A COMMUTATIVITY CONDITION FOR RINGS

HOWARD E. BELL

The object of this paper is to prove the following theorem, a special case of which was previously explored in [1].

THEOREM. Let $R$ be any associative ring with the property that

$$\text{(f)} \quad \text{for each } x, y \in R, \text{there exist integers } m, n \geq 1 \text{ for which } xy = y^m x^n.$$ 

Then $R$ is commutative.

Proof of the Theorem. We note at once that any ring $R$ satisfying (f) is a duo ring and hence has its idempotents in the center (see [7]). Moreover, if $a, b \in R$ are such that $ab = 0$, then $ba = 0$ also, so that all annihilators are two-sided and there is no distinction between right and left zero divisors. We shall denote the annihilator of a subset $T$ of $R$ by $A(T)$, and the set of zero divisors of $R$ (including 0) by $D$.

LEMMA 1. If $R$ is a division ring satisfying (f), then $R$ is commutative.

Proof. Suppose that $R$ is a counterexample, and let $a$ and $b$ be a pair of non-commuting elements. Then $ab = b^m a^n = (a^n)^i (b^m)^j$, where at least one of $n$ and $m$ is greater than 1. If $ns = 1$, then $mt > 1$ and $b^m t = e$, the identity element of $R$; similarly, if $nt = 1$, $a^n s = e$. The only other possibility is that $ns > 1$ and $nt > 1$, in which case $a^{n-1} b^{m-1} = e$. Thus, $R$ has the property that

$$(*) \quad \text{for each } x, y \in R, \text{there exist positive integers } i, j \text{ with } x^i y^j = y^j x^i.$$ 

For each $y \in R$, define $K_y = \{ x \in R | xy^i = y^j x \text{ for some positive integer } i \}$. If there exists $y \in R$ for which $K_y \neq R$, then (*) implies that $R$ is radical over a proper subring and is thus commutative by a theorem of Faith [4; 6]; on the other hand, if $K_y = R$ for all $y \in R$, commutativity of $R$ follows from Theorem 1 of [5]. This completes the proof of Lemma 1.

LEMMA 2. Let $R$ be any ring satisfying (f). If $a, b \in R$ are elements such that $a(ab - ba) = b(ab - ba) = 0$, then $a$ and $b$ commute. Moreover, $a(ab - ba)x = b(ab - ba)x = 0$ implies $(ab - ba)x = 0$.

Proof. Since $a^2 b = aba = ba^2$ and $b^2 a = bab = ab^2$, we have $a^i b = ba^i$ and $ab^i = b^i a$ for all $i \geq 2$. Thus, if $ab = b^m a^n$ and $ba = a^j b^k$, we get $ab = a^n b^m$ and $ba = b^k a^j$; and it follows that $ab = b^m a^n = b^{m+1} b^i a^{n-i} = b^{m+k-1} a^{n-i-1} = \ldots$
Thus $a^n b^m = ba$. The second assertion of the lemma is obtained by applying the same argument to the ring $R/A(x)$.

Of course, it will suffice to show that subdirectly irreducible rings satisfying $(\dagger)$ are commutative. Since subdirectly irreducible duo rings with no non-zero divisors of zero are division rings, we may assume that $D$ is non-trivial. In this case, $D = A(S)$, where $S$ denotes the heart of $R$ (the unique minimal ideal); furthermore, if $R \neq D$, then $S = A(D)$ and $R/D$ is a division ring. (These results are all contained in the proof of Theorem 4 of [7].)

**Lemma 3.** Let $R$ be a subdirectly irreducible ring satisfying $(\dagger)$ and having a non-trivial set $D$ of zero divisors. Then each of the following properties holds in $R$:

(i) $D$ is a commutative subring.

(ii) If $a \in D$ fails to commute with $b \in R$, there exists an integer $s > 1$ for which $a(b^s - b) = 0$. Thus, $b^s - b \in D$ and $ab^{s-1} = b^{s-1}a$.

