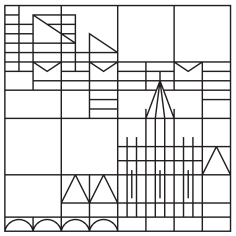
p-adic Representations of Commutative Rings

Dissertation zur Erlangung des akademischen Grades eines Doktors des Naturwissenschaften

vorgelegt von
Volkweis Leite, Samuel

an der



Mathematisch-Naturwissenschaftliche Sektion

Mathematik und Statistik

Tag der mündlichen Prüfung: 15. Februar 2013
1. Referent: Prof. Dr. Alexander Prestel
2. Referent: Jun.-Prof. Dr. Arno Fehm

Samuel Volkweis Leite
Universität Konstanz
Fachbereich Mathematik und Statistik
78464 Konstanz, Germany
samuelvolkweisleite@gmail.com

Acknowledgements

First, I would like to thank Prof. Alexander Prestel for giving me the opportunity of writing my thesis at the University Konstanz and for the inestimable lessons about the philosophy of doing mathematics and mathematical research, which I will remember for the rest of my life. His advices shaped my "mathematical character", and he was for me literally a "Doktorvater".

Secondly, I thank Prof. Cydara Cavedon Ripol for being the bridge between me and the project of studying in Germany, and for her incentive and solicitousness, without measuring efforts for helping me with everything I needed.

I also thank Professors Claus Scheiderer, Markus Schweighofer and Arno Fehm, for the knowledge they passed me during the "Vorlesungen", contributing for my academic education.

During the time of my graduate studies in Konstanz, I was sponsored by the Coordination for the Improvement of Higher Level Personnel (CAPES) of Brazil, and I am also grateful for the scholarship that I received.

At last, but not least, I would like to cordially thank my wife, Quelen Grapiglia, for supporting me in all moments during my stay in Germany, sharing with me her joy and love. Even with all the difficulties, she was always by my side encouraging me.

Abstract

Let A be a commutative ring with $\mathbb{Q} \subseteq A$ and p a prime number. We want to investigate which properties such ring must satisfy to be representable in a ring of p-adic valued continuous functions $C(X, \mathbb{Q}_p)$, where X is a Hausdorff quasi-compact topological space, i.e., compact.

By a representation, we mean a homomorphism

$$\Phi : A \to C(X, \mathbb{Q}_p)$$

such that $\Phi(1) = 1$, which is called dominant when $\Phi(A)$ is dense in $C(X, \mathbb{Q}_p)$ with respect to the p-adic sup-norm.

This will be done after studying divisibilities of commutative rings A introduced axiomatically. In particular, we will observe the canonical p-divisibility $|_0$ of $C(X, \mathbb{Q}_p)$, defined by

$$g \mid_0 f :\Leftrightarrow \forall x \in X : \ v_p(g(x)) \leq v_p(f(x)),$$

where v_p is the p-adic valuation of $\mathbb{Q}_p$.

After some results, we conclude that the existence of an abstract p-Archimedean divisibility $|$ of A is sufficient to assure the existence of a dominant representation $\Phi : A \to C(V_p^{\max}(\ | \ ), \mathbb{Q}_p)$.

Here $V_p^{\max}(\ | \ )$ denotes the set of maximal p-valuations of A extending $|$. It will be endowed with a topology which turns it into a compact space.

If $|$ satisfies a certain property, we can even characterize the kernel of Φ, using a Local-Global Principle, namely

$$1 \mid^v a \text{ for all } \ |^v \in V_p^{\max}(\ | \ ) \Rightarrow 1 \mid a,$$

where a is an arbitrary element of A. Consequently, it will be possible to determine when Φ is an isomorphism.

Part of the ideas and constructions used in this thesis can be interpreted as analogous to that used for the study of representations of commutative rings in rings of real valued continuous functions $C(X, \mathbb{R})$ with X compact.

Actually, the theory of Archimedean rings and its representations were the motivation for this work and we followed the well succeeded philosophy, already used in [11] and [20], of finding results in the p-adic case in analogy to the ones known in the real case.

Zussamenfassung

Sei A ein kommutativer Ring mit $\mathbb{Q} \subseteq A$ und p eine Primzahl. Wir wollen untersuchen, welche Eigenschaften ein solcher Ring erfüllen muss, so dass es eine Darstellung in einen Ring von p-adischen wertigen stetigen Funktionen $C(X, \mathbb{Q}_p)$ gibt, wobei X ein Hausdorffscher quasi-kompakter topologischer Raum ist, d.h., ein kompakter Raum.

Unter einer Darstellung verstehen wir einen Homomorphismus

$$\Phi : A \to C(X, \mathbb{Q}_p)$$

mit $\Phi(1) = 1$, welche dominant gennant wird, falls $\Phi(A)$ dicht in $C(X, \mathbb{Q}_p)$ bezüglich der p-adischen Supremumsnorm ist.

Um dies zu erreichen studieren wir axiomatisch eingeführte Teilbarkeiten von kommutativen Ringen A. Insbesondere betrachten wir die kanonische p-Teilbarkeit $|_0$ von $C(X, \mathbb{Q}_p)$, welche durch

$$g \mid_0 f :\Leftrightarrow \forall x \in X : \ v_p(g(x)) \leq v_p(f(x)),$$

definiert ist, wobei v_p die p-adische Bewertung von $\mathbb{Q}_p$ ist.

Nach einigen Ergebnissen schließen wir, dass die Existenz einer abstrakten p-Archimedischen Teilbarkeit $|$ von A hinreichend ist, um die Existenz einer dominanten Darstellung $\Phi : A \to C(V_p^{\max}(\ | \ ), \mathbb{Q}_p)$ zu gewährleisten.

Hierbei bezeichnet $V_p^{\max}(\ | \ )$ die Menge aller maximalen p-Bewertungen von A, welche $|$ fortsetzen. Diese wird mit einer Topologie ausgestattet, so dass sie ein kompakter topologischer Raum wird.

Wenn $|$ eine gewisse Eigenschaft erfüllt, können wir sogar den Kern von $|$ mittels eines Lokal-Global Prinzips charakterisieren, nämlich durch

$$1 \mid^v a \text{ für alle } \mid^v \in V_p^{\max}(\ | \ ) \Rightarrow 1 \mid a,$$

wobei a ein beliebiges Element von A ist. Infolgedessen wird es möglich zu bestimmen, wann Φ ein Isomorphismus ist.

Ein Teil der verwendeten Ideen und Konstruktionen, die in dieser Dissertation benutzt wurden, kann als analog zu denen interpretiert werden, die für das Studium von Darstellungen von kommutativen Ringen in Ringen von reellwertigen stetigen Funktionen $C(X, \mathbb{R})$ mit kompaktem X verwendet wurden.

Eigentlich waren die Theorie der Archimedischen Ringe und ihrer Darstellungen die Motivation für diese Arbeit und wir folgten der erfolgreichen Philosophie der Suche nach Ergebnisse im p-adischen Fall in Analogie zu bereits bekannten Ergebnissen im reellen Fall, wie es in [11] und [20] verwendet wurde.

Contents

Introduction

It is usual in mathematics the attempt of finding representations of a class of mathematical objects in another, aiming to find new properties of the class of interest.

The first question to be posed is about the existence of such representations, or more precisely, we want to answer if, given an object, there is a representation of it as an object of another desired class.

For example, we can fix the class of all rings of continuous functions $C(X, \mathbb{K})$, where $\mathbb{K}$ is a completion of $\mathbb{Q}$, with respect to some absolute value of $\mathbb{Q}$, and X is a compact space[1], and we ask when a commutative ring A containing $\mathbb{Q}$ has a representation in some $C(X, \mathbb{K})$.

Here we understand that it is reasonable to define a representation as a ring homomorphism

$$\Phi : A \to C(X, \mathbb{K}) \text{ with } \Phi(1) = 1$$

As $C(X, \mathbb{K})$ is even a normed space with respect to the sup-norm, it is also possible to observe the class of **dominant representations**, i.e., representations Φ as above, with $\Phi(A)$ dense in $C(X, \mathbb{K})$, with respect to this norm.

It is well-known that each absolute value of $\mathbb{Q}$ is equivalent, either to the usual absolute value $|\cdot|_\infty$, or to the p-adic absolute value $|\cdot|_p$, for some prime number p. It follows that the completion $\mathbb{K}$ is, either the field of real numbers $\mathbb{R}$, or a field of p-adic numbers $\mathbb{Q}_p$, for some prime p.

The representations for the case $\mathbb{K} = \mathbb{R}$ were studied since the beginning of the last century, and M. Stone was the first to give a characterization of commutative rings containing $\mathbb{Q}$ being isomorphic to $C(X, \mathbb{R})$, for some compact space X.[2]

With the advent of modern Real Algebra, the problem of finding representations, and describing its kernel, could be solved using the concepts of preorderings and orderings of commutative rings and some Local-Global

[1] By compact we mean quasi-compact and Hausdorff.

[2] Articles [24] and [25].

Principles, in particular for Archimedean preorderings, which can be deduced using the Positivstellensatz.

Following this development, it also started the study of topics related to p-adic numbers and p-adic Algebra, inspired by some ideas emerged from the real case.

In this thesis, we are interested into characterize the class of commutative rings A, containing $\mathbb{Q}$, that admit a representation in the ring of continuous functions $C(X, \mathbb{Q}_p)$, with X compact. We try to do this in analogy to the characterization given in real algebra.

In order to do this, we introduce divisibilities axiomatically and interpret them as a weak notion of valuations. In particular, the introduced p-divisibilities will be the weak notion of p-valuations.

The p-divisibilities can be interpreted as the equivalent in the p-adic case to preorderings and the p-valuations to orderings of the corresponding real case. Following this correspondence, we also define a notion of p-Archimedean divisibilities, which should correspond to Archimedean preorderings.

In this work, we will prove that each commutative ring A containing $\mathbb{Q}$ and having a p-Archimedean divisibility admits a dominant representation in $C(V_p^{\max}(\ |\ ), \mathbb{Q}_p)$, where $V_p^{\max}(\ |\ )$ is the set of all maximal p-valuations extending $|\ |$, which will be endowed with a natural topology, turning it into a compact space.

We will also find some p-adic Local-Global Principles that will help us to describe the kernel of such representations (which are interesting by themselves) and hence it will be possible to give a characterization of commutative rings isomorphic to $C(X, \mathbb{Q}_p)$, for some compact space X.

At the end, we will compare the topological properties of the spaces used by representations and the algebraic properties of the represented rings. We also determine when a commutative ring $A \supseteq \mathbb{Q}$ is in $C(X_{\mathbb{Q}_p}(A), \mathbb{Q}_p)$ representable, where $X_{\mathbb{Q}_p}(A)$ is the set of all homomorphisms of A in $\mathbb{Q}_p$, endowed with a suitable topology.

To see that there is indeed some analogies between the real case and the p-adic case, we observe that it is possible to find representations in the real case because

R1. $\mathbb{Q}$ is dense in $\mathbb{R}$.

R2. $\mathbb{R}^2$ is the unique ordering of $\mathbb{R}$.

R3. If T is an Archimedean preordering of a commutative ring A, then the set of orderings extending T is non-empty.

R4. The set of **maximal** orderings extending a given preordering T is compact with respect to the real spectral topology.

R5. Every field F having an Archimedean preordering T can be T-embedded into $\mathbb{R}$, i.e., there is an embedding α satisfying $\alpha(T) \subseteq \mathbb{R}^2$.

and the description of the kernel uses that

R6. There exists a Positivstellensatz for preordered rings, implying a real Local-Global Principle for Archimedean preorderings.

In the p-adic case it was known that

P1. $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

P2. $\mathbb{Z}_p$ is the unique p-valuation ring of $\mathbb{Q}_p$.

However, we prove in this thesis that

P3. If $|$ is an p-Archimedean divisibility of a commutative ring A, then the set of p-valuations extending $|$ is non-empty.

P4. The set of p-valuations extending a given p-divisibility $|$ is compact with respect to the p-adic spectral topology (defined in Section(2.6)).

P5. Every field F having a p-Archimedean divisibility $|$ can be $|$-embedded into $\mathbb{Q}_p$, i.e., there is an embedding α satisfying

$$a \mid b \Rightarrow v_p(\alpha(a)) \leq v_p(\alpha(b)),$$

for all $a, b \in F$.

and also

P6. There are p-adic Local-Global Principles for rings with p-divisibilities, and some special ones for a class of p-Archimedean divisibilities, enabling the description of the kernel of canonical representations and the characterization of commutative rings isomorphic to some $C(X, \mathbb{Q}_p)$, with X compact.

Even being the correspondence between the properties R1-R6 and P1-P6 not just a substitution of symbols, the similarities are clear. That is why we start our work in the first Chapter reviewing how we represent rings in the real case.

Chapter 1

Representing commutative rings in $C(X, \mathbb{R})$

In this chapter we present the well-known results about representations of commutative rings in the ring of continuous functions $C(X, \mathbb{R})$, for some compact space X.

Such representations in the real case serve as a motivation for the work developed in Chapter 3, where we study representations of commutative rings in $C(X, \mathbb{Q}_p)$, with X compact.

Most results of this chapter are presented without proofs, which can be found in the literature related to them, like [18] and [13].

Let A be a commutative ring containing $\mathbb{Q}$. We start asking

When is A in $C(X, \mathbb{R})$ representable for some compact space X?

i.e., when exists a homomorphism $\Phi : A \to C(X, \mathbb{R})$ in the ring of real valued continuous functions on X with $\Phi(1) = 1$, which is called a **representation of A in $C(X, \mathbb{R})$**.

To simplify the writing, we will also use C_X to denote the ring $C(X, \mathbb{R})$ in this chapter.

If we define the **$\mathbb{R}$-spectrum of A** as

$$X_{\mathbb{R}}(A) := \{\alpha : A \to \mathbb{R} \ : \ \alpha \text{ is a homomorphism and } \alpha(1) = 1\},$$

the next theorem can be used to solve the problem above in terms of $X_{\mathbb{R}}(A)$.

Theorem 1.1.1 *Let A be a commutative ring. There is a representation $\Phi : A \to C_X$, for some compact space X, if, and only if, $X_{\mathbb{R}}(A) \neq \emptyset$.*

Proof : In fact, if $\alpha \in X_{\mathbb{R}}(A)$, taking $X = \{x\}$, we have a representation

$$\alpha : A \to \mathbb{R} \simeq C(\{x\}, \mathbb{R}),$$

and of course X is compact with respect to the trivial topology.

Conversely, if $\Phi : A \to C_X$ is a representation, for any $x \in X$, we can define a homomorphism $\alpha_x : A \to \mathbb{R}$, putting $\alpha_x(a) := \Phi(a)(x)$.

■

Note that the implication from left to right used the information of just one point $\alpha \in X_{\mathbb{R}}(A)$, giving a very poor representation of A.

We are not interested in such representations, but in those giving us as much as possible informations about the ring A. To do this, we try to find **optimal representations** of A, which is a representation $\Phi : A \to C_X$ with X homeomorphic to $X_{\mathbb{R}}(A)$.

It is also desired to relate properties of A with topological properties of C_X. That is why we want X compact, because then we can define the sup-norm on C_X, making it a complete normed $\mathbb{R}$-algebra.

In order to have richer representations, we ask

When is A in $C_{X_{\mathbb{R}}(A)}$ representable? Is $X_{\mathbb{R}}(A)$ compact?

The first question has always a positive solution. In fact, if we endow $X_{\mathbb{R}}(A)$ with the topology generated by the open sub-basis consisting of the sets

$$U_a := \{\alpha \in X_{\mathbb{R}}(A) \ : \ \alpha(a) > 0\},$$

for each $a \in A$, then the map $a \mapsto \widehat{a}$, where

$$\widehat{a} : X_{\mathbb{R}}(A) \to \mathbb{R} \ , \ \widehat{a}(\alpha) := \alpha(a)$$

defines a representation $\Phi : A \to C_{X_{\mathbb{R}}(A)}$, because it can be verified that $\widehat{a}$ is continuous.

Moreover, $X_{\mathbb{R}}(A)$ is Hausdorff and $\Phi(A)$ separates point of $X_{\mathbb{R}}(A)$, because

$$\alpha \neq \beta \in X_{\mathbb{R}}(A) \Rightarrow (\exists a \in A) : \widehat{a}(\alpha) = \alpha(a) \neq \beta(a) = \widehat{a}(\beta),$$

and hence $\widehat{a}$ separates α and β, and, without loss of generality,

$$\begin{array}{lll} (\exists q \in \mathbb{Q}) : \alpha(a) > q > \beta(a) & \overset{\Phi(1)=1,\ \mathbb{Q}\subseteq A}{\Rightarrow} & \alpha(a-q) > 0 > \beta(a-q) \\ & \Rightarrow & \alpha \in U_{a-q},\ \beta \in U_{-a+q}, \\ & & \text{and } U_{a-q} \cap U_{-a+q} = \emptyset \end{array}$$

proving the Hausdorff property.

However, in general, $X_{\mathbb{R}}(A)$ is not quasi-compact. For example, if $A = \mathbb{R}[X_1, ..., X_n]$ is the ring of polynomials in n variables over $\mathbb{R}$, it can be verified that $\mathbb{R}^n$ and $X_{\mathbb{R}}(A)$ are homeomorphic, and hence $X_{\mathbb{R}}(A)$ is not quasi-compact.

The study of $X_{\mathbb{R}}(A)$ is also related to **(pre)orderings** of A, defined below.

Definition 1.1.2 *Let A be a commutative ring with 1. A **preordering** of A is a subset $T \subseteq A$ satisfying*

- $T + T \subseteq T$
- $T \cdot T \subseteq T$
- $A^2 := \{a^2 : a \in A\} \subseteq T$
- $-1 \notin T$

*The preordering T is called an **ordering** of A, if it also satisfies*

- $T \cup -T = A$
- $supp(T) := T \cap -T$ *is a prime ideal of A*

*The set $supp(T)$ is called **support** of T. Note that $supp(T)$ is always an ideal of A when $T \cup -T = A$.*

*We define the **real spectrum** of A as the set*

$$Sper(A) := \{P \subseteq A : P \text{ is an ordering of } A\}$$

For example, the set $\mathbb{R}^2$ defines an ordering of $\mathbb{R}$ (the usual) having also a special property, called **Archimedean** property.

Definition 1.1.3 *Let A be a commutative ring containing $\mathbb{Z}$. A (pre)ordering T of A is called **Archimedean**, if it satisfies*

$$(\forall a \in A)(\exists n \in \mathbb{N}) : (n - a) \in T$$

We define also

$$Archr(A) := \{P \in Sper(A) \ : \ P \text{ is } Archimedean\}$$

An example of Archimedean preordering is the set of **totally positive continuous functions** of C_X, when X is quasi-compact, namely

$$T_0 := T_0(X) := \{f \in C_X \ : \ (\forall x \in X) : f(x) \geq 0\}, \tag{1.1}$$

also called **canonical preordering** of C_X.

We can endow $Archr(A)$ with the relative **real spectral topology**, which is in general defined for the whole real spectrum $Sper(A)$, as the topology generated by the open subbasis consisting of the sets

$$\mathcal{U}_a := \mathcal{U}_a(A) := \{P \in Sper(A) : a \notin -P\},$$

for all $a \in A$.

The main result linking the topological space $X_{\mathbb{R}}(A)$ with Archimedean orderings is:

Theorem 1.1.4 *$Archr^{\max}(A)$ is homeomorphic to $X_{\mathbb{R}}(A)$, for each commutative ring A, where the first is the set of maximal Archimedean orderings*

$$Archr^{\max}(A) := \{P \in Archr(A) : \text{there is no } P' \in Archr(A) \text{ with } P \subsetneqq P'\}$$

The homeomorphism is given by the map $P \mapsto \alpha_P$, where $\alpha_P : A \to A/supp(P)$ is the canonical projection $a \mapsto a + supp(P)$.

Moreover, given a preordering T of A, $Archr_T^{\max}(A)$ is homeomorph to $X_{T,\mathbb{R}}(A)$, where

$$Archr_T^{\max}(A) := \{P \in Archr^{\max}(A) \ : \ P \supseteq T\}$$

and

$$X_{T,\mathbb{R}}(A) := \{\alpha \in X_{\mathbb{R}}(A) \ : \ \alpha(T) \subseteq \mathbb{R}^2\}$$

The proof of this theorem uses that $\alpha^{-1}(\mathbb{R}^2)$ is a maximal Archimedean ordering of A, for each $\alpha \in X_{\mathbb{R}}(A)$, and the following important lemma.

Lemma 1.1.5 *For each $P \in Archr(A)$,*

$$P \in Archr^{\max}(A) \Leftrightarrow [\alpha_P : A \to \mathbb{R} \text{ with } a \in P \Leftrightarrow \alpha_P(a) \geq 0]$$

For this lemma, some characteristic properties of the field of real numbers $\mathbb{R}$ were used, namely:

- $\mathbb{Q}$ is dense in $\mathbb{R}$. (used implicitly)
- $\mathbb{R}^2$ is the unique ordering of $\mathbb{R}$.
- Every Archimedean ordered field can be order-embedded into $\mathbb{R}$.

We will also need to study a certain class of representations of A in C_X, for X compact, namely, the **dominant representations** $\Phi : A \to C_X$, i.e., representations with $\Phi(A)$ dense in C_X, with respect to the sup-norm of C_X.

Remember that the representation $a \mapsto \widehat{a}$ used above separates points, and hence it is also dominant, when $X_{\mathbb{R}}(A)$ is quasi-compact, because of the Stone-Weierstrass Theorem. Thus, it is reasonable to observe such a class of representations.

We also need the following result.

Proposition 1.1.6 *For a compact space X,*

$$Archr_{T_0}^{\max}(C_X) =^{1} Sper_{T_0}^{\max}(C_X) = \{P_x : x \in X\}$$

where $P_x := \{f \in C_X : f(x) \geq 0\}$, for each $x \in X$, and T_0 is the canonical preordering of C_X.

The map $x \mapsto P_x$ defines a homeomorphism between X and $Archr_{T_0}^{\max}(C_X)$.

[1] Every ordering P, extending an Archimedean preordering T, is also Archimedean.

In general, given a surjective representation $\Phi : A \to B$, where A and B are commutative rings containing $\mathbb{Q}$, and an Archimedean preordering T of B, we can prove the following theorem, relating $Archr_T^{\max}(B)$ with some subspace of $Archr^{\max}(A)$.

Theorem 1.1.7 *Let A and B be commutative rings containing $\mathbb{Q}$. Take $\Phi : A \to B$ a surjective representation, T an Archimedean preordering of B and $T_\Phi := \Phi^{-1}(T)$ the Archimedean preordering of A induced by T and Φ. Then*

$$X_{T_\Phi,\mathbb{R}}(A) \simeq Archr_{T_\Phi}^{\max}(A) \simeq Archr_T^{\max}(B) \simeq X_{T,\mathbb{R}}(B)$$

Proof : We first claim that the maps

$$\begin{aligned} &\theta : Archr_{T_\Phi}^{\max}(A) \to Archr_T^{\max}(B)\ ,\ P \mapsto \Phi(P) \\ &\Psi : Archr_T^{\max}(B) \to Archr_{T_\Phi}^{\max}(A),\ P \mapsto \Phi^{-1}(P) \end{aligned}$$

are well-defined.

It is easy to verify that $\Phi^{-1}(P)$ is an ordering of A containing T_Φ. We will also verify that $\Phi(P)$ is an ordering of B for all $P \in Archr_{T_\Phi}^{\max}(A)$.

First note that

$$\Phi(\Phi^{-1}(Y)) = Y \text{ for all } Y \subseteq B, \tag{1.2}$$

because Φ is surjective.

Thus, if $P \in Archr_{T_\Phi}^{\max}(A)$, then

$$T = \Phi(\Phi^{-1}(T)) \subseteq \Phi(P)$$

Moreover, clearly

- $\Phi(P) + \Phi(P) \subseteq \Phi(P)$,
- $\Phi(P) \cdot \Phi(P) \subseteq \Phi(P)$,
- $B^2 = \Phi(A^2) \subseteq \Phi(P)$ (by surjectivity);

because Φ is a surjective homomorphism, but maybe $-1 = \Phi(-1) \in \Phi(P)$, and in this case

$$(\exists p \in P) : \Phi(1 + p) = 0$$

However, this does not happen, because otherwise

$$1 + p \in \Phi^{-1}(\{0\}) \subseteq \Phi^{-1}(T \cap -T) = \Phi^{-1}(T) \cap -\Phi^{-1}(T) = T_\Phi \cap -T_\Phi$$

and hence

$$-1 - p \in T_\Phi \overset{T_\Phi \subseteq P}{\Rightarrow} -1 - p \in P \overset{p \in P}{\Rightarrow} -1 \in P,$$

a contradiction.

Therefore $-1 \notin \Phi(P)$ and hence $\Phi(P)$ is a preordering of B. Now, we can extend the preordering $\Phi(P)$ to some maximal ordering of B, say

$$P' \in Sper^{\max}_{\Phi(P)}(P) \subseteq Sper^{\max}_{T}(B) = Archr^{\max}_{T}(B),$$

by the fundamental theorem:

Theorem 1.1.8 *Let T be a preordering of A. Then $Sper^{\max}_{T}(A) \neq \emptyset$.*

Therefore,

$$T_\Phi \subseteq P \subseteq \Phi^{-1}(\Phi(P)) \subseteq \Phi^{-1}(P'),$$

and hence $P = \Phi^{-1}(P')$, by the maximal choice of P.

Note that this also proves that Ψ is surjective and that the range of Ψ is indeed $Archr^{\max}_{T}(B)$.

Thus

$$\Phi(P) \supseteq \Phi(\Phi^{-1}(P')) \overset{(1.2)}{=} P',$$

As $\Phi(P)$ is a preordering of B, by maximality of P' and Theorem(1.1.8), we have $P' = \Phi(P)$. Thus $\Phi(P) \in Archr^{\max}_{T}(B)$ and hence θ has range $Archr^{\max}_{T}(B)$.

We can see that Ψ is even injective, and hence a bijection, because

$$\Phi^{-1}(P) = \Phi^{-1}(P') \Rightarrow P \overset{(1.2)}{=} \Phi(\Phi^{-1}(P)) \overset{(1.2)}{=} \Phi(\Phi^{-1}(P')) = P'$$

for each $P, P' \in Archr^{\max}_{T}(B)$.

It is also continuous, because

$$\begin{aligned} \Psi^{-1}(\mathcal{U}_a(A)) &= \{P \in Archr^{\max}_{T}(B) : -a \notin \Psi(P) = \Phi^{-1}(P)\} \\ &= \{P \in Archr^{\max}_{T}(B) : -\Phi(a) \notin P\} \\ &= \mathcal{U}_{\Phi(a)}(B) \end{aligned}$$

for all $a \in A$.

As $Archr^{\max}_{T}(B)$ and $Archr^{\max}_{T_\Phi}(A)$ are compact (because of Lemma(1.1.9) below), and Ψ is bijective and continuous, we deduce that $Archr^{\max}_{T}(B)$ is homeomorph to $Archr^{\max}_{T_\Phi}(A)$, by a known result of topology.

Lemma 1.1.9 *Let T be a preodering of A. Then $Sper_T(A)$ is a quasi-compact space and $Sper^{\max}_{T}(A)$ is a compact space. In particular, if T is Archimedean, then $Archr^{\max}_{T}(A) = Sper^{\max}_{T}(A)$ is compact.*

■

As a consequence of Theorem(1.1.7) and Proposition(1.1.6), we have

Theorem 1.1.10 *Two compact spaces X and Y are homeomorphic if, and only if, C_X and C_Y are isomorphic.*

To answer the question about optimal representations, we study first its relative question.

If A has an Archimedean preordering T, there exists a dominant representation $\Phi : A \to C_{X_{T,\mathbb{R}}(A)}$?

To find such representation will not be a big problem, if we use all the results of real algebra listed until here. The difficult problem is to determine the kernel of this representation, which is a natural question.

The characterization of the kernel will be a consequence of the description of the preimage of the preordering T_0 of C_X, under our representation, which is also a natural question to be posed when studying the (pre)ordered structure of C_X.

To describe this preimage, we use some non-trivial results of real algebra, like the "Positivstellensatz", which is used to prove the following Local-Global Principle for Archimedean preorderings, fundamental for the proof of the Real Representation Theorem.

Lemma 1.1.11 *Let T be an Archimedean preordering of A. For each $a \in A$ define $\widehat{a} : Sper_T^{\max}(A) \to \mathbb{R}$ by $\widehat{a}(P) := \alpha_P(a)$.*[2] *Then*

$$[(\forall P \in Sper_T^{\max}(A)) : \widehat{a}(P) > 0] \Rightarrow [(\exists k \in \mathbb{N}^+) : ka \in 1 + T]$$

Moreover, we can verify that

Lemma 1.1.12 *For all $a \in A$, $\widehat{a}$ is continuous.*

Now we state the Real Representation Theorem for Archimedean preorderings T of A.

Actually, the important claim is the first, because the second follows from it. The third claim is just a consequence of Stone-Weierstrass theorem, because the image of A under the homomorphism Φ_T, defined below, separates points.

Theorem 1.1.13 (Real Representation Theorem) *Let A be a commutative ring containing $\mathbb{Q}$ and T an Archimedean preodering of A.*[3] *Define*

$$\mathcal{X}_T^{\max}(A) := Sper_T^{\max}(A) = Archr_T^{\max}(A)$$

The map $a \mapsto \widehat{a}$ defines a homomorphism $\Phi_T : A \to C_{\mathcal{X}_T^{\max}(A)}$ with $\Phi_T(1) = 1$ and satisfying, for T_0 as in (1.1),

[2] As T is Archimedean, $Sper_T^{\max}(A) = Archr_T^{\max}(A)$, and hence $\alpha_P(a) \in \mathbb{R}$.

[3] In particular we must have $\mathbb{Q}^+ \subseteq T$.

1. $\Phi_T^{-1}(T_0) = \{a \in A \mid (\forall n \in \mathbb{N}^+) : 1 + na \in T\}$.

2. $\ker(\Phi_T) = \Phi_T^{-1}(\{0\}) = \{a \in A \mid (\forall n \in \mathbb{N}^+) : 1 \pm na \in T\}$.

3. Φ_T *is dominant.*

At this point, we want to give a characterization of optimal representations in the next theorem. Actually, one more lemma is also needed.

Lemma 1.1.14 *Let A be a commutative ring. Then $Archr^{\max}(A)$ is closed in $Sper^{\max}(A)$ if, and only if,*

$$T_A := \bigcap_{P \in Archr^{\max}(A)} P$$

is an Archimedean preordering of A.

Proof : If $Archr^{\max}(A)$ is closed in $Sper^{\max}(A)$, then it is also quasi-compact, by Lemma(1.1.9).

For all $a \in A$, of course

$$Archr^{\max}(A) \subseteq \bigcup_{n \in \mathbb{N}} \mathcal{U}_{n-a},$$

because each $P \in Archr^{\max}(A)$ is Archimedean.

Thus, by quasi-compactness, there are $n_1, ..., n_k \in \mathbb{N}$ such that

$$Archr^{\max}(A) \subseteq \mathcal{U}_{n_1-a} \cup \cdots \cup \mathcal{U}_{n_k-a},$$

As this holds for all $a \in A$, we can deduce the Archimedean property for T_A. It is an easy verification that T_A is indeed a preordering of A.

Conversely, if T_A is an Archimedean preordering of A, then $Archr^{\max}(A) = Sper^{\max}_{T_A}(A)$, because each ordering containing an Archimedean preordering is also Archimedean. It is closed in $Sper^{\max}(A)$, because its complement is the open set

$$\bigcup_{t \in T_A} \mathcal{U}_{-t}$$

■

Now we can determine when there is an optimal representation of A.

Theorem 1.1.15 *A commutative ring A, containing $\mathbb{Q}$, has an optimal representation, i.e., a representation $\Phi : A \to C_X$ with $X \simeq X_{\mathbb{R}}(A)$ compact, if, and only if,*

$$T_A := \bigcap_{P \in Archr^{\max}(A)} P$$

is an Archimedean preordering of A.

Proof : If T_A is an Archimedean preordering of A, then the Real Representation Theorem provides the representation $\Phi_{T_A} : A \to C_{X_{\mathbb{R}}(A)}$, because of Theorem(1.1.4) and Theorem(1.1.10), and $X_{\mathbb{R}}(A)$ is compact, by Lemma(1.1.14).

Conversely, if $\Phi : A \to C_X$ is a representation with $X \simeq X_{\mathbb{R}}(A)$ compact, then, by Theorem(1.1.4), $Archr^{\max}(A) \simeq X_{\mathbb{R}}(A)$ is closed in $Sper^{\max}(A)$ [4], and hence T_A is Archimedean by Lemma(1.1.14).

■

The reader will note that the characterization of $\Phi_T^{-1}(T_0)$, given in the Real Representation Theorem, is not needed here, but just the construction of the representation Φ_T, which is guaranteed by Lemma(1.1.5), Lemma(1.1.9) and Lemma(1.1.12). Also note that, in general, $\Phi(A)$ is just a $\mathbb{Q}$-subalgebra of C_X.

We presented a Real Representation Theorem above using some recent ideas of mathematics (of the last century) coming from real algebra.

However, an algebraic **characterization** of the commutative rings isomorphic to a given ring of continuous function C_X, for a compact space X, was first given by M. H. Stone in his articles [24] and [25][5], without using the modern language of real algebra.

In [24], Stone takes a commutative ring A, containing $\mathbb{Q}$, and observes a subset T of A (a set of positive elements) and requires that the following properties are satisfied (formulated here in a modern language):

1. T is a preordering.
2. T is Archimedean.
3. $supp(T) = T \cap -T = \{0\}$.
4. For all $a \in A$, if $\left(\frac{1}{n} + a\right) \in T$ for all $n \in \mathbb{N}^+$, then $a \in T$.

   This property guarantees that the semi-norm defined by

   $$\|a\|_T := \inf\{q \in \mathbb{Q}^+ \ : \ (q \pm a) \in T\} \tag{1.3}$$

   is indeed a norm[6].
5. The normed space $(A, \|\cdot\|_T)$ is complete.

[4] Remember that $Sper^{\max}(A)$ is compact.

[5] A more extensive discussion of the continuous functions in this context was done in Stone's previous article [26].

[6] Actually, this function is cited in [24], but only written in [25].

The conclusion of Stone's papers is then: $A \simeq C_X$, for some compact space X, if, and only if, there exists $T \subseteq A$ satisfying the five properties listed above.

In fact, by the Real Representation Theorem, the properties 1-4 implies the injectivity of the dominant representation $\Phi_T : A \to C_X$. Conversely, if $\Phi : A \to C_X$ is an injective dominant representation, with X compact, one verifies that $T_\Phi := \Phi^{-1}(T_0)$ also satisfies 1-4.

The property 5. is exactly what we need to have surjectivity of such representations, because

Proposition 1.1.16 *If A has a preordering T satisfying 1-4, then*

$$(\forall a \in A) : \|a\|_T = \|\Phi_T(a)\|,$$

where $\|\cdot\|$ denotes the sup-norm of $C_{\mathcal{X}_T^{\max}(A)}$.

Note that the property 4. is equivalent to say

$$T = \Phi_T^{-1}(T_0) =: T^*,$$

but in general we can just guarantee the inclusion $T \subseteq T^*$.

Chapter 2

Axiomatic Theory of Divisibilities

The intuitive notion of divisibilities is known by all mathematicians because of the natural divisibility defined in every ring, where an element a divides b if, and only if, there is some element c such that $b = ac$.

The study of such natural divisibilities is very important for the understanding of certain ring properties, because it is clearly related to the factorization of elements as a product of simpler elements, like prime or irreducible ones.

One of the most desired property of a ring is the unique factorization of elements, a property satisfied by the ring of integers $\mathbb{Z}$, which in general fails for arbitrary rings, and even for rings of integers of algebraic number fields, like the ring $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. [1]

This failure led to the discovery of ideal theory by Eduard Kummer, which was later refined by Richard Dedekind, where the idea of factorization of one element by elements was replaced by the factorization of ideals into ideals.

In this case, we have a binary relation $\mid$, also called divisibility, defined between elements and elements, elements and ideals, as well as between ideals and ideals, where

$$a \mid b :\Leftrightarrow b \in a \cdot A \ , \ \mathfrak{a} \mid a :\Leftrightarrow a \in \mathfrak{a} \quad \text{and} \quad \mathfrak{a} \mid \mathfrak{b} :\Leftrightarrow \mathfrak{b} \subseteq \mathfrak{a}$$

for all elements a, b and any two ideals $\mathfrak{a}, \mathfrak{b}$ of a ring A.

In this chapter, we will be concerned with the divisibility relation $\mid$ introduced axiomatically. Of course the ideal theory and other facts of commutative algebra will be used and even inspire some constructions.

[1] For the verification of this fact and historical comments we indicate Chapter I, §3. of [16].

This approach will be important for the study of rings of p-adic valued continuous functions $C(X, \mathbb{Q}_p)$, because they admit a divisibility relation $|_0$, called **canonical divisibility** of $C(X, \mathbb{Q}_p)$, and defined by

$$g \mid_0 f :\Leftrightarrow \forall x \in X : \ v_p(g(x)) \leq v_p(f(x))$$

The canonical divisibility will be fundamental for our study of representations of commutative rings in $C(X, \mathbb{Q}_p)$.

Here, and for the rest of this work, p will always denote a prime natural number, unless we say the contrary.

2.1 General Definitions and Examples

In this section we give several definitions, some remarks and a few initial results, which will be better understandable after the examples given at the end.

By analogy, one can think about divisibilities $|$ as corresponding to the preorderings T of the real case, as well as the orderings P, extending T, should correspond to valuation divisibilities $|^v$, extending $|$. The support $T \cap -T$ can be replaced here by the ideal of infinitesimals $I(\ |\ )$, defined below.

In the next sections, we will see that indeed each valuation divisibility of a commutative ring A corresponds uniquely to some valuation v of A. This result motivates the definition and study of some properties of divisibilities. Here we understand a valuation as a Bourbaki valuation (see [2] or [12]).

We will define also p-divisibilities, for some prime number $p \in \mathbb{N}$. The motivation for the definition of p-divisibilities comes from the theory of formally p-adic fields developed in [20].

In this reference, it is proven that, for a given field of characteristic zero K and a valuation v of K, v is a p-valuation[2] of K if, and only if, $v(p) > v(1)$ and $v(\gamma(K)) \geq v(1)$, where γ is the (p-adic) Kochen operator. We use then this fact to give our definition.

These conditions justify the relations (2.16) and (2.17) below if we agree that, as we will see, for each elements $a, b \in A$, the relation $v(a) \leq v(b)$ is equivalent to $a \mid^v b$, for some divisibility relation $|^v$ uniquely determined by the valuation v.

Let us start defining the concept of divisibility.

[2]In this work all p-valuations are of type $(1, 1)$.

Definition 2.1.1 *Let A be a commutative ring with 1 and $\mid \subseteq A \times A$ a binary relation. The relation $\mid$ is called a* ***divisibility*** *of A if,*

$$a \mid a \tag{2.1}$$
$$a \mid b, b \mid c \Rightarrow a \mid c \tag{2.2}$$
$$a \mid b, a \mid c \Rightarrow a \mid b \pm c \tag{2.3}$$
$$a \mid b \Rightarrow ca \mid cb \tag{2.4}$$
$$0 \nmid 1 \tag{2.5}$$

for all $a, b, c \in A$.

The set

$$I(\mid) := \{a \in A \ : \ 0 \mid a\}$$

is called the ***support of*** $\mid$ *and its elements are called* ***infinitesimals****.*

If A is a B-module, $\mid$ satisfies all the properties above, except (2.4), and

$$(\forall c \in B)(\forall a, b \in A) : (a \mid b) \Rightarrow (ac \mid cb),$$

*then $\mid$ is called a B-****divisibility*** *of A.*[3]

The support of a divisibility will play a central role in the theory of divisibilities, which can be compared with the role played by the support of a preordering in the real case.

The name infinitesimals was chosen because elements of $I(\mid)$ behave like elements of a ring that has infinite value by some (Bourbaki) valuation v (compare with Example(2.1.11)(10)).

The following proposition shows us the most basic results about supports.

Proposition 2.1.2 *For every divisibility $\mid$ of A, and all $a, b, c, d \in A$, hold*

$$(a \mid -a) \text{ and } (a \mid 0); \tag{2.6}$$
$$I(\mid) \text{ is an ideal of } A; \tag{2.7}$$
$$(0 \mid c) \wedge (0 \mid d) \wedge (a \mid b) \Rightarrow (a + c) \mid (b + d); \tag{2.8}$$

Proof : As $a \mid a$, we have $a \mid a + a$, and then also $a \mid a - (a + a) = -a$. Thus $a \mid a + (-a) = 0$, for all $a \in A$.

If $0 \mid a$ and $0 \mid b$, then $0 \mid a \pm b$. If $0 \mid a$ and $c \in A$, then $0 = (0 \cdot c) \mid ca$. Thus $I(\mid)$ is an ideal of A.

[3]This notion will be used in the examples to show that non-Archimedean semi-norms define also divisibilities.

Now note that,

$$(\forall a, b, c \in A) : (a \mid c) \Rightarrow [a \mid b \Leftrightarrow a \mid (b \pm c)]$$

Thus, if $0 \mid c$, then $a \mid c$ for all $a \in A$, by (2.6), and hence

$$(\forall a, b, c \in A) : (0 \mid c) \Rightarrow [a \mid (b \pm c) \Leftrightarrow a \mid b]$$

In particular, taking $a = b$,

$$(\forall a, c \in A) : (0 \mid c) \Rightarrow [a \mid (a \pm c) \Leftrightarrow a \mid a] \tag{2.9}$$

Replacing a by $a \mp c$, we get

$$(\forall a, c \in A) : (0 \mid c) \Rightarrow [(a \mp c) \mid a \Leftrightarrow (a \mp c) \mid (a \mp c)] \tag{2.10}$$

As $\mid$ is reflexive, we conclude from (2.9) and (2.10) that

$$(\forall a, c \in A) : 0 \mid c \Rightarrow (a + c \mid a) \wedge (a \mid a + c) \tag{2.11}$$

Thus, for all $a, b, c, d \in A$,

$$(0 \mid c) \wedge (0 \mid d) \wedge (a \mid b) \Rightarrow (a + c) \mid a \mid b \mid (b + d) \tag{2.12}$$

■

Remark 2.1.3 *The ideal $I(\ \mid\ )$ is a proper ideal of A, since $0 \nmid 1$.*

The only binary relation on A satisfying $(2.1 - 2.4)$, and not (2.5), is $A \times A$. In fact, for all $a, b \in A$,

$$0 \mid 1 \overset{(2.2)}{\Rightarrow} 0 \mid a \overset{(2.6)}{\Rightarrow} b \mid a$$

The next definitions are all motivated by the properties of valuations.

Definition 2.1.4 *Let $\mid$ be a divisibility of A and $c \in A$. We say that $\mid$ has **cancellation by** c if* [4]

$$(\forall a, b \in A) : ac \mid bc \Rightarrow a \mid b \tag{2.13}$$

*Note that, if $\mid$ has cancelation by c, then $0 \nmid c$, because otherwise, we can conclude that $0 \mid 1$. We say that $\mid$ has **cancelation** if $\mid$ has cancelation for all $c \notin I(\ \mid\ )$.*

[4] If A is a B-module and $\mid$ a B-divisibility, we define cancellation by elements $c \in B$.

For $\emptyset \neq X \subseteq A$, we say that $\mid$ is ***total on*** *X if*

$$(\forall a, b \in X) : (a \mid b) \vee (b \mid a) \tag{2.14}$$

A divisibility is called ***total*** *if it is total on A. A* ***valuation*** *(****divisibility****) is a total divisibility having cancelation.*

A divisibility $\mid$ is ***trivial*** *if*

$$(\forall a, b \in A) : a \nmid b \Leftrightarrow (0 \mid a) \wedge (0 \nmid b) \tag{2.15}$$

Remark 2.1.5 *The properties of cancellation and totality define classes of divisibilities which are in general disjunct (see Example*(2.1.11)(7) *and* (15)*).*

If $\mid$ has cancellation, then $I(\mid)$ is a prime ideal of A. In fact,

$$(a.0 \mid a.b) \wedge (0 \nmid a) \Rightarrow (0 \mid b)$$

The converse is not necessarily true, as we will see in Example(2.1.11)(15) *below. Thus cancellation is stronger than just to say that $I(\mid)$ is a prime ideal of A.*

We give now an adapted definition from that found in page 10 of [12] or Chapter VI (3.1) of [2].

