ON SIMPLE AND SEMISIMPLE QUANTALES

DAVID KRUML AND JAN PASEKA

In a recent paper [9], J. W. Pelletier and J. Rosický published a characterization of *-simple *-quantales. Their results were adapted for the case of simple quantales by J. Paseka in [7]. In this paper we present similar characterizations which do not use a notion of discrete quantale. We also show a completely new characterization based on separating and cyclic sets. Further we explain a link to simple quantale modules. To apply these characterizations, we study (*-)semisimple (*-)quantales and discuss some other perspectives. Our approach has connections with several earlier works on the subject [7, 9].

After an initial section of generalities, the next two sections consist of the above-mentioned characterizations of (*-)simple (*-)quantales and related applications. The interest is then centered on (*-)semisimple (*-)quantales and simple modules. In particular, one concludes that a quantale is semisimple if and only if it is faithful and spatial. We then use the natural concept of a simple module to give another characterization of (semi)simplicity. Finally, motivated by the concept of non-commutative topology for C*-algebras introduced in [2] and developed later in [5], we discuss the relations between C*-algebras and their irreducible representations and between some weakening of the notions of separating and cyclic sets.

1. Preliminaries

1.1. Definition. By a *sup-lattice* is meant a complete lattice, a *sup-lattice morphism* is a mapping preserving arbitrary joins.

If $f : S \to T$ is a sup-lattice morphism, the assignment

$$f(s) \leq t \Leftrightarrow s \leq f^{\dashv}(t),$$

explicitly

$$f^{\dashv}(t) = \bigvee \{s \mid f(s) \leq t\},$$

defines a mapping $f^{\dashv} : T \to S$ preserving all meets. This mapping $f^{\dashv}$ is called an *adjoint* of f.

The top element of a sup-lattice is denoted by 1, the bottom element by 0.

1.2. Definition. By a *quantale* is meant a sup-lattice Q equipped with an associative multiplication which distributes over joins

$$a\left(\bigvee a_i\right) = \bigvee (aa_i), \qquad \left(\bigvee a_i\right) a = \bigvee (a_i a)$$

for all $a, a_i \in Q$.

Financial Support of the Grant Agency of the Czech Republic under the grant No. 201/99/0310 is gratefully acknowledged. The authors thank Mamuka Jibladze for suggestive questions given during the Quantum logic/quantale/category workshop in Brussels 10–14/4/2000, from whose the paper has arised.

An element $a \in Q$ is called *right-sided* or *left-sided* if $a1 \leq a$ or $1a \leq a$, respectively. We write $a \in \mathcal{R}(Q)$, resp. $a \in \mathcal{L}(Q)$. Elements of $\mathcal{T}(Q) = \mathcal{R}(Q) \cap \mathcal{L}(Q)$ are called *two-sided*.

A *quantale morphism* is a sup-lattice morphism preserving multiplication.

An equivalence relation $\sim$ on Q is said to be a *congruence* if

$$a \sim b \Rightarrow ca \sim cb, ac \sim bc, \qquad a_i \sim b_i \Rightarrow \bigvee a_i \sim \bigvee b_i$$

for all $a, b, c, a_i, b_i \in Q$. One can easily check that congruences are exactly coset equivalences given by quantale morphisms.

Actions $a\_$, $\_a$ for fixed $a \in Q$ determine sup-lattice endomorphisms on Q. Their adjoints are denoted by $\_ \leftarrow a$, $a \rightarrow \_$, respectively. That is,

$$a \leq b \rightarrow c \;\Leftrightarrow\; ab \leq c \;\Leftrightarrow\; b \leq c \leftarrow a.$$

The operations $\rightarrow, \leftarrow$ are called *residuations*.

A set $P \subseteq Q$ is said to be *residually closed* if $a \rightarrow p \in P, p \leftarrow a \in P$ for every $a \in Q, p \in P$.

1.3. Lemma. [10] *Let Q be a quantale, $a, b, c, a_i \in Q$. Then*

$$(b \rightarrow c) \leftarrow a = b \rightarrow (c \leftarrow a),$$

$$a \rightarrow (b \rightarrow c) = (ab) \rightarrow c, \qquad (c \leftarrow a) \leftarrow b = c \leftarrow (ab),$$
$$\left(\bigvee a_i\right) \rightarrow c = \bigwedge (a_i \rightarrow c), \qquad c \leftarrow \left(\bigvee a_i\right) = \bigwedge (c \leftarrow a_i).$$

1.4. Definition. By a **-quantale*[1] is meant a quantale Q with a unary operation of *involution* such that

$$a^{**} = a, \qquad (ab)^* = b^* a^*, \qquad \left(\bigvee a_i\right)^* = \bigvee a_i^*$$

for all $a, b, a_i \in Q$.

An element $a \in Q$ is called *hermitian* if $a^* = a$, the set of hermitian elements is denoted by $\mathcal{H}(Q)$.

By a **-quantale morphism* (or simply a **-morphism*) is meant a quantale morphism of *-quantales which also preserves the involution.

A quantale congruence $\sim$ on a *-quantale Q is said to be a **-congruence* if

$$a \sim b \Rightarrow a^* \sim b^*$$

for all $a, b \in Q$.

Note that $(a \rightarrow b)^* = b^* \leftarrow a^*$.

[1]In [6, 9, 4], *-quantales are called involutive quantales, as well as the following concepts.

1.5. Definition. Let Q be a quantale. By a left (right) Q-module is meant a sup-lattice M with an action $Q \times M \to M$ ($M \times Q \to M$) provided that

$$\begin{gathered} a\left(\bigvee m_i\right) = \bigvee(am_i), \\ \left(\bigvee a_i\right) m = \bigvee(a_i m), \\ a(bm) = (ab)m \end{gathered} \qquad \left(\begin{gathered} \left(\bigvee m_i\right) a = \bigvee(m_i a), \\ m\left(\bigvee a_i\right) = \bigvee(ma_i), \\ (mb)a = m(ba) \end{gathered}\right)$$

for all $a, b, a_i \in Q, m, m_i \in M$.

