RINGS ADMITTING CERTAIN AUTOMORPHISMS [1])

I. N. HERSTEIN

In a paper published a few years ago [5] JACOBSON proved that a finite-dimensional Lie algebra which admits an automorphism of prime period leaving only the zero element fixed must be nilpotent. For finite groups the analagous theorem was conjectured by FROBENIUS and was proved as a corollary to a far more powerful result, in a remarkable piece of work by THOMPSON [8]. For associative rings this situation was studied by HIGMAN [4] who showed that here too the existence of such an automorphism rendered the ring nilpotent.

If an associative ring should have a unit element then this element is fixed by every automorphism of the ring. For an algebra with unit element over a given field, if by automorphism we mean an algebra automorphism, then every element of the field must remain fixed. Thus the assumption that an automorphism leave only 0 fixed, for rings and algebras, seems far too restrictive and unnatural. The appropriate analogue appears to be: what is the structure of an associative ring or algebra which admits an automorphism of prime period all of whose fixed points lie in some «natural» subset.

For finite-dimensional algebras and rings with descending chain conditions on left ideals, when this fixed-point set is properly conditioned, we obtain their structure, in section 1. In sections 2 and 3 respectively we determine the structure of general rings admitting automorphisms of periods 2 and 3 respectively all of whose fixed points lie in the center. We would conjecture that the results obtained, namely that the commutator ideal must be nil, hold in the general case of a ring admitting an automorphism of prime period all of whose fixed points lie in the center of the ring.

1) This research was carried out in Rome while the author was a Fellow of the JOHN SIMON GUGGENHEIM Memorial Foundation and with support from the National Science Foundation, Grant NSF–G19655 and the Army Research, Ordinance Division (AROD).

1. Finite-dimensional Algebras and Rings with Chain Conditions.

In this section we consider finite-dimensional algebras and rings with chain condition which admit automorphisms of any prime period all of whose fixed-points are restricted to lie in the center or in a particular part of the center. We show this forces the commutator ideal of the ring or algebra to be a nil (and so, in this particular case, nilpotent) ideal. In particular, in the presence of an additional hypothesis of semi-simplicity they just turn out to be commutative.

We begin with

Theorem 1. *Let R be a simple ring with descending chain condition on left ideals. Suppose that φ is an automorphism of R of prime period* p *such that $\varphi(x)=x$ implies that x the is in Z, the center of R. Then R is commutative (and so is a field).*

Proof. Since $\varphi^p = 1$, the identity automorphism of R, for all x in R,

$$\varphi[x+\varphi(x)+\cdots+\varphi^{p-1}(x)] = x+\varphi(x)+\cdots+\varphi^{p-1}(x).$$

In consequence, by our basic assumption on the nature of φ, for any x in R,

$$x+\varphi(x)+\cdots+\varphi^{p-1}(x)$$

must be in Z. Thus there exists a shortest expression (fewest number of non-zero coefficients)

$$\alpha_0 x+\alpha_1\varphi(x)+\cdots+\alpha_k\varphi^k(x),$$

where $k<p$ and where all the α_i's are in Z and not all of them are zero and such that:

(1) $$\alpha_0 x+\alpha_1\varphi(x)+\cdots+\alpha_k\varphi^k(x)\in Z \quad \text{for all} \quad x\in R.$$

Sinee Z is invariant under φ, by applying a suitable power of φ, we could realize a situation in which $\alpha_0\neq 0$, thus we may iudeed assume, without any loss of generality, that $\alpha_0\neq 0$.

Suppose now that R is not commutative, that is, that $R\neq Z$. Since Z is a field we must have $\alpha_i\neq 0$ for some $i\neq 0$, otherwise we would have that that $\alpha_0 x$ is in Z for all x in R from which it would follow that $x\in Z$ for all $x\in R$ contrary to the assumption that $R\neq Z$.

Given $\lambda\in Z$ then (1) holds if we replace in it x by λx. Using the fact that $\varphi^i(\lambda x)=\varphi^i(\lambda)\varphi^i(x)$ we get:

(2) $$\alpha_0\lambda x+\alpha_1\varphi(\lambda)\varphi(x)+\cdots+\alpha_k\varphi^k(\lambda)\varphi^k(x)\in Z.$$

Multiplying (1) by λ and subtracting (2) we obtain:

(3) $\alpha_1 [\lambda - \varphi(\lambda)] \varphi(x) + \cdots + \alpha_i [\lambda - \varphi^i(\lambda)] \varphi^i(x) + \cdots + \alpha_k [\lambda - \varphi^k(\lambda)] \varphi^k(x)$

is in Z for every x in R.

Putting $\alpha_j' = \alpha_j [\lambda - \varphi^j(\lambda)]$, since each of α_j, λ, $\varphi^j(\lambda)$ is in Z, α_j' must be iu Z for every j. But (3) then yields the *shorter* relation

$$\alpha_1' \varphi(x) + \cdots + \alpha_k' \varphi^k(x) \in Z$$

for all $x \in R$. The net result of all this is that each $\alpha_j' = 0$: in particular,

$$0 = \alpha_i' = \alpha_i [\lambda - \varphi^i(\lambda)].$$

Since these are all elements of the field Z and since we know that $\alpha_i \neq 0$ we end up with $\varphi^i(\lambda) = \lambda$ for every $\lambda \in Z$. However, φ is of prime period p and $0 < i < p$; this immediately yields for us $\varphi(\lambda) = \lambda$ for all $\lambda \in Z$.