Definition 2.1.6 *A* ***valuation function*** *(or* ***Bourbaki valuation****) of a commutative ring A, with unity 1, is a map $v : A \to \Gamma \cup \{\infty\}$ satisfying*

1. $v(a \cdot b) = v(a) + v(b)$
2. $v(a + b) \geq \min\{v(a), v(b)\}$
3. $v(1) \neq v(0)$

where Γ is a totally ordered additive abelian group with $+$ and $\leq$ denoting the operation of Γ and its ordering, respectively.

The set $\Gamma \cup \{\infty\}$ is also considered as an abelian monoid with respect to the operation $+$, where we define

$$(\forall \gamma \in \Gamma \cup \{\infty\}) : \gamma + \infty = \infty + \gamma = \infty$$

We also suppose that $\infty \geq \gamma$ for all $\gamma \in \Gamma \cup \{\infty\}$.

Note that, if $v : A \to \Gamma \cup \{\infty\}$ is a valuation function, A is a field and v is surjective, then v is also a valuation on A **in the classical sense**, i.e., defined as in Chapter(2.1) of [19], and hence is generalized by the notion for commutative rings.

If v is a valuation function of A, we can verify that $P := v^{-1}(\infty)$ is a prime ideal of A and that

$$\mathcal{O}_v := \left\{ \frac{b+P}{a+P} : a, b \in A \text{ and } v(a) \leq v(b) \right\}$$

is a valuation ring of the quotient field $Quot(A/P)$.

We say that two valuation functions v and w of A are equivalent if $v^{-1}(\infty) = w^{-1}(\infty)$ and $\mathcal{O}_v = \mathcal{O}_w$, as in Definition(2) in page 11 of [12]. We can regard equivalent valuations as "equal" and use also v to denote its equivalence class.

Moreover, the map $v \mapsto (\mathcal{O}_v, v^{-1}(\infty))$ gives us an 1-1 correspondence between the class of equivalent valuation functions v of A and pairs $(\mathcal{O}, P)$, where P is a prime ideal of A and $\mathcal{O}$ is a valuation ring of $Quot(A/P)$.

In this work, we will use the word "valuation" for "valuation functions v" and "valuation divisibilities $|$ ", when it is clear which notion we are using. This abuse of language is justified by Proposition(2.4.2) and because the class of equivalence of v is totally determined by the binary relation $|^v$ defined by[5]

$$(\forall a, b \in A) : a \mid^v b \Leftrightarrow v(a) \leq v(b)$$

We want to define now a notion of divisibility that collects good properties of p-valuations[6] and, under certain conditions, has the properties of the canonical divisibility $|_0$ of $C(X, \mathbb{Q}_p)$, for some compact space X. To motivate the definition, we do a small informal discussion.

By the result about p-adic valuations cited at the beginning of this section, we known that v is a p-valuation of some field K of characteristic zero if, and only if,

$$\frac{1}{p} \notin \mathcal{O}_v \quad \text{and} \quad \gamma(K) \subseteq \mathcal{O}_v,$$

where $\mathcal{O}_v$ is the valuation ring of K associated to v. [7]

If we interpret $(b/a) \in \mathcal{O}$ as $a \mid b$, and note that

$$\gamma(b/a) = \frac{[(a^p b - b^p a)b^{p+1}]}{p[(a^p b - b^p a)^2 - (b^{p+1})^2]},$$

[5]Definition(2) in page 11 of [12] claims this is true and left the verification to the reader. Another way to verify this is using the more general Theorem(A.2) and the Example(2.1.11)(18).

[6]In the sense of of [20].

[7]Lemma(6.1) of [20] applied for the p-adic Kochen operator of type $(1, 1)$.

for all $a, b \in K$, then the following definition for p-divisibilities seems reasonable.

Definition 2.1.7 *Let A be a commutative ring with $p^{-1} \in A$. A divisibility $\mid$ of A is called* ***p-divisibility*** *when*

$$p \nmid 1 \tag{2.16}$$

$$(\forall a, b \in A) : p[(a^p b - b^p a)^2 - (b^{p+1})^2] \mid [(a^p b - b^p a) b^{p+1}] \tag{2.17}$$

The last is called the ***Kochen property*** *and is denoted by γ_p. We say that $\mid$ is a* ***strong p-divisibility*** *if it satisfies the Kochen property and the following strong version of* (2.16)

$$(\forall c \in A) : 0 \nmid c \Rightarrow cp \nmid c \tag{2.18}$$

A ***p-valuation*** *(****divisibility****)*[8] *is a valuation (divisibility) that is also a p-divisibility. The divisibility $\mid$ is* ***p-Archimedean*** *if it is a p-divisibility and*

$$(\forall a \in A)(\exists n \in \mathbb{N}) : (1 \mid p^n a) \tag{2.19}$$

It is called ***strong p-Archimedean*** *if it is not just a p-divisibility, but also a strong p-divisibility.*

Remark 2.1.8 *In the definition of p-divisibilities, we could use the operator*

$$\delta_p(X) := \frac{\binom{X}{p}}{p^2\binom{X}{p}^2 - 1} = \frac{X(X-1)\cdots(X-(p-1))\cdot p!}{p^2 \cdot X^2(X-1)^2\cdots(X-(p-1))^2 - (p!)^2}$$

instead of γ_p, because in this case, all the theorems about p-valuation functions formulated with γ_p, and used in this work, are also true if we use δ_p.

This was first observed by Kochen in his paper [11], where he introduced the p-adic operator γ_p.

The p-Archimedean divisibilities will be the most important for us. The canonical divisibility $|_0$ of $C(X, \mathbb{Q}_p)$, for example, is p-Archimedean if X is quasi-compact.

We will also be concerned with extensions of divisibilities, in particular, if the property of being a p-divisibility is preserved by extensions. An **extension** of a divisibility $\mid$ is simply a divisibility $\mid'$ satisfying $\mid \subseteq \mid'$ (as sets).

[8] Again we allow the use of the term "p-valuation" for "p-valuation divisibilities" and "p-valuations in the sense of [20]". The first can be seen as a generalization of the second notion, because a p-valuation (function) v induces a p-valuation divisibility $|^v$, defined in the discussion above.

When we have just a p-divisibility, it is not true in general that it has an extension being a p-valuation (see Example(2.1.11)(17)). That is why we defined strong p-divisibilities above, because each strong p-divisibility has a p-valuation extending it (Theorem(3.1.2)).

Surprisingly, the weak notion of a p-divisibility is enough to assure the existence of a p-valuation extending $|$, if $|$ is assumed to be p-Archimedean. This is the content of Theorem(3.2.4), one of the most fundamental results about p-Archimedean divisibilities.

We also have the following useful remarks.

Remark 2.1.9 *Let A be a commutative ring with $p^{-1} \in A$.*

1. *Every p-divisibility is non-trivial by Remark*(2.1.3)*. Also $0 \nmid p$, because otherwise $p^{-1}0 \mid p^{-1}p = 1$.*

2. *A p-divisibility having cancellation is also a strong p-divisibility. The converse is not necessarily true by Example*(2.1.11)(14)*.*

To facilitate writing, we introduce some notations for the sets defined by the properties listed until now.

Notation 2.1.10 *Let A be a commutative ring and $|$ a divisibility of A. We use the following notations:*

- $E(\ |\ ) := \{\ |' : |' \quad$ *is a div. on A and* $\quad | \subseteq |'\ \}$ *(the set of extensions)*
- $T(\ |\ ) := \{\ |' \in E(\ |\ )\ : |' \quad$ *is total* $\}$
- $\mathcal{C}_c(\ |\ ) := \{\ |' \in E(\ |\ )\ : |' \quad$ *has cancellation by c*$\}$
- $\mathcal{C}(\ |\ ) := \{\ |' \in E(\ |\ )\ : |' \quad$ *has cancellation* $\}$
- $V(\ |\ ) := \{\ |' \in E(\ |\ )\ : |' \quad$ *is a valuation*$\} = \mathcal{C}(\ |\ ) \cap T(\ |\ )$

If $p \in \mathbb{N}$ is a prime number and $p^{-1} \in A$ we also write:

- $E_p(\ |\ ) := \{\ |' \in E(\ |\ )\ : |' \quad$ *is a p-divisibility* $\}$
- $V_p(\ |\ ) := E_p(\ |\ ) \cap V(\ |\ )$
- $E_p^{str}(\ |\ ) := \{\ |' \in E(\ |\ )\ : |'$ *is a strong p-divisibility* $\} \subseteq E_p(\ |\ )$.
- $Arch_p(\ |\ ) := \{\ |' \in E(\ |\ )\ : |'$ *is a p-Archimedean divisibility* $\}$

Sometimes we will write $E(\ |\ , A)$ instead of $E(\ |\ )$ to emphasize the ring from which we take the divisibilities. This notation is also used for the other sets above.

The replacement of $|$ by A, in the notation above, will mean that we are observing not just extensions of some fixed divisibility $|$ with some properties, but the set of all divisibilities of A satisfying them.

For example, $E(A)$ denote the set of all divisibilities of A and $V(A)$ the set of all valuation of A.

We use the superscript $^{\max}$ to denote a subset of maximal elements under inclusion. Thus,

$$Arch_p^{\max}(\ |\ ) = \{\ |^* \in Arch_p(\ |\ ) :\ \textit{there is no}\ \ |^+\ \ \textit{with}\ \ |^* \subsetneqq |^+\}$$

We give now a list of examples of divisibilities, going from the simpler to the more abstract.

The last example deserves a closer look. It presents divisibilities in another fashion, using a divisibility function $\sigma : A \to M$, where M is a partially ordered abelian monoid with 0. In particular, if M is a group and totally ordered, σ is indeed a valuation (the zero 0 under multiplication is replaced by ∞ in an additive notation).

This way of understanding divisibilities (as functions) will not be necessary for our work. However, it is useful for finding special examples of divisibilities and maybe in further studies. That is why we left some words about divisibility functions for Appendix(A).

Example 2.1.11 *1. Let A be a commutative ring. Then*

$$|_A := \bigcup_{a \in A} (\{a\} \times a \cdot \mathbb{Z})$$

*defines a divisibility of A. This is the **minimal divisibility** of A. It satisfies*

$$x\ |_A\ y \Leftrightarrow y \in x \cdot \mathbb{Z} \tag{2.20}$$

for all $x, y \in A$. Thus $I(\ |_A\ ) = \{0\}$ and $E(\ |_A) = E(A)$ is the set of all divisibilities of A.

2. *The minimal divisibility $|_{\mathbb{Z}}$ of $\mathbb{Z}$ coincides with its canonical divisibility and hence each divisibility $|$ of a ring A containing $\mathbb{Z}$ extends $|_{\mathbb{Z}}$.*

3. *Let A be a commutative ring. The relation defined by*

$$a \mid b \Leftrightarrow b = ac \ \ \textit{for some}\ c \in A$$

is the ***usual divisibility of*** A. *It has support* $\{0\}$.

The ring A *is an integral domain if, and only if,* $I(\ |\ )$ *is prime, and in this case* $|$ *has cancellation.*

4. *For each prime ideal* I *of* A

$$|^I := (A\backslash I \times A) \cup (I \times I)$$

is a trivial divisibility of A *with support* I. *In fact, clearly it satisfies* $(2.1 - 2.3)$ *and* (2.5). *Moreover,* $|^I$ *has cancellation and satisfies* (2.4) *because*

$$\begin{aligned} ac \nmid^I bc &\Leftrightarrow (ac \in I) \wedge (bc \notin I) \\ &\Leftrightarrow (ac \in I) \wedge (b, c \notin I) \\ &\Leftrightarrow (a \in I) \wedge (b, c \notin I) \\ &\Leftrightarrow (a \nmid^I b) \wedge (0 \nmid^I c) \end{aligned}$$

for all $a, b, c \in A$, *beeing* I *prime.*

Conversely, if $|^I$ *is a divisibility for some proper ideal* I *of* A *then* I *is prime. Otherwise, we can find* $a, b \notin I$ *such that* $ab \in I$, *and hence*

$$(a\ |^I\ 1) \wedge (b\ |^I\ 1) \Rightarrow 0\ |^I\ ab\ |^I\ 1$$

5. *For* I, J *prime ideals of* A, *if* $I \neq J$, *then* $|^I \neq |^J$. *To verify this take, without loss of generality,* $a \in J\backslash I$. *Then*

$$(0\ |^J\ a) \wedge (0 \nmid^I a)\ \textit{and}\ (a \nmid^J 1) \wedge (a\ |^I\ 1)$$

Hence neither $|^I \subseteq |^J$ *nor* $|^J \subseteq |^I$. *The converse is clearly true, because* $I = J$ *implies* $|^I = |^J$.

Thus there is 1-1 correspodence between the prime ideal of A *and its trivial divisibilities.*

6. *If* $|$ *is a divisibility of* A, *then*

$$(\forall a, b \in A) : a + I(\ |\ )\ \bar{|}\ b + I(\ |\ ) :\Leftrightarrow a \mid b$$

defines a divisibility of $\overline{A} := A/I(\ |\ )$, *because of Proposition(2.1.2).*

7. *Let* $|$ *be a divisibility of an integral domain* A *with support* $\{0\}$ *having cancellation. Then*

$$\frac{a}{b}\ |^*\ \frac{c}{d} :\Leftrightarrow ad \mid bc$$

defines a divisibility of $F = Quot(A)$ with cancellation. The set

$$B := B(\ |\ ) := \left\{ \frac{b}{a} \ : \ a \mid b \ \ and \ \ a \neq 0 \right\} \subseteq F$$

defines a subring of F. Also, $|^*$ is total if, and only if, $|$ is total. In this case B is a valuation ring of F.

8. *Let A be an integral domain and $B \subseteq Quot(A) =: F$ a subring. Then*

$$a \,|^B\, b :\Leftrightarrow \left(a \neq 0 \ and \ \frac{b}{a} \in B \right) \quad or \ \ a = b = 0$$

defines a divisibility having cancellation with support $\{0\}$. If B is a valuation ring, then $|$ is total.

Therefore, there is a 1-1 correspondence between the valuation rings of F and valuations of A with support $\{0\}$.

9. *Let k be a field, $A = k[X]$ and $F = k(X)$. For each $f, g \in A$*

$$f \mid g :\Leftrightarrow deg(g) \leq deg(f)$$

defines a valuation with

$$B = \left\{ \frac{g}{f} \ : \ deg(g) \leq deg(f) \right\}$$

and $B \cap A = k \neq A$.

10. *Let A be a ring with some valuation function $v : A \to \Gamma_v \cup \{\infty\}$. Then*

$$a \,|^v\, b :\Leftrightarrow v(a) \leq v(b)$$

defines a valuation of A. The support of $|^v$ is the prime ideal $v^{-1}(\infty)$. The valuation $|^v$ is trivial if, and only if, $v(A) = \{0\} \cup \{\infty\}$.

11. *Let A be a ring and $\{v : A \to \Gamma_v \cup \{\infty\}\}_{v \in V}$ a set of valuation functions of A. Then*

$$a \,|_V\, b :\Leftrightarrow (\forall v \in V) : v(a) \leq v(b)$$

defines a divisibility of A with $|_V \subseteq |^v$, for all $v \in V$, and support

$$I(\ |_V) = \bigcap_{v \in V} v^{-1}(\infty)$$

In general it is not total and has no cancellation.

12. *Let K be a field, $|\cdot|$ a non-Archimedean absolute value of K and A a K-vector space.*

    If $\rho := \|\cdot\| : A \to \mathbb{R}^+$ is a non-trivial non-Archimedean semi-norm of A, i.e., for all $a, b \in A$ and $\alpha \in K$

    - $\|a\| \geq 0$.
    - $\|\alpha \cdot a\| = |\alpha| \cdot \|a\|$.
    - $\|a + b\| \leq \max\{\|a\|, \|b\|\}$.

    Then

    $$(\forall a, b \in A) : a \mid_\rho b :\Leftrightarrow \|b\| \leq \|a\|$$

    *defines a K-**divisibility of** A. Also*

    $$I(\ \mid_\rho) = \{a \in A : \|a\| = 0\},$$

    and $\mid_\rho$ has K-cancellation and is total.

    If A is a K-algebra and

    $$(\forall a, b \in A) : \|a \cdot b\| \leq \|a\| \cdot \|b\|,$$

    *then $\mid_\rho$ is even a total **divisibility of** A, but in general has **no** cancellation.*

13. *Let $\alpha : A \to B$ be a homomorphism of rings and $\mid$ a divisibility of B. The **divisibility induced by** $\mid$ **and** α **in** A is defined by*

    $$a \mid^\alpha b :\Leftrightarrow \alpha(a) \mid \alpha(b)$$

    It inherits the properties of $\mid$, i.e., totality, cancellations and p-properties.

14. *Take $A = C(X, \mathbb{Q}_p)$ with X a compact space. Define*

    $$f \mid_0 g :\Leftrightarrow (\forall x \in X) :\ v_p(f(x)) \leq v_p(g(x))$$

    *This is **strong** p-Archimedean divisibility of A with **non-prime** support $\{0\}$, **without cancellation** and **not total**, if $C(X, \mathbb{Q}_p)$ contains non-constant maps.*

    For any $U \subseteq X$,

    $$f \mid_U g :\Leftrightarrow \forall x \in U :\ v_p(f(x)) \leq v_p(g(x))$$

defines a p-divisibility extending $|$ *with support*

$$I(\ |_U) = \{f \in A : f(x) = 0 \text{ for all } x \in U\}$$

and also, in general, it is not total and has no cancellation. However, if $U = \{x\}$ *for some* $x \in X$ *then* $|_x := |_{\{x\}}$ *is total, has cancellation and support*

$$I(\ |_x) = \{f \in A : f(x) = 0\}$$

15. *Take* $A = \mathbb{Z}_p[X]$ *and define a function* $d : A \to \mathbb{Z} \cup \{\infty\}$ *by*

$$d(a_0 + a_1X + ... + a_nX^n) = \begin{cases} -n & \text{if } n > 0 \\ v_p(a_0) & \text{if } n = 0 \end{cases}$$

and then

$$f \mid g :\Leftrightarrow d(f) \leq d(g),$$

for all $f, g \in A$.

This defines a ***total*** *divisibility of* A *with* $I(\ \mid\ ) = \{0\}$ ***prime****, but it has* ***no cancellation****, because*

$$p \nmid 1 \quad \text{and} \quad pX \mid X$$

The verification of the properties of divisibilities for $|$ *is left to the reader. It is done analyzing the relation* $g \mid f$*, with* $g, f \in \mathbb{Z}_p[X]$*, in each of the following situations:*

- $\deg(g) > 0$ *and* $\deg(f) > 0$,
- $0 = \deg(g) < \deg(f)$,
- $0 = \deg(f) < \deg(g)$,
- $0 = \deg(g) = \deg(f)$.

One property also used is

$$(\forall g, f \in \mathbb{Z}_p[X]) : g \mid f \text{ and } g \in \mathbb{Z}_p \Rightarrow f \in \mathbb{Z}_p$$

Moreover, $|$ *satisfies additionally*[9]

- $(\forall n \in \mathbb{N}) : p^{n+1} \nmid p^n$
- $(\forall g, f \in \mathbb{Z}_p[X]) : p[(g^p f - g^p f)^2 - (f^{p+1})^2] \mid [(g^p f - f^p g) f^{p+1}]$

[9]These conditions can be taken as a definition of p-divisibilities of commutative rings A with $p^{-1} \notin A$. However, we will be mainly interested in rings satisfying $p^{-1} \in A$.

The first property clearly holds and the second is verified by proving that

$$(\forall g, f \in \mathbb{Z}_p[X]) : d(p[(g^p f - f^p g)^2 - (f^{p+1})^2]) \leq d((g^p f - f^p g) f^{p+1}) \tag{2.21}$$

First note that $|^d \cap (\mathbb{Z}_p \times \mathbb{Z}_p) = |^{\mathbb{Z}_p}$ *, where*

$$g \,|^{\mathbb{Z}_p}\, f :\Leftrightarrow v_p(g) \leq v_p(f),$$

for all $g, f \in \mathbb{Z}_p$.
We observe four cases:

Case 1: If $g, f \in \mathbb{Z}_p$*, then (2.21) is true, because* $|^d \cap (\mathbb{Z}_p \times \mathbb{Z}_p) = |^{\mathbb{Z}_p}$.

Now suppose that $g \notin \mathbb{Z}_p$ *or* $f \notin \mathbb{Z}_p$.

Case 2: If $\deg(f) > \deg(g)$*, then*

$$\deg(f^{p+1}) > \deg(f^p g) > \deg(g^p f),$$

and hence

$$\begin{aligned} d(p[(g^p f - f^p g)^2 - (f^{p+1})^2]) &= -2(p+1) \cdot \deg(f) \\ &= -(2p+1) \cdot \deg(f) - \deg(f) \\ &< -(2p+1) \cdot \deg(f) - \deg(g) \\ &= d((g^p f - f^p g) f^{p+1}) \end{aligned}$$

Case 3: If $\deg(f) < \deg(g)$*, then*

$$\deg(f^{p+1}) < \deg(f^p g) < \deg(g^p f),$$

and hence

$$\begin{aligned} d(p[(g^p f - f^p g)^2 - (f^{p+1})^2]) &= -2p \cdot \deg(g) - 2 \cdot \deg(f) \\ &< -p \cdot \deg(g) - p \cdot \deg(f) - 2 \cdot \deg(f) \\ &= -p \cdot \deg(g) - \deg(f) - (p+1) \cdot \deg(f) \\ &= d((g^p f - f^p g) f^{p+1}) \end{aligned}$$

Case 4: If $\deg(g) = \deg(f)$*, then*

$$\deg(f^{p+1}) = \deg(f^p g) = \deg(g^p f)$$

In this case

$$\deg(g^p f - f^p g - f^{p+1}) = (p+1)\cdot\deg(f) = \deg(g^p f - f^p g + f^{p+1})$$

In fact, otherwise, taking the leading coefficients f_0 and g_0 of f and g, respectively, the p-adic number $r := (f_0/g_0)$ satisfies

$$r^p - r + 1 = 0 \text{ or } r^p - r - 1 = 0,$$

which is not possible for p-adic numbers.

It follows that

$$\begin{aligned} d(p[(g^p f - f^p g)^2 - (f^{p+1})^2]) &= -2(p+1)\cdot\deg(f) \\ &= (-2p-1)\cdot\deg(f) - \deg(g) \\ &\leq d((g^p f - f^p g)f^{p+1}) \end{aligned}$$

16. *If we define a function $d' : \mathbb{Q}_p[X] \to \mathbb{Z}\cup\{\infty\}$ by*

$$d'(a_0 + a_1 X + ... + a_n X^n) = \begin{cases} -n & \text{if } n > 0 \\ v_p(a_0) & \text{if } n = 0 \end{cases}$$

and

$$f \mid' g :\Leftrightarrow d'(f) \leq d'(g),$$

for all $f, g \in \mathbb{Q}_p[X]$, then $\mid'$ ***is not a divisibility of*** *$\mathbb{Q}_p[X]$, because*

$$p^{-1} \mid' X \quad \text{and} \quad 1 = p\cdot p^{-1} \nmid' p\cdot X$$

17. *Let $\mid$ be the divisibility of $\mathbb{Z}_p[X]$ defined in (15). The set*

$$\langle p\rangle := \{p^i : i \in \mathbb{N}\}$$

is multiplicatively closed in $\mathbb{Z}_p[X]$ without zero and hence we can construct the localization

$$\mathbb{Z}_p[X]_{\langle p\rangle} := \left\{\frac{f}{p^n} : f \in \mathbb{Z}_p[X],\ n \in \mathbb{N}\right\},$$

which is indeed $\mathbb{Q}_p[X]$.

If we define a binary relation $|_p$ *of* $\mathbb{Q}_p[X]$ *by*

$$\left(\frac{g}{p^n}\right) |_p \left(\frac{f}{p^m}\right) :\Leftrightarrow (p^k)(p^m)g \mid (p^k)(p^n)f \quad \textit{for some } k \in \mathbb{N},$$

for each $n, m \in \mathbb{N}$ *and* $g, f \in \mathbb{Z}_p$*, then Lemma(2.5.3) assures that* $|_p$ *is a divisibility of* $\mathbb{Q}_p[X]$*.*

We claim that $|_p$ *is also a* p***-divisibility*** *of* $\mathbb{Q}_p[X]$*, but* ***not a strong*** p***-divisibility*** *and* ***not*** p***-Archimedean****.*

In fact,

$$(\forall k \in \mathbb{N}) : p^{k+1} \nmid p^k,$$

implies $p \nmid_p 1$*.*

For the Kochen property, we will verify for all $g, f \in \mathbb{Z}_p[X]$ *and* $k, r \in \mathbb{N}$ *that*

$$p\left[\left(\left(\frac{g}{p^k}\right)^p\left(\frac{f}{p^r}\right) - \left(\frac{f}{p^r}\right)^p\left(\frac{g}{p^k}\right)\right)^2 - \left(\left(\frac{f}{p^r}\right)^{(p+1)}\right)^2\right] \tag{2.22}$$

divides

$$\left[\left(\left(\frac{g}{p^k}\right)^p\left(\frac{f}{p^r}\right) - \left(\frac{f}{p^r}\right)^p\left(\frac{g}{p^k}\right)\right)\cdot\left(\frac{f}{p^r}\right)^{p+1}\right] \tag{2.23}$$

by $|_p$*.*

To see this, we rewrite (2.22) as

$$p\left[\left(\frac{(p^r g)^p(p^k f) - (p^k f)^p(p^r g)}{p^{(p+1)(k+r)}}\right)^2 - \left(\frac{(p^k f)^{p+1}}{p^{(p+1)(r+k)}}\right)^2\right]$$

and (2.23) as

$$\left[\left(\frac{(p^r g)^p(p^k f) - (p^k f)^p(p^r g)}{p^{(p+1)(k+r)}}\right)\cdot\left(\frac{(p^k f)^{p+1}}{p^{(p+1)(r+k)}}\right)\right]$$

Thus, as

$$p^{2(p+1)(k+r)}\cdot p[(g_*^p f_* - f_*^p g_*)^2 - (f_*^{p+1})^2] \mid [(g_*^p f_* - f_*^p g_*)f_*^{p+1}]\cdot p^{2(p+1)(k+r)},$$

where $g_* := p^r g$ *and* $f_* := p^k f$*, we also have (2.22)* $|_p$ *(2.23).*

This p-divisibility is not strong, because $Xp \mid X$ implies that

$$p \nmid_p 1 \quad \textit{and} \quad pX \mid_p X$$

Also

$$(\forall k, n \in \mathbb{N}) : p^k \nmid p^k(p^n X)$$

implies that $|_p$ is not p-Archimedean.

Moreover, ***there is no p-valuation extending*** *$|_p$, i.e. $V_p(\ |_p) = \emptyset$, because if $|^* \in V_p(\ |_p)$, as $X \mid_p 1$, we conclude that $X \mid^* 1$, and hence $0 \nmid^* X$.*

On the other hand, $Xp \mid_p X$ implies $Xp \mid^* X$. By cancellation $p \mid^* 1$, contradicting $|^* \in V_p(\ |_p)$.

18. *Let A be a commutative ring and $(M, \cdot, \leq)$ a partially ordered abelian monoid with zero 0 such that $0 \not\leq 1$. This means that $\leq$ is a partial order of M and, for all $m_1, m_2, m_3 \in M$,*

$$m_1 \leq m_2 \Rightarrow (m_1 \cdot m_3) \leq (m_2 \cdot m_3) \quad \textit{and} \quad 0 \cdot m_1 = 0$$

Note that the unity 1 and the zero 0 are unique. In fact, if $1'$ is another unity and $0'$ another zero, then

$$1 = 1 \cdot 1' = 1' \quad \textit{and} \quad 0 = 0 \cdot 0' = 0'$$

If $\delta : A \to M$ is surjective and satisfies

- $\delta(a \cdot b) = \delta(a) \cdot \delta(b)$
- $\delta(a) \leq \delta(b),\ \delta(a) \leq \delta(c) \Rightarrow \delta(a) \leq \delta(b \pm c)$
- $\delta(0) \not\leq \delta(1)$

Then

$$a \mid^\delta b :\Leftrightarrow \delta(a) \leq \delta(b)$$

defines a divisibility on A.

We claim that its support is $\delta^{-1}(0)$. In fact,

$$0 \mid^\delta a \Leftrightarrow a \in \delta^{-1}(\{m \in M \ : \ 0 \leq m\})$$

and hence it is enough to prove that this set equals $\delta^{-1}(0)$. However, by the second condition, $\delta(a) \leq \delta(0)$ for all $a \in A$, and hence

$$\delta(a) \geq 0 \Rightarrow \delta(a) = 0 = \delta(0)$$

Writing $+$ for the multiplication of M and ∞ for its zero 0, we can rewrite the conditions of divisibilities maps as

- $\delta(a \cdot b) = \delta(a) + \delta(b)$
- $\delta(a) \leq \delta(b),\ \delta(a) \leq \delta(c) \Rightarrow \delta(a) \leq \delta(b \pm c)$
- $\infty \not\leq 0$

which seems similar to the definition of valuation functions.

If $\leq$ is a total order, the second condition is equivalent to

$$\delta(a+b) \geq \min\{\delta(a), \delta(b)\}, \tag{2.24}$$

because[10]

$$\delta(a) \leq \delta(b),\ \delta(a) \leq \delta(c) \overset{(2.24)}{\Rightarrow} \begin{cases} & \delta(a) \leq \delta(b) \leq \delta(a \pm b) \\ \textit{or} & \delta(a) \leq \delta(c) \leq \delta(a \pm b) \end{cases}$$

and the totality of $\leq$ implies

$$(\forall a, b \in A) : [\delta(a) \leq \delta(a+b)] \vee [\delta(b) \leq \delta(a+b)]$$

and hence

$$(\forall a, b \in A) : \delta(a+b) \geq \min\{\delta(a), \delta(b)\}$$

2.2 Minimal Extensions and Set Operators

When working with preorderings of a commutative ring A, one of the most fundamental problems to solve, is to determine when a fixed preordering T has an ordering P extending it with some desired properties.

This can be solved understanding first the minimal proper preorder extensions of T. In this case, one asks if, for a given $a \in A \backslash T$, there is some preorder extension T_a of T such that $a \in T_a$.[11]

In the divisibility case, given a (p-)divisibility $|$, we want to understand when we can find some (p-)valuation extending it. We will first study the minimal extensions of divisibilities and we leave the question about extensions to valuations for the next sections.

Let us start with the main question concerning minimal extensions: given $a, b \in A$ such that $a \nmid b$, does there exist a divisibility $|_{a,b}$ extending $|$ such that $a \mid_{a,b} b$?

In order to give an answer, we will need to use a set operator defined on the power set $\mathcal{P}(A)$ of A related to the divisibility $|$, namely $\mathfrak{S}$.

[10] For all $a \in A$; $\delta(a) \leq \delta(b)$ implies $\delta(a) \leq \delta(-b)$.

[11] Lemma(4.1.3) of [18], applied to a and $b = -a$, guarantees that, given a preordering T of A, $T + aT$ or $T - aT$ is a preordering of A. This lemma can be seen as an answer to our question.

If $X \subseteq A$, the set $\mathfrak{S}(X)$ can be thought of as a convex hull for the divisibility relation, or as a set of generalized multiples of elements of X. In fact, if $X = \{a\}$, for some $a \in A$, then $\mathfrak{S}(X)$ is equal to the set of all $y \in A$ such that $a \mid y$.

Actually, $\mathfrak{S}(X)$ is a generalization of the concept of ideal generated by $X \subseteq A$, as the next examples will show.

We start now with the definition of such an operator and some notations, that will help us in writing.

Definition 2.2.1 *Let A be a ring and $\mid$ a binary relation on A. We define, for every $X \subseteq A$,*

$$\mathbb{M}(X, \mid) := \mathbb{M}(X) := \{y \in A : x \mid y \text{ for some } x \in X\}$$

$$\sum(X) := \{x_1 \pm \cdots \pm x_n \in A : x_1, ..., x_n \in X \text{ and } n \geq 1\}$$

and hence, recursively,

- $\mathfrak{S}^0(X, \mid) := \mathfrak{S}^0(X) := X$.
- $\mathfrak{S}^{n+1}(X, \mid) := \mathfrak{S}^{n+1}(X) := \mathbb{M}(\mathfrak{S}^n(X))$, *if n is even;*
- $\mathfrak{S}^{n+1}(X, \mid) := \mathfrak{S}^{n+1}(X) := \sum(\mathfrak{S}^n(X))$, *if n is odd.*

These sets define operators $\mathfrak{S}^n : \mathcal{P}(A) \to \mathcal{P}(A)$, for each $n \in \mathbb{N}$. Using them, we define $\mathfrak{S} := \mathfrak{S}(\ \cdot\ , \mid) : \mathcal{P}(A) \to \mathcal{P}(A)$ by

$$X \mapsto \bigcup_{n \geq 0} \mathfrak{S}^n(X), \quad \text{for all} \quad X \subseteq A.$$

For each $X \subseteq A$ the set $\mathfrak{S}(X)$ is called the ***ideal generated by X with respect to $\mid$****, and the operator $\mathfrak{S}$ is called* ***ideal operator of $\mid$*** *.*

The following suggestive notations will greatly simplify our work.

Notation 2.2.2 *Let $x_1, ..., x_n \in A$, $X_1, ..., X_n \subseteq A$ and $\mathbb{O}$ a letter belonging to $\{\mathbb{M}, \sum, \mathfrak{S}\}$. We use the following notations*

$$\mathbb{O}(X_1, ..., X_n) := \mathbb{O}(X_1 \cup ... \cup X_n)$$
$$\mathbb{O}(x_1, ..., x_n) := \mathbb{O}(\{x_1, ..., x_n\})$$
$$\mathbb{O}(X, x) := \mathbb{O}(X \cup \{x\})$$

The Lemma below lists the general properties of the operator $\mathfrak{S}$ that interest us. They will be used frequently in the text.

Lemma 2.2.3 *Let $|$ be a divisibility of A and $\mathfrak{S} : \mathcal{P}(A) \to \mathcal{P}(A)$ its associated ideal operator. Then, for all $X, Y, Z \subseteq A$ and $x \in A$:*

1. $X \subseteq Y \Rightarrow \mathfrak{S}(X) \subseteq \mathfrak{S}(Y)$
2. $\mathfrak{S}^n(X) \subseteq \mathfrak{S}^m(X)$ *for all* $m \geq n$.
3. $\mathfrak{S}(\mathfrak{S}(X)) = \sum(\mathfrak{S}(X)) = \mathbb{M}(\mathfrak{S}(X)) = \mathfrak{S}(X)$
4. $\mathfrak{S}(x) = \mathbb{M}(x)$
5. $\mathfrak{S}(0, X) = \mathfrak{S}(X)$
6. $\mathfrak{S}(X) \subseteq \mathfrak{S}(Y) \Rightarrow \mathfrak{S}(X \cup Z) \subseteq \mathfrak{S}(Y \cup Z)$
7. $x \cdot \mathfrak{S}(X) \subseteq \mathfrak{S}(x \cdot X)$
8. $X \subseteq Y \Rightarrow \mathfrak{S}(X \cdot Z) \subseteq \mathfrak{S}(Y \cdot Z)$

Proof : Let $X, Y, Z \subseteq A$ and $x \in A$.

1. If $X \subseteq Y$, then $\mathbb{M}(X) \subseteq \mathbb{M}(Y)$ and $\sum(X) \subseteq \sum(Y)$. Therefore, if $\mathfrak{S}^n(X) \subseteq \mathfrak{S}^n(Y)$, then $\mathfrak{S}^{n+1}(X) \subseteq \mathfrak{S}^{n+1}(Y)$, for all $n \in \mathbb{N}$. Thus, after using induction on n, we have

$$\mathfrak{S}(X) = \bigcup_{n \geq 0} \mathfrak{S}^n(X) \subseteq \bigcup_{n \geq 0} \mathfrak{S}^n(Y) = \mathfrak{S}(Y)$$

2. This is a consequence of $X \subseteq \mathbb{M}(X)$ and $X \subseteq \sum(X)$. If $m \geq n$ then $m = n + k$. The case $k = 0$ is trivial. Suppose that $\mathfrak{S}^n(X) \subseteq \mathfrak{S}^{n+k}(X)$ for some $k \geq 0$. Thus, either

$$\mathfrak{S}^n(X) \subseteq \mathfrak{S}^{n+k}(X) \subseteq \sum(\mathfrak{S}^{n+k}(X)) = \mathfrak{S}^{n+k+1}(X)$$

or

$$\mathfrak{S}^n(X) \subseteq \mathfrak{S}^{n+k}(X) \subseteq \mathbb{M}(\mathfrak{S}^{n+k}(X)) = \mathfrak{S}^{n+k+1}(X)$$

and hence, the desired conclusion follows by induction on k.

3. If $x \in \sum(\mathfrak{S}(X))$, then there are $n_1, ..., n_r \in \mathbb{N}$ and $x_1 \in \mathfrak{S}^{n_1}(X), ..., x_r \in \mathfrak{S}^{n_r}(X)$ such that

$$x = x_1 \pm ... \pm x_r$$

Taking $n := \max\{n_1, ..., n_r\}$, we have

$$x_i \in \mathfrak{S}^{n_1}(X) \subseteq \mathfrak{S}^n(X),$$

and hence

$$x = x_1 \pm ... \pm x_r \in \sum(\mathfrak{S}^n(X)) \overset{\sum(\sum(X))=\sum(X)}{\subseteq} \mathfrak{S}^{n+1}(X) \subseteq \mathfrak{S}(X)$$

If $x \in \mathbb{M}(\mathfrak{S}(X))$, then there are $n \in \mathbb{N}$ and $z \in \mathfrak{S}^n(X)$ such that $z \mid x$. In particular,

$$x \in \mathbb{M}(\mathfrak{S}^n(X)) \overset{\mathbb{M}(\mathbb{M}(X))=\mathbb{M}(X)}{\subseteq} \mathfrak{S}^{n+1}(X) \subseteq \mathfrak{S}(X)$$

Finally, as the operator $\mathfrak{S}$ is obtained applying $\mathbb{M}$ and $\sum$ consecutively, it also follows that $\mathfrak{S}(X) \subseteq \mathfrak{S}(\mathfrak{S}(X)) \subseteq \mathfrak{S}(X)$.

4. As $\mid$ is a divisibility, we also have $\sum(\mathbb{M}(x)) = \mathbb{M}(\mathbb{M}(x))$, and then it follows by induction on n that

$$\mathfrak{S}^n(x) = \mathbb{M}(x) \text{ for all } x \in A,$$

and hence $\mathfrak{S}(x) = \mathbb{M}(x)$ for all $x \in A$.

5. As $\mathbb{M}(0) \subseteq \mathbb{M}(X)$, we have $\mathbb{M}(X) = \mathbb{M}(X, 0)$. Thus

$$\mathfrak{S}(X, 0) \overset{\mathbb{M}(\mathbb{M}(X))=\mathbb{M}(X)}{=} \mathfrak{S}(\mathbb{M}(X, 0)) = \mathfrak{S}(\mathbb{M}(X)) \overset{\mathbb{M}(\mathbb{M}(X))=\mathbb{M}(X)}{=} \mathfrak{S}(X).$$

6. Suppose that $\mathfrak{S}(X) \subseteq \mathfrak{S}(Y)$. We prove by induction on n that

$$\mathfrak{S}^n(X \cup Z) \subseteq \mathfrak{S}(Y \cup Z) \tag{2.25}$$

for all $n \in \mathbb{N}$.

If $n = 0$, then $x \in \mathfrak{S}^0(X \cup Z) = X \cup Z$ implies

$$x \in Z \subseteq \mathfrak{S}(Z) \overset{1.}{\subseteq} \mathfrak{S}(Y \cup Z) \text{ or } x \in X \subseteq \mathfrak{S}(X) \subseteq \mathfrak{S}(Y) \overset{1.}{\subseteq} \mathfrak{S}(Y \cup Z)$$

For the induction step, suppose that (2.25) is true for some $n \geq 0$ and take $x \in \mathfrak{S}^{n+1}(X \cup Z)$. If $\mathfrak{S}^{n+1}(X \cup Z) = \mathbb{M}(\mathfrak{S}^n(X \cup Z))$, then

$$x \in \mathbb{M}(\mathfrak{S}^n(X \cup Z)) \overset{(2.25)}{\subseteq} \mathbb{M}(\mathfrak{S}(Y \cup Z)) \overset{3.}{=} \mathfrak{S}(Y \cup Z),$$

If $\mathfrak{S}^{n+1}(X \cup Z) = \sum(\mathfrak{S}^n(X \cup Z))$, then

$$x \in \sum(\mathfrak{S}^n(X \cup Z)) \overset{(2.25)}{\subseteq} \sum(\mathfrak{S}(Y \cup Z)) \overset{3.}{=} \mathfrak{S}(Y \cup Z)$$

Therefore (2.25) is true for all $n \in \mathbb{N}$, and hence

$$\mathfrak{S}(X \cup Z) = \bigcup_{n \geq 0} \mathfrak{S}^n(X \cup Z) \subseteq \mathfrak{S}(Y \cup Z)$$

7. For $n = 0$, we have

$$x \cdot \mathfrak{S}^n(X) = x \cdot \mathfrak{S}^0(X) = x \cdot X = \mathfrak{S}^0(x \cdot X)$$

Note now that

$$x \cdot \sum(X) = \sum(x \cdot X) \quad \text{and} \quad x \cdot \mathbb{M}(X) \subseteq \mathbb{M}(x \cdot X) \tag{2.26}$$

for all $x \in A$ and all $X \subseteq A$, because of the divisibility properties.

For the induction step, suppose that

$$x \cdot \mathfrak{S}^n(X) \subseteq \mathfrak{S}^n(x \cdot X) \tag{2.27}$$

for some $n \geq 0$.

If $\mathfrak{S}^{n+1}(X) = \mathbb{M}(\mathfrak{S}^n(X))$, then

$$\begin{array}{ccccc} x \cdot \mathfrak{S}^{n+1}(X) & = & x \cdot \mathbb{M}(\mathfrak{S}^n(X)) & \overset{(2.26)}{\subseteq} & \mathbb{M}(x \cdot \mathfrak{S}^n(X)) \\ & \overset{(2.27)}{\subseteq} & \mathbb{M}(\mathfrak{S}^n(x \cdot X)) & = & \mathfrak{S}^{n+1}(x \cdot X) \end{array}$$

If $\mathfrak{S}^{n+1}(X) = \sum(\mathfrak{S}^n(X))$, then

$$\begin{array}{ccccc} x \cdot \mathfrak{S}^{n+1}(X) & = & x \cdot \sum(\mathfrak{S}^n(X)) & \overset{(2.26)}{\subseteq} & \sum(x \cdot \mathfrak{S}^n(X)) \\ & \overset{(2.27)}{\subseteq} & \sum(\mathfrak{S}^n(x \cdot X)) & = & \mathfrak{S}^{n+1}(x \cdot X) \end{array}$$

8. In fact,

$$\mathfrak{S}(X \cdot Z) = \mathfrak{S}\left(\bigcup_{x \in X} x \cdot Z\right) \overset{X \subseteq Y}{=} \mathfrak{S}\left(\bigcup_{y \in Y} y \cdot Z\right) = \mathfrak{S}(Y \cdot Z)$$

■

Another important property of the operator $\mathfrak{S}$ is given in the Lemma below. It says that we can understand the membership relation $y \in \mathfrak{S}(X)$ using only finitely many elements of X.

Lemma 2.2.4 *Let $\mid$ be a divisibility of A and $X \subseteq A$. Then*

$$y \in \mathfrak{S}(X) \Leftrightarrow (\exists x_1, ..., x_r \in X) : y \in \mathfrak{S}(x_1, ..., x_r)$$

Proof : ($\Leftarrow$) : This is clear, because

$$\{x_1, ..., x_r\} \subseteq X \overset{Lemma(2.2.3)}{\Rightarrow} \mathfrak{S}(x_1, ..., x_r) \subseteq \mathfrak{S}(X)$$

($\Rightarrow$) : We prove by induction on n that, for all $n \in \mathbb{N}$,

$$y \in \mathfrak{S}^n(X) \Rightarrow \exists x_1, ..., x_r \in X : y \in \mathfrak{S}^n(x_1, ..., x_r)$$

The case $n = 0$ is trivial, because then $y \in X$. Suppose that the assertion above is true for some $n \geq 0$ and

$$y \in \mathfrak{S}^{n+1}(X)$$

If $\mathfrak{S}^{n+1}(X) = \mathbb{M}(\mathfrak{S}^n(X))$, then there is $y \in \mathbb{M}(z)$ and $z \in \mathfrak{S}^n(X)$. By induction hypothesis, there are $x_1, ..., x_r \in X$ such that $z \in \mathfrak{S}(x_1, ..., x_r)$, and hence also $y \in \mathfrak{S}(x_1, ..., x_r)$.