An adjoint of the module action is called a residuation as well and denoted by $\leftarrow$ ($\rightarrow$). One can easily verify similar properties of the residuation as in 1.3, from whose it follows that M^{op} with the residuation is a right (left) Q-module. M^{op} is called a *dual module* of M. [2]

A mapping $f : M \to N$ of two left (right) Q-modules M, N is said to be a *Q-module morphism* if f is a sup-lattice morphism and $f(am) = af(m)$ ($f(ma) = f(m)a$) for every $a \in Q, m \in M$. Let us recall that the adjoint $f^{\dashv} : N^{op} \to M^{op}$ of a Q-module morphism $f : M \to N$ is a Q-module morphism of dual modules (cf. [1]. Two special cases of the module morphism is a submodule inclusion and a quotient mapping. An adjoint of inclusion is a quotient mapping and vice versa.

A Q-module M is called *faithful* if

$$(\forall m \in M)(am = bm) \Rightarrow a = b$$

for all $a, b \in Q$.

Thorough the paper we do not distinguish between left and right modules if it is not important or if the meaning is clear. We write 1_Q and 1_M for the quantale and module top, respectively, whenever a confusion is imminent.

2. Simple and semisimple quantales

The original construction [9, 7] characterizes simple quantales as discrete faithful factors. We are using stronger definition of faithfulness, in which discreteness is enclosed. In fact, this idea appeared in the proof of Pelletier and Rosický but it was not fully exploited.

2.1. Definition. By a *simple quantale* is meant a quantale Q such that $1 \cdot 1 \neq 0$ and every its quotient morphism is either an isomorphism or a constant morphism on a trivial quantale. In other words, there are exactly two congruences on Q.

By a *semisimple quantale* is meant a subdirect product of simple quantales. That is, a quantale is semisimple if it has enough surjective morphisms onto simple quantales to separate elements.

2.2. Definition. A quantale Q is called a *factor* if $\mathcal{T}(Q) = \{0, 1\}$ and $0 \neq 1$.

Q is said to be *faithful* if

$$(\forall l \in \mathcal{L}(Q), \forall r \in \mathcal{R}(Q))(lar = lbr) \Rightarrow a = b$$

for all $a, b \in Q$.

[2] The dual module, as well as submodules and quotient modules, is determined uniquely up to isomorphism. For simplicity, we ignore the difference of isomorphic modules.

2.3. Definition. Let Q be a quantale. A set $P \subseteq Q$ is said to be *separating* if, for every $a, b \in Q, a \not\geq b$, there is an element $p \in P$ provided that $a \leq p, b \not\leq p$. Note that then every element of Q is a meet of elements from P.

A nonempty set $P, 1 \notin P$ is called *cyclic* if $\{a \to p \leftarrow b \mid a, b \in Q\} = P \cup \{1\}$ for every $p \in P$. In fact, any quantale having a cyclic set is nontrivial.

2.4. Lemma. *Let Q be a quantale. A nonempty set $P \subseteq Q - \{1\}$ is cyclic, iff $P \cup \{1\}$ is residually closed, $t = \bigwedge P = 1 \to p \leftarrow 1$ for every $p \in P$, and every element $p \in P$ can be recovered from t, i.e. $p = a \to t \leftarrow b$ for some $a, b \in Q$. Then t is two-sided and a, b can be taken right-sided or left-sided, respectively.*

Proof. Let P be cyclic and $p \in P$. Then

$$1 \neq t = \bigwedge P = \bigwedge_{a,b \in Q} (a \to p \leftarrow b) = \left(\bigvee_{a \in Q} a\right) \to p \leftarrow \left(\bigvee_{b \in Q} b\right) = 1 \to p \leftarrow 1,$$

i.e. $t \in P$. Thus $P \cup \{1\} = \{a \to t \leftarrow b \mid a, b \in Q\}$. Since $1 \to t \leftarrow 1 \in P \cup \{1\}$ and $1 \to t \leftarrow 1 \leq a \to t \leftarrow b$ for every $a, b \in Q$, we have $t = 1 \to t \leftarrow 1$. Then $a \to t \leftarrow b = a \to (1 \to t \leftarrow 1) \leftarrow b = (a1) \to t \leftarrow (b1)$ and $a1 \in \mathcal{R}(Q), 1b \in \mathcal{L}(Q)$. Finally, $t = 1 \to t \leftarrow 1 \leq (1 \cdot 1) \to t \leftarrow 1 = 1 \to (1 \to t \leftarrow 1) = 1 \to t$, hence $t1 \leq t$. Similarly, $1t \leq t$. It is evident that $P \cup \{1\}$ is residually closed.

Conversely, let P satisfies the considered properties. Then for every $p \in P$ we have $p = a \to t \leftarrow b$ for some $a, b \in Q$. Thus $P' = \{c \to p \leftarrow d \mid c, d \in Q\} = \{(ca) \to t \leftarrow (bd) \mid c, d \in Q\} \subseteq P \cup \{1\}$ and $P \cup \{1\} = \{c \to t \leftarrow d \mid c, d \in Q\} = \{(c1) \to p \leftarrow (1d) \mid c, d \in Q\} \subseteq P'$, i.e. P is cyclic. □

2.5. Theorem. *Let Q be a quantale. The following conditions are equivalent:*
(1) Q is a simple quantale.
(2) Q is a faithful factor.
(3) Q has a separating cyclic set.

Proof. (1) $\Rightarrow$ (2) Let $t \in \mathcal{T}(Q)$. The assignment $a \mapsto a \vee t$ defines a surjective morphism $Q \to \uparrow t$. Since Q is simple, we have either $t = 0$ or $t = 1$, i. e. Q is a factor. From the additional condition $1 \cdot 1 \neq 0$ we conclude $1 \cdot 1 = 1$, because $1 \cdot 1$ is always two-sided. Let us put

$$a \sim b \Leftrightarrow (\forall l \in \mathcal{L}(Q), \forall r \in \mathcal{R}(Q))(lar = lbr).$$

The relation $\sim$ is a quantale congruence. Indeed, $cr \in \mathcal{R}(Q)$ and $lc \in \mathcal{L}(Q)$ for every $c \in Q, r \in \mathcal{R}(Q), l \in \mathcal{L}(Q)$ and hence $a \sim b \Rightarrow ca \sim cb$ and $ac \sim bc$. It is not hard to see that $\sim$ is a sup-lattice congruence. If $0 \sim 1$, then $0 = 1 \cdot 0 \cdot 1 = 1 \cdot 1 \cdot 1 = 1$. Thus $\sim$ is necessarily a diagonal relation, i.e. $a \sim b \Leftrightarrow a = b$, and so Q is faithful.