We have just seen that φ is an automorphism of R leaving every center element of R fixed. As is well-known, in a simple ring with descending chain conditions, such an automorphism must be inner. That is there exists an $a \in R$ such that $\varphi(x) = a x a^{-1}$ for every x in R. Thus $\varphi(a) = a a a^{-1} = a$; by assumption this puts a in Z. But then from this we get that $\varphi(x) = a x a^{-1} = x$ for every x in R. But then $\varphi = 1$, the identity automorphism of R, contradicting that φ has prime period. Thus we must have had that $R = Z$ thereby proving the theorem.

As is so often the case, once the result is known for simple rings then we can also establish it for semi-simple ones. We do this in

Theorem 2. *Suppose that R is a semi-simple ring with descending chain condition on left ideals; suppose further that R admits an automorphism φ of prime period p all of whose fixed-points are in Z, the center of R. Then R is commutative* (*and so is a direct sum of fields*).

Proof. By WEDDERBURN's theorem,

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_k$$

where each R_i is a simple with descending chain condition. The center of R is precisely the direct sum of the centers of the R_i's.

To prove the theorem we must show that each R_i is commutative. Suppose that R_1, say, is not commutative. If $\varphi(R_1) \subset R_1$ then $\varphi(R_1)$ is, in fact, equal to R_1; in this case we can apply theorem 1 to deduce the commutativity of R_1. So. suppose that $\varphi(R_1) \not\subset R_1$. We wish to show that this, too, implies that R_1 is commutative. We claim that

$$R_1 + \varphi(R_1) + \cdots + \varphi^{p-1}(R_1)$$

is a direct sum. If this were not the case, from the simplicity of the $\varphi^i(R_1)$'s we would have that for some first $m+1<p$,

$$\varphi^{m+1}(R_1) \subset R_1 + \varphi(R_1 + \cdots + \varphi^m(R_1)$$

and since the $\varphi^j(R_1)$'s are *all* the simple ideals of this sum, where $j \leq m$, we would have that

$$\varphi^{m+1}(R_1) = \varphi^j(R_1)$$

for some $j \leq m < p$. But then $\varphi^{m+1-j}(R_1) = R_1$; since $0 < m+1-j < p$ and since φ has prime period this would imply that $\varphi(R_1) = R_1$, contrary to assumption.

Therefore we may assume that the sum $T = R_1 + \varphi(R_1) + \cdots + \varphi^{p-1}(R_1)$ is a direct sum. However, given $x \in R_1$, since

$$t = x + \varphi(x) + \cdots + \varphi^{p-1}(x)$$

is left fixed by φ, t must be in the center of R, hence certainly in the center of T. Thus each component of t in the components R_1, $\varphi(R_1)$, ..., $\varphi^{p-1}(R_1)$ of this direct sum decomposition of T must be in the center of each of these respective rings. Since these components of t are x, $\varphi(x)$, ..., $\varphi^{p-1}(x)$ we deduce that x must be in the center of R_1. Since x was arbitrary in R_1 we see this way that R_1 is commutative. We have now completed the proof of theorem 2.

We conclude the section with

Theorem 3. *Let A be a finite-dimensional algebra over a field F and suppose that A has a unit element. Suppose that A admits an automorphism φ of prime period* p *all of whose fixed-points are in F. If N denotes the radical of A then A/N is commutative.*

Proof. Since N, the radical of A, is taken onto itself by every automorphism of A, $\varphi(N) = N$; thereby φ induces an automorphism $\bar{\varphi}$ on $\bar{A} = A/N$. What are the fixed points of $\bar{\varphi}$?

Suppose that $\bar{\varphi}(\bar{x}) = \bar{x}$ for some $\bar{x}$ in $\bar{A}$ and suppose that x in A maps on $\bar{x}$ in $\bar{A}$. Thus $x - \varphi(x)$ is in N. However, the mapping $T: n \to n - \varphi(n)$ is a linear transformation on the vector space N over F which annihilates no non-zero vector in N (since $N \cap F = (0)$ and by assumption only the elements in F are annihilated by T); thus, since N is finite-dimensional over F, T maps N onto itself. Since $x - \varphi(x)$ is in N there must be an element n in N such that $nT = x - \varphi(x)$, that is, such that

$$x - \varphi(x) = n - \varphi(n).$$

From this we get that

$$\varphi(x - n) = x - n;$$

by our assumptions we then know that $x = \lambda + n$ where λ is in F so that $\bar{x} = \bar{\lambda} = \lambda$. In consequence the fixed-points of $\bar{\varphi}$ are precisely the elements of F. Since A/N is semisimple, by theorem 2 it is commutative.

