Commutative Rings Whose Principal Ideals Have Unique Generators

P. N. Ánh, Keith A. Kearnes, and Ágnes Szendrei

Abstract We investigate the class of commutative unital rings in which principal ideals have unique generators. We prove that this class forms a finitely axiomatizable, relatively ideal distributive quasivariety, and also that it equals the quasivariety generated by the class of integral domains with trivial unit group.

Keywords Divisibility · Relatively distributive quasivariety

2010 Mathematics Subject Classification 13A05 · 13A15 · 08C15

1 Introduction

What can be said about the class of commutative rings in which, if a differs from b, the set of elements divisible by a differs from the set of elements divisible by b? Equivalently, what can be said about the class of rings where $a \neq b$ implies $(a) \neq (b)$? In this paper we show that this class is a relatively ideal distributive quasivariety, and we give a set of axioms for the quasivariety. Along the way we learn that this quasivariety is exactly the quasivariety of commutative rings generated by the class of integral domains with trivial unit group.

P. N. Ánh (✉)
Rényi Institute of Mathematics, Hungarian Academy of Sciences,
Pf. 127, 1364 Budapest, Hungary
e-mail: anh.pham.ngoc@renyi.mta.hu

K. A. Kearnes · Á. Szendrei
Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA
e-mail: Kearnes@Colorado.EDU

Á. Szendrei
e-mail: Szendrei@Colorado.EDU

A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_1

2 The Quasivariety of Rings Whose Principal Ideals have Unique Generators

Our goal in this section is to describe the class of commutative rings whose principal ideals have unique generators. The main result is that this class is a relatively ideal distributive quasivariety, so let us explain now what that means. (For more details about relatively congruence distributive/modular quasivarieties, we refer to [1–3].)

A *quasi-identity* in the language of commutative rings is a universally quantified implication of the form

$$(s_1 = t_1) \wedge \cdots \wedge (s_n = t_n) \to (s_0 = t_0)$$

where s_i and t_i are ring terms (= "words", or "polynomials"). We allow $n = 0$, in which case the quasi-identity reduces to an identity: $s_0 = t_0$ (universally quantified). To emphasize this last point: identities are special quasi-identities.

A *variety* is a class axiomatized by identities. A *quasivariety* is a class axiomatized by quasi-identities. For an example of the former, the class of commutative rings is a variety. For an example of the latter, the class of rings axiomatized by the identities defining commutative rings together with the quasi-identity $(x^2 = 0) \to (x = 0)$ is the quasivariety of reduced commutative rings (rings with no nonzero nilpotent elements).

If $\mathcal{Q}$ is a quasivariety of commutative rings, $R \in \mathcal{Q}$, and $I \lhd R$ is an ideal of R, then I is a $\mathcal{Q}$-*ideal* (or a *relative* ideal) if $R/I \in \mathcal{Q}$. For example, if $\mathcal{Q}$ is the quasivariety of commutative reduced rings and $R \in \mathcal{Q}$, then I is a relative ideal of R exactly when I is a semiprime ideal of R.

The collection of $\mathcal{Q}$-ideals of some $R \in \mathcal{Q}$, when ordered by inclusion, forms an algebraic lattice. It is not a sublattice of the ordinary ideal lattice, but it is a subset of the ordinary ideal lattice that is closed under arbitrary meet.

A quasivariety $\mathcal{Q}$ of commutative rings is *relatively ideal distributive* if the $\mathcal{Q}$-ideal lattice of any member of $\mathcal{Q}$ satisfies the distributive law:

$$I \wedge (J \vee K) = (I \wedge J) \vee (I \wedge K).$$

Here, the meet operation is just intersection ($I \wedge J = I \cap J$) while the join operation depends on $\mathcal{Q}$; all that can be said is that $I \vee J$ is the least $\mathcal{Q}$-ideal that contains $I \cup J$ (or, equivalently, contains $I + J$).

