COMPOSITIO MATHEMATICA

R. RAGHAVENDRAN

Finite associative rings

Compositio Mathematica, tome 21, nº 2 (1969), p. 195-229

<http://www.numdam.org/item?id=CM_1969__21_2_195_0>

COMPOSITIO MATHEMATICA, Vol. 21, Fasc. 2, 1969, pag. 195-229
Wolters-Noordhoff Publishing
Printed in the Netherlands

Finite Associative Rings[1]

by

R. Raghavendran

Introduction

Throughout this paper the symbol R will be used to denote a finite associative ring with a multiplicative identity $1 \neq 0$. We use the notation G_R for the multiplicative group of the invertible elements of the ring under consideration. The symbol S will be used to denote an arbitrary ring — not necessarily finite, and not necessarily possessing an identity element. The term "subring" is used to mean a subring containing the identity element, when one exists, of the larger ring. Also by "subfield" we mean a subring which, when regarded by itself, is a field (commutative). As is usual, Z denotes the ring of all integers and p denotes any prime integer greater than or equal to 2. We use F to denote the Galois field $GF(q)$ where $q = p^r$. Finally, for any set A we use $|A|$ to denote the cardinal number of elements in that set.

In this paper we determine the structures of prime-power rings, (i.e.) rings whose orders are powers of primes, under various conditions. For this purpose we begin by considering, in § 1, a set $\mathfrak{M}$ which is simultaneously a left vector space and a right vector space over the same field P, and which is subject to the condition that $a(xb) = (ax)b$ for all a, b in P and for all x in $\mathfrak{M}$. When $\mathfrak{M}$ has only a finite number of elements we show that it will have at least one "distinguished basis" — for definition, refer to the body of the paper — over the field P, and remark as to how this result can be used to give a proof of the well-known theorem of Wedderburn on finite division rings. Two generalisations of this theorem to the case of completely primary rings with a finite number of elements are also given in the later sections of this paper. (Cf. Ths. 5 and 7.)

[1] This is a revised version of the thesis submitted by the author for a Doctorate degree of the Annamalai University, under the guidance of Professor V. Ganapathy Iyer. This work was supported in part by the Government of India through a Scholarship.

In § 2 we consider the situation where the zero divisors of the ring R form a group under addition. After noting that the ring must then be a completely primary ring (not necessarily commutative), we exhibit R, in two special cases, as a ring of matrices over a field. (Cf. § (2.4).)

In § 3 we study a special class of rings which includes the Galois fields and the rings $Z/(p^n)$. It seems appropriate to call these rings by the name Galois rings. For their definition see § (3.1) and for some of their properties refer § (3.8) and § (3.9) below.

In § 4 we consider the situation where a ring R contains a subfield F. After noting that $|R| = (|F|)^n$ for some positive integer n, we describe (in Ths. 10 and 11) the structures of all such rings when $n = 2$ and when $n = 3$.

In § 5 we consider a problem posed by Ganesan [1, Remark 1, p 216] and generalised by Eldridge in two private communications to Ganesan. The problem may be stated as follows: "S is any ring with N^2 elements exactly N of which are left zero divisors in S. To find all the possible structures of the ring S." A complete solution of this problem may be found in Th. 12 below. One special case of this theorem may however be mentioned here. If such a ring S does not possess an identity element, then S will be isomorphic to the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b ranging over a finite field.

In the final section of this paper we determine the structures of all rings (not necessarily possessing identity) with p^2 elements, and the structures of all rings, possessing identity, with p^3 elements, where p is any prime. It is found, in particular, that (i) there is essentially only one noncommutative ring of order p^2, e.g. a ring which is isomorphic or anti-isomorphic to the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b in the field $GF(p)$, and (ii) to within isomorphism there is only one ring of order p^3, with identity, which is not commutative, e.g. the ring of all 2×2 upper triangular matrices over the field $GF(p)$.

In conclusion the author wishes to thank Professor V. Ganapathy Iyer for his encouragement and guidance during the preparation of this paper. Thanks are due to N. Ganesan for having shown the author the two communications received from Eldridge, referred to above. Special thanks are due to J.-E. Björk (of Stockholm University) for having gone through an earlier version of this paper and for giving some suggestions which enabled the author to make some improvements in the contents, as well as in the presentation, of the paper.

Section 1

(1.1) In this section we consider a set $\mathfrak{M}$ which is, at the same time, a left vector space and a right vector space over a field P, and which is subject to the condition that $a(xb) = (ax)b$ for all a, b in P and for all x in $\mathfrak{M}$. Thus $\mathfrak{M}$ is a (P,P)-unital module with P a field. We now give two definitions which will be convenient in the sequel.

DEFINITIONS. Let $\mathfrak{M}$ be a (P,P)-unital module with P a field. (i) If x is an element of $\mathfrak{M}$ such that there exists an automorphism σ of the field P with $xa = a^{\sigma} \cdot x$ for all a in P, then x is to be called a *distinguished element of* $\mathfrak{M}$ *over* P. (ii) Let $\{x_i : i \in I\}$ be a basis of $\mathfrak{M}$ regarded as a left vector space over the field P. If each element of this basis is a distinguished element over P, then the set $\{x_i : i \in I\}$ is to be called a *distinguished basis of* $\mathfrak{M}$ *over the field* P.

The following comments are in order. First of all we remark that there is no point in these definitions if $\mathfrak{M} = (0)$, or if $\mathfrak{M}$ is one-dimensional over P, or if we had presupposed that $xa = ax$ for all a in P and all x in $\mathfrak{M}$. We may, therefore, neglect these rather trivial cases. Secondly we note that, in Definition (i), if the element x were not zero, then the automorphism σ will be uniquely determined by x so that σ may be called the automorphism of P associated with the distinguished (nonzero) element x of $\mathfrak{M}$. Thirdly, we remark that, in Definition (ii), the automorphisms associated with any two distinct elements of a distinguished basis may be different from each other. Finally, we note that a distinguished basis of $\mathfrak{M}$ is a basis for $\mathfrak{M}$ also when it is regarded as a right vector space over P — but it is clear that the notion of "distinguished basis" is more special than that of a "two-sided-basis".

The question that naturally arises now is whether there exists a distinguished basis for any two-sided unital module $\mathfrak{M}$ over any given field P. The following theorem shows that when $\mathfrak{M}$ has a finite number of elements — the case which is more than adequate for applications in the present paper — the answer is in the affirmative.

THEOREM 1. *Let* $\mathfrak{M}$ *be a finite-dimensional* (F, F)*-unital module, where* F *is the Galois field* $GF(q)$. *Then* $\mathfrak{M}$ *possesses at least one distinguished basis over the field* F.

PROOF. We suppose that $\mathfrak{M} \neq (0)$, and start with an arbitrary basis $\{y_1, \cdots, y_n\}$ of $\mathfrak{M}$ regarded as a left vector space over F. Let

g be a fixed cyclic generator [2] (= a generator of the cyclic multiplicative group of the nonzero elements) of the field F, and let

$$y_i \cdot g = \sum_{j=1}^{n} g_{ij} \cdot y_j \qquad (i = 1, \cdots, n)$$

for some elements g_{ij} in F. We can have these n equations together in the matrix form $Yg = GY$, where $Y = (y_1, \cdots, y_n)^T$ is the transpose of the row matrix formed by the basis elements y_i, and $G = (g_{ij})$ is an $n \times n$ matrix over the field F. We then get $Y \cdot g^k = G^k \cdot Y$ for every positive integer k. Now, for arbitrary $n \times n$ matrices A, B over F, the equation $AY = BY$ implies that $A = B$, since the set $\{y_1, \cdots, y_n\}$ is left linearly independent over F. This observation shows that $G^{(q-1)}$ equals the identity matrix of order n over F, and that the mapping

$$\begin{cases} g^k \to G^k & \\ 0 \to 0 & \end{cases} \qquad (k = 1, \cdots, q-1)$$

is a ring isomorphism. So we see that the zero matrix of order n and the powers of the (nonsingular) matrix G form a field L (say) of order q. As the minimal polynomial of the matrix G splits over the field F into distinct linear factors, there is a nonsingular matrix Q of order n such that $Q \cdot G \cdot Q^{-1} = \text{diag}\,(g_1, \cdots, g_n) = D$ (say) is a diagonal matrix over the field F. For each fixed i, and for arbitrary integers s, t we find that the equation $g_i^s = g_i^t$ implies that $G^s - G^t$ is a singular matrix belonging to the field L obtained above, and hence that $G^s = G^t$. From this we can conclude that, for each fixed i, the mapping

$$\begin{cases} g^k \to g_i^k & \\ 0 \to 0 & \end{cases} \qquad (k = 1, \cdots, q-1)$$

is an automorphism of the field F.

If $X = Q \cdot Y$ is the transpose of the row matrix $(x_1, \cdots, x_n)$ of elements x_i in $\mathfrak{M}$, then as $Xg = DX$ and as g is a cyclic generator of the field F, we see that $\{x_1, \cdots, x_n\}$ is a distinguished basis of $\mathfrak{M}$ over F.

This completes the proof of the theorem.

(1.2) Remark. We can use the above theorem to give a proof of the celebrated theorem of Wedderburn on finite division rings. More specifically, we may use the above theorem in the place of the

[2] The author owes this terminology to Mr. Björk.

last theorem in a paper of Zassenhaus [5] in order to complete the proof of Wedderburn's theorem.

Section 2

(2.1) The following easily proved results, due to Ganesan [2], are needed for our purpose, and so are stated here for convenient reference.

Let S be a finite associative ring, not necessarily possessing a multiplicative identity. Then the following results hold:

(i) *If there is an element x in S which is not a left zero divisor, then the ring S possesses at least one left identity.*

(ii) *If there is an element x which is a right zero divisor but is not a left zero divisor in S, then every element in the ring S $(= x \cdot S)$ is a right zero divisor in S.*

(iii) *If S possesses a multiplicative identity, then every non-invertible element of S is a two-sided zero divisor in S.*

(2.2) Let R be a finite ring with identity $1 \neq 0$, and let J denote the set of all the zero divisors in R. Obviously we need consider only the case where $J \neq (0)$, and we assume this in this section. A consideration of the situation where J is an additive group is found to be fruitful. As an immediate consequence we have the result that R will, then, be a completely primary ring with J as its radical. For, as R cannot have one-sided zero divisors, we see that J will be an ideal in R — in fact, J will be the unique maximal left ideal in R, so that J will be the Jacobson radical of the ring. As every element of R not in J is an invertible element, we see that the quotient ring R/J is a division ring, so that R is a completely primary ring.

We proceed to obtain some more properties of such a ring R in the following theorem which is fundamental for the purposes of the present paper.

THEOREM 2. *Let R be a finite ring with multiplicative identity $1 \neq 0$, whose zero divisors form an additive group J. Then*

(i) *J is the Jacobson radical of R;*

(ii) *$|R| = p^{nr}$, and $|J| = p^{(n-1)r}$ for some prime p, and some positive integers n, r;*

(iii) *$J^n = (0)$;* [3]

[3] In an earlier version of this paper, this was given as: $x \in J$ implies $x^n = 0$. The present form is due to Mr. Björk.

