangle$

Let $b \in A$ be arbitrary, then since $e \in r(M)$ and $r(M)$ is an ideal, we find $be \in r(M)$. Hence for all large m we have $b^m e = (be)^m \in M$. But this means that $b \in r(M_e)$. Therefore $A \subset r(M_e)$. $\triangle$

Chapter 3

Duistermaat and Van der Kallen's Theorem

In this chapter we discuss the one-dimensional version of the theorem of Duistermaat and Van der Kallen and prove a generalized version of this theorem. In this chapter rings are commutative and have an identity.

3.1 Prerequisites from Commutative Algebra

The first two lemmas are for reference only, they are easy exercises for anyone learning basic algebra.

Lemma 3.1.1. *The only idempotents in a local ring R are $0, 1$.*

Proof. Suppose that $e \neq 0, 1$ is another idempotent of A. Then $e^2 = e$, hence $e(1-e) = 0$. Since $e \neq 0, 1$, we find that $e, 1-e$ are zero-divisors, hence not invertible. Then they are elements of the same unique maximal ideal $\mathfrak{m}$ of R, but then also $1 = (1-e) + e$ is an element of $\mathfrak{m}$, a contradiction to $\mathfrak{m}$ being maximal. △

Lemma 3.1.2. (Euclidean lemma) *In a ring R, if $\mathfrak{p}$ is a prime ideal and $\mathfrak{a}, \mathfrak{b}$ are ideals in R, then if $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, then $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.*

Proof. Suppose that $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ and $\mathfrak{a} \not\subset \mathfrak{p}$. Choose any $a \in \mathfrak{a}$ such that $a \notin \mathfrak{p}$. Let $b \in \mathfrak{b}$ be arbitrary. Then $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, we find that $b \in \mathfrak{p}$. Hence $\mathfrak{b} \subset \mathfrak{p}$. △

The Euclidean lemma can be used as another way of defining prime ideals. Suppose that $\mathfrak{p}$ is an ideal such that if $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, then $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$. Then consider any a, b such that $ab \in \mathfrak{p}$. Then $(a)(b) = (ab) \subset \mathfrak{p}$, hence $(a) \subset \mathfrak{p}$ or $(b) \subset \mathfrak{p}$. Therefore $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

The following proposition uses the Euclidean lemma and is essential in Commutative Algebra, this chapter ánd the following.

Proposition 3.1.3. *Let R be a ring and $\mathfrak{m}$ a maximal ideal of R. Then $R/\mathfrak{m}^k$ is a local ring for every $k \geq 1$.*

Proof. We know that ideals of $R/\mathfrak{m}^k$ are of the form $\mathfrak{a}/\mathfrak{m}^k$ with $\mathfrak{m}^k \subset \mathfrak{a}$. If we want maximal ideals in $R/\mathfrak{m}^k$ we need a maximal ideal $\mathfrak{a}$ in R with $\mathfrak{m}^k \subset \mathfrak{a}$. Since $\mathfrak{a}$ must be a prime ideal, we find by the Euclidean lemma that $\mathfrak{m} \subset \mathfrak{a}$ must hold, hence by maximality of $\mathfrak{m}$ we find $\mathfrak{m} = \mathfrak{a}$. Therefore, the only maximal ideal of $R/\mathfrak{m}^k$ is $\mathfrak{m}/\mathfrak{m}^k$ and hence $R/\mathfrak{m}^k$ is a local ring. □

Definition. Let R be a ring and A an R-algebra. An element $a \in A$ is called *algebraic over* R if there exists a non-zero univariate polynomial $f(X) \in R[X]$ such that $f(a) = 0$.

Lemma 3.1.4. *Let V be a finite field-extension over k. Then every element $a \in V$ is algebraic over k.*

Proof. Write $\dim_k V = n$. Let $a \in V$ be arbitrary. Then consider the set $\{a^i\}_{i=0}^n$, which is a set of $n+1$ elements. Hence there exists some linear dependence:

$$c_0 + c_1 a + \ldots + c_n a^n = 0$$

where there exists at least one $i \in \{0, \ldots, n\}$ for which $c_i \neq 0$. Then a is a root of the polynomial $f(X) = \sum_{i=0}^n c_i X^i \in k[X] \setminus \{0\}$. $\triangle$

Furthermore, we have the partial fractions decomposition of rational maps:

Theorem 3.1.5. (Partial Fractions Decomposition) *Let k be a field, $a_1, \ldots, a_n \in k$ disinct and $\alpha \in k^*$. Define $U(X) = \alpha(X - a_1) \cdots (X - a_n)$ and let $V(X) \in k[X]$ with $\deg_X V(X) < n$ be arbitrary. Then*

$$\frac{V(X)}{U(X)} = \sum_{i=1}^n \frac{A_i}{X - a_i}$$

with $A_i = \frac{V(a_i)}{U'(a_i)}$.

Proof. Note first that $U'(a_i) \neq 0$ for all $i = 1, \ldots, n$. This is since all a_i are distinct and we know that if both $U(a_i) = 0$ and $U'(a_i) = 0$, then a_i is a double root of U. Since this is not the case, and we know that $U(a_i) = 0$, we must have $U'(a_i) \neq 0$ for all $i = 1, \ldots, n$.

Then consider the set $\mathcal{V}_{U(X)} := \left\{ \frac{V(X)}{U(X)} \mid \deg V(X) < n \right\}$ as a subset of $k(X)$, the field of rational functions. Since $\deg V(X) < n$, we see that the set $\left\{ \frac{1}{U(X)}, \frac{X}{U(X)}, \ldots, \frac{X^{n-1}}{U(X)} \right\}$ spans $\mathcal{V}_{U(X)}$. It is clearly a k-linear subspace of $k(X)$. Indeed, the elements $\frac{1}{U(X)}, \frac{X}{U(X)}, \ldots, \frac{X^{n-1}}{U(X)}$ are k-linearly independent as well. Hence $\dim_k \mathcal{V}_{U(X)} = n$.

Now consider the elements $\frac{1}{X-a_1}, \ldots, \frac{1}{X-a_n}$. One easily verifies that they belong to $\mathcal{V}_{U(X)}$. We show that they are linearly independent, and hence form a basis. Therefore, suppose that there exist $\lambda_1, \ldots, \lambda_n \in k$ such that

$$\sum_{i=1}^n \frac{\lambda_i}{X - a_i} = 0.$$

Then also

$$\lambda_1 + \sum_{i=2}^n \frac{\lambda_i (X - a_1)}{X - a_i} = 0.$$

By substituting a_1 for X, we find $\lambda_1 = 0$. (Note that we nowhere divide by zero, as all a_i were distinct.) Then $\sum_{i=2}^n \frac{\lambda_i}{X-a_i} = 0$ and we repeat this procedure. We find that indeed $\frac{1}{X-a_1}, \ldots, \frac{1}{X-a_n}$ are linearly independent.

Since now these elements constitute a basis for $\mathcal{V}_{U(X)}$, given any $V(X)$ with $\deg V(X) < n$, we can write

$$\frac{V(X)}{U(X)} = \sum_{i=1}^n \frac{A_i}{X - a_i}$$

for some $A_1, \ldots, A_n \in k$. We now determine those A_i. By multiplying both sides with $(X - a_j)$ we get

$$\frac{V(X)}{U(X)} \cdot (X - a_j) = A_j + \sum_{i \neq j} \frac{A_i(X - a_j)}{X - a_i}.$$

Note that the $X - a_j$ cancels with the $X - a_j$ that occurs in $U(X)$. So we can substitute a_j for X and obtain

$$\frac{V(a_j)}{U'(a_j)} = A_j,$$

as required. Note that we used that $U'(a_j) = \alpha \prod_{i \neq j}(a_j - a_i)$. □

3.2 The Theorem of Duistermaat and Van der Kallen

In this section we state the Theorem of Duistermaat and Van der Kallen in one dimension. We shall prove a more general theorem later on, using a technique by Paul Monsky. Before we do that, we need to discuss some theorems, all of which are self-contained and needed for our proof, at the end, we shall state the Theorem of Duistermaat and Van der Kallen. The first necessary theorem is the Newton-Puiseux Theorem, which is well-covered in the literature, (see: [13], [14], [15]) hence we omit the proof.

Theorem 3.2.1. (Newton-Puiseux) *Let k be an algebraically closed field of characteristic zero and $f(X) = \sum_{i=0}^{n} a_i(t)X^i \in k((t))[X]$ with $n := \deg_X f(X) \geq 1$. Then there exists some $p \geq 1$ such that $f(X)$ splits completely in linear factors over $k((t^{1/p}))$.*

Next, we need a special ring for our proof:

Theorem 3.2.2. *Let k be a field and v a valuation on k such that k is complete with respect to v. Define $k[[X, X^{-1}]]$ to be the set of formal series $\sum_{n=-\infty}^{\infty} c_n X^n$ such that $\lim_{|n| \to \infty} c_n = 0$. Then $k[[X, X^{-1}]]$ can be made into a ring.*

Proof. We define addition point-wise, that is

$$\sum_{n=-\infty}^{\infty} a_n X^n + \sum_{n=-\infty}^{\infty} b_n X^n = \sum_{n=-\infty}^{\infty} (a_n + b_n) X^n.$$

For multiplication, we define it as we do for polynomials, i.e.,

$$\sum_{n=-\infty}^{\infty} a_n X^n \cdot \sum_{n=-\infty}^{\infty} b_n X^n = \sum_{n=-\infty}^{\infty} \left(\sum_{m=-\infty}^{\infty} a_m b_{n-m} \right) X^n.$$

We show that this multiplication is well-defined, i.e., that the product of two elements of $k[[X, X^{-1}]]$ is again an element of $k[[X, X^{-1}]]$. That $k[[X, X^{-1}]]$ is then a ring with these operations, is then straightforward.

Let $\sum_{n=-\infty}^{\infty} a_n X^n$ and $\sum_{n=-\infty}^{\infty} b_n X^n$ be elements of $k[[X, X^{-1}]]$. We define

$$c_{n,N} := \sum_{m=-N}^{N} a_m b_{n-m}$$

for all $n \in \mathbf{Z}$ and all $N \geq 1$.

Claim. *The sequence $c_{n,0}, c_{n,1}, c_{n,2}, \dots$ is a Cauchy sequence in k for every $n \in \mathbf{Z}$.*

Proof. Since $\lim_{|n|\to\infty} a_n = 0 = \lim_{|n|\to\infty} b_n$, there exists some $C > 0$ such that $|a_n|, |b_n| < C$ for all $n \in \mathbf{Z}$.

Let $\varepsilon > 0$ be arbitrary. Then there exists some $M > 0$ such that $|a_m| \leq C^{-1}\varepsilon$ and $|b_m| \leq C^{-1}\varepsilon$ if $|m| \geq \frac{1}{2}M$. (*)

Furthermore, let $p \geq q \geq M$. Then

$$c_{n,p} - c_{n,q} = \sum_{m=-p}^{-(q+1)} a_m b_{n-m} + \sum_{m=q+1}^{p} a_m b_{n-m}.$$

Since now $|m| \geq q \geq M \geq \frac{1}{2}M$, we have $|a_m| \leq C^{-1}\varepsilon$. Hence $|a_m b_{n-m}| \leq C^{-1}\varepsilon \cdot C = \varepsilon$. Indeed, $|c_{n,p} - c_{n,q}| \leq \varepsilon$, hence $(c_{n,j})_{j=0}^{\infty}$ is a Cauchy sequence. △

Now, since k is complete, we find that $(c_{n,j})_{j=0}^{\infty}$ converges. Write $c_n := \lim_{N\to\infty} c_{n,N}$. Notice that

$$c_n = \sum_{m=-\infty}^{\infty} a_m b_{n-m}.$$

All that we need now, is to show that $\lim_{|n|\to\infty} c_n = 0$.

Proof. With notations as above, let $|n| \geq M$. Consider $c_{n,N}$ as above, with $N \geq 1$. Since $n = m + (n - m)$, we find that $|m| \geq \frac{1}{2}M$ or $|n - m| \geq \frac{1}{2}M$. Hence

$$|a_m b_{n-m}| \leq C^{-1}\varepsilon \cdot C = \varepsilon.$$

Here we use (*). So $|c_{n,N}| \leq \varepsilon$ for every $N \geq 1$.

Then $|\lim_{N\uparrow\infty} c_{n,N}| \leq \varepsilon$, i.e., $|c_n| \leq \varepsilon$, as required. △

Hence multiplication is well-defined and $k[[X, X^{-1}]]$ is indeed a ring. □

Proposition 3.2.3. *Let $k = \mathbf{C}((z^{1/p}))$ and v the valuation of k such that $v(z^{1/p}) = 1/p$. Then $\mathbf{C}[X, X^{-1}][[z]]$ is a subring of $k[[X, X^{-1}]]$.*

Proof. Note that $\mathbf{C}((z^{1/p}))$ is complete with respect to v, one could write $z^{1/p} = t$, then $k = \mathbf{C}((t))$ and $v(t) = 1$. Hence $k[[X, X^{-1}]]$ is defined.

