Algebraic Characterization of Rings of Continuous p-adic Valued Functions

Samuel Volkweis Leite[1] and Alexander Prestel

Abstract The aim of this paper is to characterize among the class of all commutative rings containing $\mathbb{Q}$ the rings $C(X, \mathbb{Q}_p)$ of all continuous $\mathbb{Q}_p$-valued functions on a compact space X. The characterization is similar to that of M. Stone from 1940 (see [St]) for the case of $\mathbb{R}$-valued functions. The Characterization Theorem 4.6 is a consequence of our main result, the p-adic Representation Theorem 4.5.

1 Introduction

The ring $C(X, \mathbb{R})$ of all $\mathbb{R}$-valued continuous functions on a compact space X is an $\mathbb{R}$-Banach algebra. Not surprisingly there are numerous characterizations of these rings among the class of all $\mathbb{R}$-Banach algebras (see e.g. [A-K]). What is, however, surprising is M. Stone's purely algebraic characterization of the rings $C(X, \mathbb{R})$ among the class of all commutative rings A containing $\mathbb{Q}$. The secret of Stone's approach is that he encodes the space X in a simple algebraic subset T of A. Let us briefly indicate this approach in modern language.

A subset T of a commutative ring A with $\mathbb{Q} \subseteq A$ is called a *pre-ordering* of A if it satisfies

$$T + T \subseteq T, \quad T \cdot T \subseteq T, \quad a^2 \in T \text{ for all } a \in A, \quad -1 \notin T.$$

If the set of sums of squares of A does not contain -1, this set is a pre-ordering of A. In case of $A = C(X, \mathbb{R})$, the set of squares already forms a pre-ordering [2]. The totality of pre-orderings on A is partially ordered by inclusion and it carries a natural topology making it a quasi-compact space. For a fixed pre-ordering T_0, the *real spectrum* of (A, T_0) is the closed set of pre-orderings $P \supseteq T_0$ satisfying in addition $P \cup -P = A$ and $P \cap -P$ a prime ideal of A. These objects are usually called *orderings* of A (see [P-D]). The maximal spectrum X of (A, T_0) yields an isomorphism $A \cong C(X, \mathbb{R})$ if T_0 satisfies the conditions required by Stone. Without going into further details let us mention only the crucial step in proving this isomorphism.

T_0 is called *archimedean* if to every $a \in A$ there exists some $n \in \mathbb{N}$ such that $n - a \in T_0$. Then the crucial step is the *Local-Global-Principle*: If $a \in A$ is strictly positive for all $P \in X$ (i.e. $a \in P \setminus (-P)$), then $a \in T_0$. In this sense the pre-ordering T_0 encodes the space X. In case of the polynomial ring $A = \mathbb{R}[X_1, \ldots, X_n]$, for suitable T_0 this principle is Schmüdgen's famous Positivstellensatz (see [P-D], Theorem 5.2.9).

[1] This paper contains the main result of the Ph.D. Thesis [L] of the first author written under the supervision of the second author.

[2] Although pre-orderings on commutative rings have already been used by M. Stone, the notation "pre-ordering" was introduced much later by Krivine in a systematic study [Kr].

In the present paper we treat in a similar way the rings $C(X, \mathbb{Q}_p)$ of all $\mathbb{Q}_p$-valued continuous functions on a compact space X. We end up with a purely algebraic characterization of these rings among the class of commutative rings A containing $\mathbb{Q}$. In order to achieve this, we introduce certain subsets $|$ of $A \times A$ called *p-divisibilities* [3]. The totality $D_p(A)$ of p-divisibilities on A is partially ordered by inclusion and admits a canonical topology making it a quasi-compact space. We call a p-divisibility $|$ a *p-valuation*(-divisibility) if for all $a, b \in A$ we have *totality*: $a \mid b$ or $b \mid a$, and *cancellation*: $0 \nmid c,\ ac \mid bc \Rightarrow a \mid b$.
The class of p-valuations $|$ extending a given p-divisibility $|_0$ forms a closed subspace Spec $D_p(A, |_0)$, called the p-adic valuation spectrum above $|_0$. Let X denote the maximal spectrum $\mathrm{Spec}^{\max} D_p(A, |_0)$. Finally we call $|_0$ *p-archimedean* if for all $a \in A$ there exists $n \in \mathbb{N}$ such that $p^{-n} \mid a$. The crucial step in our approach then is the *Local-Global-Principle:*

$$\text{If } p \mid a \text{ for all } | \in X, \text{ then } p \mid_0 a.$$

This principle is essential for encoding the p-adic valuation spectrum above $|_0$ in the simple algebraic notion of the p-divisibility $|_0$. Compared with the pre-ordering case, the extension theory of p-divisibilities is considerably more difficult. In case of the integral domain $A = \mathbb{Q}_p[X_1, \ldots, X_n]$ the local-global-principle parallels Roquette's profound result on the "Kochen-ring" of $\mathbb{Q}_p(X_1, \ldots, X_n)$ in [R].

Concerning applications of the Local-Global-Principle (real or p-adic) everything depends on the demonstration of the archimedean property of T_0 or $|_0$, resp. In the well treated real situation some striking cases are known. Most interesting of all is Schmüdgen's result that the preordering T_0 corresponding to a basic closed semi-algebraic subset W of $\mathbb{R}^n$ is archimedean if and only if W is compact (see [P-D], Theorem 5.1.17). In the less treated p-adic situation a suitable counterpart to Schmüdgen's result is not yet known.

2 Divisibilities on commutative rings

Let A be a commutative ring with unit $1 \neq 0$. A binary relation $a \mid b$ on A (in set theoretic terms we shall write $| \subseteq A \times A$) will be called a *divisibility* on A, if for all $a, b, c \in A$ we have

(1) $a \mid a$

(2) $a \mid b, b \mid c \Rightarrow a \mid c$

(3) $a \mid b, a \mid c \Rightarrow a \mid b - c$

(4) $a \mid b \Rightarrow ac \mid bc$

(5) $0 \nmid 1$.

