ON THE MULTIPLICATIVE SEMIGROUP OF A COMMUTATIVE RING

J. R. ISBELL

This paper establishes the following

THEOREM. *If the multiplicative semigroup of a commutative ring is finitely generated, it is finite.*

There seems to be no approach in the literature to a general theory of the structural restrictions which a semigroup must satisfy to be the multiplicative part of a ring. Johnson has treated the case that, as in Boolean rings, the addition is uniquely determined by the multiplication [1]. I do not know whether the present theorem extends to the noncommutative case.

I am indebted to John Rainwater for arousing my interest in the problem and to the referee for suggestions on the arrangement of the proof.

Let S denote the direct product of the multiplicative and the additive semigroups of positive integers, i.e. the set of all pairs (m, a) of positive integers with $(m, a)(m', a')=(mm', a+a')$. Let X_p denote, for each prime p, the multiplicative semigroup of all polynomials over the p-element field with zero constant term. Each X_p contains an isomorphic copy of S, with $(m, a)=(q_1^{a_1} \cdots q_n^{a_n}, a)$ corresponding to $x^a P_1^{a_1} \cdots P_n^{a_n}$, for a suitable infinite list of prime polynomials P_i. We shall prove the

LEMMA. *If h is a homomorphism of S into a finitely generated commutative semigroup then there exist m, m', and a such that $h(m, a)=h(m', a)$.*

COROLLARY. *X_p is not isomorphic with a subsemigroup of any finitely generated commutative semigroup.*

From these results the theorem follows by more familiar arguments. If R is a commutative ring with multiplicative generators $x_1, \cdots, x_k$, the lemma tells us that for each x_i the semigroup of all mx_i^a satisfies a relation $(m-m')\, x_i^a=0$. Then the product of the k integers $m-m'$ annihilates all products of powers of the generators except finitely many. Some larger integer annihilates the whole ring R, and therefore, the additive group is a torsion group of bounded order. It is

Received by the editors November 29, 1958 and, in revised form, February 17, 1959.

then the direct sum of its primary components G_p; it remains to show that each G_p is a finite group.

The corollary implies that the polynomials in x_i, for each i, satisfy a relation $P(x_i) \in pR$ for some integral polynomial P not divisible by p. Since p is prime, P may be taken to be monic; then modulo pR, some power of x_i is a linear combination of smaller powers. Every higher power is also a member of this finite set of linear combinations, modulo pR, and R/pR is finite. Then G_p/pG_p is finite; so is its homomorphic image pG_p/p^2G_p, and so on. Since the order is bounded, the proof will be complete.

Proof of Lemma. It is convenient to write the semigroup additively. Let the generators be $e_1, \cdots, e_k$, so that the general element has a (nonunique) expression $e(\alpha) = \sum a_i e_i$. For the first $k+2$ primes p_j, write $h(p_j, 1)$ as $e(\alpha_j) = \sum a_{ji} e_i$. Consider the $k+2$ different $k+1$-tuples $(1, a_{j1}, \cdots, a_{jk}) = \beta_j$. As elements of rational $k+1$-space, they are linearly dependent. A rational linear relation can be rewritten with positive integral coefficients, $\sum \lambda_j \beta_j = \sum \mu_j \beta_j$. In particular, $\sum\sum \lambda_j a_{ji} e_i = \sum \lambda_j h(p_j, 1) = h(\prod p_j^{\lambda_j}, \sum \lambda_j) = h(\prod p_j^{\mu_j}, \sum \mu_j)$. Since the λ's and the μ's are not all the same, the first coordinates are different positive integers m, m'; since $\sum \lambda_j \beta_{j1} = \sum \lambda_j = \sum \mu_j$, the proof is complete.

Reference

1. R. E. Johnson, *Rings with unique addition*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 57–61.

University of Washington