60.

REVUE ROUMAINE DE MATHÉMATIQUES PURES ET APPLIQUÉES

TOME XVI, N° 4

1971

TIRAGE À PART

ÉDITIONS DE L'ACADÉMIE DE LA RÉPUBLIQUE SOCIALISTE DE ROUMANIE

IDEALS OF A RING WITH MODULAR INTERSECTION

BY

FERENC A. SZÁSZ

(Budapest)

Dedicated to the memory of
IVÁN SERES (1907–1966)

The present note dealing with the theoretical side of topic bears rather the character of the number theory in its genuine ring part.

Our paper aims firstly at giving a generalization of the well-known Chinese residue theorem for the case of noncommutative rings with divisors of zero and without twosided unity element. Secondly, we characterize the ring of the rational integers, as the most important ring with unity element among all rings, this characterization being completely abstract and not trivial.

In our note a ring, unity, ideal and radical means always an associative (but eventually noncommutative) ring; a twosided unity element, a twosided ideal and the Jacobson radical, respectively.

For the used notions we refer to D. Barbilian [2], I. Bucur [3], N. Divinsky [4], S. Eilenberg and N. Steenrod [5], H. Hasse [6], N. Jacobson [10], J. Kaplansky [12], J. Lambek [14], N. H. McCoy [15], and L. Rédei [16].

In the first part of our paper the ideals of a ring with modular intersection play an important rôle. For rings with unity the intersection of arbitrary ideals is obviously modular, and therefore this holds also for the particular case of the ring of rational integers.

The importance of modular right ideals of an arbitrary ring A consists in the well-known fact that the radical $\mathcal{J}$ of A coincides with the intersection of all modular maximal right ideals of A, where a right ideal R of A is called modular in A, if there exists an element $e \in A$ satisfying $x - ex \in R$ for every $x \in A$. The author [18] has proved the existence of a ring A with a maximal and not modular right ideal R such that $Q \subseteq R$ holds for the ideal Q, defined below:

$$Q = \{x \, ; \, x \in A, \quad Ax \subseteq R\}$$

The right ideals R and ideals Q with this property were called by the author quasimodular maximal right ideals and quasiprimitive ideals, respectively. The intersection of all quasimodular maximal right ideals and the intersection of all quasiprimitive ideals both, almost trivially, coincide with the radical $\mathcal{J}$ of the ring A. O Steinfeld [17] and in sharper form the author [19] have proved, that every quasiprimitive ideal must be primitive.

Furthermore, the author [20] has proved for arbitrary infinite cardinality $\aleph_\alpha$ the existence of a ring A having $\aleph_\alpha$ different modular right ideals, among which the intersection of every two modular right ideals is not modular. There exist also rings with 16 elements and with a non-modular intersection of modular right ideals. This fact is related by author [21] to the existence of semigroups with empty Frattini subsemigroups and having a subset which is not a semigroup. These rings cannot be radical rings.

Every Schreier-Everett ring extension of a radical ring by means of a radical ring is also a radical ring. Furthermore the coincidence of the radical of a projective limit of rings with the projective limit of the radicals of the rings was proved by Ion D. Ion [11] and D. Zelinsky [23]. (For the definitions see [3] and [5])

THEOREM 1. *Assume $m \geqq 2$ for the rational integer m, and that I_s $(s = 1, 2, \ldots, m)$ is a finite set of proper ideals of a ring A with modular intersection $I_0 = \bigcap_{s=1}^{m} I_s$ and satisfying $I_s + I_t = A$ for every $s \neq t$. Then, for any system*

$$x_1, x_2, \ldots, x_m$$

of elements of A there exists an element $x_0 \in A$ with (*) $x_0 - x_s \in I_s$ for every $s (1 \leqq s \leqq m)$ and for another y_0 satisfying (*) instead of x_0 the inclusion $X_0 - y_0 \in I_0$ holds.

Proof. By the modularity of I_0 there exists an element $e \in A$ with $x - ex \in I_0 \subseteq I_s$ for every $x \in A$ and every $s (1 \leqq s \leqq m)$, thus every I_s is also modular in A.