(2) $\Rightarrow$ (3) Put $P = \{r \to 0 \leftarrow l \mid r \in \mathcal{R}(Q), l \in \mathcal{L}(Q)\} - \{1\}$. $P \cup \{1\}$ is residually closed, because $b \to (r \to 0 \leftarrow l) = (br) \to 0 \leftarrow l$ and $(r \to 0 \leftarrow l) \leftarrow a = r \to 0 \leftarrow (la)$. From the faithfulness we have that $1 \cdot 1 \cdot 1 \neq 1 \cdot 0 \cdot 1$. Since Q is a factor and $1 \cdot 1 \in \mathcal{T}(Q)$, we have $1 \cdot 1 = 1$. For $p \in P$ we have $1 \to p \leftarrow 1 \in \mathcal{T}(Q) = \{0, 1\}$. If $1 \to p \leftarrow 1 = 1$, then $1 = 1 \cdot 1 \cdot 1 \leq p$, thus $1 \to p \leftarrow 1 = 0$ and hence P is cyclic. Let $a \not\geq b$, then there exist $r \in \mathcal{R}(Q), l \in \mathcal{L}(Q)$

such that $lar \not\geq lbr$. Since Q is a factor and lar, lbr are two-sided, $lar = 0$ and $lbr = 1$. But it means that $a \leq r \to 0 \leftarrow l$ and $b \not\leq r \to 0 \leftarrow l$, i. e. P is separating.

(3) $\Rightarrow$ (1) Let P be separating and cyclic. Then $0 = \bigwedge P = 1 \to p \leftarrow 1$ for every $p \in P$ and there are $a, b \in Q$ such that $p = b \to 0 \leftarrow a$. Let $a \in Q$ and suppose $1a1 \leq p$ for some $p \in P$. Then $a \leq 1 \to p \leftarrow 1 = 0$, that is $a \neq 0 \Rightarrow 1a1 = 1$. Further $0 \neq 1 = 1 \cdot 1 \cdot 1 \leq 1 \cdot 1$. Consider $a \not\geq b$ and a congruence $\sim$ generated by $a \sim b$. There exists a $p \in P, p = d \to 0 \leftarrow c$ such that $a \leq p, b \not\leq p$. Then $cad = 0, cbd \neq 0, cad \sim cbd$ and thus $0 = 1cad1 \sim 1cbd1 = 1$, i. e. there are only two congruences on Q, so that Q is simple. $\square$

Let us recall from [4] the following definition.

2.6. Definition. An element p of a quantale Q is said to be *prime* if

$$a1b \leq p \Rightarrow a \leq p \text{ or } b \leq p$$

for all $a, b \in Q$. Let $\mathcal{P}(Q)$ denote the set of all primes of Q.

2.7. Theorem. *Let Q be a quantale. Then there is a bijective correspondence between cyclic sets and two-sided primes.*

Proof. Let p be a two-sided prime. Hence $p \leq 1 \to p \leftarrow 1$. We show that $P = \{a \to p \leftarrow b \mid a, b \in Q\} - \{1\}$ is cyclic. It is sufficient to prove that $1 \to (a \to p \leftarrow b) \leftarrow 1 = p$ if $a \to p \leftarrow b \neq 1$, because $c \to (a \to p \leftarrow b) \leftarrow d = (ca) \to p \leftarrow (bd) \in P$ for every $c, d \in Q$. Note that from the two-sidedness of p it follows that $a1b \leq p \Leftrightarrow a \leq p$ or $b \leq p$. Then $q \leq 1 \to (a \to p \leftarrow b) \leftarrow 1 \Leftrightarrow b1q1a \leq p \Leftrightarrow b1q \leq p$ or $a \leq p \Leftrightarrow b \leq p$ or $q \leq p$ or $a \leq p$. But from $b \leq p$ or $a \leq p$ we have $b1a \leq p$, i.e. $a \to p \leftarrow b = 1$. Thus $q \leq 1 \to (a \to p \leftarrow b) \leftarrow 1 \Leftrightarrow q \leq p$, i.e. $1 \to (a \to p \leftarrow b) \leftarrow 1 = p$ and $p = 1 \to p \leftarrow 1 \in P$.

Conversely, let P be a cyclic set, $p \in P$. Put $t = 1 \to p \leftarrow 1$, then evidently $t \in \mathcal{T}(Q)$. Since P is cyclic and $1(1 \to t)1 \leq 1t \leq t$, we have that $t \leq 1 \to t \leq 1 \to t \leftarrow 1 = t$, i.e. $1 \to t = t$ and similarly $t \leftarrow 1 = t$. Suppose now that $a1b \leq t$ and $a \not\leq t$. Then $a \not\leq 1 \to t$, i.e. $t \leftarrow a \neq 1$ and thus $t = 1 \to (t \leftarrow a) \leftarrow 1 = (1 \to t \leftarrow a) \leftarrow 1 = (t \leftarrow a) \leftarrow 1$. Hence $b \to t = b \to (t \leftarrow a) \leftarrow 1 = (b \to t \leftarrow a) \leftarrow 1 = 1 \leftarrow 1 = 1$, i.e. $b \leq t \leftarrow 1 = t$. We have proved that t is prime. $\square$

2.8. Lemma. *If $p \in \mathcal{P}(Q)$ and $a \in Q$, then $a \to p, p \leftarrow a \in \mathcal{P}(Q) \cup \{1\}$.*

Proof. $b1c \leq a \to p \Rightarrow b1 \cdot 1c \leq a \to p \Leftrightarrow b1 \cdot 1ca \leq p \Rightarrow b1 \leq p$ or $ca \leq p \Rightarrow b \leq 1 \to p \leq a \to p$ or $c \leq a \to p$. Similarly for $p \leftarrow a$. $\square$

2.9. Corollary. *Elements of cyclic sets are primes.*

2.10. Proposition. *Let Q be a quantale, P a cyclic set. For $a, b \in Q$ put*

$$a \sim b \Leftrightarrow (\forall p \in P)(a \leq p \Leftrightarrow b \leq p).$$

Then $\sim$ is a quantale congruence with the property that the quotient quantale $Q/\sim$ is simple. Conversely, if $f : Q \to K$ is a surjective morphism onto simple quantale K with separating cyclic set R, then $f^{-1}[R]$ is a cyclic set in Q.

