ON A THEOREM OF HERSTEIN

M. CHACRON

Introduction. Throughout this paper, Z is the ring of integers, $f^*(t)$ ($f(t)$) is an integer monic (co-monic) polynomial in the indeterminate t (i.e., each coefficient of f^* (f) is in Z and its highest (lowest) coefficient is 1 (**5**, p. 121, Definition) and M^* (M) is the multiplicative semigroup of all integer monic (co-monic) polynomials f^* (f) having no constant term. In (**3**, Theorem 2), Herstein proved that if R is a division ring with centre C such that

(1) for all $a \in R$ there exists $f(t) \in M$ such that $f(a) \in C$,

then $R = C$. In this paper we seek a generalization of Herstein's result to semi-simple rings. We also study the following condition:

(1)* for all $a \in R$ there exists $f^*(t) \in M^*$ such that $f^*(a) \in C$.

Our results are quite complete for a semi-simple ring R in which there exists a bound for the codegree of f (f^*) (i.e., the degree of the lowest monomial of f (f^*)) appearing in the left-hand side of (1) ((1)*).

1. Preliminary results. In this section we present results on algebraic integers (co-integers) that we will need in the present paper. An element a of a ring R is said to be an *algebraic integer* (*co-integer*) if a is a root of some polynomial $f^*(t)$ ($f(t)$) in M^* (M). For example, if the cyclic semigroup generated by a,

$$[a] = \{a, a^2, \ldots, a^m, \ldots\},$$

is finite, that is, if $a^m = a^{2m}$ for some $m \geqq 1$ (Rees), then a is both an algebraic integer and an algebraic co-integer.

PROPOSITION 1. *Let R be a ring. The following conditions are equivalent:*

(i) *for all $a \in R$ there exist m, n with $m > n \geqq 1$ such that $a^m = a^n$;*

(ii) *for all $a \in R$ there exist $f^* \in M^*$ and $m, n \geqq 1$ such that $ma^n = 0$ and $f^*(a^n) = 0$.*

Proof. Obviously, (i) implies (ii). Conversely, if $a \in R$ satisfies (ii) in its own right, we shall prove that a satisfies (i). Let $b = a^n$. For some $k > 1$, we have

$$b \in \sum_{i=1}^{k} Zb^i.$$

Received June 21, 1968 and in revised form, April 20, 1969. This research has been partially supported by the National Research Council of Canada (Grant A4 807) and the Canadian Mathematical Congress (Summer Fellowship, 1968).

It follows that

$$[b] \subseteq \sum_{i=1}^{k} Zb^i.$$

Let $\theta(E)$ be the number of elements of a set E. We have $\theta(Zb^i) \leqq \theta(Zb)$ for all $i = 1, \ldots, k$ and $Zb = \{0, b, \ldots, (m-1)b\}$ is finite. Therefore, $[b]$ is finite. Hence $[a]$ is finite.

This proposition extends a remark of Rosenberg and Zelinsky on an algebra A which is algebraic over a Galois field (**7**, p. 485). If R satisfies conditions (i) and (ii), we term R a *periodic* ring (**1**, Introduction or **2**, Introduction). The following proposition has an independent interest (**4**, Theorem).

PROPOSITION 2. *If each element a of R is an algebraic co-integer, then R is a periodic ring.*

Proof. Let $a \in R - \{0\}$. We may assume that a is non-nilpotent. For some $f(t) = t^n - t^{n+1}p(t) \in M$, we have $f(a) = 0$. It follows that

$$a^n p^n(a) = e = e^2 \neq 0, \quad a^n = a^n e, \quad \text{and} \quad a^n = a^{n+1}p(a).$$

Set $R_e = eRe$ and $\alpha = ae = ea$. Clearly,

$$\alpha^n p^n(\alpha) = e, \quad \alpha^n = a^n, \quad \text{and} \quad \alpha^n = \alpha^{n+1}p(\alpha).$$

It follows that α is an invertible element of the ring R_e and that $\alpha^{-1} = p(\alpha)$. Therefore, α^{-1} is an algebraic integer of R_e of degree less than $\deg(p) + 1$. Let us assume, for the moment, that R_e is a torsion ring. By Proposition 1, α^{-1} is a root of the unit of degree less than $\theta(e)(\deg p + 1)$, where $\theta(e)$ is the additive order of the unit element e of R_e. It follows that $\alpha^k = e$ for some k less than $\theta(e)\deg f$. Then

$$a^{nk} = (a^n)^k = \alpha^{nk} = (\alpha^k)^n = e^n = e.$$

Therefore, $[a]$ has at most $2\theta(e)\deg f$ elements. It remains to prove that, for every idempotent element e of R, e has an additive order. In fact, every subring of R will inherit the property of R. In particular, the subring $\langle e \rangle$ generated by e must be π-regular. However, Z is not π-regular, whence $\langle e \rangle$ is a proper image of Z; that is to say, $\theta(e)$ is finite. The proposition is proved.

