COLLOQUIUM MATHEMATICUM

VOL. XL 1979 FASC. 2

ON MODULES PN WHICH IDEMPOTENT REDUCTS FORM A CHAIN

BY

ÁGNES SZENDREI (SZEGED)

The problem raised in the title is analogous to the one solved by Płonka in [4]. The main result of this note (Theorem 2) is based on Theorem 1, describing all those rings with identity in which the family of subrings forms a chain under set inclusion. Note that Theorem 1 settles a special case of Problem 90 in [6] (p. 224).

1. Rings with identity in which subrings form a chain. We need some well-known results in the theory of finite fields (see, e.g., [5]). For each prime p and any natural number n ($n \geqslant 1$), $F(p^n)$ will stand for the field of order p^n. Further, suppose that $F(p^{q^n}) \subset F(p^{q^m})$ if p and q are arbitrary primes and m, n ($m, n \geqslant 0$) are natural numbers such that $n < m$. Then, clearly, $\bigcup (F(p^{q^n}) \mid 0 \leqslant n < \omega)$ is also a field which will be denoted by $F(p^{q^\omega})$. The ring of integers will be denoted by Z, whereas its factor ring $Z/(n)$ with $n \in Z$ will be denoted by Z_n. For any subset H of a ring R, $[H]$ will stand for the subring of R generated by H.

THEOREM 1. *The lattice of subrings of a ring R with identity is a chain if and only if R is isomorphic to one of the rings Z_{p^n} or $F(p^{q^m})$, where p and q are primes and $0 \leqslant m \leqslant \omega$, $0 \leqslant n < \omega$.*

Proof. The sufficiency is obvious. To prove the necessity suppose that R is a ring with identity e and that the subrings of R form a chain. Then R is of characteristic p^k for a prime number p and $0 \leqslant k < \omega$, else $[\{e\}]$ ($[\{e\}] \subseteq R$) would contain two incomparable subrings. If $k = 0$, then R is the one-element ring, so that $R \cong Z_1$. For the rest of the proof we assume that $1 \leqslant k < \omega$. It is easy to see that $pR = [\{pe\}]$. Indeed, $e \notin pR$, since, otherwise, $e = pr$ for some r in R and thus $p^{k-1}e = p^k r = 0$, contradicting the fact that R is of characteristic p^k. Therefore, necessarily, $pR \subset [\{e\}]$ implying $pR \subseteq [\{pe\}]$, i.e. $pR = [\{pe\}]$. Furthermore, the ring R is commutative, since for any elements r_1 and r_2 in R either $[\{r_1\}] \subseteq [\{r_2\}]$ or $[\{r_2\}] \subseteq [\{r_1\}]$. Let us consider now an arbitrary element r

in $R-pR$. We show that $[\{r\}]$ contains the multiplicative inverse of r. In fact, since $[\{r\}] \nsubseteq pR = [\{pe\}]$, we have $[\{r\}] \neq [\{e\}]$ which implies $e \in [\{r\}]$, i.e.

$$e = \sum_{i=1}^{n} c_i r^i$$

for some integers n $(n \geqslant 1)$ and $c_1, \ldots, c_n$. Hence

$$r^{-1} = \sum_{i=1}^{n} c_i r^{i-1} \in [\{r, e\}] = [\{r\}],$$

which was to be proved.

It follows from the properties of R stated so far that the factor ring $T = R/[\{pe\}]$ is a field of characteristic p and, moreover, for any non-zero t in T the subring $[\{t\}]$ is also a field. Next we prove that $[\{t\}]$ is finite. In fact, since $e \in [\{t\}]$, there exist integers n $(n \geqslant 1)$ and $c_1, \ldots, c_n$ such that

$$e = \sum_{i=1}^{n} c_i t^i,$$

i.e.

$$c_n t^n = e - \sum_{i=1}^{n-1} c_i t^i.$$

Without loss of generality we can suppose that $0 \leqslant c_i < p$ and $c_n \neq 0$ $(1 \leqslant i \leqslant n)$. Further, let $c_n' e = (c_n e)^{-1}$ $(\in [\{t\}])$. Then

$$t^n = c_n' e - \sum_{i=1}^{n-1} c_n' c_i t^i$$

which clearly implies that $[\{t\}]$ is finite.

Obviously, if T is a finite field, then T is isomorphic to one of the fields $F(p^{q^m})$ with q prime and $0 \leqslant m < \omega$. If, on the contrary, T is infinite, then every proper subring of T is finite. Indeed, if T' were an infinite proper subring of T, then for any $t \in T-T'$ the finite field $[\{t\}]$ and the infinite ring T' would be two incomparable subrings in T, contradicting the fact that the subrings of T form a chain. Thus, by [2] or [3], R is isomorphic to $F(p^{q^\omega})$, where q is prime.

