RIGHT ALTERNATIVE DIVISION RINGS OF CHARACTERISTIC TWO

R. L. SAN SOUCIE

1. **Introduction.** A ring, R, is said to be *right alternative* if $yx\cdot x - y\cdot xx = 0$ is an identical relation in R. Right alternative division rings arise quite naturally in the study of certain projective and affine planes. More specifically, the division rings of geometric significance are those with the right inverse property. However, a division ring, R, with unit element, has the right inverse property if and only if $w(xy\cdot x) - (wx\cdot y)x$ is identically zero in R, and in this case R is right alternative. On the other hand, alternative division rings automatically have the right inverse property.

In a recent paper, L. A. Skornyakov [3][1] has shown that *right alternative division rings of characteristic not two are alternative.* He first proves that such rings satisfy the identity

$$w(xy\cdot x) = (wx\cdot y)x \tag{1.1}$$

for all w, x, y. R. H. Bruck has an example of a right alternative division ring, R, of characteristic two, which is not alternative. R, however, does not satisfy (1.1).

We prove the following theorem: *Let R be a right alternative division ring of characteristic two. Then R is alternative if and only if R satisfies* (1.1). As a geometric application of our result and that of Skornyakov, we note that if R is a division ring with the right inverse property and if π' is the affine plane with coordinates from R (in the sense of Marshall Hall [2]), then either π' is Desarguesian or R is a Cayley-Dickson algebra over its centre.

In an appendix, we include Bruck's example of a class of right alternative division rings of characteristic two which are not alternative. This has not heretofore been published, and we include it here at his request.

2. **Preliminary definitions and results.** In any ring R the associator (x, y, z) and the commutator (x, y) are defined by

$$(x, y, z) = xy\cdot z - x\cdot yz, \qquad (x, y) = xy - yx. \tag{2.1}$$

Then R is right alternative if and only if, for all x, y in R, $(y, x, x) = 0$, and R is alternative if and only if we also have $(x, x, y) = 0$. In order

Received by the editors January 15, 1954 and, in revised form, June 23, 1954.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

to state hypotheses as succinctly as possible, we adopt the following definitions. A right alternative ring, R, is said to be *strongly right alternative* if (1.1) holds in R. If such is the case, we shall say that R is SRA. Further, when R is SRA and a division ring, we shall say that R is SRAD. Finally, we shall use the letters u, v, w, x, y, z for arbitrary elements of R.

LEMMA 2.1. *If R is SRA, the following identities hold in R:*

$$(2.2) \qquad (w, x, xy) = (w, x, y)x,$$

$$(2.3) \qquad ((w, x, y), x, y) = (w, x, y)(y, x),$$

$$(2.4) \qquad (wx, y, z) = w(x, y, z) + (w, y, z)x - (w, x, (y, z)).$$

LEMMA 2.2. *Let R be SRAD. Then R has a unit element, 1; R has the right inverse property, and also*

$$(2.5) \qquad ((y, z), y, z) = 0.$$

Proofs of Lemmas 2.1 and 2.2 may be found in [3].

3. **A partition of R.** For fixed f, g in R, define the mapping π (of R into R) by $x\pi = (x, f, g)$. Then (2.4) may be written

$$(3.1) \qquad (xy)\pi = x \cdot y\pi + x\pi \cdot y - (x, y, (f, g)).$$

THEOREM 3.1. *Let R be SRAD. Let f and g be two elements of R such that $d = (g, f) \neq 0$. Let N and S be defined by $N = [n \in R \mid n\pi = 0]$, $S = [s \in R \mid s\pi = sd]$. Then $R = N + S$ and $NS = S$.*

PROOF. From (2.3), $x\pi \cdot \pi = x\pi \cdot d$ so that $x\pi$ is in S. Also $d\pi = 0$ by (2.5) so d, and hence d^{-1}, are in N. Set $q = x\pi \cdot d^{-1}$. Then $q\pi = x\pi = qd$ and so q is in S. If $y = x - q$, $y\pi = 0$, y is in N, $R = N + S$. Clearly, $z \in N$ and $z \in S$ implies $z = 0$. For any $n \in N$, $s \in S$, we have $ns \cdot \pi = ns \cdot d$ so $NS \subset S$. For $n \neq 0$, define m by $nm = s$. Then $n(n' + s') = s$, or $nn' \in S$. Hence $n' = 0$, $NS = S$.

COROLLARY 3.1. *If R has characteristic two, $S^2 = 0$ or N.*

PROOF. For any nonzero s, s' of S, we have

$$(3.2) \qquad ss' \cdot \pi = s \cdot ds' + s \cdot s'd.$$

Since the right-hand side of (3.2) is in S, we apply π using (3.1) and also using the definition of S. This gives $sd \cdot ds' + sd \cdot s'd = 0$ so that $(d, S) = 0$. Then (3.2) shows that ss' is in N. The obvious procedure yields $S^2 = N$, if $S \neq 0$.