Proof. $\sim$ is evidently a sup-lattice congruence. Suppose that $a \sim b$, i.e. $a \leq p \Leftrightarrow b \leq p$ for every $p \in P$. But then also $a \leq c \to p \Leftrightarrow b \leq c \to p$ and $a \leq p \leftarrow c \Leftrightarrow b \leq p \leftarrow c$, i.e. $ac \sim bc$ and $ca \sim cb$.

Let $g : Q \to Q/\sim$ be the corresponding quotient morphism. By definition, $g[P]$ is separating and $g^{\dashv}g|_P = id_P$. Then $g(b) \leq g(a) \to g(p) \Leftrightarrow g(ba) = g(b)g(a) \leq g(p) \Leftrightarrow ba \leq g^{\dashv}g(p) = p \Leftrightarrow b \leq a \to p \Rightarrow g(b) \leq g(a \to p)$. Since g is onto, it means that $g(a) \to g(p) = g(b)$ for some $b \in Q$ i.e. $g(a) \to g(p) \leq g(a \to p)$. Conversely, $g(a \to p) \leq g(a \to p)$ implies $g(a \to p) \leq g(a) \to g(p)$. Similarly we can show $g(p) \leftarrow g(a) = g(p \leftarrow a)$. Hence $g[P]$ is cyclic and $Q/\sim$ is simple.

The last assertion follows from $f^{\dashv}(c) \to f^{\dashv}(d) = f^{\dashv}(c \to d), f^{\dashv}(d) \leftarrow f^{\dashv}(c) = f^{\dashv}(d \leftarrow c)$. Namely, $a \leq f^{\dashv}(c) \to f^{\dashv}(d) \Leftrightarrow af^{\dashv}(c) \leq f^{\dashv}(d) \Leftrightarrow f(a)c = f(a)f(f^{\dashv}(c)) = f(af^{\dashv}(c)) \leq d \Leftrightarrow f(a) \leq c \to d \Leftrightarrow a \leq f^{\dashv}(c \to d)$ and similarly for "$\leftarrow$". $\square$

2.11. Corollary. *Let Q be a quantale. Then the following sets bijectively correspond.*

(1) two-sided primes,
(2) cyclic sets,
(3) maximal congruences,
(4) isomorphism classes of simple quotients.

2.12. Remark. (1) A semisimple factor Q is simple. Indeed, from $0 \neq 1$ it follows that Q has at least one simple quotient. On the other hand, Q has at most one two-sided prime 0. Hence the simple quotient is unique and so the quotient map is an isomorphism.

(2) A factor with at least one prime has a unique simple quotient. If p is the prime, then $1 \cdot 1 \cdot 1 \not\leq p$, i.e. $1 \to p \leftarrow 1 \neq 1$. Since $1 \to p \leftarrow 1$ is two-sided, it must be 0. By 2.8 we have that 0 is a prime. It gives a simple quotient which is unique by the same argument as in (1).

2.13. Theorem. *The following conditions are equivalent:*

(1) Q is a semisimple quantale.
(2) Q is faithful and spatial.
(3) Q is faithful and $\mathcal{T}(Q)$ is a spatial locale.
(4) The union of cyclic sets of Q is separating.

Proof. $(1) \Rightarrow (2)$: A semisimple quantale is evidently spatial. Let $a, b \in Q$ and suppose that $lar = lbr$ for all $l \in \mathcal{L}(Q), r \in \mathcal{R}(Q)$. Then for every surjective morphism $f : Q \to K$ onto simple quantale K we also have $f(l)f(a)f(r) = f(lar) = f(lbr) = f(l)f(b)f(r)$ and $\mathcal{L}(K) = f[\mathcal{L}(Q)], \mathcal{R}(K) = f[\mathcal{R}(K)]$. Thus, by the faithfulness of K, $f(a) = f(b)$ and so $a = b$.

$(2) \Rightarrow (3)$: If Q is spatial, $\mathcal{T}(Q)$ is also spatial and idempotent, i.e. it is a spatial locale [4, 8].

$(3) \Rightarrow (4)$: Let $a \not\geq b$. Then there exist $l \in \mathcal{L}(Q), r \in \mathcal{R}(Q)$ such that $lar \not\geq lbr$. Since $lar, lbr \in \mathcal{T}(Q)$ and $\mathcal{T}(Q)$ is spatial, there exists a two-sided prime p with the property $lar \leq p, lbr \not\leq p$, or equivalently $a \leq r \to p \leftarrow l, b \not\leq r \to p \leftarrow l$. Thus we have cyclic set $\{c \to p \leftarrow d \mid c, d \in Q\} - \{1\}$ separating a, b.

$(4) \Rightarrow (1)$: It follows directly from 2.10. $\square$

2.14. Remark. In [7] it was shown that every simple quantale K embeds into $\mathcal{QR}(K)$ via left action on right-sided elements. Thus every surjective morphism $f : Q \to K$ onto simple K can be extended to the quantale representation $\mu : Q \to \mathcal{QR}(K)$. One can easily check that this representation is equivalent to an arbitrary representation of the form $\mu_p : Q \to \mathcal{Q}(Q/p)$ (see [4]) where p is an element of corresponding cyclic set P. More generally, P itself (or its suitable part) can be ordered into a matrix giving an equivalent representation $\mu_P : Q \to \mathcal{Q}(Q/P)$. It means that semisimplicity could be viewed as a stricter kind of spatiality. In case of locales, every representation is of the form $f : L \to 2$ and so surjective. Hence a locale is semisimple whenever it is spatial. This result is also a consequence of the previous theorem, because $1 \wedge a \wedge 1 = a$ for every $a \in L$, i.e. locales are faithful. The interpretation of a cyclic set as a (canonical) matrix of a module will be utilized in section 4.

