RINGS OF ZERO-DIVISORS

P. M. COHN

1. Introduction. A well known theorem of algebra states that any integral domain can be embedded in a field. More generally [2, p. 39 ff.], any commutative ring R with unit-element can be embedded in a ring S with the same unit-element as R, such that any element of S is either invertible or the product of an invertible element by a zero-divisor of R. The following statement can, in a very rough sense, be regarded as a "dual":

Any commutative ring R with unit-element can be embedded in a ring S with the same unit-element as R such that every element of S is either a zero-divsor or an invertible element of R.

This statement will be proved in §2 (Theorem 1) and as in the theorem quoted we have the corollary that any commutative ring with a unit-element 1, which has no invertible elements other than 1, can be embedded in a ring in which every element $\neq 1$ is a zero-divisor. We are thus led to consider commutative rings with unit-element 1, in which every element $\neq 1$ is a zero-divisor. Such rings will be called O-rings for short. It is clear that every Boolean ring with a unit-element is an O-ring, and Theorem 1 shows without difficulty that O-rings exist which are not Boolean; this answers a question raised by Kaplansky.[1] An O-ring may be regarded as an algebra over the field of two elements and thus is a special case of an O-algebra, viz. an algebra with unit-element over a field F in which every element not in F is a zero-divisor. Again any algebra with no invertible elements other than those of F can be embedded in an O-algebra, and some theorems on the structure of these algebras are proved in §3. In particular, any O-algebra R over a field F is a subdirect product of extension fields of F; the number of components is infinite unless $R=F$ or R is Boolean. Moreover, in any representation of R as such a subdirect product, and for any element a of R and any equation (in one indeterminate) over F, there are infinitely many components of a satisfying this equation, unless a is a scalar or F is the field of two elements and a is idempotent. Nevertheless, (non-Boolean) O-rings exist which are countable. It is also noted that any O-algebra, which is regular in the sense of von Neumann, is of dimension 1 or Boolean.

Received by the editors March 14, 1958.

[1] Communicated to the writer by M. P. Drazin. It was this question which gave rise to the present note.

2. **The embedding theorem.** Throughout this note, we take "ring" to mean "commutative ring with unit-element"; further, to say "P is a subring of R" is understood to mean "subring with the same unit-element," and similarly, to embed R in a ring S means to embed as a subring, i.e. with the same unit-element.[2] The common unit-element will always be denoted by 1. These conventions apply in particular when R is an algebra over a field F, so that in this case F may be considered as a subalgebra of R.

The result to be proved may now be stated as follows:

THEOREM 1. *Any ring R may be embedded in a ring S such that any element s of S is a zero-divisor unless $s \in R$ and s has an inverse in R. If R is an algebra over a field F then S may also be taken to be an algebra over F.*

The essential step towards establishing this theorem is the proof of

LEMMA 1. *Let R be any ring and a any element of R which has no inverse in R. Then there exists a ring R' containing R as a subring such that*

(i) *R' contains an element $a' \neq 0$ satisfying $aa'=0$,*

(ii) *any invertible element of R' belongs to R and is already invertible in R.*

PROOF. Let $R[x]$ be the ring of polynomials in an indeterminate x with coefficients in R. Since R has a 1, every proper ideal of R is contained in a maximal ideal. Now a has no inverse, therefore the principal ideal generated by a is proper and hence is contained in a maximal ideal, M say, of R. Let M' be the ideal of $R[x]$ generated by the elements $mx (m \in M)$. Then M' consists precisely of the elements mxu ($m \in M$, $u \in R[x]$), and it follows that

$$M' \cap R = 0, \tag{1}$$

$$x \notin M'. \tag{2}$$

Equation (1) is clear, since an equation of the form

$$b = mxu, \qquad b \in R, m \in M, u \in R[x]$$

implies $b=0$, by a comparison of the terms of degree zero. To prove (2), let us suppose that $x \in M'$, so that

$$x = mxu, \tag{3}$$

where $m \in M$ and $u = u_0 + u_1 x + \cdots + u_n x^n$ ($u_i \in R$), say; by com-

[2] This amounts to regarding the unit-element as 0-ary operator for the class of rings considered.

paring the terms of degree 1 in (3) we obtain $1=mu_0$, which contradicts the fact that M is proper.

We now put $R'=R[x]/M'$. By (1), the natural homomorphism of $R[x]$ onto R', when restricted to R, is one-one; we may therefore identify R with a subring of R'. If we write a' for the image of x under the natural homomorphism, then (2) shows that $a'\neq 0$, while $aa'=0$, because $ax\in M$. It only remains to show that any invertible element of R' belongs to R.

