On the integer matrix conjugacy problem and p-adic numbers

Alberto Cavaleiro Pacheco

Thesis to obtain the Master of Science Degree in

Mestrado em Matemática e Aplicações

Supervisor: Prof. Pedro Martins Rodrigues

Examination Committee

Chairperson: Prof. Pedro Resende
Supervisor: Prof. Pedro Martins Rodrigues
Members of the Committee: Prof. Lennard F. Bakker

October 2021

"Se calhar a verdadeira tese foram os amigos que fizemos pelo caminho"

Acknowledgements

As everyone I'll be mentioning is Portuguese, I will proceed in our common mother-tongue.

Muito obrigado ao meu orientador, o Professor Pedro Martins Rodrigues, por me ter arranjado algo giro para fazer e pela paciência e disponibilidade para me ajudar com isso ao longo de toda a jornada.

Obrigado à Mariana, por me ter ensinado FLTC, desde os T's com tracinhos até aos triângulos. Ao meu pai por me ter trazido para o Técnico e à minha mãe por me deixar voltar a casa. Ao Rafa, por me mandar memes horríveis consistentemente. Um pedido de desculpas à Ritinha, que nunca chegou a entender muito bem o porquê de eu ter estado mais ausente durante dois anos.

Obrigado ao Bruno pela companhia durante as ceias (agradecimento dividido também pelos bichinhos de conta), à Gabi pelas palavras sábias e à Miau por toda a companhia. Mais geralmente, obrigado aos amigos que fizemos pelo caminho, pela constante existência e por terem sido o que mais houve de normal neste último ano.

Obrigado ao Eira, por me ter deixado acabar a tese dele para ganhar confiança, à Da pelas chamaDas, e ao Rêgo por me mandar bons memes consistentemente.

Derradeiramente, a todos os amigos com os quais não consigo pôr em poucas palavras o que quero agradecer (ou só não o quero explicitar num documento publicamente acessível, como no caso do Jibu), obrigado pela vossa existência.

Finalmente, de forma não relacionada com o resto dos agradecimentos, obrigado ao Vice-Almirante Gouveia e Melo e à Task Force pela eficiência do processo de vacinação.

Abstract

The conjugacy problem in $GL(n,\mathbb{Z})$ is mostly an open problem. Studying the p-adic numbers and the conjugacy problem over matrices with p-adic integer entries, we try to hopefully discover something about its integer counterpart, either by some analog of the local-global principle or by noticing invariants that manifest themselves on the action of integer matrices over other $\mathbb{Z}$-modules, such as the p-adic integers. In this work, we present a generalization of the Lifting the Exponent Lemma for p-adic matrices, we count the number of minimal sets induced by automorphisms of vector spaces over the p-adic numbers and we characterize the Bowen-Franks groups of endomorphisms over those spaces.

Keywords: conjugacy problem, integer matrices, p-adic numbers, lifting the exponent lemma

Resumo

O problema da conjugação em $GL(n, \mathbb{Z})$ é, na sua maioria, um problema em aberto. Através do estudo dos números p-ádicos e do problema da conjugação sobre as matrizes com entradas nos inteiros p-ádicos, tentamos descobrir algo sobre o problema correspondente sobre os inteiros, seja através de algo análogo ao princípio local-global ou através do descobrimento de invariantes que se revelam na ação de matrizes inteiras sobre outros $\mathbb{Z}$-módulos, como os próprios inteiros p-ádicos. Neste texto, apresentamos uma generalização do Lema do Levantamento do Expoente para matrizes p-ádicas, contamos o número de conjuntos minimais induzidos por automorfismos de espaços vetoriais sobre os números p-ádicos e caracterizamos os grupos de Bowen-Franks dos endomorfismos sobre esses espaços.

Palavras-Chave: problema da conjugação, matrizes inteiras, números p-ádicos, lema do levantamento do expoente

Contents

Part I

Introduction and Preliminaries

Chapter 1

Introduction

The conjugacy problem in $GL(n, \mathbb{Z})$ is far from a recent problem. This decision problem consists on trying to answer the following question: given two integer matrices A, B, when is there an invertible matrix C such that $AC = CB$?

Studying the conjugacy problem in $GL(n, K)$, where K is a field, amounts to simply discovering the Frobenius Normal Form [Sto98] of the matrices we're trying to compare and checking if it is the same [DF91][1].

That isn't the case when we're considering matrices with entries over a ring which isn't a field. The apparent harmfulness that may emanate from considering matrices over the integers instead of over any given field is nothing but a mere illusion. This problem, just like many others that seem absolutely harmless at first sight, has survived many years of near-constant attacks, as it is to be expected of a problem that's about answering such an easy to understand question but hasn't yet been solved.

Here, when we discuss "solving" the conjugacy problem, we mean doing so in an "elegant" way, from an aesthetic standpoint. There have been legitimate solutions of this problem [EHO19], but they have consisted in strenuous algorithms and not in any form of succinct characterization of the conjugacy classes, for instance.

Hence, our motivation for this work is mostly trying to pursue more aesthetically pleasing results about the conjugacy problem in $GL(n, \mathbb{Z})$.

We try to achieve that purpose by studying fields akin to the fields of p-adic numbers (and the fields of p-adic numbers as well) and the actions of linear endomorphisms over modules over their respective rings of integers, in search of conjugacy invariants. The hope that there can be elegant results within these problems arises from works such as [AO81] and [AO83], which we'll study later during our work.

[1] On section 12.2

Chapter 2

The p-adic numbers

We begin by listing all preliminary results we find appropriate about the p-adic numbers. We do so by presenting what might be considered a rather short course on that theme, which will in theory be enough to easily follow the following chapters.

In order to study these results and see some proofs we might have skipped or simply study this subject on a deeper level than we presented, one might want to take a look at [Cas86] or [Gou91], which cover all of the standard results we present.

2.1 Absolute Values on a Field

2.1.1 Definitions and basic properties

We start off by defining an *absolute value* on a given field. Let $\mathbb{R}^+$ be the set of nonnegative real numbers.

Definition 2.1.1 (**Absolute value in a field**). *Let K be a field. An absolute value on K is a function*

$$|\cdot| : K \to \mathbb{R}^+$$

that satisfies the following conditions:

- *Given $x \in K$, $|x| = 0 \Leftrightarrow x = 0$*
- $|xy| = |x| \cdot |y|$*, for all $x, y \in K$ **(multiplicativity)***
- $|x + y| \leq |x| + |y|$*, for all $x, y \in K$ **(triangle inequality)***

If K is a field and $|\cdot|$ an absolute value defined in it, we say $(K, |\cdot|)$ is a *valued field*. In situations where it's obvious to understand which absolute value we are talking about, we might instead just say that K is a valued field.

We might have a look at the following examples of valued fields:

- Each one of $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with the usual absolute value forms a valued field

- Given a field K, consider $|\cdot|$ such that:

  $$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$$

  This does form a valued field and this absolute value is known as the *trivial absolute value*.

Lemma 2.1.2. *Given a valued field $(K, |\cdot|)$, we have:*

i) $|1| = 1$

ii) *If $x \in K$ and n is a positive integer such that $|x^n| = 1$, $|x| = 1$. In particular, $|-1| = 1$*

iii) *If $x \in K$, $|-x| = |x|$*

iv) *If K is finite, $|\cdot|$ is trivial*

Proof. i) $|1| = |1| \times |1|$, thus we have $|1| = 0$ or $|1| = 1$. However, $1 \neq 0$ and therefore $|1| = 1$.

ii) If $x^n = 1$, $1 = |1| = |x^n| = |x|^n$, which lets us conclude that $|x| = 1$.

iii) By *ii)*, $|-1| = 1$ and so we get that $|-x| = |-1| \times |x| = |x|$.

iv) If K is finite, for all nonzero $x \in K$ there's a positive integer n such that $x^n = 1$. Thus all nonzero elements of K have 1 as their absolute value, while 0's absolute value must be zero.

□

Definition 2.1.3 (Metric space)**.** *A metric space is a set S together with a distance function $d : S \times S \to R^+$ that satisfies:*

- $d(x, y) = 0 \Leftrightarrow x = y$
- $d(x, y) = d(y, x)$*, for all* $x, y \in S$
- $d(x, y) \leq d(x, z) + d(z, y)$*, for all* $x, y, z \in S$

From a valued field $(K, |\cdot|)$ it's easy to get a metric space when we consider the distance between two points to be the absolute value of their difference. More specifically,

$$d : K \times K \to \mathbb{R}^+$$
$$(x, y) \mapsto |x - y|$$

induces a distance in K and clearly also induces a topology in K. We'll be interested in studying these objects particularly when the absolute values satisfy an extra condition.

Definition 2.1.4 (Non-Archimedean absolute value)**.** *An absolute value is said to be non-archimedean if it satisfies the ultrametric inequality*

$$|x + y| \leq \max\{|x|, |y|\}$$

Otherwise, we say it is Archimedean.

Note that the ultrametric inequality, as the name suggests, is stronger that the metric inequality.

We'll come back to these later (as the p-adic abolute value is indeed non-archimedean).

Going back to the fact that an absolute value induces a topology on the field where it's defined, it's natural to ask when two absolute values induce the same topology. That's the question we'll now answer.

Definition 2.1.5. *Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are said to be equivalent if they induce the same topology on K.*

Lemma 2.1.6. *Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on a field K. The following conditions are equivalent:*

i) $|\cdot|_1$ *and* $|\cdot|_2$ *are equivalent;*

ii) *for all $x \in K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$;*

iii) *there's a positive real number α such that $|x|_2 = |x|_1^\alpha$ for all $x \in K$.*

And with this we finish our short journey about what we consider to be the most relevant basic properties of absolute values.

2.1.2 Absolute Values in $\mathbb{Q}$

Now that we've introduced this concept, it may be time to study its behaviour on some interesting cases. The first fields that may come to our minds are finite fields and $\mathbb{Q}$. However, albeit one could guess that absolute values on finite fields could be of interest, that is not the case. Absolute values defined in them aren't interesting at all, as it was showed in Lemma 2.1.2. That leaves us with $\mathbb{Q}$[1].

In this chapter we'll focus on listing all absolute values on $\mathbb{Q}$ up to equivalence by showing a result known as **Ostrowski's theorem**.

We already know about the trivial absolute value (which isn't of much interest) and the usual absolute value in $\mathbb{Q}$, but are there any others?

Definition 2.1.7 (p-adic valuation)**.** *Given a prime $p \in \mathbb{N}$, and $x \in \mathbb{Q}$, we can write $x = p^n \frac{a}{b}$ where $p \nmid ab$. Fixed x, n doesn't depend on the choice of a and b and we call it the p-adic valuation of x, noted $v_p(x)$.*

In the case of $x = 0$, we take ∞ as its valuation.

These valuations are, as we'll now see, precisely where the other absolute values on $\mathbb{Q}$ come from. Let's take a look at those absolute values:

Definition 2.1.8 (p-adic absolute value)**.** *Given a prime $p \in \mathbb{N}$, the p-adic absolute value is the function*

$$\begin{aligned} |\cdot|_p : \mathbb{Q} &\to \mathbb{R}^+ \\ x &\mapsto p^{-v_p(x)} \end{aligned}$$

Where we consider $p^{-\infty}$ to be 0.

[1] That is, if we're talking about the simplest fields we can find

There's no reason to instantly believe this really is an absolute value, but as we can and will show, it is not only an absolute value but also a non-archimedean one. In order to do so, first we must notice a few properties of the p-adic valuation.

Lemma 2.1.9. *Given a prime $p \in \mathbb{N}$, we have that for all $x, y \in \mathbb{Q}$:*

- $v_p(x) = \infty \Leftrightarrow x = 0$
- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

Proof. Let's prove each statement.

- Trivial.
- $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$, where $p \nmid ab$ and $p \nmid cd$. Thus we have that $xy = p^{v_p(x)+v_p(y)}\frac{ac}{bd}$, where $p \nmid (ac)(bd)$, which leaves us with the fact that $v_p(xy) = v_p(x) + v_p(y)$.
- $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$, where $p \nmid ab$ and $p \nmid cd$. Let $m = \min\{v_p(x), v_p(y)\}$. $x + y = p^{v_p(x)}\frac{a}{b} + p^{v_p(y)}\frac{c}{d} = p^m \times \frac{p^{v_p(x)-m}ad + p^{v_p(y)-m}cb}{bd}$, where it's clear (using the previous statement in this lemma) that $v_p(x+y) = m + v_p(p^{v_p(x)-m}ad + p^{v_p(y)-m}cb) \geq m = \min\{v_p(x), v_p(y)\}$.

□

With these results, we can now easily prove that the p-adic absolute value is indeed an absolute value (and a non-archimedean one, more specifically).

Lemma 2.1.10. *Given a prime $p \in \mathbb{N}$, $|\cdot|_p$ is such that, for all $x, y \in \mathbb{Q}$:*

- $|x|_p = 0 \Leftrightarrow x = 0$
- $|xy|_p = |x|_p \times |y|_p$
- $|x+y|_p \leq \max\{|x|_p, |y|_p\}$

Proof. Once again, we'll prove each statement individually, this time getting some inspiration for each of them from the respective statement of the previous lemma.

- Here we have $|x|_p = 0 \Leftrightarrow p^{-v_p(x)} = 0 \Leftrightarrow v_p(x) = \infty \Leftrightarrow x = 0$.
- If $xy = 0$, it's trivial. Otherwise we have $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p \times |y|_p$
- If $xy = 0$, it's once again trivial. Otherwise, taking $m = \min\{v_p(x), v_p(y)\}$, we get $|x+y|_p = p^{-v_p(x+y)} \leq p^{-m} = \max\{|x|_p, |y|_p\}$, just as we wanted to prove.

□

Now that we're fully convinced that these are indeed absolute values on $\mathbb{Q}$, we can finally move on to stating Ostrowski's Theorem.

Theorem 2.1.11 (**Ostrowski's Theorem**)**.** *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. $|\cdot|$ is either equivalent to $|\cdot|_\infty$ or to $|\cdot|_p$ for some prime p.*

This is a pretty interesting characterization of the absolute values on $\mathbb{Q}$ and their respective induced topologies. After reaching this point, and being $(\mathbb{Q}, |\cdot|_\infty)$ a too widely studied metric space, the next step can only be studying its non-archimedean counterparts.

2.1.3 Non-Archimedean absolute values

Our objective is to study the metric and topological spaces we get from $\mathbb{Q}$ when taking into account a p-adic absolute value as the foundation of its distance function, but before doing so it might prove itself useful to take a short tour through non-archimedean metric spaces in general.

These metric spaces really do have some appeal of their own, as they verify a few properties one would deem unintuitive. For instance, there's a known "proof" in Euclidean geometry that all triangles are isosceles. In non-archimedean metric spaces, we don't have to trick anyone to prove such a thing because all triangles really are isosceles!

Proposition 2.1.12. *Let $|\cdot|$ be a non-archimedean absolute value on a field K. If $x, y \in K$ and $|x| \neq |y|$, we have that $|x+y| = \max\{|x|, |y|\}$*

Proof. Without loss of generality, $|x| < |y|$. By the ultrametric inequality over x, y we have that $|x+y| \leq \max\{|x|, |y|\} = y$. On the other hand, $y = (x+y) + (-x)$, so once again by the ultrametric inequality we have $|y| \leq \max\{|x+y|, |x|\}$, but $|y| > |x|$ so $|y| \leq |x+y|$. Thus $|y| = |x+y|$. □

As we just proved, any triangle must be isosceles! But that's just the start of the "weirdness" brought upon us by non-archimedean absolute values:

Proposition 2.1.13. *Let K be a field with a non-archimedean absolute value $|\cdot|$ and an induced metric d. Let $a, b \in K$, $s, r \in \mathbb{R}^+$.*

i) *If $b \in B(a,r)$, $B(a,r) = B(b,r)$. This is, every point in an open ball is a center of that ball.*

ii) *If $b \in \bar{B}(a,r)$, $\bar{B}(a,r) = \bar{B}(b,r)$. This is, every point in a closed ball is a center of that ball.*

iii) *The set $B(a,r)$ is both open and closed.*

iv) *If $r \neq 0$, the set $\bar{B}(a,r)$ is both open and closed.*

v) *$B(a,r) \cap B(b,s) \neq \emptyset$ if and only if ($B(a,r) \subseteq B(b,s)$ or $B(a,r) \supseteq B(b,s)$. Two open balls are either disjoint or contained in one another.*

vi) *$\bar{B}(a,r) \cap \bar{B}(b,s) \neq \emptyset$ if and only if ($\bar{B}(a,r) \subseteq \hat{B}(b,s)$ or $\bar{B}(a,r) \supseteq \bar{B}(b,s)$. Two closed balls with non-zero radius are either disjoint or contained in one another.*

Proof. i) Let $c \in B(a,r)$. $d(a,c) < r > d(a,b)$ so, by the ultrametric inequality, $d(b,c) \leq \max\{d(a,c), d(a,b)\} < r$. $B(a,r) \subseteq B(b,r)$. Similarly we get $B(a,r) \supseteq B(b,r)$ and thus $B(a,r) = B(b,r)$.

ii) The same as the item above, swapping the strict inequalities by non-strict inequalities.

iii) It's obviously an open set. Now let's prove $K \setminus B(a,r)$ is open. If $c \in (K \setminus B(a,r))$, $d(a,c) \geq r$. We can now try to prove that $B(a,r) \cap B(c,r) =$. Suppose there is $x \in B(a,r) \cap B(c,r)$. Then, $d(a,c) \leq \max\{d(x,a), d(x,c)\} < r$, which contradicts the initial statement. So we conclude that $B(a,r)$ is also closed.

iv) As it is trivial the closed ball is a closed set, all we have to prove it that it is also open. But by **ii)** it's pretty easy to see that's the case as if $c \in \bar{B}(a,r)$, $B(c,r) \subseteq \bar{B}(c,r) = \bar{B}$.

v) If the balls aren't disjoint, there's a $c \in B(a,r) \cap B(b,s)$. By **i)**, $B(a,r) = B(c,r)$ and $B(b,s) = B(c,s)$ and the statement follows from this fact.

vi) If the balls aren't disjoint, there's a $c \in \bar{B}(a,r) \cap \bar{B}b,s)$. By **ii)**, $\bar{B}(a,r) = \bar{B}(c,r)$ and $\bar{B}(b,s) = \bar{B}(c,s)$ and the statement follows from this fact.

□

We'll finish this section by proving a result regarding a non-archimedean valued field's connectedness.

Proposition 2.1.14. *Let K be a field with a non-archimedean absolute value $|\cdot|$ and an induced metric d. K is fully disconnected regarding d, as its connected components are the ones of the form $\{x\}$, with $x \in K$.*

Proof. To prove this, we must prove that each set containing two different points must be disconnected. Let $A \subseteq K$ and $x, y \in A$ such that $x \neq y$. Let $r = d(x,y)/2$. As $d(x,y) > 0$, we know that $r > 0$ and so $B(x,r)$ is both open and closed, and so is its complement. Furthermore, we know that $x \in B(x,r)$ and $y \notin B(x,r)$. This means that A can be written as the disjoint union of two open subsets: $A \cap B(x,r)$ and $A \setminus B(x,r)$. Therefore, A is disconnected. □

These notions will be relevant later, especially when we focus on the topology of the spaces we are considering.