Easy consequences from these axioms are e.g. $a \mid 0$ and $a \mid -a$. The set $I(|) := \{a \in A; 0 \mid a\}$ is a proper ideal of A. For all $\alpha, \beta \in I(|)$ and $a, b \in A$ we have $a \mid b \Rightarrow a + \alpha \mid b + \beta$.
It follows that

$$a + I \mid b + I :\Leftrightarrow a \mid b$$

defines a divisibility on the quotient ring $\overline{A} = A/I(|)$. The ideal $I(|)$ will be called the *support* of $|$.

[3] Compared with the real situation one could as well call them "pre-p-valuations".

Clearly, if $\delta : A \to B$ is a homomorphism of commutative rings with 1, i.e., $\delta(1) = 1$, and $|$ is a divisibility on B, then

$$a|'b :\Leftrightarrow \delta(a)|\delta(b)$$

defines a divisibility $|'$ on A with support $I(|') = \delta^{-1}(I(|))$.
We call a divisibility $|$ on A *total* if for all $a, b \in A$ we have $a|b$ or $b|a$. We shall say that $|$ admits *cancellation* if for all $c \notin I(|)$ (i.e., $0 \nmid c$), $ac|bc$ implies $a|b$. If $|$ is total and admits cancellation, we shall also call $|$ a *valuation divisibility.*

Proposition 2.1. *If the divisibility $|$ has cancellation, then $I(|)$ is prime.*

Proof. Assume that $0|ab$ and $0 \nmid a$. Then cancelling a in $0 \cdot a|ba$ gives $0|b$. □

Example 2.2 Let A be an integral domain and $F =$ Quot A. Then every subring B of F defines a divisibility $|$ on A by taking

$$a|b :\Leftrightarrow a = b = 0 \text{ or } (a \neq 0 \text{ and } \frac{b}{a} \in B).$$

Note that $|$ clearly has cancellation and $I(|) = \{0\}$. Conversely, if $|$ is a divisibility with cancellation and $I(|) = \{0\}$ on A, then

$$B := \{\frac{b}{a}; a, b \in A, a|b, a \neq 0\} \cup \{0\}$$

is a subring of F.
It is clear that $| \leftrightarrow B$ is a $1-1$ correspondence. Note that $|$ is total if and only if B is a valuation ring of F. Note also that A need not be a subring of B. For example let $A = \mathbb{R}[X]$ and B the valuation ring of the degree valuation on $F = \mathbb{R}(X)$. Then $A \cap B = \mathbb{R}$.

Example 2.3 Let $v : A \to \Gamma \cup \{\infty\}$ be a *valuation in the sense of Bourbaki*, i.e., Γ is an ordered abelian group $I = v^{-1}(\infty)$ is a prime ideal of $A, \overline{v} : F \to \Gamma \cup \{\infty\}$ is an ordinary valuation on the field $F =$ Quot $\overline{A}$ with $\overline{A} = A/I$, and $v(a) = \overline{v}(\overline{a})$ for all $a \in A$. Then

$$a|b \Leftrightarrow v(a) \leq v(b)$$

defines a divisibility on A with $I(|) = I$ prime. Clearly $|$ has cancellation and is total.

Our main example here is $A = F = \mathbb{Q}_p$ and $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$. We then call $|_p$, defined by

$$a|_p b \Leftrightarrow v_p(a) \leq v_p(b)$$

the *canonical p-adic divisibility.*

Example 2.4 Let $A = C(X, \mathbb{Q}_p)$ be the ring of all continuous functions $f : X \to \mathbb{Q}_p$ where X is a compact space. We call

$$f|^*g \Leftrightarrow \forall x \in X(v_p(f(x)) \leq v_p(g(x)))$$

the *canonical p-adic divisibility* on A. If X is finite and has more than one point, then $|^*$ has no cancellation, is not total, and $I(|^*) = \{0\}$, but not prime.

A valuation $v : F \twoheadrightarrow \Gamma \cup \{\infty\}$ on a field F of characteristic 0 is called a *p-valuation* if Γ is a discretely ordered abelian group with $v(p)$ as minimal positive element and the residue field $\overline{F}$ of v is the finite field $\mathbb{F}_p$ of p elements. (F, v) is called *p-adically closed* if $v : F \twoheadrightarrow \Gamma \cup \{\infty\}$ is a p-valuation, (F, v) is henselian, and the quotient group $\Gamma/\mathbb{Z}v(p)$ is divisible. Clearly, $(\mathbb{Q}_p, v_p)$

is p-adically closed. Every p-valued field admits an algebraic extension that is p-adically closed, called a p-adic closure. p-adic closures are in general not unique up to isomorphism. In case $\Gamma = \mathbb{Z}$, the p-adic closure is unique up to isomorphism as it is the henselization. For more information the reader is refered to [P-R].
Returning to a p-valued field (F, v) let us simply write 1 for the positive minimal value $v(p)$. For every $x \in F$ the quotient

$$\gamma(x) = \frac{1}{p} \cdot \frac{x^p - x}{(x^p - x)^2 - 1}$$

is defined and has value ≥ 0. The operator γ is usually called the *Kochen operator*. It plays in the theory of p-valued fields a similar role as the square operator does in the theory of pre-ordered fields.