2. Automorphisms of Period 2.

In this section we consider arbitrary rings which admit automorphisms of period 2 having fixed points only in their centers. To determine their structure is both simple and elementary. We do this in

Theorem 4. *Let R be a ring admitting an automorphism of period 2 all of whose fixed-points are in the center of R. Then the commutator ideal of R is a nil ideal.*

Proof. Let φ be the automorphism of R. Since $\varphi^2 = 1$, the identity automorphism of R, for any x in R, $\varphi[x + \varphi(x)] = x + \varphi(x)$, whence by our assumption on the fixed-points of φ we have

(1) $\quad x + \varphi(x) \in Z,$ the center of R, for every $x \in R$.

Given a, x in R, by (1)

$$\varphi(a) = -a + \lambda, \ \varphi(x) = -x + \mu$$

where λ, μ are both in Z. Thus:

$$\varphi(ax - xa) = \varphi(a)\varphi(x) - \varphi(x)\varphi(a) = (-a + \lambda)(-x + \mu) - (-x + \mu)(-a + \lambda) = ax - xa.$$

Since all the commutators $ax - xa$ are left fixed by φ, again using our assumption about φ we obtain

(2) $\quad ax - xa \in Z$ for all a, x in R.

In (2) we replace x by ax; this yields:

(3) $\quad a(ax - xa) \in Z$ for all $a, x \in R$.

Given any $y \in R$, we commute y with $a(ax - xa)$; making use of both (2) and (3) we obtain $ya(ax - xa) = a(ax - xa)y = ay(ax - xa)$ hence

(4) $\quad (ay - ya)(ax - xa) = 0$ for all a, x, y in R.

The result contained in (4) merely states that the product of any two commutators is 0 if they have an element in common. Now, given any element in the commutator ideal of R, in virtue of (2) it can be written as

$$c = \sum_{i=1}^{n} r_i (a_i b_i - b_i a_i)$$

where a_i, b_i are in R and r_i is either in R or is an integer. Thus if we consider c^{n+1}, making use of (2) and (4) we get $c^{n+1} = 0$. But then the commutator ideal of R is nil, as claimed in the theorem.

3. Automorphisms of Period 3.

In this section we obtain that a ring admitting an automorphism of period 3 all of whose fixed-points are in the center must have as commutator ideal a nil ideal. Strangely enough the argument is a great deal more complicated than the corresponding one for period 2. It makes use of a great number of fairly deep theorems from the theory of rings. One would hope to be able to give a purely formal proof theoreof, similar in spirit to that given in section 2. We have not been able to find such a proof; quite possibly we are overlooking something obvious; at any rate here is the proof that we did find.

In what follows we shall consistenly use the following notation: R is a ring, $Z(R)$ is its center, $J(R)$ is its Jacobson radical and $N(R)$ is its maximal nil ideal, and, finally, $C(R)$ is its commutator ideal.

Lemma 1. *Suppose that the ring R admits an automorphism φ of period 3 all of whose fixed-paints are in $Z(R)$. Then for any x in R, $x\varphi(x) - \varphi(x)x$ is in $Z(R)$.*

Proof. Since

$$\varphi^3 = 1, \quad \varphi[x + \varphi(x) + \varphi^2(x)] = x + \varphi(x) + \varphi^2(x),$$

whence

$$\lambda(x) = x + \varphi(x) + \varphi^2(x) \in Z(R)$$

for any x in R. Now

$$\begin{aligned} \varphi[x\varphi(x) - \varphi(x)x] &= \varphi(x)\varphi^2(x) - \varphi^2(x)\varphi(x) = \varphi(x)[\lambda(x) - x - \varphi(x)] \\ &- [\lambda(x) - x - \varphi(x)]\varphi(x) = x\varphi(x) - \varphi(x)x \end{aligned}$$

since $\lambda(\varphi)$ is in $Z(R)$. By the hypothesis imposed on the fixed-points of φ we deduce that

$$x\varphi(x) - \varphi(x)x \in Z(R),$$

which is the conclusion of the lemma.

The discussion will eventually involve settling two different cases, namely when the ring has characteristic 3 and when it does not. This explains the hypothesis of charactcristic 3 ia the

Lemma 2. *If R is of characteristic 3 admitting an automorphism such that $\varphi^3 = 1$ and sach that all the fixed points of φ are in $Z(R)$. Then for any x in R,*

$$x^3 \varphi(x^3) = \varphi(x^3) x^3.$$

Proof. By Lemma 1, $x\varphi(x) - \varphi(x)x \in Z(R)$ for any $x \in R$. Thus the third commutator of x and $\varphi(x)$,

$$\Big[x, \big[x, [x, \varphi(x)]\big]\Big] \equiv x^3 \varphi(x) - \varphi(x) x^3$$

since the characteristic of R is 3. However, since x^3 commutes with $\varphi(x)$ it also commutes with $\varphi(x)^3 = \varphi(x^3)$.