With this we conclude our short chapter on general facts about non-archimedean absolute values.

2.1.4 Completions

We know about some of these metric spaces' topological properties, but one we still haven't discussed is their completeness. For instance, given a prime p and $\mathbb{Q}$ with the p-adic absolute value, we can take a look at $(x_n)_{n\in\mathbb{N}}$ where $x_n = \sum_{i=0}^{n} p^i$. This sequence is a Cauchy sequence but it doesn't take much effort to notice it doesn't converge to any integer or even rational number.

But if this space isn't complete, we can complete it, as it is widely known (one can check Proposition 6.2.23 in [Mor89] in order to believe this general statement). However, does this completion have a good enough structure?

Proposition 2.1.15. *Let $\mathbb{Q}_p$ be the completion of $(\mathbb{Q}, |\cdot|_p)$. $\mathbb{Q}_p$ is also a field and $|\cdot|_p$ can be extended to $\mathbb{Q}_p$.*

Proof. Can be found on the section starting at page 47 in [Gou91] □

What's important to note is that not only do we keep our field structure when completing $\mathbb{Q}$, but also we don't even have to extend the image of the absolute value, as for each element of $\mathbb{Q}_p$ there's an element of $\mathbb{Q}$ that has the same absolute value.

2.2 The p-adic numbers and other valued fields

2.2.1 Algebra

We began our first chapter by defining absolute values on a field and eventually coming to a definition of the corresponding valuation. Now we intend to study the algebraic properties of a valued field, and in order to do so we'll start by defining a valuation over a given field. This is in no way different from starting from the absolute value, but it just feels smoother to follow this route.

Definition 2.2.1 (Valuation over K)**.** *A function $v : K \to \mathbb{R} \cup \{\infty\}$ is said to be a valuation if it satisfies, for all $x, y \in K$:*

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

This is currently no more than an attempt of generalizing our well known p-adic valuation. As we'll soon be able to see, most of our beloved properties do not depend on the magic of the prime numbers, but rather on the behaviour of *discrete* valuations over fields.

About that *discreteness* we just referred, let us notice that, given a valued field K and its valuation v, $v(K)$ must be an additive subgroup of $\mathbb{R}$. These can be of three kinds:

- Trivial, when they're simply $\{0\}$
- Discrete[2], when they're of the form $\alpha\mathbb{Z}$ for $\alpha \in \mathbb{R} \setminus \{0\}$
- Dense in $\mathbb{R}$

We'll be focusing on the second case and we'll omit the *discrete* on any description. If at any point we refer to a valuation that isn't discrete, it'll be pointed out.

Definition 2.2.2 (Normalized valuation)**.** *A valuation v on a field K is said to be normalized if $v(K^\times) = \mathbb{Z}$.*

Note that in $\mathbb{Q}_p$ that was the case of our chosen valuation, v_p.

Unless we suggest otherwise, from now on we'll assume our valuations to be normalized. There will be a moment when that will not happen but it will be absolutely clear when that's the case.

[2] The trivial subgroup is discrete as well, but it seemed legitimate to make the distinction between that and the general discrete case.

Definition 2.2.3 (Uniformizer)**.** *An element $\pi \in K$ is said to be a uniformizer if $v(\pi) = 1$.*

In $\mathbb{Q}_p$, p was a possible uniformizer, as well as any other element of $\mathbb{Q}_p$ that had 1 as its valuation.

Proposition 2.2.4. *Let K be a field with a normalized valuation v. Then we have that*

$$\mathcal{O}_K = \{x \in K : v(x) \geq 0\}$$

is a subring of K. We call it the subring of integers of K.

Proof. $0 \in \mathcal{O}_K$. After noticing this, we only have to notice that this subset is closed for addition and multiplication, which is a direct consequence of the second and third properties of a valuation. □

In the p-adic case, we'd be talking about $\mathbb{Z}_p$.

Proposition 2.2.5. *The group of units in $\mathcal{O}_K$, $\mathcal{O}_K^\times$ is $\{x \in \mathcal{O}_K : v(x) = 0\}$.*

Proof. If $v(x) > 0$, we know that $x^{-1} \in K \setminus \mathcal{O}_K$, as $v(x^{-1}) < 0$. If $v(x) = 0$, $x^{-1} \in K$ we be such that $v(x^{-1}) = 0$ as well, so it'll be in $\mathcal{O}_K$. □

This allows us to get the factorizations of the integers and even the other elements of K.

Corollary 2.2.6. *Let $x \in K$ and let π be a uniformizer. Then there's a unique factorization $x = \pi^n \times u$, where $u \in \mathcal{O}_K^\times$.*

With this corollary in mind we'll characterize the ideals of $\mathcal{O}_K$.

Proposition 2.2.7 (Ideals of $\mathcal{O}_K$)**.** *The ideals of $\mathcal{O}_K$ are $\{0\}$ and the ones of the form $\pi^n\mathcal{O}_K$, with n a non-negative integer.*

Proof. It's clear that these are indeed ideals. What's left to show is simply that these are all the ideals there are. Let $I \subseteq \mathcal{O}_K$ be a non-trivial ideal. Let $x \in I$ such that x's valuation n is minimal in I. $x = \pi^n \times u$, thus $x \times u^{-1} = \pi^n$ must be in I, and therefore I must be equal to $\pi^n\mathcal{O}_K$. □

Corollary 2.2.8. *$\pi\mathcal{O}_K$ is the only maximal ideal of $\mathcal{O}_K$.*

As we have a maximal ideal, we can define the residue field:

Definition 2.2.9. *The field $r_K = \mathcal{O}_K/(\pi\mathcal{O}_K)$ is called the residue field of K.*

For instance, in $\mathbb{Q}_p$ the residue field would be $\mathbb{F}_p$.

Although we have described quite a few properties of these fields, their elements may still seem an odd sight to behold. Gladly, even though those elements might appear frightening at first, that really isn't the case. In order to clearly see that, we just have to take a look at the following process, for now applied to an element of $\mathbb{Z}_p$:

Let $x_0 \in \mathbb{Z}_p$. From this, we obtain two numbers that spark our interest: the remainder modulo p of x_0, the integer $0 \leq r_0 < p$ such that $x_0 \in r_0 + p\mathbb{Z}_p$; and $x_1 = (x_0 - r_0)p^{-1}$ (which is well defined, as $x_0 - r_0 \in p\mathbb{Z}_p$). From x_1, we repeat this process, obtaining r_1 and x_2, and may repeat this same process *ad infinitum*.

From this process we obtain a sequence of non-negative integers, none of them greater than $p-1$, $(r_i)_{i\in\mathbb{N}_0}$[3], that allows us two find a "meaning" to the elements of $\mathbb{Z}_p$.

We can view x as a power series on p:

$$x = \sum_{i=0} r_i p^i$$

Lemma 2.2.10. *Let p be a prime number, $x_0 \in \mathbb{Z}_p$ and $(r_i)_{i\in\mathbb{N}_0}$ obtained from the process above.*

$$x = \sum_{i=0} r_i p^i$$

Proof. Let, for $N \in \mathbb{N}_0$, $S_N = x = \sum_{i=0}^{N} r_i p^i$. We claim that, for $N \in \mathbb{N}$, $x_N = (x_0 - S_{N-1})p^{-N}$.

For $N = 1$, it's clear from the definition of r_0 and x_1, indeed $x_1 = (x_0 - r_0)p^{-1} = x_1 = (x_0 - S_0)p^{-1}$.

If our claim is true for some N, then for $N+1$ we have that

$$\begin{aligned} x_{N+1} &= (x_N - r_N)p^{-1} = \\ &= ((x_0 - S_{N-1})p^{-N} - r_N)p^{-1} = \\ &= ((x_0 - S_{N-1}) - r_N p^N)p^{-(N+1)} = \\ &= (x_0 - S_N)p^{-(N+1)} \end{aligned}$$

which means the claim is true for $N+1$ as well.

But we know that all of the r_i and x_i are elements of $\mathbb{Z}_p$, which means that, for $N \in \mathbb{N}$, $x_0 - S_{N-1} \in p^N\mathbb{Z}_p$, which means that $|x_0 - S_{N-1}| \le p^{-N}$. Thus we conclude that the partial sums converge to x_0 and the lemma's equality holds.

□

As we can see, this isn't in any way disingenuous, as this equality is absolutely legitimate in $\mathbb{Z}_p$ and the partial sums do converge to x. Thus this way of viewing elements of $\mathbb{Z}_p$ is not only intuitive but also actually formally legitimate.

It is also possible to view elements in a different, even if related, way. Recalling the way of viewing the we've already referred, we can view an element $x = \sum_{i=0} r_i p^i$ as the limit of these series' partial sums. We can note that the the partial sum corresponding to the first N terms, noted S_N will always be an integer in the interval $[0, p^N[$. We can also note that if $N < M$ are positive integers, $S_N \equiv S_M(\mod, p^N)$.

What this allows us to conclude is that we can view an element $x \in \mathbb{Z}_p$ as a coherent sequence in the finite quotients of $\mathbb{Z}_p$, i.e. a sequence $(x_n)_{n\in\mathbb{N}}$ such that, for each natural number n, x_n is an element of $\mathbb{Z}_p/(p^n\mathbb{Z}_p)$ and if $n < m$ are natural numbers, the canonical projection from $\mathbb{Z}_p/(p^m\mathbb{Z}_p)$ to $\mathbb{Z}_p/(p^n\mathbb{Z}_p)$ maps x_m into x_n.

Once again, it seems a little disingenuous to present this last interpretation of elements of $\mathbb{Z}_p$, as we're trying to "define" $\mathbb{Z}_p$, but already using its finite quotients on that alleged definition. This is in no way an issue, as,for any natural number n, $\mathbb{Z}_p/(p^n\mathbb{Z}_p)$ and $\mathbb{Z}/(p^n\mathbb{Z})$ are isomorphic.

[3] $\mathbb{N}_0$ is, for us, the set of non-negative integers

Therefore, this last interpretation of $\mathbb{Z}_p$ is simply the one obtained by looking at $\mathbb{Z}_p$ as the inverse limit of the finite rings $\mathbb{Z}/(p^n\mathbb{Z})$[4].

It may seem like our interpretations of elements of discrete valued fields are a little lackluster, as we've only presented them for elements of $\mathbb{Z}_p$, but we can easily extend this interpretation to elements of $\mathbb{Q}_p$ and then to elements of any discrete valued field K.

In order to perform the first extension, we simply have to recall that an element $x \in \mathbb{Q}_p$ can always be written as $x = up^{v_p(x)}$, where $x \in \mathbb{Z}_p^\times$.

Lemma 2.2.11. *Let $x \in \mathbb{Q}_p$ be such that $x = u \times p^n$, for some $u \in \mathbb{Z}_p$ and $n \in \mathbb{Z}$. If*

$$u = \sum_{i=0} r_i p^i$$

where $r_i \in \{0, \dots, p-1\}$ for all i, then we must have

$$x = \sum_{i=0} r_i p^{n+i}$$

If n is a negative number and we're actually talking about $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ this means we can write x as a Laurent series in p, starting from the index $v_p(x)$. Thus we have solved the problem of "viewing" the elements of $\mathbb{Q}_p$.

But what do we do in a more general case? In the previous interpretation, the integers $1, 2, \dots, p-1$ had a major role, but there was nothing preventing us from using other class representatives of the cosets $x + p\mathbb{Z}_p$. In the same way, we can now simply consider a set R of representatives of the cosets in r_K, and view the elements of $\mathcal{O}_K$ (respectively, K) as power series (respectively, Laurent series) in a uniformizer π with coefficients in R.

Lemma 2.2.12. *Let K be a local field, π a uniformizer and $x \in \mathcal{O}_K$. Let R be a set of representatives of r_K (this is, for each element $r + \mathcal{O}_K \in r_K$, there's exactly one element $r' \in r + \mathcal{O}_K$ in R).*

$$x = \sum_{i=0} r_i \pi^i$$

for some $n \in \mathbb{Z}$ and $(r_i)_{i \in \mathbb{N}_{\geq n}}$ such that $r_i \in R$ for all $i \geq n$.

Using the proof from 2.2.10 and replacing what should be replaced (p by π, those remainders by coset representatives) we obtain the proof of this lemma, and analogously we may extend this result to the entirety of K and not simply its ring of integers.

As we know $\mathcal{O}_K$ exists, we may "cheat" a little and note that it must be the inverse limit of the quotients $\mathcal{O}_K/(\pi^n\mathcal{O}_K)$. We say we're cheating because those quotients, unlike the ones of the form $\mathbb{Z}/(p^n\mathbb{Z})$, might be a little harder to come across. Thus we're finding an alternate definition of $\mathcal{O}_K$ based on its own quotient sets, which feels a little bit like cheating.

We should note that, given a fixed R, this representation of elements of K as a Laurent series is unique (something that can't be said about the usual decimal representation of rational numbers, for

[4] For more information on this subject, check Section 1.3 in [Rib12]

instance) and that gives us an easy way of counting the number of elements in a local field. In the case where r_K is finite, which is what we will be considering most of the time, we must have that the cardinality of K is equal to $2^{\aleph_0}$, the cardinality of the continuum.

And after all we've shown and talked about regarding the properties and interpretations of valued fields, our small tour through their most general properties has come to an end.

2.2.2 Hensel's Lemma

Finding out whether a certain polynomial has real roots or not isn't always a trivial task in $\mathbb{R}$ but there are some cases where we're able to conclude that is the case and, generally, even find arbitrarily good approximations of some of its roots. For instance, noticing that polynomials are continuous functions and putting ourselves in the conditions of the Intermediate value theorem, where we have a certain interval where its endpoints have images with opposite signs through that polynomial. Afterwards, we might just iterate a binary search algorithm until we have a good enough approximation of one of its roots.

In non-archimedean valued fields, this exact idea doesn't work (the notion and connectedness of intervals is necessary for the previously referred theorem), but there still are occasions where we can conclude a certain polynomial has roots and approximate them as much as we'd like to. Hensel's Lemma is an example of a result regarding that theme.

More precisely, Hensel's Lemma is a result about the factorization of certain polynomials and even about our ability to find some of their roots in $\mathcal{O}_K$.

Theorem 2.2.13. *Let K be a complete discrete valued field and π a uniformizer.*

Let $f \in \mathcal{O}_K[X]$ be a polynomial. Let g_1, h_1 be coprime polynomials in $O_K[X]$ such that $g_1 h_1 \equiv f \pmod{\pi}$ and g_1 is monic.

Then there are $g, h \in \mathcal{O}_K[X]$ such that $g \equiv g_1 \pmod{\pi}$ and $h_1 \equiv h \pmod{\pi}$, g is monic and has the same degree as g_1, and $f = gh$.

Proof. Let $d = \deg f$ and $m = \deg g$. In order to prove this theorem, we'll look for two sequences of polynomials, $(g_n(X))_{n\in\mathbb{N}}$ and $(h_n(X))_{n\in\mathbb{N}}$ that satisfy the following conditions:

- Each g_n is monic and has degree m, while each h_n has degree not greater than $d - m$
- $g_{n+1} \equiv g_n \pmod{\pi^n}$ and $h_{n+1} \equiv h_n \pmod{\pi^n}$
- $f \equiv g_n h_n \pmod{\pi^n}$

This also implies that each g_n must have the same degree as g_1. The limits of these sequences shall be our g and h. Now we must show we can indeed find such a sequence. We will do so by induction.

Assume we already have the first n terms in our sequence, satisfying the properties we've listed. We want to find out what should be our choice for g_{n+1} and h_{n+1}. We must have the following conditions:

$$\begin{aligned} g_{n+1} &= g_n + \pi^n r_n \\ h_{n+1} &= h_n + \pi^n s_n \\ f &\equiv g_{n+1}h_{n+1} (\mod \pi^{n+1}) \end{aligned}$$

For some polynomials $r_n, s_n \in \mathcal{O}_K$. We already have, by our induction hypothesis, that $f \equiv g_n h_n (\mod \pi^n)$, or, equivalently, that there's a polynomial $t_n \in \mathcal{O}_{\mathcal{K}}$ such that $f = g_n h_n + \pi^n t_n$. We'll intend to choose r_n and s_n such that the third condition is satisfied. Let us do some calculations.

$$\begin{aligned} f &\equiv_{\pi^{n+1}} (g_n + \pi^n r_n)(h_n + \pi^n s_n) \equiv_{\pi^{n+1}} \\ &\equiv_{\pi^{n+1}} g_n h_n + \pi^n r_n h_n + \pi^n s_n g_n + \pi^{2n} r_n s_n \equiv_{\pi^{n+1}} \\ &\equiv_{\pi^{n+1}} g_n h_n + \pi^n (r_n h_n + s_n g_n) \end{aligned}$$

We know there is a t_n such that $f = g_n h_n + \pi^n t_n$, so we may proceed:

$$\begin{aligned} f &\equiv_{\pi^{n+1}} g_n h_n + \pi^n (r_n h_n + s_n g_n) \equiv_{\pi^{n+1}} \\ \pi^n t_n &\equiv_{\pi^{n+1}} \pi^n (r_n h_n + s_n g_n) \end{aligned}$$

Dividing both sides by π^n, we get the following:

$$t_n \equiv r_n h_n + s_n g_n (\mod \pi)$$

Well, now our proof is clearly almost over, as we certainly are able to choose r_n and s_n that satisfy this congruence, as the reductions of g_n and h_n are coprime modulo π, but our choices must still be somewhat careful, in order to maintain our conditions about the polynomials' degrees (and only because of that, as the conditions related to congruences have been met).

Let R_n and S_n be polynomials satisfying $t_n \equiv R_n h_n + S_n g_n (\mod \pi)$, and let $R_n = g_n q_n + r'_n$, for some polynomials $q_n, r'_n \in \mathcal{O}_K[X]$, with $\deg r'_n < \deg g_n$. Then, we must have that

$$t_n \equiv r'_n h_n + (S_n + q_n) g_n \tag{*}$$

We'll now see that r'_n and $(S_n + q_n)$ are appropriate choices for r_n and s_n, respectively. By the definition of r'_n, its degree is less than m, so $g_{n+1} = g_n + \pi^n r_n$ will still be monic and with degree m. By the definition of t_n, its degree must not be greater than d, thus by (*), as g_n's degree is m, $s_n = S_n + q_n$ may have degree not greater than $d - m$. This completes our proof of the induction step.

Our base case, $n = 1$, is our theorem's assumption. Thus our proof is complete. □

Generally speaking, this kind of result will be interesting when trying to find solutions of certain polynomial equations.

As such, we also have a similar result about roots of some polynomials.

Lemma 2.2.14. *Let K be a complete discrete valued field and v its normalized valuation function.*

Let $f \in \mathcal{O}_K[X]$ be a polynomial and f' its formal derivative. If there's an $a_0 \in \mathcal{O}_K$ such that

$$v(f(a_0)) > 2v(f'(a_0))$$

then f has a root a in $\mathbb{Z}_p$ such that $v(a - a_0) > v(f(a_0)) - v(f'(a_0))$.

