PACIFIC JOURNAL OF MATHEMATICS
Vol. 44, No. 1, 1973

A GENERALIZATION OF A THEOREM OF JACOBSON II

SUSAN MONTGOMERY

According to a well-known theorem of Jacobson, a ring R in which $x^{n(x)} = x$ ($n(x)$ an integer > 1) for each x in R must be commutative. This paper completes the description of rings with involution in which the above condition is imposed only on the symmetric elements. It is shown that in any such ring, the Jacobson radical $J(R)$ is nilpotent of index 3, and $R/J(R)$ is a subdirect sum of fields and 2×2 matrix rings. This had been shown previously under the assumption that R was an algebra over a field of characteristic not 2. In addition, it is shown that such a ring of characteristic 2 must actually be commutative. These results are best possible, since if R is 2 torsion free, R need not be commutative unless R is a division ring. Finally, using these methods, a conjecture of Jacobson on restricted Lie algebras is confirmed in a special case.

Denote the involution on R by *, and let $S = \{x \in R \mid x^* = x\}$ denote the symmetric elements. We also define

(1) $V = \{x + x^* \mid x \in R\}$, the "traces" in R and

(2) $N = \{xx^* \mid x \in R\}$, the "norms" in R.

Whereas in the characteristic not 2 situation the proofs depended on the Jordan structure of R, in the characteristic 2 case we use the Lie structure of R. Thus, consider R as a Lie ring with the product $[x, y] = xy - yx$. A Lie subring of R is an additive subgroup of R closed under $[\ ,\ ]$.

The center of R will be denoted by Z.

We first examine the situation in characteristic 2. Since the condition on elements of S may not be preserved in a homomorphic image, it will be necessary to work with Lie subrings of S.

LEMMA 1. *Let R be a ring in which $2x = 0$, all $x \in R$, and let T be an additive subgroup of R such that $s \in T$ implies $s^n \in T$, all n. Assume that $s^{n(s)} = s$ for all $s \in T$. Then $n(s)$ can be chosen to be a power of* 2.

Proof. Let $s \in T$, and let n be the smallest integer > 1 such that $s^n = s$. We claim that n is even. If not, $n = 1 + 2l$, some l. Then $s^{1+2l} = s$, so $s^{2(l+1)} = s^2$. But then $(s^{l+1} + s)^2 = 0$, which implies $s^{l+1} = s$, since $s^{l+1} + s \in T$ and no nonzero element of T can be nilpotent. By the choice of n, $l + 1 \geqq n = 1 + 2l$, a contradiction. Thus n is even. But then there exists t so $2^t \equiv 1 \pmod{n-1}$. It is easy to check that $s^{2^t} = s$.

LEMMA 2. *Let R be a ring with $*$ in which $2x = 0$, all $x \in R$. Let T be a Lie subring of R such that $S \supseteq T \supseteq V$ and that $s^{2n(s)} = s$, for every $s \in T$. Then*

(1) *Every symmetric idempotent is in Z*

(2) *A power of every element of T is in Z.*

If also R is a prime ring, then

(3) *Every nonzero element of T is invertible.*

Proof. Let $e = e^2$ be a symmetric idempotent. We show first that e commutes with S. If not, choose $s \in S$ with $[s, e] = r \neq 0$. Now $r = se + (se)^* \in V \subseteq T$, so $r^{2^k} = r$, for some k. But $[r, e] = [[s, e], e] = [s, e^2] = r$, and so $[r^2, e] = [r, [r, e]] = [r, r] = 0$; that is, e commutes with r^2. But since $r^{2^k} = r$, $[r, e] = 0$, a contradiction since $[r, e] = r \neq 0$.

Now let x be any element of R. Since $x + x^* \in S$, $(x + x^*)e = e(x + x^*)$. Thus $xe + ex = ex^* + x^*e \in S$, so $0 = [xe + ex, e] = xe^2 + e^2x = [x, e]$. Thus $e \in Z$.

If $t \in T$, $t^n = t$ for some n. Then $e = t^{n-1}$ is a symmetric idempotent, so (2) follows from (1).