(iii) If $a \in D$ and $b \in R$, then $ab - ba$ belongs to the heart $S$ of $R$.

(iv) If $D$ is not contained in the center $Z$ of $R$, then there exists a prime $p$ for which $R^+_p$ is a $p$-group and $p(ab - ba) = 0$ for all $a \in D$, $b \in R$.

**Proof.** (i) Suppose $a, b \in D$ and $ab - ba \neq 0$. The first conclusion of Lemma 2 guarantees that $(ab - ba)R$ is a non-zero ideal of $R$; hence, if $0 \neq s \in S$, we have $s = (ab - ba)x$ for some $x \in R$. However, the fact that $DS = 0$ yields $0 = as = bs = a(ab - ba)x = b(ab - ba)x$; and by the second part of Lemma 2, we get $s = 0$ — a contradiction.

(ii) Suppose $a \in D$ and $b \in R$ fail to commute. Then there exist $m, n, k$, and $j$ such that $ab = b^m a^n$ and $ba = a^k b^j$. We show first that $n = 1$ and $k = 1$.

Observe that for all $v \geq 1$, $w \geq 0$, $a^v b^w$ and $b^w a^v$ belong to $D$ and hence commute with $a$. If $n > 1$, we obtain $ab = b^m a^n = a^{n-1} b^m a = a^{n-1} b^{m-1} a b^j = a^{k+n-1} b^{m+1-1} = a^{k+n-2} b^{m+1} a b^j = a^{k+n-1} b^{m+1} a b^j = a^{k+n-1} b^{m+1} a b^j = a^{k+n} b^{m+1} a b^j = a^{k+n} b^{m+1} a b^j$, which is a contradiction. Similarly, the assumption that $k > 1$ yields a contradiction.

Continuing with the same notation, we have $ab = b^m a^n = b^{m-1} a b = b^{m-1} a b = b^{m-2} b^j = \ldots = b^{m-j}$; letting $s = mj$, we get $a(b^s - b) = 0 = (b^s - b)a$. Since $b \notin D$, it follows that $a = ab^{s-1} = b^{s-1}a$, and all the conclusions of (ii) are established.

(iii) If $D = R$, $ab - ba = 0$. If $D \neq R$, in which case $S = A(D)$, let $a, c \in D$ and $b \in R$ and note that $(ab - ba)c = a(bc) - b(ac) = (bc)a - b(ca) = 0$. Thus $ab - ba \in A(D) = S$.

(iv) Suppose $a \in D$ and $b \in R$ do not commute. Then there exists an integer $k > 1$ for which $kb$ also fails to commute with $a$; thus there exist integers $s, t > 1$ for which $a(b^s - b) = 0 = a((kb)^t - kb)$. Letting $q = (s - 1)(t - 1) + 1$, we have $a(b^s - b) = 0 = a(k^q b^s - kb)$ and therefore

1. $(k^s - k)ab = 0$.

Since $b \notin D$, this yields $(k^s - k)a = 0$. We now know $D \setminus Z$ is contained in the ideal $T$ of elements of finite additive order; and since $a \in D \setminus Z$ and $c \in D \cap Z$ implies $a + c \notin Z$, we get $D \subseteq T$. 

https://doi.org/10.4153/CJM-1976-096-3 Published online by Cambridge University Press
Next, consider any element $b$ which does not commute elementwise with $D$. Since $b$ satisfies Equation (1) for some $k, q > 1$ and some $a \in D$, we have $(k^q - k)b \in D \subseteq T$ and hence $b \in T$. Thus, all elements of $R \setminus T$ commute elementwise with $D$.

