Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **27** (2019). Number 1, pp. 37–49

The lattice of quasivarietes of modules over a Dedekind ring*

Přemysl Jedlička, Katarzyna Matczak, Anna Mućka

Communicated by A. I. Kashu

Abstract. In 1995 D. V. Belkin described the lattice of quasivarieties of modules over principal ideal domains [1]. The following paper provides a description of the lattice of subquasivarieties of the variety of modules over a given Dedekind ring. It also shows which subvarieties of these modules are deductive (a variety is deductive if every subquasivariety is a variety).

Introduction

There are many algebraic structures that are polynomially equivalent to modules; typical examples are abelian algebras with a Mal'tsev term. However, in most cases these modules are over rings with no interesting algebraic properties. There are exceptions though, for instance finite idempotent entropic quasigroups. Since the work of Toyoda [12], we know that a finite idempotent entropic quasigroup is polynomially equivalent to a module over $\mathbb{Z}[x]/(x^n - 1)$, for some n, and these rings are well described in commutative algebra; we know, for instance, that they are products of pairwise different Dedekind domains [14].

Since the polynomial equivalence preserves congruences, it is natural to study varieties and quasivarieties in better understood equivalent algebras,

*The joint research within the framework of the Polish-Czech cooperation grant no. 7AMB13PL013 and no. 8829/R13/R14.

2010 MSC: 08A62, 08C15, 20N02, 20N05.

Key words and phrases: quasivarieties, lattices, modules, Dedekind rings.

if there are some. Unfortunately, until recently, the only known facts concerning quasivarieties of modules were provided by Belkin [1] who characterised all the quasivarieties of modules over principal ideal domains, effectively generalizing the result of Vinogradov [13].

A natural question arises here: does Belkin's result apply to principal ideal domains only or can it be extended to a broader class of domains? We cannot definitely hope to extend it to the class of all domains since the structure of general domains could be very wild. Nevertheless, it turned out that the key property that Belkin used was the unique factorization of principal ideals into a product of principal prime ideals. If we drop the word "principal" then we naturally come up with the notion of a Dedekind domain. Although the generalization could seem to come directly, it is not straightforward as the structure of modules over Dedekind rings is not well described in general. Fortunately, we are actually interested in quasivarieties and they are always generated by finitely generated algebras. Hence what we really need are finitely generated Dedekind modules only. Their structure, although more complicated than the structure of principal ideal domains, is quite well understood.

The article has the following structure: In Section 1 we define Dedekind rings and recall some properties of finitely generated modules over Dedekind rings. We present Belkin's result here too. In Section 2 we focus on deductive varieties. Section 3 is the core of the paper with the main result, namely Theorem 7, describing the quasi-varieties lattice of modules over Dedekind rings. Finally, in Section 4 we present an example how our result translates to a completely different setting.

1. Basic facts

In this section we recall some properties of finitely generated modules over a Dedekind domain. All the statements in this sections are well known [14].

Definition 1. A ring $\mathcal{R}$ is said to be *a Dedekind ring* if it is an integral domain and if every nonzero proper ideal of $\mathcal{R}$ is a product of prime ideals.

If $\mathcal{R}$ is a Dedekind ring then the product decomposition of ideals is unique, up to a permutation. Let $\mathfrak{a}$ be an ideal of $\mathcal{R}$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{R}$. Then $\mathfrak{p}$ appears in the decomposition of $\mathfrak{a}$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$. Let $\mathfrak{a}$ be a nonzero ideal of a Dedekind domain and let r be any nonzero element of $\mathfrak{a}$. Then $\mathfrak{a}$ can be generated by two elements, one of which is r.

Theorem 1 ([9, Theorem 1.41]). *Let $\mathcal{M}$ be a finitely generated non-trivial torsion $\mathcal{R}$-module. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ in $\mathcal{R}$ and positive natural numbers k_i for $i = 1, \ldots, n$, such that $\mathcal{M}$ is isomorphic to the sum*

$$\mathcal{M} \cong \mathcal{R}/\mathfrak{p}_1^{k_1} \oplus \ldots \oplus \mathcal{R}/\mathfrak{p}_n^{k_n}.$$

Corollary 1. *Let $\mathcal{M}$ be a finitely generated non-trivial torsion module. Then every homomorphic image of $\mathcal{M}$ embeds into $\mathcal{M}$.*

Lemma 1 ([9, Lemma 1.38]). *For every domain R, any finitely generated and torsion-free R-module M is a submodule of a free R-module.*

Lemma 2. *Let $\mathcal{M}$ be a finitely generated non-trivial module over $\mathcal{R}$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{R}$. We define $\mathcal{M}_{\mathfrak{p}} = \{x \in \mathcal{M},\ \mathfrak{p}^m(x) = (0),\ \text{for some } m\}$. Then there exist $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_n$ such that*

$$\mathcal{M}_{\mathfrak{p}} \cong \mathcal{R}/\mathfrak{p}^{k_1} \oplus \ldots \oplus \mathcal{R}/\mathfrak{p}^{k_n}.$$