Lemma 2 allows us to conclude that any element in R satisfies a polynomial of degree 9 with coefficients in $Z(R)$, in fact a monic such polynomial. We see this as follows. Since x^3 commutes with $\varphi(x^3)$ and with

$$x^3 + \varphi(x^3) + \varphi^2(x^3)$$

which is in $Z(R)$, we see that x^3 also commutes with $\varphi^2(x^3)$. Thus the elementary symmetric functions in x^3, $\varphi(x^3)$ and $\varphi^2(x^3)$ are invariant under φ and so are in $Z(R)$. But then $y = x^3$ satisfies

$$y^3 - \alpha y^2 + \beta y - \gamma = 0$$

where the coefficients α, β, γ are all in $Z(R)$ and are respectively

$$\alpha = x^3 + \varphi(x^3) + \varphi^2(x^3),$$

$$\beta = x^3 \varphi(x^3) + x^3 \varphi^2(x^3) + \varphi(x^3) \varphi^2(x^3),$$

$$\gamma = x^3 \varphi(x^3) \varphi^2(x^3).$$

We have thus proved

Lemma 3. *If R is as in lemma 2 then any x in R satisfies a polynomial of the form*

$$x^9 - \alpha x^6 + \beta x^3 - \gamma = 0$$

where α, β, γ are in $Z(R)$.

If every element in a ring satisfies a polynomial with leading cooefficient 1 and of bounded degree over its center then it is wellknown that the ring satisfies a polynomial identity. In our case we could actually write this identity down as:

$$0 = \Big[\big[[x^9, y], [x^3, y]\big], \big[[x^6, y], [x^9, y]\big]\Big]$$

where the square brackets indicate (additive) commutators. We thus have the

Corollary. *If R is as in lemma 2 then it satisfies a polynomial identity.*

The condition that a ring admit an automorphism whose fixed-points lie in the center might very well be destroyed in a homomorphie image. Thus we want to impose conditions on our rings which are preserved under homomorphism and which are consequences of the existence of an automorphism of period 3 all of whose fixed points are in the center. This explains the weird hypothesis in the next few lemmas.

Lemma 4. *Let R be a primitive ring of characteristic 3 admitting an automorphism φ such that:*

1. $\varphi^3 = 1$.
2. $x + \varphi(x) + \varphi^2(x) \in Z(R)$.
3. *x^3 commutes with $\varphi(x^3)$.*
4. *all symmetric functions in x^3, $\varphi(x^3)$, $\varphi^2(x^3)$ are in $Z(R)$, for all x in R.*

Then R is commutative.

Proof. By the corollary to lemma 3 R satisfies a polynomial identity. Being primitive, by a result of KAPLANSKY [6] R is a finite-dimensional simple algebra over its center $Z(R)$, which is a field.

Since $x + \varphi(x) + \varphi^2(x) \in Z(R)$, replacing x by λx, where λ is in $Z(R)$ and playing the results off against each other we obtain that

$$[\lambda - \varphi(\lambda)]\, \varphi(x) + [\lambda - \varphi^2(\lambda)]\, \varphi^2(x) \in Z(R).$$

Replacing x by λx in this last expression and playing it off against the expression [multiplied by $\varphi(\lambda)$] we arrive at

$$[\lambda - \varphi^2(\lambda)]\ [\varphi(\lambda) - \varphi^2(\lambda)]\, \varphi^2(x) \in Z(R)$$

for all x in R. Thus if we supposed that R was not commutative we would have that $[\lambda - \varphi^2(\lambda)]\,[\varphi(\lambda) - \varphi^2(\lambda)] = 0$; since $Z(R)$ is a field we must have that either $\lambda = \varphi^2(\lambda)$ or $\varphi(\lambda) = \varphi^2(\lambda)$ which, since φ is of period 3 imply that $\lambda = \varphi(\lambda)$. Thus φ is an automorphism of R, which is a simple algebra, finite-dimensional over its center, which leaves every element of $Z(R)$ fixed. But this implies that φ is an inner automorphism of R, that is there is ah $a \in R$ such that $\varphi(x) = a x a^{-1}$ for every $x \in R$. However

$$x + a x a^{-1} + a^2 x a^{-2} = x + \varphi(x) + \varphi^2(x) \in Z(R)$$

by assumption. Replacing x by ax we obtain that:

$$a\,(x + a x a^{-1} + a^2 x a^{-2}) = a x + a\,(ax)\,a^{-1} + a^2\,(ax)\,a^{-2} \in Z(R)$$

by the above. If $x + a x a^{-1} + a^2 x a^{-2}$ were not 0 it would have an inverse in the field $Z(R)$ so that $a \in Z(R)$ would result. Suppose, on the other hand, that

$$x + a x a^{-1} + a^2 x a^{-2} = 0$$

for all x in R. Multiplying through by a^2 from the right yields

$$x a^2 + a x a + a^2 x = 0$$

for every x in R. Since the characteristic of R is 3 this says that

$$a(ax - xa) = (ax - xa)a$$

for every x in R. By a result of ours [2], since the characteristic of R is not 2, a must be in $Z(R)$. Thus in all cases a must be in $Z(R)$. But then

$$\varphi(x) = a x a^{-1} = x$$

for every x in R. Since

$$x^9 = x^3 \varphi(x^3) \varphi^2(x^3)$$

is in $Z(R)$ by hypothesis, we see that the ninth power of every element of R is in its center. By another result of KAPLANSKY [7] R must be commutative.