Suppose now that $R \setminus T \neq \emptyset$, and let $c$ denote any element of $R \setminus T$. For arbitrary $t \in T$ and $a \in D$, both $c$ and $c + t$ commute with $a$, and therefore $t$ commutes with $a$. Hence $R = (R \setminus T) \cup T$ commutes elementwise with $D$, contradicting the hypothesis that $D \not\subseteq Z$; thus, $R = T$, and since the subdirect irreducibility of $R$ rules out the possibility that $R^+$ has nontrivial $p$-primary components for more than one prime $p$, $R$ must be a $p$-group for some prime $p$.

It follows at once that the division ring $R/D$ is of characteristic $p$, so that for all $b \in R$, $pb \in D$ and hence commutes with all $a \in D$ by part (i).

The following lemma, used several times in the remainder of the paper, has an easy proof, which we omit.

**Lemma 4.** Let $R$ be any ring. For fixed $r \in R$, define the mapping $\delta_r : R \to R$ by

$$\delta_r(x) = xr - rx \quad \text{for all } x \in R.$$ 

Then $\delta_r$ is a derivation—that is, $\delta_r(xy) = x\delta_r(y) + \delta_r(x)y$ for all $x, y \in R$. Moreover, if $x$ commutes with $xr - rx$, then $\delta_r(x^n) = nx^{n-1}\delta_r(x)$ for all positive integers $n$.

**Lemma 5.** Let $R$ be a subdirectly irreducible ring satisfying $(†)$ and having $D \neq \{0\}$. Then $D \subseteq Z$.

**Proof.** By (i) of Lemma 3, we may assume that $R \neq D$. Lemma 3, part (i), also implies that if $a_1, a_2 \in D$, then $a_1a_2R \subseteq Z$; thus, if there exist $a_1, a_2 \in D$ for which $a_1a_2 \neq 0$, part (iii) of Lemma 3 guarantees that $ab - ba \in Z$ for all $a \in D, b \in R$. Under these circumstances, suppose $a \in D$ and $b \in R$ fail to commute. Then by Lemma 4 and (iv) of Lemma 3 we have $\delta_a(b^p) = pb^{p-1}(ba - ab) = 0$, so that $b^p$ commutes with $a$, where $p$ is the prime of Lemma 3 (iv).

Since $R/D$ has characteristic $p$ and $b^s - b \in D$ for some $s > 1$, the subring of $R/D$ generated by $b + D$ is a finite field of characteristic $p$; and there exists $k \geq 1$ such that $b^{pk} - b$ belongs to $D$, hence commutes with $a$. But this result, together with the observation that $b^p$ commutes with $a$, contradicts our original assumption about $a$ and $b$; therefore, we proceed under the assumption that $D \not\subseteq Z$ and the product of any two zero divisors is zero.

Since $px, py \in D$ for all $x, y \in R$, we have $p^2xy = 0$ for all $x, y \in R$; moreover, since $A(D) = S$, we have $S = D$. By Lemma 1, $R/D$ is commutative, so that all commutators of elements in $R$ belong to $S$. Suppose now that $pR \neq 0$, and let $px \neq 0$ and $y \in R$. The ideal $pxR$ is non-trivial, so there exists $r \in R$ such that $xy - yx = pxr$; hence, $p(xy - yx) = p^2xr = 0$ and $pR \subseteq Z$. But $D = S \subseteq pR$, so we are finished in the case that $pR \neq 0$.

Assume now that $pR = D^2 = 0$ and $a \in D$ fails to commute with $b \in R$. By
Lemma 3 (ii), there exists $s > 1$ for which $b^s - b \in D$; in fact, $b^s = b$, for otherwise it follows from $D = S$ that $a = (b^s - b)r$ for some $r \in R$ and that $ab - ba = (b^s - b)rb - b(b^s - b)r = (b^s - b)(rb - br) = 0$. This observation, together with (†) and the fact that $pR = 0$, shows that the subring $R_0$ generated by $a$ and $b$ is finite; moreover, since $b^{s-1}$ is a non-zero central idempotent of a subdirectly irreducible ring $R$, it must be a multiplicative identity for $R$ and therefore for $R_0$. Thus, if there exists a subdirectly irreducible ring $R$ satisfying (†) for which $D \not\subseteq Z$, there exists a finite non-commutative ring $R_0$ satisfying (†) and has $pR_0 = 0$. Furthermore, $R_0$ is a subdirect sum of subdirectly irreducible homomorphic images, so we may assume $R_0$ is subdirectly irreducible as well. The proof of Lemma 5 will be complete once we establish the following lemma.