Furthermore, by our assumptions, for the case $s \neq t$ one has $I_s + I_t = A$, and therefore

$$A^{m-1} = \prod_{\substack{t=1 \\ t \neq s}}^{m} (I_s + I_t) \subseteq I_s + \prod_{\substack{t=1 \\ t \neq s}}^{m} I_t \subseteq A. \tag{1}$$

But by $x - e x \subseteq I_0$ for every $x \in A$ we obtain $x \in ex + I_0 \subseteq A^2 + I_0$, consequently $A = A^2 + I_0$ and by repetition $A = A^k + I_0$ for every exponent k. Therefore, by (1) and $I_0 \subseteq I_s$ one has evidently

$$A^{m-1} + I_0 \subseteq I_s + \prod_{\substack{t=1 \\ t \neq s}}^{m} I_t \subseteq A = A^{m-1} + I_0 \tag{2}$$

which yields

$$(3) \qquad A = I_s + \prod_{\substack{t=1\\ t\neq s}}^{m} I_t \qquad \text{for every } s(1 \leqq s \leqq m)$$

Let the ideal $\prod_{\substack{t=1\\ t\neq s}}^{m} I_t$ be denoted by K_s. Then by $A = I_s + K_s$ obviously there exist elements $i_s \in I_s$ and $k_s \in K_s$ provided that

$$(4) \qquad e = i_s + k_s \text{ for every } s(1 \leqq s \leqq m).$$

For any fixed element i_0 of I_0 we consider the following sums

$$(5) \qquad x_0 = \sum k_s x_s \quad \text{and} \quad y_0 = x_0 + i_0$$

Then $x_0 - y_0 \in I_s$ trivially holds for every s, and if, conversely, we have $x_0 - y_0 \in I_s$ for every s, then $x_0 - y_0 \in I_0$. Furthermore, by a routine calculation, we obtain

$$(6) \qquad x_0 - x_s = \sum_{\substack{t=1\\ t\neq s}}^{m} k_t \cdot x_t + (k_s x_s - x_s) \in I_s$$

being

$$\sum_{\substack{t=1\\ t\neq m}}^{m} k_t \cdot x_t \in I_s$$

by

$$k_t \in K_t = \prod_{\substack{s=1\\ s\neq t}}^{m} I_s \subseteq \bigcap_{\substack{s=1\\ s\neq t}}^{m} I_s \subseteq I_s$$

and

$$k_s x_s - x_s \in I_s$$

by the assumed modularity of $I_s \supseteq I_0$ and by $k_s = e - i_s$.

This completes the proof of Theorem 1.

REMARK 1. For commutative principal ideal rings with unity and without divisors of zero, the Chinese residue theorem can be easily deduced from Theorem 1; since every ideal is principal, and $(i_s) + (i_t) = A$ is equivalent with $(i_s, i_t) = 1$, it results that the elements i_s and i_t are relatively prime. An important particular case is that of the ring of rational integers, and for the Chinese residue theorem in this particular case, cf. e.g. L. Rédei [16], Theorem 332 and its Corollary (p. 332 of the book).

REMARK 2. From the point of view of a symmetry, the proof of the former theorem is somewhat similar to the proof of the well-known, old formula of Lagrange's interpolation from the classical analysis and to that of Jacobson's density theorem for primitive rings from the abstract ring theory. (Cf. [7], [13], respectively [4], [10]).

Problem 1. Does there exist a ring A with $x + x \neq 0$ for an element $X \in A$ and with a nonmodular intersection of two modular right ideals?

Problem 2. Give a necessary and sufficient condition, that the intersection of every two modular right ideals of a ring be also modular!

Problem 3. Does there exist a ring with a nonmodular intersection of two modular (twosided) ideals?

Problem 4. Investigate the analogue of Problems 2, and 3 for semigroups having zero! (Modular right ideals for these cases were introduced by H. J. Hoehnke [8], [9]. See [22]).

THEOREM 2. An arbitrary (associative) ring A is isomorphic to the ring I of rational integers if and only if A satisfies the following four conditions:

(C_1) A is infinite;

(C_2) A cannot be decomposed into the direct sum of proper twosided ideals;

(C_3) A contains a nonzero idempotent right ideal R, that is $R^2 = R \neq 0$;

(C_4) every finitely generated proper subring S in A is a principal right ideal of A.

For the proof of Theorem 2 we discuss some preliminary propositions.

