173. *Associative Rings of Order p^3*

By Robert GILMER and Joe MOTT*)
Department of Mathematics, Florida State University

(Comm. By Kenjiro SHODA, M. J. A., Dec. 12, 1973)

For the positive integer n, let $R(n)$ be a complete set of representatives of the isomorphism classes of associative rings of order n, and let $\rho(n)$ be the number of elements in $R(n)$. We discuss here some aspects of the problem of determining the set $R(n)$, and hence of determining $\rho(n)$.

If $n=p_1^{e_1}\cdots p_k^{e_k}$ is the prime factorization of n, then it is well known that $\rho(n)=\rho(p_1^{e_1})\cdots\rho(p_k^{e_k})$; this is true since a ring R of order n is uniquely decomposable as the direct sum of ideals $I_1,\cdots,I_k$ of orders $p_1^{e_1},\cdots,p_k^{e_k}$. Hence to determine $R(n)$ or $\rho(n)$, it suffices to determine $R(p_i^{e_i})$ or $\rho(p_i^{e_i})$ for $1\leq i\leq k$. For a prime p, the sets $R(p)$ and $R(p^2)$ are known; before describing these sets, we discuss an alternate approach to a determination of the set $R(n)$.

Each ring of order n is an additive abelian group and a complete set $G(n)$ of representatives of the isomorphism classes of abelian groups of order n is well known. Moreover, $G(n)$ contains $p(e_1)p(e_2)\cdots p(e_k)$ elements, where $p(s)$ is the number of partitions of the positive integer s [4, p. 164]. Hence if $G(n)=\{G_1,\cdots,G_t\}$ and if for the abelian group G, $R(G)$ is a complete set of representatives of the isomorphism classes of associative rings with additive group G, then $R(n)=\bigcup_{i=1}^{t}R(G_i)$ is a partition of the set $R(n)$. If the group G is cyclic of order d, then the elements of $R(G)$ are in one-to-one correspondence with the positive divisors of d, and hence $R(G)$ contains $\tau(d)$ elements [3, p. 263]. In fact, if d_i is a positive divisor of d, then the ring $C_{d,d_i}=XZ[X]/(dX, X^2-d_iX)$ is in $R(G)$ and $R(G)=\{C_{d,d_i}\}_{i=1}^{\tau(d)}$, where $\{d_i\}_{i=1}^{\tau(d)}$ is the set of positive divisors of d. Each of the rings C_{d,d_i} is commutative; only the ring $C_{d,1}\simeq Z/(d)$ has an identity. The ring $C_{d,d}$ is the trivial ring on the cyclic group of order d; we also use the notation N_d (for null ring) for this ring.

It follows from the preceding paragraph that $R(p)=\{\Pi_p=Z/(p), N_p\}$. To within isomorphism there are eleven associative rings of order p^2 [1, p. 918], [5, p. 227], and in fact, $R(p^2)$ consists of the rings $Z/(p^2)$, $C_{p^2,p}$, N_{p^2} with cyclic additive group and the rings $\Pi_p\oplus\Pi_p$, $\Pi_p\oplus N_p$, $N_p\oplus N_p$, $GF(p^2)$, $\Pi_p[X]/(X^2)$, $X\Pi_p[X]/X^3\Pi_p[X]$, A, B with addi-

*) Research supported in part by NSF Grant 33027X.

tive group the direct sum of two cyclic groups of order p; here A is the ring of matrices $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ with $a, b \in \Pi_p$ and B is the ring of matrices $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ with $a,b \in \Pi_p$. Of the rings in $R(p^2)$, nine are commutative and two are noncommutative; four contain an identity element and seven do not.

A determination of a complete set of pairwise nonisomorphic associative rings of order p^3 has not appeared in the literature. Having now made such a determination ourselves, we understand why; the process is long, tedious, and involves a consideration of many cases. We present in the table below a summary of our results concerning rings of order p^3. The table also indicates our approach to a solution of the problem of determining a complete set of such rings. One of the interesting conclusions one draws from the table is that $\rho(p^3)$ is dependent upon p, whereas $\rho(p)$ and $\rho(p^2)$ are not.