Remark 1. Proposition 2 is capable of a rather wide generalization, for we can prove the following: *If each element a of R satisfies*

$$c_1 a^n + \ldots + c_{l+1}a^{n+l} = 0$$

for some $n \geqq 1$ and $l \geqq 1$ depending on a, where c_1 is the integer ± 1 or is a central algebraic co-integer lying in no right primitive ideal of R in the semi-simple case and in no prime ideal of R in the general case, and where $c_2, \ldots, c_n$ are rational integers or algebraic integers which commute elementwise, then R is periodic.

https://doi.org/10.4153/CJM-1969-148-5 Published online by Cambridge University Press

PROPOSITION 3. *Let D be a division ring and let R be a subring of D. If each element of D is an algebraic integer (co-integer), then R is a periodic field.*

Proof. For every $a \neq 0$ in D, a^{-1} is an algebraic co-integer. By Proposition 2, D is periodic, whence D is a division ring in which $x = x^{n(x)}$ for all $x \in D$. Therefore, D is a field. Since each subring of a periodic ring is periodic, R is periodic. Since every periodic ring which has no divisors of zero is a field, R is a periodic field.

2. Results. The following proposition, whose proof is similar to the first part of the proof in (**7**, Theorem 1), is the key result of this paper.

PROPOSITION 4. *Let R be a (right) primitive ring with centre C. Let Φ be a set of polynomials $g(t)$ having as coefficients rational integers or elements of C. Assume that R is a non-division ring and that Φ is closed under composition of polynomials. If for every element a of R there exists $f \in \Phi$ such that $f(a) \in C$, then there exists a field F containing C as a subring such that*

$$\text{for all } \lambda \in F \text{ there exists } g(t) \in \Phi \text{ such that } g(\lambda) = 0.$$

Moreover, each element of R is a root of some polynomial in Φ.

Proof. Let V be a faithful irreducible (right) R-module. Let Δ be the commuting ring of R on M. The centre C of R may be identified with a subring of the centre F of Δ, which is a division ring. Furthermore, we may assume that V contains two independent vectors, u and v. Let $\lambda \in \Delta$. Since R acts densely on M, we may find a in R such that $ua = 0$ and $va = v\lambda$. For some $f \in \Phi$, we have $f(a) \in C$. It follows that $u \cdot f(a) = 0$ for $f(a) \in C$. Therefore, $f(a) = 0$. Now $v \cdot f(\lambda) = v \cdot f(a) = 0$ and by the hypothesis, $f(\lambda)$ is in Δ. Therefore, $f(\lambda) = 0$, whence $F \subseteq \Delta$ satisfies the required property. Let $a \in R$. We can find $g \in \Phi$ and $f \in \Phi$ such that $(f \circ g)(a) = 0$. Since Φ is closed, a is a root of $f \circ g \in \Phi$.

Let us specialize Proposition 4 to the case that Φ consists entirely of monic (co-monic) polynomials. We have the following result.

THEOREM 1. *If R is as in Proposition 4 and if Φ consists entirely of co-monic (monic) polynomials, then either R is strong π-regular or R is a torsion-free ring having zero centre.*

Proof. There are two disjoint cases.

Case I. $C = (0)$. By Proposition 4, R consists entirely of algebraic co-integers (integers), whence R is periodic (periodic or torsion-free) (Propositions 1, 2, and 3).

Case II. $C \neq (0)$. The case where Φ consists entirely of co-monic polynomials yields R as strong π-regular (Proposition 4). In the dual case, there exists a field $F \supseteq C$ which is integral over C. By a general result, C is a subfield. Since R is algebraic over its centre C (Proposition 4), R is an algebraic algebra. Therefore, R is strong π-regular.

From Theorem 1, we derive the following result.

