Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS103010001
Volume 103, Number 1, 2018, Pages 1-19 **ISSN: 0972-0871**

ON THE LOGICAL INDEPENDENCE OF THREE AXIOMS FOR RINGS WITH IDENTITY

David E. Dobbs

Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37996-1320
U. S. A.

Abstract

We study unital algebraic systems satisfying most of the axioms for associative rings with identity, the possible exceptions being the following three axioms: (1) associativity of multiplication; (2) left-distributivity of multiplication over addition; and (3) right-distributivity of multiplication over addition. Examples are given of such systems showing that [(1) and (3)] $\not\Rightarrow$ (2), [(1) and (2)] $\not\Rightarrow$ (3), [(2) and (3)] $\not\Rightarrow$ (1).

1. Introduction

All rings considered in this note are associative rings with identity. Early in a famous set of lecture notes, Artin made the point that the axioms listed in the definitions of a group, a ring, or a field include "some of the ordinary properties of numbers" [1, p. 13]. Our focus here will be on rings. Nearly two

Received: May 5, 2017; Accepted: August 22, 2017
2010 Mathematics Subject Classification: Primary 16B99; Secondary 17B99.
Keywords and phrases: associative ring with identity, associativity of multiplication, left-distributivity of multiplication over addition, right-distributivity of multiplication over addition, algebraic system, Lie algebra, matrix.

decades after Artin's lectures, Herstein made essentially the same point when he wrote that rings "are patterned after, and are generalizations of, the algebraic aspects of the ordinary integers" [3, p. 83]. In a first course on abstract algebra, it is common to motivate the study of rings in the spirit of Artin and Herstein by pointing out that the familiar operations of addition and multiplication equip the set $\mathbb{Z}$ of integers with the structure of a ring and that the set of axioms defining a ring are simply generalizations of familiar facts about the arithmetic of integers. Typically, students have learned those facts years earlier as generalizations of the corresponding statements about arithmetic in $\mathbb{N}$, the set of positive integers. In most cases, if a child has seen any justifications for those general facts about addition and multiplication in $\mathbb{N}$, those justifications were given as explanations that involve counting. We review some explanations of that kind in Section 2. Our emphasis there will be on three of those axioms, namely, the associativity of multiplication and the distributivity of multiplication over addition from the left and from the right. As these three axioms for rings will be seen to share similar motivations that are based on counting, which is surely one of the most fundamental mathematical concepts, it is natural to ask if there is any logical dependence among these three axioms. Our purpose here is to make this question more precise and then to answer it in the negative.

The above-stated purpose is accomplished in Section 3, where we make the above question more precise as follows. Intuitively, a *unital algebraic system* is defined as a set, together with operations of addition and multiplication, satisfying most of the axioms for associative rings with identity, the possible exceptions being the above-mentioned three axioms. If one does not require the existence of a multiplicative identity element, one has the notion of an *algebraic system*. As there are several (equivalent) ways to define a ring, a more precise definition of a "unital algebraic system" is given in Section 3. Then Examples 3.3 and 3.4 each shows that the distributivity properties do not imply associativity of multiplication. Of course, the most natural example of such a non-associative algebra is a Lie algebra. In fact, the algebraic system in Example 3.3 is the two-dimensional

non-abelian Lie algebra (that is explained in more detail in Section 3) over a given field, while the algebraic system in Example 3.4 is a Lie algebra which is inferred from a (an associative) ring of 2×2 matrices. All examples in Section 3 can be extended to unital algebraic systems (with the same noted behavior) via Lemma 3.2, which carefully examines the usual method of embedding a "ring without identity" into a ring. Propositions 3.5 and 3.6 document that Examples 3.3 and 3.4 can each produce a Lie algebra that cannot be produced by the other example. Then Examples 3.7 and 3.8 each shows that associativity of multiplication does not imply either left- or right-distributivity of multiplication over addition in certain unital algebraic systems. The constructions used in these final two examples are inferred from the way that Artin showed in [1] that a semigroup with a left identity element need not be a group even if each of its elements has a right inverse.

If T is a set, then $|T|$ denotes the cardinal number of T. We assume familiarity with the basics about cardinal numbers, including the usual facts about addition and multiplication of infinite cardinal numbers, as in [2, pp. 94-99]. For that reason, we are assuming the ZFC (Zermelo-Fraenkel, together with the Axiom of Choice) foundations for set theory. To emphasize the fundamental nature of the issues considered here, the bibliography has been chosen to consist of six revered textbooks that were each published more than 50 years ago.

