THE COMMUTATIVITY OF A SPECIAL CLASS OF RINGS

WALLACE S. MARTINDALE, III

A well-known theorem of Jacobson **(1)** states that if every element x of a ring R satisfies $x^{n(x)} = x$ where $n(x) > 1$ is an integer, then R is commutative. A series of generalizations of this theorem have been proved by Herstein **(2; 3; 4; 5; 6)**, his last result in this direction **(6)** being that a ring R is commutative provided every commutator u of R satisfies $u^{(n)u} = u$. We now define a γ-ring to be a ring R in which $u^{n(u)} - u$ is central for every commutator u of R (where $n(u) > 1$ is an integer). In the present paper we verify the following conjecture of Herstein: every commutator of a γ-ring is central.

1. Semi-simple γ-rings.

The main step in our paper consists in proving

THEOREM 1. *Every division γ-ring D is a field.*

Proof. We will show that every commutator $u \in D$ satisfies $u^{m(u)} = u$ where $m(u) > 1$ is an integer. It will then follow immediately from Herstein's theorem in **(6)** that D is a field.

Suppose there exists a commutator $u = xy - yx$ which does not lie in the centre Z. Let C be the prime field of D, where either $C = R$ if the characteristic is zero or $C = P$ in the case of characteristic $p > 0$. We denote by $K = C(u)$ the subfield of D generated by C and u and let $k = K \cap Z$. We remark that k is a proper subfield of K containing C, since $u \notin k$. For all $\lambda \in k$ $\lambda u = \lambda(xy - yx) = (\lambda x)y - y(\lambda x)$ is a commutator of D lying in K. We make the important observation that $(\lambda u)^{n(\lambda)} - (\lambda u) \in k$ for all $\lambda \in k$, where $n(\lambda) > 1$ is an integer. Indeed, $(\lambda u)^{n(\lambda)} - (\lambda u) \in Z$ because D is a γ-ring, and $(\lambda u)^{n(\lambda)} - (\lambda u) \in K$ since both λ and $u \in K$.

Only three possibilities may now arise, namely,

(1) u is transcendental over C

(2) u is algebraic over R

(3) u is algebraic over P.

In (1) we know by Luroth's Theorem that k is a simple transcendental extension $C(t)$ of C. Our immediate objective is to rule out possibilities (1) and (2). In order to do so we shall require the assistance of two lemmas.

Received February 8, 1959. The material in this paper is a portion of a dissertation submitted to the University of Pennsylvania under the guidance of Dr. I. N. Herstein. The work on the paper was done at Yale University while the author was a research assistant to Dr Herstein under a National Science Foundation grant (NSF-2270).

LEMMA 1. *If* $\{\lambda_i\}$ *is an infinite sequence of distinct non-zero elements of* k, *then* $n(\lambda_i) \to \infty$, *where* $(\lambda_i u)^{n(\lambda_i)} - (\lambda_i u) \in k$, $i = 0, 1, 2. \ldots$

Proof. If the statement were not true, there would exist an infinite subsequence $\{\lambda_j'\}$ with the property that $n(\lambda_j') = n$, a constant. Setting $\lambda_j'' = \lambda_j' (\lambda_0')^{-1}$, we can write our basic equations in the form

(a) $(\lambda_j''\lambda_0'u)^n - (\lambda_j''\lambda_0'u) = (\lambda_j'u)^n - (\lambda_j'u) \in k$, $j = 0, 1, 2 \ldots$. Multiplication of the equation $(\lambda_0'u)^n - (\lambda_0'u) \in k$ by $(\lambda_j'')^n$ gives us

(b) $(\lambda_j'')^n(\lambda_0'u)^n - (\lambda_j'')^n(\lambda_0'u) \in k$, $j = 0, 1, 2 \ldots$. Subtraction of (a) from (b) yields

(c) $[(\lambda_j'')^n - \lambda_j''](\lambda_0'u) \in k$, $j = 0, 1, 2 \ldots$.

$\lambda_0'u \notin k$ because $u \notin k$ and $\lambda_0' \neq 0$; it then follows from (c) that $(\lambda_j'')^n - (\lambda_j'') = 0$, $j = 0, 1, 2 \ldots$. A contradiction results since we now have an infinite number of distinct elements of the field k satisfying the same equation $\mu^n - \mu = 0$.

