



Equivalence between varieties of square root rings and Boolean algebras with a distinguished automorphism

J. Patricio Díaz Varela¹

Departamento de Matemática, Universidad Nacional del Sur, 8000 Bahía Blanca, Argentina

Received 28 February 2005

Available online 22 March 2006

Communicated by Efim Zelmanov

Abstract

In this paper we study the variety \mathbf{R}_2 of square root rings, that is, commutative rings with unit, of characteristic two, with the square root as an additional operation. We prove that this variety is generated by the finite Galois fields $\mathbf{GF}(2^k)$ and we establish an equivalence between \mathbf{R}_2 and the variety $\mathbf{BA}\delta$ of Boolean algebras with a distinguished automorphism. Via this equivalence, we will be able to obtain properties of \mathbf{R}_2 from the results proved in [M. Abad, J.P. Díaz Varela, M. Zander, Boolean algebras with a distinguished automorphism, *Rep. Math. Logic* 37 (2003) 101–112].

© 2006 Elsevier Inc. All rights reserved.

Keywords: Boolean algebras; Finite fields; Frobenius automorphism; Commutative rings; Interpretations

1. Preliminaries

The variety $\mathbf{BA}\delta$ of Boolean algebras with a distinguished automorphism was introduced and studied in [2]. This paper deals with that variety and the variety \mathbf{R}_2 of square root rings. Our objective is to establish an equivalence between these two varieties, generalizing the well-known equivalence between Boolean algebras and Boolean rings (see [4]). We also deduce some properties for \mathbf{R}_2 from the properties proved in [2] for $\mathbf{BA}\delta$.

E-mail addresses: usdiavar@criba.edu.ar, jpdiazvarela@yahoo.com.ar.

¹ Partially supported by the Universidad Nacional del Sur, Bahía Blanca, Argentina and CONICET.

We include in this section some definitions and results on the variety $\mathbf{BA}\delta$, and we recall the notion of equivalence between varieties. For definitions and basic properties of universal algebra the reader is referred to [4,10].

To start with, we introduce the square root rings as a variety, that is, as a class of algebras closed by direct products, subalgebras and homomorphic images. In that sense, our approach to the study of this algebras is different to that of Heatherly and Blanchet in [8], as we consider the square root as a new operation in the language of rings, in the style of universal algebra. In particular, the concepts of subalgebra, congruence and homomorphic image are different.

A *square root ring* is an algebra $A = \langle A, +, \cdot, \sqrt{\cdot}, 0, 1 \rangle$ of type $\langle 2, 2, 1, 0, 0 \rangle$, that satisfies the following conditions:

- (R1) $\langle A, +, \cdot, 0, 1 \rangle$ is a commutative ring with unit,
- (R2) $2 \cdot x = 0$, i.e., A is of characteristic two,
- (R3) $\sqrt{x^2} = x$ and $(\sqrt{x})^2 = x$.

The class of all square root rings \mathbf{R}_2 is equational, and hence, it is a variety in the sense of universal algebra (see [4,10]).

By a *Boolean algebra with a distinguished automorphism* [2] we understand an algebra $\langle A; \wedge, \vee, -, \delta, \delta', 0, 1 \rangle$, such that $\langle A; \wedge, \vee, -, 0, 1 \rangle$ is a Boolean algebra, δ is an automorphism of A and $\delta' = \delta^{-1}$. Clearly, the class of Boolean algebras with a distinguished automorphism is a variety which we denote $\mathbf{BA}\delta$.

The typical example of an algebra in $\mathbf{BA}\delta$ is the field of subsets of the integers \mathbf{Z} , $2^{\mathbf{Z}}$, with the set-theoretical operations of union, meet and complementation, and where δ is the automorphism of $2^{\mathbf{Z}}$ induced by the mapping $n \mapsto n + 1$, $n \in \mathbf{Z}$. In [2] it is shown that $2^{\mathbf{Z}}$ is non-simple subdirectly irreducible, and the variety $\mathbf{BA}\delta$ is generated by the algebra $2^{\mathbf{Z}}$.