Theorem 2 ([9, Theorem 1.32]). *Let $\mathcal{M}$ be a finitely generated non-trivial $\mathcal{R}$-module and $\mathcal{M}_T$ be its submodule consisting of all torsion elements, i.e., of all elements $x \in \mathcal{M}$, which, for some non-zero $r \in \mathcal{R}$, satisfy $rx = 0$. Then $\mathcal{M}$ is isomorphic to a direct sum*

$$\mathcal{M} \cong \mathcal{R}^n \oplus \mathfrak{a} \oplus \mathcal{M}_T,$$

where $n \in \mathbb{N}$ and $\mathfrak{a}$ is an ideal of $\mathcal{R}$.

In a variety of modules over PID every ideal, as an R-module, is isomorphic to the free R-module R. This is not true for Dedekind rings in general. For a Dedekind domain $\mathcal{R}$ which is not PID, there are infinitely many non-isomorphic ideals and therefore infinitely many non-isomorphic and torsion-free $\mathcal{R}$-modules.

The lattice of quasivarieties of modules over a principal ideal domain was described in [1] as follows. Let $\mathcal{R}$ be a principal ideal domain and $\mathbb{P}$ be the set of all prime elements of the ring $\mathcal{R}$. The lattice $\mathcal{L}_q(\mathbf{Mod}_{\mathcal{R}})$ of subquasivarieties of $\mathbf{Mod}_{\mathcal{R}}$ over $\mathcal{R}$ may be characterized using the lattice $\mathcal{L}(\alpha)$ introduced by Belkin [1], and defined as follows:

Definition 2 ([1]). Let α be a set and let α^+ denote the union $\alpha \cup \{\infty\}$. Then $\mathcal{L}(\alpha)$ is defined to be the set of all functions $f : \alpha^+ \to \mathbb{N}^+$ satisfying

- $f(\infty) \in \{0, \infty\}$,
- if $f(\infty) = 0$ then $f(i) \neq \infty$, for all $i \in \alpha$, and moreover $f(i) = 0$, for almost all $i \in \alpha$.

The set $\mathcal{L}(\alpha)$ is a distributive lattice with respect to the natural order

$$f \leqslant g \textit{ if and only if } f(i) \leqslant g(i), \textit{ for each } i \in \alpha.$$

Note also that, for two sets α and β, we have $\mathcal{L}(\alpha) \cong \mathcal{L}(\beta)$ if and only if $|\alpha| = |\beta|$.

Theorem 3. *[1, Theorem 2.1] Let the ring $\mathcal{R}$ be a principal ideal domain, and denote by $\mathbb{P}$ the set of prime elements in the ring $\mathcal{R}$. Then the lattice of quasivarieties of the variety of modules over the ring $\mathcal{R}$ is isomorphic to the lattice $\mathcal{L}(\mathbb{P})$, i.e.,*

$$\mathcal{L}_q(\mathbf{Mod}_{\mathcal{R}}) \cong \mathcal{L}(\mathbb{P}).$$

2. Deductive subvarieties of the variety of modules over a Dedekind ring

In Theorem 3, a part of the quasivarieties lattice consists of varieties only, namely those quasivarieties generated by finite modules. The same happens in the Dedekind case, as we shall see in this section. What are finite Dedekind modules? The variety corresponding to an ideal $\mathfrak{a}$ is generated by the module $\mathcal{R}/\mathfrak{a}$ and denoted by $\mathcal{V}_{\mathfrak{a}}$. As any ideal $\mathfrak{a}$ of a Dedekind domain has two generators r and p, it follows that the subvariety corresponding to this ideal is defined by two identities $px = 0$ and $rx = 0$.

The following result is well-known.

Theorem 4. *Let $\mathcal{R}$ be an arbitrary ring. The lattice of subvarieties $\mathcal{L}_v(\mathbf{Mod}_{\mathcal{R}})$ of the variety $\mathbf{Mod}_{\mathcal{R}}$ of modules over the ring $\mathcal{R}$ is dually isomorphic to the lattice of ideals of $\mathcal{R}$.*

Definition 3. We say that a variety $\mathcal{V}$ is *deductive* if each subquasivariety of $\mathcal{V}$ is a variety.

We want to prove that every proper subvariety of $\mathbf{Mod}_{\mathcal{R}}$ where $\mathcal{R}$ is a Dedekind domain is deductive. It is not difficult to prove directly but it is still easier to use a characterization of deductive varieties provided by L. Hogben and C. Bergman [4].

Definition 4. An algebra $\mathrm{P} \in \mathcal{V}$ is *primitive* if P is finite, subdirectly irreducible and, for all $\mathrm{A} \in \mathcal{V}$, if P is a homomorphic image of A, then P is isomorphic to a subalgebra of A.