It is interesting to find that some particular quasivariety of rings is relatively ideal distributive. Any distributive algebraic lattice is isomorphic to the lattice of open sets of a topology defined on the set of meet irreducible lattice elements. Therefore, if $\mathcal{Q}$ is relatively ideal distributive, then to each member of $\mathcal{Q}$ there is a naturally associated topological space, its $\mathcal{Q}$-spectrum. It is possible to treat a member $R \in \mathcal{Q}$ as a ring of functions defined over its $\mathcal{Q}$-spectrum. It turns out that the quasivariety of commutative reduced rings, mentioned earlier as an example, is relatively ideal distributive, and for this $\mathcal{Q}$ the $\mathcal{Q}$-spectrum of any $R \in \mathcal{Q}$ is just the ordinary prime spectrum of R.

The main result of this section is that the class of commutative rings whose principal ideals have unique generators is a relatively ideal distributive quasivariety, and for which we provide an axiomatization.

Theorem 1. *Let $\mathcal{Q}$ be the class of all commutative rings (with 1) having the property that each principal ideal has a unique generator. Let $\mathcal{D}$ be the class of domains in $\mathcal{Q}$.*

(1) *$\mathcal{Q}$ is a quasivariety. It is exactly the class of rings axiomatized by the quasi-identity $(xyz = z) \to (yz = z)$ along with the identities defining the variety of all commutative rings. All rings in $\mathcal{Q}$ have trivial unit group and are reduced. Such rings are $\mathbb{F}_2$-algebras.*
(2) *$\mathcal{D}$ is exactly the class of domains with trivial unit group.*
(3) *$\mathcal{Q}$ consist of the subrings of products of members of $\mathcal{D}$ (we write $\mathcal{Q} = \mathsf{SP}(\mathcal{D})$).*
(4) *$\mathcal{Q}$ is a relatively ideal distributive quasivariety.*
(5) *The class of locally finite algebras in $\mathcal{Q}$ is the class of Boolean rings. This class is the largest subvariety of $\mathcal{Q}$.*

Proof. We argue the first two claims of Item (1) together. Namely, we show that $R \in \mathcal{Q}$ if and only if R belongs to the quasivariety of commutative rings satisfying $(xyz = z) \to (yz = z)$.

For the "if" part, let R be a commutative ring satisfying $(xyz = z) \to (yz = z)$. Choose $r \in R$ and assume that $(r) = (s)$ for some s. Then $s = qr$ and $r = ps$ for some $p, q \in R$. Since $pqr = r$, the quasi-identity yields $qr = r$, or $s = r$. Thus, $(r) = (s)$ implies $r = s$, showing that R satisfies the unique generator property for principal ideals. Conversely, for "only if", suppose that R does not satisfy $(xyz = z) \to (yz = z)$. R must have elements p, q, r such that $pqr = r$ and $qr \neq r$, Then $(r) = (qr)$ and $qr \neq r$, so R does not have the unique generator property.

For the second to last statement of Item (1), suppose that $R \in \mathcal{Q}$ and that u is a unit in R. Then $(u) = R = (1)$, so by the unique generator property $u = 1$. Also, to see that R is reduced, assume that $n \in R$ satisfies $n^2 = 0$. Then $1 + n$ is a unit (with inverse $1 - n$), so $1 + n = 1$, so $n = 0$.

For the final statement of Item (1), the fact that any $R \in \mathcal{Q}$ is an $\mathbb{F}_2$-algebra follows from the fact that -1 is a unit, so $1 = -1$. Then the prime subring of R is isomorphic to $\mathbb{F}_2$, which is enough to establish that R is an $\mathbb{F}_2$-algebra.

For Item (2), if $D \in \mathcal{D}$, then D is a domain by definition, and it has trivial unit group by Item (1). Conversely, suppose that D is a domain with trivial unit group. If $(a) = (b)$ in D, then a and b must differ by a unit, hence $a = b$, showing that D has the unique generator property, so D is a domain in $\mathcal{Q}$, yielding $D \in \mathcal{D}$.

In order to establish Item (3) we first prove a claim.