Let $f(z) = a_0(X) + a_1(X)z + a_2(X)z^2 + \dots$ be an arbitrary element of $\mathbf{C}[X, X^{-1}][[z]]$ and let $\varepsilon > 0$ be arbitrary. Write this element $f(z)$ as $\sum_{n=-\infty}^{\infty} c_n X^n$.

We want to determine N such that $|c_n| = 2^{v(c_n)} < \varepsilon$ for all $|n| \geq N$. This is equivalent to determining N such that $v(c_n) > \log_2(\varepsilon)$.

Write $N(\varepsilon) := \lceil \log_2(\varepsilon) \rceil$. Then determine $N := \max_{0 \leq i \leq N(\varepsilon)} \{\deg a_i(X), \deg a_i(X^{-1})\}$. Then clearly, for all c_n with $|n| \geq N$ we have $v(c_n) > \log_2(\varepsilon)$. Hence $|c_n| < \varepsilon$.

Hence indeed, $f(z) \in k[[X, X^{-1}]]$, as required. □

For completeness, we also state the higher-dimension theorem of Duistermaat and Van der Kallen here, a proof can be found in [5].

Theorem. (Duistermaat-VanderKallen) *Let $X_1, \dots, X_n$ be n commutative variables and let M be the subspace of the Laurent polynomial algebra $\mathbf{C}[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}]$ consisting of those Laurent polynomials with no constant term. Then M is an MZ-space of $\mathbf{C}[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}]$.*

We now state Duistermaat Van der Kallen in dimension one. Which is just taking $n = 1$:

Theorem 3.2.4. (Duistermaat-VanderKallen) *The set*

$$\{f \in \mathbf{C}[X, X^{-1}] \mid f_0 = 0\}$$

is an MZ-space of $\mathbf{C}[X, X^{-1}]$.

We omit the proof, as we prove a more general theorem in the next section, see 3.3.2.

3.3 Kernels of linear maps: A generalisation of Duistermaat - Van der Kallen in dimension one

In this section we will discuss a generalisation of Duistermaat-Van der Kallen. Note that

$$\varphi \colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}, f \mapsto f_0$$

is a linear map of $\mathbf{C}$-vector spaces.
We now take an arbitrary $\mathbf{C}$-linear map, $L \colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ or $L \colon \mathbf{C}[X] \to \mathbf{C}$.

Remark. 1. *If L is injective, i.e., $\operatorname{Ker} L = 0$, then $\operatorname{Ker} L$ is an MZ-space.*

2. *If $L = 0$, i.e., the trivial linear map, then $\operatorname{Ker} L = \mathbf{C}[X, X^{-1}]$ (or indeed $\operatorname{Ker} L = \mathbf{C}[X]$), an MZ-space.*

We may assume that linear maps we consider are no longer injective or trivial. So from now on, when we write L is a linear map, we mean a non-trivial non-injective linear map. If we use linear maps in a more general way, we will write: *possibly trivial* linear map, or *possibly injective* linear map.

Lemma 3.3.1. *Let $L \colon \mathbf{C}[X] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X^n) = 0$ for all $n \in \mathbf{Z}_{\geq N}$. Then $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X]$ if and only if $L(1) \neq 0$.*

Proof. $\Rightarrow$:) Suppose that $L(1) = 0$, then $1 \in \operatorname{Ker} L$. Since $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X]$, we find that $\operatorname{Ker} L = \mathbf{C}[X]$, i.e., $L = 0$, a contradiction. So $L(1) \neq 0$.
$\Leftarrow$:) Note that $L(X^N) = 0$. So for any $f = \sum_{i=0}^n a_i X^i$ we have

$$L(fX^N) = L\left(\sum_{i=0}^n a_i X^{i+N}\right) = \sum_{i=0}^n a_i L(X^{i+N}) = 0,$$

hence $(X^N) \subset \operatorname{Ker} L$. Then by Corollary 2.2.4 it suffices to show that $\operatorname{Ker} L/(X^N)$ is an MZ-space of $\mathbf{C}[X]/(X^N)$. We will also use Zhao's Theorem. We therefore need to show that all elements in $r(\operatorname{Ker} L/(X^N))$ are algebraic over $\mathbf{C}$ and that $\mathbf{C}[X]/(X^N)e \subset \operatorname{Ker} L/(X^N)$ for all idempotents e in $\operatorname{Ker} L/(X^N)$.
Note first that $\operatorname{Ker} L/(X^N) \subset \mathbf{C}[X]/(X^N)$, hence any idempotent of $\operatorname{Ker} L/(X^N)$ is an idempotent of $\mathbf{C}[X]/(X^N)$. We start by determining the idempotents of $\mathbf{C}[X]/(X^N)$. Since $(X) \subset \mathbf{C}[X]$ is a maximal

ideal, we find that $\mathbf{C}[X]/(X^N)$ is a local ring, by Proposition 3.1.3. A local ring has only idempotents $0, 1$ by Lemma 3.1.1. Since $L(1) \neq 0$, we see that 0 is the only idempotent in $\operatorname{Ker} L/(X^N)$, and we trivially have $0 \subset \operatorname{Ker} L/(X^N)$.

Hence it remains to show that every element in $r(\operatorname{Ker} L/(X^N))$ is algebraic over $\mathbf{C}$. Note that

$$r(\operatorname{Ker} L/(X^N)) \subset \mathbf{C}[X]/(X^N),$$

and every element of $\mathbf{C}[X]/(X^N)$ is algebraic over $\mathbf{C}$ due to its dimension being finite and Lemma 3.1.4.

Since we now satisfy the hypotheses of Zhao's Theorem, we find that $\operatorname{Ker} L/(X^N)$ is an MZ-space of $\mathbf{C}[X]/(X^N)$ and hence $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X]$. △

Note that the above lemma can be generalized to an arbitrary field k, with identical proof.

Theorem 3.3.2. *Let $L\colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X^n) = 0$ for all $n \in \mathbf{Z}_{\geq N}$ and all $n \in \mathbf{Z}_{\leq -N}$. Then $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X, X^{-1}]$ if and only if $L(1) \neq 0$.*

The proof of this theorem relies on the following lemmas.

Lemma 3.3.3. *Let $L\colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X^n) = 0$ for all $n \in \mathbf{Z}_{\geq N}$ and all $n \in \mathbf{Z}_{\leq -N}$. If $L(1) \neq 0$ and $f \in r'(\operatorname{Ker} L)$, then $f \in \mathbf{C}[X]$ or $f \in \mathbf{C}[X^{-1}]$.*

Proof. Suppose $f \notin \mathbf{C}[X]$ and $f \notin \mathbf{C}[X^{-1}]$, i.e. $f = \alpha X^{-s} + \ldots + \beta X^r$ with $\alpha, \beta \neq 0$ and $s, r \geq 1$. Then consider the power series

$$W(z) = \sum_{j=0}^{\infty} L(f^j) z^j.$$

We will show that $W(z) \neq 1$. That is, $L(f^m) \neq 0$ for some $m \geq 1$. This contradicts $f \in r'(\operatorname{Ker} L)$.

Write $U(X) = X^s(1 - zf(X)) \in \mathbf{C}(z)[X] \subset \mathbf{C}((z))[X]$ and $n := r + s$. Then by the Newton-Puiseux Theorem (see Theorem 3.2.1) there exists some $p \geq 1$ such that

$$U(X) = (-\beta z)(X - a_1) \cdots (X - a_n), \text{ with all } a_i \in \mathbf{C}((z^{\frac{1}{p}})).$$

Write $k := \mathbf{C}((z^{\frac{1}{p}}))$. There we have the valuation ν defined by $\nu(z^{\frac{1}{p}}) = \frac{1}{p}$ and k is complete with respect to this valuation. Furthermore $k[[X, X^{-1}]]$ is a ring, by Theorem 3.2.2. Extend L to $k[[X, X^{-1}]]$ as

$$L\colon k[[X, X^{-1}]] \to k$$

by

$$L\left(\sum_{n=-\infty}^{\infty} c_n X^n\right) = \sum_{n=-(N-1)}^{N-1} c_n L(X^n).$$

Since $\mathbf{C}[X, X^{-1}][[z]]$ is a subring of $k[[X, X^{-1}]]$ (see Proposition 3.2.3), we have

$$\sum_{m \geq 0} f^m z^m \in k[[X, X^{-1}]].$$

Then $1 - zf$ is invertible in $k[[X, X^{-1}]]$ and so is $U(X)$. Write

$$W(z) = L\left(\frac{1}{1 - zf}\right) = L\left(\frac{X^s}{U(X)}\right).$$

We will now use the partial fractions decomposition of $X^s/U(X)$. Therefore, note that since we have $(-1)^n a_1 \cdots a_n = \alpha/\beta$, we find that $a_i \neq 0$ for all $i = 1, \ldots, n$. From $U(a_i) = 0$ we find then that $f(a_i) = 1/z$ for all $i = 1, \ldots, n$.

So $f'(a_i)a_i' = -z^{-2}$. Also $U'(X) = sX^{s-1}(1 - zf(X)) + x^s(-z)f'(X)$ and $U'(a_i) = -za_i^s f'(a_i) \neq 0$. Hence all a_i are distinct. Then by Theorem 3.1.5 we get a partial fractions decomposition of the form

$$\frac{X^s}{U(X)} = \sum_{i=1}^{n} \frac{A_i}{X - a_i}$$

with $A_i = \frac{a_i^s}{U'(a_i)} = -\frac{1}{zf'(a_i)}$. Therefore

$$\frac{1}{1 - zf(X)} = \frac{X^s}{U(X)} = \sum_{i=1}^{n} -\frac{1}{zf'(a_i)(X - a_i)}. \tag{3.1}$$

We now compute the inverse of each factor $X - a_i$ in $k[[X, X^{-1}]]$. Observe that $f(a_i) = 1/z$ implies that $\nu(a_i) \neq 0$. Then $\nu(a_i) > 0$ or $\nu(a_i) < 0$.

If $\nu(a_i) > 0$, then we have

$$(X - a_i)^{-1} = X^{-1}(1 - a_i X^{-1})^{-1} = X^{-1} \sum_{m=0}^{\infty} a_i^m X^{-m} \in k[[X, X^{-1}]]$$

while if $\nu(a_i) < 0$, then

$$(X - a_i)^{-1} = -a_i^{-1}(1 - a_i^{-1}X)^{-1} = -a_i^{-1} \sum_{m=0}^{\infty} (a_i^{-1}X)^m \in k[[X, X^{-1}]].$$

So we find that

$$\begin{aligned} \frac{1}{1 - zf(X)} &= -\left(\sum_{i \in S^+} \frac{1}{zf'(a_i)(X - a_i)} + \sum_{i \in S^-} \frac{1}{zf'(a_i)(X - a_i)}\right) \\ &= -\left(\sum_{i \in S^+} \left(\frac{1}{zf'(a_i)}\right)\left(\sum_{m=0}^{\infty} a_i^m X^{-m}\right) X^{-1} - \sum_{i \in S^-} \left(\frac{1}{zf'(a_i)}\right)\left(\sum_{m=0}^{\infty} (a_i^{-1}X)^m\right) a_i^{-1}\right) \end{aligned}$$

where $S^+ = \{i \mid v(a_i) > 0\}$ en $S^- = \{i \mid v(a_i) < 0\}$.