2. Using Counting to Motivate Three of the Ring Axioms

This section can be skipped by any reader who is not interested in motivating the problems that will be solved in Section 3. The motivation given in the present section expresses some of the author's views and are based on his various life experiences as (roughly in chronological order) a child, student, tutor, teacher, father, researcher, referee, editor and grandfather. If his views are not exactly the same as those of the reader, it is hoped that they are sufficient congruent to the reader's views as to make the following comments serve as useful motivation for Section 3.

This section will describe our preferred way to use counting in order to motivate the following three properties of arithmetic in $\mathbb{N}$:

(1) $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{N}$;

(2) $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{N}$;

(3) $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{N}$.

One commonly refers to (1) as associativity of multiplication; to (2) as left-distributivity of multiplication over addition; and to (3) as right-distributivity of multiplication over addition. Since all three of these properties refer to multiplication, our explanation will begin with some ways to understand the concept of multiplication.

The most basic way to understand multiplication is surely as repeated addition. For instance, some early entries in the "5 times" table are

$$5 \times 2 = 5 + 5 = 10, \; 5 \times 3 = 5 + 5 + 5 = 15, \text{ and } 5 \times 4 = 5 + 5 + 5 + 5 = 20.$$

Some readers may think that the above display "got it backwards", so that the display's sum of three 5s should be viewed as 3×5, rather than 5×3. Both points of view have some currency. We are confident that such readers will have no trouble in converting the above and the following comments so as to conform to their view of the matter.

The "5 times" table is often taught formally after one has learned to count or recite by 5s, as in the familiar refrain, "5, 10, 15, ..., 100". What emerges from such experiences is that if b is any (positive) integer ≥ 2, then $5 \times b$ is the overall number of "things" when you have b (pairwise disjoint) collections that each consists of 5 "things". It is common to say, for instance, that 5×3 is what results from counting three 5s. More generally, if m and n are positive integers, $m \times n$ is the overall number of "things" when you have n (pairwise disjoint) collections that each consists of m "things". In short, one says that $m \times n$ is what results from counting n m's. The last expression indicates some of the difficulties in working with symbols in such discussions. We have, perhaps only partially, addressed these by inserting

extra space between "*n*" and "*m*" (to indicate that this explanation of the meaning of "$m \times n$" does not presuppose an understanding of the meaning of "$n \times m$") and by using older-fashioned spelling with an apostrophe between "*m*" and "*s*" (to indicate that *m* is not being multiplied by some number *s*).

With the above view of multiplication in hand, here is how to justify (1). The product $(ab)c$ is the result of counting c (ab)'s. Each of those individual (ab)'s, is the result of counting b *a*'s. So, in the process of counting c (ab)'s, one has really counted a certain number of *a*'s. What is that "certain number?" It is $b + \cdots + b$, where the number of summands is *c*. So, by the above discussion, that "certain number" is what results from counting *c b*'s, namely, $b \times c$; that is, *bc*. We have just shown that $(ab)c$ is the result of counting *bc a*'s. But so is $a(bc)$. This finishes a justification of (1) via counting.

Before justifying (2) and (3) via counting, we wish to address an expected objection from a formalist who may insist on using set theory to understand the addition and multiplication of cardinal numbers, especially of positive integers. Here is how to be convinced that the set-theoretic approach does capture the intuitive view of multiplication as iterated addition. Let *a* and *b* be positive integers. Pick sets $A = \{x_1, ..., x_a\}$ and $B = \{y_1, ..., y_b\}$ such that $|A| = a$ and $|B| = b$. Here is how to reconcile the formal definition of $a \cdot b$ as $|A \times B|$ with the above view of counting *b a*'s. To find $|A \times B|$, one can (since *A* and *B* are finite) count the elements of the Cartesian product:

$$A \times B = \{(x_1, y_1), ..., (x_a, y_1), ..., (x_1, y_b), ..., (x_a, y_b)\}.$$

As displayed, $A \times B$ is the union of the (pairwise disjoint) sets

$$\{(x_1, y_j), ..., (x_a, y_j)\}$$

as j goes from 1 to *b*. Thus, $|A \times B|$ is the result of counting the overall number of ordered pairs (which play the earlier role of "things") when we

have b (pairwise disjoint) collections that each consists of a ordered pairs. In other words, $|A \times B|$ does result from counting b a's, and so agrees with the view of ab that we gave above.

Before leaving (1) (it will return in Section 3), we address a formalist's possible need for a proof of (1) that explicitly uses set theory. To that end, pick sets A, B and C such that $|A| = a$, $|B| = b$ and $|C| = c$. To show that $(ab)c = a(bc)$, one would need to produce a bijection $(A \times B) \times C \to A \times (B \times C)$. The most obvious such bijection is given by $((x, y), z) \mapsto (x, (y, z))$ for all $x \in A$, $y \in B$ and $z \in C$. We leave it to the interested reader to see how the view of "multiplication as iterated addition" can be used to reformulate the proof of this bijection. For reasons of space, we also leave to the reader the proofs of (2) and (3) that explicitly use formal set theory.

