ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 12, Number 2, Spring 1982

ADDITIONS COMPATIBLE WITH MULTIPLICATION

H.K. FARAHAT

1. The study of multiplications compatible with a given additive abelian group is already well established ([3], §118). The opposite problem appears to have received little attention, and is probably intractable in its general form. Given a commutative ring (with identity) Λ, we call an addition $*$ on Λ *compatible* with the multiplicative structure of Λ if $(\Lambda, *)$ is an abelian group whose endomorphisms are precisely those of $(\Lambda, +)$. Since, for each $a \in \Lambda$, the map $(a\cdot): \Lambda \to \Lambda$ given by $b \to ab$ is an endomorphism of $(\Lambda, +)$, it follows that $(\Lambda, \cdot, *)$ will be a ring whose multiplicative structure is the same as that of Λ. Our problem may therefore be formulated more conveniently as follows: to determine the class $[\Lambda]$ of rings R whose multiplicative structure is isomorphic to that of Λ, such that every endomorphism of the additive structure of R is multiplication by some element of R.

This question was first brought to my attention by M.G. Stone (Calgary) who referred to it, in the case $\Lambda = \mathbf{Z}$, as a problem of S. Ulam. Various forms of this question are to be found on p. 552 of [7]. For this reason, we shall call a ring R an *Ulam domain* if it is a member of the class $[\mathbf{Z}]$ corresponding to the ring of integers $\mathbf{Z}$. The main purpose of this paper is to initiate the study of the general question by proving the following:

MAIN THEOREM. *If R belongs to* $[\mathbf{Z}]$ *and the additive structure of R is of finite rank then $R = \mathbf{Z}1_R \cong \mathbf{Z}$. Consequently, the only additions $*$ on $\mathbf{Z}$ which are of finite rank, and are compatible with multiplication, are those given by $(a * b) = \theta^{-1}(\theta(a) + \theta(b))$, a, $b \in \mathbf{Z}$, for some automorphism θ of the multiplicative structure of* $\mathbf{Z}$.

2. The ring of integers $\mathbf{Z}$ is, of course, a countable unique factorization domain (U.F.D.) of characteristic zero with only two units. Accordingly, the Ulam domains are precisely the countable unique factorization domains R of characteristic zero with exactly two units, such that every endomorphism of $(R, +)$ is a multiplication. This last condition implies, in particular, that $(R, +)$ is an indecomposable torsion-free abelian group. Since the classification of unique factorization domains and indecompos-

Received by the editors on September 9, 1980.

able torsion-free abelian groups is still rudimentary (see [2] and ch. VIII of [3]), the determination of all Ulam domains is probably very difficult. We have failed to find an example of an Ulam domain of infinite rank; in every case either there were too many units, or the additive group was decomposable or uncountable!

Let R be a unique factorization domain of characteristic zero. We may identify $\mathbf{Z}$ with the prime subring $\mathbf{Z}1_R$ of R. Let K be the field of fractions of R. Then, of course, K is a field extension of $\mathbf{Q}$, the rational field. It is easy to see that K has a transcendence base X whose elements belong to R, and then K will be an algebraic extension of $\mathbf{Q}(X)$, the field of rational functions in the elements of X with coefficients from $\mathbf{Q}$. The polynomial ring $\mathbf{Z}[X]$, a unique factorization domain (by p. 7 of [2]), is a subring of R, and every element of R is algebraic, not necessarily integral, over $\mathbf{Z}[X]$. Let J always denote the integral closure of $\mathbf{Z}[X]$ in K. Since R is a U.F.D., it is integrally closed in K (see Prop. 6, p. 240 of [4]), and therefore R contains J. Both R and J have K as a field of fractions, and $\mathbf{Q}(X)J = Q(X)R = K$. We shall deal with the situation $\mathbf{Z}[X] \subseteqq J \subseteqq R \subseteqq K$ throughout this section. Also, we shall use the standard notation for localization at prime ideals, namely:

$$J_P = \left\{\frac{a}{b} : a,\ b \in J,\ b \notin P\right\}$$

$$R_M = \left\{\frac{u}{v} : u,\ v \in R,\ v \notin M\right\}$$

where P, M are prime ideals of J, R respectively.