Theorem 2.5. *Let F be a field of characteristic 0 and let B be a subring of F containing the ring $\mathbb{Z}[\gamma(F)]$ generated by all $\gamma(x)$ for $x \in F$. If $p^{-1} \notin B$, then B is contained in the valuation ring O_v of some p-valuation v on F.*

Proof. Clearly, p is not a unit of B. Thus there exists a prime ideal P of B with $p \in P$. By Chevalley's place extension theorem ([E-P], ch 3.1) there exists a valuation v of F such that $O_v \supseteq B$ and $M_v \cap B = P$. Since now the valuation ring O_v containes $\mathbb{Z}[\gamma(F)]$, but not p^{-1}, v is a p-valuation by [P-R], Lemma 6.1. □

Motivated by this theorem we call a divisibility $|$ on a commutative ring with $1 \neq 0$, a *p-divisibility* if it satisfies for all $a, b \in A$

(6) $0 \nmid a \Rightarrow pa \nmid a$, and

(7) $p[(a^p b - b^p a)^2 - (b^{p+1})^2] \mid [(a^p b - b^p a) b^{p+1}]$.

Note that (6) implies in particular $p \nmid 1$.

Theorem 2.6. *Let A be an integral domain with $\mathbb{Q} \subseteq A$ and $F =$ Quot A its field of fractions. Then there is a $1-1$ correspondence between p-valuation rings $B \subseteq F$ and total p-divisibilities $|$ of A that have cancellation and support $I(|) = \{0\}$.*

Proof. If $B \subseteq F = \text{Quot } A$ is a p-valuation ring, then Example 2.2 shows that for $a, b \in A$

$$a|b :\Leftrightarrow a = 0 \text{ or } \frac{b}{a} \in B$$

gives a total p-divisibility on A with cancellation and $I(|) = \{0\}$.
Conversely, let $| \subseteq A \times A$ be a total p-divisibility with cancellation and $I(|) = \{0\}$. Then again Example 2.2 together with Theorem 2.5 shows that

$$B := \{\frac{b}{a};\ a, b \in A,\ a \neq 0,\ a|b\} \cup \{0\}$$

is a valuation ring of F being contained in the valuation ring O_v of some p-valuation of F. It then follows that $B = O_v$. In fact, the valuation ring B is mapped by the residue map $\delta : O_v \to \mathbb{F}_p$ of v to a valuation ring $\delta(B)$ of $\mathbb{F}_p$. As $\mathbb{F}_p$ is finite, it follows that $\delta(B) = \mathbb{F}_p$. Hence also $B = O_v$. □

As we have seen above the canonical p-adic valuation v_p defines on $\mathbb{Q}_p$ by $a|_p b \Leftrightarrow v_p(a) \leq v_p(b)$ a total p-divisibility $|_p$ with cancellation and support $\{0\}$. From this we also see that the canonical p-adic divisibility $|^*$ of $C(X, \mathbb{Q}_p)$ is in fact a p-divisibility. But in general $|^*$ need neither be total nor have cancellation.

3 The divisibility spectrum

In this section we shall first introduce the divisibility spectrum of a commutative A with $1 \neq 0$. We then restrict ourself to the spectrum of p-divisibilities assuming that $\mathbb{Q} \subseteq A$. This will provide us with some compact (zero-dimensional) space X on which later the elements of A will operate as continuous functions with values in $\mathbb{Q}_p$.

Let A be a commutative ring with unit $1 \neq 0$. The next proposition justifies the name 'valuation divisibility' in Section 2 for divisibilities that are total and admit cancellation.

Proposition 3.1. *The valuation divisibilities on A correspond $1-1$ to the Bourbaki valuations of A.*

Proof. Let first $v : A \to \Gamma \cup \{\infty\}$ be a Bourbaki valuation on A, i.e., $I = v^{-1}(\infty)$ is a prime ideal of A, $\overline{v}:$ Quot $\overline{A} \to \Gamma \cup \{\infty\}$ with $\overline{A} = A/I$ is an ordinary field valuation, and $\overline{v}(a+I) = v(a)$ for all $a \in A$. Then for elements a, b from A, $a|^v b \Leftrightarrow v(a) \leq v(b)$ defines a total divisibility on A having cancellation and support $I(|^v) = I$.
Conversely, let $|$ be a valuation divisibility on A. Then $I = I(|)$ is prime by Proposition 2.1 and $|$ induces a total divisibility $\overline{|}$ on the integral domain $\overline{A} = A/I$ having cancellation and support $\{0\}$. Thus by Example 2.2 the ring

$$B := \{\frac{\overline{b}}{\overline{a}};\ \overline{a} \neq \overline{0} \text{ and } a|b\} \cup \{\overline{0}\}$$

is a valuation ring of $F =$ Quot $\overline{A}$, say $B = O_{\overline{v}}$ for some ordinary valuation $\overline{v} : F \to \Gamma \cup \{\infty\}$. Now $v(a) := \overline{v}(\overline{a})$ clearly defines a Bourbaki valuation on A with $v^{-1}(\infty) = I$ inducing $\overline{v}$ on $\overline{A}$. By construction of v we have for all $a, b \in A$, $a|b \Leftrightarrow v(a) \leq v(b)$.

It is obvious that the correspondence between v and $|$ is one to one. $\square$

Remark 3.2. *Assuming $\mathbb{Q} \subseteq A$ in the construction of Theorem 3.1, all fields Quot $\overline{A}$, have characteristic 0. Thus by Theorem 2.6 the valuation divisibility $|$ of Theorem 3.1 is a p-divisibility if and only if $\overline{v}$ is a p-valuation.*

Now let us introduce

$$\begin{array}{rcl} D(A) & = & \text{class of all divisibilities of } A, \\ D_p(A) & = & \text{class of all } p\text{-divisibilities of } A. \end{array}$$

Note that both classes are closed by taking unions of chains w.r.t. inclusion. Thus by Zorn's Lemma every (p-)divisibility is contained in some maximal (p-)divisibility. On $D = D(A)$ we introduce the *spectral* topology as the topology generated by the sets

$$U(a,b) = \{| \in D;\ a \nmid b\}$$

where a, b range over A. If we add the complements $V(a,b) = \{| \in D;\ a|b\}$ to the above generators, we call this finer topology the *constructible* one.
Identifying a subset Y of $A \times A$ with its characteristic function and applying Tychonoff's Theorem to the function space $\{0,1\}^{A \times A}$ one proves by standard arguments

Lemma 3.3. *The constructible topology on $D(A)$ is compact. Thus the spectral topology is, in particular, quasi-compact (i.e. every open cover contains a finite subcover).*

We call the class

$$\text{Spec } D(A) = \{| \in D(A);\ | \text{ is total and admits cancellation}\}$$

the *divisibility spectrum* of A, and Spec $D_p(A) = D_p(A) \cap$ Spec $D(A)$ the *p-divisibility spectrum* of A.