Then

$$\begin{aligned} W(z) &= L\left(\frac{1}{1 - zf(X)}\right) \\ &= L\left(-\sum_{i \in S^+} \left(\frac{1}{zf'(a_i)}\right)\left(\sum_{m=0}^{\infty} a_i^m X^{-m}\right) X^{-1}\right) + L\left(\sum_{i \in S^-} \left(\frac{1}{zf'(a_i)}\right)\left(\sum_{m=0}^{\infty} (a_i^{-1}X)^m\right) a_i^{-1}\right) \end{aligned}$$

$$= -\sum_{i\in S^+} \frac{1}{zf'(a_i)} L\left(X^{-1}\sum_{m=0}^{\infty} a_i^m X^{-m}\right) + \sum_{i\in S^-} \frac{1}{zf'(a_i)} L\left(a_i^{-1}\sum_{m=0}^{\infty}(a_i^{-1}X)^m\right)$$

$$= -\sum_{i\in S^+} \frac{1}{zf'(a_i)} \sum_{m=0}^{N-1} a_i^m L(X^{-(m+1)}) + \sum_{i\in S^-} \frac{1}{zf'(a_i)} \sum_{m=0}^{N-1} a_i^{-(m+1)} L(X^m)$$

Since $f'(a_i)a_i' = -z^{-2}$ we have

$$W(z) = \sum_{i\in S^+}\sum_{m=0}^{N-1} za_i'a_i^m L(X^{-(m+1)}) - \sum_{i\in S^-}\sum_{m=0}^{N-1} za_i'a_i^{-(m+1)} L(X^m)$$

We want to show $W(z) \neq 1$, i.e. we need to show that

$$\sum_{i\in S^+}\sum_{m=0}^{N-1} a_i'a_i^m L(X^{-(m+1)}) - \sum_{i\in S^-}\sum_{m=0}^{N-1} a_i'a_i^{-(m+1)} L(X^m) \neq \frac{1}{z} \tag{3.2}$$

To prove this inequality, we study the a_i at infinity, i.e. we set $t = \frac{1}{z}$. Now fix an i. Then $f(a_i) = t$. Since $\mathbf{C}(z) = \mathbf{C}(t)$ we find that a_i is algebraic over $\mathbf{C}(t)$ and hence also over $\mathbf{C}((t))$. Then again by the Newton-Puiseux theorem we can regard a_i inside $\mathbf{C}((t^{\frac{1}{p}}))$ for some $p \geq 1$. Since $a_i \neq 0$ we can write $a_i = \sum_{n=m}^{\infty} c_n t^{n/p}$ for some $c_i \in \mathbf{C}$ with $c_m \neq 0$. Write w for the valuation on $\mathbf{C}((t^{1/p}))$ defined by $w(t^{1/p}) = 1/p$. Then $w(a_i) = m/p$.

Suppose that $w(a_i) > 0$, then $w(f(a_i)) = w(\alpha c_m^{-s} t^{-ms/p}) = -ms/p = -sw(a_i) < 0$ since $s \geq 1$. But since $f(a_i) = t$ we also have $w(f(a_i)) = w(t) = 1$, a contradiction.

Similarly, if $w(a_i) < 0$, then $w(f(a_i)) = w(c_m^r t^{mr/p}) = mr/p = w(a_i)r < 0$, a contradiction.

Hence $w(a_i) = 0$ and $a_i = \sum_{n=0}^{\infty} c_n t^{n/p}$ with $c_0 \in \mathbf{C}^*$.

Note that $t = \frac{1}{z}$, and $w(t) = 1$. So if we show that $w(a_i'a_i^m) > 1$ for all $m \in \mathbf{Z}$ we have shown our inequality 3.2, and hence that $W(z) \neq 1$. Note that since $f(a_i) = t$ we have $a_i \notin \mathbf{C}$. Hence there exists some $j > 0$ with $c_j \neq 0$. Choose such j minimal and write $a_i = c_0 + c_j t^{j/p} + R$ with $w(R) > j/p$. Then $w\left(\frac{da_i}{dt}\right) = \frac{j}{p} - 1$.

Also $\frac{a_i'(z)}{a_i(z)} = -\frac{\frac{da_i}{dt}}{a_i}t^2$ and $w(a_i) = 0$, therefore we have

$$w(a_i'a_i^m) = w(-\frac{da_i}{dt}t^2 a_i^m) = \frac{j}{p} - 1 + 2 > 1,$$

which concludes the proof. △

Lemma 3.3.4. *Let $L\colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X^n) = 0$ for all $n \in \mathbf{Z}_{\geq N}$ and all $n \in \mathbf{Z}_{\leq -N}$. If $L(1) \neq 0$ and $f \in \mathbf{C}[X] \cap r(\operatorname{Ker} L)$, then $f \in X\mathbf{C}[X]$.*

Proof. Let $f \in \mathbf{C}[X] \cap r(\operatorname{Ker} L)$, then $f \in r(\operatorname{Ker} L_{|\mathbf{C}[X]})$. By Corollary 2.2.7 and Lemma 3.3.1 we know that $r(\operatorname{Ker} L_{|\mathbf{C}[X]})$ is an ideal of $\mathbf{C}[X]$. Since $L(1) \neq 0$ we find that $\operatorname{Ker} L_{|\mathbf{C}[X]} \neq \mathbf{C}[X]$, and hence $r(\operatorname{Ker} L_{|\mathbf{C}[X]}) \neq \mathbf{C}[X]$. As $r(\operatorname{Ker} L_{|\mathbf{C}[X]})$ is a principal ideal ($\mathbf{C}[X]$ is Euclidean), it is generated by some monic $g \in \mathbf{C}[X] \setminus \mathbf{C}$. Since it is clear that $X \in r(\operatorname{Ker} L_{|\mathbf{C}[X]})$ we find $(X) \subset r(\operatorname{Ker} L_{|\mathbf{C}[X]})$. Hence X is a multiple of this g. Hence $g = X$. So $r(\operatorname{Ker} L_{|\mathbf{C}[X]}) = (X)$ and $f \in (X) = X\mathbf{C}[X]$. △

We will use the following definition(s):

Definition 3.3.5. *For $f \in \mathbf{C}[X, X^{-1}] \setminus \{0\}$ we have the following quantities:*

$$\deg_+ f = \max\{i : f_i \neq 0\}$$

and

$$\deg_- f = \min\{i : f_i \neq 0\}.$$

Examples 3.3.6. *1. If $f = X^{-2} + 1 + X$, then $\deg_+ f = 1$ and $\deg_- f = -2$.*

2. If $g = X$, then $\deg_+ g = 1$ and $\deg_- g = 1$.

3. If $h = 1 + X + X^3$, then $\deg_+ h = 3$ and $\deg_- h = 0$.

Remark that we have $\deg_+(fg) = \deg_+ f + \deg_+ g$ and $\deg_-(fg) = \deg_- f + \deg_- g$. Also, note that if $\deg_- g \geq 0$, then $g \in \mathbf{C}[X]$ and if $\deg_+ g \leq 0$, then $g \in \mathbf{C}[X^{-1}]$. We always have $\deg_- g \leq \deg_+ g$.

Proof. (of Theorem 3.3.2) $\Rightarrow$:) Suppose that $L(1) = 0$, then $1 \in \operatorname{Ker} L$. Since $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X, X^{-1}]$, we find that $\operatorname{Ker} L = \mathbf{C}[X, X^{-1}]$, i.e., $L = 0$, a contradiction. So $L(1) \neq 0$.
$\Leftarrow$:) Suppose that $L(1) \neq 0$ and $f \in r(\operatorname{Ker} L)$. We want to show that $gf^m \in \operatorname{Ker} L$ for all $m \gg 0$. If $f \in r(\operatorname{Ker} L)$, then by Lemma 3.3.3 we find that $f \in \mathbf{C}[X]$ or $f \in \mathbf{C}[X^{-1}]$.
Assume that $f \in \mathbf{C}[X]$, the argument is similar when $f \in \mathbf{C}[X^{-1}]$. Then $f \in \mathbf{C}[X] \cap r(\operatorname{Ker} L)$. By Lemma 3.3.4 we then find $f \in X\mathbf{C}[X]$. Hence $L(f^m) = 0$ for all $m \geq N$.
Then $L(gf^m) = 0$ for all $m \geq N - \deg_- g$. □

Theorem 3.3.2 is false in characteristic $p > 0$ as we see in this counterexample taken from [17].

Counterexample 3.3.7. *Let $k = \mathbb{F}_p$ be the base field of characteristic $p > 0$ and $f = X^{-1} + X^{p-1} \in \mathbb{F}_p[X, X^{-1}]$. Define $L\colon \mathbb{F}_p[X, X^{-1}] \to \mathbb{F}_p$ by $L(f) = f_0$, being the constant coefficient of f. Then $L(f^m) = 0$ for all $m \geq 1$, while $L(X^{-1} f^m) = (-1)^m$ for all m of the form $p^n - 1$ with $n \geq 1$. In particular*

$$\{f \in \mathbb{F}_p[X, X^{-1}] \mid L(f) = 0\} \text{ is not an MZ-space of } \mathbb{F}_p[X, X^{-1}].$$

Proof. Let $m \geq 1$. Then $L(f^m)$ is the sum of all $\binom{m}{i}$ with $0 \leq i \leq m$ such that $-(m - i) + i(p - 1) = 0$. Solving this equation for i (in terms of m, p) yields $i = m/p$ when p divides m. So when p does not divide m, we find that $L(f^m) = 0$. If p does divide m, we find that $L(f^m) = \binom{m}{i}$ with $i = m/p$, hence $L(f^m) = \binom{ip}{i}$. We will show that $\binom{ip}{i} = 0$ for all $i \geq 1$.

> **Claim.** *We have $\binom{ip}{i} = 0$ for all $i \geq 1$ in $\mathbb{F}_p$.*
>
> *Proof.* Write $i = p^r n$ with $r \geq 0$ such that $p^{r+1} \nmid i$. Note that the coefficient of X^i in $(X+1)^{ip}$ in $\mathbb{F}_p[X]$ equals $\binom{ip}{i}$. We also have
>
> $$(X + 1)^{ip} = (X + 1)^{p^{r+1} n} = (X^{p^{r+1}} + 1)^n.$$
>
> If $\binom{ip}{i} \neq 0$, then X^i appears in $(X + 1)^{ip}$ with a nonzero coefficient. Hence it also appears in $(X^{p^{r+1}} + 1)^n$ with a nonzero coefficient. But then i is of the form $p^{r+1} j$ for some $1 \leq j \leq n$, a contradiction to $p^{r+1} \nmid i$. Hence $\binom{ip}{i} = 0$. △

Hence $L(f^m) = 0$ for all $m \geq 1$.

Now let $n \geq 1$ and $m = p^n - 1$. We are concerned with $L(X^{-1}f^m)$, so interested in the coefficient of X in f^m. Note that this is again the sum of all $\binom{m}{i}$ where $0 \leq i \leq m$ such that $-(m-i) + i(p-1) = 1$. Solving this for i in terms of m, p we get $i = (1+m)/p = p^{n-1}$. So the coefficient of X in f^m is equal to $\binom{m}{i}$ with $i = p^{n-1}$. We show that $\binom{m}{i} = (-1)^i$ for all $0 \leq i \leq m$.

> **Claim.** *When $m = p^n - 1$ for some $n \geq 1$, we have $\binom{m}{i} = (-1)^i$ for all $0 \leq i \leq m$ in $\mathbb{F}_p$.*
>
> *Proof.* If we use Newton's binomial formula, we find that $(1-X)^m = \sum_{i=0}^{m}(-1)^i\binom{m}{i}X^i$. However, since $m = p^n - 1$, in $\mathbb{F}_p[X]$ we also have
>
> $$(1-X)^m = (1-X)^{p^n-1} = \frac{(1-X)^{p^n}}{1-X} = \frac{1-X^{p^n}}{1-X} = \sum_{i=0}^{p^n-1} X^i = \sum_{i=0}^{m} X^i.$$
>
> If we compare coefficients, we find that $(-1)^i\binom{m}{i} = 1$ for all $i = 0, \ldots, m$, hence $\binom{m}{i} = (-1)^i$ for all $i = 0, \ldots, m$. △

Hence the coefficient of X in f^m is equal to $(-1)^{p^{n-1}} \neq 0$ and $L(X^{-1}f^m) \neq 0$ for all $m \geq 1$ of the form p^{n-1}.

Combining these two results shows that indeed $\{f \in \mathbb{F}_p[X, X^{-1}] \mid L(f) = 0\}$ is *not* an MZ-space of $\mathbb{F}_p[X, X^{-1}]$. □

3.4 Encore : Generalizations

In this section we discuss generalizations of various theorems we have seen in this chapter. The first is a generalization of Lemma 3.3.1.

Lemma 3.4.1. (Generalization of Lemma 3.3.1) *Let $L\colon \mathbf{C}[X_1, \ldots, X_n] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $(X_1, \ldots, X_n)^l \subset \operatorname{Ker} L$ for all $l \geq N$. Then $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X_1, \ldots, X_n]$ if and only if $L(1) \neq 0$.*

Proof. $\Rightarrow$:) Suppose that $L(1) = 0$, then $1 \in \operatorname{Ker} L$. Since $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X]$, we find that $\operatorname{Ker} L = \mathbf{C}[X]$, i.e., $L = 0$, a contradiction. So $L(1) \neq 0$.

$\Leftarrow$:) Suppose that $L(1) \neq 0$. Note that by hypothesis $(X_1, \ldots, X_n)^N \subset \operatorname{Ker} L$. Then by Corollary 2.2.4 it suffices to show that $\operatorname{Ker} L/(X_1, \ldots, X_n)^N$ is an MZ-space of $\mathbf{C}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^N$.

Note that every element in $r(\operatorname{Ker} L/(X_1, \ldots, X_n)^N)$ is also an element of $\mathbf{C}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^N$, a finite-dimensional $\mathbf{C}$-vector space, hence algebraic over $\mathbf{C}$. (See Lemma 3.1.4.)