Corollary. *If R is a primitive ring of characteristic 3 which admits an automorphism of period 3 all of whose fixed-points are in $Z(R)$ then it is commutative.*

Proof. We show that the hypothesis of the lemma are satisfied. Since the element $x + \varphi(x) + \varphi^2(x)$ is left fixed by φ it must be in $Z(R)$ by hypothesis, so (2) is satisfied. Lemma 2 assures us that x^3 commutes with $\varphi(x^3)$, so by (2) it also commutes with $\varphi^2(x^3)$, hence (3) is satisfied. Any symmetric function in x^3, $\varphi(x^3)$, $\varphi^2(x^3)$, since these commute with each other, is left fixed by φ so by hypothesis it must be in $Z(R)$, therefore (4) holds also. By the lemma the corollary is then immediate.

Having disposed of the primitive case we can start the ascent to general rings along the lines laid out by the structure theory developed by JACOBSON. We now consider the semi-simple case in

Lemma 5. *Let R be a semi-simple ring of characteristic 3 having an automorphism φ such that:*

1. $x + \varphi(x) + \varphi^2(x) \in Z(R)$
2. *x^3 commutes with $\varphi(x^3)$*
3. *the symmetric elements in x^3, $\varphi(x^3)$, $\varphi^2(x^3)$ are all in $Z(R)$ for every x in R. Then R is commutative.*

Proof. Being semi-simple R is isomorphic to a subdirect sum of primitive rings R_i each of which is a homomorphic image of R. As in the proof of the corollary to lemma 3, R satisfies a polynomial identity so that each R_i, as a homomorphic image of R also satisfies the polynomial identity. Thus, being primitive, each R_i is actually a simple algebra finite-dimensional over its center.

Let R_1, say, be isomorphic to R/U. Since R_1 is simple, U is a *maximal* ideal of R. If $\varphi(U) \subset U$ then φ would induce an automorphism on R_1 satisfying all the conditions of lemma 4. But then R_1 would be commutative.

Suppose then that $\varphi(U) \not\subset U$. Since $\varphi(U)$ is an ideal of R and since U is a maximal ideal of R, $R = U + \varphi(U)$. Similarly $R = U + \varphi^2(U) = \varphi(U) + \varphi^2(U)$.

We claim that $U \cap \varphi(U) \not\subset \varphi^2(U)$, otherwise $\varphi[U \cap \varphi(U)] \subset \varphi^3(U) = U$. But since $\varphi[U \cap \varphi(U)]$ is certainly contained in $\varphi(U)$ we would have that

$$\varphi[U \cap \varphi(U)] \subset U \cap \varphi(U).$$

If this were so φ would induce an automorphism $\bar{\varphi}$ on

$$\bar{R} = R / [U \cap \varphi(U)].$$

However, by the Chinese remainder theorem, $R/[U \cap \varphi(U)]$ is isomorphic to

$$R/U \oplus R/\varphi(U) = R_1 \oplus \bar{\varphi}(R_1).$$

Now R_1 and $\bar{\varphi}(R_1)$ are the *only* simple ideals in this direct sum; thus $\bar{\varphi}^2(R_1)$ which is contained in it as a simple ideal must be either R_1 or $\bar{\varphi}(R_1)$, either of which implies that $R_1 = \bar{\varphi}(R_1)$ (we have made use of $\bar{\varphi}^3 = 1$) which would imply that $\varphi(U) \subset U$, contrary to assumption. Therefore we must have that

$$U \cap \varphi(U) \not\subset \varphi^2(U).$$

Again making use of the Chinese remainder theorem we get

$$\bar{R} = R/[U \cap \varphi^2(U)]$$

is isomorphic to

$$R/U \oplus R/\varphi(U) \oplus R/\varphi^2(U).$$

Since $U \cap \varphi(U) \cap \varphi^2(U)$ is invariant under φ, φ induces an automorphism $\bar{\varphi}$ on $\bar{R}$ such that $\bar{x} + \bar{\varphi}(\bar{x}) + \bar{\varphi}^2(\bar{x})$ is in $Z(\bar{R})$ for every $\bar{x}$ in $\bar{R}$. Now

$$\bar{R} = R_1 \oplus \bar{\varphi}(R_1) \oplus \bar{\varphi}^2(R_1),$$

so if $\bar{x} \in R_1$ then

$$\bar{t} = \bar{x} + \bar{\varphi}(\bar{x}) + \bar{\varphi}^2(\bar{x}) \in Z(\bar{R}).$$

But then each component of $\bar{t}$ is in the corresponding center of R_1, $\bar{\varphi}(R_1)$, $\bar{\varphi}^2(R_1)$ respectively. Thus $\bar{x} \in Z(R_1)$, whence R_1 is commutative.

Sinee each component of the subdirect sum decomposition of R has been shown to be commutative we know that R is commutative. Thus lemma 5 is proved.

We now settle the result that we seek for the special case of a ring of characteristic 3. This will provide us with the vital link needed to prove it in the completely general case.