Claim 2. *If $R \in \mathcal{Q}$ and $S \subseteq R$ is a subset, then the annihilator $A = ann(S)$ is a $\mathcal{Q}$-ideal (meaning that $R/A \in \mathcal{Q}$).*

Proof of claim. For this we must verify that R/A satisfies the quasi-identity $(xyz = z) \to (yz = z)$. Equivalently, we must show that if $x, y, z \in R$ and $xyz \equiv z \pmod{A}$, then $yz \equiv z \pmod{A}$. We begin: If $xyz \equiv z \pmod{A}$, then $(xyz - z) \in A$, so $(xyz - z)s = 0$ for any $s \in S$. This means that $xy(zs) = (zs)$ for any $s \in S$. Applying the quasi-identity from Item (1) with zs in place of z we derive that $yzs = zs$, or $(yz - z)s = 0$ for any $r \in I$. Hence $yz \equiv z \pmod{A}$, as desired.

Next we argue that if $R \in \mathcal{Q}$ is not a domain, then R has disjoint nonzero $\mathcal{Q}$-ideals I and J. If R is not a domain, then there exist nonzero r and s such that $rs = 0$. Take $I = \mathrm{ann}(r)$ and $J = \mathrm{ann}(I)$. I is nonzero since it contains s, and J is nonzero since it contains r. Both I and J are $\mathcal{Q}$-ideals by Claim 2. If $t \in I \cap J$, then $t^2 \in IJ = \{0\}$, so t is nilpotent. According to Item (1), any $R \in \mathcal{Q}$ is reduced, so $t = 0$. Thus I and J are indeed disjoint nonzero $\mathcal{Q}$-ideals.

The argument for Item (3) is completed by noting that any quasivariety $\mathcal{Q}$ is expressible as $\mathsf{SP}(\mathcal{K})$ where $\mathcal{K}$ is the subclass of relatively subdirectly irreducible members of $\mathcal{Q}$. This is a version of Birkhoff's subdirect representation theorem, stated for quasivarieties, and it holds for quasivarieties because relative ideal/congruence lattices are algebraic. The previous paragraph shows that the only members of $\mathcal{Q}$ that could possibly be relatively subdirectly irreducible are the domains. (That is, R not a domain $\Rightarrow$ R has disjoint nonzero $\mathcal{Q}$-ideals $\Rightarrow$ R is not relatively subdirectly irreducible.)

To prove Item (4), we refer to general criteria from [3] for proving that a quasivariety is relatively congruence distributive. Specifically, we will use Theorems 4.1 and 4.3 of that paper, along with some of the remarks between those theorems.

Here is a summary of what we are citing. From Theorem 4.1 of [3], a quasivariety is relatively congruence modular if and only if it satisfies the "extension principle" and the "relative shifting lemma". From remarks following the proof of Theorem 4.1, the "extension principle" can be replaced by the "weak extension principle". From Theorem 2.1 of that paper, the "relative shifting lemma" can be replaced by the "existence of quasi-Day terms". Finally, from Theorem 4.3 of that paper, a quasivariety is relatively congruence distributive if and only if it is relatively congruence modular and no member has a nonzero abelian congruence.

What this reduces to in our setting is this: to prove that our quasivariety $\mathcal{Q}$ is relatively ideal distributive (Item (4)) it suffices to show that $\mathcal{Q}$

(i) has "quasi-Day terms",
(ii) satisfies the "weak extension principle", and
(iii) has no member with a nontrivial abelian congruence (i.e., with a nonzero ideal A satisfying $A^2 = 0$).

Condition (i) holds since $\mathcal{Q}$ has ordinary Day terms, in fact a Maltsev term. (More explicitly, the singleton set $\Sigma_s := \{(p(w, x, y, z), q(w, x, y, z)\}$ where $p(w, x, y, z) := w - x + y$ and $q(w, x, y, z) := z$ meets the defining conditions from Theorem 2.1(2) of [3] for "quasi-Day terms".)