LEMMA 2. *In* (1) *and* (2) *suppose that* V *is non-trivial discrete non-Archimedean valuation of* k *and* W *an extension of* V *to* K. *Then* $\bar{k} = \bar{K}$, *where* $\bar{k}$ *and* $\bar{K}$ *are the completions of* k *and* K *relative to* V *and* W, *respectively.*

Proof. We begin by choosing a Cauchy sequence $\{\lambda_i\}$ of non-zero distinct elements of k converging to a non-zero element $\bar{\lambda} \in \bar{k}$, where for all i $V(\lambda_i) \geqslant 1 + |W(u)|\, i$. For each λ_i of the sequence we pick an $n(\lambda_i) > 1$ such that

$$(\lambda_i u)^{n(\lambda_i)} - (\lambda_i u) = \gamma_i \in k, \quad i = 0, 1, 2 \ldots.$$

$n(\lambda_i) \to \infty$ by Lemma 1. The relationship

$$W[(\lambda_i u)^{n(\lambda_i)}] = n(\lambda_i)[V(\lambda_i) + W(u)] \geqslant n(\lambda_i)$$

then shows that the element $(\lambda_i u)^{n(\lambda_i)}$ converges to 0 in $\bar{K}$. $\lambda_i u$ converges to $\bar{\lambda}u$, $\bar{\lambda} \neq 0$. It follows that $\{\gamma_i\}$ is a Cauchy sequence in k and thus must converge to an element $\bar{\gamma} \in \bar{k}$. We have now analysed all the terms of the equations

$$(\lambda_i u)^{n(\lambda_i)} - \lambda_i u = \gamma_i, \qquad i = 0, 1, 2 \ldots$$

and, letting $i \to \infty$, we can conclude that $\bar{\lambda}u = \bar{\gamma}$, $\bar{\lambda} \neq 0$. Hence $u \in \bar{k}$ and $\bar{k} = \bar{K}$.

We are now in a position to rule out the possibilities (1) and (2). K is a finite separable extension of k since its generator u satisfies the separable polynomial $\mu^{n(1)} - \mu \in k$. In (1) we take as our set of valuations of k all those which act trivially on the prime field C, and in (2) we consider all those which reduce to *p-adic* valuations of R. We shall denote the ring of integers of k by o and the discriminant ideal of o by d. We let $G(V)$ stand for the value group of a valuation V of k. If B is a subgroup of a group A then the index of B in A will be symbolized by $(A : B)$.

Lemma 2 tells us that no valuation V of k can ramify in K. Indeed, $\bar{K} = \bar{k}$

implies that $G(\bar{W}) = G(\bar{V})$, where $\bar{V}$ and $\bar{W}$ are the valuations of the completions $\bar{k}$ and $\bar{K}$ relative to V and any extension W. It follows then that the ramification number $e = (G(W) : G(V)) = (G(\bar{W}) : G(\bar{V})) = 1$. To say that no valuation V ramifies means that no prime ideal of o divides the discriminant ideal d. Since any proper non-zero ideal of o is a product of prime ideals we must assume that $d = o$. But this forces $K = k$, a contradiction. We must therefore conclude that the possibility (3) does occur, in which case $u^{m(u)} = u$ for suitable $m(u) > 1$, since $P(u)$ is a finite field. (What we have actually done in ruling out the possibilities (1) and (2) has been to prove a slight generalization of a theorem of Krasner **(7)**. The proof appearing in his paper could also have been used here, but the argument we have given is of a less complicated nature.)

So far in the proof of Theorem 1 we have shown that if u is any commutator of D then either $u \in Z$ or $u^{m(u)} = u$. Suppose that $u = xy - yx \neq 0 \in Z$. The commutator

$$x = (xu)u^{-1} = [x(xy) - (xy)x]u^{-1} = (xu^{-1})(xy) - (xy)(xu^{-1})$$

does not lie in Z. Also the commutator $ux \notin Z$, since

$$(ux)y - y(ux) = u(xy - yx) = u^2 \neq 0.$$

It follows that $x^{n+1} = x$, that is, $x^n = 1$, and $(ux)^{m+1} = u^{m+1}x^{m+1} = ux$, that is, $u^m x^m = 1$, for suitable $m, n > 0$. Therefore

$$1 = (u^m x^m)^n = u^{mn} x^{nm} = u^{mn}, \text{ that is, } u^{mn+1} = u.$$

We thus conclude that for all commutators u of D $u^{m(u)} = u$ where $m(u) > 1$ is an integer. This completes the proof of Theorem 1.

