On the extension of rings without divisors of zero.

By J. SZENDREI in Szeged.

It is known that any ring R can be imbedded in another ring $\bar{R}$ with unit element. But this extension may contain divisors of zero, although the original does not contain any. The following question has been arisen by T. SZELE: If the original ring contains no divisors of zero, is it possible to find an extension $\bar{R}$ with unit element containing no divisors of zero?[1]) The question is — to our knowledge — unsolved in general so far. The subject of this paper is to solve this problem.

It is well-known that in the case of commutative rings such an extension is always possible. In this case R is an integral domain and so R can be imbedded in a field of quotients. MALCEV[2]), however, has shown that this does not hold in the noncommutative case.

We shall prove the following

Theorem: *Let R be an arbitrary ring without divisors of zero. Then there exists one and only one ring $\bar{R}$ having the following properties:*

1. *$\bar{R}$ contains a unit element,*
2. *$\bar{R}$ contains no divisors of zero,*
3. *$\bar{R}$ is a minimal extension of R, that is, there is no proper subring of $\bar{R}$ which contains R and which possesses a unit element*[3]).

[1]) This problem is an instance of the question of the existence of ring extensions satisfying certain requirements. Another is the following problem, raised by L. RÉDEI and unsolved so far: Is there an extension of a given finite ring conserving the the invariants of its additive group?

[2]) A. MALCEV, On the immersion of an algebraic ring into a field, *Math. Annalen*, **113** (1937), 686—691.

[3]) In general, i. e. without condition 2, there exist more than one minimal extensions. For instance, the ring R of even integers has the following minimal extensions with a unit element:

1. the ring of all integers,
2. the ring of the elements of the from $\varrho+n\varepsilon$ ($\varrho\in R$, n an integer), sum and product being defined by

$$(\varrho+n\varepsilon)+(\varrho'+n'\varepsilon)=\varrho+\varrho'+(n+n')\varepsilon,$$
$$(\varrho+n\varepsilon)(\varrho'+n'\varepsilon)=\varrho\varrho'+n\varrho'+n'\varrho+nn'\varepsilon.$$

Of these only the first extension has no divisors of zero. Hence, property 3 alone does not imply the uniqueness of the extension.

Moreover, we shall see that *R is an ideal in $\bar{R}$ and $\bar{R}/R$ is isomorphic to one of the homomorphic images of the ring I of all integers (that is, either to I or to one of the residue class rings $I/(d)$).*

First we make the following remarks.

All elements ($\neq 0$) of the additive group of R have the same prime order $p(\neq 1)$ where p is either a positive prime number or zero. In fact, if not all elements have infinite order there exists an element $\alpha(\neq 0)$ of prime order p. Then, for every element $\xi(\neq 0)$ of R, $\alpha p \cdot \xi = \alpha \cdot p\xi = 0$. Hence, by $\alpha \neq 0$, R having no divisors of zero, we have $p\xi = 0$.

If there exist an integer m and an element $\alpha \neq 0$ in R such that

(1) $$\alpha^2 = m\alpha,$$

then on account of $(-\alpha)^2 = (-m).(-\alpha)$ there exists even a positive m satisfying (1). Among the latter ones there is a least one which we shall denote henceforth by m, and at the same time let $\alpha \in R$ be for the future an element ($\neq 0$) satisfying (1) with this minimal m. If there are no such m and $\alpha(\neq 0)$, we shall put $m = 0$ and $\alpha = 0$. We note that not only m, but also α is uniquely determined. Indeed, if $\alpha \neq 0$, it follows from (1) that $\alpha^2\xi = m\alpha\xi$ for every element ξ of R, hence $\alpha\xi = m\xi$. If $\beta \neq 0$ is another element satisfying (1) with the same m, then we get similarly $\beta\xi = m\xi$. Hence $(\alpha-\beta)\xi = 0$ and supposing $\xi \neq 0$, we have $\alpha = \beta$, as stated.

Now we are going to prove the theorem.

If $d = (p, m) = 1$, then this implies the existence of an m' with $mm' \equiv 1 \pmod{p}$. Let us consider the element $\beta = m'\alpha (\neq 0)$ of R. Then by

$$\beta^2 = (m'\alpha)^2 = m'^2\alpha^2 = m'^2 m\alpha = m'\alpha = \beta.$$

β is a unit element in R. For ξ denoting an arbitrary element in R we have $\xi\beta^2 = \xi\beta$, hence $\xi\beta = \xi$. Likewise it may be shown that $\beta\xi = \xi$. Consequently it is unnecessary to extend the ring.

Henceforth we suppose $d \neq 1$.

Let us consider the set $\bar{S}$ of the equivalence classes of all symbols of the form (ϱ, n) ($\varrho \in R$, n integer) with regard to the equivalence relation $(\varrho, n) \sim (\varrho', n')$ defined by

$$n - n' = td \qquad \varrho' - \varrho = t\alpha \qquad (t \text{ integer}).$$

We define addition and multiplication in $\bar{S}$ by the rules

$$(\varrho, n) + (\varrho'. n') = (\varrho + \varrho', n + n'),$$
$$(\varrho, n)(\varrho', n') = (\varrho\varrho' + n\varrho' + n'\varrho, nn').$$

