1993

Rings with (a, b, c) = (a, c, b) and (a, [b, c]d) = 0: A Case Study Using Albert

Irvin R. Hentzel
Iowa State University, hentzel@iastate.edu

D. P. Jacobs
Clemson University

Erwin Kleinfeld
University of Iowa

Rings with (a, b, c) = (a, c, b) and (a, [b, c]d) = 0: A Case Study Using Albert

Abstract

Albert is an interactive computer system for building nonassociative algebras [2]. In this paper, we suggest certain techniques for using Albert that allow one to posit and test hypotheses effectively. This process provides a fast way to achieve new results, and interacts nicely with traditional methods. We demonstrate the methodology by proving that any semiprime ring, having characteristic $\neq 2, 3$, and satisfying the identities $(a, b, c) - (a, c, b) = (a, [b, c], d) = 0$, is associative. This generalizes a recent result by Y. Paul [7].

Disciplines

Algebra | Mathematics

Rings with $(a, b, c) = (a, c, b)$ and $(a, [b, c], d) = 0$: A Case Study Using **Albert**

Irvin Roy Hentzel
Department of Mathematics
Iowa State University
Ames, Iowa 50011 USA
hentzel@vincent.iastate.edu

D.P. Jacobs [*]
Department of Computer Science
Clemson University
Clemson, S.C. 29634-1906 USA
dpj@clemson.edu

Erwin Kleinfeld
Mathematics Department
University of Iowa
Iowa City, IA 52242 USA
kleinfld@math.uiowa.edu

February 7, 1996

Abstract

Albert is an interactive computer system for building nonassociative algebras [2]. In this paper, we suggest certain techniques for using **Albert** that allow one to posit and test hypotheses effectively. This process provides a fast way to achieve new results, and interacts nicely with traditional methods. We demonstrate the methodology by proving that any semiprime ring, having characteristic $\neq 2, 3$, and satisfying the identities $(a, b, c) - (a, c, b) = (a, [b, c], d) = 0$, is associative. This generalizes a recent result by Y. Paul [7].

Key words: identity, nonassociative polynomial, nonassociative ring, algebra.
AMS (MOS) subject classifications: 17D99, 68N99
CR Categories: I.1.3 (Special-purpose algebraic systems), I.1.4 (Applications)

1 Introduction

Recently, an interactive computer program known as **Albert**, for building nonassociative algebras was developed [2]. With this system, the user specifies the generators and the identities that the algebra is to satisfy, as well as the underlying field of scalars. **Albert** constructs the free nonassociative algebra satisfying these identities. Then one may query

---

```
shelltool - /bin/csh

-->identity (a, [b,c], d)

    (a(bc))d  -   (a(cb))d  -   a((bc)d)  +   a((cb)d)
Entered as identity 1.


-->identity (x, y, z) - (x, z, y)

    (xy)z  -   x(yz)  -   (xz)y  +   x(zy)
Entered as identity 2.


-->identity [ [u,v],w ]

    (uv)w  -   (vu)w  -   w(uv)  +   w(vu)
Entered as identity 3.


-->generators 6x

Problem type stored.


-->
```

Figure 1: Using **Albert**

it to see if a particular nonassociative polynomial is zero in the free algebra generated. This
is equivalent to saying that this nonassociative polynomial is a consequence of the given set
of identities. The program's main algorithm [1] was motivated by the construction in [5].
Figure 1 shows **Albert** being used.

Intrinsically, **Albert** is ideal for verifying results which have already appeared in the
literature. We show how to use its ability to prove *new* theorems. In effect, we show how
the traditional approach which connects ideals and identities can be used with **Albert**. The
power of this approach can be seen in that, in one afternoon, we formulated the conjecture
that became the main result of this paper.

Recall that an ideal I is *trivial* if $I^2 = 0$, and a nonassociative ring or algebra R is called
semiprime if it has no nonzero trivial ideals. R is said to be *prime* if, for ideals I and J,
$IJ = 0$ implies either $I = 0$ or $J = 0$. Clearly prime implies semiprime. For n a natural
number, we say a ring has *characteristic* $\neq n$ if the map $x \rightarrow nx$ is both 1-1 and onto.