PROPOSITION 1. For any element a of a ring A with condition (C_4) there exist rational integers $n_i \in I$ satisfying

$$a^3 = n_1 a^2 + n_2 a^4 + \ldots + n_k a^{2k}.$$

Proof is by $(a)_r = \{a\} + aA \subseteq \{a\}$ and $a^3 = a^2 \cdot a \in \{a^2\}$ trivial, where $\{\ \}$, $(\ )_r$ denote the subring and right ideal, respectively, generated by the elements in the brackets.

PROPOSITION 2. If the additive group A^+ of a ring A with condition (C_4) is divisible (cf. Kaplansky [12]), then $A^2 = 0$ and A^+ either is isomorphic to the whole group of rational numbers, or $A^+ \cong \sum \oplus C\ (p^\infty)$ for different prime numbers p, denoting $C(p^\infty)$ the Prüfer's quasicyclic group.

Proof. By Proposition 1 there exists a rational integer $n_k \neq 0$ such that the additive group $\{n_k a\}^+$ of the subring $\{n_k a\}$ is a direct sum of finite number of cyclic groups. By condition (C_4) the subgroup $\{n_k a\}^+$ contains the divisible endomorphic image $n_k a A^+$ of the group A^+, consequently $n_k a A = 0$, and by the divisibility $n_k A = A$, therefore $aA = 0$ and $A^2 = 0$, being a an arbitrary element of A. By condition (C_4) the group A^+ must be locally cyclic, which already implies our assertions.

PROPOSITION 3. Assume that the ring A with conditions (C_3) and (C_4) is generated by a single element $a \in A$, and that its additive group A^+ is torsionfree. Then A is isomorphic with the ring I of rational integers.

Proof. By Proposition 2 the group A^+ cannot be divisible, therefore there exists a natural number $n (\neq 0)$ with $nA \neq A$. Thus $\{na\}$ is a proper subring of $A = \{a\}$, being $\{na\} \subseteq n\{a\}$. The trivial relation $na^2 = na \cdot a \in \{na\}$ implies by Proposition 1 and the torsion-freeness of A^+, that the additive group of the subring $\{a^2\}$ is cyclic. Consequently there exists a rational integer d satisfying $a^3 = d \cdot a^2$. Introducing $b = na$ and $S = \{b^2, nb\}$, we have $b^3 = ndb^2$ and $S = \{s\}$ with the form

$$s = j_1 b^2 + j_2 nb$$

where j_1 and j_2 denote suitable rational integers. Assuming, indirectly, that $\{a\}^+$ is not a cyclic group, there exist rational integers l_1 and l_2 satisfying

$$b^2 = l_1(jb^2 + nb^2) + l_2(jb^2 + nb)^2,$$

whence one has $1 = l_2 n^2 \cdot (j \cdot d + 1)^2$, $n = +1$ or $n = -1$ contradicting $nA \neq A$. Therefore, A^+ must be cyclic.

PROPOSITION 4. Assume that A is a ring with conditions (C_3) and (C_4), having a torsionfree additive group A^+. Then A is isomorphic with the ring I of the rational integers.

Proof. A^+ is not divisible by Proposition 2 and by condition (C_3); thus, there exists an integer $n \neq 0$ with $nA \neq A$. Let X and y be arbitrary elements of A. Then the subring $S = \{nx, ny\}$ is proper in A, and also S satisfies condition (C_4). Therefore $S = \{s\}$ for a suitable element $s \in S$ and by Proposition 3 and by the torsion-freeness, S^+ is cyclic. Consequently A^+ is a torsionfree group of rank one. By condition (C_3) we have $A^2 \neq 0$, consequently A is isomorphic with a subring B of the rational number field K_0. Let b be an element of $B \subseteq K_0$. If b is not a rational integer, then the additive group $\{b\}^+$ of the subring $\{b\}$ is noncyclic, consequently $A \cong B \subseteq I \subset K_0$, and by the condition (C_3) also $A \cong B \cong I$.

The proofs of the following important propositions are almost trivial, and therefore we omit their verifications.

PROPOSITION 5. Assume that $A = \{a\}$ is a nilpotent ring with conditions (C_4) and $pA = 0$ for a prime number p. Then $a^3 = 0$.

PROPOSITION 6. Assume that $A = \{a\}$ is a non-nilpotent ring with conditions (C_4) and $pA = 0$ for a prime number p. Then A^3 is a prime field, and the number $|A|$ of elements of A is a divisor of p^3.

PROPOSITION 7. Every finite ring A with condition (C_4) can be generated by two elements.