(iv) *the characteristic of the ring R is p^k for some integer k with $1 \leqq k \leqq n$; and*

(v) *if the characteristic is p^n, then R will be commutative.*

PROOF. We have already proved (i) and noted that R/J is a division ring. As R/J is finite, we see that it is the Galois field $GF(p^r)$ for some prime p and some positive integer r. As the element $p \cdot 1$ belongs to the nil ideal J, we find that the additive order of 1 is p^k for some positive integer k. This implies that $|R| = p^N$, and then that $|J| = p^{N-r}$ for some positive integer N (greater than r). So we have only to prove that $r \mid N$ in order to complete the proof of (ii). For this purpose we choose a fixed element g_1 in R such that (g_1+J) is a cyclic generator of the field $R/J \cong GF(p^r)$. As the invertible elements of the ring R form a multiplicative group G_R of order $(p^r-1) \cdot p^{N-r}$, we see that the multiplicative order of g_1 is $(p^r-1) \cdot p^s$ for some nonnegative integer s. Writing $g = g_1^{p^s}$ we find that we have obtained an element g with the following properties:

(A) g is an element of G_R with multiplicative order (p^r-1),

(B) for integers α, β the statement $(g^\alpha - g^\beta) \in J$ implies $g^\alpha = g^\beta$.

(A) is obvious, and (B) then follows from the fact that $(g+J)$ also is a cyclic generator of the field R/J. The existence of an element g with the above-mentioned properties will be found useful on a number of occasions in the sequel.

If we now write $x \sim y$ for x, y in R when, and only when $x = g^\alpha \cdot y$ for an integer α, we see that $\sim$ is an equivalence relation on the elements of R. As, for any nonzero element x of R the equation $g^\alpha \cdot x = g^\beta \cdot x$ implies $(g^\alpha - g^\beta) \in J$ and therefore that $g^\alpha = g^\beta$, we see that the p^N-1 nonzero elements of R split into equivalence classes where each class contains exactly p^r-1 elements. It follows that $(p^r-1) \mid (p^N-1)$ and then that $r \mid N$. If we write $N = nr$, we see that the proof of (ii) is complete.

The argument of the previous paragraph shows also that the number of elements in any left ideal in R is a power of p^r. So in the strictly descending sequence $J, J^2, \cdots, J^m$ of the powers of the nilpotent ideal J we must have $m \leqq n$, and in any case, we have $J^n = (0)$. Thus (iii) is proved, and (iv) follows immediately.

In order to prove (v) we first form the set

$$F_1 = \{0, g^k : k = 1, \cdots, p^r-1\}$$

of p^r elements and observe that, for elements a, b in F_1 the statement $a-b \in J$ implies $a = b$. If we now assume that the character-

istic of R is p^n, we can show, by induction on k, that, for elements a_k, b_k of F_1 the equation $\sum_{k=0}^{n-1} p^k \cdot a_k = \sum_{k=0}^{n-1} p^k \cdot b_k$ will imply that $p^{n-1} \cdot (a_k - b_k) = 0$, and then that $a_k = b_k$ for $k = 0, \cdots, n-1$. This shows that every element of R will be (uniquely) expressible in the form $\sum_{k=0}^{n-1} p^k \cdot a_k$ with a_k in F_1, so that R will be a commutative ring.

This completes the proof of the theorem.

(2.3) In this subsection we collect together a number of miscellaneous properties of a ring of the type considered in Th. 2. Throughout this subsection the symbols R, J, p, r, n are as in Th. 2.

(i) We first remark that *any subring R_1 of R is also a ring of the type considered in Th.* 2. For, if x is any element of R, there exists a positive integer m such that $x^m = 0$ or $x^m = 1$ according as x does or does not belong to the set J. From this we see that an element x of the subring R_1 will be invertible (a zero divisor) in R_1 if, and only if it is invertible (resp. a zero divisor) in the larger ring R, so that the set J_1 of all the zero divisors of R_1 is $J \cap R_1$. This proves the remark made earlier, and if p_1, r_1, n_1 (with obvious notation) refer to the subring R_1, we have $p_1 = p$, and r_1 as a factor of r, because G_{R_1} is a subgroup of G_R. There seems to be no such simple relationship between the integers n_1 and n. Of course, the characteristic of R_1 is the same as that of R.

(ii) We next observe that *any homomorphic image $R_1 \neq (0)$ of R is also a ring of the type considered in Th.* 2. For, the kernel K of a nontrivial homomorphism of R is a nil ideal in R, and it can be easily verified that an element x of R will be invertible in R if, and only if the element $(x+K)$ is invertible in the quotient ring R/K. This proves the assertion made above, and if J_1, p_1, r_1, n_1 refer to the homomorphic image $R_1 \neq (0)$ of R, we see that $p_1 = p$, $r_1 = r$ (this because $|K|$ is a power of p^r), $n_1 \leqq n$, and $J^{n_1} \subseteq K$. In case $J^{n-1} \neq (0)$ we have actually $J^{n_1} = K$, from which we can conclude that there are at least $n-1$ nontrivial homomorphisms on a ring of Th. 2 when $J^{n-1} \neq (0)$.

(iii) Then we remark that *the multiplicative group G_R is solvable.* For, as the quotient ring R/J is commutative, we find that $a^{-1} \cdot b^{-1} \cdot a \cdot b \in \{1+J\}$ for all a, b in G_R, and as $1+J$ is a multiplicative subgroup whose order is a power of a prime we can conclude that G_R is solvable.

(iv) *Let G_1 be the cyclic group of order p^r-1 generated by the element g introduced in the proof of Th.* 2(ii). *If G_2 is any subgroup of order p^r-1 in the group G_R, then the subgroups G_1 and G_2 are*

conjugate with each other in G_R. This follows from the Sylow theory of finite solvable groups, since the order of the subgroup G_1 is prime to its index in the (solvable) group G_R.

(v) Let G_1 be as in (iv) above and let N denote the normaliser of G_1 in the group G_R. For elements a in G_1, b in N we have $a^{-1} \cdot b^{-1} \cdot a \cdot b \in G_1 \cap \{1+J\} = \{1\}$, so that we find that *the normaliser of the subgroup* G_1 *coincides with the centraliser of* G_1 *in the group* G_R.

(vi) *Let* F_1 *be the set introduced in the proof of Th.* 2(v). *If the group* G_R *contains a normal subgroup of order* p^r-1, *then the set* F_1 *will be contained in the centre of the ring* R.

For, if G_1 is the multiplicative group of the p^r-1 nonzero elements of the set F_1, the result in (iv) above shows that G_1 is the unique normal subgroup of order p^r-1 in G_R, and the result in (v) above then shows that G_1 is contained in the centre of the group G_R. Now, as the statements $x \in R$, $x \notin G_R$ imply $1+x \in G_R$, we see that every element of the ring R commutes with every element of G_1. The desired result now follows.

(vii) In the proof of Th. 2 we introduced the set

$$F_1 = \{0, g^k : k = 1, \cdots, p^r-1\}$$

of p^r elements, which looks very much like the field $GF(p^r)$. So we will be naturally interested in knowing as to when this set will be a subfield of R. The obvious necessary condition — namely that the characteristic of R should be p — is easily found to be also sufficient. To see this, assume that the characteristic of R is p and take two distinct elements a, b of F_1 so that $a-b \in G_R$. If R_1 is the subring of R generated by the elements of F_1, we see that G_1 (as in (iv) above) is the unique subgroup of order p^r-1 in the (commutative) group G_{R_1}. As $(a-b)^q = a^q-b^q = a-b$, and so $(a-b)^{q-1} = 1$, where $q = p^r$, we see that $a-b \in G_1 \subset F_1$. Thus we have proved the first of the following two results:

Let R, p, r *be as in Th.* 2. *Then* R *contains a subfield of order* p^r *if, and only if the characteristic of* R *is* p. *Also if* F_1, F_2 *are two subfields of order* p^r *in* R, *then there is an invertible element* a *of* R *such that* $a^{-1} \cdot F_1 \cdot a = F_2$.

The second statement follows from the result in (iv) above. These results will be generalised in the next section.

(2.4) If R, p, r, n are as in Th. 2 we consider, in this subsection, the situation where R contains a subfield F of order p^r. We suppose first that F is contained in the centre of the ring R. Then

(and only then) we can regard R as a linear algebra over the field F. Once a basis for R over F is chosen we can use the right regular representation of R to exhibit it as a ring of matrices of order n over the field $GF(p^r)$. This simple process for exhibiting R as a ring of matrices of (this particular) order n over the field F will not be available if we do not presuppose that the subfield F of (the maximal) order p^r is contained in the centre of the ring R. The following two theorems show however that, in two special cases, it is possible to represent R as a ring of $n \times n$ matrices over the field $GF(p^r)$ — even if the subfield F is not contained in the centre of the ring R.

THEOREM 3. *Let R, J, p, r, n be as in Th. 2, and let the characteristic of R be p. If $J^2 = (0)$, then R is isomorphic to the ring of all $n \times n$ matrices of the form*

$$\begin{pmatrix} h_1 & f_2 & f_3 & \cdots & f_n \\ 0 & h_2 & 0 & \cdots & 0 \\ 0 & 0 & h_3 & \cdots & 0 \\ \cdots & & & & \\ 0 & 0 & 0 & \cdots & h_n \end{pmatrix}$$

where $h_1, f_2, \cdots, f_n$ range over the field $GF(p^r)$, and for $i = 2, \cdots, n$, $h_i = h_1^{s_i}$ with $s_i = p^{t_i}$ for some fixed integers t_i with $1 \leqq t_i \leqq r$.

Conversely, for every choice of the integers t_i the ring of matrices described above is a ring of the type considered in Th. 2 with characteristic p whose radical J satisfies $J^2 = (0)$.

PROOF. The straightforward proof of the converse part will be omitted. For the direct part, we suppose that $n \geqq 2$, and note that the ring R contains a subfield F of order p^r. Keeping F fixed, we get a distinguished basis (refer § 1) $\{x_2, \cdots, x_n\}$ of $n-1$ elements for J over F. If g is a fixed cyclic generator of the field F, and if $x_1 = g$, we see that $\{x_1, x_2, \cdots, x_n\}$ is a distinguished basis for the entire ring R over the field F. Let, for each $i \geqq 2$, $x_i \cdot g = g^{s_i} \cdot x_i$ with $s_i = p^{t_i}$ for some integers t_i such that $1 \leqq t_i \leqq r$. Our hypothesis that $J^2 = (0)$ implies that $x_i \cdot x_j = 0$ for all $i \geqq 2$, and all $j \geqq 2$.