2.15. Example. Let S be a sup-lattice and $\mathcal{Q}(S)$ a quantale of its sup-lattice endomorphisms. Then elements of the form

$$(\rho_x \vee \lambda_y)(z) = \begin{cases} 1 & z \not\leq y, \\ x & 0 \neq z \leq y, \\ 0 & z = 0 \end{cases}$$

for $x \neq 1, y \neq 0$ form a cyclic separating set of $\mathcal{Q}(S)$. But not all primes of $\mathcal{Q}(S)$ have to be of this form. For instance, if $S = \mathcal{M}_5$ is a five-element "diamond" lattice, then the identity satisfies $\alpha 1 \beta \leq id \Leftrightarrow \alpha 1 \beta = 0$. Since 0 is a prime, id must be a prime too and it is not of the above form. The same holds for all endomorphisms arising from permutations of three atoms of $\mathcal{M}_5$.

We can construct now a proper class of non-isomorphic strong modules (see [4] for definitions of used terms). Indeed, for every index set I of arbitrary cardinality we have a prime matrix with id on the diagonal and 0 otherwise. Strong modules produced by these matrices have different cardinalities, hence they are not isomorphic. On the other hand, every quantale has only a set of cyclic sets. This example explains that, in some situations, the set of cyclic sets can be a better notion of a quantale spectrum then a set of primes or a category of strong modules.

3. *-SIMPLE AND *-SEMISIMPLE *-QUANTALES

3.1. Definition. By a **-simple *-quantale* is meant a *-quantale Q such that $1 \cdot 1 \neq 0$ and every its quotient *-morphism is either a *-isomorphism or a constant *-morphism on a trivial *-quantale. In other words, there are exactly two *-congruences on Q.

By a **-semisimple *-quantale* is meant a subdirect product of *-simple *-quantales. That is, a *-quantale is *-semisimple if it has enough surjective *-morphisms onto *-simple *-quantales to separate elements.

3.2. Definition. A *-quantale Q is called a **-factor* if $\mathcal{HT}(Q) = \{0, 1\}$ and $0 \neq 1$.

3.3. Definition. Let Q be a *-quantale. A set $P \subseteq Q$ is said to be **-separating* if $P \cup P^*$ is separating (where $P^* = \{p^* \mid p \in P\}$).

3.4. Theorem. *The following conditions are equivalent:*

*(1) Q is a *-simple *-quantale.*

*(2) Q is a faithful *-factor.*

*(3) Q has a *-separating cyclic set.*

Proof. $(1) \Rightarrow (2)$ If $t \in \mathcal{HT}(Q)$, then a mapping $a \mapsto a \vee t$ gives a surjective *-morphism. Since Q is *-simple, t is either 0 or 1, i.e. Q is *-factor. From $1 \cdot 1 \in \mathcal{HT}(Q)$ we have $1 \cdot 1 = 1$. The congruence defined in 2.5 is also a *-congruence, and by the same argument Q is faithful.

$(2) \Rightarrow (3)$ Suppose that Q is faithful *-factor. Since $1 \cdot 1 \in \mathcal{HT}(Q)$ and $1 \cdot 1 \cdot 1 \neq 1 \cdot 0 \cdot 1$, we have $1 \cdot 1 = 1$. Let $u, t \in \mathcal{T}(Q) - \{1\}$. Then $uu^*, tt^* \in \mathcal{HT}(Q)$ gives $uu^* = tt^* = 0$ and $(u \vee t)(u^* \vee t^*) = ut^* \vee u^*t \in \mathcal{HT}(Q)$ implies that $u \vee t = 1$ or $ut^* = 0$. Similarly, from $(u \vee t^*)(u^* \vee t) = ut \vee t^*u^*$ we derive $u \vee t^* = 1$ or $ut = 0$. If both $ut = 0, ut^* = 0$, then $t = 0$ or $t \vee t^* = 1$, which implies $u1 = u(t \vee t^*) = 0 \Rightarrow 1u1 = 0 \Rightarrow u = 0$ by the faithfulness. If both $u \vee t = 1, u \vee t^* = 1$, then from $t \neq 1$ we have $1 = (u \vee t)(u \vee t^*) = u^2 \vee ut^* \vee tu \vee tt^* \leq u1 \vee u1 \vee 1u \vee 0 \leq u$, a contradiction. If, for instance, $u \vee t = 1, ut = 0$, then $u1 = u1 \cdot 1 = u(u^* \vee t^*)1 = ut^*1 \leq t^*1$ and $t^*1 = t^*1 \cdot 1 = t^*(u \vee u^*)1 = t^*u1 \leq u1$, i.e. $u1 = t^*1$. Now assume $ur \neq 0$ for some $r \in \mathcal{R}(Q)$. Then we have $u1r \leq ur \leq u1 = u(ur \vee r^*u^*) = u^2r \leq u1r$. Otherwise $ur = 0 \Rightarrow u1r = 0$. That is $ur = u1r$ for every $r \in \mathcal{R}(Q)$, and hence $lur = lu1r$ for every $l \in \mathcal{L}(Q), r \in \mathcal{R}(Q)$ gives that $u = u1$. Similarly it can be shown that $t^* = t^*1$, thus $u = t^*$. In the last case $u \vee t^* = 1, ut^* = 0$, by a similar trick we derive $u = t$. Altogether, $\mathcal{T}(Q)$ is a two-element chain $\{0, 1\}$ or a four-element Boolean algebra $\{0, t, t^*, 1\}$. Put $v = 0$ or $v = t$ respectively to these two cases and $P = \{r \to v \leftarrow l \mid r \in \mathcal{R}(Q), l \in \mathcal{L}(Q)\} - \{1\}$. Then P is cyclic (see 2.5) and so is P^*. In case of $v = 0$ the set P is separating by 2.5, otherwise consider $a \not\geq b$, then $lar \not\geq lbr$ for some $l \in \mathcal{L}(Q), r \in \mathcal{R}(Q)$. Thus $lbr \not\leq w$ and $lar \leq w$ for some $w \in \{v, v^*\}$. In other words $a \leq r \to w \leftarrow l, b \not\leq r \to w \leftarrow l$.