At this point we remark that subrings and homomorphic images of γ-rings are themselves γ-rings. Using the Jacobson structure theory, we know that every primitive γ-ring is either a division ring or else contains a subring which has as a homomorphic image the set D_2 of all two by two matrices over some division ring D. Since D_2 is clearly not a γ-ring, we have by Theorem 1:

LEMMA 3. *Every primitive γ-ring is a field.*

The following easy lemma is useful in simplifying our problem:

LEMMA 4. *Suppose a ring R is a subdirect sum of rings R_α, each satisfying the polynomial identity $f(\mu_1, \mu_2, \ldots, \mu_m) = 0$ with integer coefficients. Then R also satisfies this identity.*

THEOREM 2. *Every semi-simple γ-ring R is commutative.*

Proof. R is isomorphic to a subdirect sum of primitive rings R_α, each of which is a γ-ring and hence commutative by Lemma 3. Then R is commutative, from Lemma 4, if we choose as our polynomial $f(\mu_1, \mu_2) = \mu_1\mu_2 - \mu_2\mu_1$.

COROLLARY. *If R is any γ-ring, then every commutator of R lies in the radical N.*

https://doi.org/10.4153/CJM-1960-021-5 Published online by Cambridge University Press

2. The general solution. Theorem 2 enables us to assume without loss of generality that the (Jacobson) radical N of our γ-ring is non-trivial. Furthermore, R may be taken to be subdirectly irreducible. Indeed, assuming for the moment that all commutators of subdirectly irreducible γ-rings are central, any γ-ring R is a subdirect sum of subdirectly irreducible γ-rings R_α, each of which satisfies the polynomial identity

$$(\mu_1\mu_2 - \mu_2\mu_1)\mu_3 - \mu_3(\mu_1\mu_2 - \mu_2\mu_1) = 0.$$

Then by Lemma 4 R satisfies this same identity, which is precisely the property we wish R to have.

Therefore from now on R will be a γ-ring with radical $N \neq 0$, centre Z, and unique minimal two-sided ideal $S \neq 0$.

LEMMA 5. $S^2 = 0$.*

Proof. $S \subset N$ since $N \neq 0$. Let $s \in S$ and $x \in R$. $(sx - xs)^n - (sx - xs) \in S \cap Z$ for some $n = n(s, x) > 1$. If $(sx - xs)^n - (sx - xs) = 0$, then $(sx - xs) = 0$, since $sx - xs \in N$ and no non-zero radical element can be a radical multiple of itself. If

$$u = (sx - xs)^n - (sx - xs) \neq 0,$$

we consider the two-sided ideal $T = uS \subset S$. T must be trivial, for otherwise $T = S$, and $uv = u$ for some $v \in S$ forces a contradiction. Thus

$$ut = [(sx - xs)^{n-1}][(sx - xs)]t - (sx - xs)t = 0$$

for all $t \in S$, from which we get $(sx - xs)t = 0$, since $(sx - xs)t$ is a radical multiple of itself. So far then in our proof we have shown that $(sx - xs)t = 0$ for all $s, t \in S$ and all $x \in R$.

Again let $s \neq 0 \in S$. The right ideal sS is two-sided because

$$(xs)t = (xs - sx)t + s(xt) = s(xt) \in sS$$

for all $t \in S$ and $x \in R$. sS is trivial, for if $sS \neq 0$, then, since it is a two-sided ideal, $sS = S$, and we are faced with the familiar contradiction that $st = s$ for some $t \in S \subset N$. Since the choice of s was arbitrary, $S^2 = 0$.

The next lemma is actually valid for any γ-ring.

LEMMA 6. *Let $x, y \in R$. Then $(xy - yx)^n c_n - (xy - yx) \in Z$, $n = 1, 2, \ldots$, where the c_n are suitable polynomials in $xy - yx$.*

Proof. We set $w = xy - yx$ and proceed with a proof by induction on n. For $n = 1$ we set $m = n(w)$ and choose $c_1 = w^{m-1}$. We now assume the lemma true for $k = n - 1$ and prove it for $k = n$. Indeed, $w^{n-1}c_{n-1} - w \in Z$ by assumption, where c_{n-1} is a polynomial in w. We may as well suppose that m is odd, since a similar argument will prevail in case m is even. Then

$$(w^{n-1}c_{n-1} - w)^m = w^n c_n - w^m \in Z,$$

*The proofs of this lemma and the succeeding ones are patterned after those given by Herstein in his papers **(2; 4; 5)**.

with c_n clearly a polynomial in w. Combining this result with the fundamental condition $w^m - w \in Z$, we finally achieve

$$w^n c_n - w = (w^n c_n - w^m) + (w^m - w) \in Z.$$

By choosing a sufficiently large n according to Lemma 6 we are able to state a useful

COROLLARY. *If $xy - yx$ is nilpotent for some $x, y \in R$, then $xy - yx \in Z$.*

LEMMA 7. *Every commutator of R is nilpotent.*

Proof. Suppose there exists a commutator $w = xy - yx$ which is not nilpotent. Consider the collection of all ideals of R which enjoy the property that all powers of w fall outside the ideal. The zero ideal is clearly a member of this collection. Partially ordering the collection by set inclusion, we are able to choose by Zorn's Lemma an ideal U which is maximal with respect to the property that $w^n \notin U$ for $n = 1, 2, 3 \ldots$. So if V contains U properly, where V is an ideal of R, then $w^{n(V)} \in V$. In other words, for any non-zero ideal $\bar{V}$ of $\bar{R} = R/U$ there exists a natural number m, depending on V, such that $\bar{w}^m \in \bar{V}$, where $\bar{w}$ denotes the coset $w + U$.