2

Throughout this paper, (x, y, z) represents the associator, defined as $(xy)z - x(yz)$, and $[x, y]$ represents the commutator, defined as $xy - yx$. Recall that the *nucleus* of a ring or algebra R is the set $N = \{r \in R \mid 0 = (R, R, r) = (R, r, R) = (r, R, R)\}$, while the *center* is the set $C = \{n \in N \mid 0 = [n, R]\}$. We will also let N_l denote $\{n \in R \mid (n, R, R) = 0\}$, the *left nucleus* of R, and U will denote $\{u \in R \mid [R, u] = 0\}$, the *commuting center*. Finally, we let B denote $\sum(R, R, R)$, the linear span of all associators.

The identities we wish to study are

$$(a, b, c) - (a, c, b) = 0 \tag{1}$$

$$(a, [b, c], d) = 0. \tag{2}$$

Rings satisfying identities (1) and (2) were studied by Y. Paul in [7]. There he showed that a prime ring satisfying these identities is either associative or its nucleus and center coincide. We will extend his work. *In particular, we will show that any semiprime ring having characteristic $\neq 2, 3$ and satisfying (1) and (2) must be associative.*

2 Formulating the Conjecture

Assume that R is a semiprime ring satisfying identities (1) and (2). Paul's insight ([7], p. 93, eq. 3) was to prove that in such rings

$$(a, b, c) \, [[d, e], f] = 0. \tag{3}$$

Let A be the ideal generated by $B = (R, R, R)$, and let C be the ideal generated by $[[R, R], R]$. Using (3) it is straightforward to show that

$$AC = 0. \tag{4}$$

By (4) the ideal $A \cap C$ is trivial. And since R is semiprime, we must have $A \cap C = 0$. In what follows, Lemmas 1,2,4,5 are given without proof. They were established with **Albert** for algebras over the field Z_{251}. *We caution that some of these lemmas do not hold for certain characteristics, and we ask the reader to ignore this temporarily.*

Lemma 1 *If R satisfies identities (1), (2), and*

$$[[a, b], c] \;\; = \;\; 0, \tag{5}$$

then every commutator is in the center of R.

Lemma 2 *The identities (1), (2), and (5) imply, for all x,*

$$[x^2, x]^2 \;\; = \;\; 0. \tag{6}$$

Lemma 3 *A semiprime algebra satisfying (1) and (2) must also satisfy*

$$(x, x, x) \;\; = \;\; 0. \tag{7}$$

Proof: Let $u = (x, x, x) = [x^2, x]$, and let $\bar{u}$ be the image of u in R/C. By Lemma 1, $\bar{u}$ is in the center of R/C. By Lemma 2, $\bar{u}^2 = 0$. Thus $\bar{u}$ generates a trivial ideal in R/C. If I is the ideal generated by u then $\bar{I}$ is the ideal generated by $\bar{u}$. So $I^2 \subseteq C$. Since u is an associator, I and hence I^2 is contained in A. Hence $I^2 \subseteq A \cap C = 0$. Since R is semiprime, $I = 0$, and we have $u = 0$. $\square$

Lemma 4 *The identities (1), (2), and (7), together with*

$$(ab, c, d) = (a, bc, d) = (a, b, cd) = 0, \tag{8}$$

imply

$$a(b, c, d) = 0. \tag{9}$$

Lemma 5 *The identities (1), (2), and (7) imply*

$$(a, b, b) \, (c, d, d) \;\; = \;\; 0. \tag{10}$$

Lemma 6 *In algebras satisfying (1), (2), and (7), the ideal $A = (R, R, R)$.*

Proof: Since $A = B + RB$, it suffices to show $RB \subseteq B$. In the free algebra on a, b, c, d, Lemma 4 tells us that $a(b, c, d)$ is in the T-ideal generated by the polynomials in (1), (2), (7), (8). But the polynomials in (8) have the same degree as $a(b, c, d)$. Therefore, modulo the T-ideal generated by (1), (2), and (7), $a(b, c, d)$ must be a linear combination of the elements of the form (RR, R, R), (R, RR, R), and (R, R, RR). This completes the proof. $\square$

Fact: Let R be a semiprime algebra over Z_{251} satisfying (1), (2). Then R is associative.