To apply Zhao's Theorem we need to determine the idempotents in $\operatorname{Ker} L/(X_1, \ldots, X_n)^N$. Note that $\mathbf{C}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^N$ is a local ring, as $(X_1, \ldots, X_n)$ is a maximal ideal of $\mathbf{C}[X_1, \ldots, X_n]$. Hence its only idempotents are $0, 1$. (See Proposition 3.1.3 and Lemma 3.1.1.) Since $L(1) \neq 0$, we find that 0 is the only idempotent of $\operatorname{Ker} L/(X_1, \ldots, X_n)^N$.

Hence the requirements of Zhao's Theorem are trivially satisfied.

Thus we find that $\operatorname{Ker} L/(X_1, \ldots, X_n)^N$ is an MZ-space of $\mathbf{C}[X_1, \ldots, X_n]$. △

What we can't do is prove

Let $L\colon \mathbf{C}[X_1,\ldots,X_n] \to \mathbf{C}$ be a $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X_i^m) = 0$ for all $m \in \mathbf{Z}_{\geq N}$. Then $\operatorname{Ker} L$ is an MZ-space of $\mathbf{C}[X_1,\ldots,X_n]$ if and only if $L(1) \neq 0$.

For this we have the following counterexample:

Counterexample 3.4.2. *Take $n = 2$ and $N = 2$ in the following form. Let $L\colon \mathbf{C}[X_1, X_2] \to \mathbf{C}$ be the $\mathbf{C}$-linear map given by*

$$L(X_1^iX_2^j) = \begin{cases} 1 & \text{if } i = 1 \text{ or } i = j = 0 \\ 0 & \text{else} \end{cases}$$

Then we have $L(1) = 1$, and $L(X_i^m) = 0$ for all $m \geq 2$. It is then clear that $X_2 \in r(\operatorname{Ker} L)$ by construction, but $X_1X_2^m \notin \operatorname{Ker} L$ for all $m \geq 1$. Therefore $\operatorname{Ker} L$ is not an MZ-space.

While it is technically not a generalization, we also have the following lemma, which uses the same method-of-proof:

Lemma 3.4.3. *Let k be a field, A a* finite-dimensional *k-algebra and $\mathfrak{m}$ a maximal ideal of A. Let $L\colon A \to k$ be a k-linear map for which there exists an $N \geq 1$ such that $\mathfrak{m}^l \subset \operatorname{Ker} L$ for all $l \geq N$. Then $\operatorname{Ker} L$ is an MZ-space of A if and only if $L(1) \neq 0$.*

Proof. $\Rightarrow$:) The proof of this is obvious.
$\Leftarrow$:) Again, we apply Zhao's Theorem. Since A is finite-dimensional as a k-algebra, then so is $A/\mathfrak{m}^l$. Hence every element in $r(\operatorname{Ker} L/\mathfrak{m}^l)$ is algebraic by Lemma 3.1.4. Since $A/\mathfrak{m}^l$ is a local ring, we only have idempotents $0, 1$. So the hypotheses of Zhao are easily satisfied. △

The crucial part here is that there are examples of k-algebras with maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m}^l$ is not finite-dimensional, and not every element of $A/\mathfrak{m}^l$ is algebraic:

Example 3.4.4. *Let $k = \mathbf{C}$ and $A = \mathbf{C}(X)$. Then its only maximal ideal is $\mathfrak{m} = (0)$, as it is a field. Then $A/\mathfrak{m}^l = \mathbf{C}(X)$ for all $l \geq 1$, while X is clearly transcendental over $\mathbf{C}$.*

3.4.1 Generalized Zhao Theorem

In this section we discuss a generalization of Zhao's Theorem (Theorem 2.2.5).

Definition 3.4.5. *Let R be a commutative ring, S a multiplicatively closed subset of R and A an R-algebra. An R-submodule M of A is called S-*saturated *if we have $a \in M$ for all $a \in A$ for which there exists some $s \in S$ such that $sa \in M$, i.e.,*

$$\{a \in A \mid \exists s \in S[sa \in M]\} \subset M.$$

Example 3.4.6. *Let A be a domain, d a natural number and $S = A \setminus \{0\}$. Let $\mathcal{L}\colon A[X] \to A^d$ be an A-linear map. Then $\operatorname{Ker} \mathcal{L}$ is S-saturated.*

Proof. Let $s \in A \setminus \{0\}$ and $a \in A[X]$ be arbitrary. We then have the following equivalent statements:

$$\begin{gathered} sa \in \operatorname{Ker} \mathcal{L} \\ \mathcal{L}(sa) = 0 \\ s\mathcal{L}(a) = 0 \end{gathered}$$

$$\mathcal{L}(a) = 0$$
$$a \in \operatorname{Ker} \mathcal{L}$$

In particular we have $sa \in \operatorname{Ker} \mathcal{L} \implies a \in \operatorname{Ker} \mathcal{L}$. Hence $\operatorname{Ker} \mathcal{L}$ is S-saturated. $\triangle$

Proposition 3.4.7. *Let R be a commutative ring, S a multiplicatively closed subset of R and A an R-algebra. Let M be an S-saturated R-submodule of A. Then*

(i) $S^{-1}r(M) = r(S^{-1}M)$;

(ii) $S^{-1}sr(M) = sr(S^{-1}M)$;

(iii) M is an MZ-space of A if and only if $S^{-1}M$ is an MZ-space of $S^{-1}A$.

Proof. (i) Let $x \in S^{-1}r(M)$ be arbitrary. Then x is of the form $\frac{\mu}{s}$ with $s \in S$ and $\mu \in r(M)$. Therefore μ is such that $\mu^m \in M$ for all $m \gg 0$. Choose $N \geq 0$ such that $\mu^n \in M$ for all $n \geq N$. Then since $x^n = \frac{\mu^n}{s^n}$ and $s^n \in S$ for all $n \geq 1$ we find that $x^n \in S^{-1}M$ for all $n \geq N$, hence $x \in r(S^{-1}M)$.

Conversely, let $\frac{b}{s} \in r(S^{-1}M)$ be arbitrary. Then $\frac{b^m}{s^m} \in S^{-1}M$ for all $m \gg 0$. Let $N \geq 0$ be such that $\frac{b^n}{s^n} \in S^{-1}M$ for all $n \geq N$. Then we have $\frac{b^n}{s^n} = \frac{\mu_n}{t_n}$ with $\mu_n \in M$ and $t_n \in S$. Then for every $n \geq N$ there exists $u_n \in S$ such that $u_n(t_n b^n - s^n \mu_n) = 0$. Hence $u_n t_n b^n \in M$. Since M is S-saturated, it follows that $b^n \in M$ for all $n \geq N$. Hence $b \in r(M)$ and $\frac{b}{s} \in S^{-1}r(M)$.

(ii) Let $x \in S^{-1}sr(M)$, then $x = \frac{\mu}{s}$ for some $\mu \in sr(M)$ and some $s \in S$. We need to show that $x \in sr(S^{-1}M)$, i.e., that $ax^m \in S^{-1}M$ for all $a \in S^{-1}A$ and all $m \gg 0$.

Therefore, let $a \in S^{-1}A$ be arbitrary. Then $a = \frac{c}{t}$ for some $c \in A$ and $t \in S$. Let $N \geq 0$ be such that $c\mu^n \in M$ for all $n \geq N$. (Since $\mu \in sr(M)$.) Then $ax^n = \frac{c}{t}\left(\frac{\mu}{s}\right)^n = \frac{c\mu^n}{ts^n} \in S^{-1}M$ for all $n \geq N$ since $ts^n \in S$. Hence, since $a \in S^{-1}A$ was arbitrary, we find that $x \in sr(S^{-1}M)$.

Conversely, let $\frac{a}{s} \in sr(S^{-1}M)$ be arbitrary. Let $b \in A$ be arbitrary and $N \geq 0$ such that $\frac{b}{1}\frac{a^n}{s^n} \in S^{-1}M$ for all $n \geq N$. That means that for every $n \geq N$ there exist $\mu_n \in M$ and $t_n \in S$ such that $\frac{b}{1}\frac{a^n}{s^n} = \frac{\mu_n}{t_n}$. Hence there exists some $u_n \in S$ such that $u_n(t_n ba^n - s^n \mu_n) = 0$. Hence $u_n t_n ba^n \in M$. Since M is S-saturated, we find $ba^n \in M$ for all $n \geq N$. Hence $a \in sr(M)$ and $\frac{a}{s} \in S^{-1}sr(M)$.

(iii) Let M be an MZ-space of A. That means that $r(M) = sr(M)$. Hence $r(S^{-1}M) = S^{-1}r(M) = S^{-1}sr(M) = sr(S^{-1}M)$ by (i) and (ii) and $S^{-1}M$ is an MZ-space of $S^{-1}A$.

Conversely, let $S^{-1}M$ be an MZ-space of $S^{-1}A$. That is $r(S^{-1}M) = sr(S^{-1}M)$. We need to prove that $r(M) \subset sr(M)$. Therefore, let $a \in r(M)$ be arbitrary. Then $a^m \in M$ for all $m \gg 0$. Let $N \geq 1$ be such that $a^n \in M$ for all $n \geq N$. Then since $\left(\frac{a}{s}\right)^n = \frac{a^n}{s^n} \in S^{-1}M$ for all $n \geq N$, we find that $\frac{a}{s} \in sr(S^{-1}M)$, since $S^{-1}M$ is an MZ-space of $S^{-1}A$.

Hence $y\left(\frac{a}{s}\right)^m \in S^{-1}M$ for all $y \in S^{-1}A$ and all $m \gg 0$. Let $b \in A$ be arbitrary. We need to show that $ba^m \in M$ for all $m \gg 0$. Consider for some $t \in S$ the element $y = \frac{b}{t}$. By the above, we find that $\frac{b}{t}\left(\frac{a}{s}\right)^m \in S^{-1}M$ for all $m \gg 0$. Let $N' \geq 1$ be such that $\frac{b}{t}\left(\frac{a}{s}\right)^n \in S^{-1}M$ for all $n \geq N'$. Then $\frac{ba^n}{s'} \in S^{-1}M$ for all $n \geq N'$, with $s' = ts^n \in S$. Hence $\frac{ba^n}{s'} = \frac{\mu_n}{t_n}$ for some $\mu_n \in M$ and $t_n \in S$. Then there exists $u_n \in S$ such that $u_n(t_n ba^n - \mu_n s') = 0$. Hence $u_n t_n ba^n \in M$. Since M is S-saturated, we find that $ba^n \in M$ for all $n \geq N'$. Therefore we have $a \in sr(M)$.

Thus M is an MZ-space of A.

□

Definition 3.4.8. *Let R be a commutative ring, S a multiplicatively closed subset of R and A an R-algebra. Then $e \in A$ is an S-*idempotent *if there exists some $s \in S \setminus \{0\}$ such that $e^2 = se$.*

Theorem 3.4.9. (Generalized Zhao Theorem) *Let R be a domain, $S = R \setminus \{0\}$ and A an R-algebra. Let M be an S-saturated R-submodule of A such that all elements of $r(M)$ are algebraic over R. Then M is an MZ-space of A if and only if for every S-idempotent e of A which belongs to M we have that for every $a \in A$ there exists an $s \in S$ such that $sae \in M$.*

Proof. $\Rightarrow$:) Let M be an MZ-space of A and e an S-idempotent of A that belongs to M. Write $e^2 = se$ for some $s \in S$. Then $e^m = s^{m-1}e \in Re \subset M$ for all $m \geq 1$. Hence $e \in r(M)$. Since M is an MZ-space, we find that $e \in sr(M)$, i.e. for every $a \in A$ there exists some $N \in \mathbf{N}$ such that $ae^m \in M$ for all $m \geq N$. In particular $s^{N-1}ae = as^{N-1}e = ae^N \in M$. Since S is multiplicatively closed, we have $s^{N-1} \in S$.

$\Leftarrow$:) Now assume that for every S-idempotent e of A which belongs to M we have the required property. By (iii) of Proposition 3.4.7 it suffices to show that $S^{-1}M$ is an MZ-space of $S^{-1}A$. By (i) of Proposition 3.4.7, we have $r(S^{-1}M) = S^{-1}r(M)$, hence all elements of $r(S^{-1}M)$ are algebraic over the field $K = S^{-1}R$.

Now let $\tilde{e} = e/t$ be an idempotent of $S^{-1}A$ with $e \in M$ and $t \in S$. Then $\tilde{e}^2 = (e/t)^2 = e^2/t^2 = e/t = \tilde{e}$, since $\tilde{e}$ is an idempotent. Then $e^2 = te$ and e is an S-idempotent. Then by hypothesis: for every $a \in A$ there exists an $s \in S$ such that $sae \in M$. Hence $S^{-1}A\tilde{e} \subset S^{-1}M$ and by Zhao's Theorem we find that $S^{-1}M$ is an MZ-space of $S^{-1}A$. □

Using this Generalized Zhao Theorem, we can prove the following generalization of Lemma 3.3.1:

Lemma 3.4.10. *Let R be a domain and $L\colon R[Y] \to R$ be a linear map such that there exists an $N \geq 1$ for which $L(Y^n) = 0$ for all $n \geq N$. Then $\operatorname{Ker} L$ is an MZ-space of $R[Y]$ if and only if $L(1) \neq 0$.*

Proof. $\Leftarrow$:) We have $(Y^N) \subset \operatorname{Ker} L$. So it is again sufficient to show that $\operatorname{Ker} L/(Y^N)$ is an MZ-space of $R[Y]/(Y^N)$.

