Square extensions of finite rings

By L. C. A. VAN LEEUWEN in Chicago (Illinois, U.S.A.)*)

Let R and S be rings. We say that a ring T is an *extension of S by R* if S is an ideal in T and T/S is isomorphic to R. Let us call an extension T of S by R a *square extension*, if $S=T^2$, where T^2 is the ideal in T generated by all products of elements of T. Now T/T^2 is a zero-ring, so in order that there exist a square extension of S by R, R must be a zero-ring. Henceforth we assume that R is a zero-ring and moreover that R is a finite ring. On the other hand, if S^2 is the ideal in S generated by all products of elements in S, then S/S^2 is a zero-ring. We assume that S/S^2 is also finite. Our problem is to find necessary and sufficient conditions for the existence of a square extension of S by R. We shall reduce this problem to the case in which the additive group of S is a finite abelian elementary p-group and S is a zero-ring. In Theorem 4 we get the result that there does not exist a split square extension of S by R. Next we get a partial result on the existence of non-split square extensions of S by R (Theorem 5). Finally we determine all rings of order 8, which may occur either as a square extension of a ring of order 4 or as a square extension of a ring of order 2.

First we note that the ideal S^2 of S is an ideal not only in S, but also in every extension of S, since S^2 is a characteristic subring of S.

Theorem 1. *T is a square extension of S by R if and only if T/S^2 is a square extension of S/S^2 by R.*

Proof. From the isomorphism $T/S \cong T/S^2/S/S^2$ it follows that T is an extension of S by R if and only if T/S^2 is an extension of S/S^2 by R. Now suppose $T^2=S$, then $(T/S^2)^2=T^2/S^2=S/S^2$. Conversely, if $S/S^2=(T/S^2)^2$, then $S/S^2=T^2/S^2$ and hence $S=T^2$. This theorem reduces the problem to the case in which S is a finite zero-ring.

If $S=(0)$, then every extension T of S by R is a square extension because R is a zero-ring. Therefore, we assume that S is a non-trivial finite zero-ring. At this

*) This research has been supported by the National Science Foundation (GP-6539).

point we want to summarize the theory of extensions of S by R, where R and S are finite zero-rings. Let T be an extension of S by R, so that $T/S\cong R$. Let φ: $T\to R$ be the epimorphism whose kernel is S. An element $\bar{u}$ of T is called a *representative* of $u\in R$ if $\varphi(\bar{u})=u$. Let $(z_1, \dots, z_l)$ be a basis of the additive group R^+ of R and let m_i be the order of z_i. An l-tuple $(\bar{z}_1, \dots, \bar{z}_l)$ is called a *representative set* of the basis if each $\bar{z}_i$ is a representative of z_i. As the products $\bar{z}_i a$, $a\bar{z}_i\,(a\in S)$ are all in S, the mappings $a\to\bar{z}_i a$, $a\to a\bar{z}_i$ are endomorphisms of S^+, which will be denoted by $\eta_l(z_i)$ and $\eta_r(z_i)$ resp. Thus $\eta_l(z_i)a=\bar{z}_i a$ and $a\eta_r(z_i)=a\bar{z}_i$.

It is clear that if we choose another representative of $z_i\in R$, for instance $\bar{z}_i'$, then $\bar{z}_i'a=\bar{z}_i a$ and $a\bar{z}_i'=a\bar{z}_i$, as $\bar{z}_i'=\bar{z}_i$ (mod S) and S is a zero-ring. Hence the induced endomorphisms are completely determined by the element $z_i\in R$. So we get a set of $2l$ endomorphisms of S^+ and we divide them into pairs: $(\eta_l(z_1), \eta_r(z_1))$, $(\eta_l(z_2), \eta_r(z_2))$, $\dots$, $(\eta_l(z_l), \eta_r(z_l))$. Each of these pairs is a double homothetism of S, since S is a zero-ring and the endomorphisms $\eta_l(z_i)$ and $\eta_r(z_i)$ are commuting. As T is an associative ring these double homothetisms are pairwise related (cf. [2]). Now we consider the mapping: $z_i\to\eta(z_i)=(\eta_l(z_i), \eta_r(z_i))$, which associates with each $z_i\in R$ the corresponding double homothetism of S and we extend η by linearity. We claim that η is a homomorphism of R into a maximal ring D of related double homothetisms of S. First we remark that if $\bar{z}_i$ and $\bar{z}_j$ are arbitrary representatives in T then $\bar{z}_i\bar{z}_j\in S$, as $\varphi(\bar{z}_i\bar{z}_j)=\varphi(\bar{z}_i)\varphi(\bar{z}_j)=z_iz_j=0$. Hence $\bar{z}_i(\bar{z}_ja)=$ $=\eta_l(z_i)(\eta_l(z_j)a)=0$ for all $a\in S$. This implies $\eta_l(z_i)\eta_l(z_j)=$ zero-endomorphism for all $z_i, z_j\in R$. In the same way it can be shown that $\eta_r(z_i)\eta_r(z_j)=$ zero-endomorphism for all $z_i, z_j\in R$. As the product of the double homothetisms $(\eta_l(z_i), \eta_r(z_i))(\eta_l(z_j), \eta_r(z_j))=(\eta_1(z_i)\eta_l(z_j), \eta_r(z_i)\eta_r(z_j))=(0, 0)$ in D, it follows that the mapping η maps R homomorphically into a ring D; the homomorphic image $\eta(R)$ is a zero-subring of a maximal ring of related double homothetisms of S. As we saw earlier each product $\bar{z}_i\bar{z}_j\in S$; we define $\bar{z}_i\bar{z}_j=\{z_i, z_j\}$ for all i, j with $1\leqq i\leqq l$, $1\leqq j\leqq l$; the elements $\{z_i, z_j\}$ are called a *multiplicative factor set.* Finally we know that $m_i\bar{z}_i\in S$, as $\varphi(m_i\bar{z}_i)=m_iz_i=0$. So we get another set of elements $m_i\bar{z}_i=b_i$ in S.

It is easy to check that the homomorphism η, the multiplicative factor set $\{z_i, z_j\}$ and the set $\{b_i\}$ have the following properties:

(1) $\{z_i, 0\}=\{0, z_j\}=0$, if 0 is a representative of $0\in R$.

(2) $\eta_l(z_i)\{z_j, z_k\}=\{z_i, z_j\}\eta_r(z_k)$,

(3) $(b_i)\eta_r(z_j)=m_i\{z_i, z_j\}$,

(4) $\eta_l(z_j)(b_i)=m_i\{z_j, z_i\}$, for all $z_i, z_j, z_k\in R, b_i\in S$, m_i as integers.

Hence given an extension T of S by R, T determines with the representative set $(\bar{z}_1, \dots, \bar{z}_l)$ a homomorphism η of R into a maximal ring of related double homothetisms of S, a multiplicative factor set $\{z_i, z_k\}$ and a set $\{b_i\}$ $(b_i\in S)$, such that the properties (1)—(4) are satisfied.

