On the integer matrix conjugacy problem and p-adic numbers
Extended Abstract

Alberto Cavaleiro Pacheco

October 2021

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

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.

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 (**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.

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,

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

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 2.2 (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.

Definition 2.3. *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.*

2.1.2 Absolute Values in $\mathbb{Q}$

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**.

Definition 2.4 (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 2.5 (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.

Theorem 2.6 (**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.*

2.1.3 Completions

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.

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 2.7. *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 $\mathbb{Q}_p$.*

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

Definition 2.8 (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 2.9 (Normalized valuation)**.** *A valuation v on a field K is said to be normalized if $v(K^\times) = \mathbb{Z}$.*

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

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.

Definition 2.10 (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 2.11. *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.

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

Proposition 2.12. *The group of units in $\mathcal{O}_K$, $\mathcal{O}_K^\times$ is $\{x \in \mathcal{O}_K : v(x) = 0\}$.*

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

Corollary 2.13. *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 2.14 (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.*

Corollary 2.15. *$\pi\mathcal{O}_K$ is the only maximal ideal of $\mathcal{O}_K$.*

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

Definition 2.16. *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 $\mathbb{F}_p$.

Lemma 2.17. *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.*

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

Lemma 2.18. *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 $r_i \in \{0, \ldots, p-1\}$ for all i, then we must have

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

Lemma 2.19. *Let K be a local field, π a uniformizer and $x \in K$. 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).*

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

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

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 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

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 2.20. *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 $g_1h_1 \equiv f(\mod \pi)$ and g_1 is monic.

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

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 2.21. *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 $v(a - a_0) > v(f(a_0)) - v(f'(a_0))$.

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

Lemma 2.22. *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 $a - a_0 \equiv 0 \mod p$.*

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. These extensions will still be non-archimedean valued fields as well.

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

Definition 2.23 (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 2.24. *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 2.25. *Let K be a complete valued field and V a finite-dimensional vector space over K. Any two norms on V are equivalent.*

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

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 2.27. *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 2.28. *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.*

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.

It's time to finally take a look at this hypothetical extended absolute value. 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 2.29. *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*

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

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.

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

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.

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.

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 we had not mentioned that a norm based on a non-archimedean absolute value must not necessarily induce a non-archimedean metric. In order to actually have a non-archimedean metric, we'll focus on the distance induced by the sup-norm induced by the absolute value on the corresponding field.

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. *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.

Definition 3.2. *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 3.3. *If K is a local field, K is locally compact and $\mathcal{O}_K$ is compact.*

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 3.4. *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:*

$$\begin{aligned} d : K^n \times K^n &\to \mathbb{R}^+ \\ ((x_1,\dots,x_n),(y_1,\dots,y_n)) &\mapsto \sup_{1\le i\le n}\{|x_i-y_i|_\pi\} \end{aligned}$$

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

Definition 3.5. *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:*

$$\begin{aligned} v_\pi : K^n &\to \mathbb{R}^+ \\ (x_1,\dots,x_n) &\mapsto \inf_{1\le i\le n}\{v_\pi(x_i)\} \end{aligned}$$

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, let us note the following:

Theorem 3.6 (Finite Tychonoff theorem)**.** *Let $X_1,\dots,X_n$ be compact topological spaces. Then $X_1 \times \cdots \times X_n$ is compact regarding the product topology.*

Corollary 3.7. *If K is a local field and n a positive integer, $\mathcal{O}_K^n$ is a compact space.*

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.

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

This function 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.

Besides the distance, of course we also have a topology to care about: 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 $x + \mathcal{O}_K$ is the set $x+\mathcal{O}_K$ 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.

Lemma 3.8. *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

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

By taking a look at the statement provided in the previous paragraph, we can see 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.

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 3.4.

4.1 General facts about v_π and d

Now, it makes sense to generalise the concept of valuation presented in 3.5 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. *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:*

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

Remark 4.2. *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 $v_\pi(AB) = v_\pi(A) + v_\pi(B)$.*

Lemma 4.3. *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 $v_\pi(\det(A')) = v_\pi(A') = 0$.*

Remark 4.4. *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 $v_\pi(A) = 0$.