We have established so far that R is of characteristic p^k, $pR = [\{pe\}]$ is an ideal in R and $T = R/[\{pe\}]$ is isomorphic to one of the fields $F(p^{q^m})$ with p, q prime and $0 \leqslant m \leqslant \omega$. It remains to prove that either $k = 1$ implying $R \cong F(p^{q^m})$ or $m = 0$, so that $R \cong Z_{p^k}$. Assume that, contrary to our claim, $k \geqslant 2$ and $m \geqslant 1$. Since the non-existence of a ring with the properties described above for $m = m_0$ implies the non-existence of such

a ring for all m greater than m_0, we can restrict ourselves to finite m. Set $n = q^m$ and choose

$$P(x) = \sum_{i=0}^{n} c_i x^i$$

to be a polynomial of degree n, with integral coefficients satisfying $c_n = 1$ and $0 \leqslant c_i < p$ $(0 \leqslant i < n)$, such that $P(x)$ considered as a polynomial over Z_p is irreducible. Further, let f be an element in $F(p^n)$ with $P(f) = 0$. By the isomorphism $R/[\{pe\}] \cong F(p^n)$ there exists an element r in R such that $P(r) \in [\{pe\}]$, say $P(r) = pm_1 e$ in R, where $m_1 \in Z$ and $0 \leqslant m_1 < p^{k-1}$. On the other hand, $pr \in [\{pe\}]$ implying the equality $pr = pm_2 e$ in R for some $m_2 \in Z$ with $0 \leqslant m_2 < p^{k-1}$. It is easy to show by induction on j that

$$pr^j = pm_2^j e \qquad (0 < j < \omega).$$

Thus

$$p^2 m_1 e = pP(r) = pP(m_2 e) = p \sum_{i=0}^{n} c_i m_2^i e$$

holds in R yielding the congruence

$$p^2 m_1 \equiv p \sum_{i=0}^{n} c_i m_2^i \pmod{p^k}$$

in Z. Since $k \geqslant 2$, p divides $\sum_{i=0}^{n} c_i m_2^i$, i.e. the element $m_2 e$ in Z_p is a zero of the polynomial $P(x)$, contradicting the irreducibility of $P(x)$. This completes the proof of the theorem.

Remark. It is worth comparing this result with the one found independently by Kovács and Laffey in [2] and [3], respectively. We see that among infinite rings with identity those having no infinite proper subrings are just those in which subrings form a chain under set inclusion, and these rings are exactly the infinite fields $F(p^{q^\omega})$ with p and q prime. An analogous result is well known for Abelian groups, namely, among infinite Abelian groups Prüfer's quasicyclic groups $C(p^\infty)$ with p prime are exactly those having no infinite proper subgroups (see [7]) and, on the other hand, those in which subgroups form a chain under set inclusion.

I am indebted to Professor B. Csákány and to the referee of the original version of this paper for calling my attention to papers [2] and [3], respectively. Reconsidering the original version of Theorem 1 in the light of these results made it possible to obtain the stronger statement presented above.

2. Modules in which idempotent reducts form a chain. In this section we use the terminology and notation of [1] with the only exception that we adopt the notion of a heterogeneous clone due to Taylor [10].

Let $\mathfrak{A} = \langle A; F\rangle$ be an algebra. Then an algebra of the form $\langle A; F'\rangle$ with $F' \subseteq P(\mathfrak{A})$ is called a *reduct* of $\mathfrak{A}$. The reduct $\langle A; F'\rangle$ of $\mathfrak{A}$ is called *idempotent* if every operation in F' is idempotent. We shall not distinguish equivalent algebras, so that there is a one-to-one correspondence between the reducts of an algebra $\mathfrak{A}$ and the subclones of the clone $P(\mathfrak{A})$ of $\mathfrak{A}$.

Let R be a ring with identity e. For brevity, by the term *R-module* we always mean a unitary left R-module. Let $\mathfrak{M}$ be an R-module. It is clear that any n-ary polynomial of $\mathfrak{M}$ is of the form

$$\langle m_1, \ldots, m_n\rangle \mapsto r_1 m_1 + \ldots + r_n m_n \quad \text{for some } r_1, \ldots, r_n \in R,$$

which will be denoted by

$$r_1 x_1 + \ldots + r_n x_n|_{\mathfrak{M}} \quad \text{or} \quad \sum_{i=1}^{n} r_i x_i|_{\mathfrak{M}}.$$

This polynomial is idempotent if and only if $e - \sum_{i=1}^{n} r_i$ belongs to the annihilator ideal of $\mathfrak{M}$. Hence every n-ary idempotent polynomial of $\mathfrak{M}$ is of the form

$$\sum_{i=1}^{n} r_i x_i|_{\mathfrak{M}} \quad \text{for some } r_1, \ldots, r_n \in R \text{ with } \sum_{i=1}^{n} r_i = e.$$

For any subring S of R the *subclone* $\mathrm{Cl}_{\mathfrak{M}}(S)$ of the clone of $\mathfrak{M}$ (see [8]) is defined to be the collection of polynomials of the form

$$s_1 x_1 + \ldots + s_{j-1} x_{j-1} + (e + s_j) x_j + s_{j+1} x_{j+1} + \ldots + s_n x_n|_{\mathfrak{M}},$$

where

$$n \geqslant 1 \quad \text{and} \quad s_i \in S \ (1 \leqslant i \leqslant n) \text{ with } \sum_{i=1}^{n} s_i = 0.$$

The following two lemmas will be useful in the proof of Theorem 2.