Let k be a positive integer. A subset x of \mathbf{Z} is called *k-periodic* if it coincides with the set obtained by adding k to each of its elements. The set of k -periodic subsets of \mathbf{Z} is a subalgebra of $2^{\mathbf{Z}}$, which we denote by B_k .

Let $B_N = \bigcup_{i \in \mathbf{N}} B_i$. B_N is a subalgebra of $2^{\mathbf{Z}}$, and thus $B_N \in \mathbf{BA}\delta$. The following results can be found in [2].

Theorem 1.1. *The algebra B_N is simple, atomless and locally finite.*

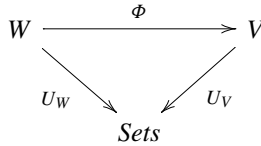
The following theorem states that the variety $\mathbf{BA}\delta$ is generated by its finite members. In what follows $V(K)$ denotes the variety generated by a class K of algebras.

Theorem 1.2. $\mathbf{BA}\delta = V(\{B_m : m > 0\})$.

Corollary 1.3. $\mathbf{BA}\delta = V(B_N)$.

We say that a variety V is *interpretable* [9,10] in a variety W if for each V -operation $F_i(x_1, \dots, x_n)$ there is a W -term $f_i(x_1, \dots, x_n)$ such that if $\langle A; G_i \rangle$ is in W , then $\langle A; f_i \rangle$ is in V . Notice that the constants in the language of V must be interpreted as constants in the language of W . Intuitively, this means that each algebra in W can be turned into an algebra in V by defining the V -operations applying a uniform procedure.

This notion can also be approached in the following way: there exists a functor $\Phi : W \rightarrow V$ which commutes with the underlying set functors, that is,



is commutative. U_V and U_W are the forgetful functors which assign to each algebra its universe. Each functor Φ is called an *interpretation of W in V* .

If $\langle A; G_I \rangle$ is any algebra and for each V -operation $F_I(x_1, \dots, x_n)$ there is a term $f_I(x_1, \dots, x_n)$ in the language of $\langle A; G_I \rangle$ such that $\langle A; f_I \rangle$ is in V , the terms $f_I(x_1, \dots, x_n)$ define an interpretation of V in $V(\langle A; G_I \rangle)$, the variety generated by the algebra $\langle A; G_I \rangle$. One only has to observe that the evaluation of any term in an algebra B in $V(\langle A; G_I \rangle)$, is determined by its evaluation in A and that both $\langle A; G_I \rangle$ and $\langle B; G_I \rangle$ satisfy the same equations. We have $V(\langle A; G_I \rangle) \xrightarrow{\Phi} V$, and we say that $\Phi(\langle A; G_I \rangle)$ is an interpretation of V in $V(\langle A; G_I \rangle)$.

By an *equivalence* [10] of the varieties V and W is meant a pair of interpretations Φ_1 of V in W and Φ_2 of W in V such that $\Phi_2\Phi_1 = \text{Id}_V$ and $\Phi_1\Phi_2 = \text{Id}_W$. Two algebras A, B are equivalent if and only if there are interpretations $\Phi : V(A) \rightarrow V(B)$ and $\Psi : V(B) \rightarrow V(A)$ such that $\Phi\Psi(B) = B$ and $\Psi\Phi(A) = A$.

Observe that A and B are equivalent if and only if every operation in the language of A can be written as a term in the language of B , and conversely.

Theorem 1.4. [10] *For varieties V and W , V is equivalent to W if and only if there exist equivalent algebras A and B such that $V = V(A)$ and $W = V(B)$.*

2. Equivalence between R_2 and $BA\delta$

In this section an equivalence between the varieties R_2 and $BA\delta$ is established and some applications are given thereof.

For $A \in R_2$ and $x \in A$, let $\sigma(x) = x^2$ be the Frobenius endomorphism. Observe that the existence of square roots in R_2 implies that σ is an automorphism. We denote $\sqrt{x} = \sigma^{-1}(x) = x^{1/2}$, and $(\sqrt{})^k(x) = \sqrt[k]{x} = x^{1/2^k}$.