If $\mathfrak{S}^{n+1}(X) = \sum(\mathfrak{S}^n(X))$, then there are $z_1, ..., z_r \in \mathfrak{S}^n(X)$ such that $y = \sum_{i=1}^r z_i$. By induction hypothesis, there are $\{x_{1k}, ..., x_{i_k k}\}_{1 \leq k \leq r} \subseteq X$ such that

$$z_k \in \mathfrak{S}(x_{1k}, ..., x_{i_k k}) \text{ for all } 1 \leq k \leq r$$

Thus

$$y = \sum_{i=1}^{r} z_i \in \mathfrak{S}(\{x_{1k}, ..., x_{i_k k}\}_{1 \leq k \leq r})$$

■

Thanks to previous lemma, the next example helps us to justify the nomenclature used for $\mathfrak{S}$. More examples using the ideal operator will be seen later.

Example 2.2.5 *Let A be a ring and $\mid$ the usual divisibility of A, i.e., for all $a, b \in A$,*

$$a \mid b \Leftrightarrow (\exists c \in A) : b = a \cdot c$$

Then $\mathfrak{S}(X)$ is equal to $\langle X \rangle$, the ideal generated by X, for each $X \subseteq A$. In fact, it can be verified that

$$\mathbb{M}(X) = \bigcup_{x \in X} x \cdot A, \mathbb{M}(\langle X \rangle) = \langle X \rangle \text{ and } \sum(\langle X \rangle) = \langle X \rangle$$

It follows that $\mathfrak{S}(X) = \langle X \rangle$.

Now we are able to present and prove the fundamental theorem of extensions of divisibilities.

The idea of the proof is similar to the idea used in mathematical logic to verify that we have a "proof" of some logical proposition using a concatenations of other "proofs".[12]

In our case, given $a, b \in A$, we will define sequences using the operator $\mathfrak{S}$, and when such a sequence is satisfied for some $x, y \in A$, we will say that $x \mid_{a,b} y$ (This means: we have a "proof" of this fact).

To see that $\mid_{a,b}$ may define a divisibility, we will verify that, under certain concatenations of valid sequences, we can find another valid sequence.

This philosophy will be better explained in the practice.

Theorem 2.2.6 *Let $\mid$ be a divisibility on A. For each $x, y \in A$ we define $x \mid_{a,b} y$ if, and only if, there are $r \in \mathbb{N}^+$ and $c_1, ..., c_r \in A$ such that*

$$\begin{aligned} & c_1 a \in \mathfrak{S}(x) \\ & c_2 a \in \mathfrak{S}(x, c_1 b) \\ & \quad \vdots \\ & c_r a \in \mathfrak{S}(x, c_1 b, ..., c_{r-1} b) \\ & y \in \mathfrak{S}(x, c_1 b, ..., c_r b) \end{aligned}$$

The binary relation $\mid_{a,b}$ of A satisfies the properties $(1-4)$ of divisibilities, extends $\mid$ and $a \mid_{a,b} b$.

*Such a sequence is called **defining sequence** for $x \mid_{a,b} y$.*

Proof : If $x \mid y$, then we have a defining sequence

$$\begin{aligned} & 0 \cdot a = 0 \in \mathfrak{S}(x); \\ & y \in \mathfrak{S}(x, 0 \cdot b) = \mathbb{M}(x) \end{aligned}$$

for $c_1 = 0$, and hence $x \mid_{a,b} y$. Therefore $\mid \subseteq \mid_{a,b}$.

We also have $a \mid_{a,b} b$, because, for $c_1 = 1$,

$$\begin{aligned} & 1 \cdot a \in \mathfrak{S}(a); \\ & b \in \mathfrak{S}(a, 1 \cdot b) \end{aligned}$$

is a defining sequence.

From now on, we will use frequently the properties of Lemma(2.2.3) in the proof. We advise the reader to remember this Lemma.

[12]More about mathematical logic can be found in [17].

If $x \mid_{a,b} y$ and $c \in A$, we can multiply the relations of the defining sequence by c and deduce

$$\begin{aligned}
&(c_1c)a \in \mathfrak{S}(cx);\\
&(c_ic)a \in \mathfrak{S}(cx, (c_1c)b, ..., (c_{i-1}c)b);\ \text{for all } 2 \leq i \leq r \text{ (if such } i \text{ exists)}\\
&cy \in \mathfrak{S}(cx, (c_1c)b, ..., (c_rc)b))
\end{aligned}$$

because $c \cdot \mathfrak{S}(X) \subseteq \mathfrak{S}(c \cdot X)$, for all $X \subseteq A$, and hence $cx \mid_{a,b} cy$.

Suppose that $x \mid_{a,b} y$ and $y \mid_{a,b} z$. Take $c_1, ..., c_r \in A$ such that

$$\begin{aligned}
&c_1a \in \mathfrak{S}(x);\\
&c_ia \in \mathfrak{S}(x, c_1b, ..., c_{i-1}b);\\
&y \in \mathfrak{S}(x, c_1b, ..., c_rb)
\end{aligned}$$

and $d_1, ..., d_s \in A$ such that

$$\begin{aligned}
&d_1a \in \mathfrak{S}(y);\\
&d_ja \in \mathfrak{S}(y, d_1b, ..., d_{j-1}b);\\
&z \in \mathfrak{S}(y, d_1b, ..., d_sb)
\end{aligned}$$

Now, using (1),(3) and (6) of Lemma(2.2.3), and the defining sequences of $y \mid_{a,b} z$ and $x \mid_{a,b} y$ above, we can write

$$\begin{aligned}
&d_1a \in \mathfrak{S}(x, c_1b, ..., c_rb);\\
&d_ja \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_{j-1}b);\\
&z \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb)
\end{aligned}$$

Therefore

$$\begin{aligned}
&c_1a \in \mathfrak{S}(x);\\
&c_ia \in \mathfrak{S}(x, c_1b, ..., c_{i-1}b);\\
&c_ra \in \mathfrak{S}(x, c_1b, ..., c_{r-1}b)\\
&d_1a \in \mathfrak{S}(x, c_1b, ..., c_rb);\\
&d_ja \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_{j-1}b);\\
&z \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb)
\end{aligned}$$

is a defining sequence for $x \mid_{a,b} z$.

Suppose that $x \mid_{a,b} y$ and $x \mid_{a,b} z$. Take $c_1, ..., c_r \in A$, as above, and $d_1, ..., d_s \in A$ such that

$$\begin{aligned}
&d_1a \in \mathfrak{S}(x);\\
&d_ja \in \mathfrak{S}(x, d_1b, ..., d_{j-1}b);\\
&z \in \mathfrak{S}(x, d_1b, ..., d_sb)
\end{aligned}$$

As clearly $\{x\} \subseteq \{x, c_1b, ..., c_rb\}$, again by Lemma(2.2.3), we can write,

$$\begin{aligned} &d_1a \in \mathfrak{S}(x, c_1b, ..., c_rb); \\ &d_ja \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_{j-1}b); \\ &z \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb) \end{aligned}$$

On the other hand, it is also true

$$y \in \mathfrak{S}(x, c_1b, ..., c_rb) \subseteq \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb)$$

and hence, as $\sum(\mathfrak{S}(X)) = \mathfrak{S}(X)$ for all $X \subseteq A$,

$$y \pm z \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb)$$

Thus $x \mid_{a,b} (y \pm z)$, because

$$\begin{aligned} &c_1a \in \mathfrak{S}(x); \\ &c_ia \in \mathfrak{S}(x, c_1b, ..., c_{i-1}b); \\ &c_ra \in \mathfrak{S}(x, c_1b, ..., c_{r-1}b) \\ &d_1a \in \mathfrak{S}(x, c_1b, ..., c_rb); \\ &d_ja \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_{j-1}b); \\ &y \pm z \in \mathfrak{S}(x, c_1b, ..., c_rb, d_1b, ..., d_sb) \end{aligned}$$

is a defining sequence for $x \mid_{a,b} (y \pm z)$.

■

We will see in Proposition(2.2.9) that this is the minimal divisibility extending $\mid$ such that a divides b, if we suppose that at least one such divisibility exists.

This will be a consequence of the proposition.

Proposition 2.2.7 *Let $\mid$ be a divisibility on A. Then*

$$a \mid b \Leftrightarrow \mid_{a,b} \subseteq \mid$$

Proof : ($\Leftarrow$) If $\mid_{a,b} \subseteq \mid$, then $a \mid b$, because $a \mid_{a,b} b$.

($\Rightarrow$) Suppose that $a \mid b$ and $x \mid_{a,b} y$. Then, there are $r \in \mathbb{N}^+$ and $c_1, ..., c_r \in A$ satisfying

$$\begin{aligned} &c_1a \in \mathfrak{S}(x); \\ &c_ia \in \mathfrak{S}(x, c_1b, ..., c_{i-1}b); \text{ for all } 2 \leq i \leq r \text{ (if such } i \text{ exists)} \\ &y \in \mathfrak{S}(x, c_1b, ..., c_rb) \end{aligned}$$

If $r = 1$ (two relations) then

$$c_1 a \in \mathfrak{S}(x) \text{ and } y \in \mathfrak{S}(x, c_1 b) \overset{a|b}{\subseteq} \mathfrak{S}(x, c_1 a) \subseteq \mathfrak{S}(x)$$

and hence

$$y \in \mathfrak{S}(x, c_1 a) \subseteq \mathfrak{S}(x)$$

For the induction step, suppose that: if $x, y \in A$ satisfy a defining sequence with at most $n \geq 2$ relations, then also $x \mid y$.

Take $x, y \in A$ and suppose that they satisfy a defining sequence with $n+1$ relations, i.e., there are $c_1, ..., c_n \in A$ such that

$$\begin{aligned}
&c_1 a \in \mathfrak{S}(x);\\
&c_2 a \in \mathfrak{S}(x, c_1 b)\\
&\quad\vdots\\
&c_i a \in \mathfrak{S}(x, c_1 b, ..., c_{i-1} b)\\
&\quad\vdots\\
&y \in \mathfrak{S}(x, c_1 b, ..., c_n b)
\end{aligned}$$

Now observe that, as in the case $r = 1$, from the first two relations, we conclude that $\mathfrak{S}(x, c_1 b) \subseteq \mathfrak{S}(x)$, and hence, after applying (6) of Lemma(2.2.3),

$$\begin{aligned}
&c_2 a \in \mathfrak{S}(x, c_1 b) \subseteq \mathfrak{S}(x)\\
&\quad\vdots\\
&c_i a \in \mathfrak{S}(x, c_1 b, ..., c_{i-1} b) \subseteq \mathfrak{S}(x, c_2 b, ..., c_{i-1} b)\\
&\quad\vdots\\
&y \in \mathfrak{S}(x, c_1 b, ..., c_n b) \subseteq \mathfrak{S}(x, c_2 b, ..., c_n b)
\end{aligned}$$

is a defining sequence for $x \mid_{a,b} y$ consisting of n relations. Thus, by induction hypothesis, $x \mid y$.

■

The following remark about extensions of divisibilities of a ring A is easily verified from the definition of $\mathfrak{S}$, and will be used in the proof of the proposition below, as well as in other proofs .

Remark 2.2.8 *If* $|^* \in E(\ |\ )$, *then* $\mathfrak{S}(X) \subseteq \mathfrak{S}_*(X)$ *for all* $X \subseteq A$. *Here* $\mathfrak{S}(\ \cdot\ )$ *and* $\mathfrak{S}_*(\ \cdot\ )$ *are defined using the operators* $\mathbb{M}(\ \cdot\ ,\ |\ )$ *and* $\mathbb{M}(\ \cdot\ ,\ |^*)$, *respectively.*

Proposition 2.2.9 *Let* $\mid$ *be a divisibility of* A*. For all* $\mid^* \in E(\mid)$

$$a \mid^* b \Leftrightarrow \mid_{a,b} \subseteq \mid^*$$

Proof : ($\Leftarrow$) : If $\mid_{a,b} \subseteq \mid^*$, then $a \mid^* b$, because $a \mid_{a,b} b$.

($\Rightarrow$) : If $a \mid^* b$, then the proposition above provides $\mid^*_{a,b} \subseteq \mid^*$. However, $\mid_{a,b} \subseteq \mid^*_{a,b}$, by Remark(2.2.8).

■

For given $a, b \in A$, Theorem(2.2.6) guarantees only that the relation $\mid_{a,b}$ satisfies the first four properties of divisibilities, missing yet $0 \nmid_{a,b} 1$. Therefore, it is natural to ask for conditions assuring that $\mid_{a,b}$ is indeed a divisibility.

The important object to understand here is the ideal $I(\mid_{a,b})$, and we want conditions to say that $1 \notin I(\mid_{a,b})$. This is the case if, for example, $I(\mid) = I(\mid_{a,b})$.

Below, we will see a condition that determines when the equality $I(\mid) = I(\mid_{a,b})$ holds. This condition is an inclusion relation between a special type of ideals I of A related to a, b and the divisibility $\mid$.

They satisfy the condition $\mathfrak{S}(I) = I$, and also receive a name.

Definition 2.2.10 *Let* $\mid$ *be a divisibility of* A *and* $a \in A$*. We define the* ***annihilator of*** a ***with respect to*** $\mid$ *by*

$$Ann(a, \mid) := Ann(a) := \{x \in A : 0 \mid ax\}$$

Observe that $Ann(1) = I(\mid)$.

Lemma 2.2.11 *Let* $\mid$ *be a divisibility of* A *and* $a \in A$*. Then* $Ann(a)$ *is an ideal of* A *and*

$$\mathfrak{S}(Ann(a)) = Ann(a)$$

Proof : Clearly $Ann(a)$ is an ideal of A. We prove that

$$\mathfrak{S}^n(Ann(a)) = Ann(a) \tag{2.28}$$

for all $n \in \mathbb{N}$, proceeding by induction on n.

Note that

$$(\forall x, y, a \in A) : (x \mid y) \wedge (0 \mid ax) \Rightarrow (0 \mid ay),$$

and hence $\mathbb{M}(Ann(a)) \subseteq Ann(a)$. It also holds $\sum(Ann(a)) = Ann(a)$, because $Ann(a)$ is an ideal.

Now suppose that (2.28) is true for some $n \geq 1$. Thus

$$\mathbb{M}(\mathfrak{S}^n(Ann(a))) \overset{Ind.hyp.}{=} \mathbb{M}(Ann(a)) = Ann(a)$$
$$\sum(\mathfrak{S}^n(Ann(a))) \overset{Ind.hyp.}{=} \sum(Ann(a)) = Ann(a)$$

proves that $\mathfrak{S}^{n+1}(Ann(a)) = Ann(a)$.

Therefore also $\mathfrak{S}(Ann(a)) = Ann(a)$.

■

After this lemma, we have a proposition characterizing, in terms of ideals, when $I(\ |_{a,b}) = I(\ |\ )$, for some divisibility $|$ and elements $a, b \in A$.

Proposition 2.2.12 *Let $|$ be a divisibility of A. For all $a, b \in A$*

$$Ann(a) \subseteq Ann(b) \Leftrightarrow I(\ |_{a,b}) = I(\ |\ )$$

Proof : If $I(\ |_{a,b}) = I(\ |\ )$, then

$$0 \mid xa \Rightarrow 0 \mid_{a,b} bx \Rightarrow 0 \mid bx$$

for all $x \in A$, and hence $Ann(a) \subseteq Ann(b)$.

Conversely, suppose that $Ann(a) \subseteq Ann(b)$. Take $x \in A$ with $0 \mid_{a,b} x$. Then there are $r \in \mathbb{N}$ and $c_1, ..., c_r \in A$ such that

$$\begin{aligned} &c_1 a \in \mathfrak{S}(0) \\ &c_2 a \in \mathfrak{S}(0, c_1 b) \\ &\quad\vdots \\ &c_r a \in \mathfrak{S}(0, c_1 b, ..., c_{r-1} b) \\ &x \in \mathfrak{S}(0, c_1 b, ..., c_r b) \end{aligned}$$

However, applying the hypothesis $Ann(a) \subseteq Ann(b)$ to these relations,

$$\begin{aligned} c_1 a \in \mathfrak{S}(0) \quad &\Rightarrow c_1 b \in \mathfrak{S}(0) \\ &\Rightarrow c_2 a \in \mathfrak{S}(0, c_1 b) \subseteq \mathfrak{S}(0) \\ &\Rightarrow c_2 b \in \mathfrak{S}(0) \\ &\quad\vdots \\ &\Rightarrow c_r a \in \mathfrak{S}(0, c_1 b, ..., c_{r-1} b) \subseteq \mathfrak{S}(0) \\ &\Rightarrow c_r b \in \mathfrak{S}(0) \\ &\Rightarrow x \in \mathfrak{S}(0, c_1 b, ..., c_r b) \subseteq \mathfrak{S}(0) \end{aligned}$$

Thus also $0 \mid x$.

■

Another information, that we can extract from the relations $|_{a,b}$, is a condition for the existence of divisibilities $|'$, extending $|$, such that $0 \mid' c$, for some fixed $c \in A$.

Corollary 2.2.13 *Let* $|$ *be a divisibility of* A *and* $c \in A$. *Then*

$$|_{0,c} \in E(\ |\ ) \Leftrightarrow 1 \notin \mathfrak{S}(c \cdot A)$$

Thus, by Proposition(2.2.9), there is $|' \in E(\ |\ )$ *such that* $0\ |'\ c$ *if, and only if,* $1 \notin \mathfrak{S}(c \cdot A)$.

Proof : In fact, $0\ |_{0,c}\ 1$ if, and only if, there are $c_1, ..., c_r \in A$ such that

$$1 \in \mathfrak{S}(0, c_1c, ..., cc_r) = \mathfrak{S}(c_1c, ..., c_rc) \subseteq \mathfrak{S}(c \cdot A)$$

The converse is also true, because

$$1 \in \mathfrak{S}(c \cdot A) \overset{Lem.(2.2.4)}{\Rightarrow} \exists c_1, ..., c_r \in A : 1 \in \mathfrak{S}(c_1c, ..., c_rc)$$

■

We note that $I_c := \mathfrak{S}(c \cdot A)$ is an ideal of A, clearly satisfying $\mathfrak{S}(I_c) = I_c$, because of the properties of $\mathfrak{S}$. In general, for each subset I of A satisfying $A \cdot I \subseteq I$, $\mathfrak{S}(I)$ is an ideal of A, because for all $c \in A$

$$c \cdot \mathfrak{S}(I) \subseteq \mathfrak{S}(c \cdot I) \subseteq \mathfrak{S}(I) \text{ and } \mathfrak{S}(I) + \mathfrak{S}(I) \subseteq \mathfrak{S}(I)$$

This indicates the existence of a relationship between certain questions about supports $I(\ |'\ )$, for some $|' \in E(\ |\ )$, and the ideals I of A satisfying $\mathfrak{S}(I) = I$. These relations will be studied in the next section.

To finish this section we would like to observe another fact about the relation $|_{a,b}$ contained in the proposition below.

Proposition 2.2.14 *Let* $|$ *be a divisibility on* A *and* $a, b \in A$. *If* $0\ |_{a,b}\ 1$, *then there exists* $r \in \mathbb{N}$ *such that* $0 \mid a^r$.

Proof : If $0\ |_{a,b}\ 1$, then there are $r \in \mathbb{N}^+$ and $c_1, ..., c_r \in A$ such that

$$\begin{aligned}
&c_1a \in \mathfrak{S}(0) = \mathbb{M}(0)\\
&c_2a \in \mathfrak{S}(0, c_1b) = \mathfrak{S}(c_1b)\\
&\quad\vdots\\
&c_ra \in \mathfrak{S}(0, c_1b, ..., c_{r-1}b) = \mathfrak{S}(c_1b, ..., c_{r-1}b)\\
&1 \in \mathfrak{S}(0, c_1b, ..., c_rb) = \mathfrak{S}(c_1b, ..., c_rb)
\end{aligned}$$

Multiplying the last relation by a, we get

$$a \in \mathfrak{S}((c_1a)b, (c_2a)b, ..., (c_ra)b),$$

Now, using the other relation to "substitute" $c_1a, ..., c_ra$ in this relation, we deduce, after a finite number of applications of Lemma(2.2.3),

$$\mathfrak{S}((c_1a)b, (c_2a)b, ..., (c_ra)b) \subseteq \mathfrak{S}(0.b, (c_1b)b, ..., (c_{r-1}b)b),$$

and hence

$$a \in \mathfrak{S}((c_1b)b, ..., (c_{r-1}b)b)$$

Proceeding in this way $r-1$ more times, i.e., multiplying the relation found by a and then using the defining relations of $0 \mid_{a,b} 1$, we will get $a^r \in \mathfrak{S}(c_1ab^r) \subseteq \mathbb{M}(0)$.

■

As a consequence, we have a corollary telling us that, at least when a is not in the radical of $I(\mid)$, for some $a \in A$, the relation $\mid_{a,b}$ is a divisibility, for each arbitrary $b \in A$.

Corollary 2.2.15 *Let $\mid$ be a divisibility of A. For all $a, b \in A$:*

$$a \notin \sqrt{I(\mid)} \Rightarrow \mid_{a,b} \in E(\mid)$$

Proof: ■

2.3 Maximal Divisibilities and Valuations

In this section, we ask about the possibility of finding a valuation extending a given divisibility.

To do this, we use the information about the minimal ones, starting proving that, for each $a, b \in A$, and each divisibility of A, there is an extension of it such that, a divides b or b divides a.

Lemma 2.3.1 *Let $\mid$ be a divisibility of A and $a, b \in A$. Then $0 \nmid_{a,b} 1$ or $0 \nmid_{b,a} 1$.*

Proof : Suppose that $0 \mid_{a,b} 1$. Then Proposition(2.2.14) implies $0 \mid a^r$ for some $1 \leq r \in \mathbb{N}$. If $0 \mid_{b,a} 1$, then there are $s \in \mathbb{N}$ and $d_1, ..., d_s \in A$ such that

$$1 \in \mathfrak{S}(0, d_1a, ..., d_sa) = \mathfrak{S}(d_1a, ..., d_sa)$$

and hence

$$\begin{aligned} 1 \in \mathfrak{S}(d_1a, ..., d_sa) &\Rightarrow a^{r-1} \in \mathfrak{S}(d_1a^r, ..., d_sa^r) = \mathfrak{S}(0) \\ &\Rightarrow a^{r-2} \in \mathfrak{S}(d_1a^{r-1}, ..., d_sa^{r-1}) = \mathfrak{S}(0) \\ &\quad\vdots \\ &\Rightarrow a \in \mathfrak{S}(d_1a^2, ..., d_sa^2) = \mathfrak{S}(0) \\ &\Rightarrow 1 \in \mathfrak{S}(d_1a, ..., d_sa) = \mathfrak{S}(0), \end{aligned}$$

but the last relation is a contradiction.

■

The same type of arguments works to verify the next lemma, concerning cancellation by elements.

Lemma 2.3.2 *Let* $\mid$ *be a divisibility of* A *and* $a, b, c \in A$. *Then*

$$(ca \mid cb) \wedge (0 \nmid c) \Rightarrow 0 \nmid_{a,b} 1$$

Proof : Suppose that $ca \mid cb$, $0 \nmid c$ and $0 \mid_{a,b} 1$. Take $r \in \mathbb{N}^+$ and $c_1, ..., c_r \in A$ such that

$$\begin{aligned}
&c_1 a \in \mathfrak{S}(0) = \mathbb{M}(0)\\
&c_2 a \in \mathfrak{S}(0, c_1 b) = \mathfrak{S}(c_1 b)\\
&\quad\vdots\\
&c_r a \in \mathfrak{S}(0, c_1 b, ..., c_{r-1} b) = \mathfrak{S}(c_1 b, ..., c_{r-1} b)\\
&1 \in \mathfrak{S}(0, c_1 b, ..., c_r b) = \mathfrak{S}(c_1 b, ..., c_r b)
\end{aligned}$$

Multiplying all these relations by c, we get

$$\begin{aligned}
&c_1(ca) \in \mathbb{M}(0)\\
&c_2(ca) \in \mathfrak{S}(c_1(cb))\\
&\quad\vdots\\
&c_r(ca) \in \mathfrak{S}(c_1(cb), ..., c_{r-1}(cb))\\
&c \in \mathfrak{S}(c_1(cb), ..., c_r(cb))
\end{aligned}$$

Now, using the assumption $ca \mid cb$ and the properties of $\mathfrak{S}$, we have

$$\begin{array}{c}
c_1(ca) \in \mathbb{M}(0)\\
\Downarrow\\
c_2(ca) \in \mathfrak{S}(c_1(cb)) \subseteq \mathfrak{S}(c_1(ca)) = \mathbb{M}(0)\\
\Downarrow\\
c_3(ca) \in \mathfrak{S}(c_1(cb), c_2(cb)) \subseteq \mathfrak{S}(c_1(ca), c_2(ca)) = \mathbb{M}(0)\\
\Downarrow\\
\vdots\\
c_r(ca) \in \mathfrak{S}(c_1(cb), ..., c_{r-1}(cb)) \subseteq \mathfrak{S}(c_1(ca), ..., c_{r-1}(ca)) = \mathbb{M}(0)\\
\Downarrow\\
c \in \mathfrak{S}(c_1(cb), ..., c_r(cb)) \subseteq \mathfrak{S}(c_1(ca), ..., c_r(ca)) = \mathbb{M}(0)
\end{array}$$

contradicting $0 \nmid c$.

■

The next lemma is the last needed for our desired theorem. It enables us to maximize extension of divisibilities using Zorn's Lemma.

Lemma 2.3.3 *Let* $(\ |_i\ )_{i\in I}$ *be chain of divisibilities of* A *with* $I \neq \emptyset$. *Then*

$$|_I := \bigcup_{i\in I} |_i$$

is a divisibility of A *with support* $\bigcup_{i\in I} I(\ |_i)$.

Proof : By definition, for all $x, y \in A$

$$x\ |_I\ y \Leftrightarrow x\ |_i\ y \ \text{ for some } \ i \in I.$$

Thus $|_i \subseteq |_I$ for all $i \in I$ and, for all $x, y, z \in A$,

$$\begin{array}{rl} x\ |_I\ y & \Rightarrow (\exists i \in I) : x\ |_i\ y \Rightarrow (\exists i \in I) : xz\ |_i\ yz \Rightarrow xz\ |_I\ yz \\ x\ |_I\ y, y\ |_I\ z & \Rightarrow (\exists i, j \in I) : x\ |_i\ y, y\ |_j\ z \Rightarrow (\exists (i, j \leq) k \in I) : x\ |_k\ y, y\ |_k\ z \\ & \Rightarrow (\exists k \in I) : x\ |_k\ z \Rightarrow x\ |_I\ z \\ x\ |_I\ y, x\ |_I\ z & \Rightarrow (\exists i, j \in I) : x\ |_i\ y, x\ |_j\ z \Rightarrow (\exists (i, j \leq) k \in I) : x\ |_k\ y, x\ |_k\ z \\ & \Rightarrow (\exists k \in I) : x\ |_k\ (y \pm z) \Rightarrow x\ |_I\ (y \pm z) \end{array}$$

We also have $0 \nmid_I 1$, because otherwise we should have $0\ |_i\ 1$ for some $i \in I$.

■

Such unions of divisibilities will be used also in Chapter(3), as well as the next lemma.

Lemma 2.3.4 *Let* $(\ |_i\ )_{i\in I}$ *be a chain of divisibilities of* A *and* $|_I$ *defined as in Lemma*(2.3.3). *For all* $X \subseteq A$ *and* $y \in A$

$$y \in \mathfrak{S}_I(X) \Leftrightarrow y \in \mathfrak{S}_i(X) \text{ for some } i \in I$$

Proof : By Lemma(2.2.4), it is enough to proof this lemma when $X \subseteq A$ is a finite set, say $X = \{x_1, ..., x_r\}$. Moreover, as $|_i \subseteq |_I$ for all $i \in I$, the implication from right to the left is a consequence of Remark(2.2.8).

Therefore, it is enough to verify, by induction on n, that

$$y \in \mathfrak{S}^n_I(x_1, ..., x_r) \Rightarrow y \in \mathfrak{S}^n_i(x_1, ..., x_r) \text{ for some } i \in I \tag{2.29}$$

for all $n \in \mathbb{N}$.

First note that

$$y \in \mathbb{M}_I(x) \Leftrightarrow x\ |_I\ y \Leftrightarrow x\ |_i\ y \text{ for some } i \in I \Leftrightarrow y \in \mathbb{M}_i(x) \text{ for some } i \in I$$

for all $x, y \in A$.

Thus

$$\begin{aligned} y \in \mathbb{M}_I(x_1, ..., x_r) &\Rightarrow \bigvee_{1\le j\le r} x_j \mid_I y \\ &\Rightarrow \bigvee_{1\le j\le r} (x_j \mid_{i_j} y \text{ for some } i_j \in I) \\ &\Rightarrow \bigvee_{1\le j\le r} x_j \mid_k y \text{ with } k := \max\{i_j : 1 \le j \le r\} \\ &\Rightarrow y \in \mathbb{M}_k(x_1, ..., x_r) \text{ for some } k \in I \end{aligned}$$

Now suppose that (2.29) is true for some $n \ge 1$ and $y \in \mathfrak{S}_I^{n+1}(x_1, ..., x_r)$. If $\mathfrak{S}_I^{n+1}(x_1, ..., x_r) = \sum(\mathfrak{S}_I^n(x_1, ..., x_r))$, then

$$y = \sum_{t=1}^{s} z_t \text{ with } z_t \in \mathfrak{S}_I^n(x_1, ..., x_r)$$

By induction hypothesis

$$z_t \in \mathfrak{S}_I^n(x_1, ..., x_r) \Rightarrow z_t \in \mathfrak{S}_{i_t}^n(x_1, ..., x_r) \text{ for some } i_t \in I$$

Taking $k := \max\{i_t : 1 \le t \le s\}$, we get

$$y = \sum_{t=1}^{s} z_t \text{ and } z_t \in \mathfrak{S}_k^n(x_1, ..., x_r) \text{ for some } k \in I,$$

and hence $y \in \sum(\mathfrak{S}_I^n(x_1, ..., x_r)) = \mathfrak{S}_k^{n+1}(x_1, ..., x_r)$.

If $\mathfrak{S}_I^{n+1}(x_1, ..., x_r) = \mathbb{M}(\mathfrak{S}_I^n(x_1, ..., x_r))$, then

$$z \mid_I y \text{ for some } z \in \mathfrak{S}_I^n(x_1, ..., x_r)$$

By induction hypothesis, and by the definition of $\mid_I$, we get

$$z \mid_i y \text{ and } z \in \mathfrak{S}_j(x_1, ..., x_r) \text{ for some } i, j \in I$$

Taking $k := \max\{i, j\}$ we have

$$z \mid_k y \text{ and } z \in \mathfrak{S}_j(x_1, ..., x_r) \subseteq \mathfrak{S}_k(x_1, ..., x_r),$$

and hence $y \in \mathbb{M}(\mathfrak{S}_k^n(x_1, ..., x_r)) = \mathfrak{S}_k^{n+1}(x_1, ..., x_r)$.

■

After this deviation of our objectives, we return to them writing the desired theorem about valuations.

Theorem 2.3.5 *If $\mid$ is a divisibility of A, then every maximal divisibility extending $\mid$ is a valuation, and hence $V^{\max}(\mid) \neq \emptyset$.*

Proof : We have $E(\ |\ ) \neq \emptyset$ and for each chain $(\ |_i)_{i\in I} \subseteq E(\ |\ )$, if we define

$$|_I := \bigcup_{i\in I} |_i\ ,$$

then one verifies that $|_I \in E(\ |\ )$ (Lemma(2.3.3)).

Therefore, we can use Zorn's Lemma. Take $|^* \in E(\ |\ )$ maximal. We claim that $|^*$ has cancellation and is total.

In fact, by Lemma(2.3.1), for all $a, b \in A$, we have

$$|^*_{a,b} \in E(\ |^*) \quad \text{or} \quad |^*_{b,a} \in E(\ |^*),$$

and then, by maximality, $|^*_{a,b} = |^*$ or $|^*_{b,a} = |^*$. Thus $a\ |^*\ b$ or $b\ |^*\ a$.

If $0 \nmid^* c$ and $ac\ |^*\ cb$, then Lemma(2.3.2) implies that $|^*_{a,b} \in E(\ |^*\ )$, and hence, by maximality again, $|^*_{a,b} = |^*$. Thus $a\ |^*\ b$.

■

As a first consequence, we can characterize the intersection of all ideals that are supports of valuations extending $|$.

Proposition 2.3.6 *Let* $|$ *be a divisibility of* A*. Then*

$$\sqrt{I(\ |\ )} = \bigcap_{|^v \in V(\ |\ )} I(\ |^v)$$

Proof : $(\subseteq)$: Suppose that $0 \mid y^r$ for some $r \in \mathbb{N}$. Then $0\ |^v\ y^r$ for all $|^v \in V(\ |\ )$. As $I(\ |^v)$ is a prime ideal, by Remark(2.1.5), we also have $0\ |^v\ y$, for all $|^v \in V(\ |\ )$.

$(\supseteq)$: If $y \notin \sqrt{I(\ |\ )}$, then $|_{y,1} \in E(\ |\ )$, by Proposition(2.2.14), and hence $y\ |^v\ 1$ for some $|^v \in V(\ |_{y,1}) \subseteq V(\ |\ )$, by Theorem(2.3.5). Therefore $0 \nmid^v y$ for such valuation.

■

Similar arguments to that used in the proofs above, using the ideal operator $\mathfrak{S}$, will be used in the p-divisibility case many times, and hence it is helpful to have some familiarity with them.

We expect that the valuation divisibilities behave like valuations in the classical sense. Then, the maximal ones, must correspond to the trivial valuations, which in the classical sense correspond to fields. We will see below that this equivalence is indeed true.

Therefore, the maximal divisibilities are not so interesting in the general theory of divisibilities, because of their triviality. However, looking at them will give us some insight of the behavior of the maximal p-divisibilities, which are not trivial, because of the condition $p \nmid 1$. It helps us to understand which ideals of A are supports of p-divisibilities (See Theorem(2.3.11)).

Such ideals have the following convex property with respect to $|$, like the special class of ideals of the end of Section(2.2).

Definition 2.3.7 *Given a divisibility $|$ of A, with associated operator $\mathfrak{S}$, an ideal I of A is called $|$-**convex**, or $\mathfrak{S}$-**convex**, if $\mathbb{M}(I) = I$.*

We denote by $\mathsf{I}(\ |\ )$ and $\mathsf{P}(\ |\ )$ the sets of all $\mathfrak{S}$-convex ideals and prime ideals of A, respectively.

Note that this is equivalent to say $\mathfrak{S}(I) = I$, because, being an ideal, of course $\mathbb{M}(I) = I$ implies $\sum(\mathbb{M}(I)) = I$, and then also $\mathfrak{S}(I) = I$.

As we noted just before Proposition(2.2.14), for each ideal I of A, the set $\mathfrak{S}(I)$ is also an ideal of A. By construction, $\mathfrak{S}(I)$ is the minimal $\mathfrak{S}$-convex ideal of A containing I.

Now we state a proposition, saying that all maximal divisibilities are the trivial ones. It also says which are the possible supports of maximal divisibilities.

Proposition 2.3.8 *Let $|$ be a fixed divisibility of A. For each $P \in \mathsf{P}(\ |\ )$*

$$|^P := (A \backslash P \times A) \cup (P \times P)$$

is a maximal divisibility.[13]

Conversely, each maximal divisibility $|^v$ extending $|$ equals $|^P$ for some prime $P \in \mathsf{P}(\ |\ )$, namely $P := I(\ |^v\ )$.

Proof : ($\Rightarrow$) : Take $P \in \mathsf{P}(\ |\ )$ and $|^P$ as above. As P is $\mathfrak{S}$-convex, $| \subseteq |^P$.

In fact, if $x \notin P$, then $x\ |^P\ y$ for all $y \in A$. In particular, x divides also all $y \in \mathbb{M}(x)$. If $x \in P$ and $x \mid y$, then $y \in P$, by $\mathfrak{S}$-convexity, and hence $x\ |^P\ y$, by definition of $|^P$.

Suppose that $|^v$ is a maximal extension of $|^P$. If $x \in I(\ |^v) \backslash P$, then $x\ |^P\ y$ for all $y \in A$. Thus $x\ |^v\ y$ for all $y \in A$, because $|^P \subseteq |^v$. In particular $0\ |^v\ x\ |^v\ 1$, a contradiction.

Therefore $I(\ |^v) = P$, and hence

$$(\forall a, b \in A) : (0\ |^v\ a) \wedge (a\ |^v\ b) \Rightarrow (a\ |^P\ b),$$

because the left side above implies also $0\ |^P\ b$ and $0\ |^P\ a$.

Moreover, supposing $0 \nmid^v a$ and $a\ |^v\ b$, we also have $0 \nmid^P a$ and $a\ |^P\ b$, by definition of $|^P$. Thus $|^v \subseteq |^P$, and hence $|^P = |^v$, by maximality of $|^v$.

[13]Compare $|^P$ with the definition of trivial divisibilities in Definition(2.1.4), or with Example(2.1.11)(4), to see that it is indeed a trivial divisibility.

($\Leftarrow$) : If $|^v \supseteq |$ is maximal, then $|^v$ is a valuation by Theorem(2.3.5), and then $I(\ |^v)$ is a prime ideal by Remark(2.1.5). By Remark(2.2.8), $I(\ |^v)$ is $\mathfrak{S}$-convex, and hence $P := I(\ |^v) \in \mathsf{P}(\ |\ )$.

As P is $\mathfrak{S}$-convex and $I(\ |^v) = P$, the same argument used in the proof of the other implication above applies here, and then $|^v \subseteq |^P$. Being $|^v$ maximal, we conclude $|^v = |^P$.

■

Not just the maximal divisibilities have the $\mathfrak{S}$-convex ideals as supports, but also the set of all valuations extending $|\ .$

Theorem 2.3.9 *Let $|$ be a divisibility of a commutative ring A. Then*

$$\mathsf{P}(\ |\ ) = \{I(\ |^v) \subseteq A : |^v \in V(\ |\ )\}$$

Proof : If P is a support of some $|^v \in V(\ |\ )$, then P is prime and, for all $a, b \in A$,

$$a \mid b\ ,\ a \in P \Rightarrow 0\ |^v\ a\ |^v\ b \Rightarrow b \in P,$$

and therefore P is $\mathfrak{S}$-convex.

Conversely, if P is $\mathfrak{S}$-convex, then $|^P$ defined above is an extension of $|$ and a valuation with $I(\ |^P) = P$, because of its maximality and Proposition(2.3.8). This proves the other inclusion.

■

Let us see now which ideals are supports of p-valuations. First we fix a notation.

Definition 2.3.10 *For each divisibility $|$ of A, where $\mathbb{Z} \subseteq A$, define*

$$\mathsf{P}^0(\ |\ ) := \{P \in \mathsf{P}(\ |\ ) : P \cap \mathbb{Z} = \{0\}\}$$
$$\mathsf{P}_p(\ |\ ) := \{P \in \mathsf{P}(\ |\ ) : P = I(\ |^v\ ) \text{ for some } |^v \in V_p(\ |\ )\}$$

Observe that $V_p(\ |\ ) \neq \emptyset$ if, and only if, $\mathsf{P}_p(\ |\ ) \neq \emptyset$. Therefore, the following theorem gives us also a necessary and sufficient condition to have $V_p(\ |\ ) \neq 0$, when $|$ is a p-valuation.

Theorem 2.3.11 *Let A be a commutative ring containing $\mathbb{Z}$. Given a p-divisibility $|$ of A, we have $P \in \mathsf{P}_p(\ |\ )$ if, and only if, $P \in \mathsf{P}^0(\ |\ )$ and*

$$(\forall a \in A) : a \notin P \Rightarrow (p \cdot \mathbb{M}(a) - a) \cap P = \emptyset, \tag{2.30}$$

or equivalently, for all $a \in A$,

$$a \in A_P^\times \Rightarrow (bp - a) \in A_P^\times \text{ for all } b \in \mathbb{M}(a),$$

where $A_P^\times$ are the units of the localization A_P.

Proof : If $P \in \mathsf{P}^0(\ |\ )$ and it satisfies the condition above, then

$$\frac{1}{p} \notin \mathcal{O}(P) \subseteq F(P) := Quot(A/P),$$

where the field $F(P)$ has characteristic zero and

$$\mathcal{O}(P) := \left\{ \left(\frac{b+P}{a+P} \right) \in F(P) : a \mid b \text{ and } a \notin P \right\}$$

is the ring of $|$ with respect P, defined in the next Definition(2.4.1).

In fact, otherwise, there are $a, b \in A$ such that

$$a \mid b,\ a \notin P \text{ and } (bp - a) \in P,$$

but (2.30) implies $a \in P$, a contradiction.

Moreover, $\gamma(F(P)) \subseteq \mathcal{O}(P)$, because $|$ is a p-divisibility, and then it has the Kochen property γ_p. By the theorem of existence of p-valuations[14], we conclude that there is a p-valuation ring $\mathcal{O}_v$ of $F(P)$ containing $\mathcal{O}(P)$.

Thus, one verifies that

$$(\forall a, b \in A) : a\ |^v\ b :\Leftrightarrow \left(a \notin P \text{ and } \frac{b+P}{a+P} \in \mathcal{O}_v \right) \text{ or } a, b \in P;$$

defines a p-valuation $|^v$ extending $|$ with support P.

Conversely, if $P \in \mathsf{P}_p(\ |\ )$, then $P = I(\ |^v)$ for some $|^v \in V_p(\ |\ )$. Thus,

$$\mathcal{O}(\ |^v) := \left\{ \left(\frac{b+P}{a+P} \right) \in F(P) : a\ |^v\ b \text{ and } a \notin P \right\}$$

defines a p-valuation ring of $F(P)$, and hence $F(P)$ has characteristic zero. Therefore $P \in \mathsf{P}^0(\ |\ )$. Moreover,

$$(a \notin P) \wedge (b \in \mathbb{M}(a)) \wedge (pb - a) \in P$$

does not happen, because otherwise

$$\frac{1}{p} = \frac{b+P}{a+P} \in \mathcal{O}(P) \subseteq \mathcal{O}(\ |^v)$$

■

[14]In fact, since $p^{-1} \notin \mathcal{O}(P)$, we can choose, by Chevalley's Extension Theorem, a valuation (function) v of $F(P)$, with associated valuation ring $\mathcal{O}_v$ of $F(P)$, such that $\mathcal{O}(P) \subseteq \mathcal{O}_v$ and $p^{-1} \notin \mathcal{O}_v$. Now, by Lemma(6.2) of [20], v is a p-valuation (function).

2.4 Divisibilities with Cancellation and Minimal Extensions in $\mathcal{C}_a(A)$

Divisibilities with cancellation have a very good property that distinguishes them from the others. They can be uniquely associated with some subring of some field, and their properties are all described by algebraic properties of this ring.

As a consequence, we will see that there is a one to one correspondence between valuations of A (in the divisibility sense) and valuation functions of A (Bourbarki valuations). Thus, we can identify them.

In this section, we also define another binary relation on A extending $|$ and depending of elements $a, b \in A$, namely $|^{a,b}$. When $|$ has cancellation by a, we will verify that this is the minimal divisibility extending $|$ satisfying a divides b.

This relation will be used later in the study of p-divisibilities, because, if $p^{-1} \in A$, then each divisibility $|$ of A has cancellation by p. Thus $|^{p,1}$ is always an extension of $|\ |$. Moreover, by its minimality, we can deduce that $a\ |^{p,1}\ b$ if, and only if, $|$ has a p-extension satisfying a divides b.

Let us start defining the rings that will be used for the correspondence with divisibilities having cancellation.

Definition 2.4.1 *Let $|$ be a divisibility of A. For each prime ideal $P \subseteq A$, we can define the field of quotients $F(P) := Quot(A/P)$ and also its subring*

$$\mathcal{O}(P) := \left\{ \left(\frac{b+P}{a+P} \right) \in F(P) : a \mid b \text{ and } a \notin P \right\},$$

*called the **ring of** $|$ **with respect to** P.*

If $|$ has support prime $P := I(\ |\ )$, then we define $F(\ |\ ) := Quot(A/P)$ and a subring

$$\mathcal{O}(\ |\ ) := \left\{ \left(\frac{b+P}{a+P} \right) \in F(\ |\ ) : a \mid b \text{ and } a \notin P \right\},$$

*called the **ring of** $|\ |$.*

Note that these are well-defined rings, because P is prime, and hence, by the properties of divisibilities,

$$a \mid b, c \mid d \text{ and } c, a \notin P \Rightarrow ac \mid (bc \pm ad), ac \mid bd \text{ and } ac \notin P$$

The characterization of divisibilities with cancellation is the proposition:

Proposition 2.4.2 *Let $|$ be a divisibility of A. There is a 1-1 correspondence between $\mathcal{C}(\ |\ )$, the set of extensions of $|$ with cancellation, and*

$$\mathcal{R} := \{R : R \text{ is a subring of } Quot(A/P) \text{ and } R \supseteq \mathcal{O}(P) \text{ for some } P \in \mathsf{P}(\ |\ )\}$$

The correspondence is given by

$$|^* \mapsto \mathcal{O}(\ |^*)\ ,\ R \mapsto |^R\ ,$$

where, for all $a, b \in A$,

$$a\ |^R\ b :\Leftrightarrow \begin{cases} (b+P)/(a+P) \in R & ,\ \text{if } a \notin P \\ b \in P & ,\ \text{if } a \in P. \end{cases}$$

Proof : For $|^* \in \mathcal{C}(\ |\ )$, as $| \subseteq |^*$, the set $\mathcal{O}(\ |^*)$ is a subring of $Quot(A/P)$ for $P := I(\ |^*) \in \mathsf{P}(\ |\ )$, and clearly $\mathcal{O}(P) \subseteq \mathcal{O}(\ |^*)$. Thus $|^* \mapsto \mathcal{O}(\ |^*)$ defines a map from $\mathcal{C}(\ |\ )$ to $\mathcal{R}$.