We now aim to use the Generalized Zhao Theorem. Let R be the domain and $R[Y]/(Y^N)$ the R-algebra.

Then $\operatorname{Ker} L/(Y^N)$ is an $R \setminus \{0\}$-saturated R-submodule of $R[Y]$: Let $b \in R[Y]/(Y^N)$ be arbitrary such that $sb \in \operatorname{Ker} L/(Y^N)$ for some $s \in R \setminus \{0\}$. We have $0 = L(sb) = sL(b)$. Since $s \neq 0$, we find that $b \in \operatorname{Ker} L/(Y^N)$ as required.

Furthermore all elements of $r(\operatorname{Ker} L/(Y^N))$ are elements of $R[Y]/(Y^N)$ which is a finitely generated R-module of $R[Y]$. Hence all of its elements are algebraic over R.

We now study $S \setminus \{0\}$-idempotents of $\operatorname{Ker} L/(Y^N)$. All $c \in R \setminus \{0\}$ are $R \setminus \{0\}$-idempotents in $R[Y]/(Y^N)$, as we have $c^2 = c \cdot c$ and $c \in R \setminus \{0\}$. Also 0 is clearly an $R \setminus \{0\}$-idempotent.

Conversely, each $R \setminus \{0\}$-idempotent e is of the form $c + (Y^N)$ with $c \in R$. Namely, let $e^2 = se$ for some $s \in R \setminus \{0\}$. Write $e = c_0 + c_1Y + \ldots + c_{N-1}Y^{N-1}$. If $c_0 = 0$ it follows easily from $e^2 = se$ that all $c_i = 0$, hence $e = 0$.

Therefore assume that $c_0 \neq 0$. Then $(e^2)_0 = (se)_0$ implies that $c_0^2 = sc_0$. Hence $c_0 = s$ (since $c_0 \neq 0$). If e is not of the form $c + (Y^N)$, then $e = s + c_rY^r + \ldots + c_{N-1}Y^{N-1}$ for some $1 \leq r \leq N-1$ and $c_r \neq 0$. Then $(e^2)_r = (se)_r$ implies $2sc_r = 0$, hence $c_r = 0$, a contradiction.

Since $L(1) \neq 0$ we find that $L(c) = c \cdot L(1) \neq 0$ for all $R - \{0\}$-idempotents e that are nonzero. Hence the condition as stated in the Generalized Zhao Theorem is satisfied and $\operatorname{Ker} L/(Y^N)$ is an MZ-space of $R[Y]/(Y^N)$. △

Chapter 4

Mathieu-Zhao spaces of finite rings

If we consider MZ-spaces of (finite) rings, we regard the ring as a $\mathbf{Z}$-algebra. In particular, an MZ-space M of a ring R is additive, closed under scalar multiplication by integers (we call this $\mathbf{Z}$-*linear*) and for all $a \in R$, if $a^m \in M$ for all $m \geq 1$, then for every $b \in R$ there exists some $N \in \mathbf{N}$ such that for all $n \geq N$ we have $ba^n \in M$.

Note that for a $\mathbf{Z}$-linear subset it is sufficient that for every element $a \in R$ we have $-a \in R$, for scalar multiplication by integers is defined as repeated addition (of course addition still needs to be checked on itself).

The main results of this chapter are Theorem 4.3.13 and Proposition 4.3.3 which give a reduction to finite local rings for classifying MZ-spaces of finite rings. We start with some examples and some discussion.

4.1 Some special cases

The first example is the one that got me thinking about classifying MZ-spaces of finite rings.

Example 4.1.1. (The rings $\mathbf{Z}/n\mathbf{Z}$) *Let n be a positive integer and let R be the ring $\mathbf{Z}/n\mathbf{Z}$. Then all $\mathbf{Z}$-linear subspaces of $\mathbf{Z}/n\mathbf{Z}$ are actually ideals. Since ideals are MZ-spaces (see Example 2.1.5), we have now classified all the MZ-spaces of $\mathbf{Z}/n\mathbf{Z}$.*

Proof. Let M be a $\mathbf{Z}$-linear subspace of $\mathbf{Z}/n\mathbf{Z}$. Let $\overline{b} \in \mathbf{Z}/n\mathbf{Z}$ and $\overline{a} \in M$ be arbitrary. Then $\overline{b}\overline{a} = b\overline{a} \in M$ as M is $\mathbf{Z}$-linear. Hence M is an ideal. △

A next class of examples are the finite fields. A bit more involved, but a nice proof on itself:

Lemma 4.1.2. *Let p be a prime, $n \geq 1$ an integer and $q = p^n$. Then all $\mathbf{Z}$-linear subspaces of $\mathbb{F}_q$ that do not contain 1 are MZ-spaces of $\mathbb{F}_q$.*

Proof. Let M be a $\mathbf{Z}$-linear subspace of $\mathbb{F}_q$ that does not contain 1. Then $r'(M) = \{m \in M \mid \forall n \geq 1 : m^n \in M\} = \{0\}$, as since the multiplicative group of $\mathbb{F}_q$ is cyclic, there exists some $N_m \in \mathbf{N}$ such that $m^{N_m} = 1$ for all $m \neq 0$, while $1 \notin M$. Hence each such $\mathbf{Z}$-linear subspace of $\mathbb{F}_q$ is an MZ-space, by Lemma 2.1.11. □

As we have seen in Counterexample 2.1.6, there exist subspaces of this form. Altogether, noting Lemma 2.2.1, we have

Example 4.1.3. (Finite Fields) *Let p be a prime, $n \geq 1$ an integer and $q = p^n$. Then the MZ-spaces of $\mathbb{F}_q$ are precisely $\mathbb{F}_q$ itself and all* **Z***-linear subspaces that do not contain* 1.

Next, we give a way of easier detection of MZ-spaces.

Definition 4.1.4. *Let R be a ring. We define an* orthogonal basis of idempotents *E in R as follows:*

- *Each element $e \in E$ is an idempotent.*

- *If $e, f \in E$ are distinct elements, then $ef = 0$.*

- *Each (non-zero) idempotent $e \in R$ can be written as a sum of elements from E.*

We will later see that for finite rings such an orthogonal basis of idempotents always exists. For infinite rings there are at least some examples known.

Lemma 4.1.5. *Let R be a ring with orthogonal basis of idempotents E and M an MZ-space of R. Then for each idempotent $e \in M$, when written as a sum of idempotents from E, each of the summands of e is an element of M. In particular, if $M \cap E = \emptyset$, then 0 is the only idempotent in M.*

Proof. Let e be an idempotent in M. Then by Lemma 2.2.1 we have $Re \subset M$. Now let e' be any of the summands of e. We have $e'e = (e')^2 = e'$, hence $e' \in Re \subset M$. $\triangle$

Lemma 4.1.6. *Let A be an associative k-algebra with orthogonal basis of idempotents E. Let M be a k-linear subspace such that all elements of $r(M)$ are algebraic over k. Then M is an MZ-space if and only if $Ae \subset M$ for every $e \in M \cap E$.*

Proof. We only need to prove: if $Ae \subset M$ for every $e \in M \cap E$, then $Af \subset M$ for all idempotents $f \in M$. The result then follows from Zhao's Theorem.

So suppose that $Ae \subset M$ for every $e \in M \cap E$ and let $f \in M$ be an idempotent. Write $f = \sum_{e \in E'} e$ with $E' \subset E$. Then since $Ae \subset M$ and M is additive, hence $\sum_{e \in E'} Ae \subset M$. Then, since $Af = A(\sum_{e \in E'} e) \subset \sum_{e \in E'} Ae$, we find $Af \subset M$. $\triangle$

We now consider rings of the form $(\mathbb{F}_p)^r$. We are interested in idempotents of $(\mathbb{F}_p)^r$ with $r \geq 1$ and p a prime. Since $\mathbb{F}_p$ is a field, the only idempotents of $(\mathbb{F}_p)^r$ are elements in $\{0, 1\}^r$. If we define $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the ith place, then the set $\mathcal{E} := \{e_1, \ldots, e_r\}$ is an orthogonal basis of idempotents of $(\mathbb{F}_p)^r$.

Corollary 4.1.7. *Let p be a prime number and let $r \geq 1$. Let $M \subset (\mathbb{F}_p)^r$ be a* **Z***-linear subspace of $(\mathbb{F}_p)^r$. Then M is an MZ-space if and only if for each idempotent e in M, when written as a sum of idempotents from $\mathcal{E}$, each of the summands of e is an element of M.*

Proof. $\Rightarrow$:) This follows directly from Lemma 4.1.5.

$\Leftarrow$:) Since $(\mathbb{F}_p)^r$ is finite, it is a finite-dimensional $\mathbb{F}_p$-algebra. Therefore, by Lemma 3.1.4, every element of $(\mathbb{F}_p)^r$ is algebraic over $\mathbb{F}_p$ and so is every element of $r(M)$.

Now let $e \in \mathcal{E} \cap M$ be arbitrary. Since M is Z-linear, we find that $me \in M$ for all $m \in \mathbf{Z}$. Note that since e is of the form e_i, we find that this implies $0 \times \ldots \times 0 \times \mathbb{F}_p \times 0 \times \ldots \times 0 \subset M$. Since

$(\mathbb{F}_p)^r e_i = 0 \times \ldots \times 0 \times \mathbb{F}_p \times 0 \times \ldots \times 0$ we are done by the previous lemma. $\triangle$

The above Corollary holds more generally for finite fields $\mathbb{F}_q$, where the proof carries over verbatim. Note that we use here that we consider them as $\mathbb{F}_p$-algebras, so we may also consider the following, for which the proof also carries over verbatim.

Corollary 4.1.8. *Let p be a prime number and $n \geq 1$. Write $q_1 = p^{e_1}, q_2 = p^{e_2}, \ldots, q_n = p^{e_n}$ where each $e_i \geq 1$. Then with $R = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \ldots \times \mathbb{F}_{q_n}$ we have that a Z-linear subspace of R is an MZ-space if and only if for each idempotent e in M, when written as a sum of idempotents from $\mathcal{E}$, each of the summands is an element of M.*

When the finite fields are not all of the same characteristic, e.g. $\mathbb{F}_2 \times \mathbb{F}_3$, we cannot apply Zhao's Theorem and hence we need more.

4.2 Necessary Commutative Algebra

In this section we discuss results from Commutative Algebra, which are well-known. In some form they can be retrieved from [1], although some of the proofs may be different.

Proposition 4.2.1. *Let A be a commutative ring and $\mathfrak{N}$ its nilradical. Then the following are equivalent:*

(i) A has exactly one prime ideal;

(ii) Every element of A is either a unit or nilpotent;

(iii) $A/\mathfrak{N}$ is a field.

Proof. $i \to ii$: Write $\mathfrak{p}$ for the prime ideal in A. Then $\mathfrak{N} = \mathfrak{p}$ and A is a local ring. Then $A \setminus \mathfrak{N} = A^*$ and by definition $\mathfrak{N}$ is the set of all nilpotent elements.

$ii \to iii$: Consider the quotient map $A \to A/\mathfrak{N}$. This is surjective. Any $x \in A$ that is nilpotent is mapped to 0, while any $x \in A^*$ is mapped to a unit. Therefore $A/\mathfrak{N}$ is a field.

$iii \to i$: For all prime ideals $\mathfrak{p}$ of A we have $\mathfrak{N} \subset \mathfrak{p}$. Since $A/\mathfrak{N}$ is a field, we find that $\mathfrak{N}$ is maximal. Hence $\mathfrak{p} = \mathfrak{N}$ and there is only one prime ideal.