If R has finite rank n then obviously X must be empty, and K must be an n-dimensional extension of $\mathbf{Q}$, while J must be the ring of algebraic integers of K. The Dirichlet Unit Theorem (see, e.g., Theorem 38, p. 142 of [6]) gives complete information regarding the group of units of J, namely, it is the direct product of a finite cyclic group and $r_1 + r_2 - 1$ infinite cyclic groups, where $n = r_1 + 2r_2$, r_1 is the number of real conjugates of K and $2r_2$ is the number of non-real conjugates. Accordingly, if R has only two units, then $r_1 + r_2 = 1$ and so $n = 1$ or 2. We have proved the following result.

LEMMA 2.1 *Let R be a* U.F.D. *of characteristic zero having finite rank and only two units. Then R is either isomorphic to a subring of* $\mathbf{Q}$, *or to a ring lying between an imaginary quadratic field extension of* $\mathbf{Q}$ *and its ring of algebraic integers.*

At this stage it may appear that we have the problem (of Ulam domains of finite rank) just about licked. However, there is a great deal to the subject of rank two rings (see, e.g., [1]). We shall use the method of localization in order to rule out the rank two case. The specific technique is an adaptation of that by Larsen and McCarthy in the study of "overrings" (see [5], Chapter VI).

LEMMA 2.2. *Let R be an Ulam domain of rank 2, and P be a maximal ideal of J such that RP is not all of R. Then $R \subseteqq J_P$.*

PROOF. Suppose that $R \nsubseteq J_P$, and choose any element r in R, not in J_P. Let $r = a/b$ with $a, b \in J$, $b \neq 0$, and consider the exact sequence of J-modules:

$$0 \to \operatorname{Ker} \theta \to J \oplus J \xrightarrow{\theta} J,$$

where $\theta(u, v) = ub - va$ ($u, v \in J$). Since J is a Dedekind domain and R is a torsion-free J-module, R is a flat J-module, being the direct limit of its finitely-generated (hence projective) submodules. Consequently the following sequence is exact.

$$0 \to \operatorname{Ker} \theta \otimes_J R \to (J \oplus J) \otimes_J R \xrightarrow{\theta \otimes 1} J \otimes_J R.$$

But $(\theta \otimes 1)[(1, 0) \otimes r + (0, 1) \otimes 1] = b \otimes r - a \otimes 1 = 0$ because of the isomorphism $J \otimes_J R \cong R$ in which $x \otimes y \to xy$. Exactness now implies that

$$(1, 0) \otimes r + (0, 1) \otimes 1 = \sum_{j=1}^{l} (c_{j1}, c_{j2}) \otimes r_j$$

for suitable elements $r_j \in R$, $(c_{j1}, c_{j2}) \in \operatorname{Ker} \theta$. It follows that $c_{j1}b - c_{j2}a = 0$, i.e., $r = c_{j1}/c_{j2}$ ($1 \leqq j \leqq l$), and $r = \sum_j c_{j1} r_j$, $1 = \sum_j c_{j2} r_j$. Since $r \notin J_P$, we have $c_{j2} \in P$ for all j, whence $1 \in P$ and $RP = R$.