These two classes are as well closed under unions of chains. Thus again by Zorn's Lemma every element is contained in a corresponding maximal one. We denote the subclasses of maximal elements by

$$\text{Spec}^{\max} D(A) \quad \text{and} \quad \text{Spec}^{\max} D_p(A).$$

Proposition 3.4. *1. $D_p(A)$, Spec $D(A)$, and Spec $D_p(A)$ are closed subclasses of $D(A)$ in the constructible topology, hence are quasi-compact in both topologies.*

2. *$D(A)^{max}$ and $D_p(A)^{max}$ are quasi-compact in the spectral topology.*
3. *Spec $D_p(A)$ and Spec$^{max} D_p(A)$ are compact in both topologies, they actually are 0-dimensional spaces: $V(a,b) = U(bp,a)$ for all $a,b \in A$.*

Proof. The proofs are straigt forward by standard arguments. Let us only mention that in 3 one shows that $V(a,b) = U(bp,a)$ on Spec D_p. In fact by Theorem 3.1 and Remark 3.2 the elements of Spec D_p correspond to Bourbaki p-valuations. Recall, if $| \in$ Spec D_p, then there is a p-valuation $\overline{v}$ on $\overline{A} = A/I(|)$ such that $a|b \Leftrightarrow \overline{v}(\overline{a}) \leq \overline{v}(\overline{b})$. As $1 = \overline{v}(p)$ is minimal positive, we get $a|b \Leftrightarrow pb \nmid a$. □

For a fixed divisibility $|_0$ on A we shall consider the subclasses of the above introduced classes consisting of extensions of $|_0$ and denote them by $D(A, |_0)$ and $D_p(A, |_0)$ respectively. As $D(A, |_0)$ is closed in the spectral topology, all topological considerations from above remain true for the relativized classes.

In the following the fixed divisibility $|_0$ will always be assumed to be *p-archimedean*, i.e.,

(8) $\forall a \in A\ \exists m \in \mathbb{Z} :\ p^m |_0 a.$

The canoncial p-adic divisibilities on $\mathbb{Q}_p$ and on $C(X, \mathbb{Q}_p)$ both satisfy axiom (8).

Theorem 3.5. *Let A be a commutative ring with $\mathbb{Q} \subseteq A$, and let $|_0$ be a p-archimedean p-divisibility on A. Then an element $|$ of Spec $D_p(A, |_0)$ is maximal if and only if $I(|)$ is prime and the corresponding p-valuation $\overline{v}$ on $F =$ Quot $A/I(|)$ has value group $\mathbb{Z}$.*

Proof. "⇒" Let $|$ be maximal in Spec $D_p(A, |_0)$. By Theorem 3.1 and Remark 3.2 $|$ corresponds uniquely to a p-valuation $\overline{v} : F \twoheadrightarrow \Gamma \cup \{\infty\}$. Denoting (as usual) the positive minimal element $\overline{v}(p)$ of Γ by $1, \mathbb{Z} = \mathbb{Z}\overline{v}(p)$ is a convex subgroup of Γ. Since $|_0$ is archimedean, so is $|$. Hence for every $a \in A$ there exists some $m \in \mathbb{Z}$ such that $m \leq \overline{v}(\overline{a})$.
If now Γ would be bigger than $\mathbb{Z}$, there existed some $b \in A \setminus I(|)$ with $m \leq \overline{v}(\overline{b})$ for all $m \in \mathbb{Z}$. Thus the set $P = \{\overline{b} \in \overline{A}; m \leq \overline{v}(\overline{b}) \text{ for all } m \in \mathbb{Z}\}$ forms a non-zero prime ideal of $\overline{A}$. Taking $w(\overline{b} + P) := \overline{v}(\overline{b})$ defines a p-valuation on the quotient field F' of $\overline{A}/P$ with value group $\mathbb{Z}$.

Setting $a|'b$ in case $w(\overline{a}+P) \leq w(\overline{b}+P)$ defines a p-divisibility $|' \in$ Spec $D_p(A, |_0)$ strictly containing $|$. This contradicts the maximality of $|$. Therefore $\Gamma = \mathbb{Z}$.

"$\Leftarrow$" Now assume that the p-valuation $\overline{v}$ corresponding to $|$ has value group $\mathbb{Z}$ on $F =$ Quot $A/I(|)$. If $|' \in$ Spec $D_p(A, |_0)$ is a proper extension of $|$ then $I(|) \subsetneqq I(|')$ or, $I(|) = I(|')$ and the valuation ring O' of $\overline{v}'$ properly extends the valuation ring O of $\overline{v}$. This second case is not possible, since (by Lemma 2.3.1 of [E-P]) a proper extension O' of O corresponds to a proper convex subgroup of the value group of O which is $\mathbb{Z}$. Such a subgroup clearly does not exist. In the first case, choose $a \in I(|') \setminus I(|)$. Since v has value group $\mathbb{Z}$ and $\overline{a}$ is non-zero in $A/I(|)$, there exists some $m \in \mathbb{Z}$ such that $\overline{v}(\overline{a}) \leq m$, i.e., $a|p^m$. But then $a \in I(|')$ implies $0|'a$. Now $| \subseteq |'$ gives $0|'p^m$, a contradiction. □

So far we did not show that Spec $D_p(A)$ is non-empty.