	$p=2$	p *odd*
Rings of order p^3	59	$4p+48$
I. Decomposable	20	20
A. Direct sum of three ideals of order p	4	4
B. Direct sum of ideals of order p^2 and p	16	16
II. Indecomposable	39	$4p+28$
A. Additive group cyclic	4	4
B. Additive group of type 2, 1	17	$3p+13$
1. With identity	2	3
2. Without identity	15	$3p+10$
a. Commutative	10	$p+7$
i. Imbeddable in a ring with identity of order p^4.	3	3
ii. Not case i.	7	$p+4$
α. Generator of the ideal of order p nilpotent of order 2	5	$p+1$
β. Not case α	2	3
b. Noncommutative	5	$2p+3$
i. Containing an idempotent element of order p^2	2	2
ii. Not case i.	3	$2p+1$
C. Additive group of type 1, 1, 1	18	$p+11$
1. Commutative	6	6
a. With identity	3	3
b. Without identity	3	3
2. Noncommutative	6	$p+5$
a. With identity	1	1

b. Without identity	5	$p+4$
i. With Pierce decomposition Re_1+N_0, $\|N_0\|=p^2$	1	1
ii. With Pierce decomposition Re_1+N_0, $\|N_0\|=p$	2	2
iii. Nilpotent	2	$p+1$
α. Containing an element x such that $x^2\neq 0$	2	p
β. Not case α	0	1

We make some remarks about the table. Case I presents no problems; its resolution depends upon a knowledge of the sets $R(p)$ and $R(p^2)$. Similarly, Case II.A. is a consequence of results we have already stated. A ring with identity of order p^3 and characteristic p^2 is commutative. For $p=2$, the two rings obtained in Case II. B.1. are $Z[X]/(4, 2X, X^2)$ and $Z[X]/(4, 2X, X^2-2)$; for p odd, they are $Z[X]/(p^2, pX, X^2)$, $Z[X]/(p^2, pX, X^2-p)$, and $Z[X]/(p^2, pX, X^2-kp)$, where k is not a square mod p.

Resolution of Cases II.B.2.a.i. and II.C.1. come fairly easily from the known structure of commutative primary rings; models for the three rings of Case II.C.1.a. are $GF(p^3)$, $Z[X]/(p, X^3)$ and $Z[X, Y]/(p, X^2, XY, Y^2)$. In the case where the ring R has no identity, we adjoin an identity of order equal to the characteristic of R. For instance, in Case II.C.1.b. any such ring is the maximal ideal of a commutative primary ring of order p^4. The models for this case are the maximal ideals of $\Pi_p[X, Y]/(X^3, XY, Y^2)$, $\Pi_p[X, Y]/(X^3, XY, Y^2-X^2)$, and $\Pi_p[X, Y]/(X^3, Y^3)$ for $p=2$, and the maximal ideals of $\Pi_p[X, Y]/(X^3, XY-X^2, Y^2-X^2)$, $\Pi_p[X, Y]/(X^3, XY, Y^2+cX^2)$ where c is not a square in Π_p, and $\Pi_p[X, Y]/(X^3, XY-X^2, Y^2)$ for p an odd prime. The models for the rings of Case II.B.2.a.i. are the maximal ideals of $Z[X]/(4, X^2)$, $Z[X]/(4, X^2-2X)$, and $Z[X]/(4, X^2-2)$ for $p=2$, and for p odd, they are the maximal ideals of $Z[X]/(p^2, X^2)$, $Z[X]/(p^2, X^2-p)$, and $Z[X]/(p^2, X^2-pk)$, where k is not a square mod p.

Our methods for resolving Cases II.B.2.a.ii., II.B.2.b., and II.C. 2.b. are not elegant, but in view of the rings we determine in those cases, we doubt that there is an elegant solution. The rings obtained in Case II.B.2.b.i. are easy to describe. They are

$$\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| \, a \in Z/(p^2),\ b \in pZ/(p^2)\right\}$$

and

$$\left\{\begin{bmatrix} 0 & b \\ 0 & a \end{bmatrix} \middle| \, a \in Z/(p^2),\ b \in pZ/(p^2)\right\};$$

Paul Hill has independently determined these two rings of Case II.B.