4. **The main theorem.** We begin with a definition. Let R be a right

alternative ring, and let $M=[m\in R \mid (R, R, m)=0]$. Then M will be called the *right nucleus* of R. We prove

LEMMA 4.1. *Let R be a not associative strongly right alternative ring without divisors of zero. Let M be the right nucleus of R. Then $(R,M)=0$.*

PROOF. Since $M\neq R$, select $h\in R$, $h\notin M$, $m, m'\in M$. Then $(R, h, m)=0$ so that $0=(uv, h, m)=(u, v, (h, m))$ and $(h, m)\in M$. But also $(R, h, hm)=0$ so that $(h, hm)\in M$. Now $(hm, h)=h(m, h)$ and this implies that $h\in M$, a contradiction, unless $(m, h)=0$. Then $0=(hm, m')=h(m, m')$ so that $(m, m')=0$ and $(R, M)=0$.

COROLLARY 4.1. $(R, u, v)=0$ *implies* $(u, v)=0$.

THEOREM 4.1. *Let R be a not alternative strongly right alternative division ring of characteristic two. Then $R=N+S$, where N and S are defined as in Theorem* 3.1. *Moreover,* $(N, R, R)=0$, $NS=SN=S$, $S^2=N^2=N$, $(N, R)=0$, *and N is a field.*

PROOF. There exist in R two elements a, b such that $(a, a, b)\neq 0$. We can assume $(a, b)\neq 0$. Indeed, if $(a, b)=0$, then $(a, ab)=(a, a, b)\neq 0$ and also $(a, a, ab)\neq 0$. We can thus apply Theorem 3.1 with $f=a$, $g=b$. This gives $R=N+S$, $NS=S$ and $S^2=N$. That $(N, R, R)=0$ may be quoted verbatim from [3, Lemma 4, p. 180]. The obvious procedure again yields $N^2=N$. For arbitrary nonzero n and s, $0=(ns, d)=(n, d)s$ so $(d, n)=0$. Now $sn\cdot\pi=s\cdot dn$, and since $s\cdot dn$ is in S, applying π to this element in two ways gives $(s\cdot dn)d=s(d\cdot dn)$. But $(d, N)=0$ so that $(s, d, n)=0$. Hence $sn\cdot\pi=sn\cdot d$ so that $SN\subset S$. The usual trick gives $SN=S$.

Clearly $(x, n, s)\in N$. Hence $0=((x, n, s), n, s)=(x, n, s)(n, s)$ and thus $(N, S)=0$. Finally, for arbitrary $n, n'\in N$, $(n, n')=(ss', n')=0$ so $(N, N)=0$. This proves the theorem.

For some fixed nonzero $s\in S$, we write $R=N+Ns$. Then, with $x=n_1+n_2s$ and $y=n_3+n_4s$, we have

$$xy = n_1n_3 + n_2n_4\theta + (n_1n_4 + n_2n_3)s, \tag{4.1}$$

where we have put $s\cdot sn=n\theta$ and $n_2(n_4\theta)=n_2n_4\theta$.

LEMMA 4.2. *If $R=N+Ns$, then* $(s, s, N)=0$.

PROOF. Using (4.1) and the properties of N, we compute $q=s(xy\cdot x)+(sx\cdot y)x$ and obtain the relation

$$q = (n_1^2n_4)\theta + n_1^2n_4\theta + n_4(n_2\theta)^2 + (n_2^2n_4\theta)\theta. \tag{4.2}$$

But by hypothesis $q=0$. Hence the right-hand side of (4.2) vanishes

for all n in N. Put $n_1=1$ in (4.2) and get the relations

$$n_4(n_2\theta)^2 + (n_2^2 n_4\theta)\theta = 0, \tag{4.3}$$

$$(n_1^2 n_4)\theta + n_1^2 n_4\theta = 0. \tag{4.4}$$

Applying (4.4) to (4.3) gives

$$n_4(n_2\theta)^2 + n_2^2 n_4\theta^2 = 0. \tag{4.5}$$

In (4.5) put $n_2=n_4=1$ and obtain $(1\theta)^2=1\cdot\theta^2$. Again, in (4.5) set $n_4=1$. This gives $n_2\theta=n_2\cdot 1\theta$. But $1\theta=s^2\in N$, so that $n_2\theta=s\cdot sn_2=s^2n_2$. This proves the lemma since n_2 is arbitrary.

It is now possible to prove the main theorem.

THEOREM 4.2. *Let R be a right alternative division ring of characteristic two. Then R is alternative if and only if $w(xy\cdot x)-(wx\cdot y)x$ is identically zero in R.*

PROOF. (i) The necessity is well known. (See [1, p. 880]). (ii) We assume the given relation and further suppose that R is not alternative. Then $R=N+Ns$, N a field, commutative with R, and $(s, s, N)=0$. Therefore $(x, y)=(n_1+n_2s, n_3+n_4s)=(n_2s, n_4s)=n_4[(n_2, s)s+(s, s, n_2)]=0$. Thus R is commutative, hence alternative, and this is a contradiction. Hence R is alternative anyway and the proof is complete.