Proof. Equivalently, we have that

$$|f(a_0)| < |f'(a_0)|^2$$

In order to prove this lemma, we'll build a succession using a very famous method from numerical analysis, Newton's method. We will consider the sequence $(a_n)_{n \in \mathbb{N}_0}$, where

- a_0 is the one given in the statement
- $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$

We want to prove that

- $|f'(a_n)| = |f'(a_0)|$, for all $n \in \mathbb{N}$
- $|(f(a_n))| \leq \frac{|f(a_0)|^{2^n}}{|f'(a_0)|^{2^{n+1}-2}} \leq (\frac{|f(a_0)|}{|f'(a_0)|^2})^{2^n-1}$, for all $n \in \mathbb{N}_0$ (particularly, it is decreasing)
- $\frac{f(a_n)}{f'(a_n)} \in \mathcal{O}_K$, for all $n \in \mathbb{N}_0$
- $(a_{n+1} - a_n)$ is decreasing

Assume we have our sequence and that it satisfies the first of these conditions until n. We will prove these three items by induction.

We know we can write $f(X)$ as its own Taylor Series centered in a_n, which means we have

$$f(a_n + Y) = f(a_n) + Yf'(a_n) + Y^2F_n(Y) \tag{*}$$

where $F_n(Y) \in \mathcal{O}_K[X]$. Replacing Y by $-\frac{f(a_n)}{f'(a_n)}$, we get that

$$f(a_{n+1}) = \frac{f(a_n)^2}{f'(a_n)^2}F_n(-\frac{f(a_n)}{f'(a_n)})$$

More specifically, as $\frac{f(a_n)}{f'(a_n)} \in \mathcal{O}_K$ and $F_n(Y) \in \mathcal{O}_K[Y]$

$$\begin{aligned}|f(a_{n+1})| &\leq \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \\ &= \frac{|f(a_n)|^2}{|f'(a_0)|^2} \leq \\ &\leq \frac{|f(a_0)|^{2^{n+1}}}{|f'(a_0)|^{2(2^{n+1}-2)+2}} = \\ &= \frac{|f(a_0)|^{2^{n+1}}}{|f'(a_0)|^{2^{n+2}-2}}\end{aligned}$$

Which concludes the induction step for the second item: until $n+1$ that absolute value is decreasing. For the first item, we may consider differentiating the expressions in (*), obtaining

$$f'(a_n+Y)=f'(a_n)+2YF_n(Y)+Y^2F_n'(Y) \tag{@}$$

Taking, once again, $Y=-\frac{f(a_n)}{f'(a_n)}$, and taking absolute values, we get, from the ultrametric inequality

$$|f'(a_{n+1})|\leq \max\{|f'(a_n)|,|-2\frac{f(a_n)}{f'(a_n)}F_n(Y)+\frac{f(a_n)^2}{f'(a_n)^2}F_n'(-\frac{f(a_n)}{f'(a_n)})|\}$$

with equality when the two absolute values on the right are different. Notice that we're only dealing with elements of $\mathcal{O}_K$, as all of those scary fractions must be elements of that set, by our induction hypothesis.

Also by our induction hypothesis, we know on one hand, that $|f'(a_n)|=|f'(a_0)|$, and on the other hand that $|\frac{f(a_n)}{f'(a_n)}|$, which is an upper bound of the absolute value of the "big looking term" on the right, is such that

$$\begin{aligned}|\frac{f(a_n)}{f'(a_n)}| &= |\frac{f(a_n)}{f'(a_0)}|\leq\\ &= |\frac{f(a_0)}{f'(a_0)}|<\\ &< |f'(a_0)|=|f'(a_n)|\end{aligned}$$

Therefore, we have that $|f'(a_{n+1})|=|f'(a_0)|$.

If the two first items verify the induction step, so does the third: $|\frac{f(a_{n+1})}{f'(a_{n+1})}|=|\frac{f(a_{n+1})}{f'(a_n)}|\leq|\frac{f(a_n)}{f'(a_n)}|\leq 1$, so $\frac{f(a_{n+1})}{f'(a_{n+1})}\in\mathcal{O}_K$.

As $|(f(a_{n+1}))|<|f(a_n|$ is decreasing and $|f'(a_{n+1})|=|f'(a_{n+1})|$ is constant, $|\frac{f(a_{n+1})}{f'(a_{n+1})}|<|\frac{f(a_n)}{f'(a_n)}|$.

Now the base case, $n=0$:

- The first point is trivial.
- $|f(a_0)|\leq\frac{|f(a_0)|}{1}\leq 1$, which is also trivial
- By our hypothesis, $|\frac{f(a_0)}{f'(a_0)}|<|f'(a_0)|\leq 1$, so this one is true as well.
- This one doesn't really need a base case, but we'll state that so it doesn't look like we've forgotten about it

With this we conclude our proof, but let us recall what we've proved. There is a sequence $(a_n)_{n\in\mathbb{N}_0}$ such that:

- It tends to some a in $\mathcal{O}_K$. More specifically, if we have non-negative integers $m>n$, $a_m\equiv a_n(\mod \pi^{\frac{f(a_n)}{f'(a_n)}}$, which means that, by taking $n=0$, we get $v(a-a_0)>v(f(a_0))-v(f'(a_0))$
- Its images through f have decreasing absolute values, so they tend to 0

□

And an even simpler corollary that ends up being used quite often.

Lemma 2.2.15. *Let $f \in \mathcal{O}_K[X]$ be a polynomial and f' its formal derivative. If there's an $a_0 \in \mathcal{O}_K$ such that $f(a_0) \equiv 0 \mod p$ and $f'(a_0) \not\equiv 0 \mod p$ then f has a root a in $\mathbb{Z}_p$ such that $a - a_0 \equiv 0 \mod p$.*

Proof. Trivial by the previous lemma. □

Besides being results that are interesting in themselves, these are results that can be used at any given time and that constitute one of the most relevant peculiarities of the p-adic numbers.

2.2.3 Extending absolute values

We might be interested in studying extensions of non-archimedean valued fields. Specifically, finite and algebraic extensions may appear as rather natural objects to consider. However, there's clearly a question that we need to answer: are those fields non-archimedean valued fields as well?

Yes, they are, but we're going to have to take a short walk across some concepts in order to reach the results we're looking for.

First off, let's define a norm on a vector space over a (not necessarily non-archimedean) valued field:

Definition 2.2.16 (Norm on a vector space)**.** *Let $(K, |\cdot|)$ be a valued field and V a K-vector field. A norm on V is a function $||\cdot|| : V \to \mathbb{R}^+$ such that, for all $v, w \in V$ and $\lambda \in K$:*

i) $||v|| = 0 \Leftrightarrow v = 0$

ii) $||v + w|| \leq ||v|| + ||w||$

iii) $||\lambda v|| = |\lambda| \times ||v||$

Given a norm on V, we can easily define a metric given by the distance function $d : (v, w) \mapsto ||v - w||$.

Definition 2.2.17. *Two norms $||\cdot||_1$ and $||\cdot||_2$ on a vector field V are said to be equivalent if there are positive constants C, D such that, for all $v \in V$,*

$$||v||_1 \leq C||v||_2 \text{ and } ||v||_2 \leq D||v||_1$$

Even if they might induce different metrics (by virtue of being different from one another), two equivalent norms induce the same topology in V. Now for the result we're really interested in:

Theorem 2.2.18. *Let K be a complete valued field and V a finite-dimensional vector space over K. Any two norms on V are equivalent.*

Proof. Found on page 123 of [Gou91]. □

We now know that, in a finite dimensional K-vector space (where K is complete), any norm is equivalent, for instance, to the sup-norm with respect to any basis of the vector space. And that is a pretty nice fact to have in mind, as the sup-norm is a rather simple object to think about.

Proposition 2.2.19. *Let K be a complete valued field, V a K-vector field and $||\cdot||$ a norm on V. V is complete with respect to $||\cdot||$.*

Proof. As we might have previously suggested, the bulk of the proof is the realization that any norm is equivalent to any sup-norm. Taking this into account, we only have to notice V is complete with respect to any given sup-norm.

Let $(v_1, \ldots, v_n)$ be a basis for V and $||\cdot||_{\text{sup}}$ be the sup-norm with respect to that basis. Let us consider a sequence

$$(u_m) = \sum_{i=1}^{n}(a_{im}v_i)$$

The norm of a vector is simply the greatest out of its coefficients, thus (u_m) converges if and only if each of (a_{im}) does so. Specifically,

$$\lim_{m\to\infty} = \sum_{i=1}^{n}((\lim_{m\to\infty} a_{im})v_i)$$

Analogously, (u_m) being a Cauchy sequence is equivalent to all of the (a_{im}) being Cauchy sequences, which we know is equivalent to them being convergent, as K is complete, which is equivalent to (u_m) being convergent. Therefore, V is complete with respect to $||\cdot||_{\text{sup}}$. As any two norms induce the same topology, V is complete with respect to any norm $||\cdot||$ on V. □

Why would this matter? Well, an absolute value is a norm in itself, so if we can effectively extend our absolute value on a complete field to a finite extension of that field, we will have a norm on that extension. That means that that extended absolute value will be pretty well behaved and, most of all, the field extension will remain a complete field with respect to that absolute value. This is interesting enough to write a corollary about.

Corollary 2.2.20. *Let K be a complete valued field and L a finite extension of K. If there is an absolute value $|\cdot|$ on L extending the absolute value on K, then L is complete with respect to $|\cdot|$*

In addition, we also know that the limit of a sequence in L can be found by looking at the sequences of coefficients for any basis.

Before moving forward and finding this extended absolute value, there is one thing we might want to notice.

Corollary 2.2.21. *If K is a complete valued field and L a finite extension of K, there is at most one absolute on L extending the absolute value on K.*

Proof. Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K extending the absolute value $|\cdot|$ on K. We'll begin by proving they're equivalent as absolute values and only then we'll prove they must be exactly the same.

The equivalence between them is equivalent to, for all $x \in L$, $|x|_1 < 1$ if and only if $|x|_2 < 1$. Given $x \in L$, consider the sequence $(x_m) = x^m$. x converges to 0 with respect to the first absolute value if and only if $|x|_1 < 1$ and to the second if $|x|_2 < 1$. Although it may not seem like the case at first, these are equivalent occurrences. Both of them are norms on L as a K-vector space, so they must be equivalent (as norms) and induce the same topology. Therefore, (x_m)'s convergence to 0 doesn't depend on the choice of absolute value.

If $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values, there is $\alpha > 0$ such that $|x|_2 = |x|_1^\alpha$ for all $x \in L$. But we know these absolute values coincide in K. As long as $|\cdot|$ isn't the trivial absolute value, this implies $\alpha = 1$ and that $|\cdot|_1$ and $|\cdot|_2$ coincide. □

This uniqueness also means that, if we have a further extension M and an element of L, we won't have a need to distinguish between its absolute value with respect to L or with respect to M, which is good to know.

Now, we've been talking about this hypothetical extended absolute value. It's time to finally take a look at it. First, let's introduce the norm function (unfortunate name, but not to be confused with a norm on a vector space).

Assume L is a normal extension of K. Then $N_{L/K} : L \to K$ sends α into the product of its conjugates, its images by the automorphisms of L that fix K.

Theorem 2.2.22. *Let $(K, |\cdot|)$ be a complete valued field and $L : K$ a finite extension with degree n. $|\cdot|$ can be extended to L uniquely and L in complete with respect to that extended absolute value. That absolute value is non-archimedean and is given by*

$$|x| = \sqrt[n]{|N_{L/K}(x)|}$$

In order to prove this result, we should first prove a small lemma about irreducible polynomials in complete valued fields.

Lemma 2.2.23. *Let K be a complete valued field and let $f \in K[X]$ be a polynomial. If $f(X) = a_n X^n + \cdots + a_0$ is irreducible, its coefficient with the least π-adic valuation is either a_n or a_0.*

Proof. Let's assume f is such that there is a $0 < k < n$ such that $v_\pi(a_k) < v_\pi(a_n)$ and $v_\pi(a_k) < v_\pi(a_0)$. Out of all coefficients with minimum π-adic valuation, we pick their minimum as k.

We can multiply f by $\pi^{-v_\pi(a_k)}$ in order to obtain a new polynomial $g(X) = b_n X^n + \cdots + b_0$ which is irreducible if and only if f is irreducible. For all $0 \le i \le n$, $v_\pi(b_i) \ge v_\pi(b_k) = 0$, thus $g \in \mathcal{O}_K[X]$. If we consider g's reduction modulo π, as $v_\pi(b_i) > v_\pi(b_k)$ for all $0 \le i < k$ (due to k's minimality), it is $\bar{b}_n X^n + \bar{b}_{n-1} X^{n-1} + \cdots + \bar{b}_k X^k$, which factors to $X^k(\bar{b}_n X^{n-k} + \bar{b}_{n-1} X^{n-1-k} + \cdots + \bar{b}_k)$. We're in condition to apply Hensel's Lemma (2.2.13), taking $\phi_1 = X^k$ and $\phi_2 = \bar{b}_n X^{n-k} + \bar{b}_{n-1} X^{n-1-k} + \cdots + \bar{b}_k$, and to conclude that there is a factorization of f in $K[X]$ as the product of two polynomials f_1 and f_2, where f_1 has degree $k < n$. Therefore, f is not irreducible, which contradicts the original statement. □

Now that we have this smaller result, we can finally go ahead and prove our theorem which allows us to get an extended absolute value for a finite extension of a complete valued field.

Proof. As the norm function is a group homomorphism between the multiplicative groups $L^\times \to K^\times$, and as $N(0) = 0$, it's clear from the beginning that

- $|x| = 0$ if and only if $x = 0$
- For any $x, y \in L$, $|xy| = |x||y|$

Therefore, what's left to prove is that this alleged absolute value satisfies the ultrametric inequality. Let $x, y \in L$. If one of them is 0, there's nothing left to prove. Then, we can assume $xy \neq 0$ and that $|x| \leq |y|$. Hence, $|x+y| \leq \max\{|x|, |y|\} \Leftrightarrow |\frac{x}{y}+1| \leq \max\{\frac{x}{y}, 1\}$. As $|\frac{x}{y}| \leq 1$, it suffices to prove that for all $z \in L$ with $|z| \leq 1$, $|z+1| \leq 1$.

Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of z. We should note that if $[L:K] = l$, $N_{L/K}(z) = (-1)^l a_0^{l/n}$, which allows us to conclude $a_0 \in \mathcal{O}_K$, as $a_0 \in K$ and $|z| \leq 1 \Rightarrow N_{L/K}(z) \leq 1 \Rightarrow |a_0| \leq 1$. Now, if $f(X)$ is a minimal polynomial, it's irreducible and, by the previous lemma, as its leading coefficient is 1 and $a_0 \in \mathcal{O}_K$, all of its coefficients are in $\mathcal{O}_K$. $f(X)$ is indeed not only in $K[X]$ but also in $\mathcal{O}_K[X]$.

Furthermore, it's clear that $z+1$'s minimal polynomial is precisely $f(X-1) = X^n + (a_{n-1} - n)X^{n-1} + \cdots + (a_0 - a_1 + a_2 + \cdots + (-1)^n a_n)$. Let $a = (a_0 - a_1 + a_2 + \cdots + (-1)^n a_n)$. This once again calls for a fact we've already stated in this proof regarding the relation between a number's minimal polynomial and its norm, $N_{L/K}(z+1) = (-1)^l a^{l/n}$. This allows us to deduce that $v_\pi(N_{L/K}(z+1)) \geq 0$, as all of f's coefficients have a non-negative valuation as well, and thus we conclude what we wanted to conclude: if $|z| \leq 1$, $|z+1| \leq 1$. Hence, $|\cdot|$ satisfies the ultrametric inequality and, as such, is indeed a non-archimedean absolute value that extends $|\cdot|_\pi$ to L. □

This provides us an absolute value on L that extends the one on K, as well as a valuation that does the same. However, this valuation isn't necessarily normalized.

Definition 2.2.24. *Let L/K be a finite extension of degree n and $e = e(L/K)$ be the positive integer such that*

$$v(L) = \frac{1}{e}\mathbb{Z}$$

We call e the ramification index of L over K. The extension L/K is said to be unramified if $e = 1$ and totally ramified if $e = n$.

The conclusion that a finite extension of a non-archimedean valued field is still a non-archimedean valued field is relevant, as that means all of the previous results still stand when we consider the extension itself.

Definition 2.2.25. *A local field is a complete and discrete valued field with a finite residue field.*

We can notice that if L is a finite extension of K, then r_L is a finite extension of r_K. Let $f = f(L/K)$ be the degree of that extension.

Proposition 2.2.26. *Let K be a local field and L a finite extension of K with degree n. Then, $n = e(L/K) \times f(L/K)$.*

There is a unique intermediate field M such that

- *M/K is unramified, and thus $[M:K] = f$*
- *L/M is totally ramified and $[L:M] = e$*

Proof. The first part of the statement corresponds to Proposition 5.4.6 in [Gou91], while the second corresponds to Proposition 5.4.11 in that same book. □

Example 2.2.27. *We know that 2 is not a square in $\mathbb{Q}_3$ (as it is not a square in its residue field), thus $\mathbb{Q}_3(\sqrt{2})$ is an extension of degree 2 of $\mathbb{Q}_3$. We can notice $v_3(\mathbb{Q}_3(\sqrt{2})) = \mathbb{Z}$, and as such that we're dealing with an unramified extension. Thus our "expansion" is noticed in the residue field, which will now be $\mathbb{F}_3(\sqrt{2})$, a field with 3^2 elements.*

3 isn't a square in $\mathbb{Q}_3$ either, which means $\mathbb{Q}_3(\sqrt{3})$ is an extension of degree 2 as well. But we can easily notice that, as $v_3(3) = 1$, $v_3(\sqrt{3}) = \frac{1}{2}$. This means this is a totally ramified extension, as $v_3(\mathbb{Q}_3(\sqrt{3})) = \frac{1}{2}\mathbb{Z}$ and 2 is the degree of the extension.

Considering $\mathbb{Q}_3(\sqrt{2}, \sqrt{3})$ we have an extension that is neither unramified nor totally ramified, with $e = f = 2$.

This concludes our brief introduction to the p-adic numbers and other similar fields. We can now move forward onto some other interesting matters.

Part II

Chapter 3

Relevant spaces

Now we've finally introduced p-adic numbers and other general local fields, it might be of interest to introduce the spaces we intend to focus on. These will be, together with their endomorphisms, the protagonists of our work. We're very interested in knowing how linear applications work over these spaces, but in order to learn anything about those actions and their properties, we need to initially focus on the spaces themselves for a while.

Without further ado, let us introduce the spaces we will be focusing on during our work:

- $\mathbb{Z}_p^n$
- $\mathcal{O}_K^n$, where K is a proper finite extension of some $\mathbb{Z}_p$
- $(\mathbb{Q}_p/\mathbb{Z}_p)^n$
- $(K/\mathcal{O}_K)^n$, where K is a proper finite extension of some $\mathbb{Z}_p$

These choices aren't completely arbitrary. First of all, we should note these are all $\mathbb{Z}$-modules and, more specifically, $\mathcal{O}_K$-modules (for some local field K). Still, they're $\mathbb{Z}$-modules, which is of our interest as our original motivation was studying $\mathbb{Z}$-linear endomorphisms.