□

Corollary 4.2.2. *Let A be a commutative ring with exactly one prime ideal. Then A has no non-trivial idempotent elements.*

Proof. By Proposition 4.2.1, we find that every element of A is either nilpotent or invertible. Suppose that $e^2 = e$ and $e \neq 0, 1$. Then $e(e-1) = 0$, hence e is a zero-divisor. Then e is not invertible and must be nilpotent. But $e^n = e$ for all $n \geq 1$, a contradiction. So A has no non-trivial idempotents. $\triangle$

Corollary 4.2.3. *Let A be a commutative ring and $\mathfrak{m}$ a maximal ideal of A. Then for every $k \geq 1$ each element in $A/\mathfrak{m}^k$ is either a unit or nilpotent.*

Proof. In the proof of Proposition 3.1.3 we actually show that $A/\mathfrak{m}^k$ has a unique prime ideal. Hence condition (i) of Proposition 4.2.1 is satisfied. △

Definition 4.2.4. *Let A be a ring that satisfies the descending chain condition on ideals, i.e., if $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \dots$ is a chain of ideals, then there exists some $n \in \mathbf{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_m$ for all $m \geq n$. Such a ring is called an* Artin ring*.*

Since in a finite ring there are only finitely many ideals, every finite ring satisfies the descending chain condition, hence is an Artin ring. We now start working on properties of Artin rings, until we arrive at the structure theorem for Artin rings. This structure theorem is essential in classifying the MZ-spaces of finite rings. For most of the properties, we shall explain why it also holds for finite rings.

Corollary 4.2.5. *Let A be an Artin ring and $\mathfrak{a}$ be an ideal in A. Then $A/\mathfrak{a}$ is an Artin ring.*

Proof. Let $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \dots$ be a descending chain of ideals in $A/\mathfrak{a}$. Then $q^{-1}(\mathfrak{a}_1) \supset q^{-1}(\mathfrak{a}_2) \supset q^{-1}(\mathfrak{a}_3) \supset \dots$ is a descending chain of ideals in A, where q is the quotient-map. Hence this becomes stationary as A is an Artin ring. Say $q^{-1}(\mathfrak{a}_n) = q^{-1}(\mathfrak{a}_m)$ for all $m \geq n$. Since q is surjective, this implies

$$\mathfrak{a}_n = qq^{-1}(\mathfrak{a}_n) = qq^{-1}(\mathfrak{a}_m) = \mathfrak{a}_m.$$

Hence $A/\mathfrak{a}$ is an Artin ring. △

Obviously, if A is a finite ring and $\mathfrak{a}$ is an ideal in A, then $A/\mathfrak{a}$ is also finite. A finite ring A has only finitely many ideals, hence only finitely many may be prime (or maximal). This holds more generally for Artin rings, see Proposition 4.2.10. If $\mathfrak{a}$ happens to be a prime ideal, then $A/\mathfrak{a}$ is a finite domain, and hence a field. Therefore $\mathfrak{a}$ is a maximal ideal. This also holds more generally for Artin rings:

Lemma 4.2.6. *Let A be an Artin ring. Any prime ideal in A is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A. Then $B := A/\mathfrak{p}$ is an Artin domain by Corollary 4.2.5. Let $x \in B$ be nonzero. Then when considering the sequence

$$(x) \supset (x^2) \supset (x^3) \supset \dots$$

we find that $(x^n) = (x^{n+1})$ for some $n \in \mathbf{N}$, since B is an Artin ring. Hence $x^n = x^{n+1}y$ for some $y \in B$. Then $xy = 1$ by the cancellation law in a domain. Since x was arbitrary nonzero, we find that B is a field and hence $\mathfrak{p}$ is maximal. △

This lemma has two nice corollaries:

Corollary 4.2.7. *Let A be an Artin ring. Then $\mathfrak{N} = \mathfrak{R}$, i.e., the nilradical of A equals the Jacobson radical of A.*

Proof. Since $\mathfrak{N}$ is the intersection of all prime ideals and $\mathfrak{R}$ is the intersection of all maximal ideals, this follows directly from Lemma 4.2.6. △

Corollary 4.2.8. *In a local Artin ring every element is either a unit or nilpotent.*

Proof. Since a local Artin ring has only one maximal ideal $\mathfrak{m}$, this is also the only prime ideal, by Lemma 4.2.6. Hence by Proposition 4.2.1 we find that every element is either a unit or nilpotent. △

Proposition 4.2.9. *The nilradical in an Artin ring is nilpotent.*

Proof. Let A be an Artin ring and $\mathfrak{N}$ its nilradical. Consider the descending chain $\mathfrak{N} \supset \mathfrak{N}^2 \supset \mathfrak{N}^3 \supset \dots$. Since A is an Artin ring, there exists some $n \in \mathbf{N}$ such that $\mathfrak{N}^n = \mathfrak{N}^m$ for all $m \geq n$.

Suppose that $\mathfrak{N}^n \neq 0$. Let Γ denote the set of ideals $\mathfrak{a}$ such that $\mathfrak{N}^n\mathfrak{a} \neq 0$. Then Γ is non-empty, since $\mathfrak{N}^{n+1} \neq 0$. Then Γ has a minimal element. Write $\mathfrak{b}$ for such a minimal element.

Then there exists some $x \in \mathfrak{b}$ for which $x\mathfrak{N}^n \neq 0$. Since $(x) \subset \mathfrak{b}$, we have $(x) = \mathfrak{b}$ by minimality of $\mathfrak{b}$. Then $(x\mathfrak{N})\mathfrak{N}^n = x\mathfrak{N}^{n+1} = x\mathfrak{N}^n \neq 0$ and $x\mathfrak{N} \subset (x)$. Hence $x\mathfrak{N} = (x)$. Therefore $xy = x$ for some $y \in \mathfrak{N}$. Hence we find

$$x = xy = xy^2 = xy^3 = \dots$$

Since y is nilpotent, we find that there exists some $k \in \mathbf{N}$ such that $xy^k = 0$. But then $x = 0$, a contradiction to the choice of x. Hence $\mathfrak{N}^n = 0$ and $\mathfrak{N}$ is nilpotent. □

Proposition 4.2.10. *Let A be an Artin ring, then A has only finitely many maximal ideals.*

Proof. Consider the set of all finite intersections $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ of maximal ideals. Then this set has a minimal element, for every decreasing sequence of ideals becomes stationary, and all elements in this set are ideals.

Write $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ for the minimal element of this set. Then for any maximal ideal $\mathfrak{m}$ of A we have $\mathfrak{m} \cap \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \supset \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ since $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ is minimal. Hence $\mathfrak{m} \supset \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \supset \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n$. Therefore by the Euclidean Lemma (3.1.2), we have $\mathfrak{m} \supset \mathfrak{m}_i$ for some $i = 1, \dots, n$. Hence $\mathfrak{m} = \mathfrak{m}_i$ since $\mathfrak{m}_i$ is maximal. □

Artin rings, and hence finite rings, have a particularly nice structure, as seen in the following theorem. In its formulation, we use Proposition 4.2.10.

Theorem 4.2.11. (Structure theorem for Artin rings) *Let A be an Artin ring, with maximal ideals $\mathfrak{m}_1, \dots \mathfrak{m}_n$. Then for some $k \in \mathbf{N}$ we have $A \cong \prod_{i=1}^n A/\mathfrak{m}_i^k$.*

Proof. Note that $\prod_{i=1}^n \mathfrak{m}_i^k = \left(\prod_{i=1}^n \mathfrak{m}_i\right)^k \subset \left(\bigcap_{i=1}^n \mathfrak{m}_i\right)^k = \mathfrak{N}^k = 0$ for some $k \in \mathbf{N}$ by Proposition 4.2.9. Since the $\mathfrak{m}_i$ are pairwise coprime, we find that the $\mathfrak{m}_i^k$ are also pairwise coprime.

> **Claim.** *If ideals I, J in a ring R are coprime, then $I^n + J^m = R$ for any $n, m \in \mathbf{N}$.*
>
> *Proof.* Since I, J are coprime, we can find $x \in I$, $y \in J$ such that $x + y = 1$. Then consider
>
> $$(x+y)^{2N} = 1^{2N} = 1,$$
>
> where $N := \max\{n, m\}$.
>
> By expanding, we find
>
> $$1 = \sum_{i=0}^{2N} \binom{2N}{i} x^i y^{2N-i} = \sum_{i=0}^{N-1} \binom{2N}{i} x^i y^{2N-i} + \sum_{i=N}^{2N} \binom{2N}{i} x^i y^{2N-i}.$$

Note that $x^i \in I^n$ if $i \geq N$ and $y^{2N-i} \in J^m$ if $i < N$. Hence indeed $I^n + J^m = R$. △

Hence $\prod \mathfrak{m}_i^k = \bigcap \mathfrak{m}_i^k = 0$. Therefore,

$$A \to \prod (A/\mathfrak{m}_i^k)$$

is an isomorphism by the Chinese Remainder Theorem. □

Remark. *Note that this description is the unique way (up to isomorphism) to express an Artin ring as a product of local Artin rings. For a proof, see Thm 8.7 in [1].*

Note that $R/\mathfrak{m}_i^k$ is a local ring, and that every element in $R/\mathfrak{m}_i^k$ is either a unit or nilpotent (see Corollary 4.2.3). If R is finite, then $R/\mathfrak{m}_i^k$ certainly is finite.

4.3 Classifying Mathieu-Zhao spaces of finite rings

By the Structure Theorem for Artin rings, we are interested in rings of the form $R/\mathfrak{m}^k$ and products of such rings. Hence the following lemma is useful:

Lemma 4.3.1. *Let R be a commutative ring with identity and let A, B be R-algebras. If $M \subset A$ and $N \subset B$ are MZ-spaces of A, B respectively, then $M \times N$ is an MZ-space of $A \times B$. In particular $M \times \{0\}$ and $\{0\} \times N$ are MZ-spaces of $A \times B$.*

Proof. Suppose that $(a,b)^m \in M \times N$ for all $m \geq 1$. Then $(a^m, b^m) \in M \times N$ for all $m \geq 1$ and hence $a^m \in M, b^m \in N$ for all $m \geq 1$.

Let $x = (x', x'') \in A \times B$ be arbitrary. Since M, N are MZ-spaces of of A, B respectively, there exist $N_{x'}$ and $N_{x''}$ such that $x'a^n \in M$ for all $n \geq N_{x'}$ and $x''b^n \in N$ for all $n \geq N_{x''}$. Write $N_x = \max\{N_{x'}, N_{x''}\}$. It follows that $(x'a^n, x''b^n) \in M \times N$ for all $n \geq N_x$. Since x was arbitrary, we find that $M \times N$ is indeed an MZ-space of $A \times B$. △

The converse of this lemma is false as we see in the following counterexample.

Counterexample 4.3.2. *Consider the ring $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ and $M := \{(0,0),(1,2)\}$. Clearly, M is not of the form $M_1 \times M_2$, but it is an MZ-space of R.*

Proof. Since $(1,2)+(1,2) = (0,0)$ we find that M is $\mathbf{Z}$-linear. Furthermore, $(1,2)^2 = (1,0) \notin M$. Hence $r'(M) = \{(0,0)\}$ and by Proposition 2.1.4, Lemma 2.1.11 and Corollary 2.1.12 we are done. △

Now we study rings of the form $R/\mathfrak{m}^k$, where R is finite. Note that for every $a \in R/\mathfrak{m}^k$ the set $\{a^m \mid m \geq 0\}$ contains 0 or 1, but not both. For if it contains 0, then a is nilpotent, hence a zero-divisor, while if it contains 1, then a is a unit.

Conversely, if $a \in R/\mathfrak{m}^k$ is nilpotent, then $0 \in \{a^m \mid m \geq 0\}$, while if $a \in R/\mathfrak{m}^k$ is a unit, then there exists some $m \in \mathbf{N}$ with $a^m = 1$, since $(R/\mathfrak{m}^k)^*$ is finite.

The following proposition is the first step in characterizing MZ-spaces of finite rings. We introduce the notations $E(R)$ for the set of idempotent elements of R and $\mathfrak{n}(R)$ for the set of nilpotent elements of R. Then we have:

Proposition 4.3.3. *(Classification Theorem) Let R be a finite ring. Let M be a $\mathbf{Z}$-linear subspace of R. If $M \cap E(R) = 0$, then $r(M) = \mathfrak{n}(R)$ and M is an MZ-space.*

Proof. Suppose that $r(M) \neq \mathfrak{n}(R)$. Then there exists some $a \in r(M) \setminus \mathfrak{n}(R)$. Write $R = R/\mathfrak{m}_1^k \times \ldots \times R/\mathfrak{m}_n^k$ using the Structure Theorem for Artin Rings (see Theorem 4.2.11). We can now write $a = (a_1, \ldots, a_n)$. Since by Corollary 4.2.3 all elements of $R/\mathfrak{m}_i^k$ are either a unit or nilpotent, and since $a \notin \mathfrak{n}(R)$, we find that there must exist some a_i that is a unit by the following lemma (see Lemma 4.3.4). Then since $R/\mathfrak{m}_i^k$ is finite, we find that there exists some $m_i \in \mathbf{N}$ such that $a_i^{m_i} = 1$. Consider all a_i in $(a_1, \ldots, a_n)$ that are units and determine the corresponding $m_i \in \mathbf{N}$. Define $m := \prod m_i$. Then we have $a_i^m = 1$ for all $i \in \{1, \ldots, n\}$ such that a_i is a unit.

