TIRAGE À PART
IDEALS OF A RING WITH MODULAR INTERSECTION

BY

FERENC A. SZÁSZ

(Budapest)

Dedicated to the memory of
Iván Sebest (1907–1966)

The present note deals with the theoretical side of topic bears rather the character of the number theory as 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 two-sided 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 two-sided unity element, a two-sided ideal and the Jacobson radical, respectively.

For the used notions we refer to D. Barbutian [2], I. Bucur [3], N. Divinsky [4], S. Eilenberg and N. Steenrod [5], H. Hasse [6], N. Jacobson [7], J. Kaplansky [9], 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 $\mathcal{F}$ 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 $x - x e \in R$ 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:

$$Q = \{x \in A; \text{ } Qx \subseteq R\}$$

REV. ROUM. MATH. PURES ET APPL., TOME XVI, N° 4, P. 509–510, BUCAREST, 1971
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 \( \mathcal{F} \) 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 \( n \), the existence of a ring \( A \) having \( n \) 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. Zelinskiy [23]. (For the definitions see [3] and [5]).

**Theorem 1.** Assume \( m \geq 2 \) 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 \( s (1 \leq s \leq m) \) 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 \( s (1 \leq s \leq m) \), 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

\[
A^{m-1} = \prod_{s=1}^{m} (I_s + I_t) \subseteq I_s + \prod_{s=1}^{m} I_t \subseteq A.
\]

But by \( x - ex \subseteq I_0 \) 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

\[
A^{m-1} + I_0 \subseteq I_s + \prod_{s=1}^{m} I_t \subseteq A = A^{m-1} + I_0.
\]

which yields

\[
A.
\]

Let the ideal \( \prod_{s=1}^{m} I_t \) there exist elements

For any fixed element

Then \( x_0 - y_0 \in I_s \)

have \( x_0 - y_0 \in I_s \)

routine calculation

being

by

and

by the assumed

This compl

**Remark:** and without div deduced from Th are relatively p of rational intei cular case, cf. e. of the book).
which yields

\[ A = I_1 + \bigoplus_{i=1}^{m} I_i \quad \text{for every } s(1 \leq s \leq m) \]

Let the ideal \( \bigoplus_{i=1}^{m} I_i \) be denoted by \( K_i \). Then by \( A = I_s + K_i \), obviously there exist elements \( i_s \in I_s \) and \( k_i \in K_i \) provided that

\[ e = i_s + k_i \quad \text{for every } s(1 \leq s \leq m). \]

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

\[ x_0 = \sum_{i=1}^{m} k_i x_i \quad \text{and} \quad y_0 = x_0 + i_0 \]

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 routine calculation, we obtain

\[ x_0 - x_s = \sum_{i=1}^{m} k_i x_i + (k_i x_s - x_s) \in I_s \]

being

\[ \sum_{i=1}^{m} k_i x_i \in I_s \]

by

\[ k_i \in K_i = \prod_{i=1}^{m} I_i \subseteq \bigcap_{i=1}^{m} I_i \subseteq I_s \]

and

\[ k_i x_s - x_s \in I_s \]

by the assumed modularity of \( I_s \supseteq I_0 \) and by \( k_i = e - i_s \).

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 \( (i_i) + (i_s) = A \) is equivalent with \( (i_s, i_i) = 1 \), it results that the elements \( i_s \) and \( i_i \) 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 [18], 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 $x + x = 0$ 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, 3 for semigroups having zero! (Modular right ideals for these cases were introduced by H. J. Heinecke [3], [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:

(a) $A$ is infinite;
(b) $A$ cannot be decomposed into the direct sum of proper twosided ideals;
(c) $A$ contains a nonzero idempotent right ideal $R$, that is $Ra = a = R 
eq 0$;
(d) 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) there exist rational integers $n, a \in I$ satisfying

$$a^2 = na + n_2a^2 + \ldots + n_ka^k.$$  

Proof. is by $(a_i) = [a_i] + a_iA \subset [a_i]$ and $a^2 = a^2 \cdot a_i \in [a^2]$, trivial, where $\{a_i\}$, $(\cdot)$, 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) is divisible (cf. Kaplansky [12]), then $A^2 = 0$ and $A^+$ either is isomorphic to the whole group of rational numbers, or $A^+ = \Sigma \oplus C(p^\infty)$ for different prime numbers $p$, denoting $C(p^\infty)$ the Prüfer's quasicyclic group.

