Commentationes Mathematicae Universitatis Carolinae

Tomáš Kepka

On a class of non-associative rings

Commentationes Mathematicae Universitatis Carolinae, Vol. 18 (1977), No. 3, 531--540

Persistent URL: `http://dml.cz/dmlcz/105797`

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

18,3 (1977)

ON A CLASS OF NON-ASSOCIATIVE RINGS

Tomáš KEPKA, Praha

Abstract: Rings satisfying the identities $x.yz = xy.xz$ and $yz.x = yx.zx$ are investigated. It is shown, among others, that these rings are direct sums of idempotent rings and rings which are nil-potent of degree three.

Key words: Ring, quasifield.

AMS: 17E05 Ref. Ž.: 2.723.5

In [1], M. Petrich has described associative distributive rings. Such rings are direct sums of boolean rings and of rings nilpotent of degree three. In the present paper, there is shown that a very similar result is valid in the non-associative case. Moreover, finite distributive rings are completely described.

1. Introduction. A ring R (possibly non-associative) is called

- distributive if it satisfies the identities $x.yz = xy.xz$ and $yz.x = yx.zx$,
- medial if it satisfies the identity $xy.uv = xu.yv$,
- idempotent if it satisfies the identity $x = xx$,
- nilpotent of degree three if it satisfies the identity $x.yz = uv.w$,
- quasiboolean if it is idempotent and distributive,

- a quasifield if the set $R \setminus \{0\}$ is a quasigroup,
- a quasidomain if $ab \neq 0$, whenever $a,b \in R \setminus \{0\}$,
- a division ring if for all $a,b \in R$, $a \neq 0$, there are $c, d \in R$ with $ac = b = da$,
- a field if it is a commutative and associative quasifield.

Further, R is said to be of characteristic two if R satisfies the identity $x + x = 0$. If moreover, the mapping $a \longrightarrow a^2$ is a permutation of R then we shall say that R is perfect. The inverse permutation will be denoted by $\sqrt{\ }$.

The following lemma is obvious.

1.1. Lemma. (i) Every idempotent ring is commutative and of characteristic two.

(ii) Every quasiboolean ring is commutative and of characteristic two.

(iii) Every boolean ring is quasiboolean.

(iv) Every ring which is nilpotent of degree three is associative, distributive and medial.

(v) A ring R is nilpotent of degree three iff it is associative and $abc = 0$ for all $a,b,c \in R$.

(vi) If R is a perfect field of characteristic two then the mapping $a \longrightarrow a^2$ is an atomorphism of R.

(vii) A ring R is a quasidomain iff the set $R \setminus \{0\}$ is a cancellation groupoid.

2. Basic properties of distributive rings. The following lemma is clear.

2.1. Lemma. Let R be a distributive ring and $a \in R$. Then the mappings $b \longrightarrow ab$ and $b \longrightarrow ba$ are endomorphisms of R.

If R is a ring then $\mathrm{Id}\, R$ denotes the set of all idempotents of R. $\mathrm{Id}\, R$ is non-empty, since $0 \in \mathrm{Id}\, R$.

2.2. Lemma. Let R be a distributive ring. Then $a.aa = aa.a \in \mathrm{Id}\, R$ for every $a \in R$.

Proof. We can write $aa.a = aa.aa = a.aa$ and $aa.aa = (a.aa)(a.aa)$ using the distributive laws for the multiplication of R.

2.3. Lemma. Let R be a distributive ring, $a \in \mathrm{Id}\, R$ and $b \in R$. Then $ab, ba \in \mathrm{Id}\, R$.

Proof. We have $ab.ab = aa.b = ab$, and hence $ab \in \mathrm{Id}\, R$. Similarly $ba \in \mathrm{Id}\, R$.

2.4. Lemma. Let R be a distributive ring. Then $a.bc \in \mathrm{Id}\, R$ and $ab.c \in \mathrm{Id}\, R$ for all $a,b,c \in R$.

Proof. Using distributive laws, we obtain the equalities $a.bc = ab.ac = (ab.a)(ab.c) = (aa.ba)(ab.c) = ((aa.a)(aa.b))(ab.c)$. However, $aa.a \in \mathrm{Id}\, R$ by 2.2, and consequently $a.bc \in \mathrm{Id}\, R$, as it follows from 2.3. Similarly $ab.c \in \mathrm{Id}\, R$.