Proof: By Lemma 3, R satisfies (7) as well. By Lemma 5, R must satisfy (10). Using (1) and the linearized form of (10) we get $(R, R, R)(R, R, R) = 0$. By Lemma 6, this says $A^2 = 0$. Since R is semiprime, we must have $A = 0$. $\square$

This fact suggests that the result might also hold for nonassociative rings of different characteristics. If we are to use the same proof approach, we can rule out certain characteristics: In the above discussion, characteristic $\neq 2$ was implicitly assumed in linearizing (10). Using **Albert**, we see Lemma 2 fails to hold over Z_3. However Lemmas 1,2,4,5 *do* hold over Z_5 and Z_7. We now have strong evidence to conjecture

Theorem: Let R be a semiprime ring having characteristic $\neq 2, 3$, satisfying (1) and (2). Then R is associative.

Before proceeding with the proof of this theorem we note that if one omits either (1) or (2) from the hypothesis, then associativity is no longer implied. If one omits (1) then there exist finite division rings which are commutative but not associative. If one omits (2) then there exist simple rings and also rings without proper divisors of zero which do not even satisfy $(x, x, x) = 0$, [6].

3 Proof of Theorem

We now abandon the computer, and prove the conjecture. Lemma 1 is easy to show, and so it suffices to establish Lemmas 2,4,5. So throughout this section, let R be a ring of characteristic $\neq 2, 3$. The following two identities are true in arbitrary rings:

$$0 = f(w, x, y, z) = (wx, y, z) - (w, xy, z) + (w, x, yz) - w(x, y, z) - (w, x, y)z \quad (11)$$

$$[xy, z] = x[y, z] + [x, z]y + (x, y, z) + (z, x, y) - (x, z, y). \quad (12)$$

Simplification of (12) occurs by applying (1), and so

$$[xy, z] = x[y, z] + [x, z]y + (z, x, y). \quad (13)$$

Proof of Lemma 2: We assume R satisfies (1), (2), and (5). Let $u = (x, x, x) = x^2 x - x x^2$ $= [x^2, x]$. Then $f(x, x, x, x) = (x^2, x, x) - (x, x^2, x) + (x, x, x^2) - x(x, x, x) - (x, x, x)x = 0$. But $-(x, x^2, x) + (x, x, x^2) = 0$, using (1), and since u is a commutator, u commutes with x by hypothesis. Thus,

$$(x^2, x, x) = 2ux. \quad (14)$$

By linearization of (14) we obtain

$$(xy + yx, x, x) + (x^2, x, y) + (x^2, y, x) = 2(y, x, x)x + 2(x, y, x)x + 2(x, x, y)x + 2uy.$$

Substituting $z = [a, b]$ in (13) and using (5) we get $([R, R], R, R) = 0$. By applying this and (1) to the previous equation we get

$$2(yx, x, x) + 2(x^2, x, y) = 2(y, x, x)x + 4(x, x, y)x + 2uy.$$

Hence division by 2 yields

$$(yx, x, x) + (x^2, x, y) = (y, x, x)x + 2(x, x, y)x + uy. \quad (15)$$

Now $f(y, x, x, x) = (yx, x, x) - (y, x^2, x) + (y, x, x^2) - yu - (y, x, x)x = 0$, and after applying (1) and (5) this becomes

$$(yx, x, x) = (y, x, x)x + uy. \quad (16)$$

6

Subtracting (16) from (15) yields

$$(x^2, x, y) \;=\; 2(x, x, y)x. \tag{17}$$

Since $f(x, x, y, x) = (x^2, y, x) - (x, xy, x) + (x, x, yx) - x(x, y, x) - (x, x, y)x = 0$, from (1) and (2) we see that $-(x, xy, x) + (x, x, yx) = 0$, and $(x^2, y, x) = (x^2, x, y)$, so

$$(x^2, x, y) \;=\; x(x, x, y) + (x, x, y)x. \tag{18}$$

But comparing (17) and (18) it follows that

$$[(x, x, y), x] \;=\; 0. \tag{19}$$

By applying (1) to (19), it follows that

$$[(x, y, x), x] \;=\; 0. \tag{20}$$

Linearizing $[(x, x, x), x] = [[x^2, x], x] = 0$, it must be that

$$[(y, x, x) + (x, y, x) + (x, x, y), x] + [u, y] = 0.$$

But $[u, y] = [[x^2, x], y] = 0$, by hypothesis and so (19) and (20) imply

$$[(y, x, x), x] \;=\; 0. \tag{21}$$

Using (21) we have $[(yx, x, x), x] = 0$. But $f(y, x, x, x) = (yx, x, x) - (y, x^2, x) + (y, x, x^2) - yu - (y, x, x)x = 0$ implies $(yx, x, x) = yu + (y, x, x)x$. Commute this equation with x. Thus

