Journal of Logical and Algebraic Methods in Programming 84 (2015) 276–282

Contents lists available at ScienceDirect

Journal of Logical and Algebraic Methods in Programming

www.elsevier.com/locate/jlamp

The structure of finite meadows

Inge Bethke, Piet Rodenburg *, Arjen Sevenster

University of Amsterdam, Faculty of Science, Informatics Institute, Section Theory of Computer Science, Science Park 904, 1098 XH Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 20 January 2014
Received in revised form 17 July 2014
Accepted 8 August 2014
Available online 12 August 2014

Keywords:
Fields
Division-by-zero

ABSTRACT

A *meadow* is a commutative ring with a total inverse operator satisfying $0^{-1} = 0$. We show that the class of finite meadows is the closure of the class of Galois fields under finite products. As a corollary, we obtain a unique representation of minimal finite meadows in terms of finite prime fields.

1. Introduction

In abstract algebra, a field is a structure with operations of addition, subtraction and multiplication. Moreover, every element has a multiplicative inverse—except 0. In a field, the rules hold which are familiar from the arithmetic of ordinary numbers. The prototypical example is the field of rational numbers. Fields can be specified by the axioms for commutative rings with identity element, and the negative conditional formula

$$x \neq 0 \rightarrow x \cdot x^{-1} = 1,$$

which is difficult to apply or automate in formal reasoning.

The theory of fields is a very active area which is not only of great theoretical interest but has also found applications, within mathematics—combinatorics and algorithm analysis—as well as in engineering sciences, in particular, in coding theory and sequence design. Unfortunately, a nontrivial product of fields is not a field. Hence the class of fields is not a variety, and cannot be axiomatized by equations only.

In [4], the equationally defined class of *meadows* was introduced, structures very similar to fields—the considerable difference being that meadows do constitute a variety. All fields and products of fields can be viewed as meadows—basically by stipulating $0^{-1} = 0$—but not conversely. Also, every commutative *Von Neumann regular ring* (see e.g. [8]) can be expanded to a meadow (cf. [2]). From a computer science point of view, the concept of a meadow contributes to the algebraic specification of number systems. Advantages and disadvantages of the algebraic specification of data types have been amply discussed in the computer science literature.

Many structures that arise in practice are finite. This motivates the study of finite structures in general. The aim of this paper is to describe the structure of finite meadows. We will show that the class of finite meadows is the closure of the class of finite fields under finite products. As a corollary, we obtain a unique representation of minimal meadows in terms of prime fields. This result also follows from the observation that meadows are *biregular* and hence *semisimple* rings, and

* Corresponding author.
E-mail addresses: I.Bethke@uva.nl (I. Bethke), P.H.Rodenburg@uva.nl (P. Rodenburg).

http://dx.doi.org/10.1016/j.jlamp.2014.08.004
2352-2208/

the connection between commuting idempotents and direct product decomposition into simple rings as expounded in [6]. Here, however, we will give a direct proof by a straightforward combination of basic properties of meadows. Some of these results were already announced in [1].

2. Preliminaries

In this section we recall the basic properties of rings and meadows.

Definition 2.1. A *commutative ring* is a structure $\langle R, +, -, \cdot, 0, 1\rangle$ such that for all $x, y, z \in R$

(1) $(x+y)+z = x+(y+z)$
(2) $x+y = y+x$
(3) $x+0 = x$
(4) $x+(-x) = 0$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $x \cdot y = y \cdot x$
(7) $x \cdot 1 = x$
(8) $x \cdot (y+z) = x \cdot y + x \cdot z.$

We will write $x - y$ for $x + (-y)$.

The following properties of commutative rings are well-known.

Proposition 2.2. *Let R be a commutative ring and $x, y \in R$. Then*

1. *the identity 1 is unique,*
2. $0 \cdot x = 0$,
3. $(-x) \cdot y = -(x \cdot y)$,
4. $(-1) \cdot x = -x$,
5. $-0 = 0$,
6. $(-x) + (-y) = -(x+y)$,
7. $-(-x) = x$.

Proposition 2.3. *Let R be a commutative ring. For any $x \in R$, there exists at most one $y \in R$ with $x \cdot x \cdot y = x$ and $y \cdot y \cdot x = y$.*

Proof. Let z be another element such that $x \cdot x \cdot z = x$ and $z \cdot z \cdot x = z$. We have

$$y = y \cdot y \cdot x = y \cdot y \cdot (x \cdot x \cdot z) = (y \cdot y \cdot x) \cdot (x \cdot z) = y \cdot x \cdot z = x \cdot y \cdot z.$$

Hence, by symmetry, $z = x \cdot y \cdot z$ and thus $y = z$. □

Definition 2.4. Let R be a commutative ring and $x \in R$. If it exists, we call the element $y \in R$ uniquely determined by $x \cdot x \cdot y = x$ and $y \cdot y \cdot x = y$ the *generalized inverse of* x and denote it by x^{-1}.

Proposition 2.5. *Let R be a commutative ring. We have*

1. $0^{-1} = 0$,
2. $1^{-1} = 1$ *and* $(-1)^{-1} = -1$,
3. $(x^{-1})^{-1} = x$ *for all $x \in R$ for which the generalized inverse exists.*

Proof. (1) From $0 \cdot 0 \cdot 0 = 0$ it follows that 0 is the generalized inverse of 0, i.e. $0^{-1} = 0$. (2) From $1 \cdot 1 \cdot 1 = 1$ it follows that 1 is the generalized inverse of 1, i.e. $1^{-1} = 1$, and similarly $(-1)^{-1} = -1$. (3) Since the equalities $x \cdot x \cdot a = x$ and $a \cdot a \cdot x = a$ are symmetric in a and x, it follows that x is the inverse of a. Thus $x = a^{-1} = (x^{-1})^{-1}$. □

Examples 2.6.

1. In the commutative ring $\mathbb{Q}$ of rational numbers, every element has a generalized inverse. If $x \neq 0$, the inverse is just the "regular" inverse, and $0^{-1} = 0$.