Lemma 6. *Let R be a ring of characteristic 3 which admits an automorphism φ of order 3 all of whose fixed-points are in $Z(R)$. Then $C(R)$, the commutator ideal of R, is a nil ideal.*

Proof. By lemma 2, x^3 commutes with $\varphi(x^3)$, from which it follows that all the symmetric functions in x^3, $\varphi(x^3)$, $\varphi^2(x^3)$ are invariant under φ, whence by the assumptions imposed on they are ail in $Z(R)$. Similarly for any x in R,

$$x + \varphi(x) + \varphi^2(x)$$

is in $R(Z)$.

Let $J(R)$ be the radical of R. $J(R)$ is invariant under all the automorphism of R, so, in particular, $\varphi[J(R)] \subset J(R)$; thus φ induces an automorphism $\bar{\varphi}$ on $R/J(R)$. The properties described in the paragraph above are ones preserved under homomorphism so they must hold in $R/J(R)$ vis-a-vis $\bar{\varphi}$. By lemma 5 we conclude that $R/J(R)$ is commutative, hence $C(R) \subset J(R)$.

Let

$$c = \sum_{i=1}^{n} r_i (x_i y_i - y_i x_i) s_i$$

he an arbitrary element in $C(R)$. Let R_0 be the ring generated by all of the

$$\{r_i, \varphi(r_i), \varphi^2(r_i), x_i, \varphi(x_i), \varphi^2(x_i), y_i, \varphi(y_i), \varphi^2(y_i), s_i, \varphi(s_i), \varphi^2(s_i)\}.$$

R_0 is a finitely generated ring which is invariant under under φ. All fixed points of φ in R_0 are in the center of R so they must certainly be in the center of R_0. By the corollary to lemma 3, R_0 satisfies a polynomial identity. Finally R_0 is an algebra over $GF(3)$, the field of 3 elements. All the conditions of a result of Amitsur [1] hold so by this this result, $J(R_0)$ is a nil ring. Since, as we have seen above, $C(R_0) \subset J(R_0)$, $C(R_0)$ must be nil. But

$$c = \sum r_i (x_i y_i - y_i x_i) s_i$$

is in $C(R_0)$ so must be nilpotent. Since c is an arbitrary element of $C(R)$ we have proved that $C(R)$ is a nil ideal.

Before continuing with our special situation we wish to digress to prove a result, which may be of some independent interest, which holds for all rings.

Lemma 7. *Let R be a ring and W an ideal of R. Suppose that $C(W)$ is a nil ideal of W. If $x \in C(R)$ satisfies $x^k \in W$ for some k, then x is nilpotent.*

Proof. Let T be the ideal of R generated by $C(V)$. In $\bar{R} = R/T$, $\bar{W}$ is an ideal which is commutative. Suppose that $\bar{w}, \bar{w}_1 \in \bar{W}$ and that $\bar{y} \in \bar{R}$; since both $\bar{w}$ and $\bar{w}_1 \bar{y}$ are in $\bar{W}$ they commute, whence $\bar{w}_1 \bar{w} \bar{y} = \bar{w}(\bar{w}_1 \bar{y}) = (\bar{w}_1 \bar{y}) \bar{w}$ so that $\bar{w}_1(\bar{w}\bar{y} - \bar{y}\bar{w}) = 0$. Let $N(\bar{R})$ be the maximal nil ideal of $\bar{R}$ and let $\bar{\bar{R}} = \bar{R}/N(\bar{R})$. In $\bar{\bar{R}}$ there are no non-zero nil ideals. $\bar{\bar{W}}$ is a commutative ideal in $\bar{R}$ so as above $\bar{\bar{w}}_1(\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}}) = 0$ for any $\bar{\bar{w}}_1, \bar{\bar{w}}$ in $\bar{\bar{W}}$ and $\bar{\bar{y}}$ in $\bar{\bar{R}}$. Replacing $\bar{\bar{y}}$ by $\bar{\bar{z}}\bar{\bar{y}}$ in this we get that $\bar{\bar{w}}_1 \bar{\bar{z}}(\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}}) = 0$; if we put $\bar{\bar{w}}_1 = \bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}}$ (which is in $\bar{\bar{W}}$) we see that $(\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}})\bar{\bar{R}}(\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}}) = (0)$, whence $(\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}})\bar{\bar{R}}$ is a nilpotent right ideal in $\bar{\bar{R}}$. From this we get that $\bar{\bar{w}}\bar{\bar{y}} - \bar{\bar{y}}\bar{\bar{w}} = 0$ for all $\bar{\bar{y}} \in \bar{\bar{R}}$, that is, $\bar{\bar{W}} \subset Z(\bar{\bar{R}})$. Since for any $\bar{\bar{w}} \in \bar{\bar{W}}$ and $\bar{\bar{y}}, \bar{\bar{z}} \in \bar{\bar{R}}$ both $\bar{\bar{w}}$ and $\bar{\bar{w}}\bar{\bar{y}}$ as elements of $\bar{\bar{W}}$ are in $Z(\bar{\bar{R}})$, we easily get $\bar{\bar{w}}(\bar{\bar{y}}\bar{\bar{z}} - \bar{\bar{z}}\bar{\bar{y}}) = 0$. Since w annihilates all commutators and is in the center it annihilates $C(\bar{\bar{R}})$. Thus $\bar{\bar{W}}\, C(\bar{\bar{R}}) = (0)$.

