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 determing $\rho(n)$.

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.