Now if R is prime, then Z consists of nonzero-divisors. Since by part (2) a power (necessarily nonzero) of every element of T is in Z, no nonzero element of T is a zero-divisor. Since $t^{n(t)} = t$, for each $t \in T$, this implies that every nonzero element of T is invertible.

LEMMA 3. *Let R be a prime ring with $*$ of characteristic 2, and assume that $s^{n(s)} = s$, all $s \in S$. Then R is a field algebraic over $GF(2)$.*

Proof. From Lemma 1, $s^{2n(s)} = s$ for all $s \in S$ and so by Lemma 2, every nonzero element of S is invertible. This implies that R is a division ring. For if not, say $x \in R$ and x is not right invertible. Then since $xSx^* \subseteq S$ but xsx^* cannot be right invertible, we have $xSx^* = 0$. If y is any element of R, then $x(y + y^*)x^* = 0$, so $xyx^* = xy^*x^*$ and $xyx^* \in S$. Again since x is not right invertible, $xyx^* = 0$. Since R is prime, $xRx^* = 0$ implies $x = 0$. Thus any nonzero element of R is invertible.

We can now apply [1, Theorem 1] to see that R is a field algebraic over $GF(2)$.

The next lemma is crucial in all that follows.

LEMMA 4. *Let R be a prime ring with $*$ of characteristic 2 in which $v^{2n(v)} = v$, all $v \in V$. Then either*

(1) *R is a commutative domain*

(2) *R is a division ring*

(3) *$R = F_2$, the 2×2, matrices over a field.*

Proof. Assume that R is neither a commutative domain nor a division ring. Now if $V = 0$, $x = x^*$ for all $x \in R$, and so R would be commutative. But then since R is prime, R would be a domain, a contradiction. Thus we may also assume that $V \neq 0$. Since R is not a division ring, by the argument in Lemma 3 there exists $s \in S$, $s \neq 0$ such that s is not invertible. However, it follows from Lemma 2 that every nonzero element of V is invertible. Since $sVs \subseteq V$, $sVs = 0$ since every nonzero element of V is invertible. Thus R has zero-divisors since $V \neq 0$.

We claim that R is simple. If not, let $I \neq 0$ be a proper ideal and let $J = I \cap I^*$. $J \neq 0$ since R is prime, so choose $x \in J$, $x \neq 0$. Then $x^* \in J$, so $x + x^* \in J$. This implies $x + x^* = 0$, for otherwise J would contain an invertible element. Thus $x = x^*$ all $x \in J$, and so J is commutative. But this implies R is commutative, and so R is an integral domain, a contradiction.

Next we show $[V, s] = 0$. If not, there exists $v \in V$ so $vs + sv \neq 0$. Since $vs + sv \in V$, $(vs + sv)^{2^k} = vs + sv$, some k, and thus $(vs + sv)^n = 1$ where n is odd. Expanding, since $sVs = 0$, we see that

$$(vs + sv)^n = vsxvs + svysv = 1$$

where x and y are monomials in s and v. But then $s^2 = s \cdot 1 \cdot s = s(vsxvs + svysv)s = 0$. Also $[v, s]s = vs^2 + svs = 0$. Since $[v, s] = vs + sv$ is invertible, $s = 0$, a contraction. Thus $[v, s] = 0$.

Now if $\dim_Z R > 4$, then V generatates R as a ring [7, Theorem 1] and so $s \in Z$. This is impossible since $s^2 = 0$. Thus $\dim_Z R = 4$ and $R = F_2$ since R is not a division ring.

We point out that the conclusions of Lemma 4 still hold if we only assume that the nonzero elements of V are invertible. It then follows that [5, Theorem 9, p. 3.32] can be generalized to assuming only that the traces are invertible. However, the proof is more complicated and the more general result is not needed here.

