Canad. Math. Bull. Vol. **22** (4), 1979

A COMMUTATIVITY THEOREM FOR RINGS AND GROUPS

BY
W. K. NICHOLSON[1] AND ADIL YAQUB

ABSTRACT. The following theorem is proved: Suppose R is a ring with identity which satisfies the identities $x^k y^k = y^k x^k$ and $x^\ell y^\ell = y^\ell x^\ell$, where k and ℓ are positive relatively prime integers. Then R is commutative. This theorem also holds for a group G. Furthermore, examples are given which show that neither R nor G need be commutative if either of the above identities is dropped. The proof of the commutativity of R uses the fact that G is commutative, where G is taken to be the group R^* of units in R.

1. **Groups.** Throughout this section, G will denote a multiplicative group and, for x, y in G, we write

$$[x, y] = xyx^{-1}y^{-1}$$

to denote the commutator of x and y. The commutator subgroup and center of a group G will be denoted by G' and Z respectively. In preparation for the proof of the main theorem, we first note the following easily verified facts.

LEMMA 1. *Let x and y be elements of a group G. If $[x, y]$ commutes with x then*

$$[x^n, y] = [x, y]^n$$

holds for all positive integers n.

LEMMA 2. *If G is a group and $G = AB$ where A and B are normal, abelian subgroups, then $G' \subseteq A \cap B \subseteq Z$.*

The commutativity theorem for groups is the following:

THEOREM 1. *Let G be a group such that, for all x, y in G*

$$x^k y^k = y^k x^k \quad \textit{and} \quad x^\ell y^\ell = y^\ell x^\ell,$$

where k and ℓ are fixed non-zero relatively prime integers. Then G is abelian.

Proof. Given an integer m, let A_m denote the (normal) subgroup of G generated by $\{x^m \mid x \in G\}$. Our hypotheses imply that both A_k and A_ℓ are

Received by the editors September 16, 1978.
AMS 1970 *Subject classification.* Primary 16A70, 20F10; Secondary 16A38.
[1] The research of this author was partially supported by NRC Grant A8075

abelian. Moreover the fact that k and ℓ are relatively prime shows that $G = A_k A_\ell$. Thus $G' \subseteq Z$ by Lemma 2. Combining this with Lemma 1, we have that

$$1 = [x^k, y^k] = [x, y^k]^k = [x, y]^{k^2}$$

for all x, y in G. Similarly $[x, y]^{\ell^2} = 1$. Since k^2 and ℓ^2 are relatively prime, this implies $[x, y] = 1$, so G is abelian as required.

We remark that the result fails if one of the hypotheses is dropped as any non-abelian group of finite exponent shows.

2. **Rings.** Throughout this section, R will denote an associative ring with identity 1 and, for x, y in R, we now write

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

to denote the (additive) commutator of x and y. The following known result [1; p. 221] is the ring-theoretic analogue of Lemma 1.

LEMMA 3. *If x, y are elements in a ring R such that $[x, y]$ commutes with x, then*

$$[x^n, y] = nx^{n-1}[x, y]$$

holds for all positive integers n.

There is no analogue in a general ring of the technique of cancelling elements in a group. However, the following lemma allows enough cancellation for our purposes.

LEMMA 4. *Let R be a ring and let $f: R \to R$ be a function such that $f(x+1) = f(x)$ holds for all $x \in R$. If for some positive integer n, $x^n f(x) = 0$ for all $x \in R$, then necessarily $f(x) = 0$ for all x.*

Proof. Clearly $(x+1)^n f(x) = 0$ for all x so, multiplying on the left by x^{n-1} and expanding by the binomial theorem yields

$$\sum_{k=0}^{n} \binom{n}{k} x^{k+n-1} f(x) = 0.$$

Since $x^n f(x) = 0$ the sum reduces to $x^{n-1} f(x) = 0$. The process continues until $xf(x) = 0$ whence $f(x) = (x+1)f(x) = 0$.

In our application of this lemma, $f(x)$ will usually be of the form $f(x) = [x, y]z$ where y and z do not depend upon x.

We shall now prove the following ring-theoretic version of Theorem 1.

THEOREM 2. *Let R be an associative ring with identity* 1, *and suppose that for all x, y in R,*

$$x^k y^k = y^k x^k, \quad \text{and} \quad x^\ell y^\ell = y^\ell x^\ell,$$

where k and ℓ are fixed relatively prime positive integers. Then R is commutative.

Proof. The argument will be broken into a series of partial results. Throughout the proof, J, Z, R^* will denote respectively the Jacobson radical, the center, and the group of units of R.

Claim 1. *R^* is abelian and R/J is commutative.*

Proof. By Theorem 1, R^* is abelian. Observe that the hypotheses are inherited by subrings and by homomorphic images of R. Also, note that no $n\times n$ complete matrix ring over a division ring can satisfy our hypotheses if $n>1$, since these imply that all the idempotents are in the center. It follows from Jacobson's Density Theorem [1; p. 33] that a primitive ring which satisfies the hypotheses of Theorem 2 must be a division ring and hence is commutative, by Theorem 1. Since R/J is a subdirect sum of primitive rings, Claim 1 follows.