Theorem 5 ([4, Theorem 3.4]). *Let $\mathcal{V}$ be residually finite and of finite type, or residually and locally finite. Then $\mathcal{V}$ is deductive if and only if every subdirectly irreducible algebra in $\mathcal{V}_{SI}$ is primitive.*

Corollary 2. *Let $\mathcal{R}$ be a Dedekind domain. Each proper subvariety of the variety $\mathbf{Mod}_{\mathcal{R}}$ is deductive.*

Proof. Every proper subvariety of $\mathcal{R}$ is $\mathcal{V}_{\mathfrak{a}}$, for some ideal $\mathfrak{a}$. This variety is locally finite. The subdirectly irreducible members of the variety $\mathcal{V}_{\mathfrak{a}}$ are $\mathcal{R}/\mathfrak{p}^k$, for some natural k such that $\mathfrak{p}^k|\mathfrak{a}$ and $\mathfrak{p}$ is a prime ideal, and hence $\mathcal{V}_{\mathfrak{a}}$ is residually finite. According to Corollary 1, all homomorphic images of torsion modules are submodules and hence all subdirectly irreducibles are primitive. □

Theorem 6. *Let $\mathcal{R}$ be a Dedekind domain and let $\mathfrak{a}$ be an ideal of this ring. The lattice $\mathcal{L}_q(\mathcal{V}_{\mathfrak{a}}) = \mathcal{L}_v(\mathcal{V}_{\mathfrak{a}})$ is isomorphic to the lattice of divisors of $\mathfrak{a}$ under divisibility.*

3. The lattice of subquasivarieties of the variety of modules over a Dedekind ring

In this section we show that the lattice of quasivarieties of modules over a Dedekind domain $\mathcal{R}$ depends only on the number of prime ideals of the ring $\mathcal{R}$. Moreover, we shall construct quasi-identities defining every quasivariety. Throughout all the section, $\mathcal{R}$ is a Dedekind domain.

Lemma 3. *For every Dedekind domain $\mathcal{R}$ and $\mathfrak{a}$ is an ideal of $\mathcal{R}$, we have:*

$$\mathcal{Q}(\mathcal{R}^n \oplus \mathfrak{a}) = \mathcal{Q}(\mathcal{R}).$$

Proof. According to Lemma 1, any finitely generated and torsion-free R-module is a submodule of a free R-module and therefore there exists m, such that

$$\mathcal{Q}(\mathcal{R}^n \oplus \mathfrak{a}) \subseteq \mathcal{Q}(\mathcal{R}^m) = \mathcal{Q}(\mathcal{R}).$$

The other inclusion is trivial. □

Lemma 4. *The quasivariety $\mathcal{Q}(\mathcal{R})$ generated by the $\mathcal{R}$-module $\mathcal{R}$ is the only minimal quasivariety which is not a variety. The $\mathcal{R}$-module $\mathcal{R}$ is relatively subdirectly irreducible in the quasivariety $\mathcal{Q}(\mathcal{R})$.*

Proof. The only non-trivial submodules of $\mathcal{R}$ are non-trivial ideals of $\mathcal{R}$ which contain submodules isomorphic to $\mathcal{R}$. Hence $\mathcal{Q}(\mathcal{R})$ is minimal. All quasivarieties contain either $\mathcal{R}$ or $\mathfrak{a}$ or some quotient of $\mathcal{R}$. □

If a Dedekind domain $\mathcal{R}$ is PID then $\mathcal{R}$-module $\mathcal{R}$ is the only relatively subdirectely irreducible in the quasivariety $\mathcal{Q}(\mathcal{R})$. If $\mathcal{R}$ is a Dedekind domain which is not PID then the quasivariety $\mathcal{Q}(\mathcal{R})$ contains infinitely many non-isomorphic relatively subdirectly irreducible modules.

Lemma 5. *Let $\mathfrak{a}$, $\mathfrak{a}_1$, $\dots$, $\mathfrak{a}_n$, $n \geqslant 0$, be ideals of $\mathcal{R}$. Then $\mathfrak{a}$ is relatively subdirectly irreducible in the quasivariety $\mathcal{Q}(\mathcal{R}, \mathcal{R}/\mathfrak{a}_1, \dots, \mathcal{R}/\mathfrak{a}_n)$. On the other hand, every finitely generated relatively subdirectly irreducible $\mathcal{R}$-module in this quasivariety is either finite subdirectly irreducible or isomorphic to an ideal $\mathfrak{a}$.*

Proof. The $\mathcal{Q}$-congruence lattice of a $\mathcal{R}$-module $\mathfrak{a}$ has the monolith: the smallest non-trivial $\mathcal{Q}$-ideal is $\mathfrak{a}(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n)$. On the other hand, every finitely generated $\mathcal{R}$-module is isomorphic to $\mathcal{R}^n \oplus \mathfrak{a} \oplus \mathcal{M}_T$, according to Theorem 2. Hence every relatively subdirectly irreducible is either isomorphic to $\mathfrak{a}$ or finite torsion module. And a quasivariety generated by a finite module is a variety hence all relatively subdirectly irreducible are subdirectly irreducible. □