$(3) \Rightarrow (1)$ Let $t = \bigwedge P$. From 2.4 we have that $t = 1 \to p \leftarrow 1$ for every $p \in P$. Further $1a1 \leq p$ for some $p \in P$ implies $a \leq t$, thus $1 \cdot 1 \leq p \Rightarrow 1 \cdot 1 \cdot 1 \leq p \Rightarrow 1 \leq t$, resp. $1 \cdot 1 \leq p^* \Rightarrow 1 \leq t^*$, hence $1 \cdot 1 = 1$. If $u \in \mathcal{T}(Q), u \neq 1$, then $u \leq p$ for some $p \in P \cup P^*$ and we have $u \leq 1 \to u \leftarrow 1 \leq 1 \to p \leftarrow 1 = t$ or $\ldots = t^*$, i.e. t, t^* are maximal two-sided. Consider a *-congruence $\sim$ generated by $a \sim b$ for some $a \not\geq b$. We have some $p \in P \cup P^*$ such that $a \leq p, b \not\leq p$, suppose $p \in P$. Then $p = d \to t \leftarrow c$ for some $c, d \in Q$. Put $u = 1cad1, v = 1cbd1$, from $a \leq d \to t \leftarrow c$ we have $cad \leq t$ and $u \leq 1t1 \leq t$, and similarly from $b \not\leq d \to t \leftarrow c$ we have $cbd \not\leq t = 1 \to t \leftarrow 1$, i.e. $v \not\leq t$. Now $u \sim v$ gives that $t = t \vee u \sim t \vee v = 1$. Hence also $t^* \sim 1$ and $0 = \bigwedge P \wedge \bigwedge P^* = t \wedge t^* \geq tt^* \sim 1 \cdot 1 = 1$, thus Q is *-simple. $\square$

We conclude with a *-analogy of 2.11.

3.5. Theorem. *Let Q be a *-quantale. Then the following sets bijectively correspond.*
*(1) pairs of mutually *-adjoint two-sided primes,*
*(2) pairs of mutually *-adjoint cyclic sets,*
*(3) maximal *-congruences,*
*(4) isomorphism classes of *-simple quotients.*

Similarly as in [4] 5.3., we have the following statement.

3.6. Theorem. *A *-quantale Q is *-semisimple, iff it is semisimple as a quantale.*

3.7. Remark. In [4], the first author introduced a notion of a D-spatial *-quantale because of the difference of simple and *-simple *-quantale. We have also an opportunity to introduce a similar concept. Let us call a quantale *D-semisimple* if it is a subdirect product of simple *-quantales. A cyclic set P is called **-cyclic* if $P^* = P$. An ardent reader can find appropriate analogies of 2.13, 2.11 using *-cyclic sets. One remarkable fact is that *-cyclic sets arises from hermitean two-sided primes.

4. Simple modules

In ring theory, by simple modules are meant modules without proper non-trivial submodules. One can easily see that any simple module M has also only two quotients — the trivial one and itself, because kernels of the quotient mappings are just the submodules of M. This simple fact is not longer true for the case of quantales, so we have to state the following notion of simplicity.

4.1. Definition. Let Q be a quantale. A Q-module M is said to be *simple* if
its only submodules are M and $\{0\}$,
its only quotient modules are M and $\{0\}$, and
the action is non-trivial in the sense that $1_Q \cdot 1_M \neq 0_M$.

Further, if R is a (unital) ring and M a simple faithful R-module, then R is a simple ring, i.e. its ideals are only R and $\{0\}$. Indeed, let $x \in M, x \neq 0$ and $I \subseteq R$ an ideal. Then $Ix = \{ix \mid i \in I\}$ is a submodule of M. Since M is simple, Ix is either M or $\{0\}$ and from the faithfulness we have that I is either R or $\{0\}$. Conversely, taking the ring itself we show that every simple ring has a simple faithful module. Although the "idealic" tricks are not disposal for the case of quantales, we are able to prove similar results.

4.2. Lemma. *Let Q be a quantale, M a simple Q-module. Then M^{op} is also simple and it is faithful whenever M is so.*

Proof. The first assertion is a consequence of module duality. Let M be a faithful left Q-module, $a \not\geq b$ elements of Q. We have some $m \in M$ such that $am \not\geq bm$. Then $m \leq am \leftarrow a$ but $m \not\leq am \leftarrow b$, i.e. M^{op} is faithful. □

4.3. Theorem. *Let Q be a quantale, M a non-trivial left Q-module. Then M is simple iff $Qm = \{am \mid a \in Q\} = M$ for every $m \in M, m \neq 0$ and $m \leftarrow Q = \{m \leftarrow a \mid a \in Q\} = M$ for every $m \in M, m \neq 1$.*

Proof. Let M be simple, $m \neq 0$. Note that the set Qm is a submodule of M. If $Qm = \{0\}$, then $\{0, m\}$ is a submodule with trivial action, thus it is proper — a contradiction. Hence Qm is a non-trivial submodule, i.e. it is M. Since M has only two quotients, M^{op} has only two submodules and by the same argument adapted to M^{op} we get the second assertion.
The backward implication is evident. □

4.4. Theorem. *A quantale Q is simple iff it has a simple faithful Q-module.*

Proof. Let Q be simple. We take $\mathcal{R}(Q)$ as a left Q-module. It is not hard to see that the assignment $a \sim b \Leftrightarrow (\forall r \in \mathcal{R}(Q))(ar = br)$ defines a quantale congruence. From $1 \cdot 1 \neq 0$ we have that $\sim$ is not a full relation, hence $a \sim b \Leftrightarrow a = b$. But it actually says that $\mathcal{R}(Q)$ is a faithful module. By 2.5 Q is a faithful factor. Since $1r \in \mathcal{T}(Q)$ for $r \in \mathcal{R}(Q)$, we have $1r = 1$ whenever

$r \neq 0$. Further $lr = lr1$ for $r \in \mathcal{R}(Q), l \in \mathcal{L}(Q)$, hence $r = r1$. Thus $rs = r1s = r1 = r$ for $r, s \in \mathcal{R}(Q), s \neq 0$. Using 4.3 we have that $\mathcal{R}(Q)$ is a simple module.