Let $\text{orb}(a) = \{\sigma^n(a) : n \in \mathbf{Z}\}$ be the orbit of an element $a \in A$. We say that a is *periodic* if $\text{orb}(a)$ is finite. In this case the least integer $n \geq 1$ such that $\sigma^n(a) = a$ is called the period of a . If A is finite we have that a is periodic for every $a \in A$. The following lemma is clear.

Lemma 2.1. *Let $A \in R_2$ be finite. Then there is $m \in N$ such that $\sigma^m(x) = x^{2^m} = x$ for every $x \in A$. In this case $\sqrt{x} = \sigma^{m-1}(x) = x^{2^{m-1}}$.*

An *sr-ideal* in an algebra $A \in R_2$ is an ideal $I \subseteq A$ closed under $\sqrt{}$, i.e., an ideal I of A such that $\sqrt{x} \in I$ whenever $x \in I$. It is easy to see that congruences in A are determined by *sr-ideals*. In fact, there is a lattice isomorphism between the lattice of congruences of A and the lattice of *sr-ideals* of A .

For $x \in A$, let (x) be the sr -ideal generated by x . Note the difference between the ideal generated by x and the sr -ideal generated by x . Indeed, the ideal generated by x is $Ax = \{y \in A: y = ax, a \in A\}$, but

$$(x) = \left\{ y \in A: y = \sum_{i=1}^k a_i x^{\alpha_i}, a_i \in A, \alpha_i = \frac{t_i}{2^{h_i}}, t_i \geq 1, h_i \geq 0 \right\}.$$

Similarly, it is well known that a commutative ring A with unit is simple if and only if A is a field. In the variety \mathbf{R}_2 , the simple objects are the fields as well.

Theorem 2.2. *In the variety \mathbf{R}_2 , A is simple if and only if A is a field.*

Proof. Let $A \in \mathbf{R}_2$ be simple. Then, $1 \in (x)$ for every $x \in A, x \neq 0$, and consequently, there are $a_i \in A$ such that $1 = \sum_{i=1}^k a_i x^{\alpha_i}$, with $\alpha_i = \frac{t_i}{2^{h_i}}, t_i \geq 1, h_i \geq 0$. Let $m = \max\{2^{h_i}, i = 1, \dots, k\}$. Then

$$1 = 1^m = \left(\sum_{i=1}^k a_i x^{\alpha_i} \right)^m = \sum_{i=1}^k a_i^m x^{\beta_i},$$

with the integers $\beta_i \geq 1$. Thus

$$1 = x \cdot \sum_{i=1}^k a_i^m x^{\beta_i - 1}.$$

From this we have that for every $x \neq 0, x$ has inverse. Thus A is a field. The other implication is trivial. \square

Observe that a field in \mathbf{R}_2 is a perfect field.

We analyze now the equational theory of \mathbf{R}_2 with the objective of proving that \mathbf{R}_2 is generated by its finite members.

Let $p(x_1, x_2, \dots, x_n)$ be a term in the language of \mathbf{R}_2 . Then

$$p(x_1, x_2, \dots, x_n) = \sum_{i=1}^s x_1^{\alpha_i^1} x_2^{\alpha_i^2} \dots x_n^{\alpha_i^n}, \quad \alpha_i^j = \frac{t_i^j}{2^{h_i^j}}, t_i^j, h_i^j \geq 0, 1 \leq i \leq s, 1 \leq j \leq n.$$

If $p_1(x_1, x_2, \dots, x_n) = p_2(x_1, x_2, \dots, x_n)$ is an identity in the language of \mathbf{R}_2 , then, for $A \in \mathbf{R}_2, A$ satisfies $p_1 = p_2$ if and only if for every n -tuple $(a_1, a_2, \dots, a_n) \in A^n, p_1(a_1, a_2, \dots, a_n) = p_2(a_1, a_2, \dots, a_n)$. But $p_1 = p_2$ is equivalent to $p_1 + p_2 = 0$. So every identity in the language of \mathbf{R}_2 is equivalent to another one of the form

$$p(x_1, x_2, \dots, x_n) = \sum_{i=1}^s x_1^{\alpha_i^1} x_2^{\alpha_i^2} \dots x_n^{\alpha_i^n} = 0.$$