For all nilpotent elements a_i we determine $N_i \in \mathbf{N}$ such that $a_i^{N_i} = 0$. Write $N = \max\{N_i\}$. Then $a_i^N = 0$ for all nilpotent a_i. Then

$$(a_1, \ldots, a_n)^{mN} \in \{0, 1\}^n.$$

The 1's occur on the places where we had a unit, and the 0's where we found a nilpotent element. But this element is a non-zero idempotent contained in M, a contradiction. Therefore $r(M) = \mathfrak{n}(R)$ and by Lemma 2.1.11 M is an MZ-space. □

Lemma 4.3.4. *Let $R_1 \times \ldots \times R_n$ be a commutative ring with identity. Then $(r_1, \ldots, r_n)$ is nilpotent iff r_i is nilpotent in R_i for all $i \in \{1, \ldots, n\}$.*

Proof. ⇒:) Suppose that $(r_1, \ldots, r_n)^N = 0$ for some $N \in \mathbf{N}$. Then $(r_1^N, \ldots, r_n^N) = 0$, hence $r_1^N = 0, \ldots, r_n^N = 0$. Hence all r_i are nilpotent.

⇐:) Suppose that all r_i are nilpotent, that is, there exist N_i such that $r_i^{N_i} = 0$. Write $N = \max\{N_i\}$. Then of course $r_i^N = 0$ for all $i \in \{1, \ldots, n\}$. Hence $(r_1, \ldots, r_n)^N = (r_1^N, \ldots, r_n^N) = 0$ and $(r_1, \ldots, r_n)$ is nilpotent. △

Note that Counterexample 4.3.2 provides an example of an MZ-space that satisfies the conditions of the previous proposition.

The following theorem is the closest converse to Lemma 4.3.1 that we have for finite rings.

Theorem 4.3.5. *Let R be a finite ring of the form*

$$R \cong R_1/\mathfrak{m}_1^{k_1} \times R_2/\mathfrak{m}_2^{k_2},$$

where the $\mathfrak{m}_i$ are maximal in R_i. If M is an MZ-space of R, then $r(M) = \mathfrak{n}(R)$ or M is of the form $M_1 \times M_2$ where each M_i is an MZ-space of $R_i/\mathfrak{m}_i^{k_i}$.

Proof. Write $S_1 := R_1/\mathfrak{m}_1^{k_1}$ and $S_2 := R_2/\mathfrak{m}_2^{k_2}$. Let M be an MZ-space of R and suppose that there exists some $(r, s) \in r(M) \setminus \mathfrak{n}(R)$. Then we distinguish three cases:

1. $r \in S_1^*$ and $s \in S_2^*$;

2. $r \in S_1^*$ and $s \notin S_2^*$;

3. $r \notin S_1^*$ and $s \in S_2^*$.

Observe that since $(r,s) \notin \mathfrak{n}(R)$, the case $r \notin S_1^*$ and $s \notin S_2^*$ cannot occur (see Corollary 4.2.3).

In the first case, by considering $m_r, m_s \in \mathbf{N}$ such that $r^{m_r} = 1 = s^{m_s}$, we find that $(r,s)^{m_s m_r} = (1,1) \in M$. Hence by Lemma 2.2.1 $M = S_1 \times S_2$, hence M is of the required form.

In the second case, note that s is nilpotent, by Corollary 4.2.3. Determine $m \in \mathbf{N}$ such that $r^m = 1$ and $N \in \mathbf{N}$ such that $s^N = 0$. Then $(r,s)^{Nm} = (1,0) \in M$. Since M is an MZ-space, we then find that $R(1,0) = S_1 \times \{0\} \subset M$ by Lemma 2.2.1, since $(1,0)$ is an idempotent.

Then by Corollary 2.2.4 we find that $M/(S_1 \times \{0\})$ is an MZ-space of $(S_1 \times S_2)/(S_1 \times \{0\}) \cong S_2$. Let $M_2 := \{m_2 \in S_2 \mid \exists s_1 \in S_1 \colon (s_1, m_2) \in M\}$. Then one readily verifies that $M = S_1 \times M_2$ and $M_2 \cong M/(S_1 \times \{0\})$.

The third case is of course similar to the second case. □

Note that there are MZ-spaces that satisfy both $r(M) \subset \mathfrak{n}(R)$ and $M = M_1 \times M_2$. For example $M = \mathfrak{n}(R)$, as then M is an ideal and we know that $M = I_1 \times I_2$ for ideals I_1, I_2.

To show the usefulness of this theorem, we shall give an example that explains how we can determine all MZ-spaces. Before that, we have another proposition, of which part (i) is a partial converse to Proposition 4.3.3.

Proposition 4.3.6. *Let R be a ring and M a $\mathbf{Z}$-linear subspace of R. Write $\mathfrak{n}(R)$ for the set of nilpotent elements of R and $E(R)$ for the set of idempotents of R. Then*

(i) If $r(M) \subset \mathfrak{n}(R)$ then $M \cap E(R) = 0$.

(ii) If $r \in M$ is such that there exist $e \in E(R) \setminus \{0\}$ and $n \in \mathbf{N}$ such that $nr = e$ then $r(M) \neq \mathfrak{n}(R)$.

Proof. (i) If $r(M) \subset \mathfrak{n}(R)$, then $e \notin r(M)$ for every non-zero idempotent. Suppose $M \cap E(R) \neq 0$. Determine $e \in M$ idempotent and non-zero. Then $e^n = e$ for all $n \in \mathbf{N}$. Hence $e \in r(M)$, a contradiction.

(ii) Suppose that there exists an $r \in M$ such that $nr = e$ as described. Then since M is additive, we have $e \in M$. But then by (i), we find that $r(M) \not\subset \mathfrak{n}(R)$.

□

Now we have all the tools we need for our example.

Example 4.3.7. *Let $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ be our ring of interest. Since it is a product of two local rings, we have four idempotents:*

$$(0,0), (0,1), (1,0), (1,1)$$

and nilpotent elements

$$(0,0), (0,2).$$

By Lemma 4.3.1 and Example 4.1.1 we find that MZ-spaces are:

$$\begin{aligned} 0 =& 0 \times 0 \\ & 0 \times 2\mathbf{Z}/4\mathbf{Z} \\ & 0 \times \mathbf{Z}/4\mathbf{Z} \\ & \mathbf{Z}/2\mathbf{Z} \times 0 \\ & \mathbf{Z}/2\mathbf{Z} \times 2\mathbf{Z}/4\mathbf{Z} \end{aligned}$$

$$R = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$$

From Counterexample 4.3.2 we know that $M = \{(0,0),(1,2)\}$ is an MZ-space. It is clear that $M \not\subset \mathfrak{n}(R)$ and $r'(M) \subset \mathfrak{n}(R)$, since $(1,2)^2 = (1,0) \notin M$.
From Theorem 4.3.5 we know that we are only interested in MZ-spaces M of the form:

- $M \not\subset \mathfrak{n}(R)$;
- $r(M) \subset \mathfrak{n}(R)$.

So by Proposition 4.3.6 (i) we are not interested in idempotent elements. So the remaining elements are

$$(0,3),(1,2),(1,3).$$

Note that $3 \cdot (0,3) = (0,1)$ and $3 \cdot (1,3) = (1,1)$, hence by Proposition 4.3.6 (ii) we know that they cannot be elements of our MZ-space. The only remaining elements are $(1,2)$, $(0,0)$ and $(0,2)$. Note that $(0,2)+(1,2) = (1,0)$ so we cannot have both as element of our MZ-space. So the following possibilities remain:

$$M = \{(0,0)\},$$

$$M = \{(0,0),(0,2)\},$$

$$M = \{(0,0),(1,2)\}.$$

The first two are product spaces, while we have also already met the third. So R has exactly 5 MZ-spaces.

We further remark that it is essential in Theorem 4.3.5 that all groups of units are finite. A generalization could be found in the following theorem:

Theorem 4.3.8. *Let $R \cong R_1/\mathfrak{m}_1^{k_1} \times R_2/\mathfrak{m}_2^{k_2}$ be an Artin ring such that R^* is finite. If M is an MZ-space of R, then either $r(M) = \mathfrak{n}(R)$ or M is of the form $M_1 \times M_2$ where each M_i is an MZ-space of $R_i/\mathfrak{m}_i^{k_i}$.*

The proof would carry over verbatim. However, since there are no infinite Artin rings with a finite unit group, as we prove in the following lemma, it is actually equivalent to the previous theorem.

Lemma 4.3.9. *Let R be an Artin ring such that R^* is finite. Then R itself is finite.*

Proof. By the Structure theorem for Artin rings, we may assume that R is a local Artin ring. Let $\mathfrak{m}$ be its maximal ideal. Note that $R \setminus \mathfrak{m} = R^*$ is finite. Also, by Corollary 4.2.7, we find that any element $x \in \mathfrak{m}$ is nilpotent. Since $1 + x \in R^*$ for every nilpotent x, and R^* is finite, we find that $\mathfrak{m}$ is finite. Hence $R = (R \setminus \mathfrak{m}) \cup \mathfrak{m}$ is finite. △

A true generalization can be found by relaxing the conditions a little further.

Theorem 4.3.10. *Let $R \cong R_1/\mathfrak{m}_1^{k_1} \times R_2/\mathfrak{m}_2^{k_2}$ be an Artin ring such that every element in R^* has finite order. If M is an MZ-space of R, then either $r(M) = \mathfrak{n}(R)$ or M is of the form $M_1 \times M_2$ where each M_i is an MZ-space of $R_i/\mathfrak{m}_i^{k_i}$.*

Certainly, the proof carries over verbatim again. However in this case we do have infinite rings that satisfy the hypothesis.

Example 4.3.11. *Consider the chain of inclusions*

$$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{64} \subset \ldots$$

Then we define $\overline{\mathbb{F}_2} := \bigcup_{n=1}^{\infty} \mathbb{F}_{2^{n!}}$*. This is the algebraic closure of* $\mathbb{F}_2$*. This is an infinite field, so it is certainly a local Artin ring. Furthermore, it is infinite, hence it has an infinite number of units. For every unit* x *we can determine* n *such that* $x \in \mathbb{F}_{2^{n!}}$*, hence the order of* n *is a divisor of* $2^{n!} - 1$*, thus finite.*

Note that for any p prime we can determine all MZ-spaces of $\overline{\mathbb{F}_p}$ with the same argument as we did for $\mathbb{F}_{p^n}$. Precisely, $r'(M) = \{0\}$ for any $\mathbf{Z}$-linear subspace M of $\overline{\mathbb{F}_p}$ that does not contain 1 by the same argument as in Lemma 4.1.2, hence all $\mathbf{Z}$-linear subspaces of $\overline{\mathbb{F}_p}$ are MZ-spaces, as well as the entire ring $\overline{\mathbb{F}_p}$ itself.

Next, we shall prove a theorem that generalizes Theorem 4.3.5 by means of larger products. But first, we need some discussion. Recall the structure theorem for Artin rings, that says that we can write any finite ring R as:

$$R \cong R/\mathfrak{m}_1^k \times \ldots \times R/\mathfrak{m}_n^k.$$

So if we can prove a general theorem for rings of the form

$$R \cong R_1/\mathfrak{m}_1^{k_1} \times \ldots \times R_n/\mathfrak{m}_n^{k_n}, \tag{4.1}$$

where the $\mathfrak{m}_i \subset R_i$ are maximal, then this is a lot more general than needed. It is very useful, however, to prove it in this form. For if we have a ring like in Example 4.3.7, then it is not of the first form. Or for example if

$$R \cong \mathbf{Z}/4\mathbf{Z} \times \mathbb{F}_p[X]/(X^2).$$

Then we can immediately apply the theorem, which saves a lot of work.

Secondly, if M is an MZ-space of R (when written in the form of 4.1) and we have an element $(r_1, \ldots, r_n) \in r(M) \setminus \mathfrak{n}(R)$, then we can again (like in the proof of Theorem 4.3.5) determine some natural number N such that $(r_1, \ldots, r_n)^N = (*, \ldots, *)$ where $* \in \{0, 1\}$ depending on whether r_i nilpotent or invertible. By Corollary 2.2.3 we may then as well assume that the 1s occur in the first positions, while the 0s occur in the last positions, i.e.

$$(r_1, \ldots, r_n)^N = (*, \ldots, *) \to (1, \ldots, 1, 0, \ldots, 0)$$

as we can interchange the factors of R.