LEMMA 1. *Let R be a ring of finite characteristic with identity and let $\mathfrak{M}$ be an R-module. Then the clone of any idempotent reduct of $\mathfrak{M}$ can be represented in the form*

$$\bigcap \left(\mathrm{Cl}_{\mathfrak{M}}(S_\gamma) \mid \gamma < \alpha\right),$$

where α is a suitable ordinal and, for $\gamma < \alpha$, S_γ is a subring of R.

LEMMA 2. *Let R be a ring with identity and let $\mathfrak{M}$ be an R-module with trivial annihilator ideal. Then, for any chain $\{S_\lambda \mid \lambda \in \Lambda\}$ of subrings of R,*

$$\bigcap \left(\mathrm{Cl}_{\mathfrak{M}}(S_\lambda) \mid \lambda \in \Lambda\right) = \mathrm{Cl}_{\mathfrak{M}}\left(\bigcap (S_\lambda \mid \lambda \in \Lambda)\right).$$

We note that Lemma 1 is implied by Theorem 1 in [8] and Lemma 1 in [9]. Finally, by taking into consideration Lemma 1 in [8], Lemma 2 is just a restatement of Lemma 11 in [8].

THEOREM 2. *Let R be a ring with identity and let $\mathfrak{M}$ be an R-module with annihilator ideal I. Then the idempotent reducts of $\mathfrak{M}$ form a chain if and only if R/I is isomorphic to one of the rings Z_{p^n} or $F(p^{q^m})$ with p, q prime and $0 \leqslant n < \omega$, $0 \leqslant m \leqslant \omega$.*

Proof. Set $R' = R/I$. It suffices to show, by Theorem 1, that the idempotent reducts of $\mathfrak{M}$ form a chain if and only if the lattice of all subrings of R' is a chain. In fact, if the idempotent reducts of $\mathfrak{M}$ form a chain, then the family $\{\mathrm{Cl}_{\mathfrak{M}}(S) \mid I \subseteq S \subseteq R\}$ is ordered under set inclusion, and thus the set $\{S \mid I \subseteq S \subseteq R\}$ of subrings of R is also ordered. Hence the subrings of $R' = R/I$ form a chain, as desired.

Conversely, suppose that the subrings of R' form a chain and denote by $\mathfrak{M}'$ the module $\mathfrak{M}$ considered as an R'-module. Obviously, $\mathfrak{M}$ and $\mathfrak{M}'$ are equivalent algebras, so that it suffices to prove that the idempotent reducts of $\mathfrak{M}'$ form a chain. By hypothesis, the subrings of R' form a chain, hence the same does its subring $[\{e\}]$. Therefore, $[\{e\}] \cong Z_{p^k}$ for a prime number p and $0 \leqslant k < \omega$, i.e. R' is of characteristic p^k. Consider now the clone C of any idempotent reduct of $\mathfrak{M}'$. Lemma 1 implies that

$$C = \bigcap \left(\mathrm{Cl}_{\mathfrak{M}'}(S_\gamma) \mid \gamma < \alpha\right)$$

for a suitable ordinal α and suitable subrings S_γ $(\gamma < \alpha)$ of R. By assumption, $\{S_\gamma \mid \gamma < \alpha\}$ is a chain, whence by Lemma 2 we obtain

$$C = \mathrm{Cl}_{\mathfrak{M}'}(S), \quad \text{where } S = \bigcap (S_\gamma \mid \gamma < \alpha).$$

This immediately implies that the idempotent reducts of $\mathfrak{M}'$ form a chain, as required.

REFERENCES

[1] G. Grätzer, *Universal algebra*, Princeton 1968.

[2] I. Kovács, *Infinite rings without infinite proper subrings*, Publicationes Mathematicae, Debrecen, 4 (1955-1956), p. 104-107.

[3] T. J. Laffey, *Infinite rings with all proper subrings finite*, American Mathematical Monthly 81 (1974), p. 270-272.

[4] J. Płonka, *On groups in which idempotent reducts form a chain*, Colloquium Mathematicum 29 (1974), p. 87-91.

[5] L. Rédei, *Algebra I*, Oxford-New York-Toronto 1967.

[6] F. Szász, *Radikale der Ringe*, Disquisitiones Mathematicae Hungaricae 6, Budapest 1975.

[7] I. Szélpál, *Die unendlichen Abelschen Gruppen mit lauter endlichen echten Untergruppen*, Publicationes Mathematicae, Debrecen, 1 (1949), p. 63-64.

[8] Á. Szendrei, *On the idempotent reducts of modules I*, Universal Algebra, Colloquia Mathematica Societatis János Bolyai, Vol. 21 (to appear).
[9] — *On the idempotent reducts of modules II*, ibidem (to appear).
[10] W. Taylor, *Characterizing Mal'cev conditions*, Algebra Universalis 3 (1973), p. 351-397.

JÓZSEF ATTILA UNIVERSITY
BOLYAI INSTITUTE, SZEGED

Reçu par la Rédaction le 7. 1. 1977;
en version modifiée le 26. 3. 1977