Proof. By Proposition 1 there exists a rational integer $n_0 \neq 0$ such that the additive group $\{n_0a\}^+$ of the subring $\{n_0a\}^+$ is a direct sum of finite number of cyclic groups. By condition (C) the subgroup $\{n_0a\}^+$ contains the divisible endomorphism image $n_0A^+$ of the group $A^+$, consequently $n_0aA = 0$, and by the divisibility $n_0A = A$, therefore $A^2 = 0$ and $A^2 = 0$, being $a$ an arbitrary element of $A$. By condition (C) the group $A^+$ must be locally cyclic, which already implies our assertions.

**Proposition 3.** The group $A^+$ is torsion.

Proof. By there exists a proper subring $na^2 = na \cdot a \in (n)$ of $A^+$, that is the there exists a $n = na$ and $S = S_n n = 0$.

whence one has $nA \neq A$. Then $A = nA_n.$

Proposition.

and (C), have with the ring $A$

Proof. $A$

(C) $A$; thus, the arbitrary elem $A$, and also $A$ element $s \in S$

cyclic. Conse$\Rightarrow$

were of the ratios $b$ is not a ratio

(b) is noncyclic (C) a

The pro$\Rightarrow$

vial, and ther

Pronoun

conditions (C)

Pronoun

with condition prime field, at

Pronoun

generated by

Pronoun

ring $A$ with co

then $A^+$ is $\infty$.
propriety, the proof of
the well-known
sential analysis and
s from the abstract
\( \alpha \neq 0 \) for an ele-
two modular right
ion, that the inter-
be also modular!
ods of intersection
ms 2, and 3 for
these cases were
is isomorphic to
the following four

n of proper twosi-
i 1, that is \( R^2 =
1 \) \( A \) is a principal

eliminary proposi-
A with condition

\( a^2, a \in \{ a^2 \} \) trivial,
respectively, gene-
ring \( A \) with con-
\( A^+ \cong \Sigma \oplus C (p^\infty) \n\) \( a^2 \) is a direct sum
egroup \( \{ a \} \) the
condition \( (C_0) \) the

Proposition 3. Assume that the ring \( A \) with conditions \((C_0)\) and
\((C_2)\) is generated by a single element \( a \in A \), and that its additive
\( A^+ \) is torsionfree. Then \( A \) is isomorphic with the ring \( I \) of rational
\( A^+ \) 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 \( a^2 = da \cdot a^2 \). Introducing \( b =
na \) and \( S = \{ b^2, nb \} \), we have \( b^2 = nb^2 \) 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
\[ b^2 = l_1(j_1 b^2 + nb^2) + l_2(j_2 b^2 + nb^2), \]
whence one has \( 1 = l_2 n^2, (j_1 d + 1)^2, n = +1 \) or \( n = -1 \) contradicting
\( nA \neq A \). Therefore, \( A^+ \) must be cyclic.

Proposition 4. Assume that \( A \) is a ring with conditions \((C_0)\) and
\((C_0)\); thus, there exists an integer \( n \neq 0 \) with \( nA \neq A \). Let \( X \) and \( y \) be
arbitrary elements of \( A \). Then the subring \( S = \{ xy, xy \} \) is proper in
\( A \), and also \( S \) satisfies condition \((C_0)\). Therefore \( S = \{ s \} \) for a suitable
\( s \in S \) and by Proposition 3 and by the torsion-freeness, \( S^+ \) is
cyclic. Consequently \( A^+ \) is a torsionfree group of rank one. By condition
\((C_0)\) we have \( A^2 \neq 0 \), consequently \( A \) is isomorphic with a subring of
the rational number field \( K \). Let \( b \) be an element of \( B \subseteq K \). If
\( b \) is not a rational integer, then the additive group \( \{ b \} \) of the subring
\( \{ b \} \) is none cyclic, consequently \( A \cong B \subseteq I \subseteq K \), and by the condition
\((C_0)\) also \( A \cong B \subseteq I \).