Conversely, assume that R and S are given finite zero-rings and that $\eta: R\to D$ is a given homomorphism of R into a maximal ring D of related double homothetisms of S. Let the functions $\{z_i, z_j\}$ of $R\times R$ into S and the set $\{b_i\}$ ($b_i\in S$) be given for all i, j with $1\leqq i\leqq l$, $1\leqq j\leqq l$, such that (1)—(4) hold. Consider the set of all symbols $\sum_{i=1}^{l} n_i\bar{z}_i+s$, $0\leqq n_i<m_i$, $s\in S$. Define equality by: $\sum_{i=1}^{l} n_i\bar{z}_i+s=\sum_{i=1}^{l} u_i\bar{z}_i+v$ if and only if $n_i=u_i$ for all i and $s=v$. Define addition by: $\left(\sum_{i=1}^{l} n_i\bar{z}_i+s\right)+\left(\sum_{i=1}^{l} u_i\bar{z}_i+v\right)=$ $=\sum_{i=1}^{i}(n_i+u_i)\bar{z}_i+s+v$, where $m_i\bar{z}_i=b_i$ and the sum is reduced mod $m_i\bar{z}_i$. Define multiplication by:

$$\left(\sum_{i=1}^{l} n_i\bar{z}_i+s\right)\left(\sum_{i=1}^{l} u_i\bar{z}_i+v\right)=\sum_{i=1}^{l}\sum_{j=1}^{l} n_iu_j\{z_i, z_j\}+\sum_{i=1}^{l} n_i\big(\eta_l(z_i)v\big)+\sum_{j=1}^{l} u_j\big(s\eta_r(z_j)\big).$$

It is easy to check that the set T of all symbols $\sum_{i=1}^{l} n_i\bar{z}_i+s$ with the addition and multiplication just defined is a ring. Now $T^2\subseteq S$, hence S is an ideal in T and $T/S\cong R$ under $\sum_{i=1}^{l} n_i\bar{z}_i+S\to\sum_{i=1}^{l} n_iz_i$. Further $\bar{z}_iv=\eta_l(z_i)v\in S$, $v\bar{z}_i=v\eta_r(z_i)\in S$ for all $v\in S$, hence the double homothetisms $\eta(z_i)=\big(\eta_l(z_i), \eta_r(z_i)\big)$ of S are induced by inner double homothetisms $(\bar{z}_{i_l}, \bar{z}_{i_r})$ of T. So T is an extension of S by R which, with the representative set $\bar{z}_i$, induces the given homomorphism η. Since $\bar{z}_i\bar{z}_j=$ $=\{z_i, z_j\}$ for all i, j and $m_i\bar{z}_i=b_i$ for all i, T has, with the same representative set $\bar{z}_i$, the multiplicative factor set $\{z_i, z_j\}$ and the additive set $\{b_i\}$.

We call an extension T of S by R combined with the homomorphism $\eta: R\to D$, where D is some maximal ring of related double homothetisms of S, an η-extension of S by R.

Let T be any η-extension of S by R which has, for the representative set $\bar{z}_i$, the multiplicative factor set $\{z_i, z_j\}$ and the additive set $\{b_i\}$. Another representative set of T/S may be: $\bar{z}_1', \bar{z}_2', \dots, \bar{z}_l'$, where $\bar{z}_i'=\bar{z}_i+\psi_{z_i}$, $\psi_{z_i}\in S$ for $i=1, \dots, l$. Then $\bar{z}_i'\bar{z}_j'=(\bar{z}_i+\psi_{z_i})(\bar{z}_j+\psi_{z_j})=\{z_i, z_j\}+\eta_l(z_i)(\psi_{z_j})+(\psi_{z_i})\eta_r(z_j)$ and $m_i\bar{z}_i'=m_i(\bar{z}_i+\psi_{z_i})=$ $=b_i+m_i\psi_{z_i}$. Hence the new factor sets are

(5) $$\{z_i, z_j\}'=\{z_i, z_j\}+\eta_l(z_i)(\psi_{z_j})+(\psi_{z_i})\eta_r(z_j)$$

and

(6) $$b_i'=b_i+m_i\psi_{z_i}.$$

We shall call two factor sets $\{z_i, z_j\}$, $\{b_i\}$ and $\{z_i, z_j\}'$, $\{b_i\}'$ *equivalent* if there exists a mapping $\psi: R\to S(\psi_0=0)$ such that (5) and (6) hold. Hence any two factor sets corresponding to the same η-extension of S by R are equivalent.

On the other hand, we shall call two η-extensions T and T' of S by R *equivalent* (and write $T\sim T'$) if there exists an isomorphism $\alpha\colon T\to T'$ such that α is the identity on S and $\varphi=\alpha\varphi'$, where $\varphi\colon T\to R$ and $\varphi'\colon T'\to R$ are the epimorphisms whose kernels are S. With these definitions we get the result: Let T_1 and T_2 be two η-extensions of S by R. Then $T_1\sim T_2$ if and only if, for some choice of representative sets in T_1 resp. T_2, the corresponding factor sets $\{z_i, z_j\}_1$, $\{b_i\}_1$, resp. $\{z_i, z_j\}_2$, $\{b_i\}_2$ are equivalent. More explicitly, if T_k, with representative set $\{\bar z_i\}_k$, has the factor set $\{z_i, z_j\}_k$, $\{b_i\}_k$ $(k=1,2)$, then the isomorphism $\alpha\colon T_1\to T_2$ is given by $\left(\sum_{i=1}^{l} n_i(\bar z_i)_1+s\right)\alpha=\sum_{i=1}^{l} n_i(\bar z_i)_2+s+\sum_{i=1}^{l} n_i\psi_{z_i}$, where $\psi\colon R\to S$ $(\psi_0=0)$ is a mapping such that (5) and (6) hold for ψ and the factor sets. The proof is straightforward.

An η-extension T of S by R is said to be a *splitting extension* over S if and only if, for some choice of representative set, all $\{z_i, z_j\}$ are 0 and all b_i are 0. Also, $T=S\oplus R$ (ringtheoretical direct sum) if and only if T is a 0-extension of S by R $(\eta=0)$ and, for some choice of representative set, all $\{z_i, z_j\}$ are 0 and all b_i are 0. The direct sum extension is a zero-ring, since R and S are supposed to be zero-rings.