Lemma 6. *Let $\mathfrak{a}_i$, for $i \in \mathbb{N}$, be pairwise different ideals of $\mathcal{R}$. Then the $\mathcal{R}$-module $\mathcal{R}$ belongs to any quasivariety $\mathcal{Q}$, containing all $\mathcal{R}/\mathfrak{a}_i$, for $i \in \mathbb{N}$. Moreover, the $\mathcal{R}$-module $\mathcal{R}$ is not subdirectly irreducible relatively to $\mathcal{Q}$.*

Proof. The ideal $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots$ is trivial and hence the $\mathcal{Q}$-congruence lattice of the $\mathcal{R}$-module $\mathcal{R}$ does not have a monolith. And this means that we have $\mathcal{R} \leqslant \prod \mathcal{R}/\mathfrak{a}_i$. □

Recall that each ideal in a Dedekind domain is generated by two elements. In the sequel we will define quasi-identities that distinguish specific prime ideals. In particular, we need to measure the valuation of prime ideals, optimally by a single element for each prime ideal. If the prime ideal is principal then we, naturally, use the generator. If it is not principal then an arbitrary generator does not need to do the job.

Lemma 7. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{R}$. Let $a \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$. Then $a^k \in \mathfrak{p}^k \smallsetminus \mathfrak{p}^{k+1}$, for each $k \in \mathbb{N}$.*

Proof. The decomposition of (a) is $(a) = \mathfrak{p} \cdot \prod \mathfrak{q}_i^{n_i}$, for some prime ideals $\mathfrak{q}_i$ distinct from $\mathfrak{p}$ and exponents n_i, since $a \in \mathfrak{p}$ and $a \notin \mathfrak{p}^2$. Now $(a^k) = (a)^k = \mathfrak{p}^k \cdot \prod \mathfrak{q}_i^{kn_i}$, showing the claim. □

For the rest of the section we shall use the following notation: fix $\mathfrak{a}$, an ideal of $\mathcal{R}$, and let $\mathfrak{a} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_n^{k_n}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are pairwise different prime ideals. As each prime ideal $\mathfrak{p}_i$, for $i \in \{1, 2, \dots, n\}$, has two generators, we write

$$\mathfrak{p}_i = (p_{\mathfrak{p}_i};\ q_{\mathfrak{p}_i})$$

(if $\mathfrak{p}_i$ is principal then $q_{\mathfrak{p}_i}$ can be arbitrary, e.g. 0) and we always choose $p_{\mathfrak{p}_i} \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Such an element always exists since $\mathfrak{p}_i \supsetneq \mathfrak{p}_i^2$ due to uniqueness of the decomposition.

Now, since $p_{\mathfrak{p}_i}^{k_i}$ lies in $\mathfrak{p}_i^{k_i}$, there exists an element $q_{\mathfrak{p}_i^{k_i}} \in \mathfrak{p}_i^{k_i}$, such that

$$\mathfrak{p}_i^{k_i} = (p_{\mathfrak{p}_i}^{k_i};\ q_{\mathfrak{p}_i^{k_i}})$$

and analogously there exists an element $q_{\mathfrak{a}}$, such that

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_n^{k_n} = \left(\prod_{i \in \{1,\dots,n\}} p_{\mathfrak{p}_i}^{k_i};\ q_{\mathfrak{a}} \right).$$

The subvariety $\mathcal{V}(\mathcal{R}/\mathfrak{a})$ of $\mathbf{Mod}_{\mathcal{R}}$ is defined by only two identities:

$$\mathrm{Mod} \left\{ \prod_{i \in \{1,\dots,n\}} p_{\mathfrak{p}_i}^{k_i} x = 0;\ q_{\mathfrak{a}} x = 0 \right\} = \mathcal{V}(\mathcal{R}/\mathfrak{a})$$

and by the Chinese remainder theorem

$$\mathcal{V}(\mathcal{R}/\mathfrak{a}) = \mathcal{V}(\prod_{i \in \{1,\dots,n\}} \mathcal{R}/\mathfrak{p}_i^{k_i}) = \mathcal{V}(\mathcal{R}/\mathfrak{p}_1^{k_1}, \mathcal{R}/\mathfrak{p}_2^{k_2}, \dots, \mathcal{R}/\mathfrak{p}_n^{k_n}).$$

Lemma 8. *Let $\mathfrak{p}^{k+1} = (p_{\mathfrak{p}}^{k+1}, q_{\mathfrak{p}^{k+1}})$ be the $k+1$-th power of a prime ideal $\mathfrak{p} = (p_{\mathfrak{p}}, q_{\mathfrak{p}})$ of the ring $\mathcal{R}$, for some $k \in \mathbb{N}$. If*

$$\mathcal{Q} = \mathrm{Mod}(p_{\mathfrak{p}}^{k+1} x = 0 \ \ \& \ \ q_{\mathfrak{p}^{k+1}} x = 0 \ \rightarrow \ p_{\mathfrak{p}}^{k} x = 0),$$

then the module $\mathcal{R}/\mathfrak{p}^{k+1}$ does not belong to the quasivariety $\mathcal{Q}$ whereas $\mathcal{R}/\mathfrak{p}^{k}$ belongs to the quasivariety $\mathcal{Q}$.