**Lemma 6.** Let $R$ be a finite subdirectly irreducible ring with identity; suppose that $R$ satisfies (†) and that $pR = 0$ for some prime $p$. Then $R$ is commutative.

**Proof.** If zero divisors are central (hence commutators are central), then an application of Lemma 4 shows that $x^p \in Z$ for all $x \in R$; and since $x \notin D$ implies that $x + D$ generates a finite field, $x^p - x \in D \subseteq Z$ for some $k \geq 1$ and therefore $R$ is commutative. Thus, we may assume that $D \not\subseteq Z$ and conclude from the argument of Lemma 5 that $D^2 = 0$.

Now finite rings having identity and having $D^2 = 0$ were studied by Corbas in [3]; under the hypothesis that $pR = 0$, the additive group of $R$ is a direct sum $K \oplus D$, where $K$ is a finite field and $D$ is a left vector space over $K$. Every one-dimensional subspace of $D$ is a left ideal; and since our example $R$ is a subdirectly irreducible duo ring, $D$ must be one-dimensional. Thus, the number of elements in $R$ is the square of the number in $D$; and by an earlier result of Corbas [2], there exists a finite field $K$ such that $R \cong K \times K$ with addition being componentwise and multiplication according to the rule

\[(a, b)(c, d) = (ac, ad + b\phi(c)),\]

where $\phi$ is an automorphism of $K$. Such a ring is commutative if and only if $\phi$ is the identity map, so it will be sufficient to show that a choice of $\phi$ different from the identity is not compatible with (†).

Let $K = GF(p^k)$, $t = p^k - 1$, and $\phi: x \mapsto x^r$ ($1 \leq r < k$) a non-identity automorphism of $K$. If $a, b \in K$, if $e$ is the identity element of $K$ and $n$ is an arbitrary positive integer, it follows from (2) that

\[(a, b)^n = (a^n, a^{n-1}b + a^{n-2}\phi(a)b + \ldots + (\phi(a))^{n-1}b).\]

In particular, for any $a, v \in K$, the condition that $(e, v)(a, e) = (a, e)^n(e, v)^m$ for some $n, m \geq 1$ becomes

\[(a, e + \phi(a)v) = (a^n, a^{n-1} + a^{n-2}\phi(a) + \ldots + (\phi(a))^{n-1})(e, mv) = (a^n, ma^{n-1} + a^{n-2}\phi(a) + \ldots + (\phi(a))^{n-1}).\]
Equating components and substituting for $\phi(a)$ then yields

$$(3) \quad a^n = a \quad \text{and} \quad e + a^p v = mav + a^{n-1} + a^{n-2}a^p + \ldots + a^{p(n-1)}.$$  

Now each non-zero element $a$ of $K$ satisfies the equation $x^i - e = (x - e)\,(x^{i-1} + x^{i-2} + \ldots + x + e) = 0$; substituting $a^i$ for $a$ shows that if $a^i \neq e$, then any sum of the form $a^{s_1} + a^{s_1+s_2} + \ldots + a^{s_1+(i-1)s}$ must be zero. Thus, if we choose $a$ to be a generator of the multiplicative group of $K$, $v$ an arbitrary non-zero element of $K$ and $s = p^r - 1$, then $(3)$ reduces to the condition that $|n - 1$ and $a$ satisfies the equation