Take $R \in \mathcal{R}$. Then $|^R$ is a divisibility of A with cancellation[15] with support $P \in \mathsf{P}(\ |\ )$.

We want to see that $| \subseteq |^R$. For this we use the assumptions $\mathcal{O}(P) \subseteq R$ and $P \in \mathsf{P}(\ |\ )$. In fact, for all $a, b \in A$,

$$(a \notin P) \wedge (a \mid b) \overset{\mathcal{O}(P)\subseteq R}{\Rightarrow} (a\ |^R\ b)$$
$$(a \in P) \wedge (a \mid b) \overset{P\in\mathsf{P}(\ |\ )}{\Rightarrow} (b \in P) \Rightarrow (a\ |^R\ b)$$

Note that the $\mathfrak{S}$-convexity is necessary for $| \subseteq |^R$, because otherwise there is $i \in I$ such that $i \notin P$, and hence $0 \mid i$, but $0 \nmid^R i$.

Finally note that, for all $a, b \in B$, using the definitions, one verifies for each $|^*$ with cancellation

$$a\ |^*\ b \Leftrightarrow \frac{b + I(\ |^*\ )}{a + I(\ |^*\ )} \in \mathcal{O}(\ |^*\ ) \text{ or } a, b \in I(\ |^*\ ) \Leftrightarrow a\ |^{\mathcal{O}(\ |^*)}\ b$$

and, for $R \in \mathcal{R}$,

$$\frac{b+P}{a+P} \in R \Leftrightarrow a\ |^R\ b \text{ and } a \notin P \Leftrightarrow \frac{b+P}{a+P} \in \mathcal{O}(\ |^R\ ),$$

proving that $|^* = |^{\mathcal{O}(\ |^*)}$ and $R = \mathcal{O}(\ |^R)$, and then the maps are inverses of each other. Thus they define bijections.

■

[15] We let this verification for the reader. Only its definition is needed.

As consequence we have the desired correspondence between valuations and valuation rings, because for each divisibility $|^v$ with cancelation and each $a, b \in A$

$$a \,|^v\, b \Leftrightarrow \frac{b+P}{a+P} \in \mathcal{O}(\ |^v)$$

We also have a bijection with the Bourbaki valuations $v : A \to \Gamma \cup \{\infty\}$, for some abelian ordered group Γ. In fact, note that $P = v^{-1}(\infty)$ is always a prime ideal of A, and then we can use this fact to prove the existence of a bijection between the Bourbaki valuations v_* of A, with $v_*^{-1}(\infty) = P$, and the valuation rings of $Quot(A/P)$.[16]

We collect the conclusions of this discussion in a corollary to be remembered later.

Corollary 2.4.3 *Let $|$ be a divisibility of A. There is a 1-1 correspondence between the set $V(\ |\ )$ of valuations extending $|$ and the set of Bourbaki valuations $v : A \to \Gamma \cup \{\infty\}$ with $v^{-1}(\infty) \in \mathsf{P}(\ |\ )$.*

In the theory of valued fields, we see that valuation rings can be used to describe the integral closure $\overline{A}$ of a subring A in the field F,[17] more precisely

$$\overline{A} = \bigcap_{\mathcal{O}_v \in V_F(A)} \mathcal{O}_v, \tag{2.31}$$

where $V_F(A)$ is the set of all valuation rings of F containing A.

Because of its importance (they play an important role in algebraic number theory), such intersections receive names: an arbitrary intersection of valuation rings $\mathcal{O}_v$ of F is called a **holomorphy ring** and the intersection of all $\mathcal{O}_v \in V_F(A)$ is called the **holomorphy ring of** A.

The equality above can be seen as a local global principle, where the local properties given by $a \in \mathcal{O}_v$, for all $\mathcal{O}_v \in V_F(A)$, can be translated into the global property $a \in \overline{A}$.

In this text, we will understand local-global properties for valuations (functions and divisibilities) as properties relating valuations extending some divisibility (or a ring) and the given divisibility (or ring).

Such local-global principles will be used, for example, to study representations of commutative rings in $C(X, \mathbb{Q}_p)$, for some compact space X.

Note that, if $\{\ |_i\}_{i\in I}$ is a given a family of divisibilities of A, then its intersection $\bigcap_{i\in I} |_i$ defines also a divisibility of A. Using this observation we can define a notion of holomorphy for divisibilities.

[16] Remember Definition(2.1.6) and the discussion below it.

[17] Theorem(3.1.3) of [19].

Definition 2.4.4 *Let D be a set of valuations of A. Then the divisibility*

$$|_D := \bigcap_{|^* \in D} |^*$$

is called the ***holomorphic divisibility of*** *D.*

If $|$ is a divisibility of A, the ***holomorphic divisibility of*** *$|$ is*

$$|^H := \bigcap_{|^v \in V(\ |\ )} |^v$$

One of the properties of $|^H$ is

$$I(\ |^H) = \bigcap_{P \in \mathsf{P}(\ |\ )} P \overset{Prop.(2.3.6)}{=} \sqrt{I(\ |\ )}$$

As all valuations have cancellation, by definition, we can use the previous discussion to give an algebraic description of $|^H$.

Theorem 2.4.5 *Let $|$ be a divisibility of A. For each $a, b \in A$*

$$a\ |^H\ b \Leftrightarrow (\forall P \in \mathsf{P}(\ |\ )) : \left(\left(\frac{b+P}{a+P} \right) \in \overline{\mathcal{O}(P)}\ ,\ a \notin P \right)\ \textit{or}\ (a, b \in P)$$

where $\overline{\mathcal{O}(P)}$ denotes the integral closure of $\mathcal{O}(P)$ in $F(P)$.

Proof : First remember that a prime ideal P is a support of some valuation extending $|$ if, and only if, P is $\mathfrak{S}$-convex (Theorem(2.3.9).).

If $a\ |^H\ b$, then $a\ |^v\ b$ for all $|^v \in V(\ |\ )$. For each $P \in \mathsf{P}(\ |\ )$, let $V(P)$ be the set of all valuations extending $|$ with $I(\ |^v) = P$.

For all $|^v \in V(P)$, the corresponding valuation ring $\mathcal{O}_v$ satisfies

$$\mathcal{O}(P) \subseteq \mathcal{O}_v \subseteq F(P)$$

Conversely, each valuation ring satisfying this defines a valuation belonging to $V(P)$, namely $|^{\mathcal{O}_v}$, as in Proposition(2.4.2). Thus

$$[(\forall\ |^v \in V(P)) : (a\ |^v\ b)] \Leftrightarrow (a, b \in P)\ \text{or}\ \left(\frac{b+P}{a+P} \right) \in \bigcap_{\mathcal{O}(P) \subseteq \mathcal{O}_v} \mathcal{O}_v = \overline{\mathcal{O}(P)}$$

where $\mathcal{O}_v$ are valuation rings of $F(P)$. Varying $P \in \mathsf{P}(\ |\ )$ we get the desired conclusion.

For the converse, observe that, if $a \nmid^H b$, then $a \nmid^v b$ for some $|^v \in V(\ |\ )$ with $P := I(\ |^v) \in \mathsf{P}(\ |\ )$, or equivalently $a \nmid^{\mathcal{O}(\ |_v)} b$.

Thus,

$$(a \in P) \wedge (b \notin P) \text{ or } (a \notin P) \wedge \left(\frac{b+P}{a+P}\right) \notin \mathcal{O}_v$$

In the last case $(b+P)/(a+P) \notin \overline{\mathcal{O}(P)}$.

■

What we have seen so far, is that the local information of some divisibility, given by $V(\ |\ )$, is closely related to the rings

$$\prod_{P \in \mathsf{P}(\ |\ )} \mathcal{O}(P) \subseteq \prod_{P \in \mathsf{P}(\ |\ )} F(P),$$

where products and sums are taken component-wise.

After these digressions about intersections of valuations, we want to show another result related to divisibilities with cancelation, which relates the membership relation $y \in \mathfrak{S}(X)$, for some fixed $X \subseteq A$, with the membership relation $\overline{y} \in \langle \overline{X} \rangle$, where $\overline{y} := y + I(\ |\ )$ and $\langle \overline{X} \rangle$ is the $\mathcal{O}(\ |\ )$-module generated by $\overline{X} := X + I(\ |\ )$ contained in the field $F(\ |\ )$.

Proposition 2.4.6 *Let $|$ be a divisibility of A with cancellation, i.e., $| \in \mathcal{C}(A)$. With the same notations as in the paragraph above, for all $X \subseteq A$ and $y \in A$*

$$y \in \mathfrak{S}(X) \Leftrightarrow \overline{y} \in \langle \overline{X} \rangle$$

Proof : Using Lemma(2.2.3), we can verify that

$$y \in \mathfrak{S}(X) \Leftrightarrow y + I(\ |\ ) \in \mathfrak{S}(X + I(\ |\ ))$$

Thus we can suppose, without loss of generality, $I(\ |\ ) = \{0\}$, and hence $B := \mathcal{O}(\ |\ ) \subseteq Quot(A)$, because $I(\ |\ )$ is prime when $|$ has cancellation.

Observe that, by Lemma(2.2.4), $y \in \mathfrak{S}(X)$ if, and only if, there are $x_1, ..., x_r \in X$ such that $y \in \mathfrak{S}(x_1, ..., x_r)$. Thus it is enough to verify the assertion above for a finite set $X = \{x_1, ..., x_r\}$. As $y \notin I(\ |\ )$ by hypothesis, we can take all x_i different from zero.

We will prove by induction on $n \in \mathbb{N}$ that, if $n \geq 2$, then

$$y \in \mathfrak{S}^n(x_1, ..., x_r) \Leftrightarrow y \in x_1 B + ... + x_r B \tag{2.32}$$

and so follows the desired conclusion for $\mathfrak{S}$.

Start with $n = 2$. By Proposition(2.4.2), for all $a, b \in A$

$$b \in \mathbb{M}(a) \Leftrightarrow a \mid b \Leftrightarrow b \in aB$$

and hence

$$y \in \mathbb{M}(x_1, ..., x_r) \Leftrightarrow y \in x_1B \vee ... \vee y \in x_rB$$

Thus

$$\begin{array}{rcl} y \in \mathfrak{S}^2(x_1, ..., x_r) & = & \sum(\mathbb{M}(x_1, ..., x_r)) \\ & \Updownarrow & \\ y \in \sum(x_1B, ..., x_rB) & = & x_1B + ... + x_rB \end{array}$$

For the induction step, suppose now that (2.32) is true for some $n \geq 2$ and take $y \in \mathfrak{S}^{n+1}(x_1, ..., x_r)$. If $y \in \mathbb{M}(\mathfrak{S}^n(x_1, ..., x_r))$, then there is $z \in \mathfrak{S}^n(x_1, ..., x_r)$ such that $z \mid y$. By induction hypothesis, this is equivalent to

$$y \in zB \text{ and } z \in x_1B + ... + x_rB$$

and hence $y \in x_1B + ... + x_rB$.

If $y \in \sum(\mathfrak{S}^n(x_1, ..., x_r))$ then there are $z_1, ..., z_s \in \mathfrak{S}^n(x_1, ..., x_r)$ such that $y = \sum_{i=1}^{s} z_i$. By induction hypothesis again, this is equivalent to

$$z_1, ..., z_s \in x_1B + ... + x_rB \text{ and } y = \sum_{i=1}^{s} z_i$$

and then $y \in x_1B + ... + x_rB$.

As $y \in x_1B + ... + x_rB \Rightarrow y \in \mathfrak{S}^2(x_1, ..., x_r) \subseteq \mathfrak{S}^n(x_1, ..., x_r)$ for all $n \in \mathbb{N}$, the equivalence in (2.32) is proved.

■

In particular,

Corollary 2.4.7 *Let* $\mid \in \mathcal{C}(A)$. *Then, for all* $y, x_1, ..., x_n \in A$,

$$y \in \mathfrak{S}(x_1, ..., x_n) \Leftrightarrow \overline{y} \in \overline{x_1} \cdot \mathcal{O}(\mid) + ... + \overline{x_n} \cdot \mathcal{O}(\mid)$$

Proof: ■

Now we want to show that, under the assumption that a divisibility of a ring A has cancellation by $a \in A$, we can give an easier description of the minimal divisibilities extending it and satisfying a divides b, for $b \in A$ fixed. The motivation for this result comes from a discussion about cancellation divisibilities and holomorphic divisibilities done below.

Let $\mid$ be a given divisibility and $\mid^*$ a minimal divisibility extending $\mid$ with $a \mid^* b$, for some $a, b \in A$. If $P \in \mathsf{P}(\mid)$ we can observe the set $\mathcal{C}(P)$ of all divisibilities with cancellation extending $\mid$ with support P. By the proof of Proposition(2.4.2), we know that there is a 1-1 correspondence between this set and the subrings of $F(P)$ containing $\mathcal{O}(P)$.

To take all $|^+ \in \mathcal{C}(P)$ with $a \mid^+ b$ is equivalent, by Proposition(2.4.2), to choose all rings $R \in F(P)$ containing $\mathcal{O}(P)$ and satisfying

$$\left((a \notin P) \wedge \left(\frac{b+P}{a+P}\right) \in R\right) \text{ or } (a, b \in P)$$

However, we know which is the minimal ring in $F(P)$ with these properties. It is exactly the ring of polynomials

$$\mathcal{O}_{a,b}(P) := \mathcal{O}(P)\left[\left(\frac{b+P}{a+P}\right)\right]$$

This ring of polynomial defines a divisibility $|^{\mathcal{O}_{a,b}(P)}$ of A extending $|$ and contained in each element of $\mathcal{C}(P)$. Now, by its definition, for all $x, y \in A$,

$$x \mid^{\mathcal{O}_{a,b}(P)} y \Leftrightarrow \left((x \notin P) \wedge \left(\frac{y+P}{x+P}\right) \in \mathcal{O}_{a,b}(P)\right) \text{ or } (x, y \in P)$$

Thus, when $x \notin P$, $x \mid^{\mathcal{O}_{a,b}(P)} y$ is equivalent to the existence of some polynomial $f \in \mathcal{O}(P)[X]$ such that

$$\frac{y+P}{x+P} = f\left(\frac{b+P}{a+P}\right),$$

After simplifying denominators and some algebraic manipulations, one can see that this is also equivalent to the existence of $r := \deg(f) \in \mathbb{N}$ and $c_0, ..., c_r \in \mathcal{O}(P)$ such that

$$ya^r + P = x \cdot (b^r + c_{r-1}b^{r-1}a + ... + c_1ba^{r-1} + c_0a^r) + P$$

Note that the same argument holds for all $P \in \mathsf{P}(\ |\ )$, what motivates us to find a generalization of this condition (modulo P).

Note that

$$c \in \mathcal{O}_{a,b}(P) \Leftrightarrow c \in \mathfrak{S}(1, |^{\mathcal{O}_{a,b}(P)}).$$

Thus, by analogy, we can infer that $c \in \mathcal{O}(P)$ should be equivalent to $c \in \mathfrak{S}(1)$. Using this intuitive reasoning, the condition above, without P, should be written as

$$(\exists r \in \mathbb{N})(\exists c_0, ..., c_r \in \mathfrak{S}(1)) : ya^r = x \cdot (b^r + c_{r-1}b^{r-1}a + ... + c_1ba^{r-1} + c_0a^r)$$

As $c_ib^ia^{r-i} \in \mathfrak{S}(b^ia^{r-i})$ for each $i \in \{0, ..., r-1\}$ and clearly $b^r \in \mathfrak{S}(b^r)$, using the equality $\sum \mathfrak{S} = \mathfrak{S}$, we conclude that

$$ya^r \in \mathfrak{S}(x \cdot (b^r + c_{r-1}b^{r-1}a + ... + c_1ba^{r-1} + c_0a^r))$$

Now we write $x \mid^{a,b} y$ if the relation above is true, and we hope that the binary relation $\mid^{a,b}$ on A satisfies at least the conditions $(1-4)$ of divisibilities and is minimal, with respect to the condition a divides b.

This will be the case, and $\mid^{a,b}$ will be a divisibility exactly when $a \notin \sqrt{I(\ \mid\ )}$, as the next theorem shows.

Theorem 2.4.8 *Let $\mid$ be a divisibility of A. For all $x, y \in A$ we define*

$$x \mid^{a,b} y \Leftrightarrow (\exists r \in \mathbb{N}) : a^r y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}),$$

where $\{b^i a^{r-i}\}_{0 \leq i \leq r} := \{1\}$ if $r = 0$.

Then $\mid^{a,b}$ is an extension of $\mid$ satisfying $(1-4)$ and $a \mid^{a,b} b$. It follows from its definition that

$$I(\ \mid^{a,b}) = \{y \in A : a^r y \in I(\ \mid\ ) \text{ for some } r \in \mathbb{N}\}$$

and then

$$0 \mid^{a,b} x \Leftrightarrow a \in \sqrt{Ann(x)} \quad \text{and} \quad 0 \mid^{a,b} 1 \Leftrightarrow a \in \sqrt{I(\ \mid\ )}$$

Proof : Suppose that $x \mid y$. Taking $r = 0$, we deduce

$$y = a^0 y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{i=r=0}) = \mathfrak{S}(x)$$

and hence $x \mid^{a,b} y$.

Taking $r = 1$,$x = a$ and $y = b$, we have

$$ab \in \mathfrak{S}(a \cdot \{a, b\}) = \mathfrak{S}(a^2, ab)$$

and then $a \mid^{a,b} b$.

If $x \mid_{a,b} y$, then

$$a^r y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}),$$

for some $r \in \mathbb{N}$. After multiplying by $c \in A$, we have

$$a^r(cy) \in \mathfrak{S}((cx) \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}),$$

and hence $cx \mid^{a,b} cy$.

Suppose that $x \mid^{a,b} y$ and $y \mid^{a,b} z$. Then there are $r, s \in \mathbb{N}$ such that

$$a^r y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}) \quad \text{and} \quad a^s z \in \mathfrak{S}(y \cdot \{b^j a^{s-j}\}_{0 \leq j \leq s}),$$

Multiplying the second relation above by a^r, and using the first, we get

$$\begin{aligned} a^{(s+r)} z \in \mathfrak{S}((a^r y) \cdot \{b^j a^{s-j}\}_{0 \leq j \leq s}) &\subseteq \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r} \cdot \{b^j a^{s-j}\}_{0 \leq j \leq s}) \\ &\subseteq \mathfrak{S}(x \cdot \{b^k a^{(s+r)-k}\}_{0 \leq k \leq (s+r)}) \end{aligned}$$

and hence $x \mid^{a,b} z$.

Now suppose that $x \mid^{a,b} y$ and $x \mid^{a,b} z$. Then there are $r, s \in \mathbb{N}$ such that

$$a^r y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}) \text{ and } a^s z \in \mathfrak{S}(x \cdot \{b^j a^{s-j}\}_{0 \leq j \leq s}),$$

Multiplying the first relation by a^s and the second by a^r, we deduce

$$a^{(s+r)} y \in \mathfrak{S}(a^s x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}) \subseteq \mathfrak{S}(x \cdot \{b^k a^{(s+r)-k}\}_{0 \leq k \leq (s+r)})$$
$$a^{(s+r)} z \in \mathfrak{S}(a^r x \cdot \{b^j a^{s-j}\}_{0 \leq j \leq s}) \subseteq \mathfrak{S}(x \cdot \{b^k a^{(s+r)-k}\}_{0 \leq k \leq (s+r)})$$

Therefore

$$a^{(s+r)}(y \pm z) = (a^{(s+r)} y \pm a^{(s+r)} z) \in \mathfrak{S}(x \cdot \{b^k a^{(s+r)-k}\}_{0 \leq k \leq (s+r)})$$

and hence $x \mid^{a,b} (y \pm z)$.

■

The next lemma shows that this relation has cancellation by a.

Lemma 2.4.9 *Let $\mid$ be a divisibility of A and $a, b \in A$. Then $\mid^{a,b}$ has cancellation by a.*

Proof : If $ax \mid^{a,b} ay$ then there is $r \in \mathbb{N}$ such that

$$a^r(ay) \in \mathfrak{S}((ax) \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}) \Rightarrow a^{r+1} y \in \mathfrak{S}(x \cdot \{b^i a^{r+1-i}\}_{0 \leq i \leq r+1}) \Rightarrow x \mid^{a,b} y$$

■

A corollary from this lemma and the proposition above is:

Corollary 2.4.10 *If $\mid$ is a divisibility on A then*

$$\mathcal{C}_a(\ \mid\ ) \neq \emptyset \Leftrightarrow a \notin \sqrt{I(\ \mid\ )}.$$

Proof : The only implication we need to verify is from left to right. But, if $0 \mid a^n$ for some $n \in \mathbb{N}$, and $\mid^* \in \mathcal{C}_a(\ \mid\ )$, then

$$0 \mid^* a^n \Rightarrow 0 \mid^* a^{n-1} \Rightarrow ... \Rightarrow 0 \mid^* a \Rightarrow 0 \mid^* 1,$$

a contradiction.

■

The next proposition (actually its corollary) will assure that $\mid^{a,b}$ is minimal in the set of extensions with cancellation by a, as promised.

Proposition 2.4.11 *Let $\mid$ be a divisibility of A with cancellation by a. Then*

$$a \mid b \Leftrightarrow \mid^{a,b} \subseteq \mid$$

Proof : ($\Leftarrow$) If $|^{a,b} \subseteq |$, then $a \mid b$, because $a \,|^{a,b}\, b$.
($\Rightarrow$) Suppose that $a \mid b$ and $x \,|^{a,b}\, y$. Then there is $r \in \mathbb{N}$ such that

$$a^r y \in \mathfrak{S}(x \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r}) \overset{a|b}{\subseteq} \mathfrak{S}(a^r x) = \mathbb{M}(a^r x),$$

and hence $x \mid y$ by iterated cancellation by a.
■

As in Section(2.2), we can deduce the minimal property of $|^{a,b}$.

Corollary 2.4.12 *Let $|$ be a divisibility of A with cancellation by a. For all $|^* \in \mathcal{C}_a(\ |\ )$ and $b \in A$*

$$a \,|^*\, b \Leftrightarrow |^{a,b} \subseteq |^*$$

In particular, for any divisibility $|$ of A and $a, b \in A$, $|^{a,b}$ is the minimal extension of $|$ with cancellation by a such that a divides b.

Proof : ($\Leftarrow$) : If $|^{a,b} \subseteq |^*$, then $a \,|^*\, b$, because $a \,|^{a,b}\, b$.
($\Rightarrow$) If $a \,|^*\, b$ and $|^* \in \mathcal{C}_a(\ |\ )$, then the Proposition(2.4.11) above implies $(\ |^*)^{a,b} \subseteq |^*$. However $|^{a,b} \subseteq (\ |^*)^{a,b}$.
■

Extensions of the type $|^{a,b}$ will be frequently used in the theory of p-divisibilities, where the validity of the relationship $p \,|^{a,b}\, 1$ will be investigated, i.e., the validity of

$$(\exists r \in \mathbb{N}) : a^r \in \mathfrak{S}(p \cdot \{b^i a^{r-i}\}_{0 \leq i \leq r})$$

2.5 Cancellation by Elements

The study of cancellation properties is important, because in general divisibilities do not have cancellation. In our study, for example, the canonical divisibility $|_0$ of $C(X, \mathbb{Q}_p)$ does not have cancellation. One way to verify this is to look at the support of $|_0$, namely

$$I(\ |_0) = \{f \in C(X, \mathbb{Q}_p)\ :\ f(x) = 0 \text{ for all } x \in X\},$$

which is not a prime ideal, and hence it is not possible for $|_0$ to have cancellation.

In the previous section we studied divisibilities with cancellation, here we will study also cancellation, but by elements.

The understanding of cancellation by elements will be useful to handle divisibilities without cancellation and provides some techniques, helping us to find some local-global principles in the coming chapter.

This section will be more technical, and some proofs will be just verifications of some fact using calculations and the properties of the operator $\mathfrak{S}$. However, the results found here will be necessary and they need proofs.

Let us start with an easy, but fundamental lemma.

Lemma 2.5.1 *Let* $\mid$ *be a divisibility of* A *and* $c \in A$ *satisfying* $0 \nmid c$ *. Then* $\mid^c$ *defined by*

$$(\forall a, b \in A) : a \mid^c b :\Leftrightarrow ac \mid cb$$

is a divisibility of A *extending* $\mid$ *. Clearly*

$$I(\ \mid^c\ ) = Ann(c) := \{x \in A\ :\ 0 \mid cx\}$$

Proof : We have $\mid \subseteq \mid^c$ and $0 \nmid^c 1$, because $0 \nmid c$ and $(x \mid y \Rightarrow cx \mid cy)$, for all $x, y \in A$. Also, for all $x, y, z \in A$,

$$\begin{aligned}
&x \mid^c y \Rightarrow cx \mid cy \Rightarrow c(zx) \mid c(zy) \Rightarrow zx \mid^c zy\\
&x \mid^c y,\ y \mid^c z \Rightarrow cx \mid cy,\ cy \mid cz \Rightarrow cx \mid cz \Rightarrow x \mid^c z\\
&x \mid^c y,\ x \mid^c z \Rightarrow cx \mid cy,\ cx \mid cz \Rightarrow cx \mid c(y \pm z) \Rightarrow x \mid^c (y \pm z)
\end{aligned}$$

■

The relation $\mid^c$ is a prototype of extensions of $\mid$ with cancellation by c. In fact, from its definition, we can see that, if $0 \nmid c$,

$$\mid \ \text{ has cancellation by } c \Rightarrow \mid^c \subseteq \mid$$

However, in general the converse is not true. To see this, remember that: there is some extension of $\mid$ with cancellation by c, i.e. $\mathcal{C}_c(\ \mid\ ) \neq \emptyset$, if, and only if, $c \notin \sqrt{I(\ \mid\ )}$, by Corollary(2.4.10).

Thus, although $\mid^c$ is an extension of $\mid$, if $0 \mid c^n$ for some natural number $n \in \mathbb{N}$, $\mid^c$ does not have cancellation. Clearly $\mid^c$ contains itself and hence the converse above is not true.

Even not having cancellation by c, we will see that this extension can be used to prove Theorem(3.1.2), which claims that $V_p(\ \mid\ ) \neq \emptyset$, when $\mid$ is a strong p-divisibility.

The extensions $\mid^c$ can also be used to give another proof of $V(\ \mid\ ) \neq \emptyset$, when combined with some ideas about divisibilities with cancellation. However, we do not follow this approach, because it could keep in secret some arguments that we wanted to show and clarify.

The relationship between $\mid^c$ and its corresponding operator $\mathfrak{S}_c$ will be also useful later. What we need is actually:

Lemma 2.5.2 *Let $\mid$ be a divisibility of A and $c \in A$ satisfying $0 \nmid c$. For all $y \in A$ and $X \subseteq A$,*

$$y \in \mathfrak{S}_c(X) \Rightarrow cy \in \mathfrak{S}(c \cdot X)$$

where $\mathfrak{S}_c$ is the ideal operator corresponding to the divisibility $\mid^c$.

Proof : It is enough to prove the lemma for X finite, by Lemma(2.2.4). Taking $X = \{x_1, ..., x_r\}$, we verify that

$$y \in \mathfrak{S}_c^n(x_1, ..., x_r) \Rightarrow cy \in \mathfrak{S}^n(cx_1, ..., cx_r), \tag{2.33}$$

for all $n > 0$.

We proceed by induction on n. For $n = 1$

$$y \in \mathbb{M}_c(x_1, ..., x_r) \Rightarrow \bigvee_{1 \le i \le r} x_i \mid^c y \Rightarrow \bigvee_{1 \le i \le r} cx_i \mid cy \Rightarrow cy \in \mathbb{M}(cx_1, ..., cx_r)$$

Suppose that (2.33) is true for some $n \geq 1$. Then

$$\begin{array}{lcl} y \in \mathbb{M}(\mathfrak{S}(x_1, ..., x_r)) & \Rightarrow & z \mid^c y \text{ and } z \in \mathfrak{S}_c(x_1, ..., x_r) \\ & \overset{Ind.hyp.}{\Rightarrow} & cz \mid cy \text{ and } cz \in \mathfrak{S}(cx_1, ..., cx_r) \\ & \Rightarrow & cy \in \mathfrak{S}(cx_1, ..., cx_r) \\ y \in \sum(\mathfrak{S}(x_1, ..., x_r)) & \Rightarrow & y = \sum_{t=1}^{s} z_t \text{ and } z_t \in \mathfrak{S}_c(x_1, ..., x_r) \\ & \overset{Ind.hyp.}{\Rightarrow} & cy = \sum_{t=1}^{s} cz_t \text{ and } cz_t \in \mathfrak{S}(cx_1, ..., cx_r) \\ & \Rightarrow & cy \in \sum(\mathfrak{S}(cx_1, ..., cx_r)) \end{array}$$

Thus also

$$y \in \mathfrak{S}_c^{n+1}(x_1, ..., x_r) \Rightarrow cy \in \mathfrak{S}^{n+1}(cx_1, ..., cx_r)$$

■

The next proposition is one of the most useful and will be proved after some technical lemmas.

It says that, if $\mathcal{C}_c(\ \mid\ ) \neq \emptyset$, for some $c \in A$, then there is a one to one correspondence between the set of divisibilities of A extending $\mid$ and the set of divisibility of A_c containing the divisibility $\mid_c$ of A_c, which is canonically associated to $\mid$.

Here

$$A_c := \left\{ \frac{a}{c^n} \ : \ a \in A \text{ and } n \in \mathbb{N} \right\}$$

is the localization of A by the multiplicative closed subset

$$\langle c\rangle := \{c^i : i \in \mathbb{N}\}$$

Note that $0 \notin \langle c\rangle$ when $\mathcal{C}_c(\ |\ ) \neq \emptyset$, because of Corollary(2.4.10).

The relation $|_c$ will be defined below in the next Lemma, where we verify that it defines a divisibility of A_c under the assumption $c \notin \sqrt{I(\ |\ )}$.

Lemma 2.5.3 *Let $|$ be a divisibility of A and $c \in A$ with $c \notin \sqrt{I(\ |\ )}$. Then*

$$\left(\frac{a}{c^n}\right) |_c \left(\frac{b}{c^m}\right) :\Leftrightarrow (c^k)(c^m)a \mid (c^k)(c^n)b \quad \textit{for some } k \in \mathbb{N}$$

defines a divisibility of the localization A_c. Moreover, it follows from its definition that, for all $a, b \in A$,

$$a \mid b \Rightarrow \left(\frac{a}{1}\right) |_c \left(\frac{b}{1}\right)$$

Proof : First we prove that $|_c$ is well-defined. Suppose that

$$\left(\frac{a}{c^n}\right) |_c \left(\frac{b}{c^m}\right) \text{ and } \left(\frac{a}{c^n}\right) = \left(\frac{a'}{c^{n'}}\right), \left(\frac{b}{c^m}\right) = \left(\frac{b'}{c^{m'}}\right)$$

i.e., $c^r(c^{n'}a) = c^r(c^n a')$ and $c^s(c^{m'}b) = c^s(c^m b')$ for some $r, s, n, n', n, m' \in \mathbb{N}$ and $a, a', b, b' \in A$. Then,

$$\begin{aligned} a(c^m)(c^k) \mid b(c^n)(c^k) &\Rightarrow (c^k)(c^m)(c^s c^{m'})(c^r c^{n'})a \mid (c^k)(c^n)(c^r c^{n'})(c^s c^{m'})b \\ &\Rightarrow (c^k)(c^m)(c^s c^{m'})(c^r c^n)a' \mid (c^k)(c^n)(c^r c^{n'})(c^s c^m)b' \\ &\Rightarrow a'(c^{m'})(c^{k'}) \mid b'(c^{n'})(c^{k'}) \end{aligned}$$

for $k' := k + m + n + r + s$.

Thus

$$\left(\frac{a'}{c^{n'}}\right) |_c \left(\frac{b'}{c^{m'}}\right)$$

Clearly, by the definition of $|_c$, if $a \mid b$, then $(a/1)\ |_c\ (b/1)$, and hence $|$ is reflexive.

Moreover, if $\dfrac{x}{c^n}, \dfrac{y}{c^m}, \dfrac{z}{c^r} \in A_c$ then

$$\begin{aligned} c^{k+m}x \mid c^{k+n}y &\Rightarrow c^{k+(r+m)}zx \mid c^{k+(r+n)}zy \\ c^{k+m}x \mid c^{k+n}y,\ c^{k'+r}y \mid c^{k'+m}z &\Rightarrow c^{k+m+k'+r}x \mid c^{k+n+k'+r}y \mid c^{k+n+k'+m}z \\ &\Rightarrow c^{(k+m+k')+r}x \mid c^{(k+m+k')+n}z \\ c^{k+m}x \mid c^{k+n}y,\ c^{k'+r}x \mid c^{k'+n}z &\Rightarrow c^{k+m+k'+r}x \mid (c^{k+n+k'+r}y \pm c^{k+m+k'+n}z) \end{aligned}$$

From the first two implications above, we conclude the transitivity and the multiplicative property of $|_c$. The property related to sums follows from the last implication above, if we take $k'' := k' + k$ and observe that

$$\left(\frac{x}{c^n}\right) |_c \left(\frac{y}{c^m} \pm \frac{z}{c^r}\right) \Leftrightarrow \left(\frac{x}{c^n}\right) |_c \left(\frac{yc^r \pm zc^m}{c^{(r+m)}}\right)$$
$$\Leftrightarrow c^{k''+(m+r)}x \mid (c^{k''+(n+r)}y \pm c^{k''+(n+m)}z)$$

where k'' is some natural number.

Also $0 \nmid_c 1$, because

$$\left(\frac{0}{1}\right) |_c \left(\frac{1}{1}\right) \Rightarrow 0 \mid c^k \quad \text{for some} \quad k \in \mathbb{N}$$

■

Remember that we can define the canonical homomorphism $s_c : A \to A_c$ given by $a \mapsto (a/1)$. Using this homomorphism, we can associate a divisibility $(|_*)^{s_c}$ of A to each divisibility $|_*$ of A_c. This is possible because of the next lemma.

Lemma 2.5.4 *Let $\alpha : A \to B$ be a ring homomorphism and $|$ a divisibility of B. Then*

$$(\forall a, b \in A) : \ a \mid^{\alpha} b :\Leftrightarrow \alpha(a) \mid \alpha(b)$$

defines a divisibility on A, inheriting the properties of $|$, i.e., totality, cancellations and p-properties.

Proof : The verification is quite easy and left to the reader.

■

Using the canonical homomorphisms s_c, we can prove then:

Proposition 2.5.5 *Let $|$ be a divisibility of A and $c \in A \backslash \sqrt{I(\ |\ )}$.*

There is a 1-1 correspondence between $\mathcal{C}_c(\ |\ , A)$ and $E(\ |_c, A_c)$ given by[18]

$$|^* \mapsto (\ |^*)_c \quad \textit{and} \quad |^* \mapsto (\ |^*)^{s_c}$$

where $s_c : A \to A_c$ is the canonical homomorphism $a \mapsto (a/1)$.

Proof : If $|^* \supseteq |_c$ is a divisibility on A_c, then $|^*$ has cancellation by c (as well as each divisibility on A_c), and hence $(\ |^*)^{s_c}$ also has cancellation by c. In fact,

$$ca(\ |^*)^{s_c} cb \Rightarrow (ca)/1 \mid^* (cb)/1 \Rightarrow a/1 \mid^* b/1 \Rightarrow a(\ |^*)^{s_c} b$$

[18]This notation was introduced in Notation(2.1.10).

Conversely, if $|^*$ has cancellation by $c \in A$, then $c \notin \sqrt{I(\ |^*\ )}$, and hence Lemma(2.5.3) implies that $(\ |^*)_c$ is a divisibility of A_c extending $|_c$. Thus, the maps defined above are well-defined.

Moreover, for all $x, y \in A$ and $|^* \in \mathcal{C}_c(\ |\ , A)$

$$x\ |^*\ y \Leftrightarrow \left(\frac{x}{1}\right)(\ |^*)_c \left(\frac{y}{1}\right) \Leftrightarrow x((\ |^*)_c)^{s_c} y$$

and, if $|^* \in E(\ |_c, A_c)$, then

$$\left(\frac{x}{c^n}\right)|^* \left(\frac{y}{c^m}\right) \Leftrightarrow \left(\frac{c^m x}{1}\right)|^* \left(\frac{c^n y}{1}\right) \Leftrightarrow c^m x(\ |^*)^{s_c} c^n y \Leftrightarrow \left(\frac{x}{c^n}\right)((\ |^*)^{s_c})_c \left(\frac{y}{c^m}\right)$$

Thus $|^* = ((\ |^*)_c)^{s_c}$ and $|^* = ((\ |^*)^{s_c})_c$, proving that the maps are inverses of each other.

■

2.6 Topologies on $E(A)$

In the last section of this chapter, we study $E(A)$, the set of all divisibilities of A, as a topological space.

We want to introduce not any topology, but a topology that catches also the properties of the topologies defined by the valuations $|^v$ of A in the fields $F(\ |^v) := Quot(A/I(\ |^v))$.

Given a valued field (F, v), the topology defined by the valuation v is generated by the open subbasis consisting of the sets

$$U_F(a, b) := \{x \in F\ :\ v(x - b) > v(a)\}$$

for all $a, b \in F$.[19]

If we understand the valuation as a divisibility relation $|^v$, then we can rewrite the sets above as

$$U_F(a, b) := \{x \in F\ :\ (x - b) \nmid^v a\}$$

This sets can be thought as the correspondent, in the valuation case, to the sets

$$U_R(a, b) := \{x \in R\ :\ (x - b) \not\leq^P a\}$$

in the real case, where R is an ordered field and $\leq^P$ is an order relation in R, defined by an ordering P of R putting

$$(\forall x, y \in R) : x \leq^P y :\Leftrightarrow (y - x) \in P$$

[19] In general, the definition is made for $a \neq 0$, but this is not problematic, because if $a = 0$, then $U_F(a, b) = \emptyset$.

The set $U_R(a,b)$ can also be rewritten as

$$U_R(a,b) := \{x \in R \ : \ a-(x-b) \notin P\}$$

Now look at Chapter(1) and remember that we defined the spectral topology on the set of all orderings of A using an open subbasis consisting of the sets

$$\mathcal{U}_a := \{P \in Sper(A) : a \notin -P\},$$

As the open sets $U_F(a,b)$ and $U_R(a,b)$ seems to be similar in its definition, we can hope that an open subbasis for the set of valuation of F should use a definition also similar to that of $\mathcal{U}_a$. However, here the unary relation $a \notin P$ is replaced by the binary relation $a \mid^v b$.

This motivates our definition.

Definition 2.6.1 *Let $E(A)$ be the set of all divisibilities on A. We define for all $a,b \in A$*

$$\mathcal{U}_a(b) := \mathcal{U}_{a,b}(A) := \{ \mid' \in E(A) \ : \ a \nmid' b\}$$
$$\mathcal{V}_a(b) := \mathcal{V}_{a,b}(A) := \{ \mid' \in E(A) \ : \ a \mid' b\}$$

- *The **spectral topology** on $E(A)$ is the topology generated by the open subbasis $\{\mathcal{U}_a(b)\}_{a,b\in A}$.*
- *The **constructive topology** on $E(A)$ is the topology generated by the open subbasis consisting of the sets $\mathcal{U}_a(b)$ and their complements, for all $a,b \in A$.*

Note that $E(A)\backslash\mathcal{U}_a(b) = \mathcal{V}_a(b)$ for all $a,b \in A$.

Later, we will see that our definition of a topology in the set of valuations is so good as the definition of the real spectral topology in the real case, because we can use it to do a p-adic representation theorem in the coming chapter.

We continue the section establishing the main properties of this topology, as quasi-compactness.

Our proof uses Tychonoff's Theorem and is similar to the proof of the same property for the real spectrum, found in § 2.4, [15].

Theorem 2.6.2 *The constructive topology on $E(A)$ is quasi-compact, and hence also the spectral topology.*

Proof: We endow $\{0,1\}$ with the discrete topology and consider $\{0,1\}^{A\times A}$ with the product topology. Then $\{0,1\}^{A\times A}$ is a quasi-compact space by Tychonoff's Theorem.

We will prove that the well-defined map

$$\begin{aligned}&\Phi : E(A) \to \{0,1\}^{A\times A},\\ &| \mapsto \ (\alpha_{(a,b)}(\ |\ ))_{a,b\in A}, \quad \text{where } \alpha_{(a,b)}(\ |\ ) = \begin{cases} 1 \text{ if } a \mid b \\ 0 \text{ else.}\end{cases}\end{aligned}$$

has a closed image homeomorphic to $E(A)$.

As each closed subspace of a quasi-compact space is quasi-compact, the assertion above is enough to prove the theorem.

If $|\ ,\ |' \in E(A)$ and $|\neq|'$, then there are $a,b\in A$ such that

$$(a \mid b) \wedge (a \nmid' b) \ \text{ or } \ (a \nmid b) \wedge (a \mid' b)$$

and hence

$$\alpha_{(a,b)}(\ |\ ) = 1 \neq 0 = \alpha_{(a,b)}(\ |'\ ) \ \text{ or } \ \alpha_{(a,b)}(\ |\ ) = 0 \neq 1 = \alpha_{(a,b)}(\ |'\ )$$

and therefore $\Phi(\ |\ ) \neq \Phi(\ |'\ )$. This proves that Φ injective and hence Φ is a bijection between $E(A)$ and its image.

Now note that

$$\begin{aligned}| \in \mathcal{U}_a(b) \Leftrightarrow \alpha_{(a,b)}(\ |\ ) = 0 \Leftrightarrow \Phi(\ |\ ) \in \{0\} \times \prod_{(x,y)\neq(a,b)} \{0,1\} =: B_{a,b}\\ | \in \mathcal{V}_a(b) \Leftrightarrow \alpha_{(a,b)}(\ |\ ) = 1 \Leftrightarrow \Phi(\ |\ ) \in \{1\} \times \prod_{(x,y)\neq(a,b)} \{0,1\} =: C_{a,b}\end{aligned}$$

and then

$$\begin{aligned}&\mathcal{U}_a(b) = \Phi^{-1}(B_{a,b}) \ , \ \mathcal{V}_a(b) = \Phi^{-1}(C_{a,b})\\ &\Phi(\mathcal{U}_a(b)) = \Phi(E(A)) \cap B_{a,b} \ , \ \Phi(\mathcal{V}_a(b)) = \Phi(E(A)) \cap C_{a,b}\end{aligned}$$

for all $a,b\in A$.

As the subsets $B_{a,b}, C_{a,b}$ of $\{0,1\}^{A\times A}$ form a subbasis of its topology, when we vary $a,b\in A$, we conclude that Φ is continuous from the first above.

The second proves that Φ is an open map from $E(A)$ to $\Phi(E(A))$. Thus Φ is a homeomorphism of $E(A)$ with its image.

Now we prove that the image of $E(A)$ is closed. Let $\beta := (\beta_{(a,b)})_{a,b\in A} \in \overline{\Phi(E(A))}$ and define

$$a \mid^{\beta} b \ :\Leftrightarrow \ \beta_{(a,b)} = 1.$$

If we verify that $|^{\beta}$ is a divisibility of A, then clearly $\Phi(|^{\beta}) = \beta$ and then $\overline{\Phi(E(A))} = \Phi(E(A))$.

One needs to verify:

1. $\beta_{(0,1)} = 0$.

2. $\beta_{(a,a)} = 1$.

3. $\beta_{(a,b)} = 1 \;\Rightarrow\; \beta_{(ca,cb)} = 1$.

4. $\beta_{(a,b)} = 1$ and $\beta_{(b,c)} = 1 \;\Rightarrow\; \beta_{(a,c)} = 1$.

5. $\beta_{(a,b)} = 1$ and $\beta_{(a,c)} = 1 \;\Rightarrow\; \beta_{(a,b\pm c)} = 1$.