LEMMA 5. *Let R be a prime ring with $*$ of characteristic 2. Let T be a Lie subring of R such that $S \supseteq T \supseteq N \cup V$ and $t^{2^{n(t)}} = t$ for all $t \in T$. Then either*

(1) *$R = F$, a field algebraic over $GF(2)$ or*

(2) *$R = F_2$, the 2×2 matrices over such a field, with the symplectic involution. In the second case, every element in T is a scalar matrix.*

Proof. By Lemma 2, every nonzero element of T is invertible. Choose $s \in S$. Then $s^2 = ss^* \in N \subseteq T$, and so $(s^2)^n = s^2$ for some n. If $s^2 \neq 0$, then s is invertible and so $s^{2n-1} = s$. Thus if $s^2 \neq 0$ for *all*

nonzero $s \in S$, then R is a field by Lemma 3. We may therefore assume that there exists $s_0 \in S$, $s_0 \neq 0$, with $s_0^2 = 0$. Thus R is not a domain. We could now conclude by a theorem on alternative rings [5, Theorem 9, p. 3.32] that R must be F_2 with the symplectic involution. Instead, however, we show this directly by a simple computation.

Since R is not a domain, $R = F_2$ by Lemma 4. Note that * fixes every element of F. For, say $\alpha \in F$ and $\alpha \neq \alpha^*$. Then $\alpha s_0 + (\alpha s_0)^* = (\alpha + \alpha^*)s_0 \in V \subseteqq T$. Since every nonzero element of T is invertible, $(\alpha + \alpha^*)s_0 \neq 0$ is invertible, a contradiction since $s_0^2 = 0$.

Now let $e \neq 0, 1$ be an idempotent in F_2. Since $e \notin F = Z$, $e^* \neq e$ by Lemma 2, and thus $e + e^* \neq 0$. Since ee^* and e^*e are in T but not invertible, $ee^* = 0 = e^*e$. Thus $(e + e^*)^2 = e + e^*$, and so $e + e^* = 1$, by Lemma 2. That is, $e^* = 1 + e$ for every idempotent $e \neq 0, 1$ in F_2. In particular, consider the matrix units e_{ij}, $i = 1, 2$. We have $e_{11}^* = 1 + e_{11} = e_{22}$, and also $e_{22}^* = e_{11}$. Letting $e = e_{11} + e_{12}$, $e^* = 1 + e_{11} + e_{12} = e_{22} + e_{12} = e_{11}^* + e_{12}$. Also $e^* = e_{11}^* + e_{12}$; combining these statements, we have $e_{12}^* = e_{12}$. Similarly $e_{21}^* = e_{21}$. Thus * is the usual symplectic involution; that is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & b \\ c & a \end{pmatrix}.$$

This means that

$$S = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \mid a, b, c \in F \right\} \supseteqq T.$$

Now for *any* $s \in S$, s^2 is a scalar matrix, so any s which is not a scalar matrix cannot satisfy $s^{2^n} = s$, for any n. Since by hypothesis $s \in T$ implies $s^{2^{n(s)}} = s$, every element of T is a scalar matrix.

As the first application of Lemma 5, we are now able to completely describe the situation in characteristic 2.

THEOREM 1. *Let R be a ring with involution in which $2x = 0$, all $x \in R$. Assume that $s^{n(s)} = s$, all $s \in S$. Then R is commutative. In fact, R is a subdirect sum of fields algebraic over $GF(2)$.*

Proof. First note that R is semi-simple. For, let $J(R)$ be the Jacobson radical of R. Then $J(R) \cap S = 0$, since a power of every symmetric element is an idempotent. But if $x \in J(R)$, then $x^* \in J(R)$, and so $x + x^* \in J(R) \cap S = 0$. Thus $x + x^* = 0$, or $x = x^*$. But then $x \in J(R) \cap S = 0$ and so $J(R) = 0$.

Since R is semi-simple, R is semi-prime and so R is a subdirect

sum of its prime images. We will show that any prime image of R is a field. Let P be a prime ideal of R.