Let T be an η-extension of S by R. A subring K of S is an ideal in T if and only if K is invariant under the double homothetisms of S, which occur as images in $\eta\colon R\to D$. Now the $\eta(z_i)=(\eta_l(z_i), \eta_r(z_i))$ are double homothetisms of K and T/K is an η^*-extension of S/K by R. If $\eta\colon R\to D$ is such that $\eta(z_i)=(\eta_l(z_i),\eta_r(z_i))$ then $\eta^*\colon R\to D^*$, where D^* is a maximal ring of related double homothetisms of S/K, is defined by $\eta^*(z_i)=(\eta_l^*(z_i), \eta_r^*(z_i))$, where $\eta_l^*(z_i)(s+K)=\eta_l(z_i)s+K$ and $(s+K)\eta_r^*(z_i)=s\eta_r(z_i)+K$. Since K is invariant in $\eta(R)$, this definition does not depend on the particular choice of a representative s in $s+K$. It is easy to show that $\eta^*(z_i)=(\eta_l^*(z_i), \eta_r^*(z_i))$ is a double homothetism of S/K and that any two of such double homothetisms are related. It can be shown also that η^* is a homomorphic mapping. Hence $\eta^*\colon R\to D^*$ is a homomorphism of R into a maximal ring of related double homothetisms of S/K. If T has the representative set $\bar z_i$, $i=1, \dots, l$, then a representative set of T/K is the set $\bar z_i+K$, $i=1, \dots l$. We have $(\bar z_i+K)(\bar z_j+K)=\{z_i, z_j\}+K$ and $m_i(\bar z_i+K)=b_i+K$, hence the corresponding factor sets are $\{z_i, z_j\}+K$ and b_i+K for all i, j with $1\leqq i, j\leqq l$ Moreover $(\bar z_i+K)(s+K)=\eta_l(z_i)s+K=\eta_l^*(z_i)(s+K)$ and $(s+K)(\bar z_i+K)=s\eta_r(z_i)+K=$ $=(s+K)\eta_r^*(z_i)$, hence η^* is induced by inner double homothetisms of T/K.

The following lemma is obvious now; in fact the proof is similar to that of Theorem 1.

Lemma 1. *If T is an η-square extension of S by R then, for each subring K of S invariant under the double homothetisms in $\eta(R)$, T/K is an η^*-square extension of S/K by R.*

Lemma 2. *Suppose that $S=S_1\oplus S_2$ (direct sum) and the orders q_1, and q_2 of S_1 resp. S_2 are relatively prime. If there exist η' resp. η''-square extensions of S_1 resp. S_2 by R, then there exists an $(\eta'+\eta'')$-square extension of S by R.*

Proof. Let $\{z_i, z_j\}'$, b_i' resp. $\{z_i, z_j\}''$, b_i'' be factor sets is S_1 resp. S_2 for an η'-resp. η''-extension of S_1 resp. S_2 by R. Here $\eta'\colon R\to D_1$ is a homomorphism of R into a maximal ring of related double homothetisms of S_1 and $\eta''\colon R\to D_2$ is a homomorphism of R into a maximal ring of related double homothetisms of S_2. Extend the double homothetisms $\eta'(z_i)=(\eta_l'(z_i), \eta_r'(z_i))$ of S_1 by letting them act trivially on S_2. Then define $\eta_l'(z_i)(s_1+s_2)=\eta_l'(z_i)s_1$ and $(s_1+s_2)\eta_r'(z_i)=$ $=s_1\eta_r'(z_i)$ for all $(\eta_l'(z_i), \eta_r'(z_i))$ in $\eta'(R)$ and all $s_1\in S_1$ and all $s_2\in S_2$. Similarly, extend the double homothetisms $\eta''(z_i)=(\eta_l''(z_i), \eta_r''(z_i))$ of S_2 by letting them act trivially on S_1. Then define $\eta_l''(z_i)(s_1+s_2)=\eta_l''(z_i)s_2$ and $(s_1+s_2)\eta_r''(z_i)=s_2\eta_r''(z_i)$ for all $(\eta_l''(z_i), \eta_r''(z_i))$ in $\eta''(R)$ and all $s_1\in S_1$ and all $s_2\in S_2$. It is easy to show now that both the extended $\eta'(z_i)$ and the extended $\eta''(z_i)$ are double homothetisms of S. Moreover the double homothetisms $\eta'(z_i)$ and $\eta''(z_i)$ of S are related double homothetisms. It follows that the sum $\eta'(z_i)+\eta''(z_i)$ is again a double homothetism of S, ([1]). We define now: $\eta'+\eta''(z_i)=\eta'(z_i)+\eta''(z_i)$ for all $z_i\in R$ and extend $\eta'+\eta''$ by linearity. Thus $\eta'+\eta''(z_i)$ is that double homothetism of S which is the sum of $\eta'(z_i)$ and $\eta''(z_i)$. More explicitly: $\eta'+\eta''(z_i)=(\eta_l'(z_i)+\eta_l''(z_i), \eta_r'(z_i)+\eta_r''(z_i))$, where $(\eta_l'(z_i)+\eta_l''(z_i))(s_1+s_2) = \eta_l'(z_i)(s_1+s_2)+\eta_l''(z_i)(s_1+s_2) = \eta_l'(z_i)s_1+\eta_l''(z_i)s_2$ for all $s_1\in S_1$ and all $s_2\in S_2$ and a similar formula holds for $\eta_r'(z_i)+\eta_r''(z_i)$. Then $\eta'+\eta''\colon R\to D$ is a homomorphic mapping of R into a maximal ring D of related double homothetisms of S, as the extended η' and η'' are homomorphisms of R into D. Here we may take $D=D_1\oplus D_2$. In order to construct an $\eta'+\eta''$-square extension of S by R, we use the sets $\{z_i, z_j\}'+\{z_i, z_j\}''$, $b_i'+b_i''$ in S as factor sets. As $\{z_i, z_j\}'$, b_i' with η' and $\{z_i, z_j\}''$, b_i'' with η'' both satisfy the conditions (1)—(4), it follows that $\{z_i, z_j\}'+\{z_i, z_j\}''$, $b_i'+b_i''$ together with $\eta'+\eta''$ satisfy the conditions (1)—(4). Hence we have obtained an $\eta'+\eta''$-extension T of $S=S_1\oplus S_2$ by R. Now we have to prove that $T^2=S$. First we remark that S_2 is mapped into itself under $\eta'+\eta''$. As T is an $\eta'+\eta''$-extension of S by R it follows that T/S_2 is an η^*-extension of S/S_2 by R, (Lemma 1). The corresponding factor set is $\{z_i, z_j\}'+S_2$, $b_i'+S_2$. Now since $\{z_i, z_j\}'$, b_i' corresponds to an η'-square extension of S_1 by R, it follows that T/S_2 is a square extension of S/S_2 by R. So $(T/S_2)^2=S/S_2$ and in the same way $(T/S_1)^2=S/S_1$. As T is an $\eta'+\eta''$-extension of S by R with the factor set $\{z_i, z_j\}'+\{z_i, z_j\}''$, $b_i'+b_i''$, it is clear that $T^2\subseteqq S$. So we have to prove $S\subseteqq T^2$. From $(T/S_2)^2=S/S_2=S_1$ it follows that, if s_1 is a given element of S_1, there exists an element $a\in T^2$ such that $s_1\equiv a \pmod{S_2}$. From $(T/S_1)^2=$ $=S/S_1=S_2$ it follows that, if s_2 is a given element of S_2, there exists an element $b\in T^2$ such that $s_2\equiv b \pmod{S_1}$. Then $q_2s_1\equiv q_2a (\mathrm{mod}\, q_2S_2=0)$, so $q_2s_1\in T^2$.