Now, there are two distinct families of spaces we will be studying: finitely generated free $\mathcal{O}_K$-modules, and quotients of the kind $(K/\mathcal{O}_K)^n$. These choices are heavily motivated by the integer case, where the free $\mathbb{Z}$-modules and the tori are the most relevant spaces.

Of course, it's important to know which metric or topology we'll define in these spaces. We have already talked about norms and non-archimedean absolute values but what we haven't done is verifying if a norm based on a non-archimedean absolute value must always induce a non-archimedean metric.

It's easy to see that's not the case, by looking for instance at $\mathbb{Z}_2^2$ with the sum-norm. If d is the distance function induced by the sum-norm related to the 2-adic value, we get that $d((0,0),(0,1)) = d((0,0),(1,0)) = 1 < 2 = d((0,0),(1,1))$. The sup-norm, however, does maintain the non-archimedean properties. This points us into considering the distance induced by the sup-norm the default distance in these spaces.

Thus it's only natural that we consider the distance on these spaces to be the one induced by the sup-norm induced by the absolute value on the corresponding field. Now, we'll focus on studying these metric spaces for a while, as a first step towards understanding how linear applications act on them.

3.1 $\mathbb{Z}_p^n$ and $\mathcal{O}_K^n$

Even though we've split these two cases apart, they are essentially the same. Hence we'll use the usual notation for a generic field K and integer ring $\mathcal{O}_K$, with π being a uniformizer, just like p is a uniformizer of $\mathbb{Q}_p$.

In order to discuss issues regarding these spaces' topology, we must first have a topology. As such, let us start by defining a distance in K.

Definition 3.1.1. *Let K be a local field, π a uniformizer and q the cardinality of r_K. We define the π-adic absolute value*

$$\begin{aligned} |\cdot|_\pi : K &\to \mathbb{R}^+ \\ x &\mapsto q^{-v_\pi(x)} \end{aligned}$$

where $q^{-\infty}$ is taken as 0.

From this, we can define a distance function in K.

$$\begin{aligned} d : K \times K &\to \mathbb{R}^+ \\ (x, y) &\mapsto |x-y|_\pi \end{aligned}$$

Now, this distance is simply one of the many distance functions that induce in the local field K the same topology as the one induced by π-adic absolute values, which is precisely the kind of thing we intend to study. A few of the things we want to know about have already been stated in 2.1.3, but not all of them.

Definition 3.1.2. *A metric (or, more generally, a topological) space X is said to be compact if, for all open covers of $X = \cup_{i\in I} X_i$, there is a finite subset $J \subseteq I$ such that $X = \cup_{j\in J} X_j$. A metric (or topological) space X is said to be locally compact if, for all $x \in X$, x has a compact neighbourhood.*

Theorem 3.1.3. *If K is a local field, K is locally compact and $\mathcal{O}_K$ is compact.*

Proof. Actually, we'll prove that $\mathcal{O}_K$ is compact first, as that will allow us to prove the other statement (every point in K has a neighbourhood that's homeomorphic to $\mathcal{O}_K$!). $\mathcal{O}_K$ is a closed subset of a complete space, so it is complete as well. Now, we'll have to see it is totally bounded, that is: for all $\varepsilon > 0$, there's a finite set of open balls with radius less than ε that covers the entire space. Let q be the cardinality of the residue field r_K. If $\varepsilon > 1$, the question is trivial. Otherwise, let m be the smallest integer such that $p^{-m} < \varepsilon$. Let $x_1, x_2, \ldots, x_{q^m}$ be representatives of all the cosets of $K/(\pi^m K)$. It's clear that $\mathcal{O}_K \subseteq \cup_{i=1}^{q^m} B(x_i, p^{-m}) \subseteq \cup_{i=1}^{q^m} B(x_i, \varepsilon)$. Now that we know this, we must prove that these two conditions imply the compactness of $\mathcal{O}_K$.

Lemma 3.1.4. *A metric space X that is complete and totally bounded must be compact.*

Proof. First we must note the widely known result that sequential compactness implies compactness. Now, we'll prove that a complete and totally bounded metric space must be sequentially compact. As completeness is one of the hypotheses, we'll prove that any sequence must have a Cauchy subsequence (that will then be convergent, by completeness of the space).

As X is totally bounded, for each m there is a finite set of open balls with radius 2^{-m} that covers X. Let, for each integer $i > 0$, S_i be a finite set of open balls with radius 2^{-i} that covers X. Now let us consider $(x_n)_{n \in \mathbb{N}}$. We'll prove by induction that there is a subsequence $(y_n)_{n \in \mathbb{N}}$ of the previous sequence which is a Cauchy sequence.

As S_1 is finite and covers the entirety of X, there must be a $A_1 \in S_1$ such that $(x_n)_{n \in \mathbb{N}}$ is infinite. Let us then consider the subsequence that arises from taking only the terms which are in A_1. We can choose the first term which is in A_1, as being y_1.

Assume we have already chosen $y_1, y_2, \ldots, y_n$ (a "finite subsequence" of (x_n)) and $A_1, A_2, \ldots, A_n$ such that

$$\{(x_n)_{n \in \mathbb{N}}\} \cap \cap_{i=1}^{n} A_i$$

is infinite and such that if $j \geq i$, $y_j \in A_i$. First, let us note that these elements look somewhat promising if we're trying to find a Cauchy sequence: as if $j \geq i$, $y_j \in A_i$, that means that if $j, k \geq i$, $d(y_j, y_k) < 2^{-i}$. Now we'll see we can find a y_{n+1} such that $y_1, y_2, \ldots, y_{n+1}$ is under the previous assumptions. As, by hypothesis,

$$\{(x_n)_{n \in \mathbb{N}}\} \cap \cap_{i=1}^{n} A_i$$

is infinite and S_{n+1} is such that its open balls cover X, and the previous intersection is infinite, there must be an A_{n+1} such that

$$\{(x_n)_{n \in \mathbb{N}}\} \cap \cap_{i=1}^{n+1} A_i$$

is infinite as well. If $y_i = x_{s_i}$ for all $0 < i \leq n$, where $0 < s_1 < \ldots < s_n$, that means there must be an index $s_{n+1} > s_n$ such that $x_{s_{n+1}}$ is in the lastly referred intersection. Thus we have found our y_{n+1}.

The sequence that arises from this process is thus a Cauchy sequence, which, by the completeness of X, must be convergent. Hence we have proved that every sequence has a convergent subsequence, as we intended to. □

As $\mathcal{O}_K$ is totally bounded and complete, it is proved that is must be complete, by the previous lemma. □

Of course, we're interested in studying $\mathcal{O}_K^n$ and not simply $\mathcal{O}_K$, but studying the latter is a relevant step towards studying the former. Let us consider the following distance function:

Definition 3.1.5. *Let K be a local field, π a uniformizer and n a positive integer. We define d, the π-adic distance on K^n, as the following function:*

$$d : K^n \times K^n \to \mathbb{R}^+$$

$$((x_1, \ldots, x_n), (y_1, \ldots, y_n) \mapsto \sup_{1 \leq i \leq n} \{|x_i - y_i|_\pi\}$$

Accordingly, we can also define a "valuation" on these vector spaces.

Definition 3.1.6. *Let K be a local field, π a uniformizer and n a positive integer. We define v_π, the π-adic valuation on K^n, as the following function:*

$$v_\pi : K^n \to \mathbb{R}^+$$
$$(x_1, \ldots, x_n) \mapsto \inf_{1 \leq i \leq n} \{v_\pi(x_i)\}$$

These two concepts of *π-adic distance* and *π-adic valuation* on K^n end up being dual concepts just as the absolute values and valuations were in the 1-dimensional case, and we have that simply $d(0, x) \equiv e^{v_\pi(x)}$.

This distance preserves the ultrametric inequality as thus seems more appropriate to study than its archimedean counterparts. It's also important to note that it induces the product topology corresponding to the topology we were considering previously on K.

Taking this into account, it's now time to prove some results about these metric spaces.

Proposition 3.1.7. *If K is a local field and n is a positive integer, K^n and $\mathcal{O}_K^n$ are fully disconnected.*

Proof. This is simply a generalization of 2.1.14. We just want to notice that, for any two different points $x, y \in K^n$, there are disjoint complementary open sets A, B such that $x \in A$ and $y \in B$. Equivalently, we want to prove there is a clopen set A such that $x \in A$ and $y \notin A$. By the definition of d, it can only take values that the π-adic absolute value is able to take. As K is a local field, it is discrete, so d can only take values in a certain discrete subset of $\mathbb{R}^+$, D.

If $d(x, y) = r$, then there is a real number $\delta \in]0, r[\backslash D$. $B(x, \delta) = \bar{B}(x, \delta)$ and hence this set is a clopen set that contains x but doesn't contain y. We have proved K^n is fully disconnected.

$\mathcal{O}_K^n$ is proved to be fully disconnected as well by the exact same proof. □

Other topological result we have proved about local fields was 3.1.3, referring to its ring of integers' compactness. Of course, it's only natural to try and prove a similar result about $\mathcal{O}_K^n$. If we're familiar with Tychonoff's theorem, which states that any product over a set of compact sets must be compact as well regarding the product topology, this is nothing but a mere corollary of 3.1.3. If that's not the case, we may then prove it for finite products.

Theorem 3.1.8 (Finite Tychonoff theorem)**.** *Let $X_1, \ldots, X_n$ be compact topological spaces. Then $X_1 \times \cdots \times X_n$ is compact regarding the product topology.*

Proof. By proving this result for $n = 2$, the general case follows by induction. Let us consider X, Y, two compact topological spaces. Let $\cup_{i \in I} U_i$ be an open cover of $X \times Y$. By the definition of product topology, if $x \in X$ and $y \in Y$ are such that $(x, y) \in U_i$ for some $i \in I$, there are open neighbourhoods $V(x, y)$ of x in X and $W(x, y)$ of y in Y such that $(x, y) \in V(x, y) \times W(x, y) \subseteq U_i$. Hence finding a finite subcover of $\cup_{i \in I} U_i$ can be reduced to finding one of $\cup_{x \in X, y \in Y} V(x, y) \times W(x, y)$.

Fixed $x_0 \in X$, $\{x_0\} \times Y$ (with the subset topology) is homeomorphic to Y (with Y's topology), hence it is compact. So we know that $\cup_{y \in Y} V(x_0, y) \times W(x_0, y)$ has a finite subcover (of $\{x_0\} \times Y$) $\cup_{1 \leq i \leq k_{x_0}} V(x_0, y_i) \times W(x_0, y_i)$. Let $V(x_0) = \cap_{1 \leq i \leq k_{x_0}} V(x_0, y_i)$. This is an open neighbourhood of x_0. We can define this analogously for any $x \in X$. Now, we know $X = \cup_{x \in X} V(x)$ has a finite subcover, as X is compact. Let $\cup_{1 \leq i \leq l} V(x_i)$ be such a finite subcover. Then we can conclude that

$$\cup_{1 \leq i \leq l} (\cup_{1 \leq j \leq k_{x_i}} V(x_i, y_j) \times W(x_i, y_j))$$

is an open finite subcover of $X \times Y = \cup_{x \in X, y \in Y} V(x, y) \times W(x, y)$, which allows us to conclude $X \times Y$ is compact.

In order to do the induction step, assume it holds for a product of n compact spaces. It also holds for the product of 2 compact spaces. Let $X_1, \dots, X_n, X_{n+1}$ be compact spaces. $X_1 \times \cdots \times X_n$ is compact by induction hypothesis, so $(X_1 \times \cdots \times X_n) \times X_{n+1}$ is compact as it is the product of two compact spaces. But $(X_1 \times \cdots \times X_n) \times X_{n+1} \cong X_1 \times \cdots \times X_n \times X_{n+1}$, so the latter is compact as well, as we wanted to prove. □

We can now conclude what we wanted to prove:

Corollary 3.1.9. *If K is a local field and n a positive integer, $\mathcal{O}_K^n$ is a compact space.*

Proof. As $\mathcal{O}_K$ is compact, this is a direct aplication of 3.1.8 □

3.2 $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ and $(K/\mathcal{O}_K)^n$

Just as in the previous section, these two cases are essentially the same and thus we'll use the same notation as in that section.

As we've already introduced our distance function for a local field K, now we may be interested in noting that we're still able to have a "well-behaved" distance function on these quotients.

$$d : (K/\mathcal{O}_K) \times (K/\mathcal{O}_K) \to \mathbb{R}^+$$
$$(x + \mathcal{O}_K, y + \mathcal{O}_K) \mapsto \begin{cases} d_K(x, y), \text{ if } (x - y) \notin \mathcal{O}_K \\ \quad 0, \text{ otherwise} \end{cases}$$

Where d_K is our distance function defined on K. This new distance being well defined depends on effectively $d(x + \mathcal{O}_K, y + \mathcal{O}_K)$ not depending on the choice of representatives when these two cosets are different. Let us prove that's the case.

Proof. If $x - y \notin \mathcal{O}_K$, $v_\pi(x - y) < 0$. If $x' \in x + \mathcal{O}_K$ and $y' \in y + \mathcal{O}_K$, $(x' - y') = x - y + z$, where $v_\pi(z) \geq 0 > v_\pi(x - y)$, which means $v_\pi(x' - y') = v_\pi(x - y)$. □

The fact that this distance is indeed a non-archimedean distance follows directly from the fact that we still have a valuation in points other than $0 + \mathcal{O}_K$, while the small nuisance that may arise from this artificial definition on 0 is easily set aside.

Besides the distance, of course we also have a topology to care about, even if it is a rather uninteresting one: the discrete topology. This is the quotient topology that comes from the topology we have in K, as we can see by the following: The pre-image of any individual point $x + \mathcal{O}_K \in K/\mathcal{O}_K$ by the canonical projection map is the set $x + \mathcal{O}_K \subset K$ which is, in itself, an open subset of K. Hence all elementary sets of $K/\mathcal{O}_K$ are open sets and the induced quotient topology is the discrete topology.

If the topology we're working with is the discrete one, topology might not suffice in the journey of trying to find out how these quotients work. As such, let us do so by finding a rather satisfying description of them.

Lemma 3.2.1. *As additive groups, $\mathcal{O}_K/(\pi^k\mathcal{O}_\mathcal{K})$ and $(\pi^{-k}\mathcal{O}_K)/\mathcal{O}_K$ are isomorphic.*

We know that $K = \cup_{i\in\mathbb{N}}(\pi^{-i}\mathcal{O}_K)$. Consequently, we have that

$$(K/\mathcal{O}_K) \cong \cup_{i\in\mathbb{N}}((\pi^{-i}\mathcal{O}_K)/\mathcal{O}_K)$$

This means that these quotients are a union of finite sets which, in itself, is something to rejoice about, but what it further means is that these quotients encapsulate the behaviour of the finite quotients of $\mathcal{O}$ and are defined by the behaviour of those finite quotients as well.

On the other hand, there's something we suggested we wouldn't talk about but isn't very nice to ignore: can we find a simple description of $\mathbb{Q}_p/\mathbb{Z}_p$? We can do so indeed by, for instance, taking a look at the statement provided in the previous paragraph. Hence we have that

$$\mathbb{Q}_p/\mathbb{Z}_p \cong \{\frac{a}{p^n} + \mathbb{Z} : a, n \in \mathbb{N}\}$$

This quotient is isomorphic to a certain relevant subset of the rational torus: the p-torsion subgroup of the rational torus, the set of elements of the ration torus with a power of p as their additive order. Maybe somewhat unexpectedly, this space is simpler than (and even a subgroup of) its standard counterpart.

With this, we end our short tour through our favourite spaces and their metrics, topologies and distances.

Chapter 4

Action of endomorphisms over p-adic vector spaces

We will now be focusing on some assertions we can make about linear algebra over the p-adic numbers. In order to find invariants of any kind, it would seem useful to shed some light on the dynamics of these actions by integer matrices.

We'll be mainly focusing on the previously referred spaces paired with their respective distance functions, which we've already defined in 3.1.5.

4.1 General facts about v_π and d

Now, it makes sense to generalise the concept of valuation presented in 3.1.6 to linear applications over K^n. That is, identifying $\mathcal{L}(K^n, K^n)$, the space of linear functions from K^n into itself with $\mathcal{M}(n, K)$, the set of $n \times n$ matrices with terms in K, we present the following definition:

Definition 4.1.1. *Let K be a local field, π a uniformizer and n a positive integer. We define v_π, the π-adic valuation on $\mathcal{M}(n, K)$, as the following function:*

$$\begin{aligned} v_\pi : \mathcal{M}(n, K) &\to \mathbb{R}^+ \\ (x_n)_{1\leq i,j\leq n} &\mapsto \inf_{1\leq i,j\leq n}\{v_\pi(x_{i,j})\} \end{aligned}$$

Remark 4.1.2. *Even though we're calling it a valuation on $\mathcal{M}(n, K)$, we're doing so in a somewhat informal way: after all, $\mathcal{M}(n, K)$ isn't a field. Besides that fact that may seem just a simple detail, it's easy to note that this valuation doesn't satisfy $v_\pi(AB) = v_\pi(A) + v_\pi(B)$.*

In order to see that, we might just take a look at the 2-adic valuation of the following matrices:

$$\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 10 \end{pmatrix}$$

The 2-adic valuation of each of the matrices on the left-hand side is 0, while the valuation of the one on the right-hand side is 1. As $0 + 0 \neq 1$, we can conclude this doesn't behave as a valuation in $\mathcal{M}(2, \mathbb{Q}_2)$.

Furthermore, as all of these matrices are actually in $GL(2, \mathbb{Q}_2)$, we can also deduce that restricting this "valuation" to the general linear group isn't enough to fix this.

Nevertheless, the inequality $v_\pi(AB) \geq v_\pi(A) + v_\pi(B)$ is clearly verified, as, for some $A', B' \in \mathcal{M}(n, K)$ such that $A = \pi_\pi^v(A)A'$ and $B = \pi_\pi^v(B)B'$,

$$AB = \pi_\pi^v(A)A'\pi_\pi^v(B)B' = \pi^{v_\pi(A)+v_\pi(B)}A'B'$$

By the definition of A' and B', both of them must have 0 as their π-adic valuation and, as such, be elements of $\mathcal{M}(n, \mathcal{O}_K)$. This means that $A'B' \in \mathcal{M}(n, \mathcal{O}_K)$ as well, which implies $v_\pi(A'B') \geq 0$ and thus that $v_\pi(AB) \geq v_\pi(A) + v_\pi(B)$.

Lemma 4.1.3. *Let $A \in \mathcal{M}(n, \mathcal{O}_K)$ be a matrix such that $v_\pi(\det(A)) = n \times v_\pi(A)$. There's a matrix $A' \in GL(n, \mathcal{O}_K)$ such that $A = \pi^{v_\pi(A)}A'$ and $v_\pi(\det(A')) = v_\pi(A') = 0$.*

Proof. Defining A' as it was previously stated, it's clear that $v_\pi(\det(A')) = v_\pi(A') = 0$. The only thing that's left to prove in that A' is invertible in $\mathcal{M}(n, \mathcal{O}_K)$. That is simply a direct consequence of its determinant being invertible in $\mathcal{O}_K$, as its π-adic valuation is 0. □

Remark 4.1.4. *Matrices in $GL(n, \mathcal{O}_K)$ must satisfy this condition. If $A \in GL(n, \mathcal{O}_K)$, $v_\pi(\det(A)) = 0$ by virtue of being in the general linear group.*

On the other hand, it's also clear that $v_\pi(A) = 0$. $v_\pi(A) \geq 0$ as $A \in \mathcal{M}(n, \mathcal{O}_K)$, and $v_\pi(A) > 0$ would imply $v_\pi(\det(A)) > 0$, thus $v_\pi(A) = 0$.