THEOREM 2. *Let R be a semi-simple ring satisfying* (1). *Then R is a subdirect product of fields or non-commutative algebraic algebras over Galois fields.*

Proof. Since (1) is preserved under ring homomorphisms, R is a subdirect product of primitive rings A satisfying (1). If A is a division ring, A is a field (Herstein's result). In the case that A is a non-division ring, A is periodic (Theorem 1). In that case, either A has non-zero characteristic or A is torsion-free (A is, in fact, primitive and hence, prime). If A is torsion-free, then A is nil (Proposition 1), contrary to the primitiveness of A. Therefore, A has a non-zero characteristic. Since A is prime, its characteristic is prime. This proves the theorem.

THEOREM 3. *Let R be a semi-simple ring with* 1. *If R satisfies* (1)*, *then R is a subdirect product of division rings or non-commutative algebraic algebras over Galois fields.*

Proof. It suffices to prove the theorem in the case that R is a primitive non-division ring. By the hypothesis, the centre C of R is not (0). Theorem 1 applies and yields C as a periodic field and R central algebraic. By Proposition 1, R is periodic. As in the foregoing, R must have a non-zero characteristic.

Theorem 3 suggests the following question.

Question. Let D be a division ring satisfying (1)*. Is D always a field?

This is an open question if D is torsion-free. It can be answered in the affirmative if the characteristic of D is a prime number (Herstein's result).

3. Finiteness assumptions. If R is a ring as in (**3**), then R satisfies (1) with the property that the codegree of f in (1) is always 1, hence bounded. Since this forces the commutativity of R (**3**, Theorem 19), it is natural to seek a generalization of (**3**, Theorems 2 and 19) in the general case where the codegree of f is bounded by some integer $\mu_1 \geqq 1$. As a counterpart of this restriction, henceforth we replace C appearing in the right-hand side of (1) by an overset S defined as follows:

$$a \in S \text{ if and only if for all } x \in R \text{ there exists } g \in Z[t] \text{ such that } xa = g(a)x.$$

Condition (1) ((1)*) will be replaced by:

$$\text{(2) for all } x \in R \text{ there exist } \mu < \infty \text{ and } f \in M \text{ such that } \operatorname{codeg} f \leqq \mu + 1 \text{ and } f(x) \in S,$$

$$\text{(2)* for all } x \in R \text{ there exist } \mu^* < \infty \text{ and } f^* \in M^* \text{ such that } \operatorname{codeg} f^* \leqq \mu^* + 1 \text{ and } f^*(x) \in S,$$

where $\operatorname{codeg} f$ denotes the codegree of f.

We make a free use of the following properties of $S = S(R)$.

https://doi.org/10.4153/CJM-1969-148-5 Published online by Cambridge University Press

Property 1. For every $s \in S$, if $C[s]$ is the subring of R generated by the centre C of R and s, then $C[s]$ is invariant under all inner automorphisms of R.

Property 2. For every subring A of R and every $s \in A \cap S$, we have $As \subseteq sA$ (i.e., s is in the right normalizer of A thought of as a ring (**8**, p. 32)).

Property 3. For every homomorphic image $\bar{R}$ of R, if $\bar{S}$ is the image of $S = S(R)$, then $\bar{S} \subseteq S(\bar{R})$.

Properties 1–3 are quite easy to prove and imply immediately that (2) ((2)*) is preserved under subrings and ring homomorphisms, which is essential for the following theorem.

THEOREM 4. *If R is a semi-simple ring satisfying* (2) ((2)*), *then R is a subdirect product of fields (division rings) or total matric rings $\Delta_{n_i}^{(i)}$, where $\Delta^{(i)}$ is a periodic (Galois) field, and where $\Delta_{n_i}^{(i)}$ is the ring of all $(n_i \times n_i)$ matrices over $\Delta^{(i)}$ with $1 < n_i \leqq \mu$ (μ*).

The proof of Theorem 4 is divided in several parts.

Part I. If R is a division (torsion division) ring satisfying (2) ((2)*), then R is a field.

Proof. Let $x \in S$. We may assume that $C[x] = C$, that is $x \in C$. Therefore, $S = C$ and R satisfies (1) ((1)*). By Herstein's result, $R = C$.

Part II. If $R = \Delta_s$ is a total matric ring over a division ring Δ of index $s > 1$ and if R satisfies (2) ((2)*), then R satisfies (1) ((1)*).