Moreover, if $m = \max\{h_i^j\}$ with $i = 1, \dots, s$ and $j = 1, \dots, n$, we have that $p(x_1, x_2, \dots, x_n) = 0$ iff $(p(x_1, x_2, \dots, x_n))^{2^m} = 0$. But

$$(p(x_1, x_2, \dots, x_n))^{2^m} = \left(\sum_{i=1}^s x_1^{\alpha_i^1} x_2^{\alpha_i^2} \dots x_n^{\alpha_i^n} \right)^{2^m} = \sum_{i=1}^s x_1^{\beta_i^1} x_2^{\beta_i^2} \dots x_n^{\beta_i^n},$$

with integers $\beta_i^j \geq 0$, for every $i = 1, \dots, s$ and $j = 1, \dots, n$. From this assertion we have the following lemma.

Lemma 2.3. *Every identity $p_1(x_1, x_2, \dots, x_n) = p_2(x_1, x_2, \dots, x_n)$ in the language of \mathbf{R}_2 is equivalent to an identity of the form*

$$\sum_{i=1}^s x_1^{\beta_i^1} x_2^{\beta_i^2} \dots x_n^{\beta_i^n} = 0,$$

where $\beta_i^j \in \mathbf{N} \cup \{0\}$, for every $i = 1, \dots, s$ and $j = 1, \dots, n$.

Observe that two identities are equivalent if the algebras of \mathbf{R}_2 that satisfy them are the same.

The following theorem proves that \mathbf{R}_2 is generated by its finite members. In fact, $\mathbf{R}_2 = V(\{\mathbf{GF}(2^k) : k \geq 1\})$.

Theorem 2.4. *\mathbf{R}_2 is generated by the fields $\mathbf{GF}(2^k)$.*

Proof. Let $p(x_1, x_2, \dots, x_n) = \sum_{i=1}^s x_1^{\beta_i^1} x_2^{\beta_i^2} \dots x_n^{\beta_i^n}$, $\beta_i^j \in \mathbf{N} \cup \{0\}$, be a term and suppose that $p(x_1, x_2, \dots, x_n) = 0$ characterizes a proper subvariety of \mathbf{R}_2 . Let us prove that there exists a finite field $\mathbf{GF}(2^k)$ such that $\mathbf{GF}(2^k)$ does not satisfy $p(x_1, x_2, \dots, x_n) = 0$.

We may assume that $p \neq 0$ and $p \neq 1$. We make induction over the number of variables.

Suppose that $n = 1$. Then $p(x) = \sum_{i=1}^s x^{\beta_i}$, with $\beta_i \geq 0$, $\beta_s > 0$ and $\beta_i > \beta_j$ if $i > j$. Choose $k = \beta_s + 1$. Let $b \in \mathbf{GF}(2^k)$ an element of the normal base. Thus $p(b) = \sum_{i=1}^s b^{\beta_i} \neq 0$.

Suppose now that the number of variables is n and let x_l be a variable such that $\beta_l^j \neq 0$, for some j . Assume, without loss of generality, that $l = 1$ and $\beta_i^1 > \beta_{i'}^1$ for $i > i'$. Then

$$p(x_1, x_2, \dots, x_n) = \sum_{i=1}^s x_1^{\beta_i^1} p_i(x_2, \dots, x_n).$$

By inductive hypothesis we can choose k and elements $b_2, \dots, b_n \in \mathbf{GF}(2^k)$ such that $p_1(b_2, \dots, b_n) = c_1 \neq 0$. Let $c_i = p_i(b_2, \dots, b_n)$. Observe that, for $c_i \neq 0$, $c_i^{2^k-1} = 1$. Thus

$$(p(x_1, b_2, \dots, b_n))^{2^k-1} = \sum_{i=1}^s x_1^{\beta_i^1(2^k-1)} c_i^{2^k-1},$$

that is a term in the language of \mathbf{R}_2 , since $c_i^{2^k-1} \in \{0, 1\}$. Now we are in the case of one variable. So we can take $k' = k\beta_i^1(2^k - 1)$, and $b_1 \in \mathbf{GF}(2^{k'})$ such that $(p(b_1, b_2, \dots, b_n))^{2^k-1} \neq 0$. Thus $p(b_1, b_2, \dots, b_n) \neq 0$. \square

Corollary 2.5. $R_2 = V(\{GF(2^k): k \geq 1\})$.