Theorem 3.6. *Let A be a commutative ring with $\mathbb{Q} \subseteq A$. Then Spec $D_p(A)$ is non-empty if and only if there exists a p-divisibility $|$ on A. Equivalently, we have that A admits a ring homomorphism δ with $\delta(1) = 1$ into some p-valued field. Spec $D_p(A)$ contains a p-archimedean element if and only if A admits a ring homomorphism with $\delta(1) = 1$ into the p-adic number field $\mathbb{Q}_p$.*

Proof. Assume $\delta : A \to F$ is a ring homomorphism with $\delta(1) = 1$ and (F, v) is a p-valued field. Then the definition

$$a|b \Leftrightarrow v(\delta(a)) \leq v(\delta(b))$$

for $a, b \in A$ obviously yields a p-divisibility on A with $I(|) =$ ker δ. If $(F, v) = (\mathbb{Q}_p, v_p)$ then clearly $|$ is p-archimedean.

Next let $|'$ be a p-divisibility on A. By Zorn's Lemma we can pass to a maximal extension $|$ of $|'$ inside the class of p-divisibilities extending $|'$. Thus also $|$ is a p-divisibility. We want to see that $|$ admits cancellation. Let $c \in A$ and assume $0 \nmid c$. We then define $a|^c b$ if $ac \mid bc$ for all $a, b \in A$. One easily checks that $|^c$ is a p-divisibility on A extending $|$. As $|$ is maximal, $| = |^c$. This implies cancellation by c. In fact, if $ac \mid bc$, then $a|^c b$ and as $| = |^c$, we get $a \mid b$. Since now $|$ has cancellation, by Proposition 2.1 $I(|)$ is prime and we may pass to the ring $\overline{A} = A/I(|)$ and its field of fractions $F =$ Quot $\overline{A}$. By Example 2.2 the divisibility $|$ corresponds to the subring

$$B = \{\frac{\overline{b}}{\overline{a}};\ 0 \nmid a,\ a|b\} \cup \{\overline{0}\}$$

of F. Since $|$ is a p-divisibility, the Kochen relations (7) imply that $\mathbb{Z}[\gamma(F)]$ is contained in B, while (6) implies that $p^{-1} \notin B$. Thus by Theorem 2.5 there exists a p-valuation $\overline{v}$ on F such that $B \subseteq O_{\overline{v}}$. Now by Remark 3.2 the definition

$$a|_1 b \Leftrightarrow \overline{v}(\overline{a}) \leq \overline{v}(\overline{b})$$

yields an extension $|_1$ of $|$ that belongs to Spec $D_p(A)$. Thus Spec $D_p(A)$ is non-empty.

Finally, let $| \in$ Spec $D_p(A)$. By Remark 3.2, $|$ induces a p-valuation $\overline{v}$ on Quot $A/I(|)$. Thus the canonical homomorphism $\delta : A \to A/I(|)$ maps A to a p-valued field.

It remains to show that the existence of a p-archimedean element $| \in$ Spec $D_p(A)$ provides us with some homomorphism from A to $\mathbb{Q}_p$.

We may assume that $|$ is maximal in $\text{Spec}\, D_p(A)$. Then by Theorem 3.5, $I(|)$ is prime and $|$ corresponds to some p-valuation $\overline{v}$ on $F = \text{Quot}\, A/I(|)$ with value group $\mathbb{Z}$. In that case, however, the completion of F w.r.t. $\overline{v}$ is isomorphic to the field $\mathbb{Q}_p$. Thus the desired homomorphism is just the canonical homomorphism $\delta : A \to A/I(|)$. □

4 p-adic representations

Now let us fix a commutative ring A with $\mathbb{Q} \subseteq A$ together with a p-archimedean p-divisibility $|_0$ on A. By Theorem 3.6 the maximal spectrum

$$X = \text{Spec}^{max} D_p(A, |_0)$$

is non-empty, and by Proposition 3.4.(3.) it is a 0-dimensional compact space. By Theorem 3.5 every $| \in X$ induces a canonical homomorphism

$$\alpha_| : A \to \overline{A} = A/I(|) \subseteq F := \text{Quot}\, \overline{A}$$

together with a p-valuation $\overline{v} : F \to \mathbb{Z} \cup \{\infty\}$ such that $a|b \Leftrightarrow \overline{v}(\overline{a}) \leq \overline{v}(\overline{b})$ for all $a, b \in A$. The completion of F w.r.t. $\overline{v}$ is just the field $\mathbb{Q}_p$ of p-adic numbers with $\overline{v}$ being the restriction of v_p to F.[4] As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ w.r.t. the topology induced by the p-adic valuation v_p on $\mathbb{Q}_p$, the embedding of F into $\mathbb{Q}_p$, is uniquely determined. Thus every $| \in X$ yields a canonical homomorphism

$$\alpha_| : A \to \mathbb{Q}_p$$

with $a|b \Leftrightarrow v_p(\alpha_|(a)) \leq v_p(\alpha_|(b))$ for all $a, b \in A$. Therefore, every $a \in A$ induces a canonical map $\widehat{a}$ from A to $\mathbb{Q}_p$ by taking

$$\widehat{a}(|) := \alpha_|(a)$$

for every 'point' $|$ in X.