Having these definitions, it's now time to try and start studying how these matrices act on the spaces we've been focusing on.

Proposition 4.1.5. *Let K be a local field, π a uniformizer, n a positive integer and $A \in GL(n, \mathcal{O}_K)$.*

If d is the distance function induced in K^n by the sup-norm regarding the π-adic absolute value, A acts as an isometry on K^n regarding d.

Proof. Equivalently, as $d(0, x) \equiv e^{v_\pi(x)}$, we will prove that, for all $w \in K^n$, $v_\pi(Aw) = v_\pi(w)$. Without loss of generality, we can assume $v_\pi(w) = 0$, as other cases differ only by multiplication by a power of π.

We intend to prove that if $w \in \mathcal{O}_K$ and $A \in GL(n, \mathcal{O}_K)$ are such that $v_\pi(w) = 0$ and $v_\pi(A) = 0$, $v_\pi(Aw) = 0$ as well. It's clear that $v_\pi(Aw) \geq 0$, as $\mathcal{O}_K$ is closed for addition and multiplication, so what's left to prove is that $v_\pi(Aw) < 1$. We can do so by considering the projections on the residue field $r_K = \mathcal{O}_K/(\pi\mathcal{O}_K)$. Let A' be the projection of A and w' the projection of w. By hypothesis, $A' \in GL(n, r_K)$ and $w' \in r_K^n$ is nonzero. We want to prove that $A'w' \neq 0$ as well.

Of course, this follows trivially from A' being an automorphism, which means its kernel is trivial. □

Corollary 4.1.6. *Let K be a local field, π a uniformizer, n a positive integer and $A \in \mathcal{M}(n, K)$ such that $v_\pi(\det(A)) = \pi^{nv_\pi(A)}$, $B \in \mathcal{M}(n, K)$. Let $w \in K^n$.*

- $v_\pi(Aw) = v_\pi(A) + v_\pi(w)$.
- $v_\pi(AB) = v_\pi(BA) = v_\pi(A) + v_\pi(B)$.

With these propositions we can conclude that these choices for distances and valuations do make some sense, as they showcase some "good behaviour" for these operations.

4.2 Dynamics

4.2.1 Periodicity and recurrence

Besides studying what happens by applying one iteration of this linear function, we're interested in studying the dynamics of this action and what happens in general when we repeatedly apply this function.

In general, there's not much to be said regarding a generic linear application's periodicity over K or $\mathcal{O}_K$, but there is something to say about *recurrence.*, deriving from its periodicity over finite quotients of $\mathcal{O}_K^n$.

Proposition 4.2.1. *Let K be a local field, n a positive integer and π a uniformizer. If $A \in GL(n, \mathcal{O}_K)$, we can say that, for the application of A:*

- *Any point in $(K/\mathcal{O}_K)^n$ is periodic.*
- *Any point $w \in K^n$ is recurrent. This is, for any $\varepsilon > 0$ there's $m \in \mathbb{N}$ such that $d(w, A^m w) < \varepsilon$.*

Proof. The first statement gets clearer if we take into account 3.2.1. The structure of this quotient is deeply connected to the finite quotients of $\mathcal{O}_K^n$. Specifically, that lemma implies that a certain $w \in (K/\mathcal{O}_K)^n$ must be in a certain $((\pi^{-i}\mathcal{O}_K)/\mathcal{O}_K)^n$, while 4.1.5 implies all of its successors by iterating the application of A will remain in that same finite quotient. As that set is finite, $(A^m w)_{m\in\mathbb{N}}$ must at one point repeat a term, which means it must be eventually periodic.

Let k be the smallest index from which the sequence starts being periodic (and t the period). If $k = 0$, there's nothing left to prove. If $k > 0$, let us notice that $A^{-1} \in GL(n, \mathcal{O}_K)$ as well, and so that $A^{k-1}w = A^{-1}A^k w = A^{-1}A^{k+t}w = A^{k+t-1}w$, which means the sequence starts being periodic at $k-1$, contradicting k's minimality. Thus the sequence must be periodic.

For the second point, we should note that the behaviour of the iteration of applications of A in quotients of the form $(\mathcal{O}_K/(\pi^i\mathcal{O}_K))^n$ is fundamentally the same as in quotients of the form $((\pi^{-i}\mathcal{O}_K)/\mathcal{O}_K)^n$. That means that, for all positive integer i, the application of A is periodic in $(\mathcal{O}_K/(\pi^i\mathcal{O}_K))^n$. If two elements of $\mathcal{O}_K$ are congruent modulo π^i, with i a positive integer, the distance between them must be less than e^{-i}. Hence, the periodicity in finite quotients proves the recurrence we wanted to prove.

□

Now, we may introduce a rather interesting lemma regarding the order of these linear applications over sets of the kind $(\mathcal{O}_K/(\pi^k\mathcal{O}_K))^n$. If we've just stated that these orders must exist, it just makes sense to effectively go ahead and compute them, when possible.

Given a matrix $A \in M(n, \mathcal{O}_K)$, let us recall that we've defined its π-adic valuation as the minimum valuation across all of its entries. In order to achieve the result we're aiming for, we'll start by proving a slightly more general result than the one we're trying to achieve.

Proposition 4.2.2. *Let K be a local field, p the characteristic of its residue field, π a uniformizer, $A, B \in GL(n, \mathcal{O}_K)$ such that $A \equiv B \mod \pi$ and $AB = BA$. Let $m \in \mathbb{N}$. We can say the following about $v_\pi(A^m - B^m)$:*

- *If $(p-1)v_\pi(A-B) > v_\pi(p)$, then $v_\pi(A^m - B^m) = v_\pi(A-B) + v_\pi(m)$*
- *If $p = 2$ and $v_2(A-B) = 1$, then $v_2(A^{2m} - B^{2m}) = v_2(A^2 - B^2) + v_2(m)$, and $v_2(A^m - B^m)$ with odd m is simply 1.*

Proof. Let us start by noticing that, given a local field K, there is a single prime number with non-zero valuation (and it is greater than zero, in fact). That prime number is the characteristic of its residue field, p, which projects onto 0 in the residue field precisely because $p \in \pi\mathcal{O}_K$. To see that every other prime number must have zero as their valuation is quite easy. Let's assume that wasn't the case and there was another prime q with non-zero valuation. We could write 1 as a linear combination with integer coefficients of p and q and that would imply that $v_\pi(1) \geq \min\{v_\pi(p), v_\pi(q)\} \geq 1$, which is trivially false.

The second case shall be treated separately. For the first, let us assume $A = \pi^k M + B$, where $v_\pi(M) = 0$. Note that if $AB = BA$, then $\pi^k MB + B^2 = B \cdot \pi^k M + B^2$, which means $BM = MB$. We'll take this into account throught the entire proof.

We'll prove the result by induction on the exponent.

If $p \not| m$, $v_\pi(A^m - B^m) = k$. Let us consider that

$$A^m - B^m = (A - B)\sum_{i=0}^{m-1} A^i B^{m-1-i}$$

The sum on the right-hand side amounts to $N = m \times A^{m-1}$, modulo π^k. As $p \not| m$ and $A \in GL(n, \mathcal{O}_K)$, $v_\pi(\det(N)) = 0 = v_\pi(N)$. By 4.1.6, $v_\pi(A^m - B^m) = v_\pi(A^m - B^m) + v_\pi(N) = v_\pi(A^m - B^m)$.

If the exponent is p, we can expand $(\pi^k M + Id)^p - Id$ as

$$\sum_{i=1}^{p} \binom{p}{i} \pi^{ki} M^i B^{p-i}$$

As all of the non-unitary binomial coefficients have the same π-adic valuation as p and as $v_\pi(p) < (p-1)k$, the term $\binom{p}{1}\pi^k M$ will be the one with the smallest valuation. Looking at the expression, the valuation of each term depends on their respective binomial coefficient and on the exponents of π and M and as such it's clear that the term with the smallest valuation had to be between that summand and the p-th one: $\binom{p}{p}\pi^{kp}M^i$. As $kp > k + v_\pi(p)$, the former must have the lowest valuation among all summands. This means the sum must have the same valuation as that term: $k + v_\pi(p)$.

These two distinct induction steps allow us to conclude the first part of the lemma, as in order to compute an arbitrary $v_\pi(A^m - Id^m)$, we simply have to do so for $m', pm', p^2m', \ldots$ until m, where m' is the greatest divisor of m that's not divisible by p.

When we don't have the inequality that's present in the first case, things get trickier. When we have the opposite inequality, we may be able to compute the valuations by performing the same calculations, but equality is, in general, terrible to deal with, as the valuation of the sum of two terms with the same valuation can be, *a priori*, arbitrarily large. That, together with the existence of other terms, constitutes a rather complicated challenge. Thus we opt into solving a simpler case: when $\pi = p = 2$ and $k = 1$.

The argument for when $2 \not| m$ is the same as the one used before. What will change, however, is the argument for when the valuation actually increases due to the exponent. First we should note that if $v_2(A - B) = 1$, $v_2(A^2 - B^2) > 1$. If $A = 2M + B$, with $2 \not| M$, $A^2 - B^2 = 4M^2 + \binom{2}{1}2MB$, which clearly has at least 2 as its 2-adic valuation. Now, we can simply apply the first part of this lemma, as A^2 and B^2 are such that $(2 - 1)v_2(A^2 - B^2) > v_2(2)$. □

This proposition might not sound completely innovative for someone who has previously met what is called the Lifting the Exponent Lemma [1]. To us, however, most of this proposition's usefulness comes when B is the identity matrix. In that case, we're pretty much just computing the order of A in finite quotients of $\mathcal{O}_K^n$.

Lemma 4.2.3. *Let K be a local field, p the characteristic of its residue field, n a positive integer, π a uniformizer, $A \in \mathcal{M}(n, \mathcal{O}_K)$, $A \equiv Id \mod \pi$. Let $m \in \mathbb{N}$. We can say the following about $v_\pi(A^m - Id)$:*

- *If $(p - 1)v_\pi(A - Id) > v_\pi(p)$, $v_\pi(A^m - Id) = v_\pi(A - Id) + v_\pi(m)$*
- *If $p = 2$ and $v_2(A - Id) = 1$, $v_2(A^{2m} - Id) = v_2(A^2 - Id) + v_2(m)$, and $v_2(A^k - Id)$ with odd k is simply 1*

Proof. Trivial by 4.2.2, by taking $B = Id$. □

Lemma 4.2.4. *Let K be a local field, n a positive integer, π a uniformizer, $A, B \in \mathcal{M}(n, \mathcal{O}_K)$. If there's $C \in GL(n, \mathcal{O}_K)$ such that $AC = CB$, then, for all $m \in \mathbb{N}$,*

$$v_\pi(A^m - Id) = v_\pi(B^m - Id)$$

Proof. If $AC = CB$, then $B = C^{-1}AC$ and $B^m = (C^{-1}AC)^m = C^{-1}A^mC$. This means that $B^m - Id = C^{-1}A^mC - Id = C^{-1}(A^m - Id)C$. As both $C, C^{-1} \in GL(n, \mathcal{O}_K)$, we can apply 4.1.6 in order to conclude that $v_\pi(B^m - Id) = v_\pi(C) + v_\pi(A^m - Id) + v_\pi(C) = 0 + v_\pi(A^m - Id) + 0 = v_\pi(A^m - Id)$. □

The statement that motivated the search of 4.2.2 and 4.2.3, which is a widely known lemma, is a result about orders of matrices modulo powers of prime numbers. That "original statement" is equivalent to a less general version of the previous lemma which we would directly obtain if we only took into account p-adic fields (and the respective primes p as their uniformizers) and not general cases of local fields. That corollary is the following:

Corollary 4.2.5. *Let p be a prime number, $A \in \mathcal{M}(n, \mathbb{Z}_p)$ such that $ord(A, p) = t$ (t is the smallest positive integer such that $A^k \equiv Id \mod p$) and $A^t = p^kM + Id$, where $M \in \mathcal{M}(n, \mathbb{Z}_p)$ is such that $p \not| M$ and $k > 0$ is an integer.*

[1] It can be found on Wikipedia

- *If $p \neq 2$ or $k > 1$, $ord(A, p^i) = t$ for all $i \leq k$, while $ord(A, p^{k+l}) = tp^l$, for all $k \geq 0$*
- *Otherwise, there's a $j \geq 2$ such that $ord(A, 2^i) = 2\,\forall 2 \leq i \leq j$ and $ord(A, 2^{j+l}) = 2^{l+1}\,\forall l \geq 0$*

Proof. The first case corresponds to the first case of 4.2.3. First, we should note that it's obvious that $ord(A, p^i) = t$ for all $i \leq k$. Now we're interested in computing the other orders.

Let's note that those orders must always be divisible by t. We can compute $v_p(A^{tm} - Id)$ for any positive integer m as, by 4.2.3, it will be equal to $k + v_p(m)$. Thus it's very easy to see that the smallest m such that $v_p(A^{tm} - Id) = k + l$, for any positive integer l, is p^l. That allows us to conclude the rest of the first item: $ord(A, p^{k+l}) = tp^l$.

The second case corresponds to the second item of 4.2.3. The integer j in the statement is equal to $v_2(A^2 - 1)$, which allows us to conclude, analogously to when we proved the first item, that, as $v_2(A^{2m} - Id) = j + v_2(m)$, $ord(A, 2^{j+l}) = 2 \times 2^l$. □

Remark 4.2.6. *The parameters t and m are invariant by conjugacy. This happens because they fully depend on the valuation of $A^k - Id$, which is invariant by conjugacy as well, as we know by 4.2.4.*

These small propositions do quite a bit for our intuition about the behaviour of the orbits through linear applications on these spaces, which will be our next focal point.

4.2.2 Orbits and minimal sets

Definition 4.2.7. *Let K be a field and $A \in GL(n, K)$. The orbit of x through A, noted $O_A(x)$, or simply $O(x)$ if it's clear which matrix A we're referring to, is the set*

$$\{y \in K^n : \exists t \in \mathbb{Z}, A^t x = y\}$$

Other than the orbits, there are some other sets (related to them) we may want to introduce:

Definition 4.2.8. *Let K be a topological field, n a positive integer and $A \in GL(n, K)$. If $x \in K^n$, its minimal set by A (noted $M_A(x)$ or simply $M(x)$) is the topological closure of its orbit by A.*

First of all, we'll be interested in these definition mostly when K is a local field. And in case this definition isn't sufficiently clear, what it means is that, if K is a local field and $\pi \in K$ is a uniformizer, $y \in K$ is in $M(x)$ if and only if, for all positive integers k, there's an integer t such that $v_\pi(y - A^t x) \geq k$. There are still some rather simple things to say about these sets.

We should note that, under these conditions, the minimal sets form a partition of K^n consisting of closed sets that are closed under the application of A.

Lemma 4.2.9. *Let K be a local field, n a positive integer and $A \in \mathcal{M}(n, K)$. Each minimal set is closed, and closed under the application of A. Moreover, the minimal sets form a partition of $\mathcal{O}_K^n$.*

Proof. It's trivial that each minimal set must be closed.

Let π be a uniformizer, $y \in M(x)$. That means that $\forall k \in \mathbb{N} \exists t(k) \in \mathbb{Z} : A^{t(k)} x \equiv y \mod \pi^k$. Let m be an integer. We want to prove that $A^m y \in M(x)$. That's a direct consequence of $y \in M(x)$, however. We simply have to apply A^m to both sides of those equalities and we'll achieve what we want: $\forall k \in \mathbb{N} \exists t'(k) \in \mathbb{Z} : A^{t'(k)}x \equiv A^m y \mod \pi^k$, where $t'(k) = t(k) + m$.

Now we want to prove that the minimal sets form a partition of $\mathcal{O}_K^n$. We have two things to prove:

- The minimal sets cover the entirety of $\mathcal{O}_K^n$
- If the intersection between two minimal sets is non-empty, those two empty sets are the same. Once again, the first statement is trivial, as $\forall x \in \mathcal{O}_K^n$, $x \in M(x)$.

  For the second statement, let us consider $x, y, z \in \mathcal{O}_K^n$ such that $z \in M(x) \cap M(y)$. That means that, $\forall k \in \mathbb{N} \exists t_x(k), t_y(k) : z \equiv A^{t_x(k)}x \equiv A^{t_y(k)}y \mod \pi^k$. From this we can conclude that $x \in M(y)$ and $y \in M(x)$: $\forall k \in \mathbb{N}\, x \equiv A^{t_y(k)-t_x(k)}y \mod \pi^k$, while $\forall k \in \mathbb{N}\, y \equiv A^{t_x(k)-t_y(k)}x \mod \pi^k$.

  As we know by the second point of this lemma, minimal sets are closed under the application of A, which must then mean $O(x) \subseteq M(y)$ and $O(y) \subseteq M(x)$. But of course, by each of those two inclusions, $M(y)$ must contain the closure of $O(x)$, while $M(x)$ must contain the closure of $O(y)$, which means that $M(x) = M(y)$.

□

This result is the first thing one might think of when considering minimal sets, but it's not everything one can prove about them. For instance, we'll now state and prove a proposition regarding the cardinality of $\{M(x) : x \in K^n\}$. In order to do so, we must first introduce the Haar measure, or rather the Haar measure specifically in $\mathcal{O}_K^n$.

4.2.3 Haar there any measures on local fields?

We're interested in introducing a measure in a local field K (or simply in its ring of integers). First of all, let us define what is a measure, before presenting our favourite measure.

Definition 4.2.10. *Let X be a set. $\Sigma \subseteq \mathcal{P}(X)$ is a σ-algebra on X if $X \in \Sigma$ and Σ is closed under complement and countable unions.*

Definition 4.2.11. *Let X be a set and Σ a σ-algebra on X. $\mu : \Sigma \to \mathbb{R} \cup \{+\infty\}$ is a measure if it satisfies the following conditions:*

- *For all $M \in \Sigma$, $\mu(M) \geq 0$*
- $\mu(\{\,\}) = 0$
- *For any countable set $\{M_i\}_{i=1}^{\infty} \subseteq \Sigma$, where $i \neq j \Rightarrow M_i \cap M_j = \{\,\}$, $\mu(\cup_{i=1}^{\infty} M_i) = \sum_{i=1}^{\infty} \mu(M_i)$*

We may now present a measure μ_0 which is called a Haar measure on $\mathcal{O}_K$, by letting $\mu_0(\bar{B}(x, q^m)) = q^m$, for any $x \in \mathcal{O}_K$ and $m \in \mathbb{Z}_{\leq 0}$, where $q = |r_K|$(Proposition 13.16 in [Sut19]).