Condition (iii) holds since if $A \lhd R \in \mathcal{Q}$ and $A^2 = 0$, then the elements of A are nilpotent. As argued in the proof of Item (1), the only nilpotent element in R is 0, hence $A = 0$.

Condition (ii) means that if $R \in \mathcal{Q}$ has disjoint ideals I and J, then I and J can be extended to $\mathcal{Q}$-ideals $\overline{I} \supseteq I$ and $\overline{J} \supseteq J$ that are also disjoint. To prove that Condition (ii) holds we modify an argument from above: If R has ideals I and J such that $I \cap J = 0$, then $IJ = 0$. The $\mathcal{Q}$-ideal $\overline{J} = \text{ann}(I)$ contains J, the $\mathcal{Q}$-ideal $\overline{I} = \text{ann}(\overline{J})$ contains I, both are $\mathcal{Q}$-ideals, and $\overline{I} \cap \overline{J} = 0$ (since the elements in this intersection square to zero and R is reduced). This shows that disjoint ideals I and J may be extended to disjoint $\mathcal{Q}$-ideals.

For Item (5), to show that a locally finite ring in $\mathcal{Q}$ is a Boolean ring it suffices to show that any finite ring $F \in \mathcal{Q}$ is Boolean. (The reason this reduction is permitted is that the property of being a Boolean ring is expressible by the identity $x^2 = x$, and a locally finite structure satisfies a universal sentence if and only if its finite substructures satisfy the sentence.)

So choose a finite $F \in \mathcal{Q}$. As F has trivial unit group, and $1 + \text{rad}(F) \subseteq U(F)$, we get that F must be semiprimitive. Since F is finite it must be a product of fields. Since F has only trivial units, each factor field must have size 2, so F is Boolean.

Conversely, if B is any Boolean ring, then multiplication is a semilattice operation, so $xyz \leq yz \leq z$ in the semilattice order for any $x, y, z \in B$. If, in B, we have first = last ($xyz = z$), then we must have middle = last ($yz = z$). Hence $B \in \mathcal{Q}$.

To complete the proof of Item (5) we must show that if $\mathcal{V}$ is a variety and $\mathcal{V} \subseteq \mathcal{Q}$, then $\mathcal{V}$ consists of Boolean rings. For this it suffices to show that if $R \in \mathcal{Q}$ is not Boolean (i.e., R has an element r satisfying $r \neq r^2$), then $R \notin \mathcal{V}$. This holds because $\langle r^2 \rangle \subsetneq \langle r \rangle$ by the unique generator property, so $r/\langle r^2 \rangle$ is a nonzero nilpotent element of $R/\langle r^2 \rangle$, establishing that some homomorphic image of R is not in $\mathcal{Q}$. □

By substituting $z = 1$ in the quasi-identity $(xyz = z) \to (yz = z)$ we obtain the consequence $(xy = 1) \to (y = 1)$, which expresses that the unit group is trivial. Since a consequence can be no stronger than the original statement, this is enough to deduce that the quasivariety of commutative rings with trivial unit group contains the quasivariety of commutative rings whose principal ideals have unique generators. This containment is proper, and the following example describes a commutative ring satisfying $(xy = 1) \to (y = 1)$ but not $(xyz = z) \to (yz = z)$.

Example 3. Let R be the commutative $\mathbb{F}_2$-algebra presented by

$$\langle X, Y, Z \mid XYZ = Z \rangle.$$

That is, R is the quotient of the polynomial ring $\mathbb{F}_2[X, Y, Z]$ by the ideal $(XYZ - Z)$.

We may view the relation $XYZ - Z = 0$ as a reduction rule $XYZ \to Z$ to produce a normal form for elements of R. This single rule is applied as follows: choose a monomial of the form $XYZW$ (W is a product of variables) of an element in a coset of $(XYZ - Z) \subseteq \mathbb{F}_2[X, Y, Z]$ and replace $XYZW$ by ZW. That is, if each of X, Y, Z appear in a monomial, we delete one instance of X and one instance of Y from that monomial.