As the order of s_1 is relatively prime to q_2 it follows that $s_1 \in T^2$. Similarly $q_1 s_2 \equiv \equiv q_1 b \pmod{q_1 S_1 = 0}$, so $q_1 s_2 \in T^2$. As the order of s_2 is relatively prime to q_1 it follows that $s_2 \in T^2$. From $s_1 \in T^2$, $s_2 \in T^2$ for all $s_1 \in S_1$, $s_2 \in S_2$ it follows that $S_1 + S_2 = S \subseteqq T^2$. Then $T^2 = S$ and T is an $\eta' + \eta''$-square extension of S by R. We apply the lemmas 1 and 2 in the following theorem:

Theorem 2. *Let R and S be finite zero-rings. There exists a square extension T of S by R if and only if, for each p_i-Sylow subgroup A_i of S (p_i a prime), there exists a square extension of A_i by R.*

Proof. Let $S = A_1 \oplus \ldots \oplus A_k$, where the p_i-Sylow subgroup A_i has the order $p_i^{\alpha_i}$ $i = 1, \ldots, k$. Now the orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ are relatively prime. Thus, if there exist square extensions of $A_1, A_2, \ldots, A_k$ by R, then there exists a square extension T of S by R by the preceding Lemma 2.

Conversely let us suppose that T is a square extension of S by R. Now the A_i are characteristic subrings of S, i.e. they are invariant under all double homothetisms of S. Hence the direct sum $A_1 \oplus \ldots \oplus A_{i-1} \oplus A_{i+1} \oplus \ldots \oplus A_k$ is a characteristic subring of S. Therefore $T/A_1 \oplus \ldots \oplus A_{i-1} \oplus A_{i+1} \oplus \ldots \oplus A_k$ is a square extension of $S/A_1 \oplus \ldots \oplus A_{i-1} \oplus A_{i+1} \oplus \ldots \oplus A_k = A_i$ by R (Lemma 1). This theorem reduces the problem to the case in which S^+ is a finite abelian p-group.

Theorem 3. *Let S^+ be a finite abelian p-group, and S a zero-ring. Let R be a finite zero-ring. T is a square extension of S by R if and only if T/pS is a square extension of S/pS by R.*

Proof. First we remark that pS is a characteristic subring of S, for if $\alpha = (\alpha_1, \alpha_2)$ is an arbitrary double homothetism of S, then $\alpha_1(ps) = p\alpha_1(s)$ and $(ps)\alpha_2 = p(s)\alpha_2$ for all $s \in S$. Hence T is a square extension of S by R implies T/pS is a square extension of S/pS by R (Lemma 1). Conversely, suppose T/pS is a square extension of S/pS by R. Then $T/pS/S/pS \cong T/S \cong R$ and T is an extension of S by R. From $(T/pS)^2 = S/pS$ it follows that, if b is a given element in T^2, there exists an element $s \in S$ such that $b \equiv s \pmod{pS}$. Thus $T^2 \subseteqq S$. Conversely, if s is a given element in S, there exists an element $a \in T^2$ such that $s \equiv a \pmod{pS}$. Then $ps = a_0 + p^2 s_1$, where $a_0 = pa \in T^2$ and $s_1 \in S$, $p^2 s_1 = a_1 + p^3 s_2$, where $a_1 \in T^2$, $s_2 \in S$, $\ldots$, $p^{k-1} s_{k-2} = = a_{k-2} + p^k s_{k-1} = a_{k-2} \in T^2$, if we assume that $p^k S = 0$. Tracing back we find $ps \in T^2$ and as s is an arbitrary element in S we have $pS \subseteqq T^2$. But this implies $(T/pS)^2 = T^2/pS = S/pS$, hence $S = T^2$. T is a square extension of S by R. We note that $S^+/(pS)^+$ is an elementary abelian p-group and therefore we have reduced the problem to the case where S^+ is an elementary abelian p-group of finite rank.

Let $\eta \colon R \to D$ be a fixed homomorphism of R into a maximal ring of related double homothetisms of S. We consider the set $S_{\eta(r)}$ of all elements of the form $\eta_l(r)s$, $s'\eta_r(r)$, where $\eta(r) = (\eta_l(r), \eta_r(r))$ is a fixed element of $\eta(R)$ and s is a variable element in S, s' is a variable element in S, independent of s. Then let S^* be the subring of S, generated by all $S_{\eta(r)}$ for $r \in R$, which is denoted by $S^* = \langle S_{\eta(r)} \rangle$. Finally, if T is an extension of S by R, then M will denote the multiplicative factor set for some choice of representative set in T, i.e. $M = (\{z_i, z_j\}, 1 \leqq i \leqq l, 1 \leqq j \leqq l)$. Now we can prove:

Lemma 3. *T is a square η-extension of S by R if and only if S is generated by M and S^*: $S = \langle M, S^* \rangle$.*

Proof. It is sufficient to show that, given an η-extension T of S by R, $\langle M, S^* \rangle = T^2$. Let us assume that this has been proved. Then if T is a square η-extension of S by R we get $T^2 = S = \langle M, S^* \rangle$. Conversely, if $S = \langle M, S^* \rangle$ for some η-extension T of S by R, then, as $\langle M, S^* \rangle = T^2$, we get $T^2 = S$ and T is a square η-extension of S by R. Now we are going to prove that $T^2 = \langle M, S^* \rangle$ for a given η-extension T of S by R. For the multiplication in T we have:

$$\left(\sum_{i=1}^{l} n_i \bar{z}_i + s\right) \cdot \left(\sum_{j=1}^{l} u_j \bar{z}_j + v\right) = \sum_{i=1}^{l} \sum_{j=1}^{l} n_i u_j \{z_i, z_j\} + \sum_{i=1}^{l} n_i (\eta_l(z_i) v) + \sum_{j=1}^{l} u_j (s \eta_r(z_j))$$

where $(\bar{z}_1, \ldots, \bar{z}_l)$ is a representative set of the basis $(z_1, \ldots, z_l)$ in R, $s, v \in S$ and n_i, u_j are integers for $1 \leqq i \leqq l, 1 \leqq j \leqq l$. Thus $T^2 \subseteqq \langle M, S^* \rangle$. Now the generators of $\langle M, S^* \rangle$ are the elements $\{z_i, z_j\}$ of M and all elements of the form $\eta_l(z_i) v$, $s \eta_r(z_j)$ where $z_i, z_j \in (z_1, \ldots, z_l)$ in R and $v, s \in S$. As $\{z_i, z_j\} = \bar{z}_i \bar{z}_j$, $\eta_l(z_i) v = \bar{z}_i v$ and $s \eta_r(z_j) = s \bar{z}_j$ it follows that all generators of $\langle M, S^* \rangle$ belong to T^2, hence $\langle M, S^* \rangle \subseteqq T^2$. Then $\langle M, S^* \rangle = T^2$.