Appendix. We here indicate Bruck's method of constructing right alternative division rings of characteristic two which are not alternative. Let F be a field of characteristic two, somewhat restricted by Theorem I below. Let R be the set of all couples (f, g), $f, g\in F$. Equality and addition in R shall be componentwise, and multiplication will be defined by

$$(f, g)(h, k) = (fh + g\cdot k\theta, fk + gh) \tag{1}$$

where θ is an additive endomorphism of F. With these definitions, it is easy to verify that R is a right alternative ring.

LEMMA I. *Let R be defined as above. R is a division ring if and only if, for each $f\in F$, the mapping $\mu(f)$, defined by*

$$x\cdot\mu(f) = x\theta + xf^2, \qquad \text{all } x\in F, \tag{2}$$

is one-to-one of F upon F.

PROOF. (i) Suppose $(f, g)(h, k)=(p, q)$. This implies

$$fh + g\cdot k\theta = p, \qquad fk + gh = q. \tag{3}$$

If h, k, p, q are given, (3) implies that f and g will exist uniquely if and only if

$$h^2 + k \cdot k\theta \neq 0. \tag{4}$$

(ii) Let f, g, p, q be given. We can assume $f \neq 0 \neq g$; multiply the first of equations (3) by g, the second by f, and add the resulting equations to obtain $f^2k+g^2 \cdot k\theta = fq+gp$. Multiplying both sides of this last equation by $(g^2)^{-1}$, we get

$$k\theta + r^2k = s \tag{5}$$

where $r = fg^{-1}$ and $s = (fq+gp)(g^2)^{-1}$. With μ defined by (2), (5) becomes $k \cdot \mu(r) = s$ so k exists uniquely if and only if μ is 1-1. In such a case, h will be unique by (3). Finally, an easy computation shows that if $\mu(f)$ is 1-1, then (4) holds.

LEMMA II. *Let R be defined as above. Then R satisfies* (1.1) *if and only if $f\theta = gf$, some fixed $g \in F$, all $f \in F$.*

The proof is the same as that of Lemma 4.2.

THEOREM I. *Let F be any field of characteristic two for which there exists an automorphism α of order 2 and an element $a \in F$ such that $a\alpha = a$ and a is not a square in F. Then, the additive endomorphism θ of F, defined by $x\theta = x\alpha + ax$, all $x \in F$, has the property that, for every fixed $f \in F$, the mapping $\mu(f)$, defined by* (2), *is* 1-1 *of F upon F.*

PROOF. For f and g any elements of F, we have to show the existence of one and only one x in F such that

$$(a + f^2)x + x\alpha = g. \tag{6}$$

Since $\alpha^2 = 1$, we apply α to (6) and obtain

$$x + (a + f^2\alpha) \cdot x\alpha = g\alpha. \tag{7}$$

Regarding (6) and (7) as simultaneous equations in x, $x\alpha$ we get

$$D \cdot x = (a + f^2\alpha)g + g\alpha, \tag{8}$$

$$D = a(f + f\alpha)^2 + (1 + a + f \cdot f\alpha)^2. \tag{9}$$

Now $D = 0$ implies that a is a square, so D is not zero and (8) determines x uniquely. Since, from (9), $D\alpha = D$, we find that $D \cdot x\alpha = g + (a+f^2) \cdot g\alpha$. Thus the x determined by (8) satisfies (6) and the proof is complete. Note that θ, as defined by the theorem, does not satisfy the condition of Lemma II so that R is not alternative.

Finally, we show that fields F, having the properties required by the theorem, actually exist, and exhibit an α and a nonsquare ele-

ment a which suffice. Let $F=B(t)$, B any field of characteristic two and t transcendental over B. If $f(t)$ denotes an arbitrary element of $B(t)$, then define α by $f(t)\alpha=f(1/t)$, and let $a=t+1/t$.

Bibliography

1. R. H. Bruck and Erwin Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc. vol. 2 (1951) pp. 878–890.

2. Marshall Hall, *Projective planes*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 229–277.

3. L. A. Skornyakov, *Right alternative fields*, Bull. Acad. Sci. URSS. Sér. Math. vol. 15 (1951) pp. 177–184.

The University of Oregon

ON THE CHARACTERISTIC FUNCTION OF A MATRIX PRODUCT

L. S. GODDARD

In a recent note [1], Roth has proved this result.

Theorem 1. *Let A and B be $n\times n$ matrices, with elements in a field F, and let*

$$|xI - A| = a_0(x^2) - xa_1(x^2), \qquad |xI - B| = b_0(x^2) - xb_1(x^2),$$

where a_0, a_1, b_0, and b_1 are elements in the polynomial ring $F[x]$. If the rank of $A-B$ is not greater than unity, then

$$|xI - AB| = (-)^n[a_0(x)b_0(x) - xa_1(x)b_1(x)].$$

In his proof, which is essentially a verification, Roth derives some interesting but unnecessary information. Here I present a proof which is shorter, direct, and leads naturally to a more general result involving three matrices.

The essential step in my proof is the observation that if A is a nonsingular matrix and M is a matrix of rank 1, then

$$|A + M| = |A| + \sum \Delta_i$$

where $\sum\Delta_i$ is a sum of n determinants, each consisting of $n-1$ columns of A and *one* column of M. This follows from the fact that, M being of rank 1, any two columns of M are linearly dependent.

Received by the editors June 25, 1954.