The Diamond Lemma applies to show that there is a normal form for elements of R, and the elements in normal form are exactly the polynomials over $\mathbb{F}_2$ in the generators X, Y, Z where no monomial is divisible by each of X, Y, and Z.

Note that each application of the reduction rule reduces the X-degree and the Y-degree of some monomial, but does not alter the Z-degree of any monomial. This is enough to prove that the unit group of R is trivial. For if R had a unit u with inverse v, then the Z-degree of the product $uv = 1$ is zero, but it is also the sum of the Z-degrees of u and v. Hence the normal form of a unit must be Z-free. But then u and v would then be inverse units in the subring $\mathbb{F}_2[X, Y]$, where all elements are in normal form. Now one can argue in this subring, using X-degree and Y-degree, to conclude that none of X, Y, Z appear in the normal form of a unit. We are left with $u = v = 1$ as the only possibility.

Notice also that $YZ - Z$ is in normal form, so $YZ - Z \neq 0$ in R. This shows that R fails to satisfy $(xyz = z) \to (yz = z)$, but does satisfy $(xy = 1) \to (y = 1)$. In particular, the fact that $XYZ = Z$ while $YZ \neq Z$ means that $(YZ) = (Z)$, while $YZ \neq Z$, so the principal ideal (Z) does not have a unique generator.

3 Some Related Quasivarieties

We saw in the previous section that the class of commutative rings whose principal ideals have unique generators is the quasivariety generated by the class of domains with trivial unit group. We also saw that this quasivariety is relatively ideal distributive, and that it is axiomatized by the quasi-identity $(xyz = z) \to (yz = z)$.

In this section we will show that the quasivariety $\mathcal{Q}_{|n}$ generated by those domains D whose unit group $U(D)$ is cyclic of order dividing n is also relatively ideal distributive, and we shall provide an axiomatization for $\mathcal{Q}_{|n}$.

Write $\mathcal{D}_{|n}$ for the class of domains whose unit group is cyclic of order dividing n.

Theorem 4. *By definition, we have that $\mathcal{Q}_{|n}$ is the quasivariety generated by $\mathcal{D}_{|n}$.*

(1) *$\mathcal{Q}_{|n}$ is axiomatized* by

   (a) *the identities defining commutative rings,*
   (b) *the quasi-identity $(x^2 = 0) \to (x = 0)$, which expresses that the only nilpotent element is* 0, *and*
   (c) *the quasi-identity $(xyz = z) \to (y^n z = z)$.*

(2) *$\mathcal{Q}_{|n}$ is a relatively ideal distributive quasivariety.*

Proof. To prove Item (1), let $\mathcal{K}$ be the quasivariety axiomatized by the sentences in (a), (b), and (c). It is easy to see that $\mathcal{D}_{|n}$ satisfies the quasi-identities in (a), (b), and (c), so $\mathcal{D}_{|n} \subseteq \mathcal{K}$, and therefore $\mathcal{Q}_{|n} \subseteq \mathcal{K}$.

Conversely, we must show that $\mathcal{K} \subseteq \mathcal{Q}_{|n}$ For this, we need the analogue of Claim 2 for $\mathcal{K}$:

Claim 5. *If $R \in \mathcal{K}$ and $S \subseteq R$ is a subset, then the annihilator $A = ann(S)$ is a $\mathcal{K}$-ideal.*

Proof of claim. Our goal is to prove that $R/A \in \mathcal{K}$, so we must prove that R/A is a commutative ring satisfying $(x^2 = 0) \to (x = 0)$ and $(xyz = z) \to (y^n z = z)$. It is clear that R/A is a commutative ring (identities are preserved under quotients), so we only need to verify that R/A satisfies $(x^2 = 0) \to (x = 0)$ and $(xyz = z) \to (y^n z = z)$. For the second of these, the proof is exactly like the proof of Claim 2, while for the first there is an extra idea. We prove the first only.