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

Proposition 5. Assume that \( A = \{ a \} \) is a nilpotent ring with
conditions \((C_0)\) 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 \((C_0)\) 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 \((C_0)\) can be
generated by three elements.

Proposition 8. If the additive group \( A^+ \) of a finite nilpotent
ring \( A \) with condition \((C_0)\) 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:

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

$$O(a) = p^n, \quad O(a^2 - p' \cdot a) = p,$$

$$k \geq 2, \quad 1 \leq f \leq k, \quad k \in I, \quad f \in I$$

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

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

with a quadratic-free rational integer $m$ and arbitrary rational integer $l$. Moreover, $A = \{a^2 - m \cdot l \cdot a\} \oplus \{a - a^3 + m \cdot l \cdot a\}$ 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 $(C_3)$, 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 $b_1, b_2, b_3$ such that $b_i = \{b_1, \ldots, b_i\}$ for $i = 1, 2, 3$. For $B^* = \{b_1, b_2, b_3, b_4\}$ one has evidently $p^4 | B^*$, denoting $Y$ the order of $Y$. By $B^* \neq B$, $B^* = \{b_4\}$ and Propositions 5 and 6 one has $|B^*| \leq p^3$, which yields the contradiction $p^4 | p^3$. 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 $C(p)$. Since every element of $C(p)$ is a twosided annihilator of $A$, by $(C_1)$ the group $A^+$ contains exactly one component $C(p^e)$ in every additive direct decomposition, that is, $A^+ = C_0 + C(p^e)$, where $C_0$ is finite $p^e$-bounded group. If $a \in C(p^e)$ and $O(a) = p^{e+1}$, then the subring $C = \{a, 0\}$ is proper and finitely generated, therefore by Proposition 4 also $C = \{0\}$. Consequently, by Proposition 8 the ring $C$ cannot be nilpotent, and by Proposition 9 one has

$$C = \{a^2 - p' \cdot c\} \oplus \{c - a^2 + p' \cdot c\},$$

where the first direct component is a prime field. But this yields also $A = \{a^2 - p' \cdot c\} \oplus C(p^e)$, contradicting condition $(C_1)$. 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, $A = \sum_{a \in A} \{a\} \text{ and by Proposition 10 also } a = \{a\} \oplus \{w\}$ where the order $O(e)$ is a quadratic form that is natural number, and $w$ is of infinite order. Eventually also $e_0 = 0$ or $w = 0$ can occur. Furthermore, in any case, $a = e$. If $T_A = \sum_{a \in A} \{a\}$ and $W_A = \sum_{a \in A} \{w\}$ then $T_A$ is a torsion (two-sided) ideal and $W_A$ is a two-sided ideal with $W_A \cap T_A = 0$. Assume that $W_A \neq 0$. Then there exist $t \in T_A$ and $w \in W_A$ with $t \cdot w = 0$, and the subring $S = \{t, w\}$ cannot be commutative. Consequently $S = A$.

There exists an idempotent $e \in A$, $e^2 = e$, with $e \cdot w = 0$, $w = 0$, $e \cdot w = k$, $k = 0$ and $O(e)$ is a quadratic form that is natural number. Since the maximal quadratic form that is natural number with $k^2$ and $k$ coincide, by $k \cdot e = (k \cdot e)^2 = e \cdot (w \cdot w) = 0$ one has nevertheless $k \cdot e = e \cdot w = 0$. Therefore $A = T_A \oplus W_A$ is a direct decomposition into proper ideals, contradicting condition (C).

This completes the proof of Theorem 2.

Remark 3. Taking one of the conditions (C), (C), (C) or (C), the other three conditions do not characterize the ring $I$ of the rational integers, as the following four examples show:

$$I/(p^k), \quad C(p^m) \oplus I/(p), \quad 2I, \quad A$$

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 25, 1959

Institute of Mathematics
of the Academy of Sciences
Budapest, Hungary

REFERENCES