Now we define n square matrices $X_1, X_2, \cdots, X_n$ of order n over the field F as follows: $X_1 = G = \text{diag}\,(g, g^{s_2}, g^{s_3}, \cdots, g^{s_n})$, and for each j greater than one, X_j is the matrix with 1 in the $(1, j)$-th entry and zeros elsewhere. The following results are then easily verified: $X_i \cdot G^k = G^{ks_i} \cdot X_i$, $G^k \cdot X_i = g^k \cdot X_i$, and $X_i \cdot X_j = 0$, for all $i \geqq 2$, all $j \geqq 2$, and all $k \geqq 1$. The mapping

$$\begin{cases} g^k \to G^k & (k = 1, \cdots, p^r-1) \\ 0 \to 0 \end{cases}$$

is easily verified to be an isomorphism of the field F into the ring of all $n \times n$ matrices over F; we shall denote the image of any element h_1 or f_j of F under this isomorphism by the corresponding capital letter (viz) H_1 or F_j respectively. Then the mapping

$$(h_1 + f_2x_2 + f_3x_3 + \cdots + f_nx_n) \to (H_1 + F_2X_2 + F_3X_3 + \cdots + F_nX_n)$$

as the elements $h_1, f_2, \cdots, f_n$ range over the field F, can be verified to be an isomorphism defined on all of the ring R onto the ring of all $n \times n$ matrices of the form given in the statement of the theorem.

This completes the proof of the theorem.

THEOREM 4. *Let R, J, p, r, n be as in Theorem 2, and let the characteristic of R be p. If $J^{n-1} \neq (0)$, then R will be isomorphic to the ring of all $n \times n$ upper triangular matrices (a_{ij}) over the field $GF(p^r)$ which satisfy the condition*

$$a_{i+1,\,j+1} = a_{ij}^{\,s} \qquad (i, j = 1, 2, \cdots, n-1)$$

where $s = p^t$ and t is some fixed positive integer with $t \leqq r$.

Conversely, for every choice of the positive integer t, the ring of matrices described above is a ring of the type considered in Theorem 2 with characteristic p whose radical J satisfies the condition $J^{n-1} \neq (0)$.

PROOF. In view of Theorem 3, we may suppose that $n \geqq 3$. We take a fixed subfield F of order p^r in the ring R, and then obtain a distinguished basis $\{y_2, \cdots, y_n\}$ of J over the field F. We note that at least one of the basis elements y_i does not belong to the ideal J^2 (which is of order $p^{(n-2)r}$). If y is a distinguished element of J over F such that $y \notin J^2$, then we assert that $y^{n-1} \neq 0$. [4] To see this, suppose the contrary that $y^{n-1} = 0$. Firstly, for arbitrary elements $f_1, f_2, \cdots, f_{n-1}$ of the field F, we have

$$(f_1y)(f_2y) \cdots (f_{n-1}y) = 0$$

if $y^{n-1} = 0$, since y is a distinguished element over F; and then, for arbitrary elements $z_1, \cdots, z_{n-1}$ of J^2 we find

$$(f_1y + z_1) \cdots (f_{n-1}y + z_{n-1}) = 0,$$

since $J^n = (0)$. But as every one of the $p^{(n-1)r}$ elements of J is uniquely expressible in the form $fy + z$ with f in F and z in J^2, the

[4] This observation is due to Mr. Björk.

above shows that the supposition $y^{n-1} = 0$ will lead to $J^{n-1} = (0)$, a contradiction. Thus our assertion that $y^{n-1} \neq 0$ is proved. Let now $y \cdot h = h^s \cdot y$ for all h in the field F, where $s = p^t$ with t a fixed positive integer (independent of h in F) such that $t \leqq r$. We then take the $n \times n$ matrix $Y = (y_{ij})$ with $y_{ij} = 1$ if $j - i = 1$ $(i = 1, \cdots, n-1)$ and $y_{ij} = 0$, otherwise. After this stage, the proof proceeds exactly as in the previous theorem. More explicitly, we have to consider the isomorphisms

$$h \to H = \text{diag}\,(h, h^s, h^{s^2}, \cdots, h^{s^{n-1}}) \qquad (h \in F)$$

and

$$(h_0 + h_1 y + \cdots + h_{n-1} y^{n-1}) \to (H_0 + H_1 Y + \cdots H_{n-1} Y^{n-1})$$

with the convention of the previous theorem. This completes the proof of the direct part of the theorem.

(2.5) Remark. For given p, r, n (with n greater than one) we see that there are at most r mutually nonisomorphic rings of the type considered in Th. 4, and when $r \geqq 2$ there are at least two distinct types. For, if we suppose that r is greater than one, we have for $t = 1$ $(< r)$ a noncommutative ring, while for $t = r$ (> 1) we have a commutative ring which can also be described as $F[x]/(x^n)$, the ring of polynomials in the indeterminate x over the field F, modulo the ideal generated by the element x^n in it.

(2.6) The following theorem mentions two conditions which are sufficient to force a ring of Th. 2 to be commutative.

Theorem 5. *Let R, J, p, r, be as in Th. 2. Let* (1) *any two elements of J commute with each other, and* (2) *the multiplicative group G_R of the invertible elements of R contain a normal subgroup of order $p^r - 1$. Then R will be commutative.*

Proof. Let F_1 be the set introduced in the proof of Th. 2. If the condition (2) of this theorem holds, the result in §(2.3) (vi) shows that the set F_1 will be contained in the centre of the ring R. As every element of R is uniquely expressible in the form $f + x$ with f in F_1 and x in J, we see that the condition (1) of this theorem will, then, imply that the entire ring R is commutative.

(2.7) Remarks. (i) If R, J, p, r, n be as in Th. 2, the ring R will reduce to the field $GF(p^r)$ when $J = (0)$ (i.e.) $n = 1$. So Th. 5 is a generalisation of Wedderburn's theorem to completely primary rings of finite order. Of course, the proof of Th. 5 makes essential use of Wedderburn's theorem.

(ii) There are two conditions in the hypothesis of Th. 5. The first of these is obviously necessary for the validity of the conclusion of the theorem. It may be asked whether this condition alone is sufficient. That the answer to this question is in the negative is seen in the example of a ring R of Th. 4 for $n = 2, r \geqq 2$, and $t = 1$. As $J^2 = (0)$, the first condition in the hypothesis of Th. 5 is satisfied, but this ring is not commutative. (See §(2.5)).

Section 3

(3.1) Let R, p, r, n be as in Th. 2. We have seen that the characteristic of R is p^k for some integer k with $1 \leqq k \leqq n$, and in the previous section we considered two cases where k was the smallest possible (i.e.) where the characteristic of R was p. In the present section we will consider the other extreme — the case where the characteristic is p^n. We recall that we have already proved that the ring must be commutative in this case. When $n = 1$ (and p, r are arbitrary) we note that the ring R of Th. 2 reduces to the Galois field $GF(p^r)$, while when $r = 1$ (and p, n are arbitrary) we note that the ring of Th. 2(v) is the ring $Z/(p^n)$ of integers modulo p^n. More generally we will prove, in the course of this section, that there exists one and, in the sense of isomorphism, only one ring of the type considered in Th. 2(v) for any given prime p, and for any given positive integers n, r. As regards existence, we can verify that the ring of Witt vectors of length n (refer Jacobson [3, Ch. III, § 4, especially Ths. 11 and 12]) over the field $GF(p^r)$ is a ring of the type considered in Th. 2(v). We shall however establish the desired results without appealing to the construction of Witt rings. For this purpose, we begin with a tentative definition.

Definition. Let Z denote the ring of all integers, x an indeterminate, p a prime, and n, r arbitrary positive integers. Let

$$f(x) = x^r + \sum_{i=0}^{r-1} a_i \cdot x^i \in Z[x]$$

be a monic polynomial of degree r which is irreducible modulo the prime p, and let (p^n, f) denote the ideal generated by the two elements p^n and f in the polynomial ring $Z[x]$. Then the quotient ring

$$R' = Z[x]/(p^n, f)$$

is to be called the *Galois ring* of order p^{nr} and characteristic p^n, and is to be denoted by the symbol $GR(p^{nr}, p^n)$.

The following remarks are in order. Firstly, we note that if the numerical values of the order (viz) p^{nr} and the characteristic (viz) p^n are given, with the understanding that p is a prime, then the values of p, n, and r are uniquely determined. Secondly, we note that at least one polynomial f with the required properties exists in $Z[x]$ for any given prime p, and for any given positive integers n, and r. To show that the definition makes sense we have only to prove that the ring R' is actually independent of the particular polynomial f used in its construction. This will be accomplished by showing that the following two statements are true.

(I) *For any particular choice of the polynomial f as in the above definition, the ring R' of the definition is a ring of the type considered in Th.* 2(v).

(II) *Any ring of the type considered in Th.* 2(v) *is isomorphic to the ring R' (for suitable values of p, r, n) obtained in* (I).

While the first statement can be proved straightaway, the proof of the second one requires some preliminary results (Th. 6 and its corollaries) which, however, appear to be of independent interest.

We proceed to prove the statement (I), assuming that n is a fixed integer greater than one. First of all we note that R' is a commutative ring with a multiplicative identity, that its characteristic is p^n, and that it has p^{nr} elements. So it remains only to show that the ring contains exactly $p^{(n-1)r}$ zero divisors, and that these zero divisors form an additive group. We note that the set $K = p \cdot R'$ is a nilpotent ideal of order $p^{(n-1)r}$ in R'. So the proof of the statement (I) will be complete if we show that every element of R' not in the ideal K is an invertible element of R'.

We now denote by A the ideal (p^n, f) and by B the ideal (p, f) in the polynomial ring $Z[x]$. Then we note that $Z[x]/A$ is the ring R' and that $Z[x]/B = F$ is the Galois field $GF(p^r)$. As the ideal A is contained in B, we see that the identity mapping on the ring $Z[x]$ induces a well-defined homomorphism on R' onto F whose kernel is the ideal K in R'. Now if an element a of R' does not belong to K, it will be mapped by the above homomorphism into a nonzero element of the field F; as K is a nil ideal, this implies that a is invertible in R'. This completes the proof of the statement (I).

(3.2) Throughout this subsection and the next, the symbol x will be used to denote an indeterminate. *For any ring S with identity, we consider the homomorphism $f \to f_S$ of $Z[x]$ into $S[x]$ defined as follows: if $f(x) = \sum a_k \cdot x^k \in Z[x]$, then*

$$f_S(x) = \sum(a_k \cdot 1) \cdot x^k \in S[x],$$

where 1 *is the identity element of* S. The use of this notation is found to be convenient in Th. 6 and its corollaries, in the course of the proofs of which we use some obvious properties of the mapping $f \to f_S$ without explicitly stating them.

Let K be an ideal in the above ring S, and for any element a of S let $\bar{a}$ denote the element $(a+K)$ of the quotient ring $\bar{S} = S/K$. Let f be any given element of $Z[x]$, and suppose that the equation $f_S(x) = 0$ has a solution, say u, in the ring S. Then the corresponding equation $f_{\bar{S}}(x) = \bar{0}$ will have a solution (e.g. $\bar{u}$) in the quotient ring $\bar{S} = S/K$. The following theorem shows that, under certain conditions, a converse of the result just stated is also true.

THEOREM 6. *Let* S *be any ring with identity* $1 \neq 0$. *Let* f *be any element of the polynomial ring* $Z[x]$, *and let* f' *denote the formal derivative of* f. *Let* K *be a nil ideal in* S, *and let* $\bar{a}$ *denote the coset* $(a+K)$ *for any element* a *in* S.