The proof of these properties are more a less the same. For example, suppose that there exists $a, b, c \in A$ such that $\beta_{(a,b)} = \beta_{(a,c)} = 1$ and $\beta_{(a,b+c)} \neq 1\ (= 0)$. Consider the set

$$U = \{\delta \in \{0,1\}^{A\times A} \;:\; \delta_{(a,b)} = \beta_{(a,b)}, \delta_{(a,c)} = \beta_{(a,c)}, \delta_{(a,b+c)} = \beta_{(a,b+c)}\}$$

This is a neighborhood of β in the product topology of $\{0,1\}^{A\times A}$. Thus, by hypothesis, intersects $\Phi(E(A))$. Therefore there is a divisibility $|$ such that $a \mid b$, $a \mid c$ and $a \nmid b + c$. A contradiction.

■

As a corollary we have.

Corollary 2.6.3 *For all $| \in E(A)$ and $a \in A$, the following subsets of $E(A)$ are closed with respect to the constructive topology,*

$$E(\ |\ ),\ T(A),\ \mathcal{C}(A),\ \mathcal{C}_c(A),\ V(A)$$

Therefore they are quasi-compact in the constructive topology, as well as in the spectral topology.

Proof : The lemma follows from the equivalences

$$\begin{aligned}
&|' \in E(\ |\ ) \Leftrightarrow |' \in \bigcap_{(a,b)\in\ |} \mathcal{V}_a(b)\\
&|' \in T(A) \Leftrightarrow |' \in \bigcap_{a,b\in A} (\mathcal{V}_a(b) \cup \mathcal{V}_b(a))\\
&|' \in \mathcal{C}(A) \Leftrightarrow |' \in \bigcap_{a,b,c\in A} (\mathcal{U}_{ac}(bc) \cup \mathcal{V}_a(b) \cup \mathcal{V}_0(c))\\
&|' \in \mathcal{C}_c(A) \Leftrightarrow |' \in \bigcap_{a,b\in A} (\mathcal{U}_{ac}(bc) \cup \mathcal{V}_a(b) \cup \mathcal{V}_0(c))\\
&V(A) = \mathcal{C}(A) \cap T(A)
\end{aligned}$$

■

As in the real case, we expect that the set of maximal points of $E(A)$ is a compact space with respect to the spectral topology.

For us, the maximal divisibilities (the trivial divisibilities) are not so interesting, but the maximal divisibilities of some subset of divisibilities is quite more interesting, like the set of maximal p-divisibilities, which are non-trivial.

The first thing we do is to analyze if the quasi-compactness property of some subspace of $E(A)$ remains when we pass to its maximal points, what is guaranteed by a lemma.

Lemma 2.6.4 *Let X be a closed subset of $E(A)$ with respect to the constructive/spectral topology. Assume also that every element of $|$ has a maximal extension $|^* \in X$. The set $X^{\max}$ of maximal points of X is quasi-compact with respect to the spectral topology.*

Proof : We claim that each open cover of $X^{\max}$ is also an open cover of X. Take some open cover $\{U_i\}_{i\in I}$ of $X^{\max}$. Without loss of generality, we can suppose that each U_i is also open in X. Then

$$U_i = \bigcup_{j\in J_i} (\mathcal{U}_{a_{k_1}}(b_{k_1}) \cap ... \cap \mathcal{U}_{a_{k_j}}(b_{k_j}))$$

for some set of indexes J_i.

To verify that this is an open cover of X it is enough to see that

$$| \subseteq |^* \quad \text{and} \quad |^* \in \mathcal{U}_a(b) \;\Rightarrow\; | \in \mathcal{U}_a(b)$$

for all $|\,, |^* \in X$ and $a, b \in A$. But this is clearly true, because $a \nmid^* b \Rightarrow a \nmid b$ for all $| \subseteq |^*$ and all $a, b \in A$.

Thus $\{U_i\}_{i\in I}$ is an open cover of X and hence also an open cover with respect to its spectral topology. As X is closed in $E(A)$ with respect to this topology, it is also quasi-compact, and therefore has a finite sub-cover. This also provides a finite sub-cover of $X^{\max}$, and hence it is quasi-compact.

■

This was the last general fact about quasi-compactness in $E(A)$ we wanted to show. We pass now to the study of the Hausdorff property.

We want to confirm that also in the divisibility case the set of all maximal divisibilities is compact. This is the content of the next proposition.

After this result, we change to the specific case of p-divisibilities and we analyze the quasi-compactness as well as the Hausdorff property of the set of maximal p-valuations.

What is remarkable here, is that the next proof (for the trivial divisibilities) is less trivial than the proof of the Hausdorff property for p-valuations, which is quite easy.

Proposition 2.6.5 *The spectral topology on $V^{\max}(A)$ is Hausdorff and*

$$\{\mathcal{U}_0(y) \cap V^{\max}(A)\}_{y\in A} \cup \{\mathcal{U}_x(1) \cap V^{\max}(A)\}_{x\in A}$$

is a clopen subbasis of this topology. Moreover, for all $x \in A$,

$$V^{\max}(A)\backslash\mathcal{U}_0(x) = \mathcal{U}_x(1) \cap V^{\max}(A)$$

Proof : Remember that each maximal divisibility is equal to $|^P$ for some prime ideal P of A (Corollary (2.3.8)).

Observe that, for all prime ideal P of A,

$$|^P \in \mathcal{U}_x(y) \;\Leftrightarrow\; x \nmid^P y \;\Leftrightarrow\; x \in P \text{ and } y \notin P. \tag{2.34}$$

In particular

$$|^P \in \mathcal{U}_x(1) \;\Leftrightarrow\; x \in P \quad \text{and} \quad |^P \in \mathcal{U}_0(y) \;\Leftrightarrow\; y \notin P \tag{2.35}$$

and therefore

$$|^P \in \mathcal{U}_x(y) \;\Leftrightarrow |^P \in \mathcal{U}_x(1) \cap \mathcal{U}_0(y) \tag{2.36}$$

Now (2.35) also provides

$$V^{\max}(A)\backslash\mathcal{U}_y(1) = \mathcal{U}_0(y) \cap V^{\max}(A)$$
$$V^{\max}(A)\backslash\mathcal{U}_0(x) = \mathcal{U}_x(1) \cap V^{\max}(A)$$

and hence $\mathcal{U}_x(1) \cap V^{\max}(A)$ and $\mathcal{U}_0(y) \cap V^{\max}(A)$ are clopen in $V^{\max}(A)$.

It follows from (2.36) that $\mathcal{U}_x(y) \cap V^{\max}(A)$ is also clopen in $V^{\max}(A)$ and

$$\{\mathcal{U}_0(y) \cap V^{\max}(A)\}_{y\in A} \cup \{\mathcal{U}_x(1) \cap V^{\max}(A)\}_{x\in A}$$

is a clopen subbasis.

If $|^P \neq |^Q$, then $P \neq Q$. Without loss of generality, we can suppose that $x \in P\backslash Q$, for some $x \in A$. Hence

$$|^P \in \mathcal{U}_x(1) \quad \text{and} \quad |^Q \in \mathcal{U}_0(x)$$

From (2.35) we conclude that

$$\mathcal{U}_x(1) \cap \mathcal{U}_0(x) = \emptyset,$$

proving the Hausdorff property.

■

We are going to finish this chapter proving that the space of all p-valuation of A is compact with respect to the spectral topology. This is different from the real case, because the real spectrum, in general, is not Hausdorff as the maximal real spectrum.

Proposition 2.6.6 *The class* $\{\mathcal{U}_a(b)\}_{a,b\in A}$ *is a clopen subbasis of* $V_p(A)$*, and hence* $V_p(A)$ *is a* ***zero dimensional space***[20]*. Moreover,* $V_p(A)$ *is compact with respect to the spectral topology.*

Proof: We start verifying that the set $\mathcal{U}_a(b)$ is also closed with respect to the spectral topology, for each $a, b \in A$.

In fact, for each $|^v \in V_p(A)$, as $v(p)$ is minimal positive in the value group of the p-valuation function $v : A \to \Gamma_v$ associated to $|^v$,

$$|^v \in \mathcal{U}_a(b) \Leftrightarrow a \nmid^v b \Leftrightarrow v(b) < v(a) \Leftrightarrow v(bp) \leq v(a) \Leftrightarrow bp \mid^v a \Leftrightarrow |^v \in \mathcal{V}_{bp}(a)$$

and hence $\mathcal{U}_a(b)$ is closed.

Now, if $|^v$, $|^w \in V_p(A)$ are different, then there are $a, b \in A$ such that $a \mid^v b$ but $a \nmid^w b$, i.e.,

$$|^v \in \mathcal{V}_a(b) = \mathcal{U}_{pb}(a),\ |^w \in \mathcal{U}_a(b)$$

However,

$$V_p(A) \cap \mathcal{U}_a(b) \cap \mathcal{U}_{pb}(a) = V_p(A) \cap \mathcal{U}_a(b) \cap \mathcal{V}_a(b) = \emptyset$$

and then $V_p(A)$ is also Hausdorff.

It is quasi-compact, because it is closed in $V(A)$ with respect to the constructive topology, because $|^v \in V_p(A)$ if, and only if,

$$|^v \in \bigcap_{a,b\in A} \mathcal{V}_{p[(a^q b - ab^q)^2 - (b^{q+1})^2]}((a^q b - ab^q)b^{q+1}) \cap \bigcap_{c\in A}(\mathcal{U}_{pc}(c) \cup \mathcal{V}_0(c))$$

■

Corollary 2.6.7 *Let* $|$ *be a divisibility on* A*. Then* $V_p(\ |\ )$ *is compact as well as* $V_p^{\max}(\ |\ )$*.*

Proof : $V_p(\ |\ ) = E(\ |\ ) \cap V_p(A)$ is closed in the compact space $V_p(A)$. As $V_p(\ |\ )$ is compact, $V_p^{\max}(\ |\ )$ is also compact by Lemma(2.6.4).

In fact, $V_p(\ |\ )$ satisfies the assumption of that Lemma, because if $|^v \in V_p(\ |\ )$, then each chain of elements of

$$X := \{\ |^* \in V_p(\ |\ ) : |^v \subseteq |^*\ \}$$

has an upper bound in X,[21] and hence we can use Zorn's Lemma to find a maximal extension of $|^v$ belonging to $V_p(\ |\ )$.

■

[20] A topological space is zero dimensional if it has a clopen base.

[21] We just need to use the divisibility $|_I$ of Lemma(2.3.3) and check the conditions $p \nmid_I 1$ and $(0 \nmid_I c) \wedge (ac \mid_I bc) \Rightarrow a \mid_I b$. The details are left to the reader.

Chapter 3

p-adic Representation Theorems

In this last chapter, we will use the concept of p-divisibilities to study representations of commutative rings in rings of p-adic valued continuous functions $C(X, \mathbb{Q}_p)$, for some compact space X.

In the first section, we develop the general theory of extensions of p-divisibilities giving some weak local-global principles. We let the study of p-Archimedean extension for the second section, where we also establish the specific local-global principles of p-Archimedean divisibilities needed for our p-adic Representation Theorem.

The third section is devoted to the study of maximal p-Archimedean divisibilities. There, we will prove Proposition(3.3.2) and Proposition(3.3.3), that assure the existence of p-adic representations for rings having p-Archimedean divisibilities, as Lemma(1.1.5) and Lemma(1.1.12) do in the real case.

In the other sections, we present p-adic representation theorems and we discuss which are the relationships between the algebraic properties of the ring represented and the topological properties of the space used for such representation.

There we will see that it is reasonable to assume that the topological space X, used for representations, is also zero dimensional, as $V_p(A)$ for each commutative ring A, because this hypothesis will guarantee that there are elements of $C(X, \mathbb{Q}_p)$ separating points of X.[1]

In the last section, we discuss the relationship between some subsets of the set of maximal p-Archimedean divisibilities of the ring of polynomials $\mathbb{Q}_p[X_1, ..., X_n]$ and subsets of $\mathbb{Q}_p^n$ satisfying a certain property.

From now on, we will always assume that $p^{-1} \in A$.

[1] This is already true in the real case if X if compact, because Urysohn's Lemma holds.

3.1 p-Extensions and p-Valuations

At the beginning of this section, we want to exhibit sufficient conditions for the existence of p-valuations extending a given p-divisibility.

This is not always true, as seen in Example(2.1.11), where we saw a p-divisibility having no extension being a p-valuation.

Such problems can be avoided if we suppose that the divisibility $|$ is a strong p-divisibility, or if we take some p-Archimedean divisibility, as we will see in the next section.

To do this, we start with a lemma.

Lemma 3.1.1 *Let $|$ be a strong p-divisibility of A.*

- *If $c \notin I(\ |\ )$, then $\ |^c \in E_p^{str}(\ |\ )$.*
- *If $(\ |_i)_{i\in I} \subseteq E_p^{str}(\ |\ )$ is a non-empty chain, then $\ |_I \in E_p^{str}(\ |\ )$.*

Proof : By Lemma(2.5.1), $\ |^c$ is a divisibility and, for all $a \in A$,

$$pa\ |^c\ a \Rightarrow p(ac)\ |\ (ac) \Rightarrow 0\ |\ (ac) \Rightarrow 0\ |^c\ a$$

If $\emptyset \neq (\ |_i)_{i\in I}$ is a chain, then $\ |_I \in E(\ |\ )$, by Lemma(2.3.3). Moreover,

$$pa\ |_I\ a \Rightarrow (\exists i \in I) : pa\ |_i\ a \Rightarrow (\exists i \in I) : 0\ |_i\ a \Rightarrow 0\ |_I\ a,$$

for all $a \in A$.

■

That is all we need to prove the existence of p-valuations extending a strong p-divisibility.

Theorem 3.1.2 *If $|$ is a strong p-divisibility of A, then $V_p(\ |\ ) \neq \emptyset$.*

Proof : As $E_p^{str}(\ |\ ) \neq \emptyset$ and, for each chain $(\ |_i\ )_{i\in I} \subseteq E_p^{str}(\ |\ )$, we have $|_I \in E_p^{str}(\ |\ )$, by Lemma(3.1.1), we can apply Zorn's Lemma. Take then some maximal $\ |^* \in E_p^{str}(\ |\ )$.

Now, by Lemma(3.1.1) again, for all $c \in A\backslash I(\ |^*)$ we also have

$$(\ |^*)^c \in E_p^{str}(\ |^*\ ) \subseteq E_p^{str}(\ |\ )$$

Thus, for all $a, b, c \in A$,

$$(ac\ |^*\ bc) \wedge (0 \not|^*\ c) \Rightarrow a(\ |^*)^c b \Rightarrow a\ |^*\ b$$

by maximality of $\ |^*$, and hence $|^*$ has cancellation.

For the totality of $|^*$, observe that there is a 1-1 correspondence between the divisibility $|^*$ and the ring

$$B(\ |^*) := \left\{ \frac{b + I(\ |^*\ )}{a + I(\ |^*\ )} \in Quot(A/I(\ |^*\ )) : a\ |^*\ b \text{ and } a \notin I(\ |^*\ ) \right\} \subseteq F(\ |^*),$$

by Proposition(2.4.2).

The ring $B(\ |^*)$ also satisfies

$$\frac{1}{p} \notin B(\ |^*) \text{ and } \gamma\left(F(\ |^*\ )\right)) \subseteq B(\ |^*)$$

As in the proof of Theorem(2.3.11), it follows that $F(\ |^*)$ has a p-valuation ring $\mathcal{O}_v$ containing $B(\ |^*)$. Then one verifies that $|^{\mathcal{O}_v}$ is a p-valuation of A extending $|^* \supseteq |$.

■

Another good property of strong p-divisibilities is the existence of some weak local global principles. We call them weak because the conclusion is dependent of some undesirable factor c, which is avoided if the observed just divisibilities having cancellation.

As a first weak local global principle, we have:

Proposition 3.1.3 *Let $|$ be a strong p-divisibility of A and $f, g \in A$. Then*

$$[\forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f] \Rightarrow (\exists c \in A) : (0 \nmid c) \wedge (cf \in \mathfrak{S}(pcf, cg))$$

Proof : Suppose that

$$(\forall c \in A) : cf \in \mathfrak{S}(pcf, cg) \Rightarrow 0 \mid c \tag{3.1}$$

Let

$$X := \{\ |^* \in E_p^{str}(\ |\ ) : |^* \text{ satisfies (3.1)}\}$$

Clearly $X \neq \emptyset$. If $(\ |_i\ )_{i \in I} \subseteq X$ is a chain, then $|_I$ is also a strong p-divisibility, by Lemma(3.1.1), and we also have

$$cf \in \mathfrak{S}_I(pcf, cg) \Leftrightarrow cf \in \mathfrak{S}_i(pfc, cg) \text{ for some } i \in I,$$

by Lemma(2.3.4), and hence

$$cf \in \mathfrak{S}_I(pcf, cg) \Rightarrow 0\ |_i\ c \text{ for some } i \in I \Rightarrow 0\ |_I\ c$$

for all $c \in A$. Therefore, $|_I \in X$.

Using Zorn's Lemma, we can take some maximal element $|^* \in X$. As $E_p^{str}(\ |^*) \subseteq E_p^{str}(\ |\ )$, we can suppose, without loss of generality, that $| = |^*$, i.e., it is maximal in X.

For each $c \in A$, if $0 \nmid c$, then $|^c \in E_p^{str}(\ |\ )$, again by Lemma(3.1.1). We claim that

$$(\forall d \in A) : df \in \mathfrak{S}_c(dpf, dg) \Rightarrow 0 \mid^c d$$

where $\mathfrak{S}_c$ is the operator constructed using the divisibility $|^c$.

In fact, using Lemma(2.5.2), we deduce

$$df \in \mathfrak{S}_c(dpf, dg) \Rightarrow (cd)f \in \mathfrak{S}((cd)pf, (cd)g) \Rightarrow 0 \mid cd \Rightarrow 0 \mid^c d$$

Therefore $| \subseteq |^c \in X$, and then $| = |^c$ by maximality. Thus $|$ has cancellation. Note that, in particular, we have

$$f \notin \mathfrak{S}(pf, g),$$

because of (3.1).

From this and Corollary(2.4.7), we can also infer that

$$\overline{f} \notin p\overline{f}B + \overline{g}B,$$

where $\overline{f} := f + I(\ |\ )$ and $B := B(\ |\ )$ is the subring of $F := F(\ |\ )$ uniquely determined by $|$.

If $\overline{g} = 0$, then $\overline{f}/p\overline{f} \in B$ or $\overline{f} = 0$. As the first case can not happen, because $p^{-1} \notin B$, we have $\overline{f} = 0$.

In this case,

$$f \in \mathfrak{S}(pf, g) = \mathfrak{S}(0) \Rightarrow 0 \mid 1$$

a contradiction.

Thus we can assume that $\overline{g} \neq 0$, and hence

$$\overline{f} \notin p\overline{f}B + \overline{g}B \Rightarrow \frac{\overline{f}}{\overline{g}} \notin \frac{\overline{f}}{\overline{g}}pB + B \Rightarrow \frac{\overline{f}}{\overline{g}} \notin \frac{B}{1+pB}$$

However, as in the theory of p-valuations (functions) of fields developed in [20], from $\gamma(F) \subseteq B$ and $p^{-1} \notin B$, we can deduce that[2]

$$\frac{B}{1+pB} = \bigcap_{\substack{B \subseteq \mathcal{O}_v \subseteq F \\ \mathcal{O}_v \text{ p-val. ring}}} \mathcal{O}_v,$$

[2]In this case, if we change the ring $\mathcal{O}[\gamma(K)]$ by B, in the results appearing in pages 99-115 of [20], then the results obtained by such substitution also hold using similar proofs (sometimes the same) to those found there. In particular, Theorem(6.14) (the Spectral Theorem) holds with $R = \frac{B}{1+pB}$.

and hence $(\overline{f}/\overline{g}) \notin \mathcal{O}_v$, for some p-valuation function of F. Therefore, $g \nmid^v f$ for some $|^v \in V_p(\ |\ )$.

■

With this result, we have a weak characterization of the set of elements of A being infinitesimals for all p-valuations extending a given strong p-divisibility.

Corollary 3.1.4 *Let $|$ be a strong p-divisibility of A. Then, for all $f \in A$,*

$$[\forall\ |^v \in V_p(\ |\ ) : 0\ |^v\ f] \Rightarrow (\exists c \in A) : (0 \nmid c) \wedge (pcf \mid cf)$$

If we assume that $|$ has cancellation, we can deduce a stronger local-global principle, namely

$$[\forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f] \Rightarrow f \in \mathfrak{S}(pf, g)$$

This is a slight generalization of the fact[3] saying that the intersection of all p-valuation rings of a field F, containing a fixed ring $B \subseteq F$, equals

$$B_p := \frac{B}{1 + pB},$$

in case $\gamma(F) \subseteq B$ and $p^{-1} \notin B$.

The theorem below essentially says that, if A/I is a domain for some ideal I of A with $F = Quot(A/I)$, and B a subring of F (which is equivalent to some divisibility of A with cancellation), then the elements of B_p are not just the elements with positive values under each p-valuation of F, but also with positive values under each (Bourbaki) p-valuation $v : A \to \Gamma \cup \{\infty\}$ with $v^{-1}(\infty)$ a $|^B$-convex ideal.

The $|^B$-convex prime ideals P of A are exactly that containing I and satisfying

$$(P + I) \cdot B \subseteq (P + I)$$

because, for all $a, b \in A$,

$$a\ |^B\ b \Leftrightarrow b \in a \cdot B$$

Theorem 3.1.5 *Let $|$ be a p-divisibility of A with cancellation[4] Then, for all $f, g \in A$,*

$$[\forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f] \Leftrightarrow f \in \mathfrak{S}(pf, g) \overset{Cor.(2.4.7)}{\Leftrightarrow} \overline{f} \in p\overline{f}\mathcal{O}(\ |\ ) + \overline{g}\mathcal{O}(\ |\ ),$$

where $\overline{a} := a + I(\ |\ )$ and $\mathcal{O}(\ |\ )$ is the ring correponding to $|$.

[3] Observed in the last footnote.

[4] Therefore it is also a strong p-divisibility.

Proof : Observe the following implications

$$\begin{array}{lll} \forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f & \overset{Prop.(3.1.3)}{\Rightarrow} & cf \in \mathfrak{S}(pcf, cg) \text{ for some } c \in A \text{ with } 0 \nmid c \\ & \overset{Cor.(2.4.7)}{\Rightarrow} & \overline{c} \cdot \overline{f} \in \overline{c} \cdot \overline{pf}\ \mathcal{O}(\ |\ ) + \overline{c} \cdot \overline{g}\ \mathcal{O}(\ |\ ) \text{ with } \overline{c} \neq 0 \\ & \Rightarrow & \overline{f} \in \overline{pf}\ \mathcal{O}(\ |\ ) + \overline{g}\ \mathcal{O}(\ |\ ) \\ & \overset{Cor.(2.4.7)}{\Rightarrow} & f \in \mathfrak{S}(pf, g) \end{array}$$

Note that $\mathcal{O}(\ |\ ) = A/I(\ |\ )$ is an integral domain, because $|$ has cancellation and hence $I(\ |\ )$ is prime.

Moreover,

$$\begin{array}{lll} \overline{f} \in \overline{pf}\ \mathcal{O}(\ |\ ) + \overline{g}\ \mathcal{O}(\ |\ ) & \overset{Cor.(2.4.7)}{\Leftrightarrow} & f \in \mathfrak{S}(pf, g) \\ & \overset{Theo.(B.3)}{\Rightarrow} & \forall\ |^v \in V_p(\ |\ ) : (g\ |^v\ f) \vee (pf\ |^v\ f) \\ & \Rightarrow & \forall\ |^v \in V_p(\ |\ ) : (g\ |^v\ f) \vee (0\ |^v\ f) \\ & \Rightarrow & \forall\ |^v \in V_p(\ |\ ) : (g\ |^v\ f) \end{array}$$

■

Other conclusion can be made if we also assume some stronger hypothesis, as in the next proposition. However, this stronger hypothesis are not so desirable.

In our case this will not be a big problem, because we will focus on p-Archimedean divisibilities, starting in the next section, which have much better local-global principles under more reasonable conditions.

Proposition 3.1.6 *Let $|$ be a strong p-divisibility of A and $f, g \in A$. If $g \mid p^k f$ for some $k \in \mathbb{N}$, then*

$$[\forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f] \Rightarrow (\exists c \in A) : (cg \mid fc) \wedge (0 \nmid c)$$

Proof : If the left side above is true, for some $g, f \in A$, then $cf \in \mathfrak{S}(pcf, cg)$, for some $c \in A$ with $0 \nmid c$, By Proposition(3.1.3).

If also $g \mid p^k f$ for some $k \in \mathbb{N}$, then $cg \mid p^k cf$. If $k = 0$, then $g \mid f$ and the implication above is true. Supposing $k > 0$, we have

$$cf \in \mathfrak{S}(pcf, cg) \Rightarrow p^{k-1}cf \in \mathfrak{S}(p^k cf, p^{k-1}cg) \subseteq \mathfrak{S}(cg)$$

and hence $cg \mid p^{k-1}cf$. Using this argument finitely many times, if necessary, we deduce $cg \mid cf$.

■

Corollary 3.1.7 *Let $|$ be a p-divisibility of A having cancellation and $f, g \in A$. If $g \mid p^k f$ for some $k \in \mathbb{N}$, then*

$$[\forall\ |^v \in V_p(\ |\ ) : g\ |^v\ f] \Rightarrow g \mid f$$

Proof : It is immediate from Proposition(3.1.6).
■

Remark 3.1.8 *In all the results above, we can change the hypothesis*

$$[\forall \ |^v \in V_p(\ |\ ) : g \ |^v \ f]$$

by

$$[\forall \ |^v \in V_p^{\max}(\ |\ ) : fp \nmid^v g],$$

and we obtain the same conclusions, because

$$\begin{aligned}[\forall \ |^v \in V_p^{\max}(\ |\ ) : fp \nmid^v g] &\Rightarrow [\forall \ |^v \in V_p(\ |\ ) : fp \nmid^v g] \\ &\Rightarrow [\forall \ |^v \in V_p(\ |\ ) : gp \ |^v \ pf] \\ &\Rightarrow [\forall \ |^v \in V_p(\ |\ ) : g \ |^v \ f]\end{aligned}$$

3.2 p-Archimedean Divisibilities

We establish here the main results about p-Archimedean divisibilities and discuss them.

p-Archimedean divisibilities have very good properties. For example, we can prove that $V_p(\ |\ ) \neq \emptyset$, if $|$ is a p-Archimedean divisibility, what in general is not true, or need some stronger conditions to holds, like the hypothesis that $|$ is a strong p-divisibility.

They have also better local-global principles under more reasonable conditions than strong p-divisibilities.

This section will be mainly devoted to two problems: to prove the assertion $V_p(\ |\ ) \neq \emptyset$ and to find local-global principles, for a given p-Archimedean divisibility $|$.

We start remembering the definition of a p-Archimedean divisibility.

Definition 3.2.1 *A p-divisibility $|$ of A is p-Archimedean if it satisfies*

$$(\forall a \in A)(\exists n \in \mathbb{N}) : 1 \mid p^n a \tag{3.2}$$

To verify that $V_p(\ |\ )$ is not empty for a p-Archimedean divisibility $|$, we will prove that each p-Archimedean divisibility has an extension $|^*$ being a strong p-divisibility. Thereafter, we can use the fact seen in the last section, saying that $V_p(\ |^*) \neq \emptyset$ when $|^*$ is a strong p-divisibility.

To do this, we need to understand the behavior of the elements $c \in A$ satisfying $cp \mid c$.

If each such c is an infinitesimal with respect to $|$, then we are done, because $|$ is then a strong p-divisibility. However, in general they do not belong to $I(\ |\ )$, but have a property also satisfied by the infinitesimals elements. This is the content of the next lemma.

Lemma 3.2.2 *Let* $|$ *be a p-Archimedean divisibility of A. Then, for all* $c \in A$

$$(cp \mid c) \Rightarrow (\forall a \in A)(\forall n \in \mathbb{N}) : (p^n \mid ac). \tag{3.3}$$

Proof : Let m be minimal such that $1 \mid p^m(ac)$. For all $n \in \mathbb{N}$,

$$p^n \mid p^{n+m}ca \mid \cdots \mid pca \mid ca,$$

because $pc \mid c$.

■

This is enough to prove the next lemma, which will imply the existence of strong p-divisibility extensions of p-Archimedean divisibilities.

Lemma 3.2.3 *Let* $|$ *be a p-Archimedean divisibility of A. If* $cp \mid c$ *for some* $c \in A$*, then* $p \nmid_{0,c} 1$.

Proof : Suppose that $p \mid_{0,c} 1$. Then there are there are $r \in \mathbb{N}^+$ and $c_1, ..., c_r \in A$ satisfying a defining sequence for $p \mid_{0,c} 1$. We can write the last relation as

$$1 \in \mathfrak{S}(p, c_1c, ..., c_rc)$$

If $cp \mid c$, then

$$p \mid cc_i \text{ for all } 1 \leq i \leq r,$$

by Lemma(3.2.2), and hence $1 \in \mathfrak{S}(p) = \mathbb{M}(p)$, a contradiction.

■

Theorem 3.2.4 *If* $|$ *is a p-Archimedean divisibility of A, then*

$$V_p^{\max}(\ |\ ) \neq \emptyset$$

Proof : Define

$$X := \{\ |^* \in E(\ |\ ) : p \nmid^* 1\}$$

This is a non-empty partially ordered set and each element of X is p-Archimedean.

If $\emptyset \neq (\ |_i)_{i \in I} \subseteq X$ is a chain, then $|_I$ is p-Archimedean and $p \nmid_I 1$, because otherwise $p \mid_i 1$ for some $i \in I$. Thus, by Zorn's lemma, we can take some maximal element $|^* \in X$.

By Lemma(3.2.3), if $cp \mid^* c$, then $|^* \subseteq (\ |^*)_{0,c} \in X$, and therefore, by maximality of $|^*$, $(\ |^*)_{0,c} = |^*$, which implies $0 \mid^* c$.

Thus $|^* \in E_p^{str}(\ |\ )$, and hence Theorem(3.1.2) implies $V_p(\ |\ ) \neq \emptyset$.

■

Now we pass to the other goal of this section, the search for local-global principles.

We will prove a local-global principle for a class of p-divisibilities, which are called LG (local-global). An example of a LG p-Archimedean divisibility is the canonical divisibility $|_0$ of C_X.

The first local-global principle is indeed a weak version of what we hope, because it just says that, for each $n \in \mathbb{N}$ and $b \in A$,

$$p^n \mid^v b \text{ for all } \mid^v \in V_p^{\max}(\ |\ ) \Rightarrow p^n \mid b,$$

and in general we want that, for all $a, b \in A$,

$$a \mid^v b \text{ for all } \mid^v \in V_p^{\max}(\ |\ ) \Rightarrow a \mid b.$$

The weak version will serve to classify the elements of the kernel of representations of commutative rings in the ring of p-adic valued continuous functions C_X, with X compact, as well as the set of **totally positive p-adic valued** elements of C_X, i.e.,

$$\mathcal{O}_0 := \{f \in C_X : (\forall x \in X) : f(x) \in \mathbb{Z}_p\}$$

At the end of this section, we also observe another property, also satisfied by the canonical p-divisibility $|_0$ and stronger than the previous one, that guarantees a strong version of the above weak local-global principle for ***p*-bounded pairs** of elements of A (defined later).

We start the work defining an auxiliary function

$$ord_p : A \to \mathbb{Z} \cup \{\infty\}$$

Remember that, when working with p-divisibilities in this text, we will always assume that $p^{-1} \in A$.

Definition 3.2.5 *Let $\mid$ be a p-Archimedean divisibility of A. For all $a \in A$*

$$ord_p(a) := \sup\{n \in \mathbb{Z} : p^n \mid a\} \in \mathbb{Z} \cup \{\infty\}$$

*is the **order of** a **with respect to** p.*

*We say that $\mid$ is **LG (Local-Global)** if*

$$(\forall a \in A)(\forall r \in \mathbb{N}) : ord_p(a^r) = r \cdot ord_p(a) \tag{3.4}$$

If we want to verify this property for some p-Archimedean divisibility $\mid$, it is better to use an easier equivalent sentence, namely

$$(\forall a \in A) : ord_p(a^2) = 2 \cdot ord_p(a) \tag{3.5}$$

The equivalence is confirmed by the following lemma collecting some basic properties of the function ord_p.

Lemma 3.2.6 *Let $|$ be a p-Archimedean divisibility of A. For all $a, b \in A$,*

1. $(\forall a, b \in A) : ord_p(ab) \geq ord_p(a) + ord_p(b)$.
2. $(\forall a \in A)(\forall k \in \mathbb{Z}) : ord_p(ap^k) = k + ord_p(a)$
3. $(\forall a \in A) : ord_p(a^2) = 2 \cdot ord_p(a)$ *if, and only if,* $|$ *is LG.*

Proof : The first is true because, for all $a, b \in A$,

$$p^{ord_p(a)} \mid a \text{ and } p^{ord_p(b)} \mid b \Rightarrow p^{ord_p(a)+ord_p(b)} \mid ab,$$

and, if $ord_p(a) = \infty$ or $ord_p(b) = \infty$, then $p^k \mid ab$ for all $k \in \mathbb{Z}$, and hence $ord_p(ab) = \infty$.

For the second, note that, given $a \in A$ and $k \in \mathbb{Z}$,

$$\begin{array}{l} p^{ord_p(p^k a)} \mid p^k a \Rightarrow p^{ord_p(p^k a)-k} \mid a \Rightarrow ord_p(a) \geq ord_p(p^k a) - k \\ p^{ord_p(a)} \mid a \Rightarrow p^{ord_p(a)+k} \mid p^k a \Rightarrow ord_p(p^k a) \geq ord_p(a) + k \end{array}$$

The third property is actually the only requiring more work. Clearly, only the implication from left to right needs a verification.

Supposing that $ord_p(a^2) = 2 \cdot ord_p(a)$, for all $a \in A$, we can prove the non-trivial implication above using induction on $r \geq 2$.

If $ord_p(a) = \infty$, then clearly $ord_p(a^r) = \infty = r \cdot ord_p(a)$ for all $r \geq 1$. Thus we can restrict our proof to the case $ord_p(a) < \infty$.

The case $r = 2$ was assumed true. Take $r \geq 2$ such that $ord_p(a^k) = k \cdot ord_p(a)$ for all $a \in A$ with $2 \leq k \leq r$.

As $p^{-1} \in A$, $ord_p(a) = s$ if, and only if, $ord_p(ap^k) = s + k$ for all $k \geq 0$. Thus, we can suppose, without loss of generality, that $ord_p(a) > 0$. In this case, by 1., we also have

$$ord_p(a^{r+1}) > ord_p(a^r)$$

If $r + 1$ is odd and $r \geq 2$, then $r + 1 = 2q + 1$ with $q + 1 \leq r$, and hence

$$\begin{array}{rl} (r+1) \cdot ord_p(a) & = ord_p(a^r) + ord_p(a) \\ & \leq ord_p(a^{r+1}) = ord_p(a^{2q+1}) \\ & < ord_p(a^{2(q+1)}) = 2 \cdot ord_p(a^{q+1}) \\ & = 2(q+1) \cdot ord_p(a) = (r+2) \cdot ord_p(a) \end{array}$$

implying that $ord_p(a^{r+1}) = (r + 1) \cdot ord_p(a)$. For $r + 1 = 2q$ follows that

$$ord_p(a^{r+1}) = ord_p(a^{2q}) = 2 \cdot ord_p(a^q) = 2q \cdot ord_p(a) = (r+1) \cdot ord_p(a)$$

■

The main property of LG p-Archimedean divisibilities, needed for the next results, is contained in the next lemma.

Lemma 3.2.7 *If $|$ is a LG p-Archimedean divisibility of A, then*

$$ord_p(a) < \infty,\ p \mid^{a,b} 1 \Rightarrow ord_p(a) > ord_p(b),$$

for all $a, b \in A$.

Proof : Suppose that $p \mid^{a,b} 1$ and $ord_p(a) \leq ord_p(b)$. The last implies

$$p^{ord_p(a)} \mid p^{ord_p(b)} \mid b \ \text{ and } \ p^{ord_p(a)} \mid a$$

Moreover, the first hypothesis implies the existence of $r \in \mathbb{N}$ satisfying

$$a^r \in \mathfrak{S}(p \cdot \{a^i b^{r-i}\}_{0 \leq i \leq r})$$

Thus

$$\begin{array}{ll} a^r \in \mathfrak{S}(p \cdot \{a^i b^{r-i}\}_{0 \leq i \leq r}) & \subseteq \mathfrak{S}(p \cdot \{p^{i \cdot ord_p(a)} p^{(r-i) \cdot ord_p(b)}\}_{0 \leq i \leq r}) \\ & \subseteq \mathfrak{S}(p \cdot \{p^{i \cdot ord_p(a)} p^{(r-i) \cdot ord_p(a)}\}_{0 \leq i \leq r}) \\ & = \mathfrak{S}(p \cdot p^{r \cdot ord_p(a)}) = \mathfrak{S}(p^{r \cdot ord_p(a)+1}), \end{array}$$

and then

$$r \cdot ord_p(a) = ord_p(a^r) \geq r \cdot ord_p(a) + 1 > r \cdot ord_p(a),$$

a contradiction.

■

Herewith, we find a weak local-global principle.

Theorem 3.2.8 (Weak LGP) *Let $|$ be a LG p-Archimedean divisibility of A. For all $f \in A$*

$$[\forall\ |^v \in V_p^{\max}(\ |\ ) : p \mid^v f] \Leftrightarrow p \mid f,$$

and hence, for all $n \in \mathbb{Z}$,

$$[\forall\ |^v \in V_p^{\max}(\ |\ ) : p^n \mid^v f] \Leftrightarrow p^n \mid f$$

Proof : ($\Leftarrow$) : Trivial.
($\Rightarrow$) : We have

$$p \nmid f \Rightarrow ord(f) \leq ord(1) < \infty \overset{Lem.(3.2.7)}{\Rightarrow} p \nmid^{f,1} 1 \Rightarrow \exists\ |^v \in V_p^{\max}(\ |\ ) : f \mid^v 1,$$

and hence $p \nmid^v f$ for such $|^v \in V_p^{\max}(\ |\ )$.

■

One way of getting stronger versions of the theorem above is to suppose stronger conditions for $|$. For example, we say that a p-Archimedean divisibility $|$ is **SLG (strong LG)**[5] if

$$(\forall n, r \in \mathbb{N})(\forall g, f \in A) : (g^r \mid p^n f^r) \wedge (r \neq 0) \Rightarrow g \mid p^{\lfloor n/r \rfloor} f \tag{3.6}$$

where $\lfloor \cdot \rfloor : \mathbb{Q} \to \mathbb{Z}$ is the floor function, i.e., for all $q \in \mathbb{Q}$,

$$\lfloor q \rfloor := \max\{n \in \mathbb{Z} : n \leq q\}$$

Observe that the canonical p-Archimedean divisibility $|_0$ is also SLG p-Archimedean divisibility.

Each SLG p-Archimedean divisibility $|$ satisfies a stronger local-global principle for p-bounded pairs of A, with respect to $|$, which are defined below.

Definition 3.2.9 *Let $|$ be a divisibility of A. An ordered pair $(g, f) \in A \times A$ is called a p-**bounded pair of** A (**with respect to** $|$), if*

$$(\exists k \in \mathbb{N}) : g \mid p^k f,$$

The principle is the following.

Proposition 3.2.10 *Let $|$ be a SLG p-Archimedean divisibility of A. Then*

$$g \mid^v f \quad \textit{for all} \quad \mid^v \in V_p^{\max}(\ \mid\ ) \Rightarrow g \mid f,$$

if (g, f) is p-bounded pair of A.

Proof : We observe two cases: $f \in \sqrt{I(\ \mid\ )}$ and $f \notin \sqrt{I(\ \mid\ )}$.

If $0 \mid f^k$ for some $k \geq 0$, then $g^k \mid f^k$ for all $g \in A$. Thus the SLG property, $g \mid f$ for all $g \in A$.

Take $f \in A \backslash \sqrt{I(\ \mid\ )}$ and $g \in A$ with $g \mid p^k f$. If $k = 0$, then trivially $g \mid f$. Suppose that $k \geq 1$ and k is minimal with the property $g \mid p^k f$.

If $h := gp^{-1}$, then

$$\begin{aligned}
\forall \mid^v \in V_p^{\max}(\ \mid\ ) : hp \mid^v f \quad &\Rightarrow \quad \forall \mid^v \in V_p^{\max}(\ \mid\ ) : f \nmid^v h \\
&\overset{f \notin \sqrt{I(\ \mid\ )}}{\Rightarrow} \quad p \mid^{f,h} 1 \\
&\overset{(p \nmid 1)}{\Rightarrow} \quad \exists r > 0 : f^r \in \mathfrak{S}(p \cdot \{f^i h^{r-i}\}_{0 \leq i \leq r}) \\
&\Rightarrow \quad \exists r > 0 : f^r p^{rk-1} \in \mathfrak{S}(p^{rk} \cdot \{f^i h^{r-i}\}_{0 \leq i \leq r}) \\
&\Rightarrow \quad \exists r > 0 : f^r p^{rk-1} \in \mathfrak{S}(\{(fp^k)^i (hp^k)^{r-i}\}_{0 \leq i \leq r}) \\
&\Rightarrow \quad \exists r > 0 : f^r p^{rk-1} \in \mathfrak{S}(\{(hp)^i (hp^k)^{r-i}\}_{0 \leq i \leq r}) \\
&\Rightarrow \quad \exists r > 0 : f^r p^{rk-1} \in \mathfrak{S}(h^r p^r) \\
&\Rightarrow \quad \exists r > 0 : f^r p^{rk-1} \in \mathfrak{S}(g^r)
\end{aligned}$$

[5]Note that each SLG p-Archimedean divisibility is also a LG p-Archimedean divisibility.

Therefore, $g^r \mid p^{rk-1}f^r$ with $r > 0$, and hence $g \mid p^{\lfloor (rk-1)/r \rfloor} f = p^{k-1}f$, by the SLG property, contradicting the minimal choice of k. Thus $g \mid f$.

■

3.3 Maximal p-Archimedean Divisibilities

The main goal of this section is to prove analogous results to Lemma(1.1.5) and Lemma(1.1.12) in the p-adic case, enabling the formulation of a p-adic representation theorem in the next section.

Given a p-Archimedean divisibility $|$, for each p-valuation $|^v$ extending it, we can define, as in the real case, the canonical projection

$$\alpha_v : A \to A/I(\ |^v),\ a \mapsto \alpha_v(a) := a + I(\ |^v)$$

To write the next results and their proofs, we also use the p-valuation maps $v : A \to \Gamma_v \cup \{\infty\}$ canonically associated to valuations $|^v$ of A.[6]

Lemma 3.3.1 *Let $|$ be a p-Archimedean divisibility of A. For each p-valuation $|^v \in V_p(\ |\ )$, there exists a homomorphism $\rho_v : A \to \mathbb{Q}_p$ such that*

$$a\ |^v\ b\ \Rightarrow\ v_p(\rho_v(a)) \leq v_p(\rho_v(b))$$

Proof : Observe the map $\alpha_v : A \to Quot(A/I(\ |^v)) =: F^v$. From the Archimedean property, we infer that

$$(\forall a \in A)(\exists n_a \in \mathbb{N}) : v(a) \geq -n_a$$

We define

$$\mathcal{O}^v := \{x \in F^v\ :\ v(x) \geq -n\ \text{ for some }\ n \in \mathbb{N}\}.$$

Clearly $\mathcal{O}(\ |^v) \subseteq \mathcal{O}^v \subseteq F^v$, where $\mathcal{O}(\ |^v)$ is the valuation ring of F^v canonically associated to $|^v$ of Definition(2.4.1). Thus $\mathcal{O}^v$ is a valuation ring of F^v. Moreover, by its definition $\alpha_v(A) \subseteq \mathcal{O}^v$ and the maximal ideal of $\mathcal{O}^v$ is

$$\mathcal{M}^v = \{x \in F^v\ :\ v(x) > n\ \text{ for all }\ n \in \mathbb{N}\}.$$

Case 1 : If $\mathcal{M}^v = \{0\}$.

It follows that $v(F^v) = \mathbb{Z}$, because $\mathbb{Z}$ is the minimal convex subgroup of p-valuation functions, and $\mathcal{O}(\ |^v)/\mathcal{M}(\ |^v) = \mathbb{F}_p$, where $\mathcal{M}(\ |^v)$ is the maximal ideal of $\mathcal{O}(\ |^v)$, because it is a p-valuation[7].

[6] The 1-1 correspondence between them was established in Corollary(2.4.3).