Theorem 4.1. *Let A be a commutative ring with $\mathbb{Q} \subseteq A$ and let $|_0$ be a p-archimedean p-divisibility on A. Then the map $\widehat{a}$ is continuous for every $a \in A$. Therefore $\phi : A \to C(X, \mathbb{Q}_p)$ defined by $\phi(a) = \widehat{a}$ is a homomorphism of rings with dense image $\phi(A)$ in $C(X, \mathbb{Q}_p)$, satisfying*

$$a|_0 b \Rightarrow \phi(a)|^* \phi(b), \text{ for all } a, b \in A.$$

Proof. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, the sets

$$U_n(r) = \{x \in \mathbb{Q}_p;\ v_p(x - r) \geq n\},\ r \in \mathbb{Q},\ n \in \mathbb{N}$$

form a base for the topology on $\mathbb{Q}_p$. Thus it suffices to show that the preimage of $U_n(r)$ under $\widehat{a}$ is open in the topology of X. This, however, follows from Proposition 3.4.(3.) and the fact that

$$(\widehat{a})^{-1}(U_n(r)) = \{| \in X;\ p^n | a - r\} = V(p^n, a - r) \cap X$$

for all $a \in A, r \in \mathbb{Q}$ and $n \in \mathbb{N}$.
In order to show that $\phi(A)$ is dense in $C(X, \mathbb{Q}_p)$ w.r.t. the maximum norm it suffices by the p-adic Stone-Weierstrass Approximation (see [K]) to show that two different points of X, say $|_1 \neq |_2$ can always be separated by some function $\widehat{a}$, i.e., $\widehat{a}(|_1) \neq \widehat{a}(|_2)$: Let $a, b \in A$ distinguish $|_1$ from $|_2$, say $a|_1 b$ and $a \nmid_2 b$. Then either $\widehat{a}$ or $\widehat{b}$ separates $|_1$ from $|_2$, as it is easily checked. □

[4]Note that every element of F has a canonical expansion as a power series in the uniformizer p with coefficients from $\{0, 1, \ldots, p-1\}$ (cf. [E-P], Proposition 1.3.5).

Let X be a compact space. We then denoted by $C(X, \mathbb{Q}_p)$ the ring of all $\mathbb{Q}_p$-valued continuous functions on X. This ring carries a canonical p-adic norm which makes it a p-adic Banach algebra over $\mathbb{Q}_p$. The norm is defined by

$$\| f \|^* := \max \{|f(x)|_p;\ x \in X\}$$

where $| \ |_p$ is the p-adic absolute value on $\mathbb{Q}_p$ defined by $|x|_p = p^{-v_p(x)}$.
The norm $\| \ \|^*$ on $C(X, \mathbb{Q}_p)$ is even *power multiplicative*, i.e., for all $n \in \mathbb{N}$

$$\| f^n \|^* = (\| f \|^*)^n.$$

Theorem 4.1 provides us with a homomorphism $\phi : A \to C(X, \mathbb{Q}_p)$ with dense image. We have, however, no information about the kernel of ϕ. In order to achieve this goal we shall introduce one more condition on the p-divisibility $|_0$ of Theorem 4.1.
Let us assume that $|$ is a p-archimedean p-divisibility on the commutative ring A with $\mathbb{Q} \subseteq A$. We can then define for every $a \in A$

$$\text{ord } a := \sup \{m \in \mathbb{Z};\ p^m | a\} \in \mathbb{Z} \cup \{\infty\} \text{ and } \| a \| = p^{-\text{ ord } a}.$$

Lemma 4.2. *For all $a, b \in A, r \in \mathbb{Q}$ we get*

(a) $\| a + b \| \leq$ *max* $(\| a \|, \| b \|)$

(b) $\| a \cdot b \| \leq \| a \| \ \| b \|$

(c) $\| r \| = |r|_p$

(d) $\| ra \| = |r|_p \ \| a \|$.

Proof. (a) and (b) are easily checked. (c) is equivalent to ord $r = v_p(r)$, and will be shown in Proposition 4.3 below.
(d) then follows from $\| ra \| \leq \| r \| \ \| a \| = |r|_p \ \| a \|$ and $\| a \| = \| r^{-1} ra \| \leq \| r^{-1} \| \ \| ra \|$. In fact, since by (c), $\| \ \|$ is multiplicative on $\mathbb{Q}$, we then get $|r|_p \ \| a \| = \| r^{-1} \|^{-1} \| a \| \leq \| ra \|$. ☐

It remains to show ord $r = v_p(r)$ for $r \in \mathbb{Q}$. This follows from

Proposition 4.3. *The only p-archimedean divisibility with $p \nmid 1$ of the field $\mathbb{Q}$ of rational numbers is the one obtained by the p-adic valuation v_p.*

Proof. The support $I(|)$ is a proper ideal of $\mathbb{Q}$. Hence $I(|) = \{0\}$. Moreover, as $\mathbb{Q}$ is a field, axiom (4) implies that $|$ has cancellation. Thus by Example 2.2 it suffices to show that the ring $B = \{\frac{b}{a};\ a, b \in \mathbb{Q},\ a \neq 0,\ a|b\} \cup \{0\}$ contains the valuation ring $\mathbb{Z}_{(p)}$ of v_p restricted to $\mathbb{Q}$. In fact, then also B is a valuation ring of $\mathbb{Q}$, hence has to be equal to $\mathbb{Z}_{(p)}$ (cf. [E-P], Theorem 2.1.4). Note that $B \neq \mathbb{Q}$ as $p^{-1} \notin B$.
Let $n, m \in \mathbb{Z}$ and n prime to p. We have to show that $n|m$. As $|$ is p-archimedean there exists $r \in \mathbb{N}$ such that $p^{-r}|n^{-1}$. Therefore $n|p^r$. Since n is prime to p there exist $k, l \in \mathbb{Z}$ with

$$kp^r + ln = 1.$$

Since $n|p^r$, also $n|kp^r$. Clearly also $n|ln$. Thus (by (3)) $n|1$. Hence $n|m$. ☐

By Lemma 4.2, $\| \ \|$ is a sub-multiplicative p-adic semi-norm on A. In the next lemma we shall give equivalent conditions for $\| \ \|$ to be even power multiplicative. Note that in this case $\| a^n \|= 0$ is equivalent to $\| a \|= 0$. It is well-known that power multiplicativity is already implied from the case $n = 2$.