We next show how to justify (2) via counting. Consider $a(b + c)$, which is the left-hand side of (2). As explained above, this number is the result of counting $(b + c)$ a's. Imagine that such a counting process is temporarily paused after one has counted b a's. The number that results from having reached that point in the process is ab. What remains to be done in the counting process is to count the overall number of "things" in (the remaining) c (pairwise disjoint) collections each of which has a "things". Considered as a separate counting process, that remaining activity eventually results in the number ac (since one has counted c a's during this separate process). The two counting processes (i.e., the activity before the pause and the later activity) have dealt with pairwise disjoint sets, and so the overall counting activity formed from these two processes results in the number $ab + ac$. (Notice that we are using the set-theoretic/intuitive definition/view of $\alpha + \beta$ as the number of elements in the union of a set of cardinality α with a disjoint set of cardinality β.) But that overall counting activity has the same result as the first counting activity considered in this paragraph, because no counting occurred during the pause. In other words, $ab + ac = a(b + c)$. This completes a justification of (2) via counting.

To close the section, we show how to justify (3) via counting. Since we have already justified (2) via counting, one could now justify (3) by combining (2) with the commutativity of multiplication in $\mathbb{N}$. This kind of argument can be viewed as a justification via counting because the commutativity of multiplication in $\mathbb{N}$ can also be justified by counting, in effect by viewing the earlier $A \times B$ as a union of its rows, rather than a union of its columns. However, we prefer to proceed in a more basic manner, if only to provide additional relief for any reader who may still view that the earlier analysis of multiplication in $\mathbb{N}$ "got it backwards".

Consider $(a + b)c,$ which is the left-hand side of (3). This number is the result of counting c $(a + b)$'s; that is, of counting the elements in the union of c pairwise disjoint sets S_i $(i = 1, ..., c),$ each of which has $a + b$ elements. For each i, we can view S_i as consisting of a "things of the first kind" and b "things of the second kind". Let T_i (resp., W_i) be the subset of S_i consisting of all the things of the first (resp., second) kind in S_i. Consider counting the elements in $\bigcup_{i=1}^{c} T_i$: this activity ends up counting all the elements of the first kind and can be viewed as counting c a's, which means that it results in the number ac. Similarly, counting the elements in $\bigcup_{i=1}^{c} W_i$ ends up counting all the elements of the second kind and can be viewed as counting c b's, which means that it results in the number bc. By pooling the results of the two counting activities, the total number of elements that have been counted is $ac + bc.$ But pooling those two counting activities results in counting all the elements of $\bigcup_{i=1}^{c} S_i$ since each "thing" in it was either a "thing of the first kind" or a "thing of the second kind". Hence, the pooled activity must have the same result as the first counting activity considered in this paragraph. Therefore, $ac + bc = (a + b)c,$ thus completing a justification of (3) via counting.

3. The Examples

We first give a precise definition of an algebraic system. No doubt, other authors have used similar terminology, possibly for other purposes, but the following definition will be the one we use in this article. An *algebraic system* is a set S that is endowed with two binary operations, addition (denoted by +) and multiplication (typically denoted by a raised dot or juxtaposition) satisfying the following four conditions:

(i) $a + b = b + a$ for all $a, b \in S$.

(ii) $(a + b) + c = a + (b + c)$ for all $a, b, c \in S$.

(iii) There exists $0 \in S$ such that $0 + a = a = a + 0$ for all $a \in S$.

(iv) If $a \in S$, there exists $-a \in S$ with $a + (-a) = 0 = (-a) + a$.

In short, an algebraic system is an abelian group under addition that is equipped with another binary operation called "*multiplication*" about which nothing further is assumed in the definition. Of course, in all the applications, multiplication will have some interesting properties.

An algebraic system S is called a *unital algebraic system* if S also satisfies the following condition:

(v) There exists $1 \in S$ such that $1a = a = a1$ for all $a \in S$.

A (possibly unital) algebraic system may satisfy some of the following three conditions (which the reader of Section 2 will recognize as generalizations of certain similarly labeled facts about $\mathbb{N}$) :

(1) $(ab)c = a(bc)$ for all $a, b, c \in S$.

(2) $a(b + c) = ab + ac$ for all $a, b, c \in S$.

(3) $(a + b)c = ac + bc$ for all $a, b, c \in S$.