To prove that R/A satisfies $(x^2 = 0) \to (x = 0)$, we must show that R satisfies $x^2 \equiv 0 \pmod{A}$ implies $x \equiv 0 \pmod{A}$. If $x^2 \equiv 0 \pmod{A}$, or $x^2 \in A$, then $x^2 s = 0$ for all $s \in S$. This implies $(xs)^2 = (x^2 s)s = 0$ for all $s \in S$. (This is the "extra idea".) But R satisfies $(x^2 = 0) \to (x = 0)$, so from $(xs)^2 = 0$ we deduce $xs = 0$ for all $s \in S$. This proves that $x \in A$ or $x \equiv 0 \pmod{A}$.

We will use Claim 5 the same way we used Claim 2 in the proof of Theorem 1. If $R \in \mathcal{K}$ is not a domain, then there exist nonzero r and s such that $rs = 0$. Take $I = \text{ann}(r)$ and $J = \text{ann}(I)$. I is nonzero since it contains s, and J is nonzero since it contains r. By Claim 5, I and J are $\mathcal{K}$-ideals. Any element in $I \cap J$ must square to zero, so since $\mathcal{K}$ satisfies axiom (b) we get $I \cap J = \{0\}$. Thus, if R is not a domain, then it has a pair of nonzero, disjoint, $\mathcal{K}$-ideals. This is enough to guarantee that R is not subdirectly irreducible relative to $\mathcal{K}$.

In the contrapositive form, we have shown that any relatively subdirectly irreducible member of $\mathcal{K}$ is a domain. Hence $\mathcal{K}$ is generated by its subclass of domains.

But if $D \in \mathcal{K}$ is a domain, then by substituting $z = 1$ in the quasi-identity (1)(c) we obtain that D satisfies $(xy = 1) \to (y^n = 1)$. This implies that the unit group $U(D)$ of D is a cyclic group of order dividing n. The reason for this is that $U(D)$ is an abelian group satisfying $x^n = 1$, hence $U(D)$ is a locally finite abelian group. If $U(D)$ is not cyclic, then it contains a finite noncyclic subgroup $G \subseteq U(D)$. But now G is a finite noncyclic subgroup of the field of fractions of D, and we all know that the multiplicative group of a field contains no finite noncyclic subgroup. This shows that the domains in $\mathcal{K}$ lie in $\mathcal{D}_{|n}$, so $\mathcal{K}$ is contained in the quasivariety generated by $\mathcal{D}_{|n}$, which is $\mathcal{Q}_{|n}$.

Item (2) of this theorem is proved exactly like Item (4) of Theorem 1. □

Observations 6. A quick test to rule out that some nonzero ring R belongs to some quasivariety $\mathcal{Q}_{|n}$ is to show that the prime subring of R does not belong to $\mathcal{Q}_{|n}$. Since the prime subring of R is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}_k$ for some $k > 1$, and since the units of $\mathbb{Z}$ and $\mathbb{Z}_k$ are easy to determine, it is not hard to derive some consequences.

Namely, $\mathbb{Z}_k$ satisfies the quasi-identity in Theorem 4(1)(b) if and only if k is square-free, and hence $k = p_1 \dots p_m$ and $\mathbb{Z}_k \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_m}$ for distinct primes $p_1, \dots, p_m$. Now, for such a k, $\mathbb{Z}_k$ satisfies the quasi-identity in Theorem 4(1)(c) if and only if $p_i - 1$ divides n for each i. Therefore, these conditions on k are necessary

for R to belong to $\mathcal{Q}_{|n}$ whenever the prime subring of R is isomorphic to $\mathbb{Z}_k$. Similarly, $\mathbb{Z}$ satisfies the quasi-identity in Theorem 4(1)(c) if and only if n is even. Hence, if the prime subring of R is isomorphic to $\mathbb{Z}$, then for R to belong to $\mathcal{Q}_{|n}$ the number n must be even.