If the equation $f_{\bar{S}}(x) = \bar{0}$ *has a solution* $\bar{u}$ *in the quotient ring* $\bar{S} = S/K$ *such that* $f'_{\bar{S}}(\bar{u})$ *is an invertible element in* $\bar{S}$, *then there exists at least one element* α *in the larger ring* S *with the properties*: $f_S(\alpha) = 0$, *and* $\bar{\alpha} = \bar{u}$.

PROOF. As K is a nil ideal, we note first that an element a of S will be invertible in S if, and only if the element $a+K$ is invertible in the quotient ring S. Let u be a particular element of S such that $\bar{u} = u+K$ has the two properties mentioned in the hypothesis of the theorem. Keeping u fixed, we now construct two subrings S_0, S_1 of S as follows. Firstly, S_0 is the subring of S generated by the element u and the identity of S. Then all the elements of S_0 and the inverses (in the ring S) of all the invertible elements of S_0 are used to generate the subring S_1. (Note: If an element a of the subring S_0 has an inverse a^{-1} in the larger ring S, it is not necessary that a^{-1} belongs to the subring S_0). So we see that S_1 is a commutative subring of S containing S_0.

If we write $a = f_{S_1}(u) = f_S(u)$, we easily see that

$$f_{S_1}(u) = a \in K \cap S_0 \subseteq K \cap S_1. \tag{1}$$

We now wish to find an element y_1 in $K \cap S_1$ such that $f_S(u+y_1) = 0$. If we provisionally assume the existence of such an element y_1 and write $\alpha = u+y_1$, then we get $f_S(\alpha) = 0$, and $\bar{\alpha} = \bar{u}$, which are precisely what we want. So we proceed to consider the elements $f_{S_1}(u+y)$ as y ranges over the ring S_1. As u belongs to the commu-

tative ring S_1 we can expand $f_{S_1}(u+y)$ in powers of y as follows:

$$f_{S_1}(u+y) = a+y \cdot f_1(u)+ \cdots +y^r \cdot f_r(u), \tag{2}$$

for all y in S_1, where the $f_i(u)$, $i = 1, \cdots, r$, are independent of y. The coefficients a, $f_1(u)$, $\cdots$, $f_r(u)$ all belong to the subring S_0, and we note that $f_1(u) = f'_S(u)$ is the formal derivative of the polynomial $f_{S_1}(u)$ in u. By hypothesis, $\overline{f_1(u)} = \overline{f'_S(u)} = f'_{\bar{S}}(\bar{u})$ is an invertible element of the quotient ring $\bar{S}$, so that $f_1(u)$ $(\in S_0)$ is an invertible element of the original ring S. On multiplying by $(f_1(u))^{-1}$, which is an element of the subring S_1, the equation (2) above becomes

$$(f_1(u))^{-1} \cdot f_{S_1}(u+y) = -b+y+a_2y^2+ \cdots +a_ry^r, \tag{3}$$

for all y in the subring S_1, where $-b = (f_1(u))^{-1} \cdot a \in K \cap S_1$, the coefficients a_2, $\cdots$, a_r belong to S_1, and where the coefficients b, a_2, $\cdots$, a_r are all independent of y. As K is a nil ideal by our hypothesis, we have $b^{n+1} = 0$ for some positive integer n. Now with α_2, $\cdots$, α_n as arbitrary elements of the subring S_1, let us substitute the element

$$b+\alpha_2b^2+\alpha_3b^3+ \cdots +\alpha_nb^n \tag{4}$$

of $K \cap S_1$ for y in the relation (3). As $b^{n+1} = 0$ the equation (3), then, becomes

$$(f_1(u))^{-1} \cdot f_{S_1}(u+y) = \beta_2b^2+\beta_3b^3+ \cdots \beta_nb^n \tag{5}$$

where

$$\beta_2 = \alpha_2+a_2$$

and

$$\beta_s = \alpha_s+c_s \quad \text{for } s \geqq 3,$$

with c_s as a well defined polynomial in the elements $a_2, \cdots, a_s$ and α_2, $\cdots$, α_{s-1} only with integer coefficients. We note that the elements $c_3, \cdots, c_n$ all belong to the subring S_1 and that these are all independent of b. We can now successively choose the (so far arbitrary) elements $\alpha_2, \alpha_3, \cdots, \alpha_n$ (in the subring S_1) in such a way that all the coefficients β_i in the equation (5) above vanish. If y_1 is the value of y given by the expression (4) above for this particular choice of values of $\alpha_2, \cdots, \alpha_n$, we find that $y_1 \in K \cap S_1$, and that $f_S(u+y_1) = 0$, from equation (5).

This completes the proof of the theorem.

(3.3) We now give some corollaries to the above theorem. The

first of these is a partial statement of a wellknown result on "lifting" an idempotent element form the quotient ring modulo a nil ideal to the original ring.

COROLLARY 1. *Let S be any ring with identity 1 $(\neq 0)$ and let K be a nil ideal in S. If $\bar{u} = u+K$ is an idempotent in the quotient ring $\bar{S} = S/K$, then there exists at least one idempotent element α in S such such that $\bar{\alpha} = \bar{u}$.*

For, if $f(x) = x^2 - x \in Z[x]$, we note that $f'_S(\bar{u})$ is its own inverse in the ring $\bar{S}$.

COROLLARY 2. *Let R, J, p, r, n be as in Th. 2, and let $f(x) = x^r - \sum_{i=0}^{r-1} a_i \cdot x^i \in Z[x]$ be a monic polynomial of degree r which is irreducible modulo the prime p. Then the equation $f_R(x) = 0$ has at least one solution in R which is an invertible element of R.*

PROOF. Let P be the prime field contained in the quotient ring $\bar{R} = R/J \cong GF(p^r)$. The hypothesis implies that the polynomial f_P is of degree r and that it is irreducible over the field P. It follows that the equation $f_P(x) = \bar{0}$ has r roots in the field R/J, each of which is a simple root. If $\bar{u}$ is one of these roots, we see that the nonzero element $f'_P(\bar{u})$ is an invertible element of $\bar{R}$. As f_P is just the restriction to P of the polynomial $f_{\bar{R}}$, we see that Th. 6 is now applicable. Also if α is a solution of the equation $f_R(x) = 0$ such that $\bar{\alpha} = \bar{u}$, we see that α is invertible in R, since $\bar{u}$ is a nonzero element of the field R/J.

COROLLARY 3. *This is a continuation of the previous corollary. Let R, J, p, r, n be as in Th. 2, and let the polynomial f be as in the previous corollary. Let α be a particular solution of the equation $f_R(x) = 0$. If the characteristic of R is p^k $(1 \leqq k \leqq n)$, then the subring generated by α will be isomorphic to the ring*

$$Z[x]/A$$

of residue classes modulo the ideal A generated by the elements p^k and f in the polynomial ring $Z[x]$. Also $|R_1| = p^{kr}$.

PROOF: The element $\bar{\alpha} = \alpha+J$ is a zero of the monic polynomial f_P which is irreducible over the prime field P. Thus the minimal polynomial of $\bar{\alpha}$ over P is f_P and this is of degree r.

We now assert that for integers n_i with $1 \leqq n_i \leqq p^k$, the equation

$$\sum_{i=0}^{r-1} (n_i \cdot 1) \cdot \alpha^i = 0 \tag{1}$$

will imply $n_i = p^k$ for each i. (The 1 in the above equation is the identity element of the ring R.) For, suppose that p^β $(0 \leqq \beta \leqq k)$ is the highest power of the prime p which is a factor of all the integers n_i in (1). If we write $n_i = p^\beta \cdot m_i$, then at least one of the integers m_i will be prime to p. The equation (1) becomes

$$p^\beta \cdot \Big(\sum_{i=0}^{r-1} m_i \cdot 1 \cdot \alpha^i \Big) = 0. \tag{2}$$

As the additive order of every invertible element of R is p^k, the supposition that $0 \leqq \beta < k$ will imply that the expression within parentheses on the left side of (2) must give an element of J, so that

$$\sum_{i=0}^{r-1} m_i \cdot \bar{1} \cdot \bar{\alpha}^i = \bar{0}. \tag{3}$$

As at least one of the integers m_i is prime to p, the equation (3) is contradictory to the fact that the minimal polynomial of $\bar{\alpha}$ over the field P is of degree r. This proves the assertion made at the beginning of this paragraph.

As α is an invertible element of the (finite) ring R, some positive integral power of α equals the identity of R. Also, as α is a zero of the (monic) polynomial f_R, we see that the subring R_1 generated by α is given by

$$R_1 = \{ \sum_{i=0}^{r-1} (n_i \cdot 1) \cdot \alpha^i : 1 \leqq n_i \leqq p^k \}.$$

The argument of the previous paragraph shows that $|R_1| = p^{kr}$ and this completes the proof of the corollary.

(3.4) The case $k = n$ of the Cor. 3 to Th. 6 proves the statement (II) made in §(3.1), thus showing that the definition of Galois ring given there is quite a legitimate one. For purposes of reference we formally state the following theorem which, in view of our method of proving that the definition of Galois ring makes sense, is a tautology.

THEOREM 7. *Let R be a finite completely primary ring with radical J, so that $|R| = p^{nr}$ and $|J| = p^{(n-1)r}$ for some prime p and some positive integers n, r. If the characteristic of R is the largest possible under these conditions, that is if the characteristic is p^n, then R will be commutative — in fact R will be the Galois ring $GR(p^{nr}, p^n)$.*

The first part of the conclusion is just a restatement of Th. 2(v); but the second part gives more specific information. It may be remarked that the above theorem generalises, in a perfect manner,

Wedderburn's theorem on finite division rings to the case of completely primary rings with a finite number of elements. The proof of this theorem however makes use of Wedderburn's theorem.

(3.5) It now follows that the Galois ring $GR(p^{nr}, p^n)$ is isomorphic to the ring of Witt vectors of length n over the field $GF(p^r)$.

It is not, however, immediately obvious as to how one can prove that any ring of Th. 2(v) is isomorphic to a Witt ring — without using Th. 6.

(3.6) We can now generalise the results of §(2.3)(vii) to the following theorem.

THEOREM 8. *Let R, p, r be as in Th. 2. Then*

(i) *R will contain a subring isomorphic to $GR(p^{kr}, p^k)$ if, and only if the characteristic of R is p^k, and*

(ii) *if R_2, R_3 are any two subrings of R, both isomorphic to $GR(p^{kr}, p^k)$, there will be an invertible element a in R such that $R_2 = a^{-1} \cdot R_3 \cdot a$.*

PROOF. The first statement follows immediately from Cor. 3 to Th. 6. To prove (ii) it is enough if we show that the subring R_1 generated by the element g introduced in the proof of Th. 2 is such that $R_1 = b^{-1} \cdot R_2 \cdot b$ for some invertible element b in R. Let G_1 be the cyclic group of order (p^r-1) generated by the element g. The solvable group G_{R_2} contains a subgroup G_2 of order (p^r-1), and so $G_1 = b^{-1} \cdot G_2 \cdot b$ for some invertible element b of R. (Refer §(2.3)(iii) and (iv).) So we find that $R_1 \subseteq b^{-1} \cdot R_2 \cdot b$. Now proceeding as in the proof of Cor. 3 to Th. 6, we can show that the subset

$$\{\sum_{i=0}^{r-1} (n_i \cdot 1) \cdot g_i : 1 \leqq n_i \leqq p^k\}$$

of the subring R_1 contains p^{kr} distinct elements. It follows that $R_1 = b^{-1} \cdot R_2 \cdot b$, and so the proof of the theorem is complete.