Claim 2. *J is a commutative ring and $J^2 \subseteq Z$.*

Proof. Suppose $a\in J$, $b\in J$. Then $1+a$ and $1+b$ are units in R, and hence commute, by Claim 1. Thus $ab=ba$ and J is commutative. Now, let $y\in R$. Then, for all a, b in J,

$$(ab)y = a(by) = (by)a = b(ya) = (ya)b = y(ab).$$

Hence $J^2\subseteq Z$, and Claim 2 is proved.

Now, since k and ℓ are relatively prime, assume $rk - s\ell = 1$ where r and s are positive integers. If $n = s\ell$ then $rk = n+1$ and we have

$$x^n y^n = y^n x^n, \quad x^{n+1}y^{n+1} = y^{n+1}x^{n+1}$$

for all x, y in R. We may assume $n>1$.

Claim 3. $n[a, y^n] = 0 = (n+1)[a, y^{n+1}]$ *for all $a\in J$, $y\in R$.*

Proof. $[a, y^n]\in J$ by Claim 1 and so commutes with $u=1+a$ by Claim 2. Hence $nu^{n-1}[u, y^n]=[u^n, y^n]=0$ by Lemma 3 and so $0=n[1+a, y^n]= n[a, y^n]$. The same argument works for $n+1$ so Claim 3 is established.

Claim 4. $[a, y^{n+1}]=0$ *for all $a\in J$, $y\in R$.*

Proof. Since $J^2\subseteq Z$ by Claim 2, the only terms in the expansion of $(y+a)^{n+1}$ which do not commute with y^{n+1} are those involving a exactly once. Hence

$$(*) \qquad 0 = [(y+a)^{n+1}, y^{n+1}] = [y^n a + y^{n-1}ay + \cdots + yay^{n-1} + ay^n, y^{n+1}].$$

Now $nay^n = ny^na$ by Claim 3 and hence

$$n(y^na + y^{n-1}ay + \cdots + ay^n)y^{n+1} = n(y^{2n}ay + \cdots + y^{n+1}ay^n) + nay^{2n+1},$$
$$ny^{n+1}(y^na + y^{n-1}ay + \cdots + ay^n) = ny^{2n+1}a + n(y^{2n}ay + \cdots + y^{n+1}ay^n).$$

Since these are equal by $(*)$ we obtain (using $n[a, y^n] = 0$)

$$0 = n(ay^{2n+1} - y^{2n+1}a) = ny^{2n}[a, y].$$

Hence $n[a, y] = 0$ by Lemma 4. But $(n+1)[a, y^{n+1}] = 0$ by Claim 3 so

$$0 = n[a, y^{n+1}] + [a, y^{n+1}] = [a, y^{n+1}].$$

This proves Claim 4.

Claim 5. $J \subseteq Z$.

Proof. As in the proof of Claim 4 we obtain, for $a \in J$, $y \in R$:

$$(**) \qquad 0 = [(y+a)^n, y^n] = [y^{n-1}a + y^{n-2}ay + \cdots + yay^{n-2} + ay^{n-1}, y^n].$$

We have $ay^{n+1} = y^{n+1}a$ by Claim 4 so

$$(y^{n-1}a + y^{n-2}ay + \cdots + yay^{n-2} + ay^{n-1})y^n$$
$$= y^{n-1}ay^n + (y^{2n-1}a + y^{2n-2}ay + \cdots + y^{n+1}ay^{n-2})$$
$$y^n(y^{n-1}a + y^{n-2}ay + \cdots + yay^{n-2} + ay^{n-1})$$
$$= (y^{2n-1}a + y^{2n-2}ay + \cdots + y^{n+1}ay^{n-2}) + y^nay^{n-1}.$$

Since these expressions are equal by $(**)$, it follows that $y^{n-1}ay^n = y^nay^{n-1}$. Multiply by y on left and right and use Claim 4 to obtain $y^{2n+1}a = ay^{2n+1}$. On the other hand, a commutes with y^{2n+2}, again by Claim 4. Combining these facts we obtain

$$0 = ay^{2n+2} - y^{2n+2}a = y^{2n+1}[a, y]$$

for all $y \in R$, $a \in J$. Hence $[a, y] = 0$ by Lemma 4 and it follows that $J \subseteq Z$. This proves Claim 5.

We can now complete the proof of Theorem 2. Choose x, y in R. Since all commutators lie in Z by Claims 1 and 5, we have $0 = [x^n, y^n] = nx^{n-1}[x, y^n]$ by Lemma 3. Thus $n[x, y^n] = 0$ by Lemma 4, and so $0 = n^2y^{n-1}[x, y]$, again by Lemma 3. A final application of Lemma 4 yields $n^2[x, y] = 0$. Similarly $(n+1)^2[x, y] = 0$, so $[x, y] = 0$.

Example. Given an integer $k > 1$, choose any prime p dividing k. Let R_k denote the ring of all 3×3 upper-triangular matrices over $GF(p)$ with equal entries on the main diagonal. Then R_k is non-commutative but $x^ky^k = y^kx^k$ holds for all x, y in R_k. Thus Theorem 2 is not true if one of the hypotheses is dropped.

Reference

1. N. Jacobson, *Structure of rings*, A.M.S. Colloq. Publ., **37** (1964).

Department of Mathematics
The University of Calgary
Calgary, Alberta T2N 1N4
and
Department of Mathematics
University of California
Santa Barbara, Califorina 93106

https://doi.org/10.4153/CMB-1979-055-9 Published online by Cambridge University Press