[7] A p-valuation of type $(1,1)$ in the nomenclature of [20].

Thus, there is an embedding $i : F^v \hookrightarrow \mathbb{Q}_p$. In fact, for each $f \in F^v$, one can prove that there are $\{a_i\}_{i \geq v(f)}$, with $a_i \in \{0, ..., p-1\}$, such that

$$v\left(f - \sum_{n \geq v(f)}^{m} a_i p^i\right) > m, \text{ for all } m \geq v(f).$$

After identifying F^v with its image, we can see that $\alpha_v : A \to \mathbb{Q}_p$ satisfies

$$a \mid^v b \Leftrightarrow v_p(\alpha_v(a)) \leq v_p(\alpha_v(b)),$$

for all $a, b \in A$.

Case 2 : If $\mathcal{M}^v \neq \{0\}$.

Take the canonical homomorphism $\pi^v : \mathcal{O}^v \to K^v := \mathcal{O}^v/\mathcal{M}^v \supseteq \mathbb{Z}$. Then $\overline{\mathcal{O}(\ |^v)} := \mathcal{O}(\ |^v)/\mathcal{M}^v$ is a p-valuation of K^v, inducing a p-valuation function $\overline{v}$, and satisfying

$$\overline{v}(K^v) = \mathbb{Z} \text{ and } \overline{\mathcal{O}(\ |^v)}/\overline{\mathcal{M}(\ |^v)} \simeq \mathcal{O}_v/\mathcal{M}_v = \mathbb{F}_p$$

Thus, as above, we can identify K^v with a subfield of $\mathbb{Q}_p$, and hence $\rho_v := \pi^v \circ \alpha_v : A \to \mathbb{Q}_p$ is a homomorphism, satisfying

$$a \mid^v b \Rightarrow v_p(\rho_v(a)) \leq v_p(\rho_v(b)),$$

for all $a, b \in A$.

■

The next proposition is the p-adic version of Lemma(1.1.5).

Proposition 3.3.2 *Let $|$ be a p-Archimedean divisibility on A. For each $|^v \in V_p(\ |\ )$,*

$$\alpha_v : A \to \mathbb{Q}_p \text{ with } a \mid^v b \Leftrightarrow v_p(\alpha_v(a)) \leq v_p(\alpha_v(b))$$

if, and only if, $|^v$ is maximal in $V_p(\ |\ )$.

Proof: ($\Leftarrow$) If $|^v$ is maximal, we must have $\mathcal{O}^v = F(\ |^v)$, the ring defined in Lemma(3.3.1), because otherwise, $|^{\mathcal{O}_v}$ defines a proper extension of $|^v = |^{\mathcal{O}(\ |^v)}$. Thus $\mathcal{M}_v = \{0\}$, and hence α_v sends A to $\mathbb{Q}_p$, as above.

Moreover,

$$a \mid^v b \ \Leftrightarrow \ v_p(\alpha_v(a)) \leq v_p(\alpha_v(b)),$$

for all $a, b \in A$, as in last lemma.

($\Rightarrow$) Suppose that $\alpha_v : A \to \mathbb{Q}_p$ and

$$a \mid^v b \;\Leftrightarrow\; v_p(\alpha_v(a)) \leq v_p(\alpha_v(b)) \tag{3.7}$$

for all $a, b \in A$.

Then $F(\mid^v) \subseteq \mathbb{Q}_p$ and

$$\mathcal{O}(\mid^v) = F(\mid^v) \cap \mathbb{Z}_p,$$

Let $\mid^{v'}$ be a maximal p-valuation of A extending $\mid^v$. Then $\alpha_{v'} : A \to F(\mid^{v'}) \subseteq \mathbb{Q}_p$ (because of the implication already proved) with

$$\mathcal{O}(\mid^{v'}) = F(\mid^{v'}) \cap \mathbb{Z}_p,$$

by the same argument as above.

Now, it is enough to show that $I(\mid^v) = I(\mid^{v'})$, because then $F(\mid^v) = F(\mid^{v'})$, and hence $\mathcal{O}(\mid^v) = \mathcal{O}(\mid^{v'})$ implies the equality $\mid^v = \mid^{v'}$.

In fact, if $x \in I(\mid^{v'}) \backslash I(\mid^v)$, then there is $k \in \mathbb{Z}$ with $x \mid^v p^k$, by (3.7). On the other hand, $x \nmid^{v'} p^k$, contradicting $\mid^v \subseteq \mid^{v'}$.

■

Our last result is the continuity of the maps $\widehat{a}$, where

$$\widehat{a} : V_p^{\max}(\ |\ ) \to \mathbb{Q}_p \quad , \quad \widehat{a}(v) := \alpha_v(a),$$

for each $a \in A$.

Proposition 3.3.3 *For each $a \in A$, the map $\widehat{a}$ is continuous.*

Proof: Varying $z \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$, the sets

$$\{x \in \mathbb{Q}_p \;:\; v_p(x - z) > n\}$$

form a subbasis of open sets of the p-adic topology of $\mathbb{Q}_p$.

Thus, it is enough to verify that

$$\widehat{a}^{-1}(\{x \in \mathbb{Q}_p : v_p(x - z) > v_p(p^n)\}) \tag{3.8}$$

is open in $V_p^{\max}(\ |\ )$, for all $z \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$.

However, Lemma(3.3.4) below implies that

$$
\begin{aligned}
(3.8)\quad &= \{\ |^v \in V_p^{\max}(\ |\ ) : v_p(\alpha_v(a)-z) > v_p(p^n)\} \\
&= \bigcup_{\substack{p,q\in\mathbb{Z},\ q\neq 0 \\ v_p(qz-p)>v_p(q(\alpha_v(a)-z))}} \{\ |^v \in V_p^{\max}(\ |\ )\ :\ v_p(\alpha_v(qa-p)) > v_p(p^nq))\} \\
&= \bigcup_{\substack{p,q\in\mathbb{Z},\ q\neq 0 \\ v_p(qz-p)>v_p(q(\alpha_v(a)-z))}} \{\ |^v \in V_p^{\max}(\ |\ )\ :\ (qa-p)\nmid^v (p^nq)\} \\
&= \bigcup_{\substack{p,q\in\mathbb{Z},\ q\neq 0 \\ v_p(qz-p)>v_p(q(\alpha_v(a)-z))}} \mathcal{U}_{(qa-p)}(p^nq) \cap\ V_p^{\max}(\ |\ ),
\end{aligned}
$$

which is open in $V_p^{\max}(\ |\ )$ with respect to the spectral topology.

■

Lemma 3.3.4 *For all $x, z \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$,*

$$v(x-z) > n \ \Leftrightarrow\ v(x-q) > n, \quad \textit{for some}\ \ q \in \mathbb{Q}\ \ \textit{with}\ \ v(z-q) > v(x-z).$$

Proof : ($\Rightarrow$): Suppose $v(x-z) > n$. As $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$, we can find a rational number q such that $v(z-q) > v(x-z)$. Thus

$$v(x-q) = v(x-z+z-q) = v(x-z) > n.$$

($\Leftarrow$): Suppose that there exists some rational number q with $v(z-q) > v(x-z)$ and $v(x-q) > n$. Then

$$n < v(x-q) = v(x-z+z-q) = v(x-z).$$

■

3.4 Representing rings in $C(X, \mathbb{Q}_p)$

In this section we put the pieces together to prove the p-adic representation theorem and a characterization of commutative rings being isomorph to C_X, for some compact X.

At the end of this section, we also discuss how we can rewrite the conditions, used in such characterization, using algebraic sentences instead of a divisibility relation $|$.

From now on, for each topological space X, we will write C_X for the ring of p-adic valued continuous functions defined on X.

We also define, for each $n \in \mathbb{Z}$,

$$\mathcal{O}_n := \{f \in C_X \ : \ p^n \mid_0 f\} = \{f \in C_X \ : \ (\forall x \in X) : f(x) \in p^n \mathbb{Z}_p\},$$

where $\mid_0$ is the **canonical p-divisibility** of C_X given by

$$(\forall g, f \in C_X) : (g \mid_0 f) :\Leftrightarrow [v_p(g(x)) \leq v_p(f(x)) \text{ for all } x \in X]$$

For aesthetic reasons, we will use sometimes a letter d to represent a divisibility relation $\mid$, avoiding subscripts with $\mid$.

Before starting the theorem, we remember some definitions.

Definition 3.4.1 *The p-**adic sup-norm** of C_X is defined by*

$$\|f\| := \sup\{|f(x)|_p \ : \ x \in X\} \tag{3.9}$$

*for each $f \in C_X$, where $|\cdot|_p$ is the p-**adic absolute value** defined by*

$$|\alpha|_p = p^{-v_p(\alpha)}, \tag{3.10}$$

for each $\alpha \in \mathbb{Q}_p$.

If X is compact, $(C_X, \|\cdot\|)$ is a complete normed space.

The p-adic representation theorem is the following collection of claims.

Theorem 3.4.2 (p-adic Representation Theorem) *Let $\mathsf{d} := \mid$ be a LG p-Archimedean divisibility of a commutative ring A containing $\mathbb{Q}$. Define*

$$\mathcal{X}^{\max}_{p,\mathsf{d}}(A) := V^{\max}_p(\ \mid\ ) = Arch^{\max}_p(\ \mid\ )$$

The map $a \mapsto \widehat{a}$, where

$$\widehat{a} : \mathcal{X}^{\max}_{p,\mathsf{d}}(A) \to \mathbb{Q}_p,\ \widehat{a}(\ |^v) = \alpha_v(a)$$

defines a homomorphism $\Phi_{\mathsf{d}} : A \to C_{\mathcal{X}^{\max}_{p,\mathsf{d}}(A)}$ satisfying $\Phi_{\mathsf{d}}(1) = 1$ and

1. $\Phi^{-1}_{\mathsf{d}}(\mathcal{O}_n) = \{a \in A : p^n \mid a\}$, *for all $n \in \mathbb{Z}$.*
2. $\ker(\Phi_{\mathsf{d}}) = \{a \in A : p^n \mid a \ \text{ for all } \ n \in \mathbb{N}\}$.
3. Φ_{d} *is **dominant**, i.e., $\Phi_{\mathsf{d}}(A)$ is dense in $C_{\mathcal{X}^{\max}_{p,\mathsf{d}}(A)}$ with respect to the p-adic sup-norm.*

Proof : By Proposition(3.3.2) and Proposition(3.3.3), the map is well-defined.

The first claim is a consequence of Theorem(3.2.8) and the second of the first, because

$$\ker(\Phi_{\mathsf{d}}) = \bigcap_{n\in\mathbb{Z}} \Phi_{\mathsf{d}}^{-1}(\mathcal{O}_n)$$

To prove the last property, it is enough to see that $\Phi_{\mathsf{d}}(A)$ separates points of $C_{\mathcal{X}_{p,\mathsf{d}}^{\max}(A)}$, because of Corollary(C.4) of the Appendix(C).

Take $|^v, |^w \in \mathcal{X}_{p,\mathsf{d}}^{\max}(A)$ with $|^v \neq |^w$. Thus, there are $a, b \in A$ such that $a \mid^v b$ and $a \nmid^w b$. We claim that $\widehat{a}(\ |^v) \neq \widehat{a}(\ |^w)$ or $\widehat{b}(\ |^v) \neq \widehat{b}(\ |^w)$. In fact, otherwise

$$\begin{array}{rcl} a \mid^v b & \overset{Prop.(3.3.2)}{\Rightarrow} & v_p(\widehat{a}(\ |^v)) \leq v_p(\widehat{b}(\ |^v)) \\ & \Rightarrow & v_p(\widehat{a}(\ |^w)) \leq v_p(\widehat{b}(\ |^w)) \\ & \overset{Prop.(3.3.2)}{\Rightarrow} & a \mid^w b \end{array}$$

Thus, $\widehat{a}$ or $\widehat{b}$ separate the points $|^v$ and $|^w$.

■

Note that this theorem does not characterize the set

$$\Phi_{\mathsf{d}}^{-1}(\ |_0) := \{(g, f) \in A \times A \ : \ \Phi_{\mathsf{d}}(g) \mid_0 \Phi_{\mathsf{d}}(f)\},$$

because LG p-Archimedean divisibilities have just a weak local-global principle, but this was enough to describe the kernel of Φ_{d}.

We search now for a "characterization" of commutative rings A, containing $\mathbb{Q}$, and isomorph to $C(X, \mathbb{Q}_p)$, for some compact space X, as did Stone in his papers [24] and [25]

In Stone's papers, he associated a map $\|\cdot\|_T : A \to \mathbb{R}$ to a given Archimedean preordering T of a ring A. In the p-adic case, given a p-Archimedean divisibility $\mathsf{d} := |$ of A, we define map $\|\cdot\|_{\mathsf{d}} : A \to \mathbb{R}$ putting

$$(\forall a \in A) : \|a\|_{\mathsf{d}} := p^{-ord_p(a)}, \tag{3.11}$$

where $ord_p(a)$ is the map of Definition(3.2.5) and, by definition, $p^{-\infty} := 0$.

Using the properties of $ord_p(\cdot)$, we prove in the next proposition that $\|\cdot\|_{\mathsf{d}}$ is a sub-multiplicative non-Archimedean semi-norm, with respect to the p-adic absolute value.

Definition 3.4.3 *A non-Archimedean semi-norm $\|\cdot\|$ of a $\mathbb{Q}$-vector space A is a real valued function satisfying, for all $a, b \in A$ and $q \in \mathbb{Q}$,*

1. $\|a\| \geq 0$

2. $\|q \cdot a\| = |q| \cdot \|a\|$

3. $\|a + b\| \leq \max\{\|a\|, \|b\|\}$

where $|\cdot|$ *is an ultrametric absolute value on* $\mathbb{Q}$.

It is called a norm if $\|a\| = 0$ *implies* $a = 0$.

In our case, we will always take $|\cdot|$ as the p-adic absolute value $|\cdot|_p$, defined in (3.10).

To assure the validity of the second condition of semi-norms for $\|\cdot\|_{\mathsf{d}}$ and the p-adic absolute value $|\cdot|_p$, we need the next lemma.

Lemma 3.4.4 *Let* $\mid$ *be a p-Archimedean divisibility of* $\mathbb{Q}$. *Then*

$$(\forall a, b \in \mathbb{Q}) : a \mid b \Leftrightarrow v_p(a) \leq v_p(b) \Leftrightarrow |a|_p \geq |b|_p$$

Thus $|^{v_p}$ *is the unique p-Archimedean divisibility of* $\mathbb{Q}$.

Proof : Clearly each $n \in \mathbb{Z}$ satisfies $1 \mid n$. As $\mid$ is p-Archimedean, for each $n \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$, we can find $m \in \mathbb{N}$ such that

$$p^{-m} \mid \left(\frac{1}{n}\right),$$

and hence $n \mid p^m$ for some $m \in \mathbb{N}$.

Moreover,

$$(\forall n \in \mathbb{Z}) : \gcd(n, p) = 1 \Rightarrow n \mid 1 \tag{3.12}$$

In fact, if $\gcd(n, p) = 1$, then $n \neq 0$ and there are $k, l \in \mathbb{Z}$ such that

$$1 = kp^m + nl,$$

by the reasoning above, and hence

$$n \mid kp^m \ , \ n \mid nl \Rightarrow n \mid (kp^m + nl) = 1$$

As $\mid$ has cancellation and $I(\ \mid\ ) = \{0\}$ (as every divisibility of a field), this divisibility is totally determined by[8] $\mathcal{O}(\ \mid\ ) \subseteq \mathbb{Q}$.

Observe now that (3.12) implies that

$$\mathbb{Z}_{(p)} = \left\{\frac{z}{n} : z, n \in \mathbb{Z} \text{ and } \gcd(n, p) = 1\right\} \subseteq \mathcal{O}(\ \mid\ ),$$

where $\mathbb{Z}_{(p)}$ is the unique p-valuation ring of $\mathbb{Q}$.

It follows that $\mathcal{O}(\ \mid\ )$ is also a p-valuation, and therefore $\mathcal{O}(\ \mid\ ) = \mathbb{Z}_{(p)}$, implying the desired equivalence.

■

[8]Remember Proposition(2.4.2).

Proposition 3.4.5 *Suppose that* $\mathsf{d} := |$ *is a p-Archimedean divisibility of a commutative ring A containing* $\mathbb{Q}$*. Then* $\|\cdot\|_{\mathsf{d}}$ *is a sub-multiplicative non-Archimedean semi-norm of the* $\mathbb{Q}$*-algebra A.*

Proof : Clearly $\|a\|_{\mathsf{d}} \geq 0$ for all $a \in A$. Let us verify condition 2.

For $r, s \in \mathbb{Z}$ with $s \neq 0$, we can write

$$\frac{r}{s} = \left(\frac{r'}{s'}\right) \cdot p^{v_p(r/s)} \quad \text{with} \quad v_p(s') = v_p(r') = 0,$$

and then $s' \mid r'$ and $r' \mid s'$, by Lemma(3.4.4).

Thus

$$(\forall a \in A)(\forall n \in \mathbb{N}) : (p^n \mid a \Leftrightarrow p^n s' \mid ar')$$

and hence

$$(\forall a \in A) : ord_p(a \cdot (r'/s')) = ord_p(a)$$

Therefore

$$\begin{array}{rcl} \left\|a \cdot \left(\frac{r}{s}\right)\right\|_{\mathsf{d}} & = & p^{-ord_p(a\cdot(r/s))} \\ & = & p^{-ord_p\left(ap^{v_p(r/s)}\cdot(r'/s')\right)} \\ & = & p^{-ord_p\left(ap^{v_p(r/s)}\right)} \\ & \overset{Lem.(3.2.6)}{=} & p^{-ord_p(a)-v_p(r/s)} = \left|\frac{r}{s}\right|_p \cdot \|a\|_{\mathsf{d}} \end{array}$$

For 3., observe that

$$\inf\{\sup\{n \ : \ p^n \mid a\}, \sup\{n \ : \ p^n \mid b\}\} \leq \sup\{n \ : \ p^n \mid a+b\} = ord_p(a+b)$$

for all $a, b \in A$, and hence

$$\begin{array}{rl} \|a+b\|_{\mathsf{d}} = p^{-ord_p(a+b)} & \leq p^{-\inf\{ord_p(a), ord_p(b)\}} \\ & = p^{\sup\{-ord_p(a), -ord_p(b)\}} = \max\{\|a\|_{\mathsf{d}}, \|b|_{\mathsf{d}}\} \end{array}$$

Finally,

$$\begin{array}{rcl} \|a \cdot b\|_{\mathsf{d}} & = & p^{-ord_p(ab)} \\ & \overset{Lem.(3.2.6)}{\leq} & p^{-(ord_p(a)+ord_p(b))} \\ & = & \|a\|_{\mathsf{d}} \cdot \|b\|_{\mathsf{d}} \end{array}$$

■

When | is LG, we can even prove the following lemma, relating $\|\cdot\|_{\mathsf{d}}$ and the p-adic sup-norm $\|\cdot\|$, used to analyze the surjectivity of Φ_{d}.

Lemma 3.4.6 *Let* $\mathsf{d} := |$ *be a LG p-Archimedean divisibility of A. Then*

$$(\forall a \in A) : \|\Phi_{\mathsf{d}}(a)\| = \|a\|_{\mathsf{d}}$$

Proof : Using the same notations of the p-adic Representation Theorem, by the weak LGP [9] and Proposition(3.3.2), we have

$$[(\forall x \in \mathcal{X}_{p,\mathsf{d}}^{\max}(A)) : v_p(\Phi_{\mathsf{d}}(a)(x)) \geq n] \Leftrightarrow p^n \mid a$$

for all $a \in A$ and $n \in \mathbb{Z}$.

Therefore,

$$\|\Phi_{\mathsf{d}}(a)\| = p^{-\sup\{n\in\mathbb{Z} \,:\, v_p(\Phi_{\mathsf{d}}(a)(x))\geq n\}} = p^{-ord_p(a)} = \|a\|_{\mathsf{d}}$$

■

As a corollary, we see that the injectivity of Φ_{d} implies that $\|\cdot\|_{\mathsf{d}}$ is indeed a non-Archimedean norm, because

$$\|a\|_{\mathsf{d}} = 0 \Leftrightarrow \|\Phi_{\mathsf{d}}(a)\| = 0 \Leftrightarrow \Phi_{\mathsf{d}}(a) = 0 \Leftrightarrow a = 0$$

We can say also:

Lemma 3.4.7 *Let* $\mathsf{d} := |$ *be a LG p-Archimedean divisibility of A, where* $\mathbb{Q} \subseteq A$. *If* $(A, \|\cdot\|_{\mathsf{d}})$ *is a complete normed* $\mathbb{Q}$*-algebra, then* Φ_{d} *is surjective.*

Proof : It is enough to verify that $\Phi_{\mathsf{d}}(A)$ is closed in $C := C_{\mathcal{X}_{p,\mathsf{d}}^{\max}(A)}$ when $(A, \|\cdot\|)$ is complete, because $\Phi_{\mathsf{d}}(A)$ is dense in C.

Let $(\Phi_{\mathsf{d}}(f_n))_{n\in\mathbb{N}}$ be a sequence in $\Phi_{\mathsf{d}}(A)$ converging to some $g \in C$. In particular it is a Cauchy sequence in C, and therefore $(f_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in A, because of Lemma(3.4.6).

As $(A, \|\cdot\|)$ is complete, there is $f \in A$ such that $f_n \to f$. Moreover

$$\begin{array}{rcl} \lim f_n = f & \Rightarrow & (\forall N \in \mathbb{N})(\exists k \in \mathbb{N}) : \|f_n - f\|_{\mathsf{d}} < p^{-N} \\ & \overset{Lem.(3.4.6)}{\Rightarrow} & (\forall N \in \mathbb{N})(\exists k \in \mathbb{N}) : \|\Phi_{\mathsf{d}}(f_n) - \Phi_{\mathsf{d}}(f)\| < p^{-N} \\ & \Rightarrow & \lim \Phi_{\mathsf{d}}(f_n) = \Phi_{\mathsf{d}}(f) \\ & \Rightarrow & \Phi_{\mathsf{d}}(f) = g \end{array}$$

Thus $g \in \Phi_{\mathsf{d}}(A)$, and hence $\Phi(A)$ is closed in C.

■

Collecting the facts until here, we have the theorem.

[9] Theorem(3.2.8).

Theorem 3.4.8 (p-adic Characterization Theorem) *Let A be a commutative ring containing $\mathbb{Q}$. There is an isomorphism $\Phi : A \to C_X$ for some compact space X if, and only if, there is a divisibility $\mathsf{d} := |$ of A satisfying:*

1. $|$ *is a p-divisibility;*
2. $|$ *is p-Archimedean;*
3. $(\forall a \in A) : ord_p(a^2) = 2 \cdot ord_p(a)$;
4. $(\forall a \in A)[(\forall n \in \mathbb{N}) : p^n \mid a] \Rightarrow a = 0$;
5. $(A, \|\cdot\|_{\mathsf{d}})$ *is a complete normed space, where* $\|a\|_{\mathsf{d}} := p^{-ord_p(a)}$ *for all* $a \in A$.

Proof : If there is some divisibility $|$ of A satisfying $1 - 5$, taking $X := \mathcal{X}^{\max}_{p,\mathsf{d}}(A)$, the homomorphism $\Phi_{\mathsf{d}} : A \to C_X$ is an isomorphism, because of Lemma(3.4.7) and the p-adic Representation Theorem.

Conversely, suppose that $\Phi : A \to C_X$ is an isomorphism for some compact space X. The canonical divisibility $|_0$ induces a divisibility of A via Φ, putting

$$a \mid^{\Phi} b :\Leftrightarrow \Phi(a) \mid_0 \Phi(b).$$

for all $a, b \in A$.

Then $\mathsf{d}_\Phi := |^\Phi$ is p-Archimedean divisibility of A, by the quasi-compactness of X. It also satisfies 3. and 4., because Φ is injective and

$$p^n \mid^{\Phi} a \Leftrightarrow p^n \mid_0 \Phi(a),$$

for all $n \in \mathbb{N}$ and $a \in A$.

This equivalence also implies

$$[(\forall x \in X) : v_p(\Phi_{\mathsf{d}}(a)(x)) \geq n] \Leftrightarrow p^n \mid^{\Phi} a,$$

and hence $\|a\|_{\mathsf{d}_\Phi} = \|\Phi(a)\|$ for all $a \in A$, by the same argument used in the proof of Lemma(3.4.6).

Using this equality and the surjectivity of Φ, we see that $(A, \|a\|_{\mathsf{d}_\Phi})$ is complete. In fact, each Cauchy sequence $(f_n)_{n\in\mathbb{N}}$ defines a Cauchy sequence $\Phi(f_n)_{n\in\mathbb{N}}$ in C_X converging to some $g = \Phi(f)$, with $f \in A$. Thus clearly $\lim f_n = f$.

■

The last thing we want to discuss in this section, is how we can rewrite the conditions of the p-adic Characterization Theorem using algebraic sentences instead of the relation $|$.

In the real case this can be done, because

$$f \in T_0 \Leftrightarrow (\exists h \in C(X, \mathbb{R})) : (f = h^2),$$

where T_0 is the canonical preorder of $C(X, \mathbb{R})$.

Therefore, all condition, inclusive the definition of $\| \cdot \|_0$ and the claim that T_0 is a preorder, can be done using the algebraic sentence of the right side above.

In the p-adic case, we also do this kind of algebraic translation for the canonical p-divisibility $|_0$ of C_X, first for the case $p \neq 2$ and later for $p = 2$.

We need here the following version of Hensel's Lemma.

Lemma 3.4.9 (Hensel's Lemma) *Let $(F, \mathcal{O})$ be a henselian valued field. Given $f \in \mathcal{O}[X]$, for all $a \in \mathcal{O}$*

$$(f(\overline{a}) = 0) \wedge (f'(\overline{a}) \neq 0) \Rightarrow (\exists \alpha \in \mathcal{O}) : (f(\alpha) = 0) \wedge (\overline{\alpha} = \overline{a}),$$

where $\overline{a} \in \overline{F}$ is the class of a in the residue field $\overline{F}$.[10]

As $(\mathbb{Q}_p, \mathbb{Z}_p)$ is a henselian valued field, we can use Hensel's Lemma for the next Lemmas.

Lemma 3.4.10 *Let X be a topological space, $C := C_X$ the ring of p-adic valued continuous functions defined on X and $|_0$ its canonical divisibility. Suppose that $\mathbb{Q} \subseteq C$ and $p \neq 2$. For all $g, f \in C$*

$$g \mid_0 f \Leftrightarrow (\exists h \in C) : h^2 = g^2 + pf^2$$

Proof : $(\Leftarrow)$: Suppose that $g^2 + pf^2 = h^2$ for some $h \in C$.

If $g(x) = 0$ for some $x \in X$, then $1 + 2v_p(f(x)) = 2v_p(h(x))$, and hence $f(x) = 0$.

If $g(x) \neq 0$, for $x \in X$, then

$$\begin{aligned}
v_p(f(x)) < v_p(g(x)) \quad & \Rightarrow v_p(pf(x)) \leq v_p(g(x)) \\
& \Rightarrow v_p(pf(x)^2) < v_p(p^2 f(x)^2) \leq v_p(g(x)^2) \\
& \Rightarrow v_p\left(p(\tfrac{f(x)}{g(x)})^2\right) < 0 \\
& \Rightarrow v_p\left(p(\tfrac{f(x)}{g(x)})^2 + 1\right) < 0 \\
& \Rightarrow 2v_p\left(\tfrac{h(x)}{g(x)}\right) = v_p\left(p\left(\tfrac{f(x)}{g(x)}\right)^2 + 1\right) = 1 + 2v_p\left(\tfrac{f(x)}{g(x)}\right) \\
& \Rightarrow v_p\left(\tfrac{h(x)}{g(x)}\right) - v_p\left(\tfrac{f(x)}{g(x)}\right) = \frac{1}{2},
\end{aligned}$$

[10] See references of valuation theory, as [19].

what is impossible. Thus, $v_p(g(x)) \leq v_p(f(x))$.

Therefore, $v_p(g(x)) \leq v_p(f(x))$ for all $x \in X$, i.e., $g \mid_0 f$.

($\Rightarrow$) : Suppose that $g \mid_0 f$, i.e., $v_p(g(x)) \leq v_p(f(x))$ for all $x \in X$. For each $n \in \mathbb{Z}$ take

$$\begin{array}{l} X_n := g^{-1}(\mathbb{Z}_{p^n} \backslash \mathbb{Z}_{p^{n+1}}) = \{x \in X : v_p(g(x)) = n\} \\ N_g := \{n \in \mathbb{Z} : v_p(g(x)) = n \text{ for some } x \in X\} \\ g_n := g \cdot p^{-n} \text{ and } f_n := f \cdot p^{-n}, \text{ for all } n \in N_g \end{array}$$

Thus, $g_n(x) \in \mathbb{Z}_p^{\times}$ and $f_n(x) \in \mathbb{Z}_p$, for all $x \in X_n$. Define

$$P_{n,x}(Y) := Y^2 - F_n(x) \in \mathbb{Z}_p[Y], \ F_n := g_n^2 + pf_n^2 \in C,$$

for each $x \in X_n$.

As

$$\begin{array}{ll} P_{n,x}(\overline{g_n(x)}) & = \overline{g_n(x)^2 - g_n(x)^2 - pf_n(x)^2} = \overline{0} \\ P'_{n,x}(\overline{g_n(x)}) & = \overline{2 \cdot g_n(x)} \neq \overline{0} \end{array}$$

there is an unique $h_n(x) \in \mathbb{Z}_p$ such that

$$P_{n,x}(h_n(x)) = 0 \text{ and } \overline{h_n(x)} = \overline{g_n(x)},$$

by Hensel's Lemma.

In particular, $v_p(h_n(x) + h_n(y)) = 0$ for all $x, y \in X_n$. In fact, otherwise,

$$\overline{0} = \overline{h_n(x) + h_n(y)} = \overline{h_n(x)} + \overline{h_n(y)} = \overline{g_n(x)} + \overline{g_n(y)} = \overline{1} + \overline{1},$$

contradicting the assumption $p \neq 2$.

Therefore, for all $x, y \in X_n$ and all $m \in \mathbb{Z}$,

$$\begin{array}{ll} v_p(F_n(x) - F_n(y)) > m & \Leftrightarrow v_p(h_n^2(x) - h_n^2(y)) > m \\ & \Leftrightarrow v_p(h_n(x) - h_n(y)) + v_p(h_n(y) + h_n(x)) > m \\ & \Leftrightarrow v_p(h_n(x) - h_n(y)) > m \end{array}$$

Thus, if

$$B_m(\beta) = \{\alpha \in \mathbb{Q}_p : v_p(\alpha - \beta) > m\},$$

then

$$h_n^{-1}(B_m(h_n(x_0))) = F_n^{-1}(B_m(F_n(x_0)))$$

is open in X_n, for each $x_0 \in X_n$, because F_n is continuous.

As $\{B_m(h_n(x_0))\}_{x_0 \in X_n}$ is a subbasis of induced p-adic topology on $h_n(X_n)$, we conclude that h_n is continuous in X_n.

Thus, the functions $h_n : X_n \to \mathbb{Q}_p$ are continuous on X_n for each $n \in N_g$. Define, for each $x \in X$,

$$h(x) := r_n(x) := p^n \cdot h_n(x), \quad \text{if } x \in X_n,$$

This is a well-defined function on X, because X is the disjunct union of the X_n's, with $n \in N_g$. Moreover, h is continuous, because

$$h^{-1}(U) = \bigcup_{n \in N_g} r_n^{-1}(U)$$

is open for each open subset $U \subseteq \mathbb{Q}_p$.

In fact, as $\mathbb{Z}_{p^n} \backslash \mathbb{Z}_{p^{n+1}}$ is (cl)open in $\mathbb{Q}_p$, $X_n = g^{-1}(\mathbb{Z}_{p^n} \backslash \mathbb{Z}_{p^{n+1}})$ is open in X, and then each open subset of X_n is also open in X.

Finally, note that h satisfies $h^2 = g^2 + pf^2$, because

$$h(x)^2 = h_n(x)^2 \cdot p^{2n} = (g_n(x)^2 + pf_n(x)^2)p^{2n} = g(x)^2 + pf(x)^2$$

■

We prove a similar result for $p = 2$.

Lemma 3.4.11 *Let X be a topological space, $C := C_X$ the ring of 2-adic valued continuous functions defined on X and $|_0$ its canonical divisibility. Suppose that $\mathbb{Q} \subseteq C$. For all $g, f \in C$*

$$g \mid_0 f \Leftrightarrow (\exists h \in C) : h^3 = g^3 + 2f^3$$

Proof : ($\Leftarrow$) : Just change the powers 2 by 3 in the corresponding proof above.

($\Rightarrow$) : We proceed as in the case $p \neq 2$, but now, we define

$$P_{n,x}(Y) := Y^3 - F_n(x) \in \mathbb{Z}_p[Y], \; F_n := g_n^3 + 2f_n^3 \in C$$

As above, we have $v_p(g_n(x)) = 0$, for all $x \in X_n$, and also

$$\begin{aligned} P_{n,x}(\overline{g_n(x)}) &= \overline{g_n(x)^3 - g_n(x)^3 - 2f_n(x)^3} = \overline{0} \\ P'_{n,x}(\overline{g_n(x)}) &= \overline{3 \cdot g_n(x)} \neq \overline{0} \end{aligned}$$

Hensel's Lemma implies then the existence of an unique $h_n(x) \in \mathbb{Z}_p$ such that $P_{n,x}(h_n(x)) = 0$ and $\overline{h_n(x)} = \overline{g_n(x)}$, for all $x \in X_n$.

From this follows that

$$v_p(h_n(x) + h_n(x)h_n(y) + h_n(y)) = 0$$

for all $x, y \in X_n$, because otherwise

$$\begin{aligned}\overline{0} &= \overline{h_n(x) + h_n(x)h_n(y) + h_n(y)} \\ &= \overline{h_n(x)} + \overline{h_n(x)} \cdot \overline{h_n(y)} + \overline{h_n(y)} \\ &= \overline{g_n(x)} + \overline{g_n(x)} \cdot \overline{g_n(y)} + \overline{g_n(y)} \\ &= \overline{1} + \overline{1} \cdot \overline{1} + \overline{1} = \overline{1},\end{aligned}$$

a contradiction.

Therefore, for all $x, y \in X_n$ and all $m \in \mathbb{Z}$,

$$\begin{aligned}v_p(F_n(x) - F_n(y)) > m \quad &\Leftrightarrow \quad v_p(h_n^3(x) - h_n^3(y)) > m \\ &\Leftrightarrow \quad v_p(h_n(x) - h_n(y)) + \\ &\qquad v_p(h_n(x) + h_n(x) \cdot h_n(y) + h_n(y)) > m \\ &\Leftrightarrow \quad v_p(h_n(x) - h_n(y)) > m\end{aligned}$$

Now, using this equivalence, we can find $h \in C_X$ such that $h^3 = g^3 + 2f^3$. The construction of such h is analogous to that given in the proof of the case $p \neq 2$. We just need to change the powers 2 by 3.

■

Using these two lemma we can rewrite the conditions of the p-adic Characterization Theorem, substituting the relation $|$ by an algebraic sentence.

Instead of writing down all the relations again, we just change the arbitrary relation $|$ by one of the following relations, defined by the equivalences

$$a \mid^2 b :\Leftrightarrow (\exists x \in A) : x^2 = a^2 + pb^2 \quad \text{and} \quad a \mid^3 b :\Leftrightarrow (\exists x \in A) : x^3 = a^3 + 2b^3$$

for all $a, b \in A$ and $p \neq 2$.

The next theorem closes the discussion of this section.

Theorem 3.4.12 *Let A be a commutative ring containing $\mathbb{Q}$. Then*

- *For $p \neq 2$. A is isomorph to $C(X, \mathbb{Q}_p)$ for some Hausdorff compact topological space X if, and only if, $|^2$ defines a divisibility of A satisfying $(1-5)$ from Theorem(3.4.8).*
- *For $p = 2$. A is isomorph to $C(X, \mathbb{Q}_p)$ for some Hausdorff compact topological space X if, and only if, $|^3$ defines a divisibility of A satisfying $(1-5)$ from Theorem(3.4.8).*

Proof : If $\varphi : A \to C := C(X, \mathbb{Q}_p)$ is an isomorphism and $|_0$ is the canonical divisibility on C, then $|_0^{\varphi}$ is a divisibility[11] of A satisfying $(1-5)$

[11]The definition of $|_0^{\varphi}$ is the same of Lemma(2.5.4).

of Theorem(3.4.8). Moreover, as φ is an isomorphism, by Lemma(3.4.10),

$$\begin{array}{rcl} a \mid_0^{\varphi} b & \Leftrightarrow & \varphi(a) \mid_0 \varphi(b) \\ & \overset{\text{surjec.}}{\Leftrightarrow} & \exists x \in A : \varphi(x)^2 = \varphi(a)^2 + p\varphi(b)^2 \\ & \overset{\text{Injec.}}{\Leftrightarrow} & \exists x \in A : x^2 = a^2 + pb^2 \\ & \Leftrightarrow & a \mid^2 b \end{array}$$

for each $p \neq 2$, and hence, in this case $|_0^{\varphi} = |^2$. Thus $|^2$ is a divisibility of A satisfying the conditions of Theorem(3.4.8).

For $p = 2$ the reasoning is similar, and we conclude that $|_0^{\varphi} = |^3$, using Lemma(3.4.11).

Conversely, if $|^2$ (resp. $|^3$) is a divisibility satisfying the conditions (1-5), then Theorem(3.4.8) assures the existence of a such isomorphism.

■

3.5 Algebraic Properties of $C(X, \mathbb{Q}_p)$ x Topological Properties of X

For a commutative ring A containing $\mathbb{Q}$, we ask:

When is A in $C(X, \mathbb{Q}_p)$ representable, for some compact space X?

The answer we found is:

If A admits a p-Archimedean divisibility.

In fact, if $\Phi : A \to C_X$ is a representation, with X compact, then $|_0$ is a p-Archimedean divisibility of C_X, and hence $(|_0)^{\Phi}$ is also a p-Archimedean divisibility of A, where $(|_0)^{\Phi}$ is the divisibility of A induced by $|_0$ and Φ .

The converse is assured by Proposition(3.3.2), Proposition(3.3.3) and Corollary(2.6.7), when taking $X := V_p^{\max}(\mid)$.

If we define the **$\mathbb{Q}_p$-spectrum of** A as

$$X_{\mathbb{Q}_p}(A) := \{\alpha : A \to \mathbb{Q}_p \ : \ \alpha \text{ is a homomorphism and } \alpha(1) = 1\},$$

as in Chapter(1), we can also solve the problem above in terms of $X_{\mathbb{Q}_p}(A)$.

Theorem 3.5.1 *Let A be a commutative ring. There is a representation $\Phi : A \to C_X$, for some compact space X, if, and only if, $X_{\mathbb{Q}_p(A)} \neq \emptyset$.*

If $\alpha \in X_{\mathbb{Q}_p}(A)$, taking $X = \{x\}$, we have the trivial representation

$$\alpha : A \to \mathbb{Q}_p \simeq C(\{x\}, \mathbb{Q}_p),$$

and of course X is compact with respect to the trivial topology.

Conversely, if $\Phi : A \to C_X$ is a representation, we can define a homomorphism $\alpha_x : A \to \mathbb{Q}_p$, putting $\alpha_x(a) := \Phi(a)(x)$.

However, we are mainly interested in finding **optimal representations** of A, giving us as much as possible informations about the ring A.

Definition 3.5.2 *A representation $\Phi : A \to C_X$ is called **optimal** if X is homeomorph to $X_{\mathbb{Q}_p}(A)$.*

We endow $X_{\mathbb{Q}_p}(A)$ with the topology generated by the open sub-basis consisting of the sets

$$U_{a,b} := U_{a,b}(A) := \{\alpha \in X_{\mathbb{Q}_p}(A) \ : \ v_p(\alpha(a)) > v_p(\alpha(b))\},$$

for each $a, b \in A$.

We also use a notation for the complements of these sets in $X_{\mathbb{Q}_p}(A)$, namely $V_{pb,a}(A) := X_{\mathbb{Q}_p}(A) \backslash U_{a,b}(A)$, for each $a, b \in A$.

With this topology we have:

Proposition 3.5.3 *$X_{\mathbb{Q}_p}(A)$ is Hausdorff and **zero dimensional**, i.e. it has a base consisting of clopen sets.*

Proof : In fact, for all $a, b \in A$,

$$U_{a,b} = \{\alpha \in X_{\mathbb{Q}_p}(A) \ : \ v_p(\alpha(a)) \geq v_p(\alpha(pb))\} = V_{pb,a},$$

and hence $U_{a,b}$ is clopen.

If $\alpha, \beta \in X_{\mathbb{Q}_p}(A)$ are different, there is $a \in A$ such that $\alpha(a) \neq \beta(a)$. Writing

$$\alpha(a) = \sum_{i \geq N}^{\infty} a_i p^i \text{ and } \beta(a) = \sum_{j \geq N}^{\infty} b_j p^j,$$

where $a_i, b_j \in \{0, ..., p-1\}$ and $N := \min\{v_p(\alpha(a)), v_p(\beta(a))\}$, we can take $k \in \mathbb{Z}$ minimal such that $k \geq N$ and $a_k \neq b_k$.

Defining

$$x_k := \sum_{N}^{k} c_i p^i \in \mathbb{Z}.$$

where $c_k := \min\{a_k, b_k\}$ and $c_i = a_i = b_i$ if $N \leq i < k$, we have

$$\begin{array}{rl} & v_p(\alpha(a - x_k)) > v_p(p^k) = v_p(\beta(a - x_k)) \\ \text{or} & v_p(\beta(a - x_k)) > v_p(p^k) = v_p(\alpha(a - x_k)), \end{array}$$

and hence

$$\begin{array}{ll} & \alpha \in U_{(a-x_k),p^k} \text{ and } \beta \in V_{(a-x_k),p^k} = U_{p^k,p^{-1}(a-x_k)} \\ \text{or} & \beta \in U_{(a-x_k),p^k} \text{ and } \alpha \in V_{(a-x_k),p^k} = U_{p^k,p^{-1}(a-x_k)}, \end{array}$$

where

$$U_{(a-x_k),p^k} \cap U_{p^k,p^{-1}(a-x_k)} = U_{(a-x_k),p^k} \cap V_{(a-x_k),p^k} = \emptyset$$

■

In general, the map $a \mapsto \widehat{a}$, where

$$\widehat{a} : X_{\mathbb{Q}_p}(A) \to \mathbb{Q}_p \ , \ \widehat{a}(\alpha) := \alpha(a);$$

defines a representation $\Phi : A \to C_{X_{\mathbb{Q}_p}(A)}$ with $\Phi(A)$ separating points of $C_{X_{\mathbb{Q}_p}(A)}$.

Clearly $\Phi(A)$ separates points, because

$$\alpha \neq \beta \in X_{\mathbb{Q}_p}(A) \Rightarrow (\exists a \in A) : \widehat{a}(\alpha) = \alpha(a) \neq \beta(a) = \widehat{a}(\beta),$$

To verify the continuity of $\widehat{a}$, note that, varying $x, y \in \mathbb{Q}_p$, the sets

$$U_{\mathbb{Q}_p}(x, y) := \{z \in \mathbb{Q}_p : v_p(z - y) > v(x)\}$$

define an open subbasis of the p-adic topology of $\mathbb{Q}_p$.

Moreover, using Lemma(3.3.4) in the second equality below, we deduce that

$$\begin{aligned} \widehat{a}^{-1}(U_{\mathbb{Q}_p}(x, y)) &= \{\alpha \in X_{\mathbb{Q}_p}(A) : v_p(\alpha(a) - y) > v_p(x)\} \\ &= \bigcup_{\substack{q \in \mathbb{Q} \text{ with} \\ v_p(\alpha(a)-q) > v_p(\alpha(a)-y)}} \{\alpha \in X_{\mathbb{Q}_p}(A) : v_p(\alpha(a) - q) > v_p(x)\} \\ &= \bigcup_{\substack{q \in \mathbb{Q} \text{ with} \\ v_p(\alpha(a)-q) > v_p(\alpha(a)-y)}} \{\alpha \in X_{\mathbb{Q}_p}(A) : v_p(\alpha(a - q)) > v_p(\alpha(p^{v_p(x)}))\} \\ &= \bigcup_{\substack{q \in \mathbb{Q} \text{ with} \\ v_p(\alpha(a)-q) > v_p(\alpha(a)-y)}} U_{(a-q),p^{v_p(x)}}(A), \end{aligned}$$

is open in $X_{\mathbb{Q}_p}(A)$, and hence $\widehat{a}$ is continuous.