2.5. Lemma. Let R be a distributive ring. Then $a + a = 0$ for every $a \in \mathrm{Id}\, R$.

Proof. We can write $a + a + a + a = aa + aa + aa + aa = (a + a + a + a)a$ and $a + a + a + a = (a + a)(a + a)$. Hence $a + a + a + a = ((a + a)(a + a))a = ((a + a)a)((a + a)a) = (a + a)(aa) = (a + a)a = a + a$. Thus $a + a = 0$.

2.6. Lemma. Let R be a distributive ring. Then $c.ab = c.ba$ and $ab.c = ba.c$ for all $a,b,c \in \mathrm{Id}\, R$.

Proof. We have $ca + cb + c.ab + c.ba = c(a + b + ab + ba) = c((a + b)(a + b)) = (c(a + b))(c(a + b)) = (cc)(a + b) = ca + cb$, and therefore $c.ab + c.ba = 0$. But $c.ab \in \mathrm{Id}\, R$

by 2.4, and hence $c.ab + c.ab = 0$ by 2.5. Now we see that $c.ab = c.ba$. Similarly we can prove the other equality.

2.7. Lemma. Let R be a distributive ring. Then $ab = ba$ for all $a,b \in \mathrm{Id}\, R$.

Proof. The elements ab, ba belong to Id R by 2.3. Using 2.6, we get $ab = ab.ab = ab.ba = ba.ba = ba$.

2.8. Lemma. A ring R is nilpotent of degree three iff it is a distributive ring and $\mathrm{Id}\, R = 0$.

Proof. Apply 1.1(iv) and 2.4.

2.9. Proposition. Let R be a distributive ring. Then:

(i) Id R is an ideal of R.

(ii) Id R is a quasiboolean ring.

(iii) The factorring R/Id R is nilpotent of degree three.

Proof. (i) Let $a,b \in \mathrm{Id}\, R$. Then $ab = ba$ and $ab + ba = 0$ by 2.5 and 2.7. Hence $(a + b)^2 = a + b + ab + ba = a + b$ and so $a + b \in \mathrm{Id}\, R$. Further, $-a = a$ and $0 \in \mathrm{Id}\, R$. We have proved that Id R is a subgroup of the additive group. The rest follows from 2.3.

(ii) is clear and (iii) is an easy consequence of 2.8.

2.10. Lemma. Let R be a distributive ring. Then $ab = ba$ for all $a \in \mathrm{Id}\, R$ and $b \in R$.

Proof. We can write $ba = b(a.aa) = (ba)(ba.ba) = $
$= (b.bb)a = a(b.bb) = (ab)(ab.ab) = (a.aa)b = ab$, since a,b, $bb \in \mathrm{Id}\, R$ and Id R is commutative.

2.11. Lemma. Let R be a distributive ring. Then $a.ba = $
$= ab.a$ for all $a,b \in R$.

Proof. By 2.4, $ab.a \in \mathrm{Id}\, R$. Hence $a.ba = ab.aa = $
$= (ab.a)(ab.a) = ab.a$.

2.12. Lemma. Let R be a distributive ring. Then $a.ab = a.ba = ab.a = ba.a$ for all $a,b \in R$.

Proof. $aa.a, aa.b \in \mathrm{Id}\, R$ and $\mathrm{Id}\, R$ is commutative. Hence $a.ab = aa.ab = (aa.a)(aa.b) = (aa.b)(aa.a) = aa.ba = ab.a$. Similarly $ba.a = a.ba$. But $a.ba = ab.a$ by 2.11.

2.13. Lemma. Let R be a distributive ring. Then $aa.b = a.bb = b.aa = bb.a$ for all $a,b \in R$.

Proof. We have $b.aa = ba.ba = bb.a$ and $aa.b = a.bb$. Further, $bb.a = (bb.a)(bb.a) = (bb.bb)a = (b.bb)a$, since $bb.a \in \mathrm{Id}\, R$. By 2.10, $(b.bb)a = a(b.bb)$. Hence $bb.a = a(b.bb) = a(bb.bb) = (a.bb)(a.bb) = a.bb$.

Let R be a distributive ring. We denote by f the mapping of R into R defined by $f(a) = a.aa$ for every $a \in R$. As we know, $f(a) = aa.aa = aa.a$.

2.14. Proposition. Let R be a distributive ring. Then f is an endomorphism of R, $f(R) = \mathrm{Id}\, R$ and $f(a) = a$ for every $a \in \mathrm{Id}\, R$. Moreover, $f^2 = f$.