Proof. Taking the element $1 + \mathfrak{p}^{k+1} \in \mathcal{R}/\mathfrak{p}^{k+1}$, we have $p_{\mathfrak{p}}^{k+1}(1 + \mathfrak{p}^{k+1}) = 0 + \mathfrak{p}^{k+1}$ since $p_{\mathfrak{p}}^{k+1} \in \mathfrak{p}^{k+1}$ and $p_{\mathfrak{p}}^{k}(1 + \mathfrak{p}^{k+1}) \neq 0 + \mathfrak{p}^{k+1}$, according to Lemma 7. Moreover $q_{\mathfrak{p}^{k+1}}(1 + \mathfrak{p}^{k+1}) = 0 + \mathfrak{p}^{k+1}$ and therefore the element $1 + \mathfrak{p}^{k+1}$ satisfies the premises of the quasi-identity and does not satisfy the conclusion. Hence

$$\mathcal{R}/\mathfrak{p}^{k+1} \nvDash (p_{\mathfrak{p}}^{k+1} x = 0 \ \& \ q_{\mathfrak{p}^{k+1}} x = 0 \rightarrow p_{\mathfrak{p}}^{k} x = 0).$$

On the other hand,

$$\mathcal{R}/\mathfrak{p}^k \models (p_{\mathfrak{p}}^{k+1}x = 0 \ \& \ q_{\mathfrak{p}^{k+1}}x = 0 \to p_{\mathfrak{p}}^k x = 0),$$

because each element of the module $\mathcal{R}/\mathfrak{p}^k$ satisfies the conclusion of the quasi-identity. □

Remark 1. If $k = 0$ in the previous lemma then the quasi-identity is of the form:

$$p_{\mathfrak{p}}x = 0 \ \& \ q_{\mathfrak{p}}x = 0 \to x = 0$$

and each element of the module $\mathcal{R}/\mathfrak{p}$ satisfies the premises of the quasi-identity but only 0 satisfies the conclusion.

As in the case of PID, the lattice $\mathcal{L}_q(\mathbf{Mod}_{\mathcal{R}})$ is isomorphic to a lattice defined in Definition 2.

Theorem 7. *Let $\mathcal{R}$ be a Dedekind ring. Then the lattice of quasivarieties of the variety of modules over the Dedekind ring $\mathcal{R}$ is isomorphic to the lattice $\mathcal{L}(\mathbb{P}(\mathcal{R}))$, where $\mathbb{P}(\mathcal{R})$ is the set of all prime ideals of $\mathcal{R}$. The isomorphism $\varphi : \mathcal{L}(\mathbb{P}(\mathcal{R})) \to \mathcal{L}_q(\mathbf{Mod}_{\mathcal{R}})$ is defined as follows:*

$$\varphi(f) = \operatorname{Mod} \Sigma_f,$$

where Σ_f is the set of quasi-identities:

(a) *if $f(\infty) = \infty$, then Σ_f contains all the quasi-identities*

$$(p_{\mathfrak{p}}^{f(\mathfrak{p})+1}x = 0 \ \& \ q_{\mathfrak{p}^{f(\mathfrak{p})+1}}x = 0 \to p_{\mathfrak{p}}^{f(\mathfrak{p})}x = 0),$$
$$\textit{for any } \mathfrak{p} \in \mathbb{P}(\mathcal{R}), \ \textit{with } f(\mathfrak{p}) \neq \infty, \quad (\beta_{\mathfrak{p}^{f(\mathfrak{p})}})$$

(b) *if $f(\infty) = 0$, then Σ_f contains only two identities:*

$$\prod_{f(\mathfrak{p})\neq 0} p_{\mathfrak{p}}^{f(\mathfrak{p})}x = 0 \quad \& \quad q_{\mathfrak{a}}x = 0, \qquad (\gamma_{\mathfrak{p}^{f(\mathfrak{p})}})$$

where $\mathfrak{a} = \prod_{f(\mathfrak{p})\neq 0} \mathfrak{p}^{f(\mathfrak{p})}$.