(3.7) We now take up Th. 6 for further consideration. Throughout this subsection we will continue to use the notation employed in the statement and proof of this theorem. Th. 6 provides us with "at least" one element α in S with the properties: $f_S(\alpha) = 0$, and $\bar{\alpha} = \bar{u}$. Naturally we would like to know whether the element α is uniquely determined by the last-mentioned two conditions. If S_2 is any commutative subring of S containing the subring S_1 we can prove that there is only one element α in S_2 with the desired

properties. (We recall that the subring S_1 depends on the particular choice of the element u in its coset $u+K$.) *In the particular case where S is a commutative ring we can then assert the uniqueness of α in the entire ring S.*

We now prove the desired result by showing that, for elements y, z in $K \cap S_2$ the equation

$$f_{S_2}(u+y) = f_{S_2}(u+z)$$

will imply that $y = z$. As S_2 is a commutative ring we can expand the two sides of the above equation in powers of y, z to get

$$(y-z) \cdot (c+d) = 0,$$

where $c = f_1(u)$ is an invertible element of S, and

$$d = ((y+z) \cdot f_2(u)+(y^2+yz+z^2) \cdot f_3(u)+ \cdots) \in K \cap S_2.$$

As $(c+d)$ is an invertible element of the ring S, the above equation implies $y-z = 0$, thus proving the desired result.

(3.8) As finite fields and the rings $Z/(p^n)$ are special cases of Galois rings we may expect some of the properties of these special rings to carry over to Galois rings. The results of this subsection and the next illustrate this remark. As an immediate illustration we have the following

PROPOSITION 1. *Every subring of the ring $GR(p^{nr}, p^n)$ is of the form $GR(p^{ns}, p^n)$ for some divisor s of r. Conversely, for every positive divisor s of r there is a unique subring of R which is isomorphic to the ring $GR(p^{ns}, p^n)$.*

The first of these two results follows from §(2.3)(i) and Th. 7, while the second can be proved by using Ths. 6 and 8.

We next consider the set of all automorphisms on a Galois ring.

PROPOSITION 2. *The automorphisms of the ring $GR(p^{nr}, p^n)$ form a cyclic group of order r.*

PROOF: As the result is obvious for $r = 1$ (in which case the ring is $Z/(p^n)$), we may suppose that $r \geqq 2$ in what follows. Let R denote the ring $GR(p^{nr}, p^n)$ and let g be the element introduced in the proof of Th. 2(ii), so that we have

$$R = \{\sum_{i=0}^{r-1} (n_i \cdot 1)g^i : n_i \in Z, 1 \leqq n_i \leqq p^n\}.$$

Then there exists a polynomial $f(x) = x^r - \sum_{i=0}^{r-1} a_i \cdot x^i \in Z[x]$, irreducible modulo the prime p such that $f_R(g) = 0$. Looking at

the proof of the Cor. 2 to Th. 6 and the discussion in §(3.7) above, we see that the equation $f_R(x) = 0$ has exactly r distinct roots in the ring R. If h be any one of these roots it is easily verified that the mapping

$$\sum_{i=0}^{r-1} (n_i \cdot 1)g^i \to \sum_{i=0}^{r-1} (n_i \cdot 1)h^i \qquad (n_i \in Z)$$

is an automorphism on the ring R. Thus we see that there are at least r distinct automorphisms on R.

Let now ϕ be any automorphism of R and let h be the image under ϕ of the element g. As $f_R(g) = 0$, we have $f_R(h) = 0$. If P is the prime field contained in the quotient ring $\bar{R} = R/J \cong GF(p^r)$, as $f_P(\bar{g}) = \bar{0} = f_P(\bar{h})$, we find that $\bar{h} = (\bar{g})^{p^k}$ for some positive integer k, so that $h = g^{p^k} \cdot (1+pa)$ for some element a of the ring R. Firstly we note that $1+pa \in 1+pR = G_2$, say, where G_2 is a multiplicative group of order $p^{(n-1)r}$. If G_1 is the cyclic group generated by the element g, then G_1 is the unique subgroup of order (p^r-1) in the group G_R. As any automorphism of the ring R will map G_1 onto itself we find that $h \in G_1$ and therefore that $1+pa = g^{-p^k} \cdot h \in G_1 \cap G_2 = \{1\}$. It follows that $h = g^{p^k}$. So the image of the element g under any automorphism of the ring R can be only one of the r distinct elements $g^p, g^{p^2}, \cdots, g^{p^r} = g$. As the image of the single element g under any automorphism ϕ will completely determine ϕ, we see, from the observation in the previous sentence and the result proved in the last paragraph, that there are exactly r automorphisms on the ring R and that these form a cyclic group. This completes the proof.

In the above two propositions the Galois rings resemble the Galois fields. On the other hand, in Prop. 3 and in Th. 9 to follow the Galois rings will be found to behave like the rings $Z/(p^n)$.

PROPOSITION 3. *For fixed p and r, let R_n denote the ring $GR(p^{nr}, p^n)$. Then any homomorphic image $(\neq (0))$ of R_n is the ring R_m for an integer m with $1 \leqq m \leqq n$. Conversely, for every integer m with $1 \leqq m \leqq n$ there are exactly r homomorphisms of R_n onto R_m.*

PROOF. The first result follows from the facts that the only proper ideals of R_n are $p^m \cdot R_n$ for $m = 1, \cdots, n$ and that $R_n/(p^m \cdot R_n)$ is isomorphic to R_m. (See §(2.3)(ii) and Th. 7). The second result follows from the fact that any homomorphism of R_n onto R_m is the composition of the canonical mapping followed by an automorphism of R_m.

(3.9) The following theorem describes the structure of the multiplicative group G_R for any Galois ring R.

THEOREM 9. *Let G be the multiplicative group of the invertible elements of the ring $GR(p^{nr}, p^n)$, where p is a prime. Then G is the direct product of a cyclic group G_1 of order (p^r-1) and a group G_2 of order $p^{(n-1)r}$ whose structure is described below.*

(1) *If* (a) *p is odd, or if* (b) *$p = 2$ and $n \leqq 2$, then G_2 is the direct product of r cyclic groups each of order $p^{(n-1)}$.*

(2) *When $p = 2$ and $n \geqq 3$, the group G_2 is the direct product of a cyclic group of order 2, a cyclic group of order $2^{(n-2)}$ and $(r-1)$ cyclic groups each of order $2^{(n-1)}$.*

PROOF: We may suppose that $n \geqq 2$. To begin with, we suppose that $r \geqq 2$ also. The modifications in the proof necessary for the case $r = 1$ will then be obvious and so will be omitted.

So we assume that R denotes the ring $GR(p^{nr}, p^n)$ where n, r are fixed positive integers both greater than 1. Let J be the Jacobson radical of R, and let $\bar{a}$ denote the element $a+J$ in the quotient ring $\bar{R} = R/J \cong GF(p^r)$, for each element a of R. We note that $1+J$ is the multiplicative group G_2 of order $p^{(n-1)r}$. If g is the element introduced in the proof of Th. 2(ii), then G_1 is the cyclic group of order (p^r-1) generated by g. We see that the (commutative) group G is the direct product of the two subgroups G_1 and G_2. To determine the structure of G_2 we need the following easily proved lemma.

LEMMA. *Let p be an odd prime, and let the nonnegative integers a_k, b_k, c_k be the coefficients of x^k in the expansions of $(1+px)^N$, $(1+2x)^N$, $(1+4x)^N$ respectively, where N is any positive integer. Then, for any nonnegative integer α we have the following results:*

(i) *if $p^\alpha | N$, then $p^{\alpha+1} \mid a_1$ and $p^{\alpha+2} \mid a_k$ for all $k \geqq 2$;*

(ii) *if $2^\alpha | N$, then $2^{\alpha+1} | b_k$ for $k = 1, 2$ and $2^{\alpha+2} | b_k$ for $k \geqq 3$;*

(iii) *if $2^\alpha | N$, then $2^{\alpha+2} | c_1$ and $2^{\alpha+3} | c_k$ for all $k \geqq 2$.*

Also we have the following trivial result

(iv) *$4 | b_k$ for all $k \geqq 2$.*

The proof of the lemma is omitted. If 2^α, with $\alpha \geqq 1$, is the highest power of 2 which is a factor of N, we note that $2^{\alpha+1}$ will be the highest power of 2 which is a factor of the coefficient b_2. This fact seems to be the source of the difference between the two cases — p odd, p even — in this theorem.

We resume the proof of the theorem. First of all, we note that

every element a of $G_2 = 1+J = 1+pR$ satisfies the equation $a^{p^{(n-1)}} = 1$. We take r elements $g_1, \cdots, g_r$ in the ring R with $g_1 = 1$ such that the set $\{\bar{g}_1, \cdots, \bar{g}_r\}$ is a basis of the quotient ring $\bar{R}$ regarded as a vector space over its prime field $GF(p)$.

First we take up the proof of the statement (2) of the theorem. So hereafter we assume that $p = 2$, and that $n \geqq 3$. We remark now that there exists at least one element β in the ring R such that the equation $x^2+x+\bar{\beta} = \bar{0}$ over $\bar{R}$ has no solution in the field $\bar{R}$. (For, as $(\bar{0})^2+\bar{0}=(\bar{1})^2+\bar{1}$, we note that the mapping

$$a \to a^2+a \qquad (a \in \bar{R})$$

is not one-one and, therefore, not onto $\bar{R}$.) We then note the following results: $(-1+2^{n-1} \cdot g_1) \in G_2$, $(-1+2^{n-1} \cdot g_1)^2 = 1$, $(1+4\beta)^{2^{(n-2)}} = 1$, and $a^{2^{(n-1)}} = 1$ for all a in G_2.