PROPOSITION 8. If the additive group A^+ of a finite nilpotent ring A with condition (C_4) is a p-group with $pA^+ \neq 0$ for a prime number p, then A^+ is cyclic.

Proposition 9. Assume that the additive group A^+ of a finite non-nilpotent ring A with condition (C_4) is a p-group and $pA^+ \neq 0$ for a prime number p. Then either A^+ is cyclic, or $A = \{a\}$ satisfying:

$$a \cdot (a^2 - p^f \cdot a) = a^2 - p^f \cdot a,$$

$$O(a) = p^k, \quad O(a^2 - p^f \cdot a) = p,$$

$$k \geqq 2, \quad 1 \leqq f \leqq k, \quad k \in I, \quad f \in I$$

Proposition 10. Assume that the ring A with condition (C_4) can be generated by a single element a, and that the additive group A^+ of A is mixed. Then a can be taken such that $A = \{a\}$ satisfying

$$a.(a^2 - m.l.a) = a^2 - m.l.a, \quad O(a^2 - m.l.a) = m$$

with a quadrat-free rational integer m and arbitrary rational integer l. Moreover, $A = \{a^2 - m.l.a\} \oplus \{a - a^2 + m.l.a\}$ is a direct decomposition into proper twosided ideals.

Proof of Theorem 2. It is clear, that the ring I of rational integers satisfies (C_1), (C_2), (C_3) and (C_4). Conversely, let A be an arbitrary ring with the conditions (C_1), (C_2), (C_3) and (C_4), and we shall verify $A \cong I$.

Firstly assume that the additive group A^+ of A is a torsion group. Then A^+ is, by condition (C_2), a p-group, being any p-component of A^+ also an ideal of A. Let B be the ideal of A, generated by the set of all elements of order p of A^+. If the subring B is not finitely generated, then there exist elements $b_1, b_2, b_3, b_4 \in B$ such that $b_{i+1} \notin \{b_1, \ldots, b_i\}$ for $i = 1, 2$, and 3. For $B^* = \{b_1, b_2, b_3, b_4\}$ one has evidently $p^4 \mid\mid B^* \mid$, denoting $\mid Y \mid$ the order of Y. By $B^* \neq B$, $B^* = \{b^*\}$ and Propositions 5 and 6 one has $\mid B^* \mid\mid p^3$, which yields the contradiction $p^4 \mid p^3$. Therefore B is finitely generated, which implies by Propositions 1, 5 and 6, that B is finite.

Consequently A^+ is an Abelian p-group having a finite rank, and by condition (C_1) containing at least one $C(p^\infty)$. Since every element of $C(p^\infty)$ is a twosided annihilator of A, by (C_4) the group A^+ contains exactly one component $C(p^\infty)$ in every additive direct decomposition, that is, $A^+ = C_0 + C(p^\infty)$, where C_0 is finite p^k-bounded group. If $a \in C(p^\infty)$ and $O(a) = p^{k+1}$, then the subring $C = \{C_0, a\}$ is proper and finitely generated, therefore by Proposition 4 also $C = \{c\}$ with an element $c \in C$. Obviously, $C_0 \neq 0$ by condition (C_3). Furthermore, by Proposition 8 the ring C cannot be nilpotent, and by Proposition 9 one has

$$C = \{c^2 - p^f.c\} \oplus \{c - c^2 + p^f.c\},$$

where the first direct component is a prime field. But this yields also $A = \{c^2 - p^f.c\} \oplus C(p^\infty)$, contradicting condition (C_2). Therefore A^+ is not a torsion group.

If A^+ is torsionfree, then A is by Proposition 4 isomorphic with the ring I of rational integers.

Now assume that A^+ is a mixed Abelian group. Obviously, $A = \sum_{a \in A} \{a\}$ and by Proposition 10 also $\{a\} = \{e_a\} \oplus \{w_a\}$ where the order $O(e_a)$ is a quadrat-free natural number, and w_a is of infinite order. Eventually also $e_a = 0$ or $w_a = 0$ can occur. Furthermore, in any case, $e_a^2 = e_a$. If $T_A = \sum_{a \in A} \{e_a\}$ and $W_A = \sum_{a \in A} \{w_a\}$ then T_A is a torsion (two-sided) ideal and W_A is a torsions-free right ideal with $W_A \cdot T_A = 0$. Assume, that $T_A \cdot W_A \neq 0$. Then there exist $t \in T_A$ and $w \in W_A$ with $t \cdot w \neq 0$, and the subring $S = \{t, w\}$ cannot be commutative. Consequently $S = A$.