Proof. We show first that the function φ is surjective. Let $\mathcal{Q}$ be a subquasivariety of $\mathbf{Mod}_{\mathcal{R}}$. Let us define a function $f : \mathbb{P}(\mathcal{R})^+ \to \mathbb{N}^+$ as follows

$$f(\infty) = \begin{cases} \infty & \text{if } \ \mathcal{R} \in \mathcal{Q}, \\ 0 & \text{if } \ \mathcal{R} \notin \mathcal{Q}, \end{cases}$$
$$f(\mathfrak{p}) = \sup\{k; \ \mathcal{R}/\mathfrak{p}^k \in \mathcal{Q}\}.$$

The function f is well defined: we see $f(\infty) \in \{0, \infty\}$ and we prove that $f(\infty) = 0$ implies $f(\mathfrak{p}) < \infty$, for all $\mathfrak{p}$, and $f(\mathfrak{p}) = 0$, for almost all $\mathfrak{p}$. Suppose first, by contradiction, that $f(\infty) = 0$ and $f(\mathfrak{p}) = \infty$ for some prime ideal $\mathfrak{p}$. Then, according to Lemma 6, we obtain $\mathcal{R} \in \mathcal{Q}$ which contradicts with $f(\infty) = 0$. Suppose now, that the number of elements of the set $\mathcal{I} = \{\mathfrak{p}; f(\mathfrak{p}) \neq 0\}$ is infinite. Then, according to Lemma 6 again, $\mathcal{R} \in \mathcal{Q}$, a contradiction.

We show now that $\operatorname{Mod} \Sigma_f = \varphi(f) = \mathcal{Q}$. Consider two cases:

(a) $f(\infty) = \infty$: Let the module $\mathcal{M} \in \mathcal{Q}$, $f(\mathfrak{p}) \neq \infty$ and let there exists an element $m \in \mathcal{M}$ such that $p_{\mathfrak{p}}^{f(\mathfrak{p})+1} m = 0$ & $q_{\mathfrak{p}^{f(i)+1}} m = 0$. Then the premises of the quasi-identity $(\beta_{\mathfrak{p}^{f(\mathfrak{p})}})$ hold and the ideal (m) is a finitely generated $\mathcal{R}$-module and therefore we can use Lemma 2. We obtain

$$(m) = (m)_{\mathfrak{p}_i} \cong \mathcal{R}/\mathfrak{p}_i^{k_1} \oplus \ldots \oplus \mathcal{R}/\mathfrak{p}_i^{k_n},$$

for some $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_n$. Since, by definition, $k_n \leqslant f(\mathfrak{p})$, according to Lemma 7, we obtain $\mathfrak{p}_i^{f(i)} m = 0$, $\mathcal{M} \models \beta_{\mathfrak{p}_i^{f(i)}}$ and $\mathcal{Q} \subseteq \operatorname{Mod} \Sigma_f$.

On the other hand, let $\mathcal{M}$ be a generator of $\operatorname{Mod} \Sigma_f$. Since a quasivariety is generated by finitely generated modules, we can assume $\mathcal{M}$ finitely generated. Then, according to Theorem 2,

$$\mathcal{M} \cong \mathcal{R}^n \oplus \mathfrak{a} \oplus \mathcal{M}_T.$$

The torsion-free part, that means $\mathcal{R}^n \oplus \mathfrak{a}$, belongs to $\mathcal{Q}$, according to Lemma 3. Now $\mathcal{M}_T \equiv \bigoplus_i \bigoplus_{k_{i,j}} \mathcal{R}/\mathfrak{p}_i^{k_{i,j}}$ and, according to Lemma 7, $k_{i,j} \leqslant f(\mathfrak{p}_i)$, for all i, j. Now the definition of the function f yields $\mathcal{M}_T \in \mathcal{Q}$ and therefore $\operatorname{Mod} \Sigma_f \subseteq \mathcal{Q}$.

(b) $f(\infty) = 0$: The module $\mathcal{R} \notin \mathcal{Q}$ and $\infty \notin \operatorname{Im}(f)$ and $f(\mathfrak{p}) = 0$, for almost all $\mathfrak{p}$. Let $\mathcal{M} \in \mathcal{Q}$, be finitely generated. Then $\mathcal{M}$ is torsion-free (otherwise $\mathcal{R}$ embeds in $\mathcal{M}$) and, according to Theorem 1, $\mathcal{M}$ is the sum of the modules $\mathcal{R}/\mathfrak{p}_i^{k_i}$ where $f(\mathfrak{p}_i) \neq 0$ and $k_i \leqslant f(\mathfrak{p}_i)$. Then

$$\mathcal{M} \models \left(\prod_{f(\mathfrak{p}_i) \neq 0} p_i^{f(\mathfrak{p}_i)} x = 0 \ \& \ q_{\prod \mathfrak{p}_i^{f(\mathfrak{p}_i)}} x = 0 \right).$$

Hence $\mathcal{M} \in \operatorname{Mod} \Sigma_f$.

On the other hand, we define $\mathfrak{a} = \cap \mathfrak{p}_i^{f(\mathfrak{p}_i)}$. Clearly $\operatorname{Mod} \Sigma_f = \mathcal{V}(\mathcal{R}/\mathfrak{a}) = \mathcal{V}(\bigoplus \mathcal{R}/\mathfrak{p}_i^{f(\mathfrak{p}_i)}) \subseteq \mathcal{Q}$.