Proposition 4.5. *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.

Corollary 4.6. *Let K be a local field, π a uniformizer, n a positive integer and $A \in \mathcal{M}(n, K)$ such that $v_\pi(\det(A)) = \pi^n v_\pi(A)$, $B \in \mathcal{M}(n, K)$. 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

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 4.7. *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 $d(w, A^m w) < \varepsilon$.*

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.

Proposition 4.8. *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 $v_2(A - Id) = 1$, 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.*

Lemma 4.9. *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 $m \in \mathbb{N}$,*

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

The statement that motivated the search of 4.8, 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 4.10. *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 $A^t = p^k M + Id$, where $M \in \mathcal{M}(n, \mathbb{Z}_p)$ is such that $p \not| M$ and $k > 0$ is an integer.*

- *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 $ord(A, 2^{j+l}) = 2^{l+1}\,\forall l \geq 0$*

Remark 4.11. *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 4.9.*

4.2.2 Orbits and minimal sets

Definition 4.12. *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 4.13. *Let K be a 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.*

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 4.14. *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 $\mathcal{O}_K^n$.*

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 $\{M(x) : x \in K^n\}$.

We're interested in introducing a measure in K (or simply in its ring of integers). We may 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 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, but it's an important step towards our next objective.

Proposition 4.15. *Let K be a local field, π a uniformizer and n a positive integer, $A \in GL(n, \mathcal{O}_K)$ and o its order modulo π. 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.*

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 $\mathbb{Q}_p$.

Proposition 4.16. *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 $\frac{p-1}{p^n}$.*

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 4.17. *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.*

Remark 4.18. *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.*

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 p-adic matrices

We may take a look at a theorem from [AO83] which reduces the conjugacy problem to checking a finite number of possible candidates for the conjugacy.

Theorem 5.1. *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 **??**, 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 $AX \equiv XB(\mod \pi^m)$ and $\det X \equiv 1(\mod \pi^m)$ (resp. $\det X \not\equiv 0(\mod \pi)$).*

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

$$\begin{aligned} f : \mathcal{O}_K^n &\to \mathcal{O}_K^n \\ (x_1, \ldots, x_n) &\mapsto (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \end{aligned}$$

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

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

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

and

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

Theorem 5.3. *Let K be a local field with absolute value $|\cdot|$, n a positive integer, d the distance induced by $|\cdot|$ in K^n and*

$$\begin{aligned} f : \mathcal{O}_K^n &\to \mathcal{O}_K^n \\ (x_1, \ldots, x_n) &\mapsto (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \end{aligned}$$

Where, for each $1 \leq i \leq n$, $f_i \in \mathcal{O}_K[X_1, \ldots, X_n]$. 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 $f(a) = 0$.

Remark 5.4. *This theorem can be viewed as a generalization of 2.21, 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 5.3 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

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

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 5.5. *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 $X \mapsto AX - XB$.*

$$\det(C) = 0$$

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 5.1 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 5.6. *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 $\mathbb{Z}$.

5.2 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 5.7. *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.*

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 $\mathcal{M}(n, \mathcal{O}_K)$: $\sum_{i_0}^{n} a_n \times A^n$

Definition 5.8. *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 5.9. *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.*

Remark 5.10. *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 5.11. *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 5.12 (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*

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

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

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 be able to describe the Bowen-Franks groups we may encounter.

Proposition 5.13. *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*

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

Besides allowing us to prove this last result, **??** 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 5.14. *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, $\#(\mathcal{O}_K/(\pi^n\mathcal{O}_K)) = q^n$.*

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

Proposition 5.15. *Let K be a local field, n a positive integer, $A \in \mathcal{M}(n, \mathcal{O}_K) \cap GL(n,K)$.*

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

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

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

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.

References

[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.

[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.

[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).