Conversely, let Q be a quantale and M a left simple faithful Q-module. For every $m \in M$ put $r_m = \bigvee\{a \in Q \mid a1_M \leq m\}$. From 4.3 it follows that there exists $a \in Q$ such that $a1_M = m$, hence $r_m 1_M = m$. Since $r_m 1_Q \cdot 1_M \leq r_m 1_M = m$, r_m is right-sided. Similarly, for $l_m = \bigvee\{a \in Q \mid 0_M \leftarrow a \geq m\}$ we have $0_M \leftarrow a = m$ for some $a \in Q$, hence $0_M \leftarrow l_m = m$ and $0_M \leftarrow (1_Q l_m) = (0_M \leftarrow 1_Q) \leftarrow l_m \geq 0_M \leftarrow l_m$, i.e. l_m is left-sided. If now $a \neq b$ in Q, then there is $m \in M$ such that $am \neq bm$ and thus $ar_m \neq br_m$. From 4.2 we have that M^{op} is also faithful, thus there is $n \in M$ such that $n \leftarrow (ar_m) \neq n \leftarrow (br_m)$, hence $l_n ar_m \neq l_n br_m$, i.e. Q is a faithful quantale. Finally, let $t \in \mathcal{T}(Q), t \neq 0$. From 4.3 it follows that $1_Q m = 1_M$ for every non-zero $m \in M$. Since M is faithful, $t1_M \neq 0$. Thus $tm \geq 1_Q t 1_Q m = 1_Q t 1_M = 1_M$ for every non-zero m, i.e. $t = 1$. We have proved that Q is a factor, and hence Q is a simple quantale by 2.5. □

4.5. Corollary. *Let Q be a quantale. Then (isomorphism classes of) simple Q-modules bijectively correspond to cyclic sets on Q.*

Proof. For a simple Q-module M consider a set of elements $p_n^m = \bigvee\{a \in Q \mid an \leq m\}$ for all pairs $(m, n) \in M \times M$. By similar calculations as in the proof of 4.4 we get $p_n^m = r_m \vee l_n$ and $r_x \to p_n^m \leftarrow l_y = p_x^y$ whenever $m \neq 1, n \neq 0$, hence $P = \{p_n^m \mid m \neq 1, n \neq 0\}$ is cyclic.

Conversely, for a cyclic set P take arbitrary $p \in P$ and put $M = \{a \to p \mid a \in Q\}$. Then M with operations $\bigwedge, \to$ forms a left Q-module. ¿From [4] it follows that the dual module is $M^{op} = \{p \leftarrow a \mid a \in Q\}$ with $\bigwedge, \leftarrow$. Hence the condition in 4.3 is fulfilled and M is simple.

An element $n \in M$ corresponds to a subset $\{p_n^m \mid m \in M, m \neq 1\}$. It is not hard to check that $a \to p_n^m = p_{an}^m$ if $m \neq 1$, i.e. the module action on M works as $\to$ on P. Finally, the assignment $n \mapsto p_n^-$ converts $\bigvee$ in M to $\bigwedge$ in P. □

4.6. Corollary. *A quantale Q is semisimple iff a family of simple Q-modules separates elements, i.e. for $a \neq b$ there is a simple module M and $m \in M$ such that $am \neq bm$.*

4.7. Remark. If Q is a *-quantale, then for every left Q-module M there is a right Q-module M^* with the same sup-lattice structure but with an action "$*$" given by $m * a = a^* m$. Using duality we have a left Q-module M^{*op}. Obviously, M^{*op} is simple iff M is so. One can check that if P is a cyclic set of Q and defines a module M, then P^* defines M^{*op}. If P is *-cyclic, then $M \cong M^{*op}$, i.e. M is a *-module (cf. [4]).

5. Simple quantales versus C*-algebras

In this section, we point out which role the notion of cyclic sets can play in theory of C*-algebras. A non-expert reader is recommended to some monograph, e.g. [3], and a substantive paper [6].

5.1. Definition. Recall from [6] that by a *spectrum* of a C*-algebra A is meant a *-quantale $\operatorname{Max} A$ of all closed subspaces of A with operations

$$\bigvee X_i = \overline{\sum X_i},$$
$$XY = \overline{\{xy \mid x \in X, y \in Y\}}.$$

5.2. Example. Let $A = M_2(\mathbb{C})$ be an algebra of 2×2 matrices over $\mathbb{C}$, i.e. A is a C*-algebra of all (bounded) linear operators on a 2-dimensional Hilbert space. By easy computations we see that all proper non-zero right ideals of A are of the form

$$R_{k,l} = \left\{ \begin{pmatrix} ka & kb \\ la & lb \end{pmatrix} \middle| \, a, b \in \mathbb{C} \right\}$$

for some fixed $k, l \in \mathbb{C}, k^2 + l^2 = 1$. Similarly, proper non-zero left-sided ideals of A are of the form

$$L_{k,l} = \left\{ \begin{pmatrix} ka & la \\ kb & lb \end{pmatrix} \middle| \, a, b \in \mathbb{C} \right\}.$$

Thus all of these right (left) ideals are maximal and $R^*_{k,l} = L_{\bar{k},\bar{l}}$. From the theory of operator algebras it follows that a given functional on a C*-algebra is a pure state iff its kernel is $R \vee R^*$ for some maximal right ideal R. Further, $AMA = A$ for every non-zero matrix M, hence $AXA = A$ for every non-zero (closed) subspace X of A and thus $A \to X \leftarrow A = \{0\}$ for every proper subspace X. This guarantees that the set $P = \{X \to \{0\} \leftarrow Y \mid X, Y \in \operatorname{Max} A\}$ is cyclic. We assert that P contains all kernels of pure functionals (see 5.4) of A. Indeed, $L_{l,-k} R_{k,l} = \{0\}$ and we observe that $R_{k,l}$ is the greatest subspace with this property, i.e. $R_{k,l} = \{0\} \leftarrow L_{k,-l}$. By similar computations we get

$$R_{k,l} \vee L_{m,n} = R_{n,-m} \to \{0\} \leftarrow L_{l,-k},$$

particularly for $m = \bar{k}, n = \bar{l}$ it gives a kernel of a pure state. Further, one could easily check that every one-dimensional subspace of A is a meet of elements of the form $R \vee L$ for some maximal right ideal R and some maximal left ideal L. Although P is not a separating set for P, from the above observation it follows that P separates atoms of $\operatorname{Max} A$. So $\operatorname{Max} A$ is "almost simple",[3] and the algebra A can be fully recovered from $\operatorname{Max} A$. By little more complicated calculations one can get a similar result for every $M_n(\mathbb{C}), n \in \mathbb{N}$.