Let GF_2 be the algebraic closure of $GF(2)$. It is known that GF_2 is the field of roots of polynomials in $GF(2)[x]$, and that GF_2 has a copy (as subalgebra) of $GF(2^k)$ for every $k \geq 1$. Moreover, GF_2 is isomorphic to the direct limit of the system $\{\{GF(2^k)\}_{k \geq 1}, \{\phi_{k,l}\}_{k \geq 1}\}$ where $\phi_{k,l}: GF(2^k) \rightarrow GF(2^l)$ is the natural immersion for $k|l$.

Corollary 2.6. $R_2 = V(GF_2)$.

Moisil established relationships between finite fields $GF(2^k)$ and cyclic Boolean algebras, but it was Cendra in [5] who gave a constructive method to define a simple k -cyclic Boolean algebra $\langle A; \delta \rangle$ on a given finite field $GF(2^k)$, $k \geq 1$, and conversely.

Theorem 2.7. [2,5] *Given a finite field $GF(2^k)$, there exists a structure of simple k -cyclic Boolean algebra defined on $GF(2^k)$ isomorphic to B_k , and conversely, such that*

- (1) *the constants are the elements of the prime field $GF(2)$;*
- (2) *the operations \wedge and \vee are terms in the language of R_2 . In addition, $\sim x = 1 + x$ and $\delta(x) = \sigma(x) = x^2$;*
- (3) *the operations $+$ and \cdot are uniquely determined terms in the language of $BA\delta$. Moreover, $\sqrt{x} = \delta^{-1}(x) = \delta^{k-1}(x)$ and $x + y = x \Delta y$.*

As an immediate consequence of Theorem 2.7 we have the following (see [10, Theorem 4.140] and [2]).

Corollary 2.8. *The varieties $V(B_k)$ and $V(GF(2^k))$ are equivalent, that is, there exists an interpretation Φ_k of $V(B_k)$ in $V(GF(2^k))$ and an interpretation Ψ_k of $V(GF(2^k))$ in $V(B_k)$ such that $\Psi_k \Phi_k(B) = B$ for every $B \in V(B_k)$ and $\Phi_k \Psi_k(A) = A$ for every $A \in V(GF(2^k))$.*

Lemma 2.9. GF_2 is equivalent to B_N .

Proof. Consider $\Phi_k: V(B_k) \rightarrow V(GF(2^k))$ and $\Psi_k: V(GF(2^k)) \rightarrow V(B_k)$ of Corollary 2.8. Then we can define $\Phi: B_N \rightarrow GF_2$, where $\Phi(B_k) = \Phi_k(B_k)$ and $\Psi: GF_2 \rightarrow B_N$, where $\Psi(GF(2^k)) = \Psi_k(GF(2^k))$. \square

By the preceding lemma and Corollaries 2.6 and 1.3 we have

Theorem 2.10. R_2 is equivalent to $BA\delta$.

As an application of the previous results we can obtain many properties for the variety R_2 that are immediate consequences of the corresponding results for $BA\delta$ [2]. As an example we can state:

- (1) R_2 is not locally finite, even though it is generated by GF_2 which is locally finite.
- (2) The locally finite simple algebras in R_2 are subalgebras of GF_2 .
- (3) The locally finite subdirectly irreducible algebras in R_2 are simple, and consequently, isomorphic to subfields of GF_2 .

- (4) Every locally finite algebra $A \in \mathbf{R}_2$ is semisimple, and consequently, A can be embedded into $(\mathbf{GF}_2)^k$.
- (5) A subvariety of \mathbf{R}_2 is locally finite if and only if it is finitely generated.