In fact, a unital algebraic system S is a ring (that is, an associative ring with identity) if and only if S satisfies (1), (2) and (3). It is well known that one could define a ring in a more compact fashion for readers with

appropriate background. (For instance, some authors define a ring as an abelian group under addition which is also a monoid under multiplication so that multiplication is both left- and right-distributive over addition.) However, the above list of eight axioms for a ring (namely, (i)-(v) together with (1)-(3)) will help us focus on certain questions of possible logical dependence among the eight axioms. Some nontrivial instances of such dependence are well known. For instance, (ii), (iii), (iv), (v), (2) and (3) jointly imply (i), as follows: if $a, b \in S,$ then

$$a + b + a + b = 1(a + b) + 1(a + b) = (1 + 1)(a + b)$$

$$= (1 + 1)a + (1 + 1)b = 1a + 1a + 1b + 1b = a + a + b + b;$$

so, by adding $-a$ on the left and $-b$ on the right to the extreme members of the last equation, we deduce that $b + a = a + b.$ The preceding argument used the fact that associativity of addition implies its generalization for any finite number of summands $\geq 3;$ the same is true of any associative binary operation: cf. [6, p. 16].

Our interest here is in the somewhat more substantial question of whether (1), (2) or (3) is a logical consequence of the other seven axioms for a ring. Lemma 3.1 begins that study by giving a useful way of constructing algebraic systems.

Lemma 3.1. *Let K be a ring and V be a free left K-module having a K-basis* $\{e_i \mid i \in I\}.$ *For each ordered triple* $(i, j, k) \in I \times I \times I,$ *pick an element* $c_{ijk} \in K.$ *Define a* (*binary operation called*) *multiplication on V as follows. Let* $x = \sum_{i \in I} a_i e_i$ *and* $y = \sum_{j \in I} b_j e_j,$ *where all* $a_i, b_j \in K, a_i \neq 0$ *for only finitely many* $i \in I,$ *and* $b_j \neq 0$ *for only finitely many* $j \in I.$ *Then* $xy := \sum_{(i, j) \in I \times I} \sum_{k \in I} a_i b_j c_{ijk}.$ *Let S denote the entity whereby V is endowed with both this binary operation of multiplication and the given binary operation of addition* (*on the left K-module V*). *Then S has the structure of an algebraic system in which multiplication is both left- and right-distributive over addition.*

Proof. The construction of S was given by Jacobson [4, p. 3] in case K is a field and V is finitely generated as a left K-module (that is, V is a finite-dimensional vector space over K). Jacobson's conclusion was that (in his context) S is a "non-associative algebra", a concept that he had defined one page earlier. Jacobson wisely omitted the proof of his conclusion, indicating that it is something that "one checks immediately" [4, p. 3]. Quite so! Moreover, anyone who carries out that immediate check will recognize that its reasoning can be applied when K and V satisfy our current, more general hypotheses and that (in view of the definition of a non-associative algebra [4, p. 2]) its conclusion is precisely the conclusion that we stated above. □

Jacobson went on to add that "The notion of a non-associative algebra is too general to lead to interesting structural results" [4, p. 3]. We would never dream of challenging this opinion of one of the foremost contributors to the subject of non-associative algebras. However, while Example 3.3 may not be constructing what Jacobson would have viewed as "structural results", Lemma 3.1 will be used in Example 3.3, with K a field, to construct a certain Lie algebra. While the reader will not need to know the definition of a Lie algebra over a field (that definition can be found in [4, pp. 2-3]), one should probably know that Lie algebras are a (definitely "interesting") certain kind of non-associative algebra. As alluded to in the proof of Lemma 3.1, the definition of a non-associative algebra [4, p. 2] ensures that the multiplication in any Lie algebra must be both left- and right-distributive over addition. Since Jacobson's base ring was a field, he referred to these distributivity properties as the "bilinearity condition (1)" on [4, p. 2]. Jacobson's other "bilinearity condition" appears as "bilinearity condition (2)" on [4, p. 2]; it states that $\alpha(xy) = (\alpha x)y = x(\alpha y)$ for all $\alpha \in K$ and all $x, y \in V$. This condition is implied by the definition of multiplication in the statement of Lemma 3.1.

In each of the examples in this section, we shall obtain a unital algebraic system with certain specified behavior by first constructing an algebraic system which exhibits that behavior and then subjecting that system to a

process which is motivated by the usual method for embedding a "ring without identity" as a subring of a suitable ring (with identity): cf. [5, p. 8]. That process is described and analyzed in Lemma 3.2. There and later, if p is a prime number, $\mathbb{F}_p$ will, as usual, denote the finite field with p elements.