Therefore we see that in $\bar{R}$, $\bar{W}C(\bar{R}) \subset N(\bar{R})$ thus is a nil ideal. But then, since $\bar{x} \in C(\bar{R})$ and $\bar{x}^k \in \bar{W}$; we get $\bar{x}^{k+1} \in \bar{W}C(\bar{R})$ so is nilpotent. That is $\bar{x}^m = 0$, whence $x^m \in T$ for some m. However

$$T^3 \in RC(W)R\ RC(W)R\ RC(W) \subset WC(W)W \subset C(W),$$

so is a nil ideal; thus $(x^m)^3$, being in T^3, is nilpotent, whence x is nilpotent.

We return to the question of rings with an automorphism of period 3.

Lemma 8. *If R is a ring such that $3^n R = (0)$ for some n and admits an automorphism φ of period 3 all of whose fixed-points are in $Z(R)$ then $C(R)$ is a nil ideal.*

Proof. The case $n = 1$ is precisely lemma 6, so we proceed from this by induction on n.

Let $W = \{x \in R \mid 3x = 0\}$. First note that W is invariant under φ and is an algebra over $GF(3)$. By lemma 6 we know that $C(W)$ is nil. Let $\bar{R} = R/W$; since W is invariant under φ, φ induces an automorphism $\bar{\varphi}$ on $\bar{R}$. Suppose that $\bar{\varphi}(\bar{x}) = \bar{x}$; then if x in R maps on $\bar{x}$, we have that $x - \varphi(x) \in W$, whence $3[x - \varphi(x)] = 0$. Thus $\varphi(3x) = 3x$, which forces $3x$ to be in $Z(R)$. But then, for any $y \in R$, $3(xy - yx) = (3x)y - y(3x) = 0$, that is, $xy - yx \in W$ for all y in R. In $\bar{R}$ this translates to $\bar{x}\bar{y} = \bar{y}\bar{x}$, which is to say, $\bar{x} \in Z(\bar{R})$. Thereby the conditions carry over from R to $\bar{R}$; since $3^{n-1}\bar{R} = (0)$ by the induction $C(\bar{R})$ is a nil ideal. Therefore, if $c \in C(R)$, $c^k \in W$ for some k. Since $C(W)$ is nil, by lemma 7 c is nilpotent. Thus $C(R)$ is nil and the lemma is established.

We remove the condition in lemma 8 that $3^n R = (0)$, replacing it by a slightly weaker one in

Lemma 9. *Let R be a ring such that $3^k x = 0$ for every $x \in R$, where k depends on x; farther suppose that R admits an automorphism φ of period 3 all of whose fixed-points are in $Z(R)$. Then $C(R)$ is a nil ideal.*

Proof. If $c \in C(R)$, then

$$c = \sum r_i (x_i y_i - y_i x_i) s_i ;$$

let R_0 be the subring of R generated by all of the r_i, x_i, y_i, s_i; and their images under φ and φ^2. R_0 is invariant under φ; moreover, since it is finitely generated by elements having additive orders which are powers of 3 we get that $3^n R_0 = (0)$ for some n. By lemma 8, $C(R_0)$ is nil; since $c \in C(R_0)$ we then have that c is nilpotent. We have proved that $C(R)$ is a nil ideal of R.

We now are able to prove the principal result of this section, namely

Theorem 5. *Let R be a ring which admits an automorphism of period 3 all of whose fixed-points are in the center of R. Then the commutator ideal of R is a nil ideal.*

Proof. Let $U = \{x \in R \mid 3^k x = 0$ for some $k\}$; U is an ideal of R invariant under φ. By Lemma 9, $C(U)$ is a nil ideal of U.

Since U is invariant under φ, φ induces an automorphism $\bar{\varphi}$ on $\bar{R} = R/U$. If $\bar{\varphi}(\bar{x}) = \bar{x}$ then since $\bar{x} + \bar{\varphi}(\bar{x}) + \bar{\varphi}^2(\bar{x}) \in Z(\bar{R})$, we would have that $3\bar{x} \in Z(\bar{R})$; but then $3(\bar{x}\bar{y} - \bar{y}\bar{x}) = 0$ for all $\bar{y} \in \bar{R}$. However, in $\bar{R}$, $3\bar{t} = 0$ implies that $\bar{t} = 0$; thus $\bar{x}\bar{y} - \bar{y}\bar{x} = 0$ for all $\bar{y} \in \bar{R}$. Thus we see that the only fixed points of $\bar{\varphi}$ in $\bar{R}$ are in $Z(\bar{R})$.