Let u' then be an element of R' with inverse v', so that $u'v'=1$. Going back to $R[x]$, we find elements u, v mapping onto u', v' respectively, i.e. we have an equation of the form

$$uv = 1 + xmw \qquad w \in R[x]. \tag{4}$$

Let $u=\sum u_i x^i$, $v=\sum v_i x^i$, $w=\sum w_i x^i$, where u_i, v_i, $w_i\in R$. If u is of degree 0, then $u\in R$, and by comparing the terms independent of x in (4) we find that $uv_0=1$; thus u belongs to R and is invertible in R, and hence the same is true for u'. In what follows we may therefore suppose that u is of positive degree, r say. By symmetry, v may also be taken to have positive degree, s say. Now $u_r x^r\in M'$ whenever $u_r\in M$, and since we are only interested in the residue class of u (mod M'), we may assume $u_r\notin M$. Similarly $v_s\notin M$ and since M is maximal, $u_r v_s\notin M$. Equating coefficients of x^{r+s} in (4) we find

$$u_r v_s = m w_{r+s-1} \in M,$$

a contradiction. This shows that all the invertible elements of R' belong to R and have their inverses in R, and the lemma is established.

It is now easy to prove Theorem 1, using a Steinitz tower construction. Given any ring R and any $a\in R$ which has no inverse we can by Lemma 1, embed R in a ring in which a becomes a zero-divisor, without increasing the set of invertible elements. By transfinite induction we can embed R in a ring R' without increasing the set of invertible elements, and such that every element of R which is not invertible becomes a zero-divisor in R'. Starting with $R_0=R$, we now define R_n inductively by the equation $R_{n+1}=R_n'$. In this way we obtain an ascending sequence of rings

$$R \subset R_1 \subset R_2 \subset \cdots.$$

The union S of these rings is again a ring; this ring contains R and by construction, every invertible element of S belongs to R and is invertible in R. Further, any element of S which is not invertible belongs to R_n for some n, and hence is a zero-divisor in R_{n+1}; a fortiori it is a zero-divisor in S, and this completes the proof of the theorem in the case of rings. If R is an algebra over a field F, all the rings occurring become algebras over F and the proof goes through unchanged.

From the proof of Theorem 1 it is clear that S has the same cardinal as R or $\aleph_0$, whichever is the greater. In particular, if R is countable, then so is S.

If in Theorem 1 we replace elements by finite subsets, we obtain the following generalization:

THEOREM 1′. *Any ring R may be embedded in a ring S such that* (i) *S has no invertible elements other than those of R,* (ii) *every proper ideal of R generates a proper ideal of S and* (iii) *every finitely generated proper ideal of S has a nontrivial annihilator.*

Clearly this includes Theorem 1, since an element a of S either generates a proper ideal, in which case it is a zero-divisor, by (iii), or it is invertible and then both a and its inverse belong to R, by (i). As we shall not have occasion to use Theorem 1′, we omit the proof which is very similar to that of Theorem 1.

3. Algebras without nontrivial units and *O*-algebras.

Let R be a ring in which no element $\neq 1$ is invertible. Since -1 necessarily has an inverse, we have $-1=1$, whence $2x=0$ for all $x\in R$. Therefore R can be regarded as an algebra over $F=GF(2)$, the field of two elements, and R has no "units" other than the nonzero elements of F. More generally, we shall say that an algebra R over a field F *has no nontrivial units* if the only invertible elements of R are the nonzero elements of F.[3] If moreover, all the elements of R except those in F are zero-divisors, we call R an *O-algebra.* From Theorem 1 and the remark following it we now obtain

THEOREM 2. *Any algebra R over F without nontrivial units may be embedded in an O-algebra S. If R is countable, so is S.*

Taking the groundfield to be GF(2), we obtain the

COROLLARY. *Any ring with no invertible elements other than* 1 *may be embedded in an O-ring, which is countable if the given ring was countable.*

Returning to algebras without nontrivial units, we have the following structure theorem.

[3] We recall that R contains 1 and hence all the elements of F. The observation that the arguments as originally presented for the case $F=\mathrm{GF}(2)$ carry over to the general case is due to the referee.

THEOREM 3. *Let R be an algebra over F without nontrivial units. Then R is a subdirect product*[4] *of extension fields of F, and every element x of R which is not in F is transcendental over F, unless $F=GF(2)$ and x is idempotent.*[5] *If, moreover, R has finite dimension over F, then either $R=F$ or R is a Boolean algebra.*

PROOF. We begin by showing that J, the Jacobson radical of R, is zero. Let $a\in J$, then $1+a$ has an inverse and so belongs to F, whence $a\in F$; this shows that $J\subseteq F$. But $1\notin J$, so that J is a proper ideal in R and therefore also in F, whence $J=0$. It follows[6] that R is a subdirect product of fields which in our case are algebras over F, i.e. extension fields of F. If R is of finite dimension then the number of factors is finite and R is in this case a *direct* product of extension fields of F.[7] Since R has no nontrivial units, this is possible only if (i) $R=F$ or (ii) $F=\mathrm{GF}(2)$ and R is the direct sum of a finite number of copies of F, i.e. if R is a Boolean algebra. This proves the last part; to complete the proof, we consider an element x of R which is algebraic over F. Then the subalgebra $F[x]$ generated by x is finite-dimensional and has no nontrivial units, whence by the part just proved, either $F[x]=F$, i.e. $x\in F$, or $F[x]$ is Boolean, in which case $F=\mathrm{GF}(2)$ and $x^2=x$, which is what we wished to show.