Next we investigate the η-extensions of S by R which are splitting extensions over S. First we consider the case where S^+ is an elementary abelian p-group of rank 1. We prove:

Lemma 4. *Let $S^+ = (0, a, \ldots, (p-1)a)$ be an elementary abelian p-group of rank 1. S is a zero-ring, i.e. $a^2 = 0$. Let R^+ be the direct sum of l cyclic groups (z_i) of order m_i, $i = 1, \ldots, l$. R is a zero-ring, i.e. $z_i z_j = 0$ for all i, j with $1 \leqq i \leqq l$, $1 \leqq j \leqq l$. Then there does not exist a splitting square η-extension T of S by R, whatever η may be.*

Proof. Let T be an η-extension of S by R with representative set $(\bar{z}_1, \ldots, \bar{z}_l)$. Addition and multiplication in T are performed according to: $\left(\sum_{i=1}^{l} n_i \bar{z}_i + sa\right) + \left(\sum_{i=1}^{l} u_i \bar{z}_i + va\right) = \sum_{i=1}^{l} (n_i + u_i) \bar{z}_i + (s+v)a$, with $n_i + u_i$ reduced mod $m_i (i = 1, \ldots, l)$ and $s+v$ reduced mod p; $\left(\sum_{i=1}^{l} n_i \bar{z}_i + sa\right)\left(\sum_{i=1}^{l} u_i \bar{z}_i + va\right) = \sum_{i=1}^{l} n_i v (\eta_l(z_i) a) + \sum_{j=1}^{l} u_j s (a \eta_r(z_j))$, if we assume that T is a splitting extension over S. But then

$0=a(\bar{z}_1^2)=(a\bar{z}_1)\bar{z}_1=(a\eta_r(z_1))\eta_r(z_1)$, which implies that $a\eta_r(z_1)=0$. So we get $a\eta_r(z_i)=0$ for all z_i with $i=1, \ldots, l$. Similarly $\eta_l(z_i)a=0$ for all z_i with $i=1, \ldots, l$. Hence T is a zero-ring and $T^2 \neq S$, as $S \neq (0)$. In this case there exists no splitting square η-extension T of S by R.

Theorem 4. *Let R and S be finite zero-rings. Let $\eta: R \to D$ be an arbitrary homomorphism of R into a maximal ring of related double homothetism of S. Then there does not exist an η-square extension T of S by R, such that T splits over S.*

Proof. It is sufficient to show that there does not exist an η-square extension T of S by R, such that T splits over S for the case that S^+ is an elementary abelian p-group of finite rank. Let us assume that this has been proved. First let S^+ a finite abelian p-group, not elementary, S a zero-ring and R a finite zero-ring. Then pS ($\neq 0$, $\neq S$) is a characteristic subring of S. Suppose T is an η-square extension of S by R which splits over S. Then, by Lemma 1, T/pS is an η^*-square extension of S/pS by R and from the results preceding Lemma 1, it is easy to see that T/pS splits over S/pS. But S/pS is an elementary abelian p-group, hence by assumption there does not exist an η^*-square extension of S/pS which splits over S/pS. So we get that there does not exist an η-square extension T of S by R which splits over S in case S^+ is a finite abelian p-group and R and S are finite zero-rings. Next let S^+ be an arbitrary finite abelian group and S a zero-ring. Let $S^+=A_1 \oplus \ldots \oplus A_k$, where the p_i-Sylow subgroup A_i has the order $p_i^{\alpha_i}$, $i=1, \ldots k$, and the p_i are primes. Suppose T is an η-square extension of S by R, which splits over S. Then, again by Lemma 1, $T/A_1 \oplus \ldots \oplus A_{i-1} \oplus A_{i+1} \oplus \ldots \oplus A_k$ is an η^*-square extension of $S/A_1 \oplus \ldots \oplus \ldots \oplus A_{i-1} \oplus A_{i+1} \oplus \ldots \oplus A_k = A_i$ by R, which splits over A_i, $1 \leqq i \leqq k$. But A_i^+ is a finite abelian p_i-group, hence there does not exist an η^*-square extension T of A_i by R which splits over A_i. This contradiction implies that there does not exist an η-square extension T of S by R which splits over S, if R and S are finite zero-rings.

Now S^+ is supposed to be an elementary abelian p-group of finite rank and we are going to prove that there does not exist an η-square extension T of S by R which splits over S whatever η may be. For a split extension, for some choice of representative set, $\{z_i, z_j\}=0$ and $b_i=0$ for all i and j, $1 \leqq i \leqq l$, $1 \leqq j \leqq l$. Hence T is an η-square extension of S by R which splits over S if and only if $S=S^*= =\langle S_{\eta(r)} | r \in R\rangle$ (Lemma 3). Now suppose that T is an η-square extension of S by R which splits over S. Since $S=S^* \neq 0$, $\eta(R) \neq 0$, where $\eta(R)$ is the image of R in the homomorphical mapping $\eta: R \to D$. Since R is generated by the z_i, $1 \leqq i \leqq l$, it is clear that $\eta(R)$ is generated by the pairs (A_i, B_i), $1 \leqq i \leqq l$, where $A_i=\eta_l(z_i)$, $B_i=\eta_r(z_i)$, such that $\eta(z_i)=(\eta_l(z_i), \eta_r(z_i))$ is the double homothetism of S corresponding to $z_i \in R$. The $2l$ endomorphisms A_i, B_j have the properties:

(i) $A_iA_k=0$, $B_jB_t=0$ for all i, j, k, t with $i\leqq i, k, j, t\leqq l$;

(ii) $A_iB_j=B_jA_i$ for all i, j with $1\leqq i, j\leqq l$.

In particular both the A_i and B_j are nilpotent endomorphisms such that $A_i^2=0$ and $B_j^2=0$ for all i, j with $1\leqq i, j\leqq 1$. Since $\eta(R)\neq 0$, at least one of these endomorphisms is $\neq 0$, say $A_1\neq 0$. Now consider the set $A_1S=\{A_1s|s\in S\}$. Then A_1S is a subring of S, as $A_1s_1+A_1s_2=A_1(s_1+s_2)$ and $(A_1s_1)(A_1s_2)=0$. Moreover A_1S is invariant under $A_1, \ldots, A_l; B_1, \ldots, B_l$, as $A_i(A_1S)=0$ (i), $B_j(A_1S)==A_1(B_jS)\subseteqq A_1S$ for all A_i, B_j (ii) with $1\leqq i, j\leqq l$. This means A_1S is a subring of S invariant under the double homothetisms of $\eta(R)$. Further $A_1S\neq 0$, as $A_1\neq 0$ and $A_1S\neq S$. If $A_1S=S$ then $A_1s=A_1\ (A_1s')=0$ for every $s\in S$ (i) and this would imply $A_1=0$ which is a contradiction. By Lemma 1, as T is an η-square extension of by R, $T/A_1\ S$ is an η^*-square extension of S/A_1S by R, where η^* is induced by η. In fact, $\eta^*\colon R\to D^*$, D^* a maximal ring of related double homothetisms of S/A_1S, is such that $\eta^*(z_i)=(\eta_l^*(z_i), \eta_r^*(z_i))$, where, by definition, $\eta_l^*(z_i)(s+A_1S)==\eta_l(z_i)s+A_1S$ and $(s+A_1S)\eta_r^*(z_i)=s\eta_r(z_i)+A_1S$. Since $S=S^*=\langle S_{\eta(r)}|r\in R\rangle$, it follows from the definition of $\eta_l^*(z_i)$, that $S/A_1S=(S/A_1S)^*=\langle S/A_1S_{\eta^*(r)}|r\in R\rangle$. Hence T/A_1S is an η^*-square extension of S/A_1S by R, which splits over S/A_1S. As $A_1S\neq 0$, and $A_1S\neq S$, the dimension of S/A_1S is less than r and greater than 0, if we consider S^+ as an r-dimensional vector space over the prime Galois field $F=GF(p)$. By Lemma 4, there does not exist an η-square extension T of S by R, which splits over S, in case S^+ has dimension 1. So, by induction on the dimension of S, it follows that there does not exist an η-square extension T of S by R which splits over S whatever η may be. This completes the proof of Theorem 4.