First consider the case when $P^* \not\subseteq P$. Then $\bar{I} = P + P^*/P$ is a nonzero ideal in $\bar{R} = R/P$. If $x \in P + P^*$, $x = a + b$, where $a \in P$, $b \in P^*$. Then $b^* \in P$. Now $b + b^* = x + (b^* - a) \equiv x \pmod{P}$; that is, every element $\bar{x} \in \bar{I}$ is the image of a symmetric element of R. Thus $\bar{x}^{n(\bar{x})} = \bar{x}$, all $\bar{x} \in \bar{I}$, and so $\bar{I}$ is commutative by Jacobson's theorem [4, p. 217]. Since $\bar{R}$ is a prime ring containing a commutative ideal, $\bar{R}$ itself is commutative, and so an integral domain. But then every nonzero element of $\bar{I}$ is invertible. Thus $\bar{I} = \bar{R}$ and $\bar{R}$ is a field.

Next consider the case when $P^* \subseteq P$. In this situation R/P has an induced involution given by $(x + P)^* = x^* + P$, for every element $\bar{x} = x + P$ of R/P. Let T denote the image in $\bar{R}$ of the symmetric elements of R. By Lemma 1, $s^{2n(s)} = s$ for all $s \in S$, and so $\bar{s}^{2n(s)} = \bar{s}$ for all $\bar{s} \in T$. It is trivial that T satisfies the other hypotheses for Lemma 5. Thus T is in the center of $\bar{R}$.

Combining this with the case $P^* \not\subseteq P$ above, it must be that $S \subseteq Z$. Choose $x, y \in R$. Then $x + x^* \in S \subseteq Z$, so $[x + x^*, y] = 0$, or $[x, y] = [x^*, y]$ all $x, y \in R$ since $2x = 0$ in R. Thus $[x, y] = [x^*, y^*] = [x, y]^*$, all $x, y \in R$ and so $[x, y] \in S \subseteq Z$; that is, every commutator is in the center. This property must be preserved in any homomorphic image of R. In particular, F_2 cannot be a homomorphic image of R (for, let $\bar{x} = e_{11}$, $\bar{y} = e_{12}$; then $[\bar{x}, \bar{y}] = \bar{y} \notin Z$). Thus by Lemma 5, R/P must also be a field when $P^* \subseteq P$.

We are now able to improve the main results of [6] by eliminating the assumption that R is an algebra over a field of characteristic not 2.

THEOREM 2. *If R is any ring with $*$ such that $s^{n(s)} = s$ for all $s \in S$, then any primitive image of R is either a field or the 2×2 matrices over a field.*

Proof. Let P be a primitive ideal of R. If $P^* \not\subseteq P$, then just as in Theorem 1, R/P is a field. We therefore assume that $P^* \subseteq P$, and so R/P has an induced involution.

First consider the case when the characteristic of R/P is not 2. Let $\bar{x}$ be a symmetric element of R/P. Then $2\bar{x} = \bar{x} + \bar{x}^* = \overline{x + x^*} \neq 0$, and so $(2\bar{x})^n = 2\bar{x}$, some $n > 1$, since $2\bar{x}$ is the image of a symmetric element of R. Thus $2(2^{n-1}\bar{x}^n - \bar{x}) = 0$, and so $2^{n-1}\bar{x}^n = \bar{x}$. Since $\bar{x} = 2\bar{y}$, where $\bar{y} = \bar{y}^*$, we must have $\bar{x}^m = \bar{x}$ as above. Since every symmetric element $\bar{x}$ of R/P satisfies $\bar{x}^{n(x)} = \bar{x}$, R/P is a field or the 2×2 matrices over a field by [6, Theorem 1].

We may thus assume that R/P has characteristic 2. Let T denote the image of the symmetric elements of R in R/P. By Lemma 1,

$\bar{s}^{2n(s)} = \bar{s}$ for all $\bar{s} \in T$. It is trivial that T satisfies the other hypotheses of Lemma 5. Thus R/P is a field or 2×2 matrices over a field.