Finally, we point out that M. Zander proved that any proper subvariety of $\mathbf{BA}\delta$ is locally finite, that is to say, any proper subvariety is a finite join of $V(B_n)$'s. Consequently we have

Theorem 2.11. *Any proper subvariety of \mathbf{R}_2 is locally finite, that is, any proper subvariety is a finite join of $V(\mathbf{GF}(2^k))$'s.*

Corollary 2.12. *Every proper subvariety of \mathbf{R}_2 is a discriminator variety and if $V = V(\{\mathbf{GF}(2^{k_i}); i = 1, \dots, n\})$, V is determined by the identity*

$$\gamma_{k_1, \dots, k_n}(x) = \prod_{i=1}^n (x^{2^{k_i}} + x) = 0.$$

Moreover, the lattice of subvarieties of \mathbf{R}_2 is isomorphic to the lattice $\langle N \cup \{0\}, | \rangle$, where $a | b$ is the order relation a is a divisor of b .

This equivalence between \mathbf{R}_2 and $\mathbf{BA}\delta$ can be extended without difficulty to varieties of p th root rings \mathbf{R}_p , p prime, and p -valued Post algebras with a distinguished automorphism $\mathbf{PA}_p\delta$ (see [1,3]), that is, we have the following theorem.

Theorem 2.13. *The varieties of p th root rings \mathbf{R}_p and p -valued Post algebras with distinguished automorphism $\mathbf{PA}_p\delta$ are equivalent.*

It is worth to mention that in recent articles [6,7], R. Cignoli et al. introduced functors between the categories of locally finite MV-algebras, multisets and locally finite Boolean algebras with a distinguished automorphism. Via the equivalence established in this work, the relationships between these classes of algebras can be extended to square root rings. Besides, it is immediate that $\mathbf{BA}\delta$ is dually equivalent to the class $\mathbf{St}\delta$ of Stone spaces with a distinguished homeomorphism, so \mathbf{R}_2 is dually equivalent to $\mathbf{St}\delta$. In a forthcoming paper we will develop further applications of this equivalence.

Acknowledgment

It is a pleasure to acknowledge conversations with M. Abad.

References

- [1] M. Abad, Cyclic post algebras of order n , An. Acad. Brasil. Ciênc. 53 (2) (1981) 243–246.
- [2] M. Abad, J.P. Díaz Varela, M. Zander, Boolean algebras with a distinguished automorphism, Rep. Math. Logic 37 (2003) 101–112.
- [3] M. Abad, J.P. Díaz Varela, F. López Martinolich, M. del C. Vannicola, M. Zander, Varieties Generated by Finite Fields and Cyclic Post Algebras, submitted for publication.
- [4] S. Burris, H. Sankappanavar, A Course in Universal Algebra, Grad. Texts in Math., vol. 78, Springer-Verlag, Berlin, 1981.
- [5] H. Cendra, Cyclic Boolean algebras and Galois fields $F(2^k)$, Port. Math. 39 (1–4) (1980) 435–440.

- [6] R. Cignoli, E. Dubuc, D. Mundici, Extending Stone duality to multisets and locally finite MV-algebras, *J. Pure Appl. Algebra* 189 (1–3) (2004) 37–59.
- [7] R. Cignoli, E. Dubuc, D. Mundici, An MV-algebraic invariant for Boolean algebras with a finite-orbit automorphism, in: Special Issue in Honour of Prof. J. Jakubik for his 80th Birthday, *Tatra Mt. Math. Publ.* 27 (2003) 23–43.
- [8] H. Heatherly, A. Blanchet, n th root rings, *Bull. Austral. Math. Soc.* 35 (1987) 111–123.
- [9] R. Lewin, Interpretability into Łukasiewicz algebras, *Rev. Un. Mat. Argentina* 41 (3) (1999) 81–98.
- [10] R. McKenzie, G. McNulty, W. Taylor, *Algebras, Lattices, Varieties*, vol. I, Wadsworth and Brooks, Monterey, CA, 1987.