We're just defining this measure on the semi-ring of open balls[2] of $\mathcal{O}_K$, but as it is additive in that semi-ring, we can easily extend it to the ring that's generated by those same open balls. The fact that this measure over this semi-ring is additive is a consequence of it being translation invariant and, as such,

[2] We actually define it on closed balls, but we know they are open balls as well. We did this because the numbers look nicer this way, with the measure of a ball coinciding with its radius

$$\mu(\bar{B}(0,q^m)) = q^m = q \times q^{m-1} = \sum_{i=1}^{q} B(y_i q_m, q^{m+1})$$

Where the y_i are representatives of the cosets in r_K.

We can extend it to to a measure μ on $\mathcal{K}^n$, $n \in \mathbb{N}$ by letting $\mu(\bar{B}(x_1, q^{m_1}) \times \ldots \times \bar{B}(x_n, q^{m_n})) = q^{\sum_{i=1}^{n} m_i}$. The existence of this measure isn't a feat in itself, at least for us, as we're doing nothing other than stating the existence of this Haar measure for $\mathcal{K}^n$, which is a locally compact topological group, where those do exist for certain.

This measure will eventually be a means to an end, when we use it to prove a result we'll present later.

4.2.4 Counting minimal sets

Proposition 4.2.12. *Let K be a local field, π a uniformizer and n a positive integer, $A \in GL(n, \mathcal{O}_K)$. If $v_\pi(A - Id)(p-1) > v_\pi(p)$ and either $n > 1$ or K isn't isomorphic to some $\mathbb{Q}_p$, then $\{M(x) : x \in K^n\}$ is uncountable.*

Proof. First of all, let us recall what is the closed ball $\hat{B}(x, l)$, for a given integer t and $x = (x_1, \ldots, x_n) \in K^n$. By the definition of our distance function in K^n, it is $\{y = (y_1, \ldots, y_n) \in K^n : |y_i - x_i| \leq l \forall 1 \leq i \leq n\}$, where, if π is a uniformizer, we have

$$\begin{aligned} |\cdot| : K &\to \mathbb{R}^+ \\ x &\mapsto P^{-v_\pi(x)} \end{aligned}$$

where P is the cardinality of r_K. We should note that a closed ball $\bar{B}(x, P^{-t})$ must have P^{-nt} as its Haar measure. Taking that into account, we can use 4.2.3 to get some upper bounds for the Haar measure of a minimal set.

We know, in abstract, that the following must be true, as $M(x)$ is the closure of $O(x)$:

$$M(x) \subseteq \cup_{i \in \mathbb{N}_0} \bar{B}(A^i x, \varepsilon)$$

for any $\varepsilon > 0$. We can use 4.2.3 in order to turn this into a more useful statement. By that lemma, if o is the order of A modulo π and $w = v_\pi(A^o - Id)$, and $v_\pi(A - Id)(p-1) > v_\pi(p)$, then $v_\pi(A^{om} - Id) = w + v_\pi(m)$ for any positive integer m. Well, this means that, for any $x \in K^n$, $A^{om} x \in \bar{B}(x, P^{-w - v_\pi(m)})$. This allows us to reduce that infinite union to a finite union of measurable balls[3]! Therefore we get the following inclusion, for any positive integer t:

$$M(x) \subseteq \cup_{i=0}^{p^t(o-1)} \bar{B}(A^i x, P^{-w - v_\pi(p)t})$$

Which immediately provides us an upper bound for the measure of $M(x)$

$$p^t(o-1)P^{n(-w - v_\pi(p)t)}$$

[3] We should recall that any point in a non-degenerate closed ball is a center of that ball

We know that $P = p^q$ for some positive integer q, so we may further simplify the expression

$$(o-1)p^{t-qn(w+v_\pi(p)t)} = (o-1)p^{-qnw}p^{t(1-qnv_\pi(p))}$$

Which means that, as long as $qnv_\pi(p) > 1$, we're facing a sequence of upper bounds that tends to 0. Which means that, if $qnv_\pi(p) > 1$, $M(x) = 0$, for any $x \in K^n$. A countable union of sets with measure 0 must have 0 as its measure, thus $\{M(x) : x \in K^n\}$ must be uncountable.

Of course, $qnv_\pi(p) > 1$ if and only if either $n > 1$ or $qv_\pi(p) > 1$. This last statement is true if and only if K is not a p-adic field. If it is a p-adic field, clearly both of those integers are equal to 1; if both those integers are equal to 1, on on hand p is a uniformizer of K and on the other its residue field is isomorphic to $\mathbb{F}_p$. By our characterizations of local fields, specifically the one that views its elements as power series in a uniformizer, this immediately shows K must be isomorphic to $\mathbb{Q}_p$. □

It's important to note that, even though the conditions on this proposition might seem strange, they are satisfied for instance when we're simply talking about any $\mathbb{Z}_p^n$ with $n > 1$. Of course, it's natural to be curious about the case where $n = 1$ and K is isomorphic to some $\mathbb{Q}_p$. Is it still true but it requires another proof, or does it not hold up? Well, it just doesn't hold up, as we will now prove.

Proposition 4.2.13. *Let $p > 2$ be a prime number. There are matrices $A \in GL(1, \mathbb{Z}_p)$ such that, for each positive integer n, there's a minimal set with Haar measure $\frac{p-1}{p^n}$.*

Proof. In order to prove this, we must first choose A wisely. Well, we may stop pretending this is a problem about matrices, as this is the one-dimensional case, and identify $\mathcal{M}(1, \mathbb{Z}_p)$ with $\mathbb{Z}_p$.

Now, our choice will be a $p-1$-th root of $p+1$. The polynomial $f = X^{p-1} - p - 1 \in \mathbb{Z}_p[X]$ is such that it's under the conditions of Hensel's lemma (2.2.15). Its formal derivative is $f' = (p-1)X^{p-2}$. Replacing X by 1, we get that $f(1) \equiv 0 \mod p$, while $f'(1) \not\equiv 0 \mod p$. This means there is a $\zeta \in \mathbb{Z}_p$ such that its order modulo p is $p-1$ and $v_p(\zeta^{p-1}) = 1$.

Now we're interested in showing this ζ must be a primitive root modulo all powers of p. That's clear by applying the one-dimensional case of 4.2.3 on $\zeta^{p-1} = p+1$. As $p > 2$, we're under the first conditions, and thus $v_p(\zeta^{p^t(p-1)} - 1) = 1 + t$, which means that in order to have a power of ζ be 1 modulo a certain power of p, p^{t+1}, its exponent must be $p^t(p-1)$. Thus ζ is a primitive root modulo all powers of p.

Now we will prove that if $y \in \mathbb{Z}_p$ is such that $v_p(y) = n$, then $y \in M(p^n)$. Actually, and equivalently, we'll show that if $y \in \mathbb{Z}_p^\times$, then $y \in M(1)$. Let t be a positive integer. ζ is a primitive root of p^t and y is coprime with p, thus there is a positive integer k such that $\zeta^k \equiv y \mod p^t$. This is true for any t, so y must be an accumulation point of $O(1)$.

Therefore, we have that $\mu(M(1)) = 1 - \mu(p\mathbb{Z}_p) = \frac{p-1}{p}$ and, consequently, $\mu(M(p^n)) = \frac{p-1}{p^n}$. Besides that, we also have that

$$\mathbb{Z}_p = M(0) \cup \bigcup_{i=0} M(p^i)$$

which shows that $\mathbb{Z}_p$ is covered by a countable number of minimal sets. □

This last detail of the proof seems like it should be the main focus of a proposition surrounding this theme. We've finally seen that in dimension 1, there are minimal sets with positive Haar measure. Now we can see that the number of minimal sets must always be countable in dimension 1 over the p-adic numbers.

Proposition 4.2.14. *Let $p > 2$ be a prime number and $A \in GL(1, \mathbb{Z}_p)$ such that A is not a root of unity. $\{M(x) : x \in \mathbb{Z}_p\}$ is countable.*

Proof. This proof will roughly follow the same ideas as the previous one. We will prove that $\mathbb{Z}_p^\times$ can be covered by a finite number of minimal sets. As $\mathbb{Z}_p = \{0\} \cup \bigcup_{i=0} p^i \mathbb{Z}_p^\times$, from that we can conclude that $\mathbb{Z}_p$ can be covered by a countable number of minimal sets.

Let $z \in \mathbb{Z}_p^\times$ be the p-adic integer corresponding to A. Let o be its order modulo p and $w = v_p(z^o - 1)$. From 4.2.3, just like in the previous proof, we can conclude that $v_p(z^{p^t o} - 1) = w + t$. Unlike in the previous proof, this doesn't mean anything about primitive roots, but instead it means something a little more delicate than that. Let $S \subseteq \mathbb{Z}_p/(p^w\mathbb{Z}_p)$ be the set of the remainders of all the powers of z modulo p^w. This set must have cardinality o, as that's z's order modulo p^w. Now, as z has order op^t modulo p^{wt}, the set of its remainders modulo p^{wt} must have cardinality op^t. But we know that each of those remainders' last w digits must correspond to an element of S.

If we try to get an upper bound for the number of remainders modulo p^{wt} of the powers of z, we can do so rather naively by counting the number of ways there are of picking the last w digits, which is o, and multiplying it by the number of ways of picking the first t digits, which is p^t. We say this is a naive way of counting because it uses absolutely no knowledge about how the first t digits are related to the last w, but we can now see it isn't naive at all. Our "upper bound" is precisely op^t, which we know is the cardinality of that set. That can only happen if for each sequence of last w digits corresponding to an element of S, all combinations of first t digits appear it the remainders of powers of z modulo p^{wt}. This means that any number in the cosets in S must be in $M(1)$.

Analogously, we can prove the same thing for any other $M(x)$, $x \in \mathbb{Z}_p^\times$, and $S(x) \subseteq \mathbb{Z}_p/(p^w\mathbb{Z}_p)$ set of the remainders of numbers of the form xz^n modulo p^w. All the conclusions from before follow by multiplying all of those elements by x, which is invertible in all of the considered quotients.

Thus we're allowed to conclude that

$$\mathbb{Z}_p^\times = \bigcup_{i=1} M(i)$$

which means that $\mathbb{Z}_p$ is covered by a countable number of minimal sets. □

Remark 4.2.15. *In the case where A is a root of unity of order o, the finitude of its orbits (which must then be their own closure) implies that there must be an uncountable number of minimal sets, as $\mathbb{Z}_p$ is uncountable.*

Even though the one-dimensional case may seem a little trivial *a priori*, and not all that interesting in the grand scheme of things (don't forget, our original motivation was the conjugacy problem, which isn't interesting at all in the one-dimensional case), its contrast with the multidimensional seems like enough of a reason to go through it.

But mostly, we've gone through these results to complement the result about the general case. By doing so, we feel like it's time to finish this section about the action on these spaces and move onward to the next chapter.

Chapter 5

Conjugacy problem

Let $M(n, R)$ be the set of $n \times n$ matrices over a ring R and $G \subseteq M(n, R)$ a group of matrices. The conjugacy problem over $M(n, R)$ and G tries to answer if, given $A, B \in M(n, R)$, there is a $C \in G$ such that $CA = BC$.

In the case where R is a field and G is the group of invertible matrices in $M(n, R)$, the problem is solved, as it amounts to computing the Frobenius Normal Form of both of them and seeing if they're the same. However, in other cases the problem isn't quite that simple.

The problem that motivated this work was precisely the conjugacy problem on integer matrices: finding out if for two matrices $A, B \in M(n, \mathbb{Z})$ there is a matrix $C \in GL(n, \mathbb{Z})$ such that $CA = BC$.

5.1 Conjugacy problem on integer matrices

One of the most classic instances of the conjugacy problem, and the greatest motivation behind this thesis, is the conjugacy problem over $\mathcal{M}(n, \mathbb{Z})$. More precisely, there are two "subproblems", the conjugacy problem over $\mathcal{M}(n, \mathbb{Z})$ and $GL(n, \mathbb{Z})$, and the one over $\mathcal{M}(n, \mathbb{Z})$ and $SL(n, \mathbb{Z})$.

Now, the conjugacy problem on integer matrices (both regarding the linear group and the special linear group) is currently an almost completely open problem, and attempts of enumerating conjugacy classes or providing an algorithm that's capable of deciding if two matrices are similar haven't succeeded, other than in some rather specific cases.

In order to provide some context, we'll go through some relevant results about this problem. The first rather specific case we'll want to consider is when $n = 2$. In that case, the problem is solved [AO81], as we shall see.

With the aim of presenting this result, we must first introduce the concept of *continued fractions*.

Definition 5.1.1. *A continued fraction is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

and is represented by $[a_0, a_1, a_2, a_3, \dots]$, where the a_i are positive real numbers.

$[a_0, a_1, \dots, a_n]$ is used to note

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots + \cfrac{1}{a_n}}}}$$

and $[a_0, a_1, a_2, a_3, \dots]$ represents the limit of the sequence $(x_n)_{n \in \mathbb{N}}$ where $x_n = [a_0, a_1, \dots, a_n]$.

Given $\alpha = [a_0, a_1, a_2, a_3, \dots]$ with $a_i \in \mathbb{Z}$ for all i, we note α_n the real number such that $\alpha = [a_0, a_1, \dots, a_{n-1}, \alpha_n]$.

We say a continued fraction $[a_0, a_1, a_2, a_3, \dots]$ is *eventually periodic* if $a_i \in \mathbb{N}$ for all $i \in \mathbb{N}$ and $(a_n)_{n \in \mathbb{N}}$ is eventually periodic. If $(a_n)_{n \in \mathbb{N}}$ is such that, for all $i \geq k$, $a_i = a_{i+P}$ for some $P \in \mathbb{N}$, then we may write $[a_0, a_1, a_2, a_3, \dots]$ as $[a_0, a_1, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+P-1}}]$.

The theme of continued fractions is very widely known and has been studied for a long time - we won't be taking a long tour through it. We'll simply present an equally known result that we'll be needing soon.

Lemma 5.1.2. *A continued fraction is eventually periodic if and only if it represents a number of the form $\frac{A+\sqrt{D}}{B}$, where A, B, D are integers and $D > 0$.*

Taking this into account, we can now enunciate the result that solves the conjugacy problem over $GL(2, \mathbb{Z})$ (and $GL(2, \mathbb{Z})$ or $SL(2, \mathbb{Z})$).

Theorem 5.1.3. *Let $A, B \in GL(n, \mathbb{Z})$ with the same characteristic polynomial $x^2 - tx + 1$. Assume $t \geq 0$ (if not, multiply both by $-Id$).*

- *if $t = 0$, A is similar to $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, respectively if $b > 0$ or $c > 0$.*
- *if $t = 1$, A is similar to $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, if $b > 0$ or $c > 0$, respectively.*
- *if $t = 2$, A is similar to a power of $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ or a power of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, if $b > 0$ or $c > 0$, respectively.*
- *If $t > 2$, let $\phi(\left(\begin{smallmatrix} x_1 & x_3 \\ x_2 & x_4 \end{smallmatrix}\right)) = \frac{t+\sqrt{t^2-4}-2x_4}{2x_2}$ (assuming the determinant is 1). If $\alpha = \phi(A)$ and $\beta = \phi(B)$, A and B are conjugates over $GL(n, \mathbb{Z})$ (over $SL(n, \mathbb{Z})$) if and only if $\alpha_n = \beta_m$ (and, for the special linear group case, there are $n, m \in \mathbb{N}$ such that $2|m - n$).*

This result may be pretty specific, as it's only regarding dimension 2 over the integers, but there are some things we can say about more general cases. For instance, the Latimer-MacDuffee-Taussky Theorem [LM33], which will come next in our tour.

Let D be a principal ideal domain and $A \in \mathcal{M}(n, D)$ with an irreducible characteristic polynomial $f(X)$. In the quotient $D[X]/(f(X))$, we identify X's equivalence class with β, and hereinafter we denote this ring as $D[\beta]$.

Considering its field of fractions F, we can look at A as an F-linear application, which means there must be an eigenvector u associated to the eigenvalue β. Let $u_1, \ldots, u_n$ be its entries and let I_A be the D-submodule of K generated by $u_1, \ldots, u_n$.

Now that we've introduced this whole thematic, we can present the theorem:

Theorem 5.1.4 (Latimer-MacDuffee-Taussky)**.** *Let $A, B \in M(n, D)$ with the same irreducible and separable characteristic polynomial. There is a $C \in GL(n, D)$ such that $CA = BC$ if and only if there's an $\alpha \in K$ such that $I_A = \alpha I_B$.*

As we said, this second result is a lot more general than the previous one, both in the dimension we are working on and the ring that we are studying.

Besides these two results, the similarity problem over the integers with $n = 3$ is also solved, as we can see in [AO82]. However, compared to dimension 2, it's a little more complicated, with this result depending both on the case where $n = 2$ and on the Latimer-MacDuffee-Taussky theorem.

Our initial focus was the conjugacy problem on integer matrices and our motivation for studying the p-adic numbers was the local-global principle: maybe the conjugacy of matrices over the p-adic numbers has implications on the problem over the integers.

It isn't as straightforward as "Any two matrices that are similar over the p-adic numbers for all p are similar over the integers", as there are counter examples for that attempt of a proposition, but even then it's possible that something interesting could come to light when studying the conjugacy problem over the p-adic numbers.

5.2 Conjugacy problem on p-adic matrices

As we were previously saying, studying the conjugacy problem on p-adic matrices clearly has its motivations. What there may be to prove, however, is not clear to see.

When it comes to the conjugacy problem over the p-adic numbers, a proposition such as the one about dimension 2 over the integers may seem interesting, but issues arise when looking at the role of continued fractions in the original case, as the factorizations related to them do not seem to exist in the p-adic case.

On the other hand, if we blindly believed in the magic of continued fractions, independently of their role in the proof, we should also end up disappointed as there still isn't any consensually good notion of continued fraction on the p-adic numbers [Mil07].

However, these apparent setbacks shouldn't affect our hopes of finding any theorem specific to the conjugacy problem on p-adic matrices as we may note, for instance, by taking a look at a theorem from [AO83] which reduces the conjugacy problem to checking a finite number of possible candidates for the conjugacy.

First of all, let us try to "unify" conjugacy over $SL(n, \mathcal{O}_K)$ and $GL(n, \mathcal{O}_K)$.

Lemma 5.2.1. *Let K be a local field, π a uniformizer, and $n > 1$ an integer. There's an integer λ such that if $x \equiv 1(\mod \pi^\lambda)$, then there's $\zeta \in \mathcal{O}_K$ such that $x = \zeta^n$.*

Proof. This can be proved by considering 2.2.14. Let $\lambda = 2v_\pi(n) + 1$. We can consider the polynomial $f(X) = X^n - x$ and its formal derivative, $f'(X) = nX^{n-1}$. By evaluating these polynomials on x, we get that $v_\pi(f'(x)) = v_\pi(n)$, while $v_\pi(f(x)) = v_\pi(x(x^{n-1} - 1)) \geq \lambda = 2v_\pi(n) + 1$, as $x \equiv 1(\mod \pi^\lambda)$.

We are then in the conditions of 2.2.14, as $v_\pi(f(x)) > 2v_\pi(f'(x))$, which means there's a $u \in \mathcal{O}_K$ such that $u^n = x$. □

This lemma will be useful later during the proof. Now, in order to move forward, it's a good idea to mention the Smith Normal Form.