For positive integers $m, n_1, n_2, \cdots, n_r$ with $m \leqq 2$, $n_1 \leqq 2^{n-2}$ and $n_i \leqq 2^{(n-1)}$ for $i \geqq 2$, we assert that the equation

$$(1) \qquad (-1+2^{n-1} \cdot g_1)^m \cdot (1+4\beta)^{n_1} \cdot \prod_{i=2}^{r} \{(1+2g_i)^{n_i}\} = 1$$

will imply $m = 2$, $n_1 = 2^{n-2}$, and $n_i = 2^{n-1}$ for $i \geqq 2$. To show this, we will suppose first that $m = 1$ and obtain a contradiction. Noting that 2^{n-1} is a multiple of 4, and using the result (iv) of the lemma in expanding the left hand side of the equation (1) we see that (1) reduces to

$$(2) \qquad 2 \cdot (1+ \sum_{i=2}^{r} n_i \cdot g_i+2a) = 0$$

for some element a of the ring R. As the additive order of every invertible element of R is 2^n we see that the expression within parentheses in above gives an element of J, so that we get

$$(3) \qquad \bar{1}+\sum_{2}^{r} n_i \cdot \bar{g}_i = \bar{0}.$$

Since $\bar{1} = \bar{g}_1$ and $\bar{g}_2, \cdots, \bar{g}_r$ are linearly independent over $GF(2)$, the equation (3) gives the desired contradiction. So we must have $m = 2$ in (1) — in which case it reduces to

$$(4) \qquad (1+4\beta)^{n_1} \cdot \prod_{i=2}^{r} \{(1+2g_i)^{n_i}\} = 1.$$

As we can now get the result $\sum_{i=2}^{r} n_i \cdot \bar{g}_i = \bar{0}$ we see that each one of the $(r-1)$ integers $n_2, \cdots, n_r$ is even. Let α be the integer with $0 \leqq \alpha \leqq (n-2)$ such that $2^{\alpha+1}$ is the highest power of 2 which is a factor of all the r even integers $2n_1, n_2, n_3, \cdots, n_r$. (If we show

that $\alpha = n-2$, then the assertion made at the beginning of this paragraph will be proved.) We write $n_1 = 2^{\alpha} \cdot m_1$, $n_i = 2^{\alpha+1} \cdot m_i$ for $i \geqq 2$ and note that the choice of α implies that at least one of the r integers $m_1, \cdots, m_r$ is odd. Now using the result (ii) (with $\alpha+1$ in the place of α) and the result (iii) of the above lemma, we can reduce the equation (4) to

$$(5) \quad 2^{\alpha+2} \cdot \{m_1 \cdot \beta + \sum_{i=2}^{r} m_i \cdot g_i + \sum_{2}^{r} m_i \cdot (m_i \cdot 2^{\alpha+1} - 1) \cdot g_i^2 + 2b\} = 0,$$

for some element b of the ring R. If $(\alpha+2)$ were less than n in (5), we can get from (5) the result

$$(6) \qquad m_1 \cdot \bar{\beta} + (\sum_{2}^{r} m_i \cdot \bar{g}_i) + (\sum_{2}^{r} m_i \cdot \bar{g}_i)^2 = \bar{0},$$

as $\bar{R}$ is a field with characteristic 2. Our choice of the element β implies that m_1 must be even, so that at least one of the remaining integers m_i must be odd. But then (6) gives

$$\sum_{i-2}^{r} m_i \cdot \bar{g}_i = \bar{0} \quad \text{or} \quad \sum_{i=2}^{r} m_i \cdot \bar{g}_i = \bar{1} = \bar{g}_1$$

both of which are in contradiction to our choice of the elements g_i. Thus we see that the supposition $\alpha < (n-2)$ leads to a contradiction, so that the proof of the assertion made at the beginning of this paragraph is complete.

If we set

$H_0 = \{(-1+2^{n-1} \cdot g_1)^m : m = 1, 2\}$,
$H_1 = \{(1+4\beta)^k : k = 1, \cdots, 2^{n-2}\}$, and for $i \geqq 2$,
$H_i = \{(1+2g_i)^k : k = 1, \cdots, 2^{n-1}\}$,

we can see that $H_0, \cdots, H_r$ are all cyclic subgroups of the group G_2 and that these are of the precise orders indicated by their definition. (For example, if we had started with $m = 2$, $1 \leqq n_1 \leqq 2^{n-2}$, $n_i = 2^{n-1}$ for all $i \geqq 2$ in the equation (1), we would have obtained $n_1 = 2^{n-2}$. This would imply that the order of the cyclic group H_1 is 2^{n-2} and not a proper factor of this integer.) The argument of the previous paragraph shows that the product of the $r+1$ subgroups H_i is direct. So their product will exhaust the group G_2, and we see that the proof of the statement (2) of the theorem is complete.

We now indicate the proof of the statement (1). When p is an odd prime we have to consider the equation $\prod_{i=1}^{r} \{(1+pg_i)^{n_i}\} = 1$, and use the result (i) of the lemma. When $p = 2$ and $n = 2$, as

the square of every element of G_2 equals 1, we see that G_2 will be an elementary abelian group.

This completes the proof of the theorem.

(3.10) In this subsection we show that *any finite ring with identity will contain at least one Galois ring as a subset.* Let R be a finite ring with identity 1, and let S be any commutative subring of R. By a well-known result, S can be expressed as the direct sum of rings $S_1, \cdots, S_k$ $(k \geqq 1)$ where each S_i is a completely primary ring. By Th. 8 each S_i contains a unique subring R_i which is a Galois ring. So every finite ring R with identity contains at least one subset R_1 which, under the operations induced on it by R, is a Galois ring. The identity element of R_1 is not the same as that of R except when the characteristic of R is a power of a prime and $k = 1$.

(3.11) In this subsection, we consider rings which are very nearly Galois rings. More specifically if R, J, p, r, n are as in Th. 2 and $n \geqq 3$, we consider the possibility where the characteristic of R is p^{n-1}.

(i) First we describe a process of extending the ring $GR(p^{(n-1)r}, p^{(n-1)})$ to a ring of order p^{nr}. Let R_1 be the ring $GR(p^{(n-1)r}, p^{(n-1)})$ and $J_1(= pR_1)$ be its radical. We find an element g of multiplicative order (p^r-1) in R_1 with the property that, for integers s, t the statement $g^s-g^t \in J_1$ implies $g^s = g^t$. Then we adjoin an element z to the ring R_1 in order to get the set R defined as follows:

$$R = \{a+h \cdot z : a \in R_1, \text{ and } h \in F_1\}. \tag{1}$$

Here we assume that the formal sums of the formal products of z with the elements of R_1 satisfy the associative and distributive laws, and that, in addition, the element z satisfies the conditions

$$\begin{aligned} &z \cdot 1 = 1 \cdot z = z, \qquad p \cdot z = 0, \\ &z \cdot g = p^{n-2} \cdot b + c \cdot z, \qquad z^2 = p^{n-2} \cdot d, \end{aligned} \tag{2}$$

where 1 is the identity element of R_1 and b, c, d are some fixed (but arbitrary) elements of F_1. As every element of R_1 is expressible in the form $h+py$ with h in F_1 and y in R_1 we see that $R_1 \cdot z = F_1 \cdot z$ and $z \cdot R_1 = z \cdot F_1$. We can now verify that the set R is a ring under the obvious operations. We note that $|R| = p^{nr}$, that $1(\in R_1)$ is the multiplicative identity for R and hence that the characteristic of R is $p^{(n-1)}$. If we set $J = \{py+hz : y \in R_1$ and $h \in F_1\}$, we see that the set J of order $p^{(n-1)r}$ will be a nilpotent

ideal in the ring R. As the set $\{g^k+J : k = 1, \cdots, p^r-1\}$ gives (p^r-1) distinct invertible elements in the quotient ring R/J of order p^r, we see that R/J is a field. Thus R, J, p, r, n are as in Th. 2 and so we have proved the *existence* of such a ring R with characteristic $p^{(n-1)}$.

(ii) We now prove a converse of the result proved above. *If R, p, n, with $n \geqq 3$, be as in Th, 2 and if the characteristic of R be $p^{(n-1)}$, then we can show that the ring R may be obtained by the construction described above.* For, let g be the element introduced in the proof of Th. 2 (ii) and let $F_1 = \{0, g^k : k = 1, \cdots, p^r-1\}$. Then the subring R_1 generated by g will be isomorphic to $GR(p^{(n-1)r}, p^{n-1})$. If y is an element belonging to J but not to R_1 we can express every element of R uniquely in the form $a+hy$ with a in R_1 and h in F_1. As $J \cap R_1 = p \cdot R_1$ we have $p \cdot y = p \cdot a_1 + h_1 \cdot y$ for some a_1 in R_1 and some h_1 in F_1. If h_1 were not zero, $(p-h_1)$ will be an invertible element of R_1 and $y = (p-h_1)^{-1} \cdot pa_1$ will be an element of R_1, a contradiction. So $h_1 = 0$ and if we write $z = y-a_1$ we get $p \cdot z = 0$. Therefore, the element z belongs to J but not to R_1 and we find that R, R_1, F_1 and z satisfy the relation (1) given in (i). Since $p \cdot z = 0$ we find that

$$z \cdot g = p^{n-2} \cdot b + c \cdot z, \quad z^2 = p^{n-2} \cdot d + h \cdot z$$

for some elements b, c, d, h of F_1. We remark that the element h in above must be zero. If it were not so, then as $z \cdot h^{-1}$ is nilpotent and $p \cdot z = 0$, we will get

$$\begin{aligned} -z &= h^{-1} \cdot (1-z \cdot h^{-1})^{-1} \cdot p^{n-2} \cdot d \\ &= h^{-1} \cdot (1+z \cdot h^{-1}+(z \cdot h^{-1})^2+ \cdots) \cdot p^{n-2} \cdot d \\ &= h^{-1} \cdot p^{n-2} \cdot d+0+0+ \cdots, \end{aligned}$$

a contradiction because the element z does not belong to R_1. This shows that h must be zero, and so the statement made at the beginning of this paragraph is proved.

(iii) We now specialise the above results for the case $n = 3$ and $r = 1$. Let

$$\begin{aligned} R = \{k_1 \cdot 1 + k_2 \cdot z : 1 \leqq k_1 \leqq p^2,\ 1 \leqq k_2 \leqq p, \\ p \cdot 1 \neq 0,\quad p^2 \cdot 1 = 0 = p \cdot z, \text{ and } z^2 = p \cdot m \cdot 1\}, \end{aligned}$$

where m is any integer. Denoting this set by $R(m)$ and assuming the obvious operations we see that $R(m)$ will be a ring of Th. 2 with $n = 3$, $r = 1$ and characteristic p^2, and conversely that every ring R of Th. 2 with $n = 3$, $r = 1$ and characteristic p^2 is of this form for a suitable integer m. Let $R(m_1)$, $R(m_2)$ be two

rings of this form with z_1, z_2 respectively in the place of z. If σ is an isomorphism of the ring $R(m_1)$ onto $R(m_2)$ we find that $\sigma(z_1) = k \cdot 1 + d \cdot z_2$ where k, d are integers such that $p|k$, while d is prime to p. As $p \cdot m_1 \cdot 1 = \sigma(z_1^2) = d^2 \cdot z_2^2 = d^2 \cdot p \cdot m_2 \cdot 1$, we get $m_1 \equiv d^2 \cdot m_2$ (modulo p). If we write $m_1 \sim m_2$ for m_1, m_2 in Z when, and only when $m_1 \equiv d^2 \cdot m_2$ (modulo p), where d is prime to p, we see that "$\sim$" is an equivalence relation on Z, and the equivalence classes under this are:

(a) $C_0 = p \cdot Z$, (b) $C_1 = 1 + p \cdot Z$, and when the prime p is odd (c) the (nonempty) set C_2 which is the complement of $C_0 \cup C_1$ in Z. (In other words, C_1 is the set of all quadratic residues, and C_2 of all nonresidues for the prime p.) We can now easily verify that two rings $R(m_1)$, $R(m_2)$ will be isomorphic with each other if, and only if the integers m_1, m_2 belong to the same class C_i of integers described above. It follows that *the exact number of mutally nonisomorphic rings $R(m)$ is 2 or 3 according as the prime p is even or odd.*

The last-mentioned result will be needed in Th. 14 below.