Proof. The centre of R can be identified to the centre C of Δ. If $C = \mathrm{GF}(2)$, then Δ is a torsion division ring. Since every subring of R inherits (2) ((2)*), we see that $\Delta = C$ (Part I). Therefore, $R = (\mathrm{GF}(2))_s$ and R satisfies, obviously, (1) ((1)*). If $C \neq \mathrm{GF}(2)$, then (**6**, Theorem 1.15) applies and yields (0), C, R to be the only subalgebras of R (considered as an algebra over its centre) invariant under all inner automorphisms of R. It follows that $S = C$ and R satisfies (1) ((1)*).

Part III. If R is a prime ring satisfying (1) ((2)*), then the degree of nilpotence of R is at most μ (μ*).

Proof. Let $a \in R$ be a nilpotent element. For some f (f*) as in (2) ((2)*), $f(a) = a^{n+1} - a^{n+2}p(a) \in S$ ($f^*(a) = p(a) - a^{n+l} \in S$), where $p(t)$ is an integral polynomial depending on a (of degree less than $n + l$). Since $\langle a \rangle$ is nil, $f(a)$ ($f^*(a)$) is nilpotent. Since $R \cdot f(a) \subseteq f(a)R$ ($Rf^*(a) \subseteq f^*(a)R$) and since R is prime, $f(a) = 0$ ($f^*(a) = 0$), whence $a^{n+1} = 0$ ($a^{n+l} = 0$).

Part IV. Let R be a ring having a non-zero characteristic c. If R satisfies the following conditions:

(3) for all $x \in R$ there exist $\eta < \infty$ and $f \in M$ such that $\deg f \leqq \eta$ and $f(x) = 0$,

(3)* for all $x \in R$ there exist $\eta < \infty$ and $f^* \in M^*$ such that $\deg f^* \leqq \eta$ and $f^*(x) = 0$,

https://doi.org/10.4153/CJM-1969-148-5 Published online by Cambridge University Press

then for some integer N $(1 \leqq N \leqq (2c\eta)!)$ depending on c and η, we have $x^N = x^{2N}$ for all $x \in R$.

Proof. By Proposition 2 (Proposition 1) and by Rees' result.

Proof of Theorem 4. It is an immediate consequence of Theorem 2 (Theorem 3) and the foregoing.

From Theorem 4, which is a generalization of (**3**, Theorem 6; **8**, Theorem 6), we derive the following corollaries similar in the spirit to (**7**, Theorem 2).

COROLLARY 1. *Any semi-simple ring satisfying* (1) *with* $\deg f$ *bounded is a subdirect product of fields or finite non-commutative rings.*

COROLLARY 2. *Any torsion semi-simple ring satisfying* (1)* *with* $\deg f^*$ *bounded, is a subdirect product of fields or finite non-commutative rings.*

Using the representation in Theorem 4, we derive the following result.

COROLLARY 3. *Any semi-simple ring satisfying* (2), *in particular, if* (1) *with co-degree of* f *bounded, satisfies a polynomial identity with coefficients* ± 1 *of degree less than* 2μ.

Finally, if we combine Theorem 4 with one of the liberal commutativity assumptions that R is a ξ-ring or that R is radical over its right normalizer (**9**; **8**), it follows that R is a commutative ring.

REFERENCES

1. M. Chacron, *Certains anneaux périodiques*, Bull. Soc. Math. Belgique *20* (1968), 66–77.
2. ——— *On quasi periodic rings*, J. Algebra *12* (1969), 49–60.
3. I. N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. *75* (1953), 866–871.
4. ——— *A note on rings with central nilpotent elements*, Proc. Amer. Math. Soc. *5* (1954), 620.
5. ——— *Topics in algebra* (Blaisdell, Waltham, Massachusetts, 1964).
6. ——— *Topics in ring theory*, Mathematics Lecture Notes, University of Chicago, Chicago, Illinois, 1965.
7. A. Rosenberg and D. Zelinsky, *On Nakayama's extensions of the* $x^{n(x)}$ *theorems*, Proc. Amer. Math. Soc. *5* (1954), 484–486.
8. G. Thierrin, *Extensions radicales et quasi-radicales dans les anneaux*, Can. Math. Bull. *5* (1962), 29–35.
9. Y. Utumi, *On* ξ*-rings*, Osaka Math. J. *33* (1957), 63–65.

Queen's University,
Kingston, Ontario;
University of Windsor,
Windsor, Ontario