$$[yu, x] + [(y, x, x)x, x] \;=\; 0. \tag{22}$$

Expanding $[(y, x, x)x, x]$ through the use of (13) we obtain

$$[(y, x, x)x, x] = (y, x, x)[x, x] + [(y, x, x), x]x + (x, (y, x, x), x).$$

But then (21) applied to this gives

$$[(y, x, x)x, x] \;=\; (x, (y, x, x), x). \tag{23}$$

7

Now (13) implies $[yu, x] = y[u, x] + [y, x]u + (x, y, u)$, and so (2) and (5) yield $[yu, x] = [y, x]u = u[y, x] = -u[x, y]$. Comparison of this with (22) and (23) shows

$$(x, (y, x, x), x) = u[x, y]. \tag{24}$$

Letting $y = x^2$ in (24) we get $(x, (x^2, x, x), x) = -u^2$. Using (14) we have

$$2(x, ux, x) = -u^2. \tag{25}$$

Note that since u is a commutator, $(R, u, R) = 0$. Then (1) implies $(R, R, u) = 0$. By assumption $[R, u] = 0$. Now (13), starting with $[RR, u] = 0$, shows $(u, R, R) = 0$. Hence u is in the center of R, so that $2(x, ux, x) = 2(x, x, ux) = 2(x, x, xu) = 2u^2$. Substituting this into (25), shows $2u^2 = -u^2$, or $3u^2 = 0$. Consequently $u^2 = 0$. This completes the proof of Lemma 2. $\square$.

Proof of Lemma 4: We assume R satisfies (1), (2), and (7). It suffices to show that $6w(x, y, z) \in B$. For then $6w(x, y, z)$ can be written as a linear combination of the terms in (8), and if (8) holds, so must (9). Using $f(w, x, y, z) = 0$ we obtain

$$w(x, y, z) + (w, x, y)z = (wx, y, z) - (w, xy, z) + (w, x, yz) = b \in B. \tag{26}$$

Define $r \equiv s$ whenever $r - s \in B$. Thus $w(x, y, z) \equiv -(w, x, y)z$. Since $-(w, x, y)z = -(w, y, x)z$, we have $w(x, y, z) \equiv w(y, x, z)$. But then $w(x, y, z) \equiv w(y, x, z) \equiv w(y, z, x) \equiv w(z, y, x) \equiv w(z, x, y) \equiv w(x, z, y)$. Since $w(x, x, x) = 0$, linearization shows

$$0 = w\{(x, y, z) + (x, z, y) + (y, x, z) + (y, z, x) + (z, x, y) + (z, y, x)\}.$$

Thus $6w(x, y, z) \equiv 0$ and hence $6w(x, y, z) \in B$. This completes the proof. $\square$

Proof of Lemma 5: We assume R satisfies (1), (2), and (7). As observed in [4], identity $2'$, a ring which satisfies (1) and (7) must satisfy

$$(x, y, z) + (y, z, x) + (z, x, y) = 0, \tag{27}$$

8

and so is of type $(1, 1)$. From identity (8) of $[3]$ such rings satisfy

$$[(w, y, z), x] = -[(x, y, z), w].\qquad(28)$$

From $f(x, y, z, y) = 0$, it follows using (1) and (2) that

$$(xy, z, y) = x(y, z, y) + (x, y, z)y.\qquad(29)$$

However $(xy, z, y) = (xy, y, z)$ using (1), and from $f(x, y, y, z) = 0$ it now follows that

$$(xy, z, y) = (xy, y, z) = (x, y^2, z) - (x, y, yz) + x(y, y, z) + (x, y, y)z.\qquad(30)$$

Comparing (29) and (30) and using $x(y, z, y) = x(y, y, z)$, we get

$$(x, y^2, z) = (x, y, yz) + (x, y, z)y - (x, y, y)z.\qquad(31)$$

But $(x, y^2, z) = (x, z, y^2)$ and $f(x, z, y, y) = 0$ yields

$$(x, y^2, z) = (x, z, y^2) = (x, zy, y) - (xz, y, y) + x(z, y, y) + (x, z, y)y.\qquad(32)$$