Finally, we prove the injectivity. Let $f(\mathfrak{p}) \neq g(\mathfrak{p})$ for some $f, g \in \mathcal{L}(\mathbb{P}(\mathcal{R}))$. If $f(\mathfrak{p}) < g(\mathfrak{p})$, then $\mathcal{R}/\mathfrak{p}^{g(\mathfrak{p})} \in \operatorname{Mod} \Sigma_g$ and $\mathcal{R}/\mathfrak{p}^{g(\mathfrak{p})} \notin \operatorname{Mod} \Sigma_f$. Then $\varphi(f) \neq \varphi(g)$ and $\operatorname{Mod} \Sigma_f \neq \operatorname{Mod} \Sigma_g$.

Similarly, we can show that φ preserves the lattice order. $\square$

4. Quasigroup modes

In this section we present an example of a variety which is equivalent to a variety of modules over a Dedekind ring and we use the results of this paper to compute its sub(quasi)varieties with its defining (quasi)identities. We give many arguments without proofs as they are not difficult to check on a computer.

The equivalence of the variety of quasigroup modes (idempotent and entropic quasigroups) with the variety $\underline{\underline{\mathbb{Z}[p,q,r]}}$ of affine spaces over the ring $\mathbb{Z}[p,q,r]$ where $p+q=pq$ and $pr=1$ was discovered by B. Csákany and L. Magyesi in 1975. J. Ježek and T.Kepka in 1977 characterized entropic quasigroups as polynomially equivalent to modules over certain rings. A. B. Romanowska and J. D. H. Smith in [10] investigated varieties of modes that are equivalent to varieties of $\mathcal{R}$-modules or equivalent to varieties of affine spaces. Any variety $\mathbf{Mod}_{\mathcal{R}}$ of modules over a fixed ring $\mathcal{R}$ is a Mal'cev variety, with $P(x,y,z)=x-y+z$. All $\mathcal{R}$-modules $(\mathcal{A},+,R)$ are diagonally normal, i.e. are central, since $\widehat{\mathcal{A}}=\{(a,a)|a\in\mathcal{A}\}$ is a congruence class of the congruence θ defined by $(a,b)\ \theta\ (a',b')\ \ iff\ \ a-b=a'-b'$. Algebras in central varieties are close to modules.

Theorem 8 ([10, Theorem 6.2.5])**.** *Let $(\mathcal{A},\Omega)=(\mathcal{A},\Omega,P)$ be a non-empty Mal'cev algebra. Then $(\mathcal{A},\Omega)$ is central if and only if it is polynomially equivalent to a module $(\mathcal{A},+,\mathcal{R})$ over some ring $\mathcal{R}$.*

Quasigroups form a Mal'cev variety with $P(x,y,z):=(x/(y\backslash y))\cdot(y\backslash z)$ and for quasigroup modes the Malc'ev term is given by $P(x,y,z):=(x/y)\cdot(y\setminus z)$. Moreover [10, Corollary 6.5.3, 6.5.4], there are countably many varieties of quasigroup modes. The equationally complete varieties of quasigroups modes are equivalent to the varieties of affine spaces over the finite fields $GF(q)$ for $q\neq 2$.

Here comes our example: consider $\mathcal{V}$ to be the variety of all quasigroups satisfying

$$x*x=x, \tag{1}$$

$$(x*y)*(u*z)=(x*u)*(y*z), \tag{2}$$

$$(x*y)*(y\backslash((((((((x/y)*(y\backslash x))/y)*(y\backslash x))/y*(y\backslash x)))/y*(y\backslash x)))=y. \tag{3}$$

Identities (1) and (2) define a mode; all such quasigroups can be obtained from an abelian group $(A,+)$ and and φ, an automorphism of A such that $(1-\varphi) \in \mathrm{Aut}(A)$, as follows:

$$a * b = \varphi(a) + (1-\varphi)(b). \tag{4}$$

On the other hand, choosing an element 0 in an idempotent abelian group, we can reconstruct $+$, $-$ and φ as follows

$$a+b = ((a/0)*(0\backslash b)), \qquad a-b = ((a/b)*(b\backslash 0)) \qquad \text{and} \qquad \varphi(a) = a*0.$$

From this point of view, Identity (6.3) can be rewritten as

$$\varphi^2(x-y) + 5x - 4y = y \tag{5}$$

which holds if and only if $\varphi^2(x) + 5x = 0$, for each x. This means that every quasigroup in $\mathcal{V}$ is polynomially equivalent to a module over $\mathcal{R} = \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$, which is a Dedekind domain. This correspondence does not work the other way round since quasigroups have an additional condition to fulfill, namely $1-\sqrt{-5} \in \mathcal{R}^*$. This is true in $\mathcal{R}$, as well as in most of the fields $\mathcal{R}/\mathfrak{p}$, for $\mathfrak{p}$ a prime ideal, except of $\mathfrak{p}_1 = (2, 1-\sqrt{-5})$ and $\mathfrak{p}_2 = (3, 1-\sqrt{-5})$; this follows from the fact that the norm of $1-\sqrt{-5}$ is 6.