Main Lemma 4.4. *Let $|_0$ be a p-archimedean p-divisibility on A. Then the following three conditions are equivalent:*

(i) $p|_0a^2 \Rightarrow p|_0a$ for all $a \in A$,

(ii) the norm $\| \ \|$ defined by $|_0$ is power multiplicative.

(iii) (Local-Global-Priciple) Let $X = Spec^{max} D_p(A, |_0)$. Then $p \mid a$ for all $| \in X$ implies $p|_0a$.

Proof. (iii) $\Rightarrow$ (i) follows from Theorem 4.1 and the fact that all $| \in X$ satisfy (i).
(i) $\Rightarrow$ (ii): As $\| a^2 \|\leq\| a \|^2$ is obvious, it remains to prove $\| a \|^2\leq\| a^2 \|$. By the definition of $\| \ \|$, this amounts to prove that ord $a^2 \leq 2$ ord a. Let $m =$ ord a and assume $p^{2m+1} |a^2$. Then clearly $p|(ap^{-m})^2$. Hence by (i) we would get $p|ap^{-m}$ or equivalently $p^{m+1}|a$, a contradiction.
(ii) $\Rightarrow$ (iii): Let us assume $p \nmid_0 a$. We shall then construct some extension $| \in$ Spec $D_p(A, |_0)$ such that $a \mid 1$. This clearly implies $p \nmid a$. The extension $|$ of $|_0$ will be obtained in three steps:

- In step 1 we construct $|_1 \supseteq |_0$ such that $a |_1 1$ and $|_1$ satisfies all axioms of a p-divisibility except (6). Instead, we shall only obtain $p \nmid 1$.
- In step 2 we maximalize $|_1$ to $|_2$ such that $|_2$ satisfies axiom (6), hence is a p-divisibility.
- In step 3 we apply Theorem 3.6 to $D_p(A, |_2)$ in order to obtain $| \in$ Spec $D_p(A, |_0)$ with $a \mid 1$.

For step 1 and 2 we need a little preparation: We call an additive subgroup C of A *convex* w.r.t. $|$ if for all $a, b \in A$ we have: $a \in C, a \mid b \Rightarrow b \in C$. For a subset S of A we define the convex group $C(S)$ generated by S to be obtained by iterating countably many times in alternating order the two operations

$$\begin{aligned} G(S) &= \text{additive group generated by } S \\ M(S) &= \{b \in A; x \mid b \text{ for some } x \in S\}. \end{aligned}$$

Then $C(S)$ is a convex subgroup of A containing S. The operator C obviously satisfies $S \subseteq C(S) = CC(S)$ and $aC(S) \subseteq C(aS)$. Moreover we have

$$a \mid b \Rightarrow C(\{b\} \cup S) \subseteq C(\{a\} \cup S).$$

Step 1: We define $x|_1y :\Leftrightarrow ya^r \in C(\{xa^i; 0 \leq i \leq r\})$ for some $r \in \mathbb{N}$. First observe that $|_1$ extends $|_0$. In fact: $x|_0y \Rightarrow y \in C(x)(r = 0)$. Moreover we get $a |_1 1$ since $a \in C(\{a, a^2\})(r = 1)$. Next one checks the axioms (1) - (4) using the above mentioned properties of the operator C. The axioms (7) and (8) follow from $|_0 \subseteq |_1$. It remains to prove $p \nmid_1 1$ (then also axiom (5) follows). Let us assume on the contrary the existence of some $r \in \mathbb{N}$ such that

$$a^r \in C(\{pa^i; 0 \leq i \leq r\}).$$

By (ii) we have ord $a^i = i$ ord a. From our assumption $p \nmid_0 a$ we get ord $a \leq 0$. Hence we have the following contradiction:

$$\text{ord } a^r \geq 1 + \min{}_{0 \leq i \leq r} \text{ ord } a^i = 1 + \text{ ord } a^r.$$

Step 2: Let now $|_2$ be an extention of $|_1$ maximal with the properties (1) - (4), (7), (8) and $p \nmid_2 1$. We then prove (6) for $|_2$. Assume $cp|_2 c$ for some $c \in A$. Since $|_2$ is p-archimedean, to every $b \in A$ we find some $m \in \mathbb{N}$ such that $1 \;|_2\; p^m bc$. Applying $pc \;|_2 c$ iteratively yields $p \;|_2\; p^{1+m}bc \;|_2\; p^m bc \;|_2\; p^{m-1}bc \;|_2 \cdots |_2\; pbc \;|_2\; bc$.
Now define

$$x \;|'\; y :\Leftrightarrow y \in C(cA \cup \{x\}).$$

Clearly $|'$ extends $|_2$. The axioms (1) to (4) are easy to check and the axioms (7) and (8) are interited. Since $p \;|_2\; bc$ for all $b \in A$, we find $C(cA \cup \{p\}) \subseteq C(p)$. As $p \nmid_2 1$ we therefore get $1 \notin C(cA \cup \{p\})$, i.e. $p \nmid' 1$. Since $|_2$ was maximal with these properties, we have $|_2 = |'$, and therefore $0 \;|'\; c$ yields $0 \;|_2\; c$. Thus we have shown that $|_2$ is a p-divisibility.