Comparing (31) and (32), it follows, using (1) and (2), that

$$(xz, y, y) = (x, y, y)z + x(z, y, y).\qquad(33)$$

Interchanging x and z in (33) shows

$$(zx, y, y) = (z, y, y)x + z(x, y, y).\qquad(34)$$

Now (2) and a linearization of (7) imply $(xz, y, y) = (zx, y, y)$, and this together with (33) and (34) yields

$$[(x, y, y), z] = [(z, y, y), x].\qquad(35)$$

But (28) implies

$$[(x, y, y), z] = -[(z, y, y), x].\qquad(36)$$

9

Now (35) and (36) combine to yield $2[(x, y, y), z] = 0$, so that $[(x, y, y), z] = 0$. Linearization then implies

$$[(R, R, R), R] = 0. \tag{37}$$

Thus $(R, R, R) \in U$. If $u \in U$, then (13) shows $0 = [xy, u] - x[y, u] - [x, u]y = (u, x, y)$ so that $u \in N_l$. Thus $U \subseteq N_l$. It now follows from Lemma 4 and (37) that

$$(R, R, R)R \subseteq B \subseteq U \subseteq N_l. \tag{38}$$

If $b \in B$, then $f(b, x, y, z) = 0$ implies $(bx, y, z) - (b, xy, z) + (b, x, yz) = (b, x, y)z + b(x, y, z)$. Now using (38) we obtain $b(x, y, z) = 0$, and thus

$$(R, R, R)(R, R, R) = 0. \tag{39}$$

This completes the proof of the lemma as well as the theorem. □

4   Discussion and Conclusion

In section 2, we did not always construct equations and proofs. For example, in Lemma 2 we did not construct the equation showing how $[x^2, x]^2$ could be written in terms of the form $(R, [R, R], R)$, $[[R, R], R]$, and $(u, v, w) - (u, w, v)$. Our method was to proceed because of **Albert**'s output, knowing such equations existed. In our view, *just what these equations look like does not matter.*

Albert allows the researcher to ignore these proofs, at least temporarily, and work at a *higher level of abstraction.* By focusing on high level ideas – ideals, the center, the nucleus, and so forth – the researcher can carry on with the outline of the argument. Later, as shown in section 3, he or she can fill in the details by constructing the equations.

We do not see **Albert** as a substitute for mathematical proofs. Rather, it is a tool which can allow the researcher to proceed with reasonable confidence toward a result, without

having to fill in low-level detail. This results in a top-down approach. In this way the researcher plots out the path to a major theorem. He or she is reasonably confident that the intervening steps can be satisfactorily proven if necessary. By using **Albert**, the researcher can test quickly whether certain directions are worth pursuing. When one direction leads to a good result, the researcher then fills in the details.

Theoretically, it would be possible for **Albert** to print out a proof that a certain identity held. However, as **Albert** has no understanding of elegance, such a proof would likely be long, complicated and useless.

Our point is *not* that the output of **Albert** should or shouldn't be regarded as legitimate mathematical proof. This philosophical issue is beyond the scope of our paper. Rather, our point is simply that this system allows research to be done at a higher level of abstraction, thereby enhancing efficiency. As our example shows, reasonable conjectures can be quickly reached that can later be proven.

References

[1] I.R. Hentzel and D.P. Jacobs, A dynamic programming method for building free algebras, *Computers & Mathematics with Applications* **22** (1991), 61-66.

[2] D.P. Jacobs, and S.V. Muddana, A.J. Offutt, A computer algebra system for nonassociative identities, Hadronic Mechanics and Nonpotential Interactions, Proceedings of the Fifth International Conference, Cedar Falls, Myung, H.C. (Ed.), Nova Science Publishers, Inc., New York, 1992.

[3] E. Kleinfeld, Rings of (γ, δ) type, *Portugaliae Math.* **18** (1959), 107-110.

[4] E. Kleinfeld, Simple algebras of type $(1,1)$ are associative, *Canadian J. Math.* **13** (1961), 129-148.

[5] E. Kleinfeld, On centers of alternative algebras, *Communications in Algebra* **8** (1980), 289-297.

[6] E. Kleinfeld, On rings satisfying $(x, y, z) = (x, z, y)$, *Algebras, Groups, and Geometries* **4** (1987), 129-138.

[7] Y. Paul, Prime rings satisfying $(x, y, z) - (x, z, y)$, Proceedings of the Symposium on Algebra and Number Theory, Kochi, Kerala, India, July, 1990, 91-95.