However, $X_{\mathbb{Q}_p}(A)$ is not quasi-compact in general. For example, for the ring of polynomials $A = \mathbb{Q}_p[X_1, ..., X_n]$, the next proposition shows that $X_{\mathbb{Q}_p}(A)$ is homeomorph to $\mathbb{Q}_p^n$, which is not quasi-compact.

Proposition 3.5.4 *For all natural number $n > 0$, $\mathbb{Q}_p^n$ is homeomorph to $X_{\mathbb{Q}_p}(\mathbb{Q}_p[X_1, ..., X_n])$.*

Proof: We write $\mathbb{Q}_p[\underline{X}]$ for $\mathbb{Q}_p[X_1, ..., X_n]$. Of course the map

$$\alpha \overset{\varphi}{\mapsto} (\alpha(X_1), ..., \alpha(X_n))$$

defines a bijection $\varphi : X_{\mathbb{Q}_p}(\mathbb{Q}_p[\underline{X}]) \to \mathbb{Q}_p^n$, with inverse map φ^{-1}, mapping $(a_1, ..., a_n) \in \mathbb{Q}_p^n$ into

$$\begin{array}{rcl} \varphi^{-1}(a_1, ..., a_n) : \mathbb{Q}_p[\underline{X}] & \to & \mathbb{Q}_p, \\ \\ f = \sum_{k=0}^{\deg(f)} f_i X_i & \mapsto & \sum_{k=0}^{\deg(f)} f_i a_i \end{array}$$

Now take the sup-norm[12] $\| \cdot \|$ of $\mathbb{Q}_p$, i.e.,

$$(\forall (a_1, ..., a_n) \in \mathbb{Q}_p^n) : \|(a_1, ..., a_n)\| = \sup_{1 \leq i \leq n} \{|a_i|_p\}$$

For each $a = (a_1, ..., a_n) \in \mathbb{Q}_p^n$ and $r \in \mathbb{Z}$,

$$\begin{array}{rl} \varphi^{-1}(B_r(a)) & = \{\alpha \in X_{\mathbb{Q}_p}(\mathbb{Q}_p[\underline{X}]) : \|(\alpha(X_1) - a_1, ..., \alpha(X_n) - a_n)\| \leq r\} \\ \\ & = \bigcap_{1 \leq i \leq n} \{\alpha \in X_{\mathbb{Q}_p}(\mathbb{Q}_p[\underline{X}]) : v_p(\alpha(X_i) - a_i) \geq v_p(p^r)\} \end{array}$$

and the each set of this intersection is equal to the open set

$$\bigcup_{\substack{q \in \mathbb{Q} \text{ with} \\ v_p(\alpha(X_i) - q) > v_p(\alpha(X_i) - a_i)}} U_{(X_i - q), p^{r-1}}(A),$$

and hence φ is continuous.

Furthermore, for each $f, g \in \mathbb{Q}_p[\underline{X}]$,

$$\begin{array}{rcl} \varphi(U_{g,f}) & = & \{\varphi(\alpha) \in \mathbb{Q}_p^n : v_p(\alpha(g)) > v_p(\alpha(f))\} \\ & = & \{\varphi(\alpha) \in \mathbb{Q}_p^n : v_p(g(\varphi(\alpha))) > v_p(f(\varphi(\alpha)))\} \\ & \overset{surj.}{=} & \left\{a \in \mathbb{Q}_p^n : v_p\left(\frac{g}{f}(a)\right) > 0\right\} \cap \{a \in \mathbb{Q}_p^n : f(a) \neq 0\} \\ & = & \left(\frac{g}{f}\right)^{-1}(\mathbb{Z}_p) \ \cap \ (\mathbb{Q}_p^n \backslash f^{-1}(\{0\})) \end{array}$$

As the rational function given by $(g/f) : \mathbb{Q}_p^n \to \mathbb{Q}_p$ is continuous, in the points where it is defined, as well as f, the image $\varphi(U_{g,f})$ is open in $\mathbb{Q}_p^n$

Therefore φ is a homeomorphism.

■

Thus we can ask, as in the real case,

[12]It doesn't matter which norm we take. All $\mathbb{Q}_p$-norms of $\mathbb{Q}_p^n$ are equivalent, see [6],§5.2.

When is $X_{\mathbb{Q}_p}(A)$ compact?

To answer this, we need more results about p-adic representations. We start proving the main result relating $X_{\mathbb{Q}_p}(A)$ and the set $Arch_p^{\max}(A)$, of all maximal p-Archimedean divisibilities of A.

Theorem 3.5.5 *$Arch_p^{\max}(A)$ is homeomorph to $X_{\mathbb{Q}_p}(A)$, for each commutative ring A, where the homeomorphism is given by the map $|^v \mapsto \alpha_v$, and $\alpha_v : A \to A/I(\ |^v)$ is the canonical projection $a \mapsto a + I(\ |^v)$.*

Moreover, given a divisibility $\mathsf{d} := |$ of A, $Archr_{p,\mathsf{d}}^{\max}(A)$ is homeomorph to $X_{\mathsf{d},\mathbb{Q}_p}(A)$, where

$$Arch_{p,\mathsf{d}}^{\max}(A) := \{\ |^v \in Arch_p^{\max}(A)\ :\ |^v \supseteq |\ \}$$

and

$$X_{\mathsf{d},\mathbb{Q}_p}(A) := \{\alpha \in X_{\mathbb{Q}_p}(A)\ :\ (\forall a, b \in A) : a \mid b \Rightarrow v_p(\alpha(a)) \leq v_p(\alpha(b))\}$$

Proof : The map is well-defined by Proposition(3.3.2). By the same proposition, for each $|^{v_1}\ ,\ |^{v_2} \in V_p^{\max}(\ |\ )$, $\alpha_{v_1} = \alpha_{v_2}$ implies

$$a\ |^{v_1}\ b\ \Leftrightarrow\ v_p(\alpha_{v_1}(a)) \leq v_p(\alpha_{v_1}(b))\ \Leftrightarrow\ v_p(\alpha_{v_2}(a)) \leq v_p(\alpha_{v_2}(b))\ \Leftrightarrow\ a\ |^{v_2}\ b$$

and hence $|^{v_1} = |^{v_2}$. Thus the map is injective.

Given $\alpha \in X_{\mathbb{Q}_p}(A)$, we can define a p-Archimedean divisibility $|^{v_\alpha}$ of A, declaring

$$(\forall a, b \in A) : a\ |^{v_\alpha}\ b\ :\Leftrightarrow\ v_p(\alpha(a)) \leq v_p(\alpha(b)) \tag{3.13}$$

We claim that $\alpha_{v_\alpha} = \alpha$, and hence the map is surjective.

First observe that $\ker(\alpha) = I(\ |^{v_\alpha})$, and hence $\alpha_{v_\alpha} : A \to \mathbb{Q}_p$. Thus $|^{v_\alpha}$ is maximal and

$$(\forall a, b \in A) : a\ |^{v_\alpha}\ b \Leftrightarrow v_p(\alpha_{v_\alpha}(a)) \leq v_p(\alpha_{v_\alpha}(b)), \tag{3.14}$$

again by Proposition(3.3.2).

Therefore, by (3.13) and (3.14),

$$(\forall a, b \in A) : v_p(\alpha_{v_\alpha}(a)) \leq v_p(\alpha_{v_\alpha}(b)) \Leftrightarrow v_p(\alpha(a)) \leq v_p(\alpha(b)) \tag{3.15}$$

This equivalence implies, in particular, that $\alpha_{v_\alpha}(a) = \alpha(a)$ for all $a \in A$. In fact, for each $a \in A$, we can write

$$\alpha(a) = \sum_{i \geq n}^{\infty} a_i p^i, \quad \text{with } a_i \in \{0, ..., p-1\},\ n = v_p(\alpha(a)),$$

and as $v_p(\alpha(a)) = v_p(\alpha_{v_\alpha}(a))$, by (3.15), we also have

$$\alpha_{v_\alpha}(a) = \sum_{i \geq n}^{\infty} b_i p^i, \quad \text{with } b_i \in \{0, ..., p-1\}$$

Therefore

$$v_p(\alpha(a) - a_n p^n) > 0 \overset{(3.15)}{\Rightarrow} v_p(\alpha_{v_\alpha}(a) - a_n p^n) > 0 \Rightarrow a_n = b_n$$

Now, if we suppose that

$$\sum_{i=n}^{k} a_i p^i = \sum_{i=n}^{k} b_i p^i,$$

for some $k \geq n$, then

$$v_p\left(\alpha(a) - \sum_{i=n}^{k} a_i p^i\right) > 0 \overset{(3.15)}{\Leftrightarrow} v_p\left(\alpha_{v_\alpha}(a) - \sum_{i=n}^{k} b_i p^i\right) > 0$$

implies that $a_{k+1} = b_{k+1}$, by the same argument used above to prove $a_n = b_n$.

Thus, after using an inductive argument for k, we can deduce that $a_i = b_i$ for all $i \geq n$, and hence $\alpha(a) = \alpha_{v_\alpha}(a)$.

To verify that the map $|^v \overset{\varphi}{\mapsto} \alpha_v$ is a homeomorphism, note that

$$\begin{array}{rcl} \varphi^{-1}(U_{a,b}) & = & \{\ |^v \in Arch_p^{\max} : v_p(\alpha_v(a)) > v_p(\alpha_v(b))\} \\ & \overset{Prop.(3.3.2)}{=} & \{\ |^v \in Arch_p^{\max} : a \nmid^v b\} \\ & = & \mathcal{U}_{a,b}(A) \end{array}$$

for all $a, b \in A$, and hence also $\varphi(\mathcal{U}_{a,b}(A)) = \varphi(\varphi^{-1}(U_{a,b})) = U_{a,b}$, by bijectivity.

At last, for a given divisibility $\mathsf{d} := |$ of A, note that

$$|^v \in Arch_{p,\mathsf{d}}^{\max}(A) \Rightarrow \alpha_v \in X_{\mathsf{d},\mathbb{Q}_p}(A)$$

and, for each $\alpha \in X_{\mathsf{d},\mathbb{Q}_p}(A)$, we have $\varphi^{-1}(\alpha) = |^{v_\alpha} \supseteq |$, and hence the map φ defines a homeomorphism between $Arch_{p,\mathsf{d}}^{\max}(A)$ and $X_{\mathsf{d},\mathbb{Q}_p}(A)$.

■

As $Arch_p^{\max}(A)$ is homeomorph to $X_{\mathbb{Q}_p}(A)$, the next theorem gives us a necessary and sufficient condition for the compactness of $X_{\mathbb{Q}_p}(A)$.

Theorem 3.5.6 *Let A be a commutative ring. Then $Arch_p^{\max}(A)$ is closed in $V_p^{\max}(A)$ if, and only if,*

$$|^A := \bigcap_{|^v \in Arch_p^{\max}(A)} |^v$$

is a p-Archimedean divisibility of A.

Moreover, as $V_p^{\max}(A)$ is compact[13]*,*

$$X_{\mathbb{Q}_p}(A) \simeq Arch_p^{\max}(A) \text{ is compact } \Leftrightarrow |^A \in Arch_p(A)$$

Proof : If $Arch_p^{\max}(A)$ is closed in $V_p^{\max}(A)$, then it is also quasi-compact (even compact!), by Proposition(2.6.6).

For all $a \in A$, of course

$$Arch_p^{\max}(A) \subseteq \bigcup_{n\in\mathbb{N}} \mathcal{V}_1(p^n a),$$

because of the p-Archimedean property of the elements of $Arch_p^{\max}(A)$.

Thus, by quasi-compactness[14], there are $n_1, ..., n_k \in \mathbb{N}$ such that

$$Arch_p^{\max}(A) \subseteq \mathcal{V}_1(p^{n_1}a) \cup \cdots \cup \mathcal{V}_1(p^{n_k}a)$$

Taking $n := \max\{n_1, ..., n_k\}$, we see that $1 \mid^v p^n a$ for all $|^v \in Arch_p^{\max}(A)$, implying that $1 \mid^A p^n a$.

Conversely, if $|^A$ is a p-Archimedean divisibility of A, then $Arch_p^{\max}(A) = V_p^{\max}(\ |^A)$, because each p-valuation containing a p-Archimedean divisibility is also p-Archimedean. Thus $Arch_p^{\max}(A)$ is closed in $V_p^{\max}(A)$, and hence compact (see the proof of Corollary(2.6.7).).

■

This theorem, together with the p-adic Representation Theorem, gives us a necessary and sufficient condition for the *existence* of a dominant representation $\Phi : A \to C_{X_{\mathbb{Q}_p}(A)}$ with $X_{\mathbb{Q}_p}(A)$ compact.

We want also to answer the following question, concerned with the *uniqueness* (up to homeomorphisms) of the choice of the space $X_{\mathbb{Q}_p}(A)$ for dominant representations of A in rings C_X.

Given a commutative ring A containing $\mathbb{Q}$, a compact space X and a dominant representation $\Phi : A \to C_X$, when is $X \simeq X_{\mathbb{Q}_p}(A)$?

[13] It is quasi-compact by Lemma(2.6.4) and Hausdorff, as well as $V_p(A)$.

[14] Proposition(2.6.6) also assures that $\mathcal{V}_a(b)$ is a clopen set, for each $a, b \in A$.

To answer this question[15], we use the following result.

Two zero dimensional compact spaces X and Y are homeomorphic if, and only if, C_X are C_Y isomorphic.

We want to give a self-contained proof of this fact later. To do this, we will need some analytical facts.

Observe also that C_X and C_Y are not just $\mathbb{Q}$-algebras, but even $\mathbb{Q}_p$-algebras, and hence, at some point, we can restrict our results to the case of $\mathbb{Q}_p$-algebras.

First we fix a standard notation.

Definition 3.5.7 *Let X be a topological space and C_X the ring of p-adic valued continuous functions. For each $I \subseteq C_X$ define*

$$\mathcal{Z}(I) := \{x \in X : a(x) = 0 \text{ for all } a \in I\}$$

We prove then a fundamental lemma.

Lemma 3.5.8 *Let X be a quasi-compact space and I an ideal of C_X. Then,*

$$\mathcal{Z}(I) = \emptyset \Rightarrow I = (1) = C_X$$

Proof : Suppose that $\mathcal{Z}(I) = \emptyset$. Thus, for each $x \in X$, there is $a_x \in I$ such that $a_x(x) \neq 0$. As a_x is continuous, we can take an open set U_x of X with $x \in U_x$ and

$$a_x(y) \neq 0 \text{ for all } y \in U_x$$

Therefore $X = \bigcup_{x \in X} U_x$, and hence, by quasi-compactness, we can choose $x_1, ..., x_n \in X$ such that $X = \bigcup_{1 \leq i \leq n} U_{x_i}$.

Taking the corresponding a_{x_i}'s, define

$$f := a_{x_1}^n + pa_{x_2}^n + ... + p^{n-1}a_{x_n}^n \in I$$

Then, for all $x \in X$, we have $v_p(f(x)) = v_p(p^{i-1}(a_{x_i}(x))^n)$ for some $1 \leq i \leq n$. In fact, for each $x \in X$ and $i \in \{1, ..., n\}$,

$$v_p(p^{i-1}(a_{x_i}(x))^n) \equiv (i-1) \pmod{n}, \tag{3.16}$$

and hence $v_p(p^{i-1}(a_{x_i}(x))^n) \neq v_p(p^{j-1}(a_{x_j}(x))^n)$, for all $i \neq j$.

We claim that $f(x) \neq 0$ for all $x \in X$. In fact, otherwise, we can suppose, without loss of generality, that $0 = |f(x)|_p = |(a_{x_1}(x))^n|_p$, and hence

$$x \notin U_{x_1} \text{ and } 0 = f(x) = p(a_{x_2}(x))^n + ... + p^{n-1}(a_{x_n}(x))^n$$

[15]More precisely, to prove Theorem(3.5.13).

By (3.16), we can suppose, without loss of generality, that

$$0 = |f(x)|_p = |p(a_{x_2}(x))^n|_p,$$

and then

$$x \notin U_{x_2} \text{ and } 0 = f(x) = p^2(a_{x_3}(x))^n + ... + p^{n-1}(a_{x_n}(x))^n$$

After iterating this argument a finite number of times, we will conclude that $x \notin \bigcup_{1\leq i\leq n} U_{x_i} = X$, a contradiction.

Thus, the real function $x \mapsto |f(x)|_p$ is continuous on a quasi-compact space X and is always greater then zero.

Therefore there is $M > 0$ such that $|f(x)|_p \geq M$ for all $x \in X$. It follows that $1/f \in C_X$, because, for all $x_0 \in X$, given $\epsilon \cdot M^2 > 0$, there is an open $x_0 \in U_\epsilon \subseteq X$ such that, for all $x \in U_\epsilon$,

$$\left|\frac{1}{f(x)} - \frac{1}{f(x_0)}\right|_p = \left|\frac{f(x) - f(x_0)}{f(x)f(x_0)}\right|_p \leq \frac{|f(x) - f(x_0)|_p}{M^2} < \frac{\epsilon \cdot M^2}{M^2} = \epsilon,$$

by the continuity of f.

As $f \in I$, it follows that $1 = f \cdot (1/f) \in I$.

■

The next proposition describes explicitly the set $Arch^{\max}_{p,\mathsf{d}_0}(C_X)$, where $\mathsf{d}_0 := |_0$ is the canonical p-divisibility of C_X.

Proposition 3.5.9 *Let X be a zero dimensional compact space and $\mathsf{d}_0 := |_0$ the canonical p-divisibility of C_X. Then*

$$V^{\max}_{p,\mathsf{d}_0}(C_X) = Arch^{\max}_{p,\mathsf{d}_0}(C_X) = \{\ |^{v_x} :\ x \in X\}$$

where

$$(\forall a, b \in C_X) : a\ |^{v_x}\ b \Leftrightarrow v_p(a(x)) \leq v_p(b(x))$$

The map $x \mapsto |^{v_x}$ defines a homeomorphism between X and $Arch^{\max}_{p,\mathsf{d}_0}(C_X)$.

Proof: For each $x \in X$, clearly $|^{v_x}$ is a p-valuation extending $|_0$.

If $\alpha_x : C_X \to \mathbb{Q}_p$ is the evaluation map $a \mapsto a(x)$, then α_x is a ring homomorphism and $I(\ |^{v_x}) = \ker(\alpha_x)$. Thus

$$\alpha_{v_x} = \alpha_x : C_X \to C_X/I(\ |^{v_x}) = C_X/\ker(\alpha_x) \hookrightarrow \mathbb{Q}_p$$

It follows from Proposition(3.3.2) that $|^{v_x}$ is maximal, for all $x \in X$, and hence the map $x \mapsto |^{v_x}$ has indeed range $Arch^{\max}_{p,\mathsf{d}_0}(C_X)$.

It is injective, because $|^{v_x} = |^{v_y}$, for some $x, y \in X$, implies

$$\ker(\alpha_y) = I(\ |^{v_x}) = I(\ |^{v_x}) = \ker(\alpha_x),$$

and hence $x = y$, by Lemma(3.5.10) below.

For the surjectivity, take $|^v \in Arch^{\max}_{p,\mathsf{d}_0}(C_X)$ and $I_v := I(\ |^v) \subseteq C_X$. Then there is $x \in X$ such that $x \in \mathcal{Z}(I_v)$, by Lemma(3.5.8), and hence $I_v \subseteq \ker(\alpha_x)$.

As $|^v$ and $|^{v_x}$ are maximal, Proposition(3.3.2) guarantees that

$$a\ |^v\ b \Leftrightarrow v_p(a + I_v) \leq v_p(b + I_v) \Leftrightarrow (b + I_v) \in (a + I_v) \cdot \mathbb{Z}_p$$

and also

$$a\ |^{v_x}\ b \Leftrightarrow v_p(a + I(\ |^{v_x})) \leq v_p(b + I(\ |^{v_x})) \Leftrightarrow (b + I(\ |^{v_x})) \in (a + I(\ |^{v_x})) \cdot \mathbb{Z}_p$$

for all $a, b \in B$.

Thus, $I_v \subseteq \ker(\alpha_x) = I(\ |^{v_x})$ implies that $|^v \subseteq |^{v_x}$. It follows that $|^v = |^{v_x}$, by the maximality of $|^v$, and then the surjectivity.

To verify the map $x \mapsto |_x$ is a homeomorphism, it is enough to prove that it is continuous, because $Arch^{\max}_{p,\mathsf{d}_0}(C_X)$ and X are compact spaces.

The map is continuous, because the inverse image of

$$\begin{aligned} \mathcal{U}_{a,b}(C_X) &= \{\ |^{v_x} \in Arch^{\max}_{p,\mathsf{d}_0}(C_X) :\ a \nmid^{v_x} b\} \\ &= \{\ |^{v_x} \in Arch^{\max}_{p,\mathsf{d}_0}(C_X) :\ v_p(a(x)) > v_p(b(x))\} \end{aligned}$$

is equal to

$$\left\{x \in X\ :\ b(x) \neq 0 \text{ and } v_p\left(\frac{a}{b}(x)\right) > 0\right\},$$

which is open in X, for all $a, b \in C_X$, because a and b are continuous on X, and hence also $(1/b)$ on the open set

$$\{x \in X\ :\ b(x) \neq 0\}$$

■

The auxiliary lemma used above is

Lemma 3.5.10 *Let X be a zero dimensional compact space and $\mathcal{M}(C_X)$ the set of all maximal ideal of C_X. Then*

$$\mathcal{M}(C_X) = \{\ker(\alpha_x) : x \in X\},$$

where $\alpha_x : C_X \to \mathbb{Q}_p$ with $\alpha_x(f) := f(x)$.

Moreover, the map $x \mapsto \ker(\alpha_x)$ defines a bijection between X and $\mathcal{M}(C_X)$.

Proof : Take X a zero dimensional compact space. The maps

$$C_X/\ker(\alpha_x) \to \mathbb{Q}_p$$

are isomorphisms, because $\mathbb{Q}_p \subseteq C_X$, and hence $\ker(\alpha_x) \in \mathcal{M}(C_X)$.

If $M \in \mathcal{M}(C_X)$, then Lemma(3.5.8) assures the existence of some $x \in X$ such that $M \subseteq \ker(\alpha_x)$. By maximality $M = \ker(\alpha_x)$. This also proves the surjectivity of $x \mapsto \ker(\alpha_x)$.

For the injectivity, note that $\ker(\alpha_x) = \ker(\alpha_y)$, for some $x, y \in X$, implies

$$f(x) = f(y) \text{ for all } f \in C_X, \tag{3.17}$$

because

$$f(x) = r \Leftrightarrow (f-r)(x) = 0 \Leftrightarrow (f-r)(y) = 0 \Leftrightarrow f(y) = r,$$

for each $r \in \mathbb{Q}_p$.

As X is a zero dimensional Hausdorff space, we must have $x = y$. In fact, if $x \neq y$, there is a clopen subset $U \subseteq X$ satisfying $x \in U$ and $y \notin U$.

Furthermore, the characteristic function $\chi_U : X \to \mathbb{Q}_p$, defined by

$$\chi_U(x) := \begin{cases} 1 & , \text{ if } x \in U \\ 0 & , \text{ if } x \notin U \end{cases}$$

is continuous[16] and hence $\chi_U \in C_X$.

However, $\chi_U(x) = 1 \neq 0 = \chi_U(y)$ and $\chi_U \in C_X$ contradicts (3.17).

■

We state now an important general theorem about p-Archimedean divisibilities.

Theorem 3.5.11 *Let A and B be commutative rings containing $\mathbb{Q}$. Take some surjective representation $\Phi : A \to B$, $\mathsf{d} := |$ a p-Archimedean divisibility of B and $\mathsf{d}_\Phi := |^\Phi$ the p-Archimedean divisibility of A induced by d and Φ, i.e.,*

$$(\forall a, b \in A) : a \mid^\Phi b :\Leftrightarrow \Phi(a) \mid \Phi(b)$$

Then

$$Arch^{\max}_{p,\mathsf{d}}(B) \simeq Arch^{\max}_{p,\mathsf{d}_\Phi}(A),$$

and in particular, also $X_{\mathsf{d},\mathbb{Q}_p}(B) \simeq X_{\mathsf{d}_\Phi,\mathbb{Q}_p}(A)$.

[16]In the real case, we do not need the zero dimensional hypothesis, because Urysohn's Lemma guarantees that C_X has an element f separating distinct points of X. This lemma is also used in the proof of Theorem(1.1.10).

Proof : We define the map

$$\Psi : Arch^{\max}_{p,\mathsf{d}}(B) \to Arch^{\max}_{p,\mathsf{d}_\Phi}(A),\ |^v \mapsto\ (|^v)^\Phi,$$

where $(|^v)^\Phi$ is the divisibility of A induced by Φ and $|^v$.

By its definition, $(|^v)^\Phi$ is a p-Archimedean divisibility of A containing $|^\Phi$. It is also maximal, because

$$I((|^v)^\Phi) = \{a \in A : 0 \mid^v \Phi(a)\} = \{a \in A : \alpha_v(\Phi(a)) = 0\} = \ker(\alpha_v \circ \Phi)$$

and hence, as $\alpha_v \circ \Phi : A \to \mathbb{Q}_p$, because $|^v$ is maximal (Proposition(3.3.2)), we also have

$$\alpha_{v^\Phi} : A \to A/I((|^v)^\Phi) = A/\ker(\alpha_v \circ \Phi) \hookrightarrow \mathbb{Q}_p$$

where $v^\Phi := (|^v)^\Phi$.

Therefore it is maximal, again by Proposition(3.3.2), and hence the map Ψ has indeed range $Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$.

Now we want to define a map

$$\theta : Arch^{\max}_{p,\mathsf{d}_\Phi}(A) \to Arch^{\max}_{p,\mathsf{d}}(B),\ |^v \mapsto (|^v)_\Phi$$

that is the inverse map of Ψ.

To do this, for each $|^v \in Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$ we define a binary relation $(|^v)_\Phi$ of B by

$$(\forall g, f \in B) : g(|^v)_\Phi f :\Leftrightarrow a \mid^v b \text{ for some } a \in \Phi^{-1}(g),\ b \in \Phi^{-1}(f)$$

We will verify that:

Claim: $(|^v)_\Phi \in Arch^{\max}_{p,\mathsf{d}}(B)$, *for all* $|^v \in Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$.

Take $|^v \in Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$. Then

$$\begin{aligned}(\forall g, f \in B) : g \mid f \ &\Rightarrow (\exists a, b \in A) : \Phi(a) = g \mid f = \Phi(b)\\ &\Rightarrow a \mid^\Phi b \text{ with } \Phi(a) = g,\ \Phi(b) = f\\ &\Rightarrow a \mid^v b \text{ with } a \in \Phi^{-1}(g),\ b \in \Phi^{-1}(f)\\ &\Rightarrow g(|^v)_\Phi f,\end{aligned}$$

and hence $(|^v)_\Phi \supseteq |$.

Of course $f(|^v)_\Phi f$ for all $f \in B$. Moreover, for all $g, f, h \in B$, there are $a, b, c \in A$ such that $\Phi(g) = a, \Phi(b) = f$ and $\Phi(c) = h$, by surjectivity, and

hence

$$g(|^v)_\Phi f \;\Rightarrow\; a\,|^v\,b \Rightarrow ac\,|^v\,bc \overset{\Phi(A)\cdot\Phi(A)=\Phi(A)}{\Rightarrow} gh(|^v)_\Phi fh$$

$$g(|^v)_\Phi f,\ f(|^v)_\Phi h \;\Rightarrow\; a\,|^v\,b,\ b\,|^v\,c \Rightarrow a\,|^v\,c \Rightarrow g(|^v)_\Phi h$$

$$g(|^v)_\Phi f,\ g(|^v)_\Phi h \;\Rightarrow\; a\,|^v\,b,\ a\,|^v\,c \Rightarrow a\,|^v\,b \pm c \overset{\Phi(A)\pm\Phi(A)=\Phi(A)}{\Rightarrow} g(|^v)_\Phi h$$

As $|^v$ satisfies the Kochen property, using the properties of the homomorphism Φ (and some usual algebraic calculation), we can prove that $(|^v)_\Phi$ satisfies also the Kochen property.

At last, note that $p(\nmid^v)_\Phi 1$. In fact, otherwise there are $a, b \in A$ such that $a\,|^v\,b$ and $a \in \Phi^{-1}(p), b \in \Phi^{-1}(1)$, and in particular

$$p = \Phi(p) \mid \Phi(a) = p \;\Rightarrow\; p\,|^\Phi\,a \overset{|^\Phi\subseteq|^v}{\Rightarrow} p\,|^v\,a$$
$$1 = \Phi(b) \mid \Phi(1) = 1 \;\Rightarrow\; b\,|^\Phi\,1 \overset{|^\Phi\subseteq|^v}{\Rightarrow} b\,|^v\,1$$

and hence, also $p\,|^v\,1$, contradicting our choice of $|^v \in Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$.

Therefore $(|^v)_\Phi$ is actually a p-divisibility of B, and it is p-Archimedean, because it contains $|$.

Let us see that $(|^v)_\Phi$ is maximal, i.e., $(|^v)_\Phi = |^{v'}$ for some $|^{v'} \in Arch^{\max}_{p,\mathsf{d}}(B)$.

Take a maximal p-divisibility $|^{v'}$ of B extending $(|^v)_\Phi$, which exists by Theorem(3.2.4). Then

$$|^v \subseteq ((|^v)_\Phi)^\Phi \subseteq (|^{v'})^\Phi$$

because, for all $a, b \in A$,

$$a\,|^v\,b \Rightarrow \Phi(a)(|^v)_\Phi\Phi(b) \Rightarrow a((|^v)_\Phi)^\Phi b$$

By the maximal choice of $|^v$, we must have

$$|^v = \ (|^{v'})^\Phi \tag{3.18}$$

Therefore,

$$(|^v)_\Phi = |^{v'}, \tag{3.19}$$

because the surjectivity of Φ implies that, for each $f, g \in B$, there are $a, b \in A$ such that $\Phi(a) = g$ and $\Phi(b) = f$, and then

$$g\,|^{v'}\,f \Rightarrow \Phi(a)\,|^{v'}\,\Phi(b) \Rightarrow a(|^{v'})^\Phi b \overset{(3.18)}{\Rightarrow} a\,|^v\,b \Rightarrow f = \Phi(a)(|^v)_\Phi\Phi(b) = g$$

and hence $Arch^{\max}_{p,\mathsf{d}}(B)$ is indeed the range of θ.

Moreover, our argument also implies that Ψ is surjective, by (3.19). Indeed, Ψ is also injective (also a consequence of the surjectivity of Φ). One way of seen this is verifying that θ and Ψ are inverses of each other.

In fact, for all $c, d \in A$, $f, g \in B$ with $f = \Phi(b), g = \Phi(a)$, for some $a, b \in A$, $|^{v'} \in Arch^{\max}_{p,\mathsf{d}}(B)$ and $|^{v} \in Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$,

$$g \,|^{v'}\, f \;\Rightarrow\; a\ (|^{v'})^{\Phi}\ b \;\Rightarrow\; g\ ((|^{v'})^{\Phi})_{\Phi}\ f$$

$$c \,|^{v}\, d \;\Rightarrow\; \Phi(c)\ (|^{v}\ )_{\Phi}\ \Phi(d) \;\Rightarrow\; c\ ((|^{v}\ )_{\Phi})^{\Phi}\ d$$

and hence, by the maximal choice of $|^{v'}$ and $|^{v}$, we must have

$$|^{v'} \;=\; ((|^{v'})^{\Phi})_{\Phi} \;=\; \theta(\Psi(\ |^{v'}))$$

$$|^{v} \;=\; ((|^{v}\ )_{\Phi})^{\Phi} \;=\; \Psi(\theta(\ |^{v}))$$

Thus Ψ is a bijection with inverse map θ. Furthermore, Ψ is continuous, because

$$\Psi^{-1}(\mathcal{U}_{a,b}(A)) = \{\ |^{v'} \in Arch^{\max}_{p,\mathsf{d}}(B) : \Phi(a) \nmid^{v'} \Phi(b)\} = \mathcal{U}_{\Phi(a),\Phi(b)}(B),$$

for all $a, b \in A$.

As $Arch^{\max}_{p,\mathsf{d}}(B)$ and $Arch^{\max}_{p,\mathsf{d}_\Phi}(A)$ are both compact, by Corollary(2.6.7), Ψ is a homeomorphism.

■

Now we are ready to prove our claim.

Theorem 3.5.12 *Two zero dimensional compact spaces X and Y are homeomorphic if, and only if, C_X and C_Y are isomorphic.*

Proof : Let X and Y be zero dimensional compact spaces. If $\varphi : X \to Y$ is a homeomorphism, then

$$\Phi : C_Y \to C_X,\ f \mapsto f \circ \varphi$$

is a homomorphism, and it is even an isomorphism, because

$$(\forall f, g \in C_Y) : f \circ \varphi = g \circ \varphi \Rightarrow f = f \circ (\varphi \circ \varphi^{-1}) = g \circ (\varphi \circ \varphi^{-1}) = g$$

$$g \in C_X \Rightarrow g = g \circ (\varphi^{-1} \circ \varphi) = \Phi(g \circ \varphi^{-1}) \text{ with } g \circ \varphi^{-1} \in C_Y$$

The proof of the converse is less trivial. Let $\Phi : C_X \to C_Y$ be an isomorphism, where X and Y are zero dimensional compact spaces. Define the canonical p-Archimedean divisibilities

$$\mathsf{d}_X := |_X := \{(g, f) \in C_X \times C_X \ :\ v_p(g(x)) \leq v_p(f(x)) \text{ for all } x \in X\}$$
$$\mathsf{d}_Y := |_Y := \{(g, f) \in C_Y \times C_Y \ :\ v_p(g(y)) \leq v_p(f(y)) \text{ for all } y \in Y\}$$

We claim that

$$\mathsf{d}_\Phi := |_Y^\Phi = |_X \tag{3.20}$$

where $|_Y^\Phi$ is the p-divisibility of C_X induced by Φ and $|_Y$.

In fact, for $p \neq 2$ and $g, f \in C_X$

$$\begin{array}{rll} g \mid_X f & \overset{\text{Lem.(3.4.10)}}{\Leftrightarrow} & h^2 = g^2 + pf^2 \text{ for some } h \in C_X \\ & \overset{\text{Bijection}}{\Leftrightarrow} & r^2 = \Phi(g)^2 + p\Phi(f)^2 \text{ for some } r \in C_Y \\ & \overset{\text{Lem.(3.4.10)}}{\Leftrightarrow} & \Phi(g) \mid_Y \Phi(f) \Leftrightarrow g \mid_Y^\Phi f \end{array}$$

and the same argument works for $p = 2$, because of Lemma(3.4.11).

This implies the desired homeomorphism, because

$$\begin{array}{rll} X & \overset{Prop.(3.5.9)}{\simeq} & Arch_{p,\mathsf{d}_X}^{\max}(C_X) = Arch_{p,\mathsf{d}_\Phi}^{\max}(C_X) \\ & \overset{Theo.(3.5.11)+Bij.}{\simeq} & Arch_{p,\mathsf{d}_Y}^{\max}(C_Y) \\ & \overset{Prop.(3.5.9)}{\simeq} & Y \end{array}$$

■

Using this theorem, we can say when there exists an optimal representation of a commutative ring A containing $\mathbb{Q}$.

Theorem 3.5.13 *A commutative ring A, containing $\mathbb{Q}$, has an optimal representation, i.e., a dominant representation $\Phi : A \to C_X$ with $X \simeq X_{\mathbb{Q}_p}(A)$ compact*[17]*, if, and only if,*

$$|^A := \bigcap_{|^v \in Arch_p^{\max}(A)} |^v$$

is a p-Archimedean divisibility of A.

Proof : If $\mathsf{d}_A := |^A$ is a p-Archimedean divisibility of A, then the p-adic Representation Theorem provides a dominant representation

$$\Phi_{T_A} : A \to C_{Arch_{p,\mathsf{d}_A}^{\max}(A)} = C_{Arch_p^{\max}(A)}$$

As $X_{\mathbb{Q}_p}(A) \simeq Arch_p^{\max}(A)$ and they are zero dimensional, we conclude that $C_{Arch_p^{\max}(A)} \simeq C_{X_{\mathbb{Q}_p}(A)}$, by Theorem(3.5.12), and hence we have a dominant representation

$$\Psi : A \to C_{X_{\mathbb{Q}_p}(A)}$$

[17]Thus X is zero dimensional as $X_{\mathbb{Q}_p}(A)$.

with $X_{\mathbb{Q}_p}(A)$ compact, by Theorem(3.5.6).

Conversely, if $\Phi : A \to C_X$ is a dominant representation with $X \simeq X_{\mathbb{Q}_p}(A)$ compact, then $Arch_p^{\max}(A) \simeq X_{\mathbb{Q}_p}(A)$ is closed in the compact space $V_p^{\max}(A)$, and hence $|^A$ is a p-Archimedean, by Theorem(3.5.6).

■

It is important to observe that $\Phi(A)$ is in general just a $\mathbb{Q}$-algebra, in the theorem above.

The results about $\mathbb{Q}_p$-algebras were used just to prove Theorem(3.5.12), where we worked with the $\mathbb{Q}_p$-algebra C_X.

3.6 Maximal p-valuations of $\mathbb{Q}_p[X_1, ..., X_n]$

In this last section, we want to study p-divisibilities $|^B$ of the ring of polynomials $\mathbb{Q}_p[\underline{X}] := \mathbb{Q}_p[X_1, ..., X_n]$ generated by subrings B of its quotient field $\mathbb{Q}_p(\underline{X}) := \mathbb{Q}_p(X_1, ..., X_n)$, and given by

$$(\forall g, f \in \mathbb{Q}_p[\underline{X}]) : g \mid^B f \Leftrightarrow \left(\frac{f}{g}\right) \in B$$

Note that, $|^B$ is a p-divisibility, if, and only if,

$$p^{-1} \notin B \text{ and } \gamma_p(\mathbb{Q}_p(\underline{X})) \subseteq B,$$

where γ_p is the p-adic Kochen operator.[18]

By its definition, we also see that $|^B$ is p-Archimedean if, and only if,

$$(\forall f \in \mathbb{Q}_p[\underline{X}])(\exists n \in \mathbb{N}) : p^n f \in B \tag{3.21}$$

In particular the next proposition is true.

Proposition 3.6.1 *For each $B \subseteq \mathbb{Q}_p(\underline{X})$, $|^B$ is a p-Archimedean divisibility of $\mathbb{Q}_p[\underline{X}]$ if, and only if,*

$$\gamma_p(\mathbb{Q}_p(\underline{X}))[p^{m_1}X_1, ..., p^{m_n}X_n] \subseteq B \tag{3.22}$$

for some $m_1, ..., m_n \in \mathbb{Z}$.

Proof : If $|^B$ is a p-Archimedean divisibility, then of course the inclusion above is true by (3.21) applied to $X_1, ..., X_n$.

Conversely, suppose that (3.22) holds. For each

$$f = \sum_{i_1+...+i_n \leq \deg(f)} a_{i_1,...,i_n} X_1^{i_1} \cdots X_n^{i_n} \in \mathbb{Q}_p[\underline{X}],$$

[18] Also $\mathbb{Z}_p \subseteq B$, because $\gamma_p(\mathbb{Q}_p) = \mathbb{Z}_p$.

taking

$$n_f := \min\{v_p(a_{i_1,...,i_n}) : i_1 + ... + i_n \leq \deg(f)\}$$

we have

$$p^{-n_f+m_1+...+m_n} f \in B$$

■

If $|^B$ is a p-Archimedean divisibility, then every p-divisibility extending it is also p-Archimedean, and in particular its maximal p-extensions too.

What we want to see now, is a necessary and sufficient condition assuring that all maximal p-divisibilities, extending a given p-divisibility $|^B$, are p-Archimedean, even without knowing if $|^B$ is p-Archimedean

By Proposition(3.3.2), this is equivalent to say that

$$\alpha_v : \mathbb{Q}_p[X_1, ..., X_n] \to \mathbb{Q}_p.$$

for all $|^v \in V_p^{\max}(\ |^B)$.

We do this for the special class of subrings

$$B = \gamma(\mathbb{Q}_p[\underline{X}])[h_1, ..., h_r],$$

where $h_1, ..., h_r \in \mathbb{Q}_p[\underline{X}]$ and $p^{-1} \notin B$.

First we observe some subsets of $\mathbb{Q}_p^n$, defined below. We also do some useful definitions.

Definition 3.6.2 *For every $I \subseteq \mathbb{Q}_p[\underline{X}]$, we define*

$$W_p(I) := \{x \in \mathbb{Q}_p^n : h(x) \in \mathbb{Z}_p \text{ for all } h \in I\}$$

$$V_p(I) := \{\ |^v \in V_p(\mathbb{Q}_p[\underline{X}]) : 1\ |^v\ h \text{ for all } h \in I\}$$

If $I = \{h_1, ..., h_r\}$, then we write

$$W_p(h_1, ..., h_r) := W_p(I) \quad \text{and} \quad V_p(h_1, ..., h_r) := V_p(I)$$

Observe that of course

$$W_p(I) = \bigcap_{h \in I} W_p(h) \quad \text{and} \quad V_p(I) = \bigcap_{h \in I} V_p(h)$$

*We say that a subset $X \subseteq \mathbb{Q}_p^n$ is p-**bounded in** $\mathbb{Q}_p^n$, if*

$$X \subseteq p^m \mathbb{Z}_p^n := p^m \mathbb{Z}_p \times \cdots \times p^m \mathbb{Z}_p,$$

for some $m \in \mathbb{Z}$.

The main result we need, is the next proposition. To prove it we use the model-completeness of the theory of p-adic closed fields of p-rank 1, as found in [20]. The results needed from Model Theory can be found in [17].

Proposition 3.6.3 *For* $h_1, ..., h_l \in \mathbb{Q}_p[\underline{X}]$,

$W_p(h_1, ..., h_l)$ *is p-bounded* $\Leftrightarrow \alpha_v : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p$ *for all* $|^v \in V_p^{\max}(h_1, ..., h_l)$

where $\alpha_v : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p[\underline{X}]/I(\ |^v)$.

Proof : Take $|^v \in V_p^{\max}(h_1, ..., h_l)$. If we verify that

$$W_p(h_1, ..., h_l) \text{ is } p\text{-bounded } \Rightarrow (\exists k \in \mathbb{Z}) : p^k \ |^v \ X_i \text{ for all } 1 \leq i \leq n,$$

then we are done, because, for all

$$f = \sum f_{i_1 ... i_n} X_1^{i_1} \cdot ... \cdot X_n^{i_n} \in \mathbb{Q}_p[\underline{X}],$$

we will have

$$\begin{aligned} v(\alpha_v(f)) &= v(f(\alpha_v(X_1), ..., \alpha_v(X_n))) \\ &\geq \min\left\{ v_p(f_{i_1 ... i_n}) + \textstyle\sum_{j=1}^n p^{k \cdot i_j} : \sum_{j=1}^n i_j \leq \deg(f) \right\} \\ &= v(p^s), \end{aligned}$$

for some $s \in \mathbb{Z}$.

In this case, the same argument as used in the proof of Proposition(3.3.2) can be applied to conclude that $\alpha_v : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p$, because of the maximality of $|^v$.

To find such k, we observe the elementary sentence

$$\varphi \ : \ \forall x_1, ..., x_n \left(\bigwedge_{1 \leq j \leq l} \mathcal{O}(h_j(x_1, ..., x_n)) \to \bigwedge_{1 \leq i \leq n} \mathcal{O}(x_i \cdot p^k) \right)$$

is satisfied by $\mathbb{Q}_p$, because $W_p(h_1, ..., h_l)$ is p-bounded.

Now observe that

$$\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p[\underline{X}]/I(\ |^v) \subseteq Quot(\mathbb{Q}_p[\underline{X}]/I(\ |^v)) =: F(\ |^v),$$

because $|^v$ restricted to $\mathbb{Q}_p$ defines a p-valuation of $\mathbb{Q}_p$ (the only p-valuation!), and hence $\mathbb{Q}_p \cap I(\ |^v) = \{0\}$. Thus $F(\ |^v)$ is a p-valued extension of $\mathbb{Q}_p$.

Let K be a p-adic closure of $F(\ |^v)$. As the theory of p-adic closed fields (of a fixed p-rank) is model complete, $\mathbb{Q}_p \subseteq K$ implies that the sentence φ is also satisfied by K.

From

$$v(h_j(\alpha_v(X_1), ..., \alpha_v(X_n))) = v(\alpha_v(h_j)) = v(h_j) \geq 0,$$

for all $1 \leq j \leq l$, we conclude that also

$$v(\alpha_v(X_i)) \geq k \text{ for all } 1 \leq i \leq n,$$

proving that $\alpha_v : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p$.