Lemma 5.2.2. *Let $A \in \mathcal{M}(n, R)$, where n is a positive integer and R is a principal ideal domain. Then, there are matrices $B, C \in GL(n, R)$ and a diagonal matrix $D = diag(\alpha_1, \dots, \alpha_r, 0, \dots, 0)$ with $r \leq n$ such that $\alpha_i | \alpha_{i+1}\ \forall 1 \leq i < r$ and $A = BDC$. The terms α_i are unique up to multiplication by a unit.*

Proof. Section 3.7 in [Jac12] □

For any matrix $A \in \mathcal{M}(n, \mathcal{O}_K)$ we can take $D = diag(\pi^{k_1}, \dots, \pi^{k_r}, 0, \dots, 0)$, where the exponents $0 \leq k_1 \leq \dots \leq k_r$ are non-negative integers and $r \leq n$ is the rank of A. That leads us to the next lemma.

Lemma 5.2.3. *Let K be a local field, n a positive integer and π a uniformizer. Let $A \in \mathcal{M}(n, \mathcal{O}_K)$ with smith normal form $D = diag(\pi^{k_1}, \dots, \pi^{k_r}, 0, \dots, 0)$, $x', y \in \mathcal{O}_K^n$, $z \in K^n$ and λ a non-negative integer such that $Az = y$ and $Ax' \equiv y(\mod \pi^{k_r + \lambda})$.*

Then there's $x \in \mathcal{O}_K^n$ such that $Ax = y$ and $x \equiv x'(\mod \pi^\lambda)$.

Proof. This essentially looks like a version of Hensel's lemma for matrices. However, the proof isn't very similar to that lemma's proof.

First and foremost, let us consider $B, C \in GL(n, \mathcal{O}_K)$ such that $BAC = D$. Now let us consider the vectors $C^{-1}z$ and $h' = C^{-1}x'$. We have

$$D(C^{-1}z) = BAC(C^{-1}z) = By = (b_1, \dots, b_r, 0, \dots, 0)$$

These b_i, $1 \leq i \leq r$ must be in $\mathcal{O}_K$ as this is equal to By and these two only have entries that are in $\mathcal{O}_K$, and its other entries must be 0 as it is equal to $D(C^{-1}z)$. Analogously, and considering our hypothesis, we have

$$Dh' = D(C^{-1}x) = BAC(C^{-1}x') \equiv By(\mod \pi^{k_r + \lambda})$$

Then we have, for all $1 \leq i \leq r$

$$\pi^{k_i} h'_i \equiv b_i(\mod \pi^{k_r+\lambda}) \tag{**}$$

As, for each $1 \leq i \leq r$ $k_i \leq k_r + \lambda$, we know that $\pi^{k_i} | \pi^{k_r+\lambda}$, and by the previous congruence that $\pi^{k_r+\lambda} | \pi^{k_i} h'_i - b_i$ for each $1 \leq i \leq r$. As trivially $\pi^{k_i} | \pi^{k_i} h'_i$ for each i, this means that, for each i,

$$\pi^{k_i} | b_i$$

We can then consider, for each $1 \leq i \leq r$, $h_i = b_i \pi^{-k_i}$. By dividing both sides by π^{k_i} we obtain from ** that

$$h_i \equiv h_i(\mod \pi^{k_r - k_i + \lambda})$$

Which yields $h \equiv h'(\mod \pi^{\lambda})$. By our definition of h, $Dh = b$, thus by taking $x = Ch$, we get

$$Ax = (B^{-1}DC^{-1})(Ch) = B^{-1}Dh = B^{-1}b = B^{-1}By = y$$

The only thing that's left to prove is that $x \equiv x'(\mod \pi^{\lambda})$. Let us recall that $x = Ch$ and h' was defined as $C^{-1}x'$, which means $x' = Ch'$. From $h \equiv h'(\mod \pi^{\lambda})$, it's then clear $x \equiv x'(\mod \pi^{\lambda})$. □

This was the most important part of the journey towards the result we're going to present. The only thing that's left to notice is that we can consider the linear map

$$\begin{aligned} C_{A,B} : \mathcal{M}(n, \mathcal{O}_K) &\to \mathcal{M}(n, \mathcal{O}_K) \\ X &\mapsto AX - XB \end{aligned}$$

as a linear map from $\mathcal{O}_K^{n^2}$ to itself. If $D = diag(\pi_{k_1,\dots,\pi^{k_r},0,\dots,0)}$ is the Smith Normal Form of $C \in \mathcal{M}(n^2, \mathcal{O}_K)$ corresponding to the map $C_{A,B}$, we take $\mu_{A,B} = k_r$ We now have all of the ingredients we need in order to present that result about the conjugacy problem in $\mathcal{O}_K$.

Theorem 5.2.4. *Let K be a local field, π a uniformizer, and $A, B \in M(n, \mathcal{O}_K)$. If we consider $\mu_{A,B}$ as the greatest exponent present in the Smith Normal Form of $C_{A,B} : X \mapsto AX - BX$ and λ as in 5.2.1, A and B are similar over $SL(n, \mathcal{O}_K)$ (resp. over $GL(n, \mathcal{O}_K)$) if and only if there's a matrix $X \in M(n, \mathcal{O}_K)$ such that $AX \equiv XB(\mod \pi^{\mu_{A,B}+\lambda})$ and $\det X \equiv 1(\mod \pi^{\lambda})$ (resp. $AX \equiv XB(\mod \pi^{\mu_{A,B}})$ and $\det X \not\equiv 0(\mod \pi)$).*

Proof. This proof depends mainly on 5.2.3 and 5.2.1. For the general linear group case, we simply need to use the former. Notice that even though we're presenting this result as one about products and sums of matrices, this is simply about a linear map on X.

We know $X = 0$ is such that $AX - XB = 0$. If there's also an $X \in \mathcal{M}(n, \mathcal{O}_K)$ such that $AX - XB \equiv 0(\mod \pi^{\mu_{A,B}+\lambda})$ and $\det(X) \not\equiv 0(\mod \pi)$, then we know there must be $Y \equiv X(\mod \pi^{\lambda})$ such that $AY = YB$. By this last congruence we can also conclude that $\det(Y) \not\equiv 0(\mod \pi)$, which means $Y \in GL(n, \mathcal{O}_K)$.

If we consider the problem over the special linear group, we need something else. $X = 0$ is such that $AX - XB = 0$, and we know there is a certain $X \in \mathcal{M}(n, \mathcal{O}_K)$ such that $AX - XB \equiv 0(\mod \pi^{\mu_{A,B}+\lambda})$ and $\det(X) \equiv 1(\mod \pi^{\lambda})$. Then, by 5.2.3, once again, we get that there's a certain $Y \in GL(n, \mathcal{O}_K)$ such that $AY = YX$ and $Y \equiv X(\mod \pi^{\lambda})$, and thus $\det(Y) \equiv 1(\mod \pi^{\lambda})$. However, this isn't in itself stating that $Y \in SL(n, \mathcal{O}_K)$. In order to find a matrix that satisfies that, we must consider 5.2.1: λ is such that there is a $\zeta \in \mathcal{O}_K$ that verifies $\zeta^n = \det(Y)$. Therefore, $Z = \zeta^{-1}Y \in SL(n, \mathcal{O}_K)$ and $AZ = ZB$.

The reciprocal is trivial. If A and B are similar by a matrix X, then they're also similar modulo any power of π by X. □

This effectively solves the conjugacy problem over $\mathcal{M}(n, \mathbb{Z}_p)$ and $SL(n, \mathbb{Z}_p)$ (or $GL(n, \mathcal{O}_K)$), but it doesn't do so in the "cleanest" of ways. We are presented with an algorithm that checks in finite time if two matrices are similar.

But even though we can even find upper bounds for how long it takes to decide the answer, as this integer m is computable, it's nevertheless a bruteforce algorithm we are talking about and not an elegant description of the conjugacy classes.

We have at some point stated that this looked somewhat similar to a Hensel lemma about linear maps. One could ask if it was possible to apply some kind of multivariate version of Hensel's lemma to the conjugacy problem. As it turns out, there's at least not many reasons to believe that is the case.

First of all, we should actually get a hold of some actual multivariate Hensel's lemma [Con20]. In order to do so, let us define the concepts we'll be using.

Definition 5.2.5. *Let K be a local field, n a positive integer and*

$$f : \mathcal{O}_K^n \to \mathcal{O}_K^n$$
$$(x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

Where, for each $1 \le i \le n$, $f_i \in \mathcal{O}_K[X_1, \dots, X_n]$.

The Jacobian matrix and the Jacobian determinant of f are, respectively

$$Df(x_1, \dots, x_n) = \left(\frac{\partial f_i}{X_j}(x_1, \dots, x_n)\right)_{1 \le i,j \le n}$$

and

$$J_f(x_1, \dots, x_n) = \det(Df(x_1, \dots, x_n))$$

Theorem 5.2.6. *Let K be a local field with absolute value $|\cdot|$, n a positive integer, d the distance induced by $|\cdot|$ in K^n and*

$$f : \mathcal{O}_K^n \to \mathcal{O}_K^n$$
$$(x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

Where, for each $1 \le i \le n$, $f_i \in \mathcal{O}_K[X_1, \dots, X_n]$. Let the Jacobian matrix and the Jacobian determinant *of f be, respectively, Df and J_f. If there's an $a_0 \in \mathcal{O}_K^n$ such that*

$$d(f(a_0), 0) < |J_f(a_0)|^2$$

Then, there's an $a \in \mathcal{O}_K^n$ such that $d(a, a_0) < |J_f(a)|$ and $f(a) = 0$.

Proof. Available in [Con20] □

Remark 5.2.7. *This theorem can be viewed as a generalization of 2.2.14, as when $n = 1$, $d(f(x_1), 0) = |f(x_1)|$ and $|J_f(x_1)| = |f'(x_1)|$.*

This theorem is effectively a multivariate version of Hensel's lemma, thus we may consider applying it to the linear function

$$\begin{aligned} C_{A,B} : \mathcal{O}_K^{n^2} &\to \mathcal{O}_K^{n^2} \\ X &\mapsto AX - XB \end{aligned}$$

Where $A, B, C \in \mathcal{M}(n, \mathcal{O}_K)$ are considered as vectors of length n^2. If we try to apply 5.2.6 to this function, the computations are quite simple, as, if $C \in \mathcal{M}(n^2, \mathcal{O}_K)$ is the matrix corresponding to the linear application $C_{A,B}$, we have

$$DC_{A,B}(X) = C,\ J_{C_{A,B}}(X) = \det(C)$$

Unfortunately for our aspirations, however, these simple computations only end up allowing us to conclude more quickly that naively applying this theorem won't help us obtain a new perspective on the conjugacy problem in $\mathcal{O}_K$.

That's due to the fact that, if A, B have the same characteristic polynomial, the Jacobian determinant of $C_{A,B}$ will always be 0, which won't allow the inequality $d(f(a_0), 0) < |J_f(a_0)|^2$ to ever be satisfied.

Lemma 5.2.8. *Let K be a field, n a positive integer and $A, B \in \mathcal{M}(n, K)$ with the same characteristic polynomial f. Let $C \in \mathcal{M}(n, K)$ be the matrix corresponding to the linear map $X \mapsto AX - XB$. Then,*

$$\det(C) = 0$$

Proof. Let L be a field extension of K where there is a $z \in L$ such that $f(z) = 0$. Such an extension must exist, by Kronecker's Field Extension Theorem (Theorem 21.5 in [Jud09]). Let λ be an eigenvalue shared by A and B. Let B^T be the transpose of B. It has the same characteristic polynomial as B, so it must also have λ as an eigenvalue. Let $u, v \in K^n$ be λ-eigenvectors of A and B^T, respectively.

Let v^T be the transpose of v (which means it is a row vector). We claim $Y = uv^T$ is a non-trivial zero of the linear application corresponding to C. As both vectors are different from the zero vector, $Y \neq 0$.

Now let us note it is indeed a zero of that linear map.

$$\begin{aligned} AY - YB = A(uv^T) - (uv^T)B &= \\ = \lambda uv^T - u(v^T B) &= \\ = \lambda uv^T - u(\lambda v^T) &= \\ = \lambda uv^T - \lambda uv^T &= \\ = 0 & \end{aligned}$$

Therefore C has a non-trivial kernel, which means its determinant must be 0. □

From this lemma we end up concluding that this multivariate Hensel lemma doesn't seem to be of much use in this problem, as we aren't under the conditions that are necessary in order to apply it: the inequality $d(f(a_0), 0) < |J_f(a_0)|^2$ can never be verified.

Noticing this ends up showing that 5.2.4 is a lot more than a mere application of the ideas present in Hensel's lemma and that tackling the conjugacy problem must involve new ideas that go beyond the scope of the most standard results about local fields.

Nevertheless, there's no need to lose hope in finding results that seem more elegant than reducing the conjugacy problem to a finite brute force verification. For instance, we may take a look at the following theorem present in [AO83].

Theorem 5.2.9. *Let K be a local field and v_π its normalized valuation function. Let $S(f) \subset M(n, \mathcal{O}_K)$ be the set of matrices with characteristic polynomial f and let δ be the discriminant of f. If $v_\pi(\delta) < 1$ then any two matrices in $S(f)$ are similar over $SL(n, \mathcal{O}_K)$.*

If the characteristic polynomial of an integer matrix is separable, it must have a non-zero discriminant. Therefore, it must have a finite number of integer divisors, which means that the conjugacy problem regarding that matrix is trivial for $\mathbb{Z}_p$, for almost all primes p. This means that two matrices being similar over $\mathbb{Z}_p$ for all primes p is, in fact, a condition far weaker than we would like it to be, considering our original aspirations, as it simply corresponds to being similar over a finite set of finite quotients of $\mathbb{Z}$.

Example 5.2.10. *Let us take a look at a case where similarity over the integers and over all of the p-adic integers clearly isn't the same. For instance, let us consider $A = \left(\begin{smallmatrix} 9 & 8 \\ 1 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 8 & 5 \\ 3 & 2 \end{smallmatrix}\right)$, with characteristic polynomial $X^2 - 10X + 1$ and discriminant 96.*

By 5.2.9, they are similar over $GL(2, \mathbb{Z}_p)$ for all primes other than 2 or 3. In order to discover if they are similar over $GL(2, \mathbb{Z}_2)$ and $GL(2, \mathbb{Z}_3)$, we'll only have to discover if they are similar as matrices over certain finite quotients of $\mathbb{Z}$, by 5.2.4.

We can compute $C_{A,B}$'s Smith Normal Form and conclude $\mu_{A,B} = 0$, which means we simply have to guarantee they are similar by a matrix with non-zero determinant in $\mathbb{Z}/p\mathbb{Z}$, with $p \in \{2, 3\}$. This is, we simply have to verify if they're similar in $GL(2, \mathbb{Z}/p\mathbb{Z})$, for $p \in \{2, 3\}$.

And they certainly are, as we can see by considering the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix}\right)$, which are witnesses of their similarity over the two non-trivial cases. This means A and B are similar over $GL(2, \mathbb{Z}_p)$ for all primes p.

However, they aren't similar over $GL(2,\mathbb{Z})$, as we can see by applying 5.1.3. Their associated continued functions are, respectively, $[\overline{8,1}]$ and $[\overline{2,1,1,1}]$. The tails of their corresponding sequences are always different from one another, so A and B are not similar over $GL(2,\mathbb{Z})$.

5.3 Bowen-Franks groups

In this section we intend to focus on a certain class of conjugacy invariants related to the kernels and finite orbits of an automorphism. In order to notice we're actually dealing with invariants over conjugacy, we must first prove the following lemma:

Lemma 5.3.1. *Let K be a local field, n a positive integer and $A, B \in \mathcal{M}(n, \mathcal{O}_K)$, $C \in GL(n, \mathcal{O}_K)$ such that $CA = BC$. Considering these as endomorphisms of $(K/\mathcal{O}_K)^n$, we know that the kernels of the conjugated endomorphisms are isomorphic to one another.*

Proof. Let $\ker(A), \ker(B) \subseteq (K/\mathcal{O}_K)^n$. We must simply notice that $x \in (K/\mathcal{O}_K)^n$ is in $\ker(A)$ if and only if $Cx \in \ker(B)$.

If $Ax = 0$, then $0 = C0 = CAx = B(Cx)$, thus $x \in \ker(A) \Rightarrow Cx \in \ker(B)$.

If $BCx = 0$, then $0 = BCx = CAx$, so $Ax \in \ker(C) = \{0\}$. □

This means that, up to isomorphism, the kernels of endomorphisms of the torus are invariant over conjugacy. However, this isn't everything that can be said about this line of thought.

Given a matrix $A \in \mathcal{M}(n, \mathcal{O}_K)$ and a polynomial $f \in K[X]$, where $f = a_n X^n + \cdots + a_1 X + a_0$ we can easily define $f(A)$ (when $f(A) \in \mathcal{M}(n, \mathcal{O}_K)$) as the following endomorphism of $\mathcal{M}(n, \mathcal{O}_K)$:

$$\sum_{i_0}^{n} a_n \times A^n$$

This definition allows us to look into an infinity of conjugacy invariants known as the Bowen-Franks groups.

Definition 5.3.2. *Let K be a local field, n a positive integer, $A \in GL(n, K)$ and $f \in K[x]$ such that $f(A) \in \mathcal{M}(n, \mathcal{O}_K)$.*

The Bowen-Franks group of A regarding f is

$$BF_f(A) = ker(f_{K/\mathcal{O}_K}(A))$$

where $f_{K/\mathcal{O}_K}(A)$ is the endomorphism of $K/\mathcal{O}_K$ induced by $f(A)$.

The infinite amount of choices for the polynomial f is precisely what lets us have an infinite amount of conjugacy invariants - however it might be a good idea to make sure we're really in the presence of conjugacy invariants.

Corollary 5.3.3. *Let K be a local field, n a positive integer and $A, B \in \mathcal{M}(n, \mathcal{O}_K)$, $C \in GL(n, \mathcal{O}_K)$ such that $CA = BC$, $f \in K[X]$ such that $f(A), f(B) \in \mathcal{M}(n, \mathcal{O}_K)$. $BF_f(A)$ and $BF_f(B)$ are isomorphic.*

Proof. As it's suggested by virtue of this being a corollary, it's a direct consequence of the previous lemma, 5.3.1. That is, if $CA = BC$, then it's trivial that $Cf(A) = f(B)C$ and, as such, we can simply apply the previous lemma to conclude that $BF_f(A)$ and $BF_f(B)$ are indeed isomorphic. □

Remark 5.3.4. *We might refer to $BF_{X^k-1}(A)$ simply as $BF_k(A)$. No confusions should arise, as Bowen-Franks groups regarding constant polynomials serve no interest at all.*

$$per_A(k) = \{x \in (K/\mathcal{O}_K)^n : A^k x = x\}$$

Now that we've shown that Bowen-Franks groups are indeed invariants, we're interested in proving an isomorphism between those groups and some rather simpler quotients of $\mathcal{O}_K^n$.

Theorem 5.3.5. *Let K be a local field, n a positive integer, $A \in \mathcal{M}(n, \mathcal{O}_K)$, $f \in K[X]$ such that $f(A) \in GL(n, K) \cap \mathcal{M}(n, \mathcal{O}_K)$. Then, $BF_f(A)$ is isomorphic to $\mathcal{O}_K^n/((f(A))\mathcal{O}_K^n)$.*

In order to prove this theorem, we must make use of the Snake lemma.