Proof. Let $a,b \in R$. Then $f(a + b) = a.aa + a.bb + a.ab + a.ba + b.aa + b.bb + b.ab + b.ba$. However, $a.bb + b.aa + b.ba + b.ab + a.ab + a.ba = 0$, as it follows from 2.4, 2.5, 2.11, 2.12 and 2.13. Hence $f(a + b) = f(a) + f(b)$. Further, $f(ab) = (ab)(ab.ab) = a(b.bb) = af(b) = f(af(b)) = af(b)((af(b))(af(b))) = f(a)f(b)$, since $af(b)$ belongs to $\mathrm{Id}\, R$. The rest is clear.

If R is a distributive ring then we put $A(R) = \{a \in R \mid f(a) = 0\}$.

2.15. Proposition. Let R be a distributive ring. Then:

(i) $A(R)$ is an ideal of R.

(ii) $A(R)$ is isomorphic to the ring $R/\mathrm{Id}\, R$.

(iii) $A(R)$ is nilpotent of degree three.

(iv) $A(R) \cap \mathrm{Id}\, R = 0$ and $A(R) + \mathrm{Id}\, R = R$.

Proof. (i) follows from 2.14, since $A(R) = \ker f$ and (ii) is an easy consequence of (iii).

(iii) The equality $A(R) \cap \mathrm{Id}\, R = 0$ is evident. Further, if $a \in R$ then $f(a - f(a)) = f(a) - f^2(a) = f(a) - f(a) = 0$, $a - f(a) \in A(R)$ and $f(a) \in \mathrm{Id}\, R$. However $a = a - f(a) + f(a)$.

2.16. Theorem. Let R be a distributive ring. Then:

(i) $\mathrm{Id}\, R$ and $A(R)$ are ideals of R.

(ii) $\mathrm{Id}\, R$ is a quasiboolean ring.

(iii) $A(R)$ is nilpotent of degree three.

(iv) R is the direct sum of $\mathrm{Id}\, R$ and $A(R)$.

Proof. Apply 2.9 and 2.15.

2.17. Corollary. Every distributive ring is isomorphic to the cartesian product of a quasiboolean ring and of a ring which is nilpotent of degree three.

2.18. Corollary ([1]). Every associative distributive ring is isomorphic to the cartesian product of a boolean ring and of a ring which is nilpotent of degree three.

2.19. Proposition. Every distributive ring is medial.

Proof. With respect to 2.17 and 1.1 (iv), we can assume that R is idempotent. Let $a,b,c,d \in R$. We can write $ad.b + ad.c = (ad)(b + c) = (a(b + c))(d(b + c)) = (ab + ac)(db + dc) = ab.db + ab.dc + ac.db + ac.dc = ad.b + ab.dc + ac.db + ad.c$. Hence $ab.dc + ac.db = 0$, and so $ab.dc = ac.db$. However. R is commutative and $ab.cd = ab.dc = ac.db = ac.bd$.

3. Distributive quasidomains

3.1. Lemma. Every distributive quasidomain is idempotent.

Proof. Let R be a distributive quasidomain and $0 \neq a \in R$. Then $a.aa = aa.aa$ and $aa \neq 0$. With respect to 1.1 (vii), $a = aa$.

3.2. Proposition. Every subdirectly irreducible quasiboolean ring is a quasidomain.

Proof. Let R be a non-trivial subdirectly irreducible quasiboolean ring. Then R contains an ideal L which is the smallest non-zero ideal. Let $a,b \in R \setminus \{0\}$ and $ab = 0$. Put $I = \{c \in R \mid ac = 0\}$. Then I is a non-zero ideal and $L \subseteq I$. Hence $La = 0$. Let $K = \{d \in R \mid Ld = 0\}$. Again, K is a non-zero ideal and $L \subseteq K$. Then $L = L^2 = 0$, a contradiction.

An ideal I of a commutative ring R is said to be prime if the ring R/I is a quasidomain. The ring R is called semiprime if the intersection of all prime ideals of R is equal to zero.

3.3. Lemma. Let R be a subring of a quasiboolean quasidomain S, I be a prime ideal of R and $a \in R \setminus I$ be an element. Suppose that $aS \subseteq R$. Then $I = K \cap R$ for some prime ideal K of S.

Proof. Put $K = \{b \in S \mid ab \in I\}$. It is easy to see that K is a prime ideal of S and $K \cap R = I$.

3.4. Lemma. Let R be a quasiboolean quasidomain and $0 \neq a \in R$. Then there exists a quasiboolean quasidomain S such that R is a subring of S and $aS = R$.

Proof. Let $g(b) = ab$ for every $b \in R$. Then g is an injective endomorphism of R and g(R) is isomorphic to R. Clearly, $aR = g(R)$. Now we can identify R with $g(R)$ and S with R.