2.b.i. The result of Case II.C.2.a.—that to within isomorphism there is a unique noncommutative ring S with identity of order p^3—is due to Klaus Eldridge [2]. This ring S is the ring of 2×2 upper triangular matrices over $Z/(p)$.

Models for the three rings of Cases II.C.2.b.i. and ii. are

$$R_1=\{(a,b,c)\mid a,b,c\in \Pi_p \quad \text{and} \quad (a,b,c)(d,e,f)=(ad,ae,af)\}$$

$$R_2=\left\{\begin{bmatrix} a & b & c\\ 0 & a & 0\\ 0 & 0 & 0\end{bmatrix}\middle| \, a,b,c\in \Pi_p\right\},$$

and

$$R_3=\left\{\begin{bmatrix} 0 & a & 0 & 0 & 0 & 0\\ 0 & b & 0 & 0 & 0 & 0\\ 0 & 0 & b & 0 & 0 & 0\\ 0 & 0 & 0 & b & 0 & 0\\ 0 & 0 & 0 & 0 & b & c\\ 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}\middle| \, a,b,c\in \Pi_p\right\}.$$

Case II.C.2.b.iii.α. is less involved than Cases II.B.2.a.ii. and II.B.2.b. Also, the approach used in this case gives some indication of the type of proof used in other cases, and hence we sketch a proof of this case.

Suppose that R is a non-commutative, nilpotent ring of order p^3 and of characteristic p. Suppose, further, that R contains an element x such that $x^2\neq 0$. Conclude that $\{x, x^2\}$ is a linearly independent set over Π_p, that $x^3=0$, and that $\{x, x^2, y\}$ is a basis for R over Π_p for each y not in $\Pi_p x+\Pi_p x^2$. Next, conclude that the product of any three elements of R is zero. By a change of variables, we see that R is a member of the class of rings $\{R_a\mid 0\leq a\leq p-1\}$, where R_a is defined as follows: $R_a=\Pi_p x+\Pi_p x^2+\Pi_p y$, where $x^3=x^2y=yx^2=0$, $xy=x^2$, $yx=0$, and $y^2=ax^2$. We show that $R_a\simeq R_b$ if and only if $a=b$. Thus, assume there are linearly independent elements $s, t, s^2\in R_a$ such that (1) $st=s^2$, (2) $ts=0$, and (3) $t^2=bs^2$. If $s=s_1x+s_2x^2+s_3y$ and $t=t_1x+t_2x^2+t_3y$, there is no loss in generality in assuming $s_2=1$, and then equations (1), (2), and (3) yield

(1′) $(s_1^2+s_1+a)=s_1t_1+s_1t_2+t_2a$

(2′) $s_1t_1+t_1+t_2a=0$

(3′) $t_1^2+t_1t_2+t_2^2a=b(s_1^2+s_1+a)$.

Linear independence of s, t, s^2 yields $(s_1t_2-t_1)(s_1^2+s_1+a)\neq 0$. But this fact, together with (1′) and (2′), yields

(4′) $s_1t_2-t_1=s_1^2+s_1+a\neq 0$.

Solve (2′) for t_2a, multiply (3′) by a, then substitute for t_2a. This gives $t_1^2=ab$. But then (4′) yields $a=-t_1$, and $t_1^2=a^2=ab$ implies $a=b$. Thus, the class $\{R_a\mid 0\leq a\leq p-1\}$ contains p pairwise nonisomorphic

rings.

If p is odd, there is one ring in Case II.C.2.b.iii.β. A model for this ring is $\{(a, b, c) \mid a, b, c \in \Pi_p$ and $(a, b, c)(d, e, f) = (0, 0, ae - bd)\}$.

References

[1] D. M. Bloom: Rings of order four. Amer. Math. Monthly, **71**, 918–920 (1964).
[2] K. Edridge: Orders of finite noncommutative rings with unity. Amer. Math. Monthly, **75**, 512–514 (1968).
[3] L. Fuchs: Abelian Groups. Pergamon Press, London (1967).
[4] I. N. Herstein: Topics in Algebra. Blaisdell, New York (1964).
[5] R. Raghavendran: Finite associative rings. Compositio Math., **21**, 195–229 (1969).