Lemma 3.2. *Let S be an algebraic system. Then*:

(a) *Let $S^* := \mathbb{Z} \oplus S$ be an abelian group and equip S with a binary operation of multiplication that is defined as follows*: $(n_1, s_1)(n_2, s_2) := (n_1n_2, n_1s_2 + n_2s_1)$ *for all $n_1, n_2 \in \mathbb{Z}$ and all $s_1, s_2 \in S$. Then*:

(1) *S^* is a unital algebraic system.*

(2) *If S satisfies condition* (1)*, then so does S^*.*

(3) *If S satisfies condition* (2)*, then so does S^*.*

(4) *If S satisfies condition* (3)*, then so does S^*.*

(5) *If S satisfies conditions* (1), (2) *and* (3)*, then S^* is a ring* (*that is, an associative ring with identity*).

(b) *Suppose that the additive structure of S is such that there exists a prime number p with $ps = 0$ for all $s \in S$. Let $S^\dagger := \mathbb{Z}/p\mathbb{Z} \oplus S$ be an abelian group and equip S with a binary operation of multiplication that is* (*well-*) *defined as follows*:

$$(n_1 + p\mathbb{Z}, s_1)(n_2 + p\mathbb{Z}, s_2) := (n_1n_2 + p\mathbb{Z}, n_1s_2 + n_2s_1)$$

for all $n_1, n_2 \in \mathbb{Z}$ and all $s_1, s_2 \in S$. Then:

(α) *$S^\dagger$ is a unital algebraic system.*

(β) *If S satisfies condition* (1)*, then so does $S^\dagger$.*

(γ) *If S satisfies condition* (2)*, then so does $S^\dagger$.*

(δ) *If S satisfies condition* (3), *then so does* $S^\dagger$.

(ε) *If S satisfies conditions* (1), (2) *and* (3), *then* $S^\dagger$ *is a ring* (*that is, an associative ring with identity*) *of characteristic p and, hence, a unital* (*associative*) *algebra over* $\mathbb{F}_p$.

Proof. An algebraic system is nothing more than an abelian group under addition which is endowed with a binary operation of multiplication about which nothing further has been assumed. Thus, (a)(1) follows easily, and so will (b)(α) once we verify that the multiplication in $S^\dagger$ is well-defined. This fact about $S^\dagger$ is well known in the special case of a ring-theoretic setting: cf. [5, Exercise 25, p. 10]. The underlying point remains the same in the present context, namely, that if $s \in S$ satisfies $ps = 0$ and $n_1, n_2 \in \mathbb{Z}$ satisfy $n_1 - n_2 = pz$ for some $z \in \mathbb{Z}$, then $n_1 s - n_2 s = 0$. This, in turn, follows because multiplication in $\mathbb{Z}$ is commutative and *S* is an abelian group (and, hence, a $\mathbb{Z}$-module). Indeed,

$$n_1 s - n_2 s = (n_1 - n_2)s = (pz)s = (zp)s = z(ps) = z \cdot 0 = 0.$$

This completes the proof of (a)(1) and (b)(α).

The remaining verifications are straightforward. For instance, in proving (a)(2), one uses the associativity and commutativity of multiplication in $\mathbb{Z}$ and the fact that *S* is a $\mathbb{Z}$-module; the parallel proof of (b)(β) uses the corresponding facts about $\mathbb{Z}/p\mathbb{Z}$ and the structure of *S* as a module over $\mathbb{Z}/p\mathbb{Z}$ $(= \mathbb{F}_p)$. Since $\mathbb{Z}$ is a ring, similar reasoning gives the proofs of (a)(3) and (a)(4), as well as the parallel respective proofs of (b)(γ) and (b)(δ). Finally, (a)(5) and (b)(ε) are immediate consequences of the above comments and the earlier parts of (a) and (b), respectively. The proof is complete. □

Example 3.3 and Example 3.4 will each show that [(2) and (3)] $\not\Rightarrow$ (1) for unital algebraic systems.

Example 3.3. Let K be a field and V be a two-dimensional vector space over K. Let $\{e_1, e_2\}$ be a K-basis of V. Use Lemma 3.1 to give V the structure of an algebraic system S in which multiplication is both left- and right-distributive over addition by means of the structure constants c_{ijk} defined as follows: $c_{121} := 1$; $c_{211} := -1$; and otherwise, $c_{ijk} := 0$. (In other words, $e_1e_2 = e_1$, $e_2e_1 = -e_1$, and $e_1^2 = 0 = e_2^2$.) Then S does not satisfy associativity of multiplication. When the method of Lemma 3.2 is applied to S, the resulting unital algebraic system S^* (or, if it is defined, $S^\dagger$) satisfies (2) and (3) but does not satisfy (1). In particular, [(2) and (3)] $\not\Rightarrow$ (1) for unital algebraic systems.