It is clear that $\bar{S}$ is a ring with $(0, 1)$ as unit element. The correspondence $(\varrho, 0) \leftrightarrow \varrho$ defines an isomorphism between a subring of $\bar{S}$

and the ring R. Since R and $\bar{S}$ have no elements in common and $\bar{S}$ contains a subring isomorphic to R, the well-known theorem of imbedding leads us to a ring $\bar{R}$ which contains R and which is isomorphic to $\bar{S}$ such that under this isomorphism we have

$$(\varrho, 0) \leftrightarrow \varrho.$$

Suppose we have under the same isomorphism

$$(0, 1) \leftrightarrow \varepsilon$$

with $\varepsilon \in \bar{R}$, then we have in general

$$(\varrho, n) \leftrightarrow \varrho + n\varepsilon. \tag{2}$$

In the ring $\bar{R}$ we add and multiply in the following way with regard to $m\varepsilon = \alpha$ (if m, α are zero, this says nothing):

$$(\varrho + n\varepsilon) + (\varrho' + n'\varepsilon) = \varrho + \varrho' + (n + n')\varepsilon.$$
$$(\gamma + n\varepsilon)(\varrho' + n'\varepsilon) = \varrho\varrho' + n\varrho' + n'\varrho + nn'\varepsilon.$$

We prove that $\bar{R}$ has no divisors of zero.

If $m = 0$, that is, only the zero element satisfies (1) then assume

$$(\varrho + n\varepsilon)(\varrho' + n'\varepsilon) = 0. \tag{3}$$

Hence $\varrho\varrho' + n\varrho' + n'\varrho = 0$ and $nn'\varepsilon = 0$. The latter implies either $n = 0$ or $n' = 0$; suppose $n = 0$, say. Thus $\varrho\varrho' + n'\varrho = 0$.

a) If also $n' = 0$, then $\varrho\varrho' = 0$, consequently $\varrho = 0$ or $\varrho' = 0$, that is, either $\varrho + n\varepsilon = 0$ or $\varrho' + n'\varepsilon = 0$.

b) If $n' \neq 0$, we show $\varrho = 0$. Indeed, if $\varrho \neq 0$, then $\varrho\varrho' = n'(-\varrho)\ (\neq 0)$, $\varrho\varrho'^2 = n'(-\varrho)\varrho'$, hence $(-\varrho')^2 = n'(-\varrho)$, this contradicts the hypothesis.

Consequently one of the factors in (3) must be zero.

Finally let us consider the case $m > 1$ and $p = 0$. Since $m\varepsilon = \alpha$, the elements of $\bar{R}$ are of the form $\varrho + n\varepsilon$ with $0 \leqq n \leqq m - 1$. Supposing

$$(\varrho + n\varepsilon)(\varrho' + n'\varepsilon) = 0 \qquad (0 \leqq n, n' \leqq m - 1) \tag{4}$$

we shall prove that one of the factors must be zero. We have by (4) with regard to $m\varepsilon = \alpha$

$$m(\varrho + n\varepsilon)\, m(\varrho' + n'\varepsilon) = (m\varrho + n\alpha)(m\varrho' + n'\alpha) = 0.$$

Since both factors belong to R, one of them is zero. Assume, for example, $m\varrho + n\alpha$. Then

$$m\varrho\alpha + n\alpha^2 = m\varrho\alpha + nm\alpha = m(\varrho\alpha + n\alpha) = 0$$

implies, p being zero, that

$$\varrho\alpha + n\alpha = 0, \tag{5}$$
$$\varrho^2\alpha + n\varrho\alpha = (\varrho^2 + n\varrho)\alpha = 0,$$

hence, by $\alpha \neq 0$, $\varrho^2 + n\varrho = 0$, that is

$$(-\varrho)^2 = n(-\varrho) \qquad (0 \leqq n \leqq m - 1).$$

This is a contradiction to the minimality of m. Therefore $\varrho=0$ and $n=0$, that is, $\varrho+n\varepsilon=0$ which proves our statement.

In order to prove property 3 in the theorem, let us consider an extension $\overline{\overline{R}}$ (with the unit element ε_1 and without divisors of zero) of R. Condition (1), i. e. $\alpha^2=m\alpha=m\varepsilon_1\alpha$, implies $\alpha=m\varepsilon_1$. If $m>0$, m is the least positive integer with this property, for if we had $\alpha=m_1\varepsilon_1$ with $0<m_1<m$, then $\alpha^2=m_1\varepsilon_1\alpha=m_1\alpha$ would contradict the minimality of m in (1). The equation $\alpha=m\varepsilon_1$ defines the same rules of counting in the set $\overline{\overline{R}}_1$ of all elements of the form $\varrho+n\varepsilon_1$ ($\varrho\in R$, n an integer) as the rules in $\overline{R}$. Hence the one-to-one correspondence defined by $\varepsilon_1\longleftrightarrow\varepsilon$ is an isomorphism between $\overline{\overline{R}}_1$ and R. If $\overline{\overline{R}}$ is also a minimal extension, then $\overline{\overline{R}}=\overline{\overline{R}}_1\approx\overline{R}$ which implies the uniqueness of the extension.

Finally, it is clear that R is an ideal in $\overline{R}$. Furthermore it is easy to see that $\overline{R}/R\approx I/(d)$. In fact, in case $d=1$, $\overline{R}/R\approx 0$ which shows that it is unnecessary to extend. In the case $m=0$ if $p=0$, $\overline{R}/R\approx I$, and if $p>1$, $\overline{R}/R\approx I/(p)$. Finally, in the case $m>1$ and $p=0$, $\overline{R}/R\approx I/(m)$.

(Received August 24, 1950.)