Lemma 5.3.6 (Snake lemma)**.** *Let A, B, C, A', B', C' be abelian groups. Consider the following diagram*

$$\begin{tikzcd}
 & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' &
\end{tikzcd}$$

where the rows are exact sequences and 0 is the group with one element. Then there is an exact sequence of the form

$$\ker a \to \ker b \to \ker c \to A'/a(A) \to B'/b(B) \to C'/c(C)$$

Proof. Lemma 9.1 in [Lan02] □

With this in mind, we can now prove the theorem we've stated.

Proof. In order to prove the previous theorem, we need to consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^n \arrow[r] \arrow[d, "T_{\mathcal{O}_K}"] & K^n \arrow[r] \arrow[d, "T_K"] & (K/\mathcal{O}_K)^n \arrow[r] \arrow[d, "T_{(K/\mathcal{O}_K)}"] & 0 \\
0 \arrow[r] & \mathcal{O}_K^n \arrow[r] & K^n \arrow[r] & (K/\mathcal{O}_K)^n \arrow[r] & 0
\end{tikzcd}$$

where the functions within the rows are the canonical functions to be considered in such cases. Respectively, from left to right, the inclusion function and the projection function. It's clear the inclusion map is injective and the projection map is surjective and, as such, we're indeed in the presence of an exact sequence. Now, the functions that go from one row to the other are the linear maps corresponding to $f(A)$, differing of course in their domains and codomains.

As we've assumed $f(A) \in GL(n, K)$, T_K must be an automorphism, which means its kernel is trivial and so is the quotient $K^n/(T_K(K^n))$. That means we get the following from the Snake lemma:

$$0 \to \ker T_{(K/\mathcal{O}_K)^n} \to \mathcal{O}_K^n/(T_{\mathcal{O}_K}(K)) \to 0$$

More specifically, the two sets in the middle are isomorphic. As the left-hand side is, by definition, $BF_f(A)$, we get that

$$BF_f(A) \cong \mathcal{O}_K^n/((f(A))\mathcal{O}_K)$$

□

Let us take a quick glance at what happens when we focus on periodic points on the torus. This is,

Definition 5.3.7. *Let K be a local field, n, k positive integers and $A \in GL(n, K)$. We define the set of k-periodic points*

$$per_k(A) = \{x \in (K/\mathcal{O}_K)^n : A^k x = x\}$$

In other words, $per_k(A) = BF_{X^k-1}(A)$.

We can then apply the theorem about the structure of Bowen-Franks groups on this particular case, obtaining the following:

Corollary 5.3.8. *Let K be a local field, n, k positive integers, $A \in \mathcal{M}(n, \mathcal{O}_K)$ with no points with period k (other than 0).*

$per_k(A)$ is isomorphic to $(\mathcal{O}_K^n/((A^k - Id)\mathcal{O}_K^n))$.

We may be tempted to believe that these Bowen-Franks groups are finitely generated abelian groups. That's, however, untrue as a local field in itself is not a finitely generated $\mathbb{Z}$-module.

Lemma 5.3.9. *Let K be a local field. Neither K nor $\mathcal{O}_K$ are finitely generated $\mathbb{Z}$-modules*

Proof. Both K and $\mathcal{O}_K$ have the cardinality of $\mathbb{R}$, while any finitely generated $\mathbb{Z}$-module must be countable. Thus it's clear they aren't finitely generated $\mathbb{Z}$-modules. □

Even though we can't provide such a strong statement as these Bowen-Franks groups being finitely generated abelian groups, we can provide a somewhat similar statement. In fact, they must be finitely generated $\mathcal{O}_K$-modules. And as we know by 2.2.7, $\mathcal{O}_K$ is a Principal Ideal Domain. This means that the structure theorem for finitely generated modules over a principal ideal domain might be of use in trying to characterise the Bowen-Franks groups that occur in the situations we are studying.

Theorem 5.3.10. *Let R be a principal ideal domain and M a finitely generated R-module. There's a unique non-negative integer m and a unique sequence of proper ideals $\langle d_1 \rangle \supseteq \ldots \supseteq \langle d_n \rangle$ such that*

$$M \cong R^m \oplus R/\langle d_1 \rangle \oplus \ldots \oplus R/\langle d_n \rangle$$

Proof. Theorem 5 on section 12.1 of [DF91]. □

This theorem has pretty straightforward consequences on trying to characterise the Bowen-Franks groups that may occur in our problem. If π is a uniformizer of K, we get the following result:

Proposition 5.3.11. *Let K be a local field, n a positive integer, π a uniformizer of K, $A \in \mathcal{M}(n, \mathcal{O}_K)$ and $f \in K[X]$ such that $f(A) \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$. There are positive integers m, $i_1 \leq \ldots \leq i_n$ such that*

$$BF_f(A) \cong \mathcal{O}_K^m \oplus \bigoplus_{j=1}^{n} \mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$$

This same result is slightly more amusing when we focus on p-adic fields, as the finite quotients are, themselves, isomorphic to finite quotients of $\mathbb{Z}$. That is,

Corollary 5.3.12. *Let p be a prime number, n a positive integer, $A \in \mathcal{M}(n, \mathbb{Z}_p)$ and $f \in \mathbb{Q}_p[X]$ such that $f(A) \in \mathcal{M}(n, \mathbb{Z}_p)$. There are positive integers m, $i_1 \leq \ldots \leq i_n$ such that*

$$BF_f(A) \cong \mathbb{Z}_p^m \oplus \bigoplus_{j=1}^{n} \mathbb{Z}/(p^{i_j}\mathbb{Z})$$

We should note, however, that these results aren't something deeply related to the definition of Bowen-Franks groups, but simply to the structure of $\mathcal{O}_K$ submodules of $\mathcal{O}_K^n$.

We may, however, use that fact in order to get a better description of the Bowen-Franks groups that may come up. We were only considering Bowen-Franks groups $BF_f(A)$ in the case where $f(A) \in GL(n, K) \cap \mathcal{M}(n, \mathcal{O}_K)$, thus the determinant of $f(A)$ must not be 0. With some help from the Smith Normal Form, we'll move onward towards a more specific description of the Bowen-Franks groups we may encounter.

Lemma 5.3.13. *Let n be a positive integer, K a local field, and let $D \in \mathcal{M}(n, \mathcal{O}_K)$ be a diagonal matrix with entries $\alpha_1, \alpha_2, \ldots, \alpha_n$ and π a uniformizer of K.*

$$BF_X(D) \cong \bigoplus_{i=1}^{n} \mathcal{O}_K/(\pi^{v_\pi(\alpha_i)}\mathcal{O}_K)$$

Proof. This is a rather simple lemma. In order to know $BF_X(D)$, we must know the image of D, which will be

$$\bigoplus_{i=1}^{n} \alpha_i \mathcal{O}_K$$

which is obviously isomorphic to

$$\bigoplus_{i=1}^{n} \pi^{v_\pi(\alpha_i)}\mathcal{O}_K$$

In the end, we're looking for the quotient $\mathcal{O}_K^n/(D\mathcal{O}_K^n)$, which must be isomorphic to

$$\bigoplus_{i=1}^{n} \mathcal{O}_K/(\pi^{v_\pi(\alpha_i)}\mathcal{O}_K)$$

as we've stated. □

Proposition 5.3.14. *Let n be a positive integer, K a local field, π a uniformizer, $A \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$, and $B, C \in GL(n, \mathcal{O}_K)$, $D = diag(\pi^{i_1}, \ldots, \pi^{i_n}) \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$, such that D is A's Smith Normal Form (and thus $(1 \leq j \leq k \leq n) \Rightarrow i_j \leq i_k$). Then*

$$\mathcal{O}_K^n/(A\mathcal{O}_K^n) \cong \bigoplus_{j=1}^{n} \mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$$

Proof. First of all, let us note that it does make sense to talk about A's Smith Normal Form being D. $\mathcal{O}_K$ is a principal ideal domain, so that matrix D exists, and $A \in GL(n, K)$, so D must have non-zero determinant, as $\det(A) = \det(B)\det(D)\det(C)$, which means all of its diagonal entries are non-zero. Clearly we can choose D only having powers of π on its diagonal, as any non-zero element of $\mathcal{O}_K$ is a product of a power of π by a unit.

Now we're interested in showing that

$$\mathcal{O}_K^n/(A\mathcal{O}_K^n) \cong \mathcal{O}_K^n/(D\mathcal{O}_K^n)$$

We can do so by presenting an isomorphism between these two spaces. We claim that

$$\begin{aligned} F : \mathcal{O}_K^n/(A\mathcal{O}_K^n) &\to \mathcal{O}_K^n/(D\mathcal{O}_K^n) \\ x + A\mathcal{O}_K^n &\mapsto Bx + D\mathcal{O}_K^n \end{aligned}$$

is an isomorphism. First, we should note it is well defined.

With the aim of proving that, we should first note that, under our assumptions, $BA\mathcal{O}_K = BACC^{-1}\mathcal{O}_K = D\mathcal{O}_K$, as $C \in GL(n, \mathcal{O}_K)$.

Now, if $x, x' \in \mathcal{O}_K^n$ such that $x - x' \in A\mathcal{O}_K^n$, then $F(x') = Bx + B(x' - x) + D\mathcal{O}_K^n$. According to the previous paragraph, as $x - x' \in A\mathcal{O}_K^n$, $B(x' - x) \in D\mathcal{O}_K^n$, so our function is well defined.

Proving that F is surjective is trivial. By picking $B^{-1}x$ as a class representative of our object, we can find an object whose image is $x + D\mathcal{O}_K^n$, for any $x \in \mathcal{O}_K^n$. Its injectivity is simple to deduce as well: if $Bx \in D\mathcal{O}_K$, equivalently $Bx \in BA\mathcal{O}_K$, which is equivalent to $x \in A\mathcal{O}_K$. Thus $F(x + A\mathcal{O}_K) = 0$ if and only if $x \in A\mathcal{O}_K$.

This allows us to conclude that $\mathcal{O}_K^n/(A\mathcal{O}_K^n) \equiv \mathcal{O}_K^n/(D\mathcal{O}_K^n)$. On the other hand, by 5.3.13, $\mathcal{O}_K^n/(D\mathcal{O}_K^n) \equiv \bigoplus_{j=1}^{n} \mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$, and therefore we have the result we intended to prove. □

In this last result, 5.3.14, we take $A \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$, which is precisely what we require $f(A)$ to satisfy throughout this chapter. Therefore, let us state what we actually were intending to prove.

Proposition 5.3.15. *Let K be a local field, n a positive integer, π a uniformizer of K, $A \in \mathcal{M}(n, \mathcal{O}_K)$ and $f \in K[X]$ such that $f(A) \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$. There are non-negative integers $i_1 \leq \ldots \leq i_n$ such that*

$$BF_f(A) \cong \bigoplus_{j=1}^{n} \mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$$

Remark 5.3.16. *Given the conditions set in this last proposition, one could ask oneself if considering some kind of finite extension of $\mathcal{O}_K$ could give us some more information to work with, like some kind of conjugacy invariant to try and distinguish some matrices we're trying to compare.*

However, those hopes are unfounded, as these Bowen-Franks groups solely depend on the Smith

Normal Form of those matrices. If they have the same Smith Normal Form over $\mathcal{O}_K$, extending that ring won't change anything. If $\mathcal{O}_L$ is the new ring of integers, both Bowen-Franks groups will be obtained by replacing each quotient $\mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$ by $\mathcal{O}_L/(\pi^{i_j}\mathcal{O}_L)$, which doesn't provide us any kind of new information regarding the conjugacy problem and our two matrices.

Besides allowing us to prove this last result, 5.3.14 also allows us to quickly count the cardinality of a quotient $\mathcal{O}_K/(A\mathcal{O}_K)$, which also seems like a pretty amusing result. We'll start with a tiny lemma about counting the cardinality of a quotient of a local field.

Lemma 5.3.17. *Let K be a local field, n a non-negative integer and π a uniformizer. Let q be the cardinality of $r_K = \mathcal{O}_K/(\pi\mathcal{O}_K)$. Then, $\#(\mathcal{O}_K/(\pi^n\mathcal{O}_K)) = q^n$.*

Proof. This amounts to recalling an idea we've talked about a long time ago, in the end of section 2.2.1. Elements of $\mathcal{O}_K$ are power series in π, which means that counting $\#(\mathcal{O}_K/(\pi^n\mathcal{O}_K))$ is equivalent to counting the number of polynomials of degree less that n with coefficients in r_K. Now, there are q^n possibilities of doing so, like we wanted to prove. □

Taking this into account, we can now try to prove our result about counting $\#(\mathcal{O}_K/(A\mathcal{O}_K))$.

Proposition 5.3.18. *Let K be a local field, n a positive integer, $A \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n, K)$. Then*

$$\#(\mathcal{O}_K/(A\mathcal{O}_K)) = \frac{1}{|\det(A)|_\pi}$$

Proof. As we've seen in 5.3.14, the quotient we get from a matrix A is isomorphic to the one we get from its Smith Normal Form. This means, if its Smith Normal Form is $D = diag(\pi^{i_1}, \dots, \pi^{i_n})$, that

$$(\mathcal{O}_K/(A\mathcal{O}_K)) \cong \bigoplus_{j=1}^{n} \mathcal{O}_K/(\pi^{i_j}\mathcal{O}_K)$$

According to our last lemma, the cardinality of this set is $\prod_{j=1}^{n} q^{i_j}$, which we can notice is $|\det(D)|_\pi^{-1}$. But if $A = BDC$ is written in Smith Normal Form, with $B, C \in GL(n, \mathcal{O}_K)$, we have that

$$\begin{aligned} |\det(A)|_\pi &= |\det(BDC)|_\pi = \\ &= |\det(B)\det(D)\det(C)|_\pi \\ &= |\det(B)|_\pi |\det(D)|_\pi |det(C)|_\pi \\ &= |\det(D)|_\pi \end{aligned}$$

as B and C must have invertible determinants. □

This result, besides being somewhat amusing for any given case, ends up seeming even more amusing when we notice that it actually has its own *Local-global principle*. Let us show what we mean

Proposition 5.3.19. *Let $A \in \mathcal{M}(n, \mathbb{Z}) \cap GL(n, \mathbb{Q})$. Let, for any prime number p, $|\cdot|_p$ be the p-adic absolute value. Then, we have*

$$\#(\mathbb{Z}/(A\mathbb{Z})) = \prod_{p \text{ prime}} \#(\mathbb{Z}_p/(A\mathbb{Z}_p))$$

Proof. We should note all of the results we've proved from 5.2.2 and 5.3.13 for local fields can be trivially adapted to $\mathbb{Z}$. More specifically, we can prove that $\#(\mathbb{Z}/(A\mathbb{Z})) = \det(A)$.

But we know, for any $r \in \mathbb{Q}$, that $|r|_\infty \times \prod_{p \text{ prime}} |r|_p = 1$. By noticing that equality for $\det(A)$ and recalling that $|\det(A)|_p = \#(\mathbb{Z}_p/(A\mathbb{Z}_p))$, we prove our result. □

With this specific Local-global principle regarding the cardinality of a certain Bowen-Franks group regarding each ring of p-adic integers (and regarding $\mathbb{Z}$ itself) we finish this last section of our work.

Chapter 6

Conclusion

6.1 Our work in a nutshell

Our journey is almost over.

We started our adventure with a clear motivation, the integer matrix conjugacy problem. Yet, it's difficult to say that we've made any progress on it specifically. That isn't to say, however, that we didn't achieve anything with our work, even if the conjugacy problem ended up being little more that a motivation behind it.

We've studied some of the topological properties of modules over the rings of integers of local fields. We worked on a generalization of a valuation for matrices and went through some of its properties: more notably, we proved a generalization of the Lifting the Exponent Lemma for matrices and, by using that lemma, we stepped onto the dynamics of this problem to prove that, in general, there must be an uncountable amount of minimal sets.

Afterwards, we went through some known results about the conjugacy problem (both regarding the integers and the p-adic integers) and ended up proving some results about the Bowen-Franks groups of the endomorphisms we were studying.

6.2 Future Work

There still are many things that were left undone. For instance:

- Figuring out how (or if it is possible) to achieve a more general Lifting the Exponent Lemma, that works even when we're not under the conditions we imposed in our lemma.
- Figuring out if it is possible to apply the Multivariate Hensel Lemma to the conjugacy problem over local fields in a sensible way, for instance by picking a more appropriate function than the linear application itself.
- Finding more conjugacy invariants. This is a pretty open point, honestly, but it's one of the possible roads towards solving the conjugacy problem, so we can never be wrong by listing it.

Bibliography

[LM33] Claiborne G Latimer and CC MacDuffee. ‘A correspondence between classes of ideals and classes of matrices’. In: *Annals of Mathematics* (1933), pp. 313–316.

[AO81] Harry Appelgate and Hironori Onishi. ‘Continued fractions and the conjugacy problem in SL2;(Z)’. In: *Communications in Algebra* 9.11 (1981), pp. 1121–1130.

[AO82] Harry Appelgate and Hironori Onishi. ‘The similarity problem for 3x3 integer matrices’. In: *Linear Algebra and its Applications* 42 (1982), pp. 159–174.

[AO83] H Appelgate and H Onishi. ‘Similarity problem over $SL(n,\mathbb{Z}_p)$’. In: *Proceedings of the American Mathematical Society* 87.2 (1983), pp. 233–238.

[Cas86] John William Scott Cassels. *Local fields*. Vol. 3. Cambridge University Press Cambridge, 1986.

[Mor89] Sidney A Morris. *Topology without tears*. University of New England, 1989.

[DF91] David S Dummit and Richard M Foote. *Abstract algebra*. Vol. 1999. Prentice Hall Englewood Cliffs, NJ, 1991.

[Gou91] Fernando Q Gouvêa. ‘p-adic Numbers’. In: *p-adic Numbers*. Springer, 1991.

[Sto98] Arne Storjohann. ‘An $O(n^3)$ algorithm for the frobenius normal form’. In: *Proceedings of the 1998 international symposium on Symbolic and algebraic computation*. 1998, pp. 101–105.

[Lan02] Serge Lang. *Graduate Texts in Mathematics: Algebra*. Springer, 2002.

[Mil07] Justin Miller. *On p-adic continued fractions and quadratic irrationals*. The University of Arizona, 2007.

[Jud09] Thomas Judson. *Abstract algebra: theory and applications*. Virginia Commonwealth University Mathematics, 2009.

[Jac12] Nathan Jacobson. *Basic algebra I*. Courier Corporation, 2012.

[Rib12] Luis Ribes. ‘Introduction to profinite groups’. In: *Galois cohomology’, Queen’s papers in Pure and Applied Mathematics* 24 (2012).

[EHO19] Bettina Eick, Tommy Hofmann and Eamonn A O’Brien. ‘The conjugacy problem in GL (n, Z)’. In: *Journal of the London Mathematical Society* 100.3 (2019), pp. 731–756.

[Sut19] Andrew Sutherland. ‘18.785 Number Theory I, Fall 2019’. In: (2019).

[Con20] Keith Conrad. ‘A multivariable Hensel’s lemma’. In: *Lecture note available at http://kconrad. math. uconn. edu/blurbs* (2020).