3.5. <u>Corollary</u>. Every quasiboolean quasidomain is a subring of a quasiboolean quasifield.

Proof. Apply 3.4 and some usual constructions.

3.6. <u>Proposition</u>. Every quasiboolean ring is semiprime.

Proof. This assertion is an easy consequence of 3.2.

4. <u>Distributive division rings</u>

4.1. <u>Lemma</u>. Every distributive division ring is idempotent.

Proof. Let R be a distributive division ring and $0 \neq a \in \in R$. There is $b \in R$ such that $a = ab$. Then $a = ab.b$ and $a \in \in \mathrm{Id}\, R$ by 2.4.

A ring R is said to be simple if 0 and R are the only ideals of R. It is clear that every division ring is simple.

4.2. <u>Lemma</u>. Every simple quasiboolean ring is a quasidomain.

Proof. Let R be a simple quasiboolean ring and $ab = 0$ for some $0 \neq a, b \in R$. Put $I = \{c \in R \mid ac = 0\}$. If $c \in I$ and $d \in R$ then $a.cd = ac.ad = 0.ad = 0$ and we see that I is an ideal. But $b \in I$ and $I = R$. Consequently $a \in I$ and $a = aa = 0$, a contradiction.

4.3. <u>Corollary</u>. Every distributive division ring is a quasiboolean quasifield.

Let R be a perfect field of characteristic two. Put $a * b = \sqrt{ab}$ for all $a, b \in R$. Then $a * (b + c) = a * b + a * c$, $(b + c) * a = b * a + c * a$ for all $a, b, c \in R$ and we see that $R(*)$ is a ring having the same underlying group as R. Moreover, as one may check easily, $R(*)$ is a quasiboolean quasifield. On the other hand, every quasiboolean quasifield can be obtained in such a way.

4.4. Theorem. Let $R(*)$ be a quasiboolean quasifield. Then there exists a perfect field R of characteristic two such that R has the same additive group as $R(*)$ and $a * b = \sqrt{ab}$ for all $a, b \in R$.

Proof. Let $j \in R \setminus \{0\}$ and $g(a) = a * j$ for every $a \in R$. Then g is an automorphism of $R(*)$. Put $ab = g^{-1}(a * b)$. Then $a(b + c) = g^{-1}(a * (b + c)) = g^{-1}(a * b) + g^{-1}(a * c) = ab + ac$. Further, $aj = g^{-1}(a * j) = g^{-1}g(a) = a$ and $aa = g^{-1}(a * a) = g^{-1}(a)$. Hence R is a commutative ring with unit, the mapping $a \longrightarrow a^2$ is a permutation of R, $a * b = \sqrt{ab}$ and $a + a = 0$ for all $a, b \in R$. Moreover, it is easy to see that R is a quasifield. Now it remains to show that R is associative. For, let $a, b, c \in R$. Then $a.bc = g^{-1}(a * g^{-1}(b * c)) = g^{-1}(a) * (g^{-2}(b) * g^{-2}(c)) = (g^{-2}(a) * j) * (g^{-2}(b) * g^{-2}(c)) = (g^{-2}(a) * g^{-2}(b)) * (j * g^{-2}(c)) = g^{-1}(g^{-1}(a) * g^{-1}(b)) * g^{-1}(c) = ab.c$ by 2.19.

5. Finite distributive rings

5.1. Theorem. Every finite distributive ring is isomorphic to the cartesian product of a finite number of quasiboolean quasifields and of a ring which is nilpotent of degree three.

Proof. Let R be a finite distributive ring. With respect to 2.17, we can assume that R is a quasiboolean ring. Since R is finite, R is a direct sum of directly indecomposable rings. Suppose that R is directly indecomposable. As it is easy to see, every finite quasidomain is a quasifield. Hence every prime ideal of R is a maximal ideal. If I, K are non-zero ideals of R, I is a maximal ideal and $I \cap K = 0$, then $R = I + K$ and R is the direct sum of I and K, a contradiction. Now it follows from 3.6 that R is a quasidomain.

5.2. Corollary. Every finite associative distributive ring is isomorphic to the cartesian product of a finite number of two-element fields and of a ring which is nilpotent of degree three.

R e f e r e n c e

[1] M. PETRICH: Structure des demi-groupes et anneaux distributifs, C.R. Acad. Sci. Paris 268, A849-A852

Matematicko-fyzikální fakulta
Karlova universita
Sokolovská 83, 18600 Praha 8
Československo

(Oblatum 1.4. 1977)