Step 3: Finally we apply Theorem 3.6 to $D_p(A, |_2)$ in order to obtain some $| \in \text{Spec}D_p(A, |_0)$ with $a|1$. clearly $|$ may be chosen maximal. ☐

p-adic Representation Theorem 4.5. *Let A be a commutative ring with $\mathbb{Q} \subseteq A$ that admits a p-archimedean p-divisibility $|_0$ satisfying $p|_0 a^2 \Rightarrow p|_0 a$ for all $a \in A$. Then the homomorphism $\phi : A \to C(X, \mathbb{Q}_p)$ of Theorem 4.1 with $X =$ Spec$^{max} D_p(A, |_0)$ satisfies $\| \phi(a) \|^* = \| a \|_0$. Consequently:*

- *ker $\phi = \{a \in A; p^n \;|_0\; a$ for all $n \in \mathbb{N}\}$,*
- *ϕ is injective, if the semi-norm $\| \; \|_0$ defined by $|_0$ is a norm,*
- *ϕ is surjective, if A is complete w.r.t. the norm $\| \; \|_0$.*

Proof. By Theorem 4.1 and Main Lemma 4.4 we have $\| \phi(a) \|^* = \| a \|_0$. Thus if $\| \; \|_0$ is a norm, $\phi(a) = 0$ implies $\| a \|_0 = 0$ and hence $a = 0$. This proves injectivity.
In order to get surjectivity, let $f \in C(X, \mathbb{Q}_p)$ be given. As $\phi(A)$ is dense in $C(X, \mathbb{Q}_p)$ by Theorem 4.1, there exists a sequence $(\phi(a_n))_{n \in \mathbb{N}}, a_n \in A$, converging to f. Then clearly $(a_n)_{n \in \mathbb{N}}$ is a Cauchy-sequence in $(A, \| \; \|_0)$. Thus by completeness there exists a limit a of $(a_n)_{n \in \mathbb{N}}$ in A. Now $\phi(a) = f$. ☐

From Theorem 4.5 we finally get our

Characterization Theorem 4.6. *Let A be a commutative ring with $\mathbb{Q} \subseteq A$. Then, as a ring, $A \cong C(X, \mathbb{Q}_p)$ for some compact (actually 0-dimensional) space X if and only if there exists a p-divisibility $a \mid b$ on A such that*

(i) A is p-archimedean with respect to $|$,

(ii) the p-adic semi-norm canonically defined by $|$ on A is a norm satisfying $\| a^2 \| = \| a \|^2$ for all $a \in A$,

(iii) A is complete with respect to this norm.

So far the characterization 4.6 does not seem to be a completely algebraic one, as it involves the binary relation $|$. There is, however, a way to avoid this. The canonical p-adic divisibility $|^*$ on $C(X, \mathbb{Q}_p)$ can actually be algebraically expressed in the following way

Proposition 4.7. *The canonical p-adic divisibility* $|^*$ *on* $C(X, \mathbb{Q}_p)$*,* X *a compact space, satisfies for all* $f, g \in C(X, \mathbb{Q}_p)$

$$g|^* f \Leftrightarrow \exists h \ h^q = g^q + pf^q$$

where $q \in \mathbb{N}$ *is a prime different from* p*.*

Proof. "$\Leftarrow$" Let $x \in X$. Then the values of $g^q(x)$ and $pf^q(x)$ are different. From $h^q = g^q + pf^q$ we see that the value of

$$(g^q + pf^q)(x)$$

has to be divisible by q. Hence $v_p(g^q(x)) < v_p(pf^q(x))$ which clearly implies $v_p(g(x)) \leq v_p(f(x))$. Thus by definition $g|^* f$.
"$\Rightarrow$" Assuming $v_p(g(x)) \leq v_p(f(x))$ for all $x \in X$ we have to construct a continuous function $h : X \to \mathbb{Q}_p$ such that $h^q = g^q + pf^q$.
Using the fact that the function $g^q + pf^q$ can only take values in $\mathbb{Z}$ all of which are divisible by q, the fact that the residue class field is finite, and by patching h from suitable continuous functions, we are reduced to the case where $g = 1$ on an open and closed subset Y of X. Now we can apply Hensel's Lemma to the 1-unit $1 + pf(x)^q$ (as the characteristic of the residue field is different to q). □

Using Proposition 4.7 we may replace any use of $a|b$ in the Characterization Theorem 4.6 by the algebraic expression

$$(*) \quad \exists c \ c^q = a^q + pb^q,$$

requiring in addition that (*) is a p-divisibility satisfying (i)-(iii). This way we obtain a completely algebraic characterization of the rings $C(X, \mathbb{Q}_p)$ with X compact.

References

[A-K] F. Albiac, N. J. Kalton: *A characterization of real C(K)-spaces*, The AMS Monthly 114 (2007), 737-743.

[E-P] A. Engler, A. Prestel: *Valued Fields*, Springer Monographs in Mathematics (2005).

[K] I. Kaplansky: *The Weierstrass theorem in fields with valuations*, Proc. Amer. Math. Soc. 1, 356-357 (1950).

[Kr] J.-L. Krivine: *Anneaux préordonnés*, J. Analyse Math. 12 (1964), 307-326.

[L] S. Volkweis Leite: *p-adic representations of commutative rings*, Universität Konstanz (2012).

[P-D] A. Prestel, C. N. Delzell: *Positive polynomials*, Springer Monographs in Mathematics (2001).

[P-R] A. Prestel, P. Roquette: *Formally p-adic fields*, Springer Lecture Notes in Mathematics, 1050 (1984).

[R] P. Roquette: *Bemerkungen zur Theorie der formal p-adischen Körper*, Beitrag zur Algebra und Geometrie 1 (1971), 177-193.

[St] M. H. Stone: *A general theory of spectra I*, Proc. Nat. Acad. Sci., 26, 280-283 (1940).

samuelvolkweisleite@gmail.com
alex.prestel@uni-konstanz.de