First of all, $\bar{R}$ cannot be subdirectly irreducible. Indeed, suppose that its minimal ideal $\bar{T} \neq 0$. By the corollary to Theorem 2 $w \in N$, which means that $\bar{w}$ is a non-zero element in the radical $\bar{M}$ of $\bar{R}$. Since $\bar{M} \neq 0$, Lemma 5 yields $\bar{T}^2 = 0$. A contradiction is quickly reached when we pick the m such that $\bar{w}^m \in \bar{T}$ and see that $\bar{w}^{2m} = 0$ or $w^{2m} \in U$. Hence we must assume that $\bar{T} = 0$.

Now let $\bar{V}$ be any non-zero ideal of $\bar{R}$. $\bar{w}^m \in \bar{V}$ for sufficiently large m. By Lemma 6 $\bar{w}^m \bar{c}_m - \bar{w}$ is in the centre $\bar{Y}$ of $\bar{R}$, where $\bar{c}_m$ is a polynomial in $\bar{w}$. Noting that $\bar{w}^m \bar{c}_m \in \bar{V}$, we see that

$$(\bar{w}^m \bar{c}_m)\bar{r} - \bar{r}(\bar{w}^m \bar{c}_m) = \bar{w}\bar{r} - \bar{r}\bar{w} \in \bar{V}$$

for all $\bar{r} \in \bar{R}$. It follows that for all $\bar{r} \in \bar{R}$ $\bar{w}\bar{r} - \bar{r}\bar{w} = 0$ since the intersection of all the ideals of $\bar{R}$ is 0. In other words, $\bar{w} \in \bar{Y}$.

$\bar{w}\bar{x} = \bar{x}\bar{y}\bar{x} - \bar{y}\bar{x}\bar{x}$ is also a commutator of $\bar{R}$. As we have just shown that $\bar{w} \in \bar{Y}$, $(\bar{w}\bar{x})^k = \bar{w}^k \bar{x}^k$ for all natural numbers k. Thus for any non-zero ideal $\bar{V}$ of $\bar{R}$ a sufficiently high power of $\bar{w}\bar{x}$ lies in V. Using exactly the same argument as in the proof that $\bar{w} \in \bar{Y}$ but replacing $\bar{w}$ by $\bar{w}\bar{x}$, we can conclude that $\bar{w}\bar{x} \in \bar{Y}$.

Because $\bar{w}$ and $\bar{w}\bar{x}$ are both in $\bar{Y}$, $\bar{w}^2 = \bar{w}(\bar{x}\bar{y} - \bar{y}\bar{x}) = (\bar{w}\bar{x})\bar{y} - \bar{y}(\bar{w}\bar{x}) = 0$, or $w^2 \in U$, a contradiction.

Lemma 7 and the corollary to Lemma 6, together with the remarks made in the opening paragraph of this section yield the

MAIN THEOREM. *If R is a γ-ring, then every commutator of R lies in the centre of R.*

We cannot in general hope to arrive at the sharper conclusion that any γ-ring is commutative. Indeed, the set of all three by three properly triangular matrices over any field is an example of a non-commutative γ-ring.

References

1. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. Math., *46* (1945), 695–707.

2. I. N. Herstein, *A generalization of a theorem of Jacobson*, Amer. J. Math., *73* (1951), 756–762.

3. ——— *A generalization of a theorem of Jacobson II*, Abstract, Bull. Amer. Math. Soc., *58* (1952), 383.

4. ——— *A generalization of a theorem of Jacobson III*, Amer. J. Math., *75* (1953), 105–111.

5. ——— *The structure of a certain class of rings*, Amer. J. Math., *75* (1953), 864–871.

6. ——— *A condition for the commutativity of rings*, Can. J. Math., *9* (1957), 583–586.

7. M. Krasner, *The non-existence of certain extensions*, Amer. J. Math., *75* (1953), 112–116.

8. O. F. G. Schilling, *The theory of valuations*, Math. Surveys IV (New York, 1950).

9. H. Weyl, *Algebraic theory of numbers* (Princeton, 1940).

University of Pennsylvania
Yale University