(iv). The rings $R(m)$ considered above are all commutative. We can generalise the final result of (iii) to the commutative rings of (ii) above. We can prove the following result:

Let $k(n)$ denote the precise number of mutually nonisomorphic commutative rings R of Th. 2 with characteristic $p^{(n-1)}$, where the integer n is as in Th. 2. Then $k(2) = 1$, and for $n \geqq 3$, $k(n) = 2$ or 3 according as the prime p is even or odd.

The result for $n = 2$ follows from Th. 4 and the remark in §(2.5). For $n \geqq 3$ we have to use the fact that the order of the cyclic group formed by the nonzero elements of the set F_1 (introduced in Th. 2) is odd or even according as p is even or odd. Further details of the proof are omitted.

Section 4

(4.1) In this section, we consider the situation where a (finite) ring R contains a subfield F of order q. (We recall from the introduction that when we use the terms subring, subfield we assume that these subsets contain the identity element — if one exists — of the larger ring.) We begin the discussion by stating some of the properties of such a ring which are very often used in the course of this section.

(i) If A is any left (resp. right) ideal in the ring R, then as A is a left (right) vector space over the field F, we see that $|A|$ will be

a power of $|F| = q$; if $|A|$ were equal to q, then A will be a minimal left (right) ideal in R.

(ii) $|R| = q^n$ for some positive integer n. (In this section we describe completely the structures of all such rings R when $n = 2$, and when $n = 3$.)

(iii) As any nontrivial homomorphism on a field is an isomorphism we see that, for any proper ideal K in R, the quotient ring R/K contains a subfield of order $|F| = q$.

(iv) If $R = A_1 \oplus \cdots \oplus A_m$ is the direct sum of nonzero ideals A_i, then each A_i, treated as a ring by itself, will contain a subfield of order q.

We need also the following

LEMMA. *Let K_n denote the ring of all $n \times n$ matrices over a field $K = GF(p^k)$. Then K_n will contain a subfield of order p^r if, and only if $r|kn$.*

PROOF: The "only if" part follows from the remark (i) above since K_n contains minimal left ideals of order p^{kn}. To prove the "if" part it is clearly sufficient to show that K_n contains a subfield of order p^{kn}. For getting this we have only to adjoin to the field of scalar matrices any particular matrix of order n whose characteristic polynomial is irreducible over the scalar field K.

(4.2) The following theorem describes the structures of all the rings of order q^2 (with identity) which contain a subfield of order q.

THEOREM 10. *Let R be a ring with identity, containing a subfield F of order $q = p^r$ where p is a prime. If $|R| = q^2$, then R is isomorphic to a ring of one, and only one of the types described below.*

(i) $GF(q^2)$.

(ii) *If $r = 2k$ for an integer k, then the ring of all 2×2 matrices over the field $GF(p^k)$.*

(iii) $GF(q) \oplus GF(q)$.

(iv) *The ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & a^s \end{pmatrix}$ with a, b in $GF(p^r)$ where $s = p^t$ and t is some fixed integer with $1 \leqq t \leqq r$.*

PROOF: If J is the Jacobson radical of R, then either $J = (0)$ or $|J| = q$. In the latter case the quotient ring R/J of order q is a field and so R is a ring of Th. 2 with $n = 2$. Thus if $|J| = q$ we see, by using Th. 4, that R is of the type (iv) described above. We suppose hereafter that R is semisimple. By Wedderburn-Artin structure theorem, R is expressible as the direct sum of ideals

$A_1, \cdots, A_m$ where each A_i, regarded by itself, is a total matrix ring over a suitable (finite) field. As each $|A_i|$ is a power of q, we have only $m = 1$ or $m = 2$. In the latter case the rings A_1, A_2 of order q are fields and so R will be of type (iii). If $m = 1$, let R be the ring of all $n \times n$ matrices over the field $K = GF(p^k)$ so that $k \cdot n^2 = 2r$. By the above lemma, $r|kn$ so that $n|2$. If $n=1$, R is of type (i). n can be equal to 2 only if $r = 2k$ is an even integer. If $r = 2k$ for an integer k, the above lemma shows that R may be of type (ii) also.

If R_1, R_2 are any rings belonging to two of the distinct types described above, it is obvious that R_1 and R_2 will be mutually nonisomorphic. This remark completes the proof of the theorem.

(4.3) The following theorem describes the structures of all rings of order q^3 (with identity) which contain a subfield of order q.

THEOREM 11. *Let R be a ring with identity, which contains a subfield F of order $q = p^r$, where p is a prime. If $|R| = q^3$, then R is isomorphic to a ring of one, and only one of the types described below.*

(i) $GF(q^3)$.

(ii) *If $r = 3k$ for an integer k, then the ring of all 3×3 matrices over the field $GF(p^k)$.*

(iii) $GF(q^2) \oplus GF(q)$.

(iv) *If $r = 2k$ for an integer k, the direct sum of $GF(q)$ with the ring of all 2×2 matrices over the field $GF(p^k)$.*

(v) $GF(q) \oplus GF(q) \oplus GF(q)$.

(vi) *A ring of Th. 4 with $n = 3$.*

(vii) *A ring of Th. 3 with $n = 3$.*

(viii) *The direct sum of the field $GF(q)$ with a ring of the type described in Th. 10* (iv).

(ix) *The ring of all 2×2 upper triangular matrices over $GF(q)$.*

PROOF. If J is the Jacobson radical of R, then either $J = (0)$ or $|J| = q$ or $|J| = q^2$.

Suppose first that $J = (0)$ and that R is decomposable into a direct sum of ideals A, B with $|A| = q^2$, and $|B| = q$. Then, as A is a semisimple ring of Th. 10, we see that R will be of type (iii) or (iv) or (v) described here. If R were a simple ring, then proceeding as in the proof of the previous theorem, we can see that R must be of type (i) or (ii) described above.

Suppose next that J is of order q^2. Then R is a ring of Th. 2

with $n = 3$ so that $J^3 = (0)$. So R will be of type (vi) or (vii) according as $J^2 \neq (0)$ or $J^2 = (0)$.

We assume hereafter that $|J| = q$ so that the quotient ring R/J is a semisimple ring of Th. 10. The supposition that R/J is a field will (on using Th. 2) imply that J contains at least q^2 elements, a contradiction. So R/J can be only of type (ii) or type (iii) given in Th. 10. "Lifting" idempotents from R/J we get two mutually orthogonal nonzero idempotents e_1, e_2 in R with $e_1+e_2 = 1$. Since J is a minimal left ideal it follows that $J^2 = (0)$ and if $Je_i \neq (0)$ then $Je_i = J$. So we may (and hereafter, do) assume that $Je_1 = (0)$ and $Je_2 = J$.

Now we assert that R/J cannot be of type (ii) given in Th. 10. For, if it were, we can find two elements a, b in R such that $ae_1be_2 = e_2+x$ for some element x in J. It follows that $(0) = Je_1 = (Ja)e_1be_2 = J(e_2+x) = J+(0)$, a contradiction. So R/J is the direct sum of the field $GF(q)$ with itself. This implies that $e_1Re_2 \subseteqq J$, $e_2Re_1 \subseteqq J$, and that $(xy-yx) \in J$ for all elements x, y in R. As $Je_1 = (0)$, we have $e_2Re_1 = (0)$.

If $e_1J = (0)$ also we will have $e_1Re_2 = (0) = e_2Re_1$ so that R will be the direct sum of the two nonzero ideals e_iRe_i. As the ring e_2Re_2 with radical $e_2Je_2 = J$ is of the type (iv) of Th. 10, we see that R will be of type (viii) in this case.

We assume hereafter that $e_1J = J = Je_2 = e_1Je_2$. Let g be a fixed cyclic generator of the field F, and let e_3 be a fixed nonzero element of J. We assert that if g commutes with e_3 then g will commute with e_1 and e_2 also. For, if we write $e_1g = ge_1+x$, then, as the element x (belonging to the set $J = Fe_3$) commutes with g, we can get $e_1g^k = g^k \cdot e_1+k \cdot g^{k-1} \cdot x$, by induction on k. $k = p$ gives $e_1g^p = g^pe_1$ and it follows that g commutes with e_1. This proves the assertion made earlier.[5] Suppose now that g does not commute with e_3 so that (in the order p^r of the field F) the integer r is greater than one. We have $e_3 \cdot g = g^s \cdot e_3$ with $s = p^t$ for an integer t with $1 \leqq t < r$. As $x \cdot g = g^s \cdot x$ for all elements x of J, we can easily verify that the element $y = (g^s-g)^{-1} \cdot (ge_1-e_1g)$ of J satisfies the relation $(e_1+y) \cdot g = g \cdot (e_1+y)$. If we write $f_1 = e_1+y$, and $f_2 = 1-f_1$, we see that f_1 is an idempotent element and that $J = f_1J = Jf_2 = f_1Jf_2$. Also, the element g commutes with the idempotents f_i.

So, without loss of generality, we may assume that the element g commutes with the idempotents e_i that we started with. We then

[5] The proof for the case $|J| = q$ upto this stage is due to Mr. Björk.

get the following table of relations between the elements e_i and the elements of the field F.

$$\begin{aligned} e_1^2 &= e_1, & e_1e_2 &= 0, & e_1e_3 &= e_3, \\ e_2e_1 &= 0, & e_2^2 &= e_2, & e_2e_3 &= 0, \\ e_3e_1 &= 0, & e_3e_2 &= e_3, & e_3^2 &= 0, \quad \text{and} \\ e_1f &= fe_1, & e_2f &= fe_2, & e_3f &= f^s \cdot e_3 \\ & & & & & \text{for all } f \in F, \end{aligned}$$

where $s = p^t$ for a fixed integer t with $1 \leqq t \leqq r$. The above relations imply that $\{e_1, e_2, e_3\}$ is a distinguished basis of R over the field F, and then that the mapping

$$(a \cdot e_1 + b \cdot e_2 + c \cdot e_3) \to \begin{pmatrix} a & c^s \\ 0 & b \end{pmatrix}$$

as a, b, c range over F, is an isomorphism of R onto the ring of all 2×2 upper triangular matrices over the field $F = GF(q)$.

Let R_1 be the ring of the type (ix) and R_2 be any ring of type (viii). For each nontrivial idempotent element e in the ring R_1 it can be verified that at least one of the sets R_1e, eR_1 is of order q^2. This remark shows that the rings R_1, R_2 cannot be isomorphic with each other, and hence completes the proof of the theorem.

(4.4) Remarks. (i) Let S be any ring with identity 1 and let S_n denote the total matrix ring of order n over S. If $Q = (q_{ij})$ in S_n is defined by $q_{ij} = 1$ if $i+j = n+1$ and $q_{ij} = 0$ otherwise we see that the inner automorphism determined on S_n by the (non-singular) matrix Q transforms an upper triangular matrix into a lower triangular one, and vice versa. This explains, in a very simple manner, as to why we may replace the adjective "upper" by "lower" in the alternative (ix) of Th. 11.