Proof. In view of Lemmas 3.1 and 3.2, we need only to show that the multiplication on S is not associative. (Indeed, since the multiplication in S is inherited from that in S^*, it would then follow that the multiplication in S^* is not associative. A similar comment applies to the multiplication on $S^\dagger$ if it is defined.) That, in turn, follows since

$$(e_1e_2)e_2 = e_1e_2 = e_1 \neq 0 = e_1(0e_1 + 0e_2) = e_1(0) = e_1(e_2e_2). \qquad \square$$

Recall from [4, p. 10] that a Lie algebra $\mathcal{L}$ is called *abelian* if $xy = 0$ for all $x, y \in \mathcal{L}$. The algebraic system S constructed in Example 3.3 has been described by Jacobson [4, p. 11] as being the unique two-dimensional non-abelian Lie algebra (up to isomorphism of Lie algebras over the field K). Note that "non-abelian" means "not abelian" here if the characteristic of K is not 2. By way of contrast, a non-associative algebra can have an associative multiplication. For instance, if one takes all the structure constants c_{ijk} to be 0, with V a finite-dimensional vector space over the field K, then the non-associative algebra S in Lemma 3.1 has an associative (albeit trivial) multiplication. However, that S would not be a ring (with identity), since the triviality of its multiplication implies that there is no neutral element in S for that multiplication. However, when Lemma 3.2 (a)(5) is applied to this data, the resulting system S^* is a ring.

The construction that will be used in Example 3.4 depends on the following background from [4, p. 6]. Let K be a field and A be an associative K-algebra. Define a new multiplication on A as follows: if $x, y \in A$, the new product of x and y, when these factors are multiplied in that order, is $[x, y] := xy - yx$. When A is endowed with this new multiplication and its given structure as a vector space over K, the resulting entity is denoted by $\mathcal{L}$. Then $\mathcal{L}$ is a Lie algebra over K and is called the *Lie algebra of* (*the associative algebra*) A. In particular, $\mathcal{L}$ is a non-associative algebra and, hence, the multiplication on $\mathcal{L}$ is both left- and right-distributive over addition.

Example 3.4. Let K be a field and let $A := M_2(K)$, the ring of 2×2 matrices with entries in K. Let $\mathcal{L}$ be the Lie algebra of (the associative algebra) A. Then the multiplication on $\mathcal{L}$ is both left- and right-distributive over addition, but $\mathcal{L}$ does not satisfy associativity of multiplication. When the method of Lemma 3.2 is applied to $\mathcal{L}$, the resulting unital algebraic system $\mathcal{L}^*$ (or, if it is defined, $\mathcal{L}^\dagger$) satisfies (2) and (3) but does not satisfy (1). In particular, [(2) and (3)] $\not\Rightarrow$ (1) for unital algebraic systems.

Proof. In view of the above comments, we need only to show that the multiplication on $\mathcal{L}$ is not associative. Suppose first that the characteristic of K is not 2. Consider the elements $x := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $y := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of $\mathcal{L}$. It suffices to show that $[[x, y], y] \neq [x, [y, y]]$. Observe that $[x, [y, y]] = [x, 0] = 0$ and

$$[[x, y], y] = [x, y]y - y[x, y] = (xy - yx)y - y(xy - yx)$$

$$= xy^2 - 2yxy + y^2x$$

$$= \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} - \begin{pmatrix} 4 & 6 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix},$$

which is not the zero matrix in $\mathcal{L}$ because the characteristic of K is not 2.

Next, suppose that the characteristic of K is 2. Consider the elements $x_1 := \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $y_1 := \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ of $\mathcal{L}$. As above, it suffices to show that $[[x_1, y_1], y_1] \neq 0$ (since $[x_1, [y_1, y_1]] = 0$). As the characteristic of K is 2, one can easily verify that $[[x_1, y_1], y_1] = x_1 y_1^2 + y_1^2 x_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, which is not the zero matrix in $\mathcal{L}$. This completes the proof. □

Since Example 3.3 and Example 3.4 each served to show that [(2) and (3)] $\not\Rightarrow$ (1), it is natural to ask why both of these results were included above. The fact of the matter is, as explained next in Propositions 3.5 and 3.6, that neither Example 3.3 nor Example 3.4 supersedes the other.

Proposition 3.5. *There exists an algebraic system S that can be constructed as in Example* 3.3 *but cannot be constructed as in Example* 3.4. *When the method of Lemma* 3.2 *is applied to S, the resulting unital algebraic system S^* (or, if it is defined, $S^\dagger$) satisfies* (2) *and* (3) *but does not satisfy* (1). *For a suitable prime number p, this $S^\dagger$ cannot be constructed by applying the method of Lemma* 3.2 *to any construction emanating from Example* 3.4.