$$(4) \quad a^{p^r} = ma.$$  

Clearly, $a$ cannot satisfy $(4)$ for any integer $m \equiv 0 (\mod p)$; if $m \neq 0 (\mod p)$, raising both sides of $(4)$ to the exponent $p - 1$ and applying Fermat’s theorem shows that $a$ satisfies $a^{p^r(p-1)} = a^{p-1}$ or $a^{(p^r-1)(p-1)} = e$—an impossibility since $(p^r - 1)(p - 1) < p^k - 1$. Thus, condition $(3)$ cannot be satisfied for the given choice of $a$ and $v$ and the proof of Lemma 6 is finished.

**Completion of proof of theorem.** We now need to establish commutativity for subdirectly irreducible $R$ satisfying $(\dagger)$ and having $|0| \neq D \subseteq Z$.

Assume first that $R/D$ has characteristic $0$, and suppose $a, b \in R$ do not commute. By essentially the argument used in Lemma 1, there will exist positive integers $i, j$ for which $a^ib^j = b^ja^i$; and we may assume that $i > 1$. Letting $c = b^j$ and applying Lemma 4, we get $0 = \delta(c(a^i)) = ia^{i-1}\delta(c(a))$; and since $ia^{i-1} \notin D$, $\delta(c(a)) = 0$, so that $a$ commutes with $b^j$. Applying the same argument again if $j > 1$, we get $ab = ba$—a contradiction.

Now consider $R$ with $R/D$ of characteristic $p$. For all $x \in R, px \in D$ and hence $p(xy - yx) = 0$ for all $x, y \in R$; it follows from Lemma 4 that $x^p \in Z$ for all $x \in R$. Suppose that there exist non-commuting elements $a, b \in R$ and let $ab = b^na^m$. If either $n$ or $m$ is $1$, say $n = 1$, let $[a] = a + D$ and $[b] = b + D$ and apply the commutativity of $R = R/D$ to get $[a]^m = [a]$; as before, $[a]$ will generate a finite subfield of $R$, and it follows that $a^{p^k} - a \in D \subseteq Z$ for some $k \geq 1$—a result which is incompatible with non-commutativity of $a$ and $b$.

We now proceed on the assumption that $a$ and $b$ do not commute and $ab = b^na^m$ with $n, m > 1$. Again operating in the factor ring $R = R/D$, we get $[a]^{m-1}[b]^{n-1} = [e]$, where $[e] = e + D$ is the identity of $R/D$. Since $e^p \in Z$ and $e^p - e \in D \subseteq Z$, we see that $e \in Z$, so that $a^{m-1}b^{n-1} \in Z$ and $a^{m-1}$ commutes with $b$. Applying Lemma 4 again shows that $p$ divides $m - 1$ and, of course, $n - 1$ as well. It follows (since $a^p, b^p \in Z$) that $ab = bab^{w}a^{ba}$ for some $g, h \geq 1$; and since the same arguments yield $ba = aba^{w}b^{bp}$, for $v, w \geq 1$, we get $ab = aba^{w}b^{bp}$ for some $j, k \geq 1$. Consequently $a^{bp}b^{bp}$ is a non-zero central idempotent, necessarily a multiplicative identity for $R$; hence $a$ and $b$ are invertible and there are positive integers $J = jp$ and $K = kp$ such that $a^J = b^{-K}$. Applying the same argument to $a$ and $b^{-1}$ yields positive integers $S, T$ such that $a^S = b^T$; and it follows that $a^{JS} = b^{-Ks} = b^{JT}$, so that $b^S = b$ for
some $N > 1$. Once again, we can conclude that $b^{pk} - b \in D \subseteq Z$ for some $k \geq 1$, thereby contradicting the assumption that $ab \neq ba$. The proof of the theorem is now complete.

References

3. ——— Finite rings in which the product of any two zero divisors is zero, Arch. Math. 21 (1970), 466–469.

Brock University,
St. Catharines, Ontario