Consider $\bar{R}$ as a Lie ring under the product $[\bar{a}, \bar{b}] = \bar{a}\bar{b} - \bar{b}\bar{a}$. Form the Lie ring $\bar{\bar{R}} = \bar{R}/Z(\bar{R})$. In $\bar{\bar{R}}$, $\bar{\varphi}$ induces an automorphism $\bar{\bar{\varphi}}$. We claim that $\bar{\bar{\varphi}}$ leaves only 0 fixed; for if $\bar{\bar{\varphi}}(\bar{\bar{x}}) = \bar{\bar{x}}$ then $\bar{x} - \bar{\varphi}(\bar{x})$ is in $Z(\bar{R})$. Since $\bar{x} + \bar{\varphi}\bar{x} + \bar{\varphi}^2(\bar{x}) \in Z(\bar{R})$ we get $3\bar{x} \in Z(\bar{R})$ whence $\bar{x} \in Z(\bar{R})$ so that $\bar{\bar{x}} = 0$. By a result of Higman [4] $\bar{\bar{R}}$ must be nilpotent as a Lie ring. Thus as an associative ring $\bar{R}$ must enjoy the property that there exists an integer n such that the n-fold commutator of any n elements in $\bar{R}$ is 0. In particular $\bar{R}$ satisfies a fixed Engel condition (see [2]) whence by the main result of [2] the commutator ideal of $\bar{R}$ is a nil ideal. Consequently if $c \in C(R)$, c^k must be in U for some integer k. Since we already know that $C(U)$ is nil, applying lemma 7 we obtain that c is nilpotent. Thus $C(R)$ is a nil ideal of R and the theorem is proved.

BIBLIOGRAPHY

[1] S. A. AMITSUR : *A generalization of* HILBERT'*s Nullstellensatz*, Proc. Am. Math. Soc., **8**, Pp. 649—650, (1951).

[2] I. N. HERSTEIN : *Sugli anelli soddisfacenti ad una condizione di Engel*, to appear in the Rendiconti dell' Accademia dei Lincei.

[3] » » : *Lie and Jordan systems in simple rings with involution*, Amer. Jour. Math., **78**, Pp. 629—649, (1956).

[4] GRAHAM HIGMAN : *Groups and rings having automorphism without non—trivial fixed elements*, Jour. Lond. Math. Soc., **32**, p. 321—334, (1957).

[5] NATHAN JACOBSON : *A note on automorphisms and derivations of Lie algebras*, Proc. Amer Math. Soc., **6**, Pp. 281—283, (1955).

[6] IRVING KAPLANSKY : *Rings with a polynomial identity*, Bull. Amer. Math. Soc., **54**, pp. 575—580, (1948).

[7] » » : *A theorem on division rings*, Canadian Jour. of Math., **3**, pp. 290—292, (1951).

[8] JOHN THOMPSON : *Finite groups with fixed—point free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A., **45**. pp. 578—581, (1959).

DEPT. OF MATHEMATICS
CORNELL UNIVERSITY
U. S. A.

(Manuscript received on July 15, 1962)

ÖZET

Birkaç sene evvel bir makalede JACOBSON [5], yalnız sıfır elemanını sabit bırakan asal peryodlu bir otomorfizmi haiz sonlu boyutlu bir Lie cebirinin nilpotent olmak mecburiyetinde olduğunu göstermiştir. Sonlu gruplar halindeki benzer neticenin doğru olacağı FROBENIUS tarafından tahmin edilmiş ve ispatı THOMPSON'un çok güzel bir yazısında [8] elde edilen daha kuvvetli bir teoremin sonuça olarak verilmiştir. Asosyatif halkalaların durumu HIGMAN [4] tarafından incelenmiş ve kendisi bu tarzda bir otomorfizmin mevcudiyeti halkayı nilpotent yaptığını göstermiştir.

Bir asosyatif halkanın bir birim elemanı mevcut ise, bu eleman halkanın bütün otomorfizmleri için sabit kalmaktadır. Verilen bir cisim üzerinde inşa edilen birim elemanı haiz bir cebir için otomorfizmi cebrik otomorfizm manasında anlayacak olursak, cismin her bir elemanı sabit kalmalıdır. Bu itibarla halka veya cebirler için bir otomorfizm sadece sıfır elemanı sabit bırakması hipotezi aşırı derecede tahdit edici ve gayritabidir. Evvelki neticenin hakiki benzeri şu halde daha çok bu şekilde ifade edilmelidir: asal peryodlu bir otomorfizmin sabit noktaları muayyen «tabiî» bir alt cümlede kalmaları halinde asosyatif halka veya cebirin yapısı nedir?

Kısım I'de sol ideallerinde inen zincir şartını haiz sonlu boyutlu cebir ve halkalar için bu yapı, sabit noktalar cümlesi iyice belirtilmesi halinde elde edilmiştir. İkinci ve üçüncü Kısımlarda ise, bütün sabit noktaların halkanın merkezinde bulunmaları halinde peryodu 2 ve 3 olan otomorfizmleri haiz umumî halkaların yapısı elde edilmiştir. Burada elde edilen neticeler, yani komütatör idealinin sıfır oluşu, umumî halde bütün sabit noktaları merkezinde bulunan asal peryodlu otomorfizmleri haiz halkalar için doğru kalacağı da tahmin edilmektedir.