Proof. Let S be the algebraic system constructed in Example 3.3 with $K := \mathbb{F}_3$. Since S is a two-dimensional vector space over K, we have $|S| = |K|^2 = 9$. We shall next obtain a contradiction from the assumption that S can be constructed as in Example 3.4, say via a base field F of cardinality q. That assumption would entail that

$$9 = |S| = |M_2(F)| = |F|^4 = q^4.$$

This gives the desired contradiction, since there is no cardinal number q such that $q^4 = 9$.

Next, consider S^* and (if it is defined) $S^\dagger$. By Lemma 3.2, these unital algebraic systems satisfy (2) and (3) but not (1). Since S is a vector space

over $\mathbb{F}_3$, $p := 3$ is such that $ps = 0$ for all $s \in S$. Therefore, we can build $S^\dagger$ as in Lemma 3.2 (b) by using $p = 3$; that is, $S^\dagger = \mathbb{Z}/3\mathbb{Z} \oplus S$ (insofar as addition is concerned). Hence

$$| S^\dagger | = | \mathbb{Z}/3\mathbb{Z} \oplus S | = | \mathbb{Z}/3\mathbb{Z} | \cdot | S | = 3 \cdot 9 = 27.$$

It will suffice to prove that when the method of Lemma 3.2 (b) is applied to a Lie algebra $\mathcal{L}$ constructed as in Example 3.4, the resulting $\mathcal{L}^\dagger$ cannot have cardinality 27. (Of course, $\mathcal{L}^* \neq S^\dagger$, since $\mathcal{L}^*$ is infinite.) Recall that $\mathcal{L}$ was constructed in Example 3.4 as the Lie algebra of the associative algebra $M_2(F)$ (consisting of the 2×2 matrices with entries in a field F). Without loss of generality, F is a finite field (for otherwise, $| \mathcal{L}^\dagger | \geq | \mathcal{L} | = | M_2(F) |$ is infinite). For $\mathcal{L}^\dagger$ to be built as in Lemma 3.2 (b), it must be the case that there exists a prime number q such that $qs = 0$ for all $s \in \mathcal{L}$. Then $qM = 0$ for all $M \in M_2(F)$. Taking M to be the identity matrix in $M_2(F)$, we see that q must be the characteristic of F, and so $| F | = q^n$ for some $n \in \mathbb{N}$. As $\mathcal{L}^\dagger = \mathbb{Z}/q\mathbb{Z} \oplus \mathcal{L} = \mathbb{Z}/q\mathbb{Z} \oplus M_2(F)$ insofar as addition is concerned,

$$| \mathcal{L}^\dagger | = | \mathbb{Z}/q\mathbb{Z} \oplus M_2(F) | = | \mathbb{Z}/q\mathbb{Z} | \cdot | M_2(F) | = q| F |^4 = q(q^n)^4 = q^{4n+1}.$$

There do not exist a prime number q and a positive integer n such that $q^{4n+1} = 27$. This completes the proof. □

To facilitate the proof of Proposition 3.6, we next introduce some ad hoc notation that is motivated by the notation used for the normal series of a Lie algebra. Let T be an algebraic system (for instance, a Lie algebra). Let $T^{[1]}$ be the set of all products of two (possibly equal) elements of T. (If T is the Lie algebra of an associative algebra B, the "products" that were just mentioned are taken using the multiplication in T rather than the original multiplication in B. In contrast to the definition of the derived algebra (or ideal) T' of a Lie algebra T, as in [4, p. 10], the definition of $T^{[1]}$ (or that of

$T^{[2]}$ below) does not include sums of products. The reason for this omission of vector space operations in the definition of $T^{[1]}$ is our intent to avoid any question in the proof of Proposition 3.6 as to whether two Lie algebras happen to be Lie algebras over the same field.) Similarly, let $T^{[2]}$ denote the set of all products of two (possibly equal) elements of $T^{[1]}$.

Proposition 3.6. *There exists an algebraic system* $\mathcal{L}$ *that can be constructed as in Example* 3.4 *but cannot be constructed as in Example* 3.3. *When the method of Lemma* 3.2 *is applied to* $\mathcal{L}$, *the resulting unital algebraic system* $\mathcal{L}^*$ (*or, if it is defined,* $\mathcal{L}^\dagger$) *satisfies* (2) *and* (3) *but does not satisfy* (1).

Proof. Let S be any algebraic system constructed as in Example 3.3 (with respect to some field, say F). The definition of S leads easily to $S^{[1]} = Fe_1$. Since $e_1^2 = 0$, it follows that $S^{[2]} = \{0\}$. Therefore, it suffices to find some algebraic system (in fact, the Lie algebra of some associative algebra) $\mathcal{L}$ which is constructed as in Example 3.4 and satisfies $\mathcal{L}^{[2]} \neq \{0\}$.