Lastly, we have the following example, to show that we cannot generalize Theorem 4.3.5 trivially as:

False Theorem. *Let* $R \cong R_1/\mathfrak{m}_1^{k_1} \times \ldots \times R_n/\mathfrak{m}_n^{k_n}$ *be a finite ring. If* M *is an MZ-space of* R*, then either* $r(M) = \mathfrak{n}(R)$ *or* M *is of the form* $M_1 \times \ldots \times M_n$ *where each* M_i *is an MZ-space of* $R_i/\mathfrak{m}_i^{k_i}$*.*

Counterexample 4.3.12. *Let* $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$*. Then the* $\mathbf{Z}$*-linear subspace* M *defined by*

$$M := \{(0,0), (1,2)\} \times \mathbf{Z}/4\mathbf{Z}$$

is not of the form $M_1 \times M_2 \times M_3$ *and it is not of the form* $r(M) \subset \mathfrak{n}(R)$*, since* $(0,0,1) \in M$*. By Lemma 4.3.1 we see that it is indeed an MZ-space.*

Now for the true theorem and afterwards, we will correct the previous counterexample.

Theorem 4.3.13. *(Classification-Reduction Theorem) Let $R \cong R_1/\mathfrak{m}_1^{k_1} \times \ldots \times R_n/\mathfrak{m}_n^{k_1}$ be a finite ring, with the $\mathfrak{m}_i \subset R_i$ maximal. Write $S_i := R_i/\mathfrak{m}_i^{k_i}$. If M is an MZ-space of R, then M is of one of the following forms:*

- $r(M) \subset \mathfrak{n}(R)$;
- $\varphi^{-1}(S_{i_1} \times \ldots \times S_{i_l} \times M_{j_{l+1}\cdots j_n})$

where $\varphi\colon R \to S_{i_1} \times \ldots \times S_{i_l} \times S_{j_{l+1}} \times \ldots \times S_{j_n}$ is a canonical isomorphism and $M_{j_{l+1}\cdots j_n}$ is an MZ-space of $S_{j_{l+1}} \times \ldots \times S_{j_n}$.

Proof. Suppose that M is an MZ-space of R such that $r(M) \not\subset \mathfrak{n}(R)$. Let $x \in r(M) \setminus \mathfrak{n}(R)$ be arbitrary. Write $x = (x_1, \ldots, x_n)$. Since $x \notin \mathfrak{n}(R)$, there exists some i such that $x_i \notin \mathfrak{n}(S_i)$.

Write $i_1 < \ldots < i_l$ for the $0 < l \leq n$ positions where $x_i \notin \mathfrak{n}(S_i)$ and $j_{l+1} < \ldots < j_n$ be the remaining positions. Write

$$R' \cong S_{i_1} \times \ldots \times S_{i_l} \times S_{j_{l+1}} \times \ldots \times S_{j_n}.$$

Let $\varphi\colon R \to R'$ be the canonical isomorphism.

Determine (as in Theorem 4.3.5) N such that $\varphi(x)^N = (1, \ldots, 1, 0, \ldots, 0)$ where there are precisely l 1s and $n - l$ 0s. Then $R'(1, \ldots, 1, 0 \ldots, 0) = S_{i_1} \times \ldots \times S_{i_l} \times 0 \times \ldots \times 0 \subset M$ by Lemma 2.2.1.

Hence by Corollary 2.2.4 we find that $M/(S_{i_1} \times \ldots \times S_{i_l} \times 0 \times \ldots \times 0)$ is an MZ-space of $R'/(S_{i_1} \times \ldots \times S_{i_l} \times 0 \times \ldots \times 0) \cong S_{j_{l+1}} \times \ldots \times S_{j_n}$.

Then $M \cong S_{i_1} \times \ldots \times S_{i_l} \times M_{j_{l+1}\cdots j_n}$, where $M_{j_{l+1}\cdots j_n}$ is some MZ-space of $S_{j_{l+1}} \times \ldots \times S_{j_n}$.

So $\varphi^{-1}(S_{i_1} \times \ldots \times S_{i_l} \times M_{j_{l+1}\cdots j_n})$ is an MZ-space of R. □

The above proof gives a method to determine the MZ-spaces of a certain ring, that are (images of) MZ-spaces of factors. We call those MZ-spaces *productwise MZ-spaces*. The MZ-spaces that have $r(M) \subset \mathfrak{n}(R)$ are determinable by the procedure stated in Example 4.3.7 using Proposition 4.3.6.

To demonstrate the above theorem, we work out the example of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

Example 4.3.14. *Let $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Then we have MZ-spaces of the form $M_1 \times M_2 \times M_3$ where $M_1 \in \{0, \mathbf{Z}/2\mathbf{Z}\}$, $M_2, M_3 \in \{0, 2\mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}\}$, i.e., 18 MZ-spaces (by Example 4.1.1). Note however, that for M_1 arbitrary we have*

$$M_1 \times 2\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \cong M_1 \times \mathbf{Z}/4\mathbf{Z} \times 2\mathbf{Z}/4\mathbf{Z}$$

and more "isomorphic" MZ-spaces.

Next, we have MZ-spaces of the form $M' \times M_3$ where $M' = \{(0,0), (1,2)\}$ and $M_3 \in \mathbf{Z}/4\mathbf{Z}$ by Examples 4.1.1 and 4.3.7.

Trusting that the MZ-spaces of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ with $r(M) \subset \mathfrak{n}(R)$ are:

$$\{(0,0), (0,2), (2,1), (2,3)\},$$

$$\{(0,0), (1,2), (2,0), (3,2)\},$$

$$\{(0,0), (1,3), (2,2), (3,1)\},$$

$$\{(0,0), (2,2)\}$$

we have MZ-spaces of the form $M_1 \times M''$, where M'' is one of the above four MZ-spaces of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

Then lastly, we have MZ-spaces

$$\hat{M}_1 = \{(0,0,0),(1,0,2)\}$$

$$\hat{M}_2 = \{(0,0,0),(1,0,2),(0,2,0),(1,2,2)\}$$

$$\hat{M}_3 = \{(0,0,0),(1,0,2),(0,1,0),(1,1,2),(0,2,0),(1,2,2),(0,3,0),(1,3,2)\}$$

where, under the isomorphism $\varphi\colon R \to \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ we have $\varphi^{-1}(\hat{M}_1) = 0 \times M'$, $\varphi^{-1}(\hat{M}_2) = 2\mathbf{Z}/4\mathbf{Z} \times M'$ and $\varphi^{-1}(\hat{M}_3) = \mathbf{Z}/4\mathbf{Z} \times M'$.

We have now determined the productwise MZ-spaces. The remaining spaces are of the form $r(M) \subset \mathfrak{n}(R)$. The procedure that we need to follow to obtain them is as in Example 4.3.7. We list here the MZ-spaces obtained in that fashion:

$$M_I = \{(0,0,0),(0,0,2),(0,2,1),(0,2,3)\}$$

$$M_{II} = \{(0,0,0),(0,1,3),(0,2,2),(0,3,1)\}$$

$$M_{III} = \{(0,0,0),(0,0,2),(1,2,1),(1,2,3)\}$$

$$M_{IV} = \{(0,0,0),(0,2,2),(1,1,3),(1,3,1)\}$$

$$M_V = \{(0,0,0),(0,1,2),(0,2,0),(0,3,2)\}$$

$$M_{VI} = \{(0,0,0),(0,2,0),(1,1,2),(1,3,2)\}$$

$$M_{VII} = \{(0,0,0),(1,2,0)\}$$

$$M_{VIII} = \{(0,0,0),(1,0,2)\}$$

$$M_{IX} = \{(0,0,0),(1,2,2)\}$$

$$M_X = \{(0,0,0),(1,0,2),(1,2,0),(0,2,2)\}$$

$$M_{XI} = \{(0,0,0),(1,2,0),(1,2,2),(0,0,2)\}$$

$$M_{XII} = \{(0,0,0),(1,0,2),(1,2,2),(0,2,0)\}$$

Even though many MZ-spaces can be seen to be "isomorphic," we have at least managed to find them all. There are now 44 MZ-spaces of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

We now define two MZ-spaces M_1, M_2 of a ring R isomorphic, if there exists some ring R' and a ringisomorphism $\varphi\colon R \to R'$ such that $M_2 = \varphi(M_1)$. So for example in the previous example, the spaces M_{VII} and M_{VIII} are isomorphic by the isomorphism $(x,y,z) \mapsto (x,z,y)$. Counting the MZ-spaces of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ up to isomorphism, we arrive at a number of 29 MZ-spaces of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

All-in-all, if we are able to determine for all finite local rings what their MZ-spaces are, with these two procedures, we can determine all MZ-spaces of finite rings.

For classifying MZ-spaces of finite rings of the form $R/\mathfrak{m}^k$ the following known example (see [16]) cannot be omitted.

Lemma 4.3.15. *Let K be a field and $f(X) \in K[X]$ be an irreducible polynomial. Then every K-linear subspace V of $K[X]/(f)^k$ that does not contain 1 is an MZ-space of $K[X]/(f)^k$.*

Proof. By Lemma 3.1.4 all elements of $K[X]/(f)^k$ are algebraic over K. By Corollary 4.2.3 we find that $K[X]/(f)^k$ has only units or nilpotent elements. By Lemma 3.1.1 $K[X]/(f)^k$ has no nontrivial idempotents.

Let V be a K-linear subspace of $K[X]/(f)^k$ with $1 \notin V$. Then 0 is the only idempotent of $K[X]/(f)^k$ in V. Now since $K[X]/(f)^k \cdot 0 = (0) \subset V$, we find that this subspace satisfies the hypotheses for Zhao's Theorem (2.2.5). Thus V is an MZ-space of $K[X]/(f)^k$. △

Lastly, we note that the generalizations of Theorem 4.3.5 carry over to Theorem 4.3.13 as well. So we have:

Theorem 4.3.16. *Let $R \cong R_1/\mathfrak{m}_1^{k_1} \times \ldots \times R_n/\mathfrak{m}_n^{k_1}$ be an Artin ring, with the $\mathfrak{m}_i \subset R_i$ maximal, such that every element in R^* has finite order. Write $S_i := R_i/\mathfrak{m}_i^{k_i}$. If M is an MZ-space of R, then M is of one of the following forms:*

- $r(M) \subset \mathfrak{n}(R)$;
- $\varphi^{-1}(S_{i_1} \times \ldots \times S_{i_l} \times M_{j_{l+1} \cdots j_n})$

where $\varphi\colon R \to S_{i_1} \times \ldots \times S_{i_l} \times S_{j_{l+1}} \times \ldots \times S_{j_n}$ is a canonical isomorphism and $M_{j_{l+1} \cdots j_n}$ is an MZ-space of $S_{j_{l+1}} \times \ldots \times S_{j_n}$.

Bibliography

[1] M.F. Atiyah and I. G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley Publishing, 1994.

[2] J. S. Birman. An Inverse Function Theorem for Free Groups. *Proc. Am. Math. Soc.*, **41**: pp. 634–638, 1973.

[3] D. E. Cohen. *Groups of cohomological dimension one*. Springer-Verlag, 1972.

[4] A. Crachiola, A. van den Essen, and S. Kuroda. *Polynomial Automorphisms Vol. 2 Recent Developments*. Birkhäuser, *to appear*.

[5] J.J. Duistermaat and W. van der Kallen. Constant terms in powers of a Laurent polynomial. *Indagationes Mathematicae*, 9: pp. 221–231, 06 1998.

[6] A. van den Essen. *Polynomial Automorphisms and the Jacobian Conjecture*. Birkhäuser, 2000.

[7] A. van den Essen. The Amazing Image Conjecture. *arXiv:1006.5801*, 2010.

[8] R. H. Fox. Free differential calculus I. Derivation in the free group ring. *Ann. of Math.*, **57**: pp. 547–560, 1953.

[9] J.P. Francoise, F. Pakovich, Y. Yomdin, and W. Zhao. Moment Vanishing Problem and Positivity: Some Examples. *Bull. des Sci. Math.*, **135**: pp. 10–32, 2011.

[10] I. Kaplansky. *Rings of Operators*. Benjamin, 1968.

[11] O. Mathieu. Some Conjectures about Invariant Theory and Their Applications, Algebre non commutative, groupes quantiques et invariants. *Soc. Math. France*, **2**: pp. 263–279, 1997.

[12] M. S. Montgomery. Left and right inverses in group algebras. *Bull. Amer. Math. Soc.*, **75**: pp. 539–540, 1969.

[13] I. Newton. Letter to Oldenburg dated 1676 Oct 24. *The correspondence of Isaac Newton*, II: pp. 126–127, 1960.

[14] V.A. Puiseux. Recherches sur les fonctions algébriques. *J. Math. Pures Appl.*, 15: pp. 365–480, 1850.

[15] V.A. Puiseux. Nouvelles recherches sur les fonctions algébriques. *J. Math. Pures Appl.*, 16: pp. 228–240, 1851.

[16] W. Zhao. Mathieu Subspaces of Associative Algebras. *Journal of Algebra*, **350**: pp. 245–272, 2010.

[17] W. Zhao and R. Willems. An analogue of the Duistermaat-Van der Kallen theorem for group algebras. *Central European J. of Math.*, **10**: pp. 974–986, 2012.