Conversely, suppose that

$$\alpha_v : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p \text{ for all } \ |^v \in V_p^{\max}(h_1, ..., h_l)$$

In particular, for all $|^v \in V_p^{\max}(h_1, ..., h_l)$ and all $g, f \in \mathbb{Q}_p[\underline{X}]$,

$$g \ |^v \ f \Leftrightarrow v_p(\alpha_v(g)) \leq v_p(\alpha_v(f)), \tag{3.23}$$

because $\mathcal{O}(\ |^v) = \mathbb{Z}_p \cap F(\ |^v) \subseteq \mathbb{Q}_p$ is the only p-valuation ring of $F(\ |^v)$.

Therefore, taking

$$U_{i,r} := \{ \ |^v \in V_p^{\max}(h_1, ..., h_r) : p^r \ |^v \ X_i\} = \mathcal{V}_{p^r, X_i}(\mathbb{Q}_p[\underline{X}]), \tag{3.24}$$

for each $r \in \mathbb{Z}$ and $1 \leq i \leq n$, we have a clopen cover

$$V_p^{\max}(h_1, ..., h_l) \subseteq \bigcup_{r \in \mathbb{Z}} U_{i,r},$$

for each fixed $1 \leq i \leq n$.

Note that

$$V_p^{\max}(h_1, ..., h_l) = \mathcal{V}_{1,h_1}(\mathbb{Q}_p[\underline{X}]) \cap ... \cap \mathcal{V}_{1,h_l}(\mathbb{Q}_p[\underline{X}]) \cap V_p^{\max}(\mathbb{Q}_p[\underline{X}])$$

is a closed subset of $V_p^{\max}(\mathbb{Q}_p[\underline{X}])$, and hence it is also quasi-compact.

By quasi-compactness, we can choose a finite subcover of $V_p^{\max}(h_1, ..., h_l)$, for each fixed $1 \leq i \leq n$, say

$$V_p^{\max}(h_1, ..., h_l) \subseteq U_{i,k_{(1,i)}} \cup \cdots \cup U_{i,k_{(r_i,i)}}, \tag{3.25}$$

for some $k_{(1,i)}, ..., k_{(r_i,i)} \in \mathbb{Z}$.

Taking

$$k_i := \min\{k_{(1,i)}, ..., k_{(r_i,i)}\}$$

for each $1 \leq i \leq n$, by (3.24) and (3.25), we see that

$$p^{k_i} \ |^v \ X_i \text{ for all } \ |^v \in V_p(h_1, ..., h_l)$$

Taking

$$k := \min\{k_i : 1 \leq i \leq n\},$$

we conclude that

$$p^k \mid^v X_i \text{ for all } \mid^v \in V_p(h_1, ..., h_l) \text{ and all } 1 \leq i \leq n,$$

and hence, by the equivalence (3.24),

$$k = v_p(p^k) \leq v_p(\alpha_v(X_i)) \text{ for all } \mid^v \in V_p(h_1, ..., h_l) \text{ and all } 1 \leq i \leq n \quad (3.26)$$

Finally observe that for each $x = (x_1, ..., x_n) \in W_p(h_1, ..., h_l)$ we can define a p-divisibility $\mid^{v_x}$ of $\mathbb{Q}_p[\underline{X}]$ putting

$$(\forall f, g \in \mathbb{Q}_p[\underline{X}]) : g \mid^{v_x} f :\Leftrightarrow v_p(g(x)) \leq v_p(f(x))$$

Of course $1 \mid^{v_x} h_1, ..., 1 \mid^{v_x} h_l$, because $h_1(x), ..., h_l(x) \in \mathbb{Z}_p$, and $\mid^{v_x}$ is also maximal by Proposition(3.3.2), because

$$\alpha_{v_x} = \alpha_x : \mathbb{Q}_p[\underline{X}] \to \mathbb{Q}_p$$

with

$$(g, f \in \mathbb{Q}_p[X]) : g \mid^{v_x} f \Leftrightarrow v_p(\alpha_{v_x}(g)) \leq v_p(\alpha_{v_x}(f)),$$

where α_x is the evaluation function on x, and hence $\mid^{v_x} \in V_p(h_1, ..., h_l)$ for all $x \in W_p(h_1, ..., h_l)$.

Thus

$$\begin{array}{rcl} x \in W_p(h_1, ..., h_l) & \Rightarrow & \mid^{v_x} \in V_p^{\max}(h_1, ..., h_l) \\ & \overset{(3.26)}{\Rightarrow} & v_p(x_i) = v_p(\alpha_{v_x}(X_i)) \geq k \text{ for all } 1 \leq i \leq n \\ & \Rightarrow & x \in p^k \mathbb{Z}_p^n \end{array}$$

■

Moreover, we can prove:

Proposition 3.6.4 *Take $h_1, ..., h_r \in \mathbb{Q}_p[\underline{X}]$. If $W_p(h_1, ..., h_r)$ is p-bounded, then*

$$W_p(h_1, ..., h_r) \simeq V_p^{\max}(h_1, ..., h_r)$$

where the homeomorphism, and its inverse, are given by

$$\mid^v \overset{\Psi}{\mapsto} (\alpha_v(X_1), ..., \alpha_v(X_n)) \ , \ x \overset{\theta}{\mapsto} \mid^{v_x}$$

Proof: In fact, if $x \in W_p(h_1,...,h_r)$, then $|^{v_x} \in V_p^{\max}(h_1,...,h_r)$, by the same argument used in the proof of Proposition(3.6.3).

As $W_p(h_1,...,h_r)$ is p-bounded, for each $|^v \in V_p^{\max}(h_1,...,h_r)$ we have

$$(\alpha_v(X_1),...,\alpha_v(X_n)) \in \mathbb{Q}_p^n,$$

by Proposition(3.6.3).

Clearly Ψ and θ are inverses of each other, because

$$\begin{array}{c} x \mapsto |^{v_x} \mapsto (\alpha_{v_x}(X_1),...,\alpha_{v_x}(X_n)) = x \\ |^v \mapsto (\alpha_{v_x}(X_1),...,\alpha_{v_x}(X_n)) =: x \mapsto |^{v_x} = |^v \end{array}$$

and being $|^v$ maximal, for every $g, f \in \mathbb{Q}_p[\underline{X}]$,

$$\begin{array}{c} g \,|^v\, f \\ \Updownarrow \\ v_p(g(\alpha_v(X_1),...,\alpha_v(X_n))) = v_p(\alpha_v(g)) \leq v_p(\alpha_v(f)) = v_p(f(\alpha_v(X_1),...,\alpha_v(X_n))) \\ \Updownarrow \\ g \,|^{v_x}\, f \end{array}$$

and hence we have a bijection.

As both are compact spaces and

$$\theta^{-1}(\mathcal{U}_{g,f}(\mathbb{Q}_p[\underline{X}])) = \{x \in W_p(h_1,...,h_r) : v_p(g(x)) > v_p(f(x))\} = \left(\frac{g}{f}\right)^{-1}(p\mathbb{Z}_p^n)$$

implies the continuity of θ, we conclude that θ is a homeomorphism.

■

Let us observe the holomorphic divisibility of $V_p(h_1,...,h_r)$ for some $h_1,...,h_r \in \mathbb{Q}_p[\underline{X}]$, i.e., the p-divisibility

$$|^* := \bigcap_{|^v \in V_p(h_1,...,h_r)} |^v$$

When $W_p(h_1,...,h_r)$ is p-bounded, this p-divisibility is well behaved, as says next proposition.

Proposition 3.6.5 *Take $h_1,...,h_r \in \mathbb{Q}_p[\underline{X}]$. If $W_p(h_1,...,h_r)$ is p-bounded, then the holomorphic divisibility of $V_p(h_1,...,h_r)$ is a SLG p-Archimedean divisibility.*

Proof : Let $|^*$ be the holomorphic divisibility of $V_p(h_1,...,h_r)$, i.e.,

$$|^* := \bigcap_{|^v \in V_p(h_1,...,h_r)} |^v$$

and suppose that $W_p(h_1,...,h_r)$ is p-bounded.

By Proposition(3.6.3), we can conclude that

$$V_p(h_1,...,h_r) \subseteq \bigcup_{n\in\mathbb{N}} \mathcal{V}_{1,ap^n}(\mathbb{Q}_p[\underline{X}])$$

and hence, being $V_p(h_1,...,h_r)$ compact, we can extract a finite subcover

$$V_p(h_1,...,h_r) \subseteq \mathcal{V}_{1,ap^{n_1}}(\mathbb{Q}_p[\underline{X}]) \cup ... \cup \mathcal{V}_{1,ap^{n_s}}(\mathbb{Q}_p[\underline{X}])$$

for some $n_1,...,n_s \in \mathbb{N}$.

Taking $n_a := \min\{n_1,...,n_s\}$ we see that

$$V_p(h_1,...,h_r) \subseteq \mathcal{V}_{1,ap^N}(\mathbb{Q}_p[\underline{X}])$$

Therefore, for all $a \in A$ there exists $n_a \in \mathbb{N}$ such that

$$1 \mid^v p^{n_a}a \text{ for all } \mid^v \in V_p^{\max}(h_1,...,h_r),$$

and hence also $1 \mid^* p^{n_a}a$, proving that $\mid^*$ is p-Archimedean.

Moreover, by Proposition(3.6.4), we know that

$$V_p(h_1,...,h_r) = \{ \mid^{v_x} : \ x \in W_p(h_1,...,h_r)\},$$

and hence, for all $g, f \in \mathbb{Q}_p[\underline{X}]$, $n, r \in \mathbb{N}$, with $r \neq 0$,

$$\begin{aligned} g^r \mid^* p^n f^r \ &\Leftrightarrow g^r \mid^{v_x} p^n f^r \text{ for all } \mid^{v_x} \in V_p(h_1,...,h_r) \\ &\Leftrightarrow v_p(g^r(x)) \geq v_p(p^n f^r(x)) \text{ for all } \mid^{v_x} \in V_p(h_1,...,h_r) \\ &\Leftrightarrow v_p(g(x)) \geq v_p(p^{\lfloor n/r \rfloor} f(x)) \text{ for all } \mid^{v_x} \in V_p(h_1,...,h_r) \\ &\Leftrightarrow g \mid^{v_x} p^{\lfloor n/r \rfloor} f \text{ for all } \mid^{v_x} \in V_p(h_1,...,h_r) \\ &\Leftrightarrow g \mid^* p^{\lfloor n/r \rfloor} f \end{aligned}$$

■

We would like to compare now such p-divisibility with the p-divisibility $\mid^B$ contained in $\mid^*$, where

$$B := \gamma(\mathbb{Q}_p[\underline{X}])[h_1,...,h_r]$$

Note that $V_p^{\max}(\ \mid^B) = V_p(h_1,...,h_r)$, what motivates the natural question

If $W_p(h_1,...,h_r)$ is p-bounded, is $\mid^B$ equal to $\mid^*$?

As $|^B$ is a p-divisibility with cancellation, we know by Corollary(3.1.7) that, for each $g, f \in \mathbb{Q}_p[\underline{X}]$, if

$$p^n \cdot \left(\frac{f}{g}\right) \in \gamma(\mathbb{Q}_p[\underline{X}])[h_1, ..., h_r] \text{ for some } n \in \mathbb{N},$$

i.e., (g, f) is a p-bounded pair of $\mathbb{Q}_p[\underline{X}]$ with respect to $|^B$, then

$$\left(\frac{f}{g}\right)(x) \in \mathbb{Z}_p \text{ for all } x \in W_p(h_1, ..., h_r) \Rightarrow \left(\frac{f}{g}\right) \in \gamma(\mathbb{Q}_p[\underline{X}])[h_1, ..., h_r]$$

However, we don't know yet if the implication above is true for all $g, f \in \mathbb{Q}_p[\underline{X}]$. Thus we have a conjecture to be proved, or disproved.

Conjecture 3.6.6 *Take $h_1, ..., h_r \in \mathbb{Q}_p[\underline{X}]$. If $W_p(h_1, ..., h_r)$ is p-bounded, then*

$$\left(\frac{f}{g}\right)(x) \in \mathbb{Z}_p \textit{ for all } x \in W_p(h_1, ..., h_r) \Rightarrow \left(\frac{f}{g}\right) \in \gamma(\mathbb{Q}_p[\underline{X}])[h_1, ..., h_r],$$

for all $g, f \in \mathbb{Q}_p[\underline{X}]$.

Appendix A

Alternative Descriptions of Divisibilities

There are another ways of interpreting divisibilities and they may be useful if someone is interested into finding examples of abstract divisibilities or to understand them using another point of view.

In this appendix, we would like to show an equivalent notion of divisibility, namely, of divisibility maps, which is very similar to the notion of (Bourbaki) valuations of commutative rings.

Such maps seem to have a better intuitive appeal for who is familiar with valuation maps.

What we actually do to define divisibility maps is to change the ordered abelian group, used for valuation maps, by a partially ordered abelian monoid, the infinity symbols ∞ by the 0 of the multiplicative monoid, and the second condition of valuations by another weaker condition.[1]

More precisely:

Definition A.1 *Let $(M, \cdot, \leq)$ a partially ordered (p.o.) abelian monoid with zero 0. A **divisibility map** of A is a surjective map $\delta : A \to M$ satisfying*

1. $\delta(a \cdot b) = \delta(a) \cdot \delta(b)$
2. $\delta(a) \leq \delta(b),\ \delta(a) \leq \delta(c) \Rightarrow \delta(a) \leq \delta(b \pm c)$
3. $0 \not\leq 1$

Note that we allready have $\delta(1) = 1$ and $\delta(0) = 0$ because of the surjectivity of δ.

[1] A theory of monoids can be found, for example, in [7] or [23].

In Example(2.1.11)(18), we have seen that a divisibility map δ always defines a divisibility $|^\delta$ of A putting

$$(\forall a, b \in A) : a \mid^\delta b :\Leftrightarrow \delta(a) \leq \delta(b)$$

The next theorem shows that the converse is also true, i.e., for each divisibility $\mid$ of A we can define a divisibility map $\delta(\ \mid\ )$.

Theorem A.2 *For each divisibility $\mid$ of A there is an associated divisibility map $\delta(\ \mid\ ) : A \to D$, for some partially ordered abelian monoid $(D,\ \cdot\ , \leq)$, such that*

$$a \mid b \Leftrightarrow \delta(a) \leq \delta(b)$$

Proof : Let $\mid$ be a divisibility on A. For each $a, b \in A$ define

$$a \mid\mid b :\Leftrightarrow (a \mid b) \wedge (b \mid a)$$

From the transitivity and reflexivity of $\mid$ follows that $\mid\mid$ defines an equivalence relation on A. Let $\delta(a)$ denote the equivalence class of some $a \in A$ and $\delta(A)$ the set of equivalence classes of A under this relation.

We define an operation $\odot : \delta(A) \times \delta(A) \to \delta(A)$ by

$$(\delta(a), \delta(b)) \mapsto \delta(a) \odot \delta(b) := \delta(ab)$$

Taking $a, a', b, b' \in A$ such that $\delta(a) = \delta(a')$ and $\delta(b) = \delta(b')$, then

$$a \mid a', b \mid b' \Rightarrow ab \mid ab' \mid a'b' \ \text{ and } \ a' \mid a, b' \mid b \Rightarrow a'b' \mid ab' \mid ab$$

and hence $ab \mid\mid a'b'$, i.e., $\delta(ab) = \delta(a'b')$. Thus $\odot$ is well-defined on $\delta(A)$.

By definition the map $\delta : (A,\ \cdot\ ) \to (\delta(A), \odot)$ is an epimorphism, and hence $(\delta(A), \odot)$ is an abelian monoid. We define a partial order on $\delta(A)$ associated to $\mid$ declaring

$$(\forall a, b \in A) : \delta(a) \leq \delta(b) :\Leftrightarrow a \mid b$$

It is well-defined, because, if $a \mid\mid a'$ and $b \mid\mid b'$, then $a \mid b \Leftrightarrow a' \mid b'$. By properties (2.1), (2.2, (2.4), (2.5) of divisibilities it follows that $(\delta(A), \odot, \leq)$ is a partially ordered monoid with $0_\delta \not\leq 1_\delta$.

Moreover, for all $a, b, c \in A$,

$$\delta(a) \leq \delta(b),\ \ \delta(a) \leq \delta(c) \Rightarrow a \mid b,\ \ a \mid c \Rightarrow a \mid (b \pm c) \Rightarrow \delta(a) \leq \delta(b \pm c)$$

and therefore δ is a divisibility map.

■

In the valuation case, there is a 1-1 correspondence between valuation rings and equivalence classes of valuation maps. Here the same will be true if we define:

Definition A.3 *Two divisibility maps $\delta_1 : A \to D_1$ and $\delta_2 : A \to D_2$ are* ***equivalent*** *if there is some order-isomorphism $\rho : D_1 \to D_2$ such that $\delta_2 = \rho \circ \delta_1$. In this case we write $\delta_1 \equiv \delta_2$.*

In the next theorem we use the same letter to denote th divisibility map δ and its equivalence class.

Theorem A.4 *The maps*

$$| \overset{\alpha}{\mapsto} \delta(\ |\ ) \ , \ \delta \overset{\beta}{\mapsto} |^{\delta}$$

induce bijections between the set of divisibilities of A and the sets of equivalent divisibility maps of A.

Proof : Suppose that δ is equivalent to γ, i.e., there is an order-isomorphism $\rho : \gamma(A) \to \delta(A)$ such that $\delta = \rho \circ \gamma$.

Then, for all $a, b \in A$,

$$a \mid^{\delta} b \Leftrightarrow \rho(\gamma(a)) = \delta(a) \leq_{\delta} \delta(b) = \rho(\gamma(b)) \Leftrightarrow \gamma(a) \leq_{\gamma} \gamma(b) \Leftrightarrow a \mid^{\gamma} b$$

and hence β is well-defined.

For each divisibility map $\delta : A \to \delta(A)$, divisibility $|$ of A and $a, b \in A$

$$a \mid b \Leftrightarrow \delta(\ |\ )(a) \leq \delta(\ |\ )(b) \Leftrightarrow a \mid^{\delta(\ |\ )} b$$
$$\delta(a) \leq \delta(b) \Leftrightarrow a \mid^{\delta} b \Leftrightarrow \delta(\ |^{\delta}\ )(a) \leq \delta(\ |^{\delta}\ )(b)$$

From the first we conclude that $| = |^{\delta(\ |\ )}$, i.e., $\alpha \circ \beta = id$. From the second

$$\delta(a) = \delta(b) \Leftrightarrow \delta(\ |^{\delta}\ )(a) = \delta(\ |^{\delta}\ )(b), \tag{A.1}$$

We define then

$$\rho : \delta(A) \to \delta(\ |^{\delta})(A) \ , \ \delta(a) \mapsto \delta(\ |^{\delta})(a)$$

It follows at once from (A.1) that ρ is a bijection and it is well-defined. Moreover,

$$\rho(\delta(a) \cdot \delta(b)) = \rho(\delta(ab)) \mapsto \delta(\ |^{\delta})(ab) = \delta(\ |^{\delta})(a) \cdot \delta(\ |^{\delta})(b)$$

and hence ρ is a homomorphism, and as the same argument can be used for ρ^{-1}, we have an isomorphism, which implies the equality of the equivalence classes of δ and $\delta(\ |^{\delta})$.

Thus $\beta \circ \alpha = id$ and hence α and β are inverses of each other.

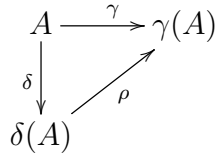
■

Remark A.5 *δ_1 and δ_2 are equivalent if, and only if, $|^{\delta_1} = |^{\delta_2}$.*

Definition A.6 *Let δ, γ be two divisibility maps of A. We say that γ **extends** δ if, and only if, $|^{\delta} \subseteq |^{\gamma}$.*

The relationship between a divisibility an extension of itself can be described via the diagram of the next proposition.

Proposition A.7 *Let $\delta : A \to \delta(A)$ and $\gamma : A \to \gamma(A)$ be two divisibility maps of A. Then γ extends δ if, and only if, there is an order-preserving epimorphism $\rho : \delta(A) \to \gamma(A)$ such that the following diagram commutes*



Proof : If there is such order-preserving epimorphism $\rho : \delta(A) \to \gamma(A)$ then

$$a \,|^{\delta}\, b \Leftrightarrow \delta(a) \leq_{\delta} \delta(b) \Rightarrow \gamma(a) = \rho(\delta(a)) \leq_{\gamma} \rho(\delta(b)) = \gamma(b) \Leftrightarrow a \,|^{\gamma}\, b$$

for all $a, b \in A$.

Conversely, suppose that $|^{\delta} \subseteq |^{\gamma}$. Define $\rho : \delta(A) \to \gamma(A)$ by $\delta(a) \mapsto \gamma(a)$ for all $a \in A$. We claim that it is well-defined, because

$$\delta(a) = \delta(b) \Leftrightarrow a \,||^{\delta}\, b \Rightarrow a \,||^{\gamma}\, b \Leftrightarrow \gamma(a) = \gamma(b)$$

for all $a, b \in A$. By its definition ρ is an epimorphism satisfying $\rho \circ \delta = \gamma$ and respects the ordering, as the following shows

$$\delta(a) \leq_{\delta} \delta(b) \Leftrightarrow a \,|^{\delta}\, b \Rightarrow a \,|^{\gamma}\, b \Leftrightarrow \gamma(a) \leq_{\gamma} \gamma(b)$$

■

We also note that we can always define the operator $\mathfrak{S}$ just using the divisibility maps δ, instead of its associated binary relation $|$, and hence all the results using $\mathfrak{S}$ could be written using divisibility maps.

In fact, If $|$ is a divisibility of A, we can see that,

$$\forall X \in \mathcal{P}(A) : \mathbb{M}(X) = \delta^{-1}(U(X))$$

where

$$U(X) := \{\gamma \in M : \gamma \geq \delta(x) \text{ for some } x \in X\}$$

and δ is some divisibility map associated to $|$.

Now, the last thing we want to do in this appendix is to exhibit the divisibility map of the divisibility $|^d$ of Example(2.1.11)(15), defined by the map $d : \mathbb{Z}_p[X] \to \mathbb{Z}$, where

$$d(a_0 + a_1X + ... + a_nX^n) = \begin{cases} -n & \text{if } n > 0 \\ v_p(a_0) & \text{if } n = 0 \end{cases}$$

The first observation is that d is **not** a divisibility map from A to the ordered abelian group $(\mathbb{Z}, +, \leq)$, because d is **not** a monoid homomorphism between the monoids $(A, \cdot)$ and $(\mathbb{Z}, +)$. In fact,

$$-1 = d(X \cdot p) \neq d(X) + d(p) = -1 + 1 = 0$$

Actually $\mathbb{Z}$ must be seen as just the universe of the commutative monoid $(\mathbb{Z}, \oplus, \leq)$ of our divisibility map, where $\oplus$ is not necessarily the usual addition or the usual multiplication.

However, taking $\leq$ as the usual order relation of $\mathbb{Z}$ and $\oplus$ as the operation defined, for all $n, m \in \mathbb{Z}$, by

$$n \oplus m = \begin{cases} n + m & \text{, if } s(n) = s(m) \\ \min\{n, m\} & \text{, if } s(n) \neq s(m) \end{cases}$$

where

$$s(n) := \begin{cases} 1 & \text{, if } n \geq 0 \\ -1 & \text{, if } n < 0 \end{cases}$$

the reader can easily verify, using an operation table, that $(\mathbb{Z}, \oplus, \leq)$ is an ordered abelian monoid.

Moreover, the map $d : \mathbb{Z}_p[X] \to (\mathbb{Z}, \oplus, \leq)$ is indeed a divisibility map associated to $|^d$!

Appendix B

A Minimum Principle

In this appendix, we give a minimum principle for total divisibilities. Although total divisibilities are not of our main interest, this principle can be useful, at least to simplify some calculation with $\mathfrak{S}$, when this is defined using a total divisibility $|$.

First we remember the part of Definition(2.1.4) related to totality.

Definition B.1 *Let $|$ be a divisibility of A and $X \subseteq A$. Then $|$ is called* ***total on*** *X if*

$$(\forall x, y \in X) : (x \mid y) \vee (y \mid x)$$

Clearly $|$ is total if, and only if, $|$ is total on A.

The next proposition is actually the main result.

Proposition B.2 *Let $|$ be a divisibility of A. If $|$ is total on $X \subseteq A$, then*

$$\mathfrak{S}(X) = \mathfrak{S}\left(\bigcup_{x \in X} \{x\}\right) = \bigcup_{x \in X} \mathfrak{S}(x)$$

Proof : If $y \in \mathfrak{S}(X)$ then there are $x_1, ..., x_n \in X$ such that

$$y \in \mathfrak{S}(x_1, ..., x_n)$$

If $n = 1$ then $y \in \mathfrak{S}(x_1) \subseteq \bigcup_{x \in X} \mathfrak{S}(x)$. Suppose that for all sets with $1 \leq r \leq n$ elements we have

$$\mathfrak{S}(x_1, ..., x_r) = \bigcup_{1 \leq i \leq r} \mathfrak{S}(x_i)$$

If we take $x_1, ..., x_n, x_{n+1} \in A$, then we can suppose, without loss of generality, that $x_n \mid x_{n+1}$. Therefore

$$y \in \mathfrak{S}(x_1, ..., x_n, x_{n+1}) \subseteq \mathfrak{S}(x_1, ..., x_n, x_n) = \mathfrak{S}(x_1, ..., x_n) = \bigcup_{1 \leq i \leq n} \mathfrak{S}(x_i)$$

■

The minimum principle that we want is the following consequence of the last proposition.

Theorem B.3 (Minimum Principle) *Let $\mid$ be a divisibility of A and $X \subseteq A$. Then*

$$\forall \ |^v \in V(\ \mid\ ) : \left(y \in \mathfrak{S}(X) \Rightarrow \bigvee_{x \in X} x \ |^v \ y \right)$$

Proof : As $|^v$ is total on each subset $X \subseteq A$ for all $|^v \in V(\ \mid\ )$, we conclude that

$$\mathfrak{S}_v(X) = \bigcup_{x \in X} \mathfrak{S}_v(x)$$

by Proposition(B.2).

Now, by Remark(2.2.8), we have $\mathfrak{S}(X) \subseteq \mathfrak{S}_v(X)$, and then follows the conclusion.

■

Lastly, we would like to note that in general total divisibilities do not have a prime support. However, their supports have a property closer to primality, namely,

Proposition B.4 *If $\mid$ is total, then*

$$ab \in I(\ \mid\ ) \Rightarrow a^2 \in I(\ \mid\ ) \text{ or } b^2 \in I(\ \mid\ )$$

Proof : For each $a, b \in A$, $a \mid b$ or $b \mid a$. Then

$$0 \mid ab \Rightarrow (0 \mid ab \mid a^2) \vee (0 \mid ab \mid b^2)$$

■

Appendix C

Kaplansky's Lemma

In this appendix, we prove the theorem used in the p-adic Representation Theorem, assuring that each subalgebra of $C_X := C(X, \mathbb{Q}_p)$ separating points is dense in C_X, when X is a compact space.

We prove a more general version[1] that holds for each $C(X, K)$, where K is a field with a non-Archimedean absolute value $|\cdot|$, or equivalently, with a valuation v of rank 1.

The main result used in the proof of this theorem is the following lemma due to I. Kaplansky[2].

Lemma C.1 *Let $(F, |\cdot|)$ be a non-Archimedean valued field and $x \in F\backslash\{0\}$ a fixed element. Then, for each compact subset $K \subseteq F$, there is a polynomial $f \in F[X]$ such that*

- $f(x) = 1$.
- $f(0) = 0$.
- $|f(k)| \leq 1$ *for all* $k \in K$.

Proof : Let v be the valuation corresponding to $|\cdot|$ and [3]

$$\mathcal{O}_v := \{a \in F : |a| \leq 1\},\ \mathcal{M} := \{a \in F : |a| < 1\}$$

its valuations ring and maximal ideal, respectively.

Take $x \in F\backslash\{0\}$ and $K \subseteq F$ compact. For each $c \in K$, the sets

$$c \in U_c := \{k \in K : v(k) = v(c)\},$$

[1] Such known result can be found in [3] or [21].

[2] As in his article [10].

[3] If $|\cdot|$ is an absolute value, then $v(\cdot) := -\ln|\cdot|$ is the valuation of rank 1 corresponding to $|\cdot|$. For more details see Chapter(1) of [19].

are clopen set in K, and then

$$K = \bigcup_{c \in K} U_c \overset{K \text{ compact}}{\Rightarrow} K = \bigcup_{1 \leq i \leq n} U_{c_i}, \text{ for some } c_i \in K,$$

As U_{c_i} is closed in K, it is also compact in F, and hence $1 - c_i^{-1}U_{c_i}$ is compact too, because

$$x \mapsto c_i^{-1}x \text{ and } x \mapsto 1 - x$$

are homeomorphisms.

Now note that

$$U_c \subseteq c(1 + \mathcal{M}_v)$$

for all $c \in K$, and hence $1 - c_i^{-1}U_{c_i} \subseteq \mathcal{M}_v$, for each $c_i \neq 0$.

Thus,

$$1 - c_i^{-1}U_{c_i} \subseteq \bigcup_{m \in \mathcal{M}_v} \{a \in F : v(a) \geq v(m)\} = \mathcal{M}_v$$

implies, by its compactness, the existence of $m_1, ..., m_{l_i} \in \mathcal{M}$ such that

$$1 - c_i^{-1}U_{c_i} \subseteq \bigcup_{1 \leq j \leq l_i} \{a \in F : v(a) \geq v(m_j),\ m_j \in \mathcal{M}_v\},$$

and then, for each $i \in \{1, ..., n\}$, there is

$$\min\{v(m_j) : 1 \leq j \leq l_i\} =: \alpha_i \in \mathbb{Z}^+$$

such that

$$v(x) \geq \alpha_i > 0 \text{ for all } x \in 1 - c_i^{-1}U_{c_i}$$

We can suppose that the c_i's are numbered such that

$$v(c_1) \geq ... \geq v(c_n) \tag{C.1}$$

We take just the c_i's different to zero. Thus, without loss of generality, we can suppose that $c_1 \neq 0$.

Then, the Proposition follows from the next claim.

Claim C.2 *There are $n_1, ..., n_r \in \mathbb{N}$ such that*

$$f(x) := 1 - (1 - x^{-1}X)(1 - c_1^{-1}X)^{n_1}...(1 - c_r^{-1}X)^{n_r}$$

satisfies the conditions of the Proposition.

In fact, $f(x) = 1$ and $f(0) = 0$, and hence it is enough to choose the n_i's such that

$$|f(k)| \leq 1 \text{ for all } k \in K,$$

or equivalently, $v(f(k)) \geq 0$ for all $k \in K$.

Thus, it is sufficient to verify that

$$v(1 - x^{-1}k) + n_1 \cdot v(1 - c_1^{-1}k) + ... + n_r \cdot (1 - c_r^{-1}k) \geq 0, \tag{C.2}$$

for all $0 \neq k \in K$.

As $\alpha_i > 0$, for each $0 \leq i \leq n$, we can define n_i recursively by

$$\begin{array}{rcl} i = 1 & : & \text{Take } n_1 \text{ such that } v(x^{-1}c_1) + n_1\alpha_1 \geq 0 \\ i = 2 & : & \text{Take } n_2 \text{ such that } v(x^{-1}c_2) + n_1 \cdot v(c_2^{-1}c_1) + n_2\alpha_2 \geq 0 \\ \vdots & & \\ i = r & : & \text{Take } n_r \text{ such that } v(x^{-1}c_r) + \sum_{j=1}^{r-1} n_j \cdot v(c_j^{-1}c_r) + n_r\alpha_r \geq 0 \end{array}$$

With such choice, (C.2) is true. In fact, if

$$0 \neq k \in K = \bigcup_{1 \leq i \leq r} U_r,$$

then $k \in U_i$, for some i, and hence

$$v(k) = v(c_i),\ v(1 - c_i^{-1}k) \geq \alpha_i \text{ and } v(c_j^{-1}c_i) = v(c_j^{-1}k) \text{ for all } 1 \leq j \leq r$$

Moreover, by our assumption in (C.1),

$$0 \leq v(c_j^{-1}c_i) = v(c_j^{-1}k), \text{ for all } j \geq i$$

Thus,

$$v(x^{-1}c_i) + \sum_{j=1}^{i-1} n_j \cdot v(c_j^{-1}c_i) + n_i\alpha_i \geq 0$$

implies (C.2).

■

Let X be a compact space and $(F, |\cdot|)$ a non-Archimedean valued field with associated valuation v of rank 1, where $|\cdot| := e^{v(\ \cdot\ )}$.

We endow the ring of continuous functions $C(X, F)$ with the topology given by the sup-norm

$$||f|| := sup\{|f(x)| \ : \ x \in X\}.$$

Then we have the following analogous to Stone-Weierstrass theorem in this case also due to I. Kaplansky.[4]

[4]The proof of this theorem was adapted from Chapter(9) §2 of [21].

Theorem C.3 *Let $(F, |\cdot|)$ be a non-Archimedean valued field and X a compact space. Let $A \subseteq C(X, F)$ be a F-algebra with $1 \in A$ and separating points of X. Then A is dense in $C(X, F)$ with respect to the sup-norm.*

Proof: Take $f \in A$. Since X is compact, $f(X) \subseteq F$ is compact. Now, for every $\epsilon > 0$,

$$f(X) \subseteq \bigcup_{t \in X} B_\epsilon(f(t)),$$

where $B_\epsilon(f(t))$ is the open ball of radius ϵ and center $f(t)$.

By compactness of $f(X)$, there are $t_1, ..., t_n \in X$ such that

$$f(X) \subseteq B_\epsilon(f(t_1)) \cup \cdots \cup B_\epsilon(f(t_n)).$$

Let $B_1 := B_\epsilon(f(t_1))$ and, for each $2 \leq i \leq n$,

$$B_i := B_\epsilon(f(t_i)) - \bigcup_{j<i} B_\epsilon(f(t_j)).$$

Then B_i are pairwise disjoint and clopen, and their union covers $f(X)$. Therefore, the union of the sets $U_i := f^{-1}(B_i)$ forms a pairwise disjoint clopen cover of X.

If $t \in X$, then $t \in U_i$ for some $1 \leq i \leq n$ and $t \notin U_j$ for all $j \neq i$. Thus, if $\chi_k := \chi_{U_k}$ is the characteristic function of U_k, we have $\chi_i(t) = 1$ and $\chi_j(t) = 0$ for all $j \neq i$.

Now, $t \in U_i$ implies $|f(t) - f(t_i)| \leq \epsilon$ and then $|f(t) - g(t)| \leq \epsilon$, where

$$g := \sum_{k=1}^{n} f(t_k) \cdot \chi_k.$$

Therefore, it is sufficient to prove that g is in the closure of A in $C(X, F)$. To show this, it is enough to see that χ_k is in the closure of A for each $1 \leq k \leq n$.

Let U be a clopen subset of X and $0 < \epsilon < 1$. Fix $x \in X$ with $x \notin U$. For each $t \in U$, as $t \neq x$ and A is a separating unitary algebra ($1 \in A$) of $C(X, F)$, there is $g_t \in A$ such that

$$g_t(t) = 0 \text{ and } g_t(x) = 1$$

In fact, there is $h \in A$ such that $h(x) \neq h(t)$, and then we can take

$$g_t := \frac{h - h(t)}{h(x) - h(t)}$$

By Kaplansky's lemma, i.e., Lemma(C.1), there exists a polynomial $p_t : F \to F$, whose constant term is zero, $p_t(1) = 1$ and $|p_t(s)| \leq 1$ for all s in the compact set $g_t(X) \subseteq F$.

Then $f_t = p_t \circ g_t$ belongs to A, $f_t(t) = 0$, $f_t(x) = 1$ and

$$||f_t|| = sup\{|f_t(y)| \ : \ y \in X\} \leq 1.$$

By continuity of f_t, there exists a neighborhood N_t of t such that $f_t(y) < \epsilon$ for all $y \in N_t$.

Since U is compact, there are $t_1, ..., t_n \in U$ such that

$$U \subseteq N_{t_1} \cup \cdots \cup N_{t_n}$$

If

$$f_x = f_{t_1} \cdot ... \cdot f_{t_n},$$

then

$$f_x \in A, \ f_x(x) = 1, \ \|f(x)\| \leq 1 \text{ and } |f_x(y)| < \epsilon \text{ for all } y \in U$$

Now $h_x = 1 - f_x$ belongs to A too, since $1 \in A$. Moreover,

$$h_x(x) = 0 \text{ and } |1 - h_x(y)| < \epsilon \text{ for all } y \in U$$

By continuity of h_x, there exists an open neighborhood W_x of x such that $|h_x(y)| < \epsilon$ for all $y \in W_x$. Since $X \backslash U$ is compact, there are $x_1, ..., x_m \in X \backslash U$ such that

$$X \backslash U \subseteq W_{x_1} \cup \cdots \cup W_{x_m}.$$

Define $h = h_{x_1} \cdot ... \cdot h_{x_m}$. Then $h \in A$. Moreover, if $y \notin U$, then $y \in W_{x_i}$ for some $1 \leq i \leq m$ and $|h_{x_i}(y)| < \epsilon$, because $||h_{x_i}|| \leq 1$ for all i. Thus

$$|h(y)| < \epsilon \text{ for all } y \notin U \tag{C.3}$$

On the other hand, if $y \in U$, then $|1 - h_{x_i}(y)| < \epsilon$ for all $1 \leq i \leq m$. We claim that

$$|1 - h_{x_1}(y) \cdot ... \cdot h_{x_k}(y)| < \epsilon, \ \text{ for all } 1 \leq k \leq m.$$

This is clear for $k = 1$. Suppose the claim is true for $1 \leq k < m$. Then

$$\begin{array}{ll} & |1 - h_{x_1}(y) \cdot ... \cdot h_{x_{k+1}}(y)| = \\ = & |1 - h_{x_{k+1}}(y) + h_{x_{k+1}}(y) - h_{x_1}(y) \cdot ... \cdot h_{x_k}(y) \cdot h_{x_{k+1}}(y)| \\ \leq & \max\{|1 - h_{x_{k+1}}(y)|, |h_{x_{k+1}}(y)| \cdot |1 - h_{x_1}(y) \cdot ... \cdot h_{x_k}(y)|\} \\ \leq & \max\{|1 - h_{x_{k+1}}(y)|, |1 - h_{x_1}(y) \cdot ... \cdot h_{x_k}(y)|\}, \end{array}$$

because $|h_{x_{k+1}}(y)| \leq 1$.

By induction hypothesis $|1 - h_{x_1}(y) \cdot ... \cdot h_{x_k}(y)| < \epsilon$, and then the claim is true for $k+1$. In particular, for $k = m$

$$|1 - h(y)| < \epsilon \text{ for all } y \in U \tag{C.4}$$

From (C.3) and (C.4), we see that $||\chi_U - h|| < \epsilon$ for all $0 < \epsilon < 1$ and all clopen $U \subseteq X$.

■

As a corollary we have.

Corollary C.4 *Let A be an unitary $\mathbb{Q}$-subalgebra of the ring of p-adic valued continuous functions $C(X, \mathbb{Q}_p)$, where X is a compact space.*

If A separates points of X, then it is a dense $\mathbb{Q}$-subalgebra of $C(X, \mathbb{Q}_p)$ with respect to the p-adic sup-norm induced by the p-adic absolute value $|\cdot|_p$, i.e., the norm $\|\cdot\|$ given by

$$\|f\| = \sup\{|f(x)|_p : x \in X\}$$

for all $f \in C(X, \mathbb{Q}_p)$.

Proof: If A is an unitary $\mathbb{Q}$-subalgebra of $C(X, \mathbb{Q}_p)$ separating points of X, then $B := \mathbb{Q}_p \cdot A$ [5] is an unitary $\mathbb{Q}_p$-subalgebra of $C(X, \mathbb{Q}_p)$ separating points of X (For each $x \neq y$ take some separating function $f \in A$).

As X is compact, Theorem(C.3) assures that B is dense in $C(X, \mathbb{Q}_p)$. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it follows that $\mathbb{Q} \cdot A = A$ is dense in $\mathbb{Q}_p \cdot A = B$, and hence A is dense in $C(X, \mathbb{Q}_p)$.

■

[5] Here we use $\mathbb{Q}_p \cdot A$ to denote the $\mathbb{Q}_p$-vector space generated by A, and not the set $\{\alpha \cdot a : \alpha \in \mathbb{Q}_p \text{ and } a \in A\}$, as used in the other parts of this dissertation.

Bibliography

[1] F. Albiac, N. J. Kalton, *A Characterization of Real $\mathcal{C}(K)$-Spaces*, The American Mathematical Monthly, Vol. 114, No. 8, 737-743, Oct., (2007): http://www.jstor.org/stable/27642310

[2] N. Bourbaki, *Elements of Mathematics: Commutative Algebra*, Chapters 1-7, Softcover ed. of the 2. print., Springer-Verlag Berlin Heidelberg (1989).

[3] P. R. Chernoff, R. A. Rasala, W. C. Waterhouse, *The Stone-Weierstrass theorem for valuable fields*, Pacific J. Math. Vol. 27, Number 2, 233-240 (1968).

[4] A. J. Engler, A. Prestel: *Valued Fields*, Monographs in Mathematics, Springer-Verlag Berlin Heidelberg (2005).

[5] L. Fuchs, *Partially Ordered Algebraic Systems*, International Series of Monographs on Pure and Applied Mathematics - 28, Pergamon Press, Oxford; New York (1963).

[6] F. Q. Gouvêa, *p-adic Numbers: An Introduction*, Universitext, Springer-Verlag Berlin Heidelberg; (1997).

[7] T. Harju, *Lecture Notes on Semigroups*, University of Turku, Finland (1996) : http://users.utu.fi/harju/semigroups/semigroups.pdf

[8] E. Hewitt, *Rings of Real-Valued Continuous Functions. I*, Transactions of the American Mathematical Society, Vol. 64, No. 1 (Jul., 1948), pp. 45-99 : http://www.jstor.org/stable/1990558

[9] P. T. Johnstone, *Stone Spaces* ,Cambridge Studies in Advanced Mathematics 3, Cambridge University Press (1982).

[10] I. Kaplansky, *The Weierstrass Theorem in Fields with Valuations*, Proc. Amer. Math. Soc. 1, 356-357 (1950).

[11] S. Kochen, *Integer Valued Rational Functions over the p-adic Numbers: A p-adic Analogue of the Theory of Real Fields*, Proc. Symp. Pure Math. XII, 57-73, AMS (1969).

[12] M. Knebusch, D. Zhang, *Manis Valuation and Prüfer Extensions I: A New Chapter in Commutative Algebra*, Lecture Notes in Mathematics - 1791, Springer-Verlag Berlin Heidelberg (2002).

[13] S. Lang, *Real and Functional Analysis*, Graduate Texts in Mathematics 142, Third Edition, Springer-Verlag New York, Inc. (1993).

[14] M. D. Larsen, P. J. McCarthy, *Multiplicative Theory of Ideals*, Monographs and Textbooks, Academic Press Inc., New York (1971).

[15] M. Marshall, *Positive Polynomials and Sums of Squares*, Mathematical Surveys and Monographs, Vol. 146, AMS (2008).

[16] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften - 322, *A Series of Comprehensive Studies in Mathematics*, Springer-Verlag Berlin Heidelberg (1999).

[17] A. Prestel, C. N. Delzell: *Mathematical Logic and Model Theory: A Brief Introduction*, Universitext, Springer-Verlag London (2011).

[18] A. Prestel, C. N. Delzell: *Positive Polynomials: From Hilbert's 17th Problem to Real Algebra*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg (2001).

[19] A.Prestel, A. J. Engler, *Valued Fields*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg (2005).

[20] A. Prestel, P. Roquette: *Formally p-adic Fields*, Lecture Notes in Mathematics, Springer-Verlag Berlin Heidelberg (1984).

[21] J. B. Prolla, *Approximation of Vector Valued Functions*, Mathematics Studies No. 25, North-Holland Amsterdan (1977).

[22] A. M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics - 198, Springer - Verlag New York (2000).

[23] J. C. Rosales, P. A. Gárcia-Sánchez, *Finitely Generated Commutative Monoids*, Nova Science Publishers, Inc., New York (1999).

[24] M. H. Stone, *A General Theory of Spectra I*, Proceedings of the National Academy of Sciences of the United States of America, Vol. 26, No. 4, Apr. 15, (1940).

[25] M. H. Stone, *The Generalized Weierstrass Approximation Theorem*, Mathematics Magazine, Vol. 21 , No. 4, pp. 167 - 184 (1948).

[26] M. H. Stone, *Applications of the theory of Boolean Rings to General Topology*, Trans. Am. Math. Soc. - 41, 375-481 (1937).

[27] A. C. M. Van Rooij, *Non-Archimedean functional analysis*, Monographs and Textbooks in Pure and Applied Mathematics - 51, M. Dekker, New York (1978).