These considerations imply, in particular, that if n is odd, then $\mathbb{Z}_k \notin \mathcal{Q}_{|n}$ unless $k = 2$, and $\mathbb{Z} \notin \mathcal{Q}_{|n}$. Hence, each ring in $\mathcal{Q}_{|n}$ may be thought of as an $\mathbb{F}_2$-algebra.

Notice also that, when n is odd, the axiom $(x^2 = 0) \to (x = 0)$ from Theorem 4(1)(b) is a consequence of the axiom $(xyz = z) \to (y^n z = z)$ from Theorem 4(1)(c). For if R satisfies $(xyz = z) \to (y^n z = z)$ for some odd n, and some $r \in R$ satisfies $r^2 = 0$, then as observed in the previous paragraph the characteristic of R must be 2, so $(1 + r)^2 = 1$. This implies that $1 + r$ is a unit of order dividing 2 (and also n), so necessarily $1 + r = 1$, which implies that $r = 0$.

We can use Observation 6 to show that not all the quasivarieties $\mathcal{Q}_{|n}$ are distinct, in particular

Theorem 7. *If p is an odd prime, then $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ unless p is a Mersenne prime.*

Proof. To prove that $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ when p is an odd non-Mersenne prime, it will suffice to show that these quasivarieties contain the same domains. We always have $\mathcal{Q}_{|m} \subseteq \mathcal{Q}_{|n}$ when $m \mid n$, from the definition of these quasivarieties, so we must show that any domain $D \in \mathcal{Q}_{|p}$ is contained in $\mathcal{Q}_{|1}$ (i.e., has a trivial unit group).

Choose $D \in \mathcal{Q}_{|p}$. From Observation 6, we know (since p is odd) that D is an $\mathbb{F}_2$-algebra. Suppose that $\theta \in D$ is a nontrivial unit. Since θ has finite multiplicative order, and the prime subring of D is finite, the subring $S \subseteq D$ generated by θ is finite. S is a subring of a domain itself, hence it is a field, and $U(S) = S^\times$. S belongs to $\mathcal{Q}_{|p}$, so $S^\times$ has order dividing p, and it must therefore be that $|S^\times| = p$. This shows that S is a finite field of characteristic 2 and of cardinality $|S| = p + 1$. We derive that $p + 1 = 2^s$ for some s, or $p = 2^s - 1$. This completes the proof that $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ unless p is a Mersenne prime.

The primality of p did not play a big role in the proof. The same argument shows that if n is any odd number, then $\mathcal{Q}_{|n} = \mathcal{Q}_{|1}$ unless n is divisible by some number $x > 1$ of the form $x = 2^s - 1$. So, for example, $\mathcal{Q}_{|55} = \mathcal{Q}_{|25} = \mathcal{Q}_{|1}$. But if n is divisible by some number $x > 1$ of the form $x = 2^s - 1$, then $\mathcal{Q}_{|n}$ will contain some finite fields that are not in $\mathcal{Q}_{|1}$.

Acknowledgements This material is based upon work supported by the National Research, Development and Innovation Office NKFIH K119934, the Vietnam Institute for Advanced Study in Mathematics (VIASM), the Vietnamese Institute of Mathematics, the National Science Foundation grant no. DMS 1500254, the Hungarian National Foundation for Scientific Research (OTKA) grant no. K115518, and the National Research, Development and Innovation Fund of Hungary (NKFI) grant no. K128042.

References

1. Kearnes, K.A.: Relatively congruence distributive subquasivarieties of a congruence modular variety. Bull. Austral. Math. Soc. **41**(1), 87–96 (1990). https://doi.org/10.1017/S0004972700017871
2. Kearnes K.A.: Relatively congruence modular quasivarieties of modules. In: Czelakowski, J. (eds.) Don Pigozzi on Abstract Algebraic Logic, Universal Algebra, and Computer Science. Outstanding Contributions to Logic, vol. 16, pp. 221–232. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74772-9_8
3. Kearnes, K., McKenzie, R.: Commutator theory for relatively modular quasivarieties. Trans. Amer. Math. Soc. **331**(2), 465–502 (1992). https://doi.org/10.2307/2154123