Next we investigate the existence of 0-square extensions of S by R i.e. extensions where the homomorphism $\eta\colon R\to D$ is the zero-homomorphism. Here we get the result:

Theorem 5. *Let S be a zero-ring and S^+ an elementary abelian p-group of finite rank r. Let R be a finite zero-ring, where $R^+=\sum_{i=1}^{l}\oplus z_i$, $O(z_i)=m_i$, $1\leqq i\leqq l$. Then there exists a* 0*-square extension T of S by R if and only if the following conditions are satisfied:* (i) $l^2\geqq r$; (ii) *if $(n-1)^2<r\leqq n^2$ for some n with $1\leqq n\leqq l$, then $p|m_i$ for at least n integers $m_i (1\leqq i\leqq l)$.*

Proof. Let T be a 0-square extension of S by R. Then $T^2=S$ and S is generated by M, for some choice of representative set (Lemma 3). As S has rank r, the number of generators of S in M is greater than or equal to r. Since $O(M)=l^2$, it follows that $l^2\geqq r$. As $\eta(R)=0$ we must have $m_i\{z_i, z_j\}=0$ and $m_i\{z_j, z_i\}=0$ for a fixed z_i and all z_j, $1\leqq j\leqq l$ ((3) and (4)). But if $\{z_i, z_j\}\neq 0$ then it has order p, hence $p|m_i$ if $\{z_j, z_i\}\neq 0$ for any z_j. Likewise if $\{z_j, z_i\}\neq 0$ for any z_j then $p|m_i$. The question is now: how many different elements $z_i(\in R)$ have the property that either $\{z_i, z_j\}\neq 0$

or $\{z_j, z_i\} \neq 0$ for at least one $z_j (\in R)$? Now let $(n-1)^2 < r \leqq n^2$ for some n with $1 \leqq n \leqq l$, and let B be a basis of S in M. Since $(n-1)^2 < r = O(B)$, there are more than $(n-1)^2$ elements $\{z_i, z_j\}$ in M $(1 \leqq i \leqq l, 1 \leqq j \leqq l)$ which are not equal to 0, i.e. the elements of the basis B. It is clear now that the minimal number of *different* $z_i (\in R)$ which occur either as a first or as a second component in at least one element in B is n. Hence $p | m_i$ for at least n integers m_i $(1 \leqq i \leqq l)$.

Conversely suppose the conditions (i) and (ii) are satisfied. We define functions $\{z_i, z_j\}$ of $R \times R$ into S for the basic elements of R in the following way. First let $\{z_i, 0\} = \{0, z_j\} = 0$ for all z_i, z_j with $1 \leqq i \leqq l$ and $1 \leqq j \leqq l$. We know $r \leqq l^2$, hence we may suppose that $(n-1)^2 < r \leqq n^2$ for some n with $1 \leqq n \leqq l$. We denote $r = (n-1)^2 + v$, where $1 \leqq v \leqq 2n-1$. Now S has rank r and let $(s_1, \ldots, s_r)$ be a basis of S. From (ii) we infer that there are n integers, say $m_1, \ldots, m_n$, such that $p | m_i$ for all i with $1 \leqq i \leqq n$. Then set $\{z_1, z_1\} = s_1, \{z_1, z_2\} = s_2, \ldots, \{z_1, z_{n-1}\} = = s_{n-1}, \{z_2, z_1\} = s_n, \ldots, \{z_2, z_{n-1}\} = s_{2n-2}, \ldots, \{z_{n-1}, z_1\} = s_{n^2-3n+3}, \ldots, \{z_{n-1}, z_{n-1}\} = = s_{(n-1)^2}$ and set $\{z_i, z_n\}$ and/or $\{z_n, z_i\}$ equal to $s_{(n-1)^2+1}, \ldots, s_r$ for v functions $\{z_i, z_n\}$ and/or $\{z_n, z_i\}$ with $1 \leqq i \leqq n$. Then set all other $\{z_i, z_j\} = 0$. It is clear now that S is generated by the set of all $\{z_i, z_j\}$ with $1 \leqq i \leqq n$ and $1 \leqq j \leqq n$. If we put $\eta(R) = 0$ then the conditions (1)—(4) are satisfied for the functions $\{z_i, z_j\}$ $(1 \leqq i \leqq l, 1 \leqq j \leqq l)$ and an arbitrary set $b_i \in S$ $(1 \leqq i \leqq l)$. Hence T is an 0-extension of S by R, if we define T as the set of all symbols $\sum_{i=1}^{l} n_i \bar{z}_i + s$ ($s \in S$, n_i integers) with the addition and multiplication: $\left(\sum_{i=1}^{l} n_i \bar{z}_i + s\right) + \left(\sum_{i=1}^{l} u_i \bar{z}_i + v\right) = = \sum_{i=1}^{l} (n_i + z_i)\bar{z}_i + s + v$, where $m_i \bar{z}_i = b_i (\in S)$ for $1 \leqq i \leqq l$, $\left(\sum_{i=1}^{l} n_i \bar{z}_i + s\right)\left(\sum_{i=1}^{l} u_i \bar{z}_i + v\right) = = \sum_{i=1}^{l} \sum_{j=1}^{l} n_i u_j \{z_i, z_j\}$. As $S = \langle M \rangle$, it follows that T is a 0-square extension of S by R, which completes the proof of Theorem 5.

Now we determine the rings T which may occur as a square extension of a ring S of order 2 by a ring R of order 4. Both S and R are supposed to be zero-rings. Let $S^+ = (0, a)$ with $2a = 0$ and $a^2 = 0$. Let $R^+ = (z_1) \oplus (z_2)$ be the direct sum of two cyclic groups (z_1) and (z_2) both of order 2 and $z_1^2 = z_1 z_2 = z_2 z_1 = z_2^2 = 0$. Now the endomorphism ring of S^+ consists of the zero-endomorphism and the identity mapping. Hence in this case we must have $\eta(R) = 0$, so that there are only 0-square extensions of S by R possible. As the conditions of Theorem 5 are satisfied there exist 0-square extensions of S by R. There are 2 cases: (i) $2\bar{z}_1 = 2\bar{z}_2 = 0$, which means $b_1 = b_2 = 0$ in S. (ii) at least one of b_1 and $b_2 \neq 0$.