THEOREM 3. *Let R be a ring with in which $s^{n(s)} = s$, all $s \in S$. Denote the Jacobson radical of R by $J(R)$. Then*

(1) *$x \in J(R)$ implies $x^2 = 0$, and $J(R)^3 = 0$*

(2) *$R/J(R)$ is a subdirect sum of fields and 2×2 matrix rings over fields*

(3) *R satisfies $S_4(x_1, x_2, x_3, x_4)^2$, where S_4 denotes the standard identity of degree 4.*

Proof. (2) follows immediately from Theorem 3, since $R/J(R)$ is a subdirect sum of primitive images of R.

For part (1), first observe that $S \cap J(R) = (0)$, since a power of every symmetric element is an idempotent. But then if $x \in J(R)$, $x + x^* \in J(R) \cap S = (0)$, and so $x^* = -x$. We claim that $2x = 0$ implies $x = 0$, all $x \in J(R)$. For if $2x = 0$, then $x = -x$ and so $x^* = x$. Then $x \in J(R) \cap S = (0)$. (1) now follows from the characteristic not 2 case [6, Theorem 2].

Since any 2×2 matrix ring over a field satisfies S_4, $R/J(R)$ satisfies S_4. But then $S_4(x_1, \cdots, x_4) \in J(R)$, all $x_1, \cdots, x_4 \in R$, and so $S_4(x_1, \cdots, x_4)^2 = 0$ by (2).

Before proceeding, we need the following theorem due to Herstein (unpublished). It is a strengthening of [1, Theorem 1] in characteristic 2.

THEOREM (*Herstein*). *Let D be a division ring with $*$ of characteristic 2 such that $v^{n(v)} = v$, all $v \in V$. Then D is a field.*

Proof. Choose $v \in V$ and let $C_D(v)$ denote the centralizer of v in D. We claim that $C_D(v)$ is commutative. Now $C_D(v)$ is a division ring closed under $*$. Let $s \in C_D(v) \cap S$. Then $svs \in V$ and so $(svs)^k = svs$, some k. Also $v^l = v$, some l, so if we let $n = (k-1)(l-1) + 1$, we have both $v^n = v$ and $(svs)^n = svs$. Since $sv = vs$, $s^{2n}v^n = s^2v$, and so $s^{2n-1} = s$; that is, s is periodic. By [1, Theorem 1], $C_D(v)$ is a field algebraic over $GF(2)$.

Now if $Z \cap V \neq 0$, we would be done, for if $v \in Z \cap V$, $v \neq 0$ then $C_D(v) = D$ is a field by the above. We may thus assume that $Z \cap V = 0$. Now choose $v \in V$, $v \notin Z$. Since $v^k = v$, some k, there exists $a \in D$ so $ava^{-1} = v^i \neq v$ by [2, Lemma 3.1.1]. Since conjugation by a induces an automorphism of the finite field $GF(2)(v)$, there is some n so $a^n v a^{-n} = v$. This gives $a^n \in C_D(v)$, and so a is algebraic over $GF(2)$. But now the subdivision ring generated by a and v over $GF(2)$

is finite, and so must be commutative by Wedderburn's theorem. This contradicts $ava^{-1} \neq v$. Thus it must happen that $V = 0$. This implies $D \subseteq S$, and so D is commutative.

Note that the above proof works equally well if the division ring has characteristic not 2 and V is replaced by the set of skew elements, and so gives a simpler proof of [1, Theorem 3].

Using the theorem of Herstein, we can improve Lemma 4 to the following:

LEMMA 6. *Let R be a prime ring with $*$ of characteristic 2 in which $v^{2n(v)} = v$, all $v \in V$. Then R is a commutative domain or the 2×2 matrices over a field.*

We now apply our results to a problem in Lie algebras. Jacobson has made the following conjecture [3, p. 196]:

"If $\mathscr{L}$ is a restricted Lie algebra of characteristic p such that $a^{p^{n(a)}} = a$, $n(a) > 0$ for all $a \in \mathscr{L}$, then $\mathscr{L}$ is abelian".

The following theorem confirms Jacobson's conjecture in a special case.