There exists an idempotent $e \in A$, $e^2 = e$, with $ew \neq 0$, $we = 0$, $ew = ke$, $k \in I$ and $O(e)$ is a quadrat-free natural number. Since the maximal quadrat-free divisors of k^2 and k coincide, by $k^2 e = (ke)^2 = e(wc)\, w = 0$ one has nevertheless $ke = ew = 0$. Therefore $A = T_A \oplus W_A$ is a direct decomposition into proper ideals, contradicting condition (C_2).

This completes the proof of Theorem 2.

REMARK 3. Taking one of the conditions (C_1), (C_2), (C_3) or (C_4), the other three conditions do not characterize the ring I of the rational integers, as the following four examples show:

$$I/(p^k), \quad C(p^\infty) \oplus I/(p), \quad 2I, \quad K_0$$

Problem 5. Give an essentially shorter but completely elementary proof of Theorem 2!

Problem 6. Give a proof for Theorem 2 without group theoretical methods! (This may be also not elementary).

Received October 15, 1969

Institute of Mathematics
of the Academy of Sciences
Budapest, Hungary

REFERENCES

1. D. BARBILIAN, *Teoria aritmetica a Idealelor*. Ed. Acad., Bucharest, 1956.
2. — *Grupuri cu Operatori*. Ed. Acad. Bucharest, 1960.
3. I. BUCUR, *Algebra homologică*. Ed. Didactica şi Pedagogica, Bucharest, 1965.
4. N. DIVINSKY, *Rings and Radicals*. London, 1965.
5. S. EILENBERG and N. STEENROD, *Foundations of Algebraic Topology*. University Press, Princeton, 1952.
6. H. HASSE, *Zahlentheorie*. Akademie Verlag, Berlin, 1963.
7. CH. HERMITE, *Sur la formule d'interpolation de Lagrange*. Journal f. reine u. angew. Math. 1878, **84**, 70.
8. H. J. HOEHNKE, *Zur Strukturtheorie der Halbgruppen*. Math. Nachrichten, 1963, **26**, 1–13.
9. — *Structure of semigroups*. Canadian J. Math. 1966, **18**, 449–491.
10. N. JACOBSON, *Structure of Rings*, 2nd ed. Providence, 1964.

11. ION D. ION, *Radicalul limitei proiective de inele asociative.* St. Cercet. Mat. Bucharest, 1964, **16** : *9*, 1141–1145.
12. J. KAPLANSKY, *Infinite Abelian Groups.* Ann. Arbor, Michigan, 1954.
13. J. L. LAGRANGE, *Leçons élémentaires sur les mathématiques.* École Normale, 1795, Œuvres 7, p. 284–287.
14. J. LAMBEK, *Lectures on Rings and Modules.* Massachusetts, Toronto, London, 1966.
15. N. H. McCOY, *The Theory of Rings.* MacMillan, New York, 1964.
16. L. RÉDEI, *Algebra,* I (in English), Akadémiai Kiadó, Budapest, 1967.
17. O. STEINFELD, *Eine Charakterisierung der primitiven Ideale eines Ringes,* Acta Math. Acad. Sci. Hungar, 1968, **19**, 219–220.
18. F. SZÁSZ, *Lösung eines Problems bezüglich einer Characterisierung des Jacobsonschen Radikals,* Acta Math. Acad. Sci. Hungar. 1967, **18**, 261–272.
19. — *The sharpening of a result concerning primitive ideals of an associative ring.* Proc. Amer. Math. Soc., 1967, **18**, 910–912.
20. — *Die Lösung eines Problems bezüglich des Durchschnittes zweier modularer Rechtsideale in einem Ring.* Acta Math. Acad. Sci. Hungar, 1969, **20**, 211–216.
21. — *Simultane Lösung eines halbgruppentheoretischen und eines ringtheoretischen Problems.* Acta Sci. Math. Szeged, 1969, **30**, 289–294.
22. — *Radikalbegriffe für Halbgruppen mit Nullelement, die dem Jacobsonschen ringtheoretischen Radikal ähnlich sind.* Math. Nachrichten, 1967, **34**, 157–161.
23. D. ZELINSKY, *Linearly compact modules and rings,* Amer. J. Math., 1953, **75**, 79–90.