To that end, work with the field $K := \mathbb{F}_3 = \{0, 1, 2\}$ to build $\mathcal{L}$ as in Example 3.4. Recall that as a set, $\mathcal{L} = M_2(K)$. Consider the elements $x := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $y := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of $\mathcal{L}$. Then $\mathcal{L}^{[1]}$ contains the element $z := [x, y] = xy - yx = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Next, consider the elements $x_1 := \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $y_1 := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ of $\mathcal{L}$. Then $\mathcal{L}^{[1]}$ also contains the element $z_1 := [x_1, y_1] = x_1y_1 - y_1x_1 = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$. Then $\mathcal{L}^{[2]}$ contains the element $[z, z_1] = zz_1 - z_1z = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which is not the zero matrix. This completes the proof. □

The next two examples will show that (1) implies neither (2) nor (3) for a unital algebraic system. The constructions in these examples are motivated by a famous example of Artin [1, Exercise 5, p. 4].

Example 3.7. For any cardinal number $\kappa \geq 2$, there exists an algebraic system S such that $|S| = \kappa$, S is an abelian group with respect to addition, S satisfies associativity of multiplication, S satisfies left-distributivity of multiplication over addition, but S does not satisfy right-distributivity of multiplication over addition. When the method of Lemma 3.2 is applied to S, the resulting unital algebraic system S^* (or, if it is defined, $S^\dagger$) satisfies (1) and (2) but does not satisfy (3). In particular, [(1) and (2)] $\not\Rightarrow$ (3) for unital algebraic systems.

Proof. If κ is finite, say n, we can take the additive structure of S to be that of $\mathbb{Z}/n\mathbb{Z}$, in order to be sure that $|S| = \kappa$ and that S is an abelian group with respect to addition. If κ is infinite, we can be sure of these same two facts by taking the additive structure of S to be that of the polynomial ring $F[\{X_i\}]$, where F is a countable field and $\{X_i\}$ is a set, of cardinality κ, consisting of algebraically independent indeterminates over F. (Note that this polynomial ring can be shown to have cardinal number κ by using the usual rules for the arithmetic of cardinal numbers.) Define a multiplication operation on S as follows: if $x, y \in S$, then $xy := y$. Let $a, b, c \in S$. Then this multiplication is associative, since $(ab)c = c = bc = a(bc)$. Moreover, it is left-distributive over addition, since $a(b + c) = b + c = ab + ac$. However, it need not be right-distributive over addition. Indeed, since $(a+b)c = c$ and $ac + bc = c + c$, we can arrange that $(a + b)c \neq ac + bc$ by taking c to be any nonzero element of the abelian group S (for that ensures that $c \neq c + c$) with a, b chosen arbitrarily in S. An application of Lemma 3.2 completes the proof. □

Example 3.8. For any cardinal number $\kappa \geq 2$, there exists an algebraic system S such that $|S| = \kappa$, S is an abelian group with respect to addition, S

satisfies associativity of multiplication, S satisfies right-distributivity of multiplication over addition, but S does not satisfy left-distributivity of multiplication over addition. When the method of Lemma 3.2 is applied to S, the resulting unital algebraic system S^* (or, if it is defined, $S^\dagger$) satisfies (1) and (3) but does not satisfy (2). In particular, [(1) and (3)] $\not\Rightarrow$ (2) for unital algebraic systems.

Proof. As in the proof of Example 3.7, we can find an abelian group S with respect to addition such that $|S| = \kappa$. Tweak the earlier construction by defining a multiplication operation on S as follows: if $x, y \in S$, then $xy \coloneqq x$. Let $a, b, c \in S$. Then this multiplication is associative, since $(ab)c = ab = a = a(bc)$. Moreover, it is right-distributive over addition, since $(a + b)c = a + b = ac + bc$. However, it need not be left-distributive over addition. Indeed, since $a(b + c) = a$ and $ab + ac = a + a$, we can arrange that $a(b + c) \neq ab + ac$ by taking a to be any nonzero element of the abelian group S (for that ensures that $a \neq a + a$) with b, c chosen arbitrarily in S. An application of Lemma 3.2 completes the proof. □

References

[1] E. Artin, Modern Higher Algebra: Galois Theory, Notes by Albert A. Blank, New York University, New York, 1947.

[2] P. R. Halmos, Naive Set Theory, Van Nostrand, Princeton, 1960.

[3] I. N. Herstein, Topics in Algebra, Blaisdell, New York, 1964.

[4] N. Jacobson, Lie Algebras, Wiley-Interscience, New York, 1962.

[5] N. H. McCoy, Theory of Rings, Macmillan, New York, 1964.

[6] B. L. van der Waerden, Modern Algebra, Volume I, 2nd ed., Ungar, New York, 1953.