It is clear that a Boolean algebra is an O-ring, since each x satisfies $x(1-x)=0$. To obtain an O-ring which is not Boolean, we take a non-Boolean algebra over GF(2) without nontrivial units, e.g. the algebra of polynomials in a single variable over GF(2). By Theorem 2, Corollary, this algebra may be embedded in an O-ring, which is not Boolean since it contains elements which are not idempotent. Moreover it is countable. In a similar way we obtain for a general field F an O-algebra different from F and of cardinal $\max(\aleph_0, \text{card } F)$.

We note that an algebra R over F without nontrivial units which is regular[8] either coincides with F or is Boolean. For by the regularity there exists for each $a\in R$ an element $x\in R$ such that $xa^2=a$. Hence $(1+a(1-x))(1-xa(1-x))=1$, so that $1+a(1-x)=\gamma\in F$. Now $a=\gamma+ax-1$, and multiplying by a we find that $a^2=\gamma a+xa^2-a=\gamma a$, which shows that a is algebraic over F; the result stated now follows from Theorem 3.

---

[4] The term "product" is used here in the sense of Bourbaki.

[5] I am indebted to the referee for the assertion about elements of R, which allows some of the later proofs to be shortened.

[6] McCoy [**1**, p. 135].

[7] This follows from Theorem 32 of McCoy [**1**, p. 125].

[8] I.e., to every $a\in R$ there corresponds an $x\in R$ satisfying $axa=a$. M. P. Drazin has proved, somewhat more generally, that in any (not necessarily commutative) ring with 1 and no other invertible elements, every regular element is idempotent.

From the proof of the last assertion of Theorem 3 we see that for an algebra over F without nontrivial units which is not equal to F itself or Boolean, any representation as a subdirect product must contain infinitely many factors. In the case of O-algebras we can say rather more.

THEOREM 4. *Let R be any O-algebra over F, and a an element of R which is transcendental over F. Then in any representation of R as a subdirect product of fields and for any equation*

$$f(\xi) = 0 \tag{5}$$

of positive degree over F, there are infinitely many components of a satisfying (5).

An O-algebra has no nontrivial units, so that R can be written as a subdirect product of fields, by Theorem 3. This shows that the assertion is never vacuous. To prove it, we consider first the special case $f(\xi)=\xi$, i.e. we show that infinitely many components of a are zero. For if there is a transcendental element of R with only finitely many components equal to zero, let $a=(a_i)$ $(i\in I)$ be such an element, with components a_i, where[9] $a_1 = a_2 = \cdots = a_k = 0$, $a_i \neq 0$ $(i\neq 1, 2, \cdots, k)$. We may suppose a chosen so that k has its least value $(k\geqq 0)$. Since $a\notin F$, there exists $b\in R$, $b\neq 0$, such that $ab=0$. This equation shows that for each $i\in I$ either $a_i=0$ or $b_i=0$. In particular $b_i=0$ except possibly for $i=1, \cdots, k$, and since $b\neq 0$, some b_i must be different from zero, which shows that $k>0$. Now the element $a+b$ has fewer than k components equal to 0, since $a_i+b_i=0$ only if $a_i=b_i=0$. By the hypothesis on k, $a+b$ is algebraic over F; therefore either $a+b=\gamma\in F$ and $ab=a^2-\gamma a=0$, or $F=\mathrm{GF}(2)$ and $a+b$ is idempotent. But then each a_i (and each b_i) is either 0 or 1, so that we have $a^2=a$. In either case we have found an equation satisfied by a, which contradicts the fact that a was chosen transcendental.

To complete the proof, suppose that a has only finitely many components satisfying (5). This means that $f(a)$ has only finitely many components equal to zero, and by what has been proved, $f(a)$ is algebraic over F, i.e. either $f(a)=\gamma\in F$ or $f(a)^2=f(a)$. In either case a is algebraic over F, and this establishes the theorem.

REFERENCES

1. N. H. McCoy, *Rings and ideals*, New York, 1948.
2. D. G. Northcott, *Ideal theory*, Cambridge, 1953.

THE UNIVERSITY, MANCHESTER, ENGLAND

[9] To save notation we suppose that the appropriate factors in the product have been indexed by the integers from 1 to k.