THEOREM 4. *Let $\mathscr{L}$ be a restricted Lie algebra of characteristic 2 such that $a^{2^{n(a)}} = a$, $n(a) > 0$ for all $a \in \mathscr{L}$. Assume that $\mathscr{L}$ has a faithful (restricted) representation φ into R_L, where R is an associative algebra with involution, such that $\varphi(\mathscr{L}) \supseteq V$, the traces of R. Then $\mathscr{L}$ is abelian.*

Proof. To simplify notation, assume that $\mathscr{L}$ is actually contained in R_L. Let $J(R)$ be the Jacobson radical of R. Then $J(R) \cap \mathscr{L} = (0)$, since a power of every element of $\mathscr{L}$ is an idempotent in R. Thus in $\bar{R} = R/J(R)$, $\mathscr{L} \cong \overline{\mathscr{L}}$, where $\overline{\mathscr{L}} = \mathscr{L} + J(R)$. We may therefore assume that R is semi-simple. Then R is a subdirect sum of its prime images, so let P be any prime ideal of R. We will show that $\overline{\mathscr{L}}$, the image of $\mathscr{L}$ in R/P, is abelian.

Now if $P^* \not\subseteq P$, then R/P is a field by exactly the same argument as in Theorem 1. Thus, assume that $P^* \subseteq P$. Let S_1 denote the symmetric elements of R/P, and let $T = \overline{\mathscr{L}} \cap S_1$. Now $T \supseteq V$, and so by Lemma 6 either R/P is a field (and we are done) or $R/P = F_2$, 2×2 matrices. To finish the Theorem, it will be enough to show that any Lie subring A of F_2 such that $a^{2^{n(a)}} = a$, all $a \in A$, is abelian.

Choose $a, b \in A$. Then $[a, b]^2 \in Z$ (This is true for *any* commutator in F_2) and so $[a, b] \in Z$ since $[a, b]^{2^k} = [a, b]$, some k. Thus $[[a, b], a] = 0 = [b, a^2]$; that is, b commutes with a^2. But $a^{2^k} = a$, some k, and thus $[b, a] = 0$. We have shown that A is abelian.

It should be pointed out that R in Theorem 4 is not necessarily commutative, as it may happen that $\varphi(\mathscr{L})$ does not contain all of S. As an example consider F_2, where F is algebraic over $GF(2)$. With the symplectic involution, $V = \{\text{all scalar matrices}\}$. If $\mathscr{L} = \{\alpha I + \beta(e_{11} + e_{12}) \mid \alpha, \beta \in F\}$, then $\mathscr{L}$ satisfies the hypotheses of Theorem 4 but $S \not\subseteq \mathscr{L}$ and $\mathscr{L} \not\supseteq S$.

Note also that the converse of Theorem 4 is trivially true. For if $\mathscr{L}$ is abelian, let R be the u-algebra for $\mathscr{L}$ [3, p. 192]. Then the identity map is an involution on R (since R is commutative), and $V = \{x + x^*\} = \{x + x\} = 0$, so $\mathscr{L} \supseteq V$.

Added in Proof. I. N. Herstein has now shown that Theorem 4 is true for any characteristic, if V is replaced by the skew elements of R.

REFERENCES

1. I. N. Herstein and S. Montgomery, *A note on division rings with involution*, Michigan Math. J., **18** (1971), 75-79.
2. I. N. Herstein, *Noncommutative Rings*, Carus Monograph no. 15. The Mathematical Association of America 1968, p. 70.
3. N. Jacobson, *Lie Algebras*, Interscience, 1962.
4. ———, *Structure of Rings*, AMS Colloquium Publ. No. 37, 1964.
5. ———, *Lectures on Quadratic Jordan Algebras*, Tata Institute of Fundamental Research, Bombay (1969).
6. S. Montgomery, *A generalization of a theorem of Jacobson*, Proc. Amer. Math. Soc., **28** (1971), 366-370.
7. ———, *Lie structure of simple rings of characteristic* 2, J. Algebra **15** (1970), 387-407.

Received September 27, 1971 and in revised form October 29, 1971. This research was supported by NSF Grant No. GP-29119 X.

UNIVERSITY OF SOUTHERN CALIFORNIA