All the previous considerations imply that the lattice of (quasi)varieties of $\mathcal{V}$ is isomorphic to the lattice of (quasi)-varieties of modules over $\mathcal{R}$ that are not non-trivial $\mathcal{R}/(1-\sqrt{-5})$ modules. This lattice forms a principal ideal in the lattice of quasivarieties of $\mathcal{R}$-modules. Hence we see that $\mathcal{L}_q(\mathcal{V}) \cong L(\omega)$. We now describe one variety and one quasivariety in terms of identities and quasiidentities.

The ideal $(3, 1+\sqrt{-5})$ is a prime ideal of $\mathcal{R}$. The module $\mathcal{R}/(3, 1+\sqrt{-5})$ generates a variety with an equational basis

$$x + x + x = 0, \qquad \text{and} \qquad x\sqrt{-5} + x = 0.$$

These identities, when translated to quasigroups, are

$$(((x/y) * (y\backslash x))/y) * (y\backslash x) = y \qquad \text{and} \qquad x * (y\backslash x) = y,$$

since 0 can be chosen arbitrarily and $\varphi(x)/0 = x$. Note also that the second identity is equivalent to the involutory identity $(y * x) * x = y$. There are, of course, many other (and shorter) equational bases of the variety generated by the 3-element idempotent quasigroup.

Consider now the largest quasivariety of $\mathcal{R}$-modules not containing $\mathcal{R}/(3, 1+\sqrt{-5})$. The defining quasiidentity is

$$x + x + x = 0 \ \& \ x\sqrt{-5} + x = 0 \rightarrow x = 0.$$

In the language of quasigroups we obtain

$$(((x/y) * (y\backslash x))/y) * (y\backslash x) = y \ \& \ x * (y\backslash x) = y \rightarrow x = y.$$

Describing the lattices of quasivarieties of modules over the rings, which are not Dedekind rings, can be complicated. We know, that there are examples of rings for which the lattices of quasivarieties of modules over the given rings are not distributive and even are not modular. In the next papers we are going to describe, at least partially, such lattices for some generalizations of Dedekind domains.

References

[1] D. V. Belkin, *Constructing Lattices of Quasivarieties of Modules,* (in Russian), Ph.D. Thesis, Novosibirsk State University, Novosibirsk, Russia, 1995.

[2] C. Bergman and A. Romanowska, *Subquasivarieties of regularized varieties,* Algebra Universalis **36** (1996), 536–563.

[3] V. A. Gorbunov, *Algebraic Theory of Quasivarieties,* Consultants Bureau, New York, 1998.

[4] L. Hogben and C. Bergman, *Deductive varieties of modules and universal algebras,* Trans. Amer. Math. Soc. **289** (1985), 303–320.

[5] A. I. Mal'cev, *Algebraic Systems,* Springer-Verlag, Berlin, 1973.

[6] K. Matczak and A. Romanowska, *Quasivarieties of cancellative commutative binary modes,* Studia Logica **78** (2004), 321–335.

[7] K. Matczak and A. Romanowska, *Irregular quasivarieties of commutative binary modes,* International Journal of Algebra and Computation **15** (2005), 699-715.

[8] R. N. McKenzie, G.F. McNulty and W. F. Taylor, *Algebra, Lattices, Varieties,* vol. I, Wadsworth, Monterey, 1987.

[9] W. Narkiewicz *Elementary and Analytic Theory of Algebraic Numbers,* Springer Monographs in Mathematics, 2004

[10] A. B. Romanowska and J. D. H. Smith, *Modes,* World Scientific, Singapore, 2002.

[11] W. Stephenson *Modules Whose Lattice of Submodules is Distributive,* Proc. London Math. Soc. **s3-28**, 2 (1974), 291–310

[12] K. Toyoda *On axioms of linear functions,* Proc. Imp. Acad. Tokyo **17** (1941), 221–227

[13] A. A. Vinogradov, *Quasivarieties of abelian groups,* (in Russian), Algebra i Logika **4**(1965), 15–19.

[14] O. Zariski, P. Samuel, *Commutative algebra*, vol. I, Springer-Verlag, Berlin 1975.

Contact information

P. Jedlička Department o Mathematics, Faculty of Engineering, Czech University of Life Sciences, 165 21 Prague, Czech Republic
E-Mail(s): jedlickap@tf.czu.cz

K. Matczak Faculty of Civil Engineering, Mechanics and Petrochemistry in Płock, Warsaw University of Technology, 09-400 Płock, Poland
E-Mail(s): katarzyna.matczak@pw.edu.pl

A. Mućka Faculty of Mathematics and Information Sciences, Warsaw University of Technology, 00-661 Warsaw, Poland
E-Mail(s): a.mucka@mini.pw.edu.pl

Received by the editors: 22.06.2017
and in final form 12.09.2017.