(ii) Supposing $r = 1$ in Th. 11 we can get the following result.

The exact number of mutually nonisomorphic rings of order p^3, with identity and with characteristic p, is seven; only one of these rings (namely, the ring of all 2×2 upper triangular matrices over the field $GF(p)$) is noncommutative.

This result will be used in Th. 14 below.

(iii) If $r \geqq 2$, we remark that each of the alternatives (vi), (vii), and (viii) of Th. 11 contains at least two mutually nonisomorphic rings. (See §(2.5).)

(iv) Theorems 7, 10, 11 and the remark (ii) of §(3.11) show that we now know the structures of all rings of Th. 2 for the cases $n = 2$ and $n = 3$.

Section 5

(5.1) In this section we consider the problem of Ganesan and Eldridge which was described in the introduction. This paper, in fact, owes its existence to an attempt to solve this problem completely. In this connection we prove the following theorem.

THEOREM 12. *Let S be a ring with N^2 (> 1) elements, exactly N of which are left zero divisors in S. Then the following results hold.*

(i) *$N = p^r$ for some prime p and some positive integer r.*

(ii) *The characteristic of S is either p or p^2.*

(iii) *When the characteristic of S is p, either*
(a) *S is a ring of the type described in Th.* 10 (*iv*), *or*
(b) *S is isomorphic to the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b in $GF(p^r)$.*

(iv) *When the characteristic of S is p^2, S is isomorphic to the Galois ring $GR(p^{2r}, p^2)$.*

PROOF. Let J denote the set of all the N left zero divisors of the ring S and let J_1 be the Jacobson radical of S. It is obvious that the (nil) ideal J_1 is contained in J. To prove the reverse inclusion we take some fixed, but arbitrary, nonzero element z of J and consider the homomorphism $x \to x \cdot z$ of the additive group of S onto that of the left ideal Sz. If K is the kernel of this mapping, we see that every element of the two sets K, Sz is a left zero divisor in S, so that $K \subseteq J$, and $Sz \subseteq J$. But then the result $|K| \cdot |Sz| = |S| = |J|^2$ implies that $K = J = Sz$ and hence that $Jz = Kz = (0)$. As z was arbitrary in J, we find that $J^2 = (0)$ and therefore that the left ideal J is contained in J_1. It follows that the set of all the N left zero divisors of the ring S constitutes the Jacobson radical of the ring S. For any two elements a, b of the ring S with $a \notin J$, $b \notin J$, the definition of the set J shows that $a \cdot b \notin J$. It follows that the quotient ring S/J is a (finite) division ring, and then that S/J (of order N) is the field $GF(p^r)$ for some prime p and some positive integer r. The statement (i) has been proved.

From the results given in §(2.1) we see that we have to distinguish between two cases which are discussed below.

Case (1). Let S contain at least one element x which is not a right zero divisor. Then S contains a (two-sided) multiplicative identity, and (as S/J is a field) S is a ring of Th. 2 with $n = 2$. It follows that the characteristic of S is either p or p^2. From Ths. 4, 10 and 7,

we can conclude that only the situations envisaged in the statements (iii) (a) and (iv) of this theorem can occur in this case.

Case (2). Here we suppose that every element of S is a right zero divisor. Then S cannot have a two-sided identity. But S possesses at least one left identity, say e_1. If we show that, in this case, S is isomorphic to the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b in $GF(p^r)$ we can see that the proof of the theorem will be complete.

Initially, the proof proceeds as for Th. 2. If g is a fixed element of S such that $(g+J)$ is a cyclic generator of the field $S/J \cong GF(p^r)$ and if

$$F_1 = \{0,\ g^k : k = 1, \cdots, p^r-1\}$$

we can easily see that every element of the ring S is uniquely expressible in the form $a+b\cdot z$ with a, b in F_1, where z is some fixed nonzero element of J. In particular, we note that $J = F_1 z$.

We now consider the subring S_1 generated by the element g. Then S_1 is commutative and $F_1 \subseteqq S_1$. We first suppose that F_1 is a proper subset of S_1. Then S_1 contains an element $f+y$, where $f \in F_1 \subset S_1$, $y \in J$ and $y \neq 0$. This implies that $y \in S_1$, and so leads to $S = \{a+by : a, b \in F_1\} \subseteqq S_1$, a contradiction, because S_1 is commutative and S contains one-sided zero divisors. This contradiction proves that $F_1 = S_1$ is a subring of S. As S/J is a field of order N, we find that $g^N-g \in J \cap F_1 = (0)$. So F_1 is a subfield of S (with g^{N-1} as the identity for F_1).

We now show that $zS = 0$. For, as the element g is a right zero divisor, there is a nonzero element cz (because the set of all left zero divisors is $J = F_1 z$) such that $czg = 0$. As $0 \neq c \in F_1$, $c \notin J$ and so $zg = 0$. This implies that $zS = 0$.

Finally, the observation that the mapping

$$a+bz \to \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \quad a, b \in F_1 \cong GF(p^r)$$

is an isomorphism completes the proof of the theorem.

(5.2) Remarks. (i) If we replace the adjective "left" by "two-sided" in the hypothesis of the above theorem, we see that we have only to change the word "isomorphic" to "isomorphic or anti-isomorphic" in the statement (iii) (b) of its conclusion.

(ii) The result proved in Case (2) of the above theorem may be regarded as a converse of a result given by Ganesan [2, Example 1, p 242].

(iii) From the argument given in the first paragraph of the proof of Th. 12, we can get the following properties of the set J: (a) J is the unique maximal left ideal in S, and then, (b) J is the unique minimal left ideal in S.

(iv) In the course of the proof of his Theorem II, Koh [4] has proved the statement (i) of Th. 12, under an additional hypothesis. The previous remark shows why this additional hypothesis is superfluous for proving Th. 12(i). Koh's proof, however, makes essential use of this additional hypothesis.

It is to be noted that what is usually known as a left zero divisor has been called a "right" zero divisor in Koh's paper.

Section 6

(6.1) In this section, we determine the structures of all rings of order p^2 (not necessarily possessing an identity element) and the structures of all rings of order p^3 with identity, where p is any prime. The results are summarised in the following two theorems.

THEOREM 13. *There are in all eleven mutually nonisomorphic rings of order p^2, for any prime p. Only two of these are noncommutative — (e.g) those which are isomorphic or anti-isomorphic to the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b in the field $GF(p)$.*

PROOF: Let S denote any ring of order p^2. If the characteristic of S is p^2, then the cyclic additive group of S will contain a generator α such that either $\alpha^2 = 0$, or $\alpha^2 = \alpha$, or $\alpha^2 = p\alpha$. This accounts for 3 mutually nonisomorphic rings (as may be seen, for instance, by considering the ideals S^2 in these rings). Hereafter we suppose that the characteristic of S is p. If J is the Jacobson radical of S, then either $J = (0)$, or $|J| = p$, or $J = S$, and we see that the first of these gives two rings. If S is a radical ring (with ch. p), we can embed S in a ring R of order p^3 with an identity element such that S is the radical of R. As R will be a (unique) ring of either Th. 3 or Th. 4 (with $n = 3$) we see that there are two and only two radical rings S of order p^2 and ch. p.

Hereafter we suppose that $|J| = p$ (in addition to the fact that the ch. of S is p). Then $J^2 = (0)$, and we find that we have to distinguish between two cases. *Case* (1). Let every two-sided zero divisor of S belong to J. Remark (i) of §(5.2) implies that there are 3 rings in this case. One of these is commutative and the other two are the noncommutative rings (possessing one-sided identities only) mentioned in the statement of the theorem. *Case* (2). Let

there be a two-sided zero divisor z of S which is not in J. It can be shown that $JS = SJ = (0)$. The ring S contains a nonzero idempotent e and if $K = \{n \cdot e : n = 0\ 1, \cdots, p-1\}$ we see that $S = K \oplus J$ is the direct sum of the field of order p, and the zero ring of order p.

This completes the discussion and we see that there are in all $3+2+2+3+1 = 11$ mutually nonisomorphic rings of order p^2.

THEOREM 14. *The exact number of mutually nonisomorphic rings of order p^3, each possessing an identity element, is eleven or twelve according as the prime p is even or odd. Only one of these rings is noncommutative — (e.g.) the ring of all 2×2 upper triangular matrices over the field $GF(p)$.*

PROOF: Let R denote any ring of order p^3, with identity 1 and with radical J. The characteristic of R is either p or p^2 or p^3. We note that $J \neq (0)$ when the characteristic is p^2. In view of the remark (ii) in §(4.4) and the remark (iii) of §(3.11) we need consider only the case where R has characteristic p^2 and J is of order p. In this case R contains mutually orthogonal idempotents e_1, e_2 with $e_1+e_2 = 1$. In the Peirce decomposition $R = Re_1 \oplus Re_2$, we may suppose that $|Re_1| = p$ and that $|Re_2| = p^2$. As $p \cdot e_2 = p \cdot 1 \neq 0$, we find that R will be isomorphic to the direct sum of the ring $Z/(p)$ with $Z/(p^2)$ in this case.

So we can conclude that there are in all $7+(1+2)+1 = 11$ or $7+(1+3)+1 = 12$ mutually nonisomorphic rings of order p^3, each with identity, according as the prime p is even or odd.

6.2) REMARKS. (i) For any prime p it is obvious that there are only two mutually nonisomorphic rings of order p, namely the field $GF(p)$ and the zero ring of order p.

(ii) Let $N = p_1^{n_1}, \cdots, p_k^{n_k}$ be any fixed positive integer where the p_i are distinct primes and the n_i are positive integers. It is known that any ring S of order N is expressible, in a unique manner, as the direct sum of rings $S_1, \cdots, S_k$ with $|S_i| = p_i^{n_i}$ for each i. Also, the ring S will have an identity element if, and only if all the component rings S_i have identity. So we find that we now know the structures of all rings S of order N when $1 \leqq n_i \leqq 2$, and also the structures of all rings S of order N, each with identity, when $1 \leqq n_i \leqq 3$ for each i.

REFERENCES

N. GANESAN
[1] Properties of Rings with a Finite Number of Zero Divisors, Math. Annalen 157, (1964) 215—218.

N. GANESAN
[2] Properties of Rings with a Finite Number of Zero Divisors II, Math. Annalen 161, (1965) 241—246.

N. JACOBSON
[3] Lectures in Abstract Algebra vol. III, Van Nostrand Company, Princeton—London—Toronto (1964).

K. KOH
[4] On "Properties of Rings with a Finite Number of Zero Divisors", Math. Annalen 171, (1967) 79—80.

H. J. ZASSENHAUS
[5] A group-theoretic proof of a theorem of Wedderburn, Proc. Glasgow Math. Association vol. 1, (1952—53) 53—63.

(Oblatum 13-9-68)

Department of Mathematics,
Annamalai University, Annamalainagar,
Madras State, India