Since pure states separate elements in arbitrary C*-algebra, one could hope that its spectrum holds the above properties. Unfortunately, two irreducible representations of a general C*-algebra may have the same kernel but they need not be equivalent. This is the main reason why not all pure states are contained in cyclic sets. Thus we do not know if cyclic sets are separating for one-dimensional subspaces.

A way out could arise from the following concept.

[3]It is mentioned in [8] that $\operatorname{Max} A$ contains a subspace not reachable by primes, hence it is not spatial in the sense of [9, 4].

5.3. Definition. Let Q be a quantale, S its multiplicative subsemigroup such that $0 \in S$.

A set P is called *S-separating* if for every $a, b \in S, a \ngeq b$ there is an element $p \in P$ provided that $a \leq p, b \nleq p$.

A set P is called *residually S-closed* if $a \to p, p \leftarrow a \in P \cup \{1\}$ for every $a \in S, p \in P$.

A nonempty set $P, 1 \notin P$ is called *S-cyclic* if $\{a \to p \leftarrow b \mid a, b \in S\} = P \cup \{1\}$ for every $p \in P$.

5.4. Example. Let A be a C*-algebra. Put

$$S = \{\langle a \rangle \mid a \in A\},$$

where $\langle a \rangle$ denotes a one-dimensional subspace spanned by a,

$$P = \{\ker \phi(a \lrcorner b) \mid a, b \in A, \phi \text{ is a pure state}\},$$

i.e. P contains subspaces of codimension 1 and 0 which are kernels of functionals of the form $\phi(a \lrcorner b)$, so called *pure functionals*. ¿From the general theory of C*-algebras we know that pure states correspond to vector states of irreducible representations. More generally, pure functionals correspond to vector functionals. If a, b are two linearly independent elements of A, then there exists an irreducible representation $\pi : A \to \mathcal{B}(H)$ in which $\pi(a), \pi(b)$ are also independent, i.e. we can choose a basis of H such that one of a, b vanishes at some matrix element, while the second one is nonzero, for instance suppose $(\eta \mid \pi(a)\zeta) = 0, (\eta \mid \pi(b)\zeta) \neq 0$ for some $\eta, \zeta \in H$. Put $\phi = (\eta \mid \pi(\lrcorner)\zeta)$ and we have that $\langle a \rangle \leq \ker \phi, \langle b \rangle \nleq \ker \phi$, hence P is S-separating. One can see that

$$\langle b \rangle \to \ker \phi \leftarrow \langle a \rangle = \ker \phi(a \lrcorner b),$$

thus P is residually S-closed. Now we will show that the set

$$P_\phi = \{\ker \phi(a \lrcorner b) \mid a, b \in A, \phi(a \lrcorner b) \neq 0\}$$

for some fixed pure state ϕ is S-cyclic. If $\phi(a \lrcorner a^*)$ is nonzero, then it is (real) multiple of some other equivalent pure state ψ (i.e. $\ker \phi(a \lrcorner a^*) = \ker \psi$) and so there is some unitary $u \in A$ such that $\psi(u \lrcorner u^*) = \phi$ and thus $\ker \phi = \ker \phi(ua \lrcorner a^* u^*)$. Similarly, we can find unitary v such that $\ker \phi = \ker \phi(v^* b^* \lrcorner bv)$. Hence $\langle a^* u^* v \rangle \to \ker \phi(a \lrcorner b) \leftarrow \langle v^* b^* u \rangle = \ker \phi(v^* b^* (ua \lrcorner ba^* u^*) v) = \ker \phi(v^* b^* \lrcorner bv) = \ker \phi$. We conclude that the union of S-cyclic sets of $\operatorname{Max} A$ is S-separating for arbitrary C*-algebra A.

One tantalizing question left open is whether there are appropriate concepts of S-faithful, S-simple, S-semisimple quantales. Is there some link to simple and semisimple C*-algebras? We hope that an answer to this question, in either direction, will shed some light on the current debate about the quantale—C*-algebra connections.

References

[1] Abramsky, S., and Vickers, S. Quantales, observational logic and process semantics. *Mathematical Structures in Computer Science 3(2)* (1993), 161–227.

[2] Giles, R., and Kummer, H. A non-commutative generalization of topology. *Indiana University Mathematics Journal 21(1)* (1971), 91–102.

[3] Kadison, R. V., and Ringrose, J. R. *Fundamentals of the Theory of Operator Algebras I, II*, vol. 15, 16 of *Graduate Studies in Mathematics*. American Mathematical Society, 1997.

[4] Kruml, D. Spatial quantales. *Applied categorical structures* (2000). In print.

[5] MULVEY, C. J. &. *Supplemento ai Rendiconti del Circolo Matematico di Palermo II(12)* (1986), 99–104.
[6] MULVEY, C. J., AND PELLETIER, J. W. On the quantisation of points. *Journal of Pure and Applied Algebra* (2000). In print.
[7] PASEKA, J. Simple quantales. In *Proceedings of the Eighth Prague Topological Symposium* (1997), Topology Atlas, pp. 314–428.
[8] PASEKA, J., AND ROSICKÝ, J. Quantales. In *Current Research in Operational Quantum Logic: Algebras, Categories and Languages* (2000), vol. 111 of *Fundamental Theories of Physics*, Kluwer Academic Publishers, pp. 245–262.
[9] PELLETIER, J. W., AND ROSICKÝ, J. Simple involutive quantales. *Journal of Algebra 195* (1997), 367–386.
[10] ROSENTHAL, K. I. *Quantales and their applications*, vol. 234 of *Pitman Research Notes in Mathematics Series*. Longman, Essex, 1990.

DEPARTMENT OF MATHEMATICS, MASARYK UNIVERSITY, JANÁČKOVO NÁM. 2A, 635 00 BRNO
E-mail address: `kruml@math.muni.cz, paseka@math.muni.cz`