(i) In this case the elements a, $\bar{z}_1$ and $\bar{z}_2$ all have order 2 and we get $T^+ = = (a) \oplus (\bar{z}_1) \oplus (\bar{z}_2)$ is of typus $(2, 2, 2)$. As $\eta(R) = 0$, $a\bar{z}_1 = a\bar{z}_2 = \bar{z}_1 a = \bar{z}_2 a = 0$. If $\{z_1, z_1\}, \{z_1, z_2\}, \{z_2, z_1\}$ and $\{z_2, z_2\}$ are 0, then $T^2 = (0)$ which contradicts that $T^2 = S$. Hence we must have at least one of the four elements $\{z_1, z_1\}$, $\{z_1, z_2\}$ $\{z_2, z_1\}$ and $\{z_2, z_2\}$ equal to a. We get 15 different rings T with multiplications:

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	0
$\bar{z}_2$	0	0	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	0
$\bar{z}_2$	0	0	0

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	a
$\bar{z}_2$	0	a	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	a
$\bar{z}_2$	0	a	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	0
$\bar{z}_2$	0	0	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	a
$\bar{z}_2$	0	a	0

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	0
$\bar{z}_2$	0	a	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	a
$\bar{z}_2$	0	0	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	0
$\bar{z}_2$	0	a	0

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	0
$\bar{z}_2$	0	a	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	a
$\bar{z}_2$	0	0	0

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	a
$\bar{z}_2$	0	0	a

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	a	0
$\bar{z}_2$	0	a	0

	a	$\bar{z}_1$	$\bar{z}_1$
a	0	0	0
$\bar{z}_1$	0	a	a
$\bar{z}_2$	0	0	0

	a	$\bar{z}_1$	$\bar{z}_2$
a	0	0	0
$\bar{z}_1$	0	0	a
$\bar{z}_2$	0	a	0

Thus we get 15 non-equivalent 0-square extensions T of S by R.

(ii) In this case at least one of the elements $\bar{z}_1$ and $\bar{z}_2$ is of order 4, and T^+ is of typus (2, 4), say $T^+ = (\bar{z}_1) \oplus (\bar{z}_2)$ where $O(\bar{z}_1) = 2$ and $O(\bar{z}_2) = 4$. For the multiplication in T one has again: $\bar{z}_1^2 = k_1 a, \bar{z}_1\bar{z}_2 = k_2 a, \bar{z}_2\bar{z}_1 = k_3 a, \bar{z}_2^2 = k_4$ a where

$0 \leqq k_i \leqq 1$, $i = 1, 2, 3, 4$. Hence we get the same multiplication tables as in case (i), if we omit the first row and the first column. Thus we find 15 non-equivalent 0-square extensions T of S by R. Next we suppose S to be a zero-ring of order 2 as above and $R^+ = (z)$ a cyclic group of order 4. R is a zero-ring i.e. $z^2 = 0$. Again $\eta(R) = 0$ so there are only 0-square extensions of S by R possible and by Theorem 5 there are such extensions. As $\bar{z}^2 = 0$ or a, we get $\{z, z\} = 0$ or a. But if $\{z, z\} = 0$ then $T^2 = (0)$, contradiction. So we must have $\{z, z\} = a$. We have two possibilities for the addition according to $4\bar{z} = 0$ or a, which means $b = 0$ or a. If $b = 0$, then $T^+ = (a) \oplus (\bar{z})$ is of typus $(2, 4)$, if $b = a$, then $T^+ = (\bar{z})$ is a cyclic group of order 8. Thus we get 2 non-equivalent 0-square extensions T of S by R. Finally we want to discuss the rings T which may occur as a square extension of a ring S of order 4 by a ring R of order 2. Both R and S are supposed to be zero-rings. Let $S^+ = (a_1) \oplus \oplus (a_2)$ be the direct sum of two cyclic groups (a_1) and (a_2) each of order 2 and $a_1^2 = a_1 a_2 = a_2 a_1 = a_2^2 = 0$. Let $R^+ = (0, z)$ with $2z = 0$ and $z^2 = 0$. As the condition (i) of Theorem 5 is not satisfied in this case $(l = 1, r = 2)$, there do not exist 0-square extensions of S by R now. The nilpotent endomorphisms in the endomorphismring of S^+ are: $s_1\colon a_1 \to 0, a_2 \to 0$; $s_2\colon a_1 \to 0, a_2 \to a_1$; $s_3\colon a_1 \to a_2, a_2 \to 0$; $s_4\colon a_1 \to a_1 + a_2$; $a_2 \to a_1 + a_2$. So the possible double homothetisms are (s_1, s_1), (s_1, s_2), (s_1, s_3), (s_1, s_4), (s_2, s_1), (s_2, s_2), (s_3, s_1), (s_3, s_3), $(s_4, s_1)(s_4, s_4)$, which may occur as the element $(\eta_l(z), \eta_r(z))$ in $\eta(R)$. For $\bar{z}^2 = \{z, z\}$ as well as for $2\bar{z} = b$ we may choose $0, a_1, a_2$ or $a_1 + a_2$. But as $2\{z, z\} = 0$ we must have $(b)\eta_r(z) = \eta_1(z)(b)^{\circ} = 0$, ((3) and (4)). Then we distinguish the following cases:

(i) Let $b = a_1$. Then $(\eta_l(z), \eta_r(z)) = (s_2, s_2)$ for a square extension of S by R. As $S^* = \langle S_{\eta(r)} \rangle = (0, a_1)$ we must have $\{z, z\} = a_2$ or $a_1 + a_2$ for a square extension of S by R (Lemma 3). Since $\eta_l(z) = \eta_r(z) = s_2$ the condition (2) is satisfied. The additive group T^+ of a square extension T of S by R has the form: $T^+ = (\bar{z}) \oplus (a_2)$ where $(\bar{z})$ has order 4 and a_2 has order 2. So T^+ is of typus $(2, 4)$. For the multiplication in T one has: $a_2^2 = 0$, $\bar{z}a_2 = s_2 a_2 = a_1$; $a_2\bar{z} = a_2 s_2 = a_1$ and $\bar{z}^2 = a_2$ or $a_1 + a_2$. Hence one gets 2 non-equivalent η-square extensions T of S by R.

(ii) Let $b = a_2$. Then we must take $(\eta_l(z), \eta_r(z)) = (s_3, s_3)$ for a square extension of S by R. As $S^* = \langle S_{\eta(r)} \rangle = (0, a_2)$ we must have $\{z, z\} = a_1$ or $a_1 + a_2$ (Lemma 3). Since $\eta_l(z) = \eta_r(z) = s_3$ the condition (2) is satisfied. The additive group T^+ of a square extension T of S by R has the form: $T^+ = (\bar{z}) \oplus (a_1)$ where $(\bar{z})$ has order 4 and a_1 has order 2. So T^+ is of typus $(2, 4)$. For the multiplication in T one has: $a_1^2 = 0$, $\bar{z}a_1 = s_3 a_1 = a_2$, $a_1\bar{z} = a_1 s_3 = a_2$ and $\bar{z}^2 = a_1$ or $a_1 + a_2$. Hence one gets 2 non-equivalent η-square extensions T of S by R.

