Proof. By the theorem $S' \subset S$. But trivially $S \subset S'$, since, if $a \in A$, $b \in B$ and $(a, b) = d$, then $(d, n) = ((a, b), n) = (a, b, n) = 1$.

I am indebted to the referee for two helpful suggestions.

Reference

1. F. Klein and R. Fricke, Theorie der elliptischen Modulfunctionen, I, Teubner, 1890.

ORDERS FOR FINITE NONCOMMUTATIVE RINGS

D. B. ERICKSON, Concordia College, Moorhead, Minnesota

Introductory Comments. The solution to problem E 1529 (this MONTHLY, 70, 1963, p. 441) answers the question of the order for the smallest noncommutative ring. It is 4. This paper answers the more general question concerning a characterization of the orders for finite noncommutative rings in a series of three theorems. (In view of the first theorem the comment following the solution of E 1529, to the effect that there exists a noncommutative ring of each composite order N, must be incorrect.)

THEOREM 1. *If R is a finite ring of order $n > 1$ and if n has square free factorization, then R is a commutative ring.*

Proof. It is well known that if the additive group of a ring is cyclic then the ring is commutative. The additive group of R is a finite abelian group which, by the Basis Theorem for Finite Abelian Groups, may be expressed as the direct product of s cyclic subgroups of R, say $R_1, \cdots, R_s$, where the order of each R_i divides the order of R_{i+1} $(i = 1, \cdots, s-1)$, and s is the number of elements in a minimal generating system (basis) for R. But by the Lagrange Theorem the order of each R_i divides the order of R. Since the order of R is square free, the additive group of R is the cyclic group of order n (abbr. C_n), and therefore R is a commutative ring.

In the next two theorems we construct a noncommutative ring of order m for each positive integer $m > 1$ having square factors.

THEOREM 2. *If p is a prime integer, then there exists a noncommutative ring of order p^2.*

Proof. Let R be the direct product of C_p with itself. It is clear that R is an abelian group of order p^2 and that R is not cyclic. A minimal generating system for R is $\{(a, 0), (0, a)\}$, where a is a generator for C_p. We define multiplication on the basis elements by the requirement that the product of two basis elements is the left factor, and extend it to the whole system by the distributive law, whence

$$(j_1a, k_1a) \cdot (j_2a, k_2a) = (j_2 + k_2)(j_1a, k_1a),$$

for all (j_ia, k_ia) in R, where the j_i and k_i are integers. Closure, the associative law, and the distributive laws are easily verified; thus, R is a ring of order p^2. Since $(0, a)(a, 0)=(0, a)$ but $(a, 0)(0, a)=(a, 0)$ R is not commutative.

This last result is extended to all orders np^2 by Theorem 3.

THEOREM 3. *Let R_1 be a ring of order p^2 as constructed in Theorem 2, and let R_2 be any ring of order n, then the ring $R=R_1\dot{+}R_2$ (i.e. the direct sum of R_1 and R_2) is a noncommutative ring of order np^2.*

REMARK. The proof of this statement is obvious from the properties of direct sums of rings. We only remark that for R_2 we may use the trivial ring of order n which has as its additive group C_n and in which all products are zero; note also that R contains a subring isomorphic to R_1 and is therefore noncommutative.

We summarize in the following corollary.

COROLLARY. *If m is a positive integer, $m>1$, then there exists a noncommutative ring of order m if and only if m has square factors.*

Supported by NSF Grant GE-1082.

ON SOME THEOREMS OF BRAM FOR SUBNORMAL OPERATORS

G. H. ORLAND, University of Illinois, Urbana

Subnormal operators were defined and studied by Halmos in [**3**] and [**4**]. His results were further extended by Bram [**1**]. A (bounded) operator S on a complex Hilbert space H is *subnormal* if on a Hilbert space K containing H as a subspace, there is a normal operator N whose restriction to H is S. In other words, an operator is subnormal if it is the restriction of a normal operator to an invariant subspace. To avoid trivial complications it is customary to assume that N is a minimal extension of S in the sense that the only subspace of K which contains H and on which N is normal is K itself. For the spectra of S and N, the interesting result, $\sigma(S)\supset\sigma(N)$, was proved in [**4**]. The resolvent set of N can be expressed as

$$\rho(N) = U_\infty \cup \bigcup_{n=1}^{\infty} U_n,$$

where each U is one of its (open) connected components; U_∞ is the single unbounded component. Following Bram, each bounded U_n is called a *hole* of $\sigma(N)$. Set $H(N)=\bigcup_{n=1}^{\infty} U_n$. In Theorem 3 of [**1**], Bram proved that $\sigma(S)\subset\sigma(N)\cup H(N)$. In Theorem 4 he proved that for any hole of $\sigma(N)$, either all of it is contained in $\sigma(S)$, or none of it. By using some ideas from [**5**], a simpler and simultaneous proof of both theorems will be given.

Let $d(\lambda, \sigma(A))$ represent the distance, in the complex plane, from the point λ to $\sigma(A)$. Then from $\sigma(S)\supset\sigma(N)$ it follows that $d(\lambda, \sigma(S))\leqq d(\lambda, \sigma(N))$ for any λ. If $\lambda\in\rho(S)$ so that the resolvents $R_\lambda(S)$ and $R_\lambda(N)$ both exist, then $R_\lambda(N)$ extends $R_\lambda(S)$ and $\|R_\lambda(N)\|\geqq\|R_\lambda(S)\|$. It is also true that for any operator A,