(iii) Let $b = a_1 + a_2$. Now we must have $(\eta_l(z), \eta_r(z)) = (s_4, s_4)$ for a square extension of S by R. As $S^* = \langle S_{\eta(r)} \rangle = (0, a_1 + a_2)$ we must have $\{z, z\} = a_1$ or a_2, (Lemma 3). Since $\eta_l(z) = \eta_r(z) = s_4$ the condition (2) is satisfied. The additive group T^+ of a square extension T of S by R has the form: $T^+ = (\bar{z}) \oplus (a_1)$, where $(\bar{z})$

has order 4 and a_1 has order 2. So T^+ is of typus $(2, 4)$. For the multiplication in T one has: $a_1^2=0$, $\bar{z}a_1=s_4a_1=a_1+a_2$, $a_1\bar{z}=a_1s_4=a_1+a_2$ and $\bar{z}^2=a_1$ or a_2. Hence one gets 2 non-equivalent η-square extensions T of S by R.

(iv) Let $b=0$. Then the conditions (3) and (4) are satisfied. For a square extension T of S by R we need only satisfy condition (2): $\eta_l(z)\{z, z\}=\{z, z\}\eta_r(z)$. We have again different cases:

(iv. a) Let $\{z, z\}=a_1$. Now we must have $(\eta_l(z), \eta_r(z))=(s_3, s_3)$ or (s_4, s_4). In both cases the condition (2) is satisfied. So we get 2 rings T each of which has an additive group $T^+=(a_1)\oplus(a_2)\oplus(\bar{z})$ of typus $(2, 2, 2)$. Hence there are 2 square extensions T of S by R, an η'-square extension where $\eta'(z)=(s_3, s_3)$ and an η''-square extension where $\eta''(z)=(s_4, s_4)$.

(iv. b) Let $\{z, z\}=a_2$. Then we must have $(\eta_l(z), \eta_r(z))=(s_2, s_2)$ or (s_4, s_4). In both cases the condition (2) is satisfied. Thus we get 2 rings T each of which has an additive group $T^+=(a_1)\oplus(a_2)\oplus(\bar{z})$ of typus $(2, 2, 2)$. So there are 2 square extensions T of S by R, an η'-square extension for $\eta'(z)=(s_2, s_2)$ and an η''-square extension for $\eta''(z)=(s_4, s_4)$.

(iv. c) Let $\{z, z\}=a_1+a_2$. Here we must have $(\eta_l(z), \eta_r(z))=(s_2, s_2)$ or (s_3, s_3). In both cases the condition (2) is satisfied. Again we get 2 rings T each of which has as an additive group $T^+=(a_1)\oplus(a_2)\oplus(\bar{z})$ of typus $(2, 2, 2)$. Therefore we get 2 square extensions T of S by R, an η-square extension where $\eta(z)=(s_2, s_2)$ and an η'-square extension where $\eta'(z)=(s_3, s_3)$.

(iv. d) Let $\{z, z\}=0$. Now we would get a square extension T of S by R which splits over S which is impossible by Theorem 4. Hence there do not exist square extensions in this case.

There is a second class of rings T which may occur as a square extension of a ring S of order 4 by a ring R of order 2. Now we put $S^+=(a)$ is a cyclic group of order 4 and $a^2=0$ (S is a zero-ring). Again $R^+=(0, z)$ with $2z=0$ and $z^2=0$. The nilpotent endomorphism in the endomorphismring of S^+ are: $s_1: a\to 0$, and $s_2: a\to 2a$. So the pairs (s_1, s_1), (s_1, s_2), (s_2, s_1) and (s_2, s_2) may occur as the element $(\eta_l(z), \eta_r(z))$ in $\eta(R)$. The elements $\bar{z}^2=\{z, z\}$ and $2\bar{z}=b$ in an extension T of S by R must satisfy the conditions (3) and (4), i.e. $(b)\eta_r(z)=2\{z, z\}$ and $\eta_l(z)(b)=$ $=2\{z, z\}$, $(b\in S, \{z, z\}\in S)$. This implies that if $b=0$ or $b=2a$, then $\{z, z\}=0$ or $\{z, z\}=2a$. In either case $T^2=(0)$ or $T^2=(0, 2a)$ and $T\neq S$, so T is not a square extension of S by R. Hence we must have $b=a$ or $b=3a$. By the conditions (3) and (4) we get square extensions if we take $(\eta_l(z), \eta_r(z))=(s_2, s_2)$ and $\{z, z\}=a$ or $3a$, (cf. also Lemma 3). The condition (2) is satisfied.

(i) Let $\{z, z\}=a$ and $b=a$ resp. $b=3a$. Let T_1 be an η-extension of S by R with factor set $\{z, z\}=a$, $b=a$ and let T_2 be an η-extension of S by R with factor set $\{z, z\}'=a$, $b'=3a$. Then $T_1\sim T_2$ as the conditions (5) and (6) are satisfied for $\psi_z=a$. Here $(\eta_l(z), \eta_r(z))=(s_2, s_2)$ and T_1 and T_2 have the same additive group

$T^+ = (\bar{z})$ which is a cyclic group of order 8. As $S = \langle M, S^* \rangle$ both for T_1 and T_2, we get 2 equivalent η-square extensions of S by R (Lemma 3).

(ii) Let $\{z, z\} = 3a$ and $b = a$ resp. $b = 3a$. In the same way as in case (i) we get 2 equivalent η-square extensions T_1 and T_2 of S by R, where T_1 resp. T_2 has the factor set $(3a, a)$ resp. $(3a, 3a)$. Both T_1 and T_2 have again the additive group $T^+ = (\bar{z})$ (cyclic of order 8).

Remark. Our results obtained in Theorems 1, 2 and 3 and Lemmas 1, 2 and 3 are quite analogous to the corresponding Theorems and Lemmas in the paper: H. ONISHI, Commutator extensions of finite groups *Mich. Math. J.*, **13** (1966), 119—126, if one replaces "commutator extension" by "square extension". In fact, the results of ONISHI for finite groups led us to consider the situation for finite rings.

Literature

[1] L. C. A. VAN LEEUWEN, Holomorphe von endlichen Ringen, *Nederl. Akad. Wet. Proc.*, ser. A, **68** (1965), 632—645.

[2] L. RÉDEI, *Algebra*. I (Leipzig, 1959).

UNIVERSITY OF ILLINOIS AT CHICAGO CIRCLE
CHICAGO, ILLINOIS, U.S.A.
AND
INSTITUTE OF TECHNOLOGY
DELFT, THE NETHERLANDS

(Received July 4, 1967)