LEMMA 2.3. *Let R be an Ulam domain of rank 2, and M be a maximal ideal of R. Then $M \cap J \neq 0$ and $R_M = J_{M \cap J}$.*

PROOF. If $M \cap J = 0$ then $M + J$ has rank (as abelian group) equal to $\operatorname{Rank}(M) + \operatorname{Rank}(J) > 2$, whence R has rank greater than 2, a contradiction. Hence $M \cap J$ is a non-zero ideal of J, and in fact a prime (hence maximal) ideal of J. By definition we have the trivial inclusion $J_{M \cap J} \subseteqq R_M$. On the other hand, let $w = r/s \in R_M$ where $r, s \in R$, $s \notin M$, and define $C = \{u \in J : ur \in J, us \in J\}$, an ideal of J. If $C = P_1 P_2 \cdots P_k$ is the factorization of C as a product of prime ideals of J then $RC = RP_1 \cdot RP_2 \cdots \cdot RP_k$, and we claim that RC is all of R. Otherwise, RP is not all of R for some $P \in \{P_1, P_2, \ldots, P_k\}$, whence by (2.2), $R \subseteqq J_P$. But then $r = a/c$, $s = b/c$ where $a, b, c \in J$ and $c \notin P$, and yet $cr \in J$, $cs \in J$ forces $c \in C \subseteqq P$, a contradiction. Thus $RC = R$. This implies that $C \nsubseteq M \cap J$, since $R(M \cap J) \subseteqq M \neq R$. Choose $c \notin C$, $c \in M \cap J$. Then $w = r/s = cr/cs \in J_{M \cap J}$. This completes the proof.

Observe that the above two lemmas have not utilized the full hypothesis defining Ulam domains.

We now proceed to show that no Ulam domains of rank 2 exist. Let R be such a domain. If $a, b \in R$, $b \neq 0$ and $a/b \notin R$ then Rb is a proper ideal of R, hence Rb is contained in some maximal ideal M of R and so $a/b \notin R_M$. This argument shows that $R = \bigcap_M R_M$, the intersection being over all maximal ideals M of R (this is a standard fact). By (2.3) we conclude that

$$R = \bigcap_M J_{M \cap J}. \tag{2.4}$$

Hence every non-unit of J belongs at least to one of the "contracted" ideals $M \cap J$ (because R has only the units ± 1). In our situation this forces every prime ideal of J to be a contracted ideal. To see this, let P be any prime ideal of J. By finiteness of the class number [**6**], $P^h = gJ$ for some positive integer h and some $g \in P$. By hypothesis g belongs to some "contracted" ideal, which must coincide with P by unique factorization of ideals of J. It now follows from (2.4) that $R = J$. But J is free of rank 2 as abelian group, hence decomposable. Thus R is not an Ulam domain. This proves that Ulam domains of rank 2 do not exist.

Corollary 2.5. *If R is an Ulam domain of finite rank, then* $R = \mathbf{Z}1_R \cong \mathbf{Z}$.

Proof. We have seen that every Ulam domain R of finite rank must have rank 1. If $x \in R$ then $bx = a1_R$ for suitable relatively prime integers $a, b, b \neq 0$. Write $aa' + bb' = 1$ with $a', b' \in \mathbf{Z}$. Then $b(a'x + b'1_R) = 1_R$, and, since R has only two units, $b = \pm 1_R$ and $x \in \mathbf{Z}1_R$ as asserted.

Finally, let us complete the proof of the main theorem. Let $*$ be an addition on $\mathbf{Z}$ which is compatible with multiplication. Then $R = (\mathbf{Z}, \cdot, *)$ is an Ulam domain, and so by the above Corollary, $R = \mathbf{Z}1_R$, that is, the structure of R as a $\mathbf{Z}$-module which arises from the addition $*$ is free with $1_R = 1$ as generator. In order to avoid confusion of this module multiplication with ordinary multiplication, let $\eta(k)$ denote the module product of $k \in \mathbf{Z}$ with 1_R. For example, if $k > 0$ then $\eta(k) = 1 * \cdots * 1$ (k terms). The map η: $(\mathbf{Z}, +, \cdot) \to (\mathbf{Z}, *, \cdot) = R$ is then the standard ring imbedding of $\mathbf{Z}$ in R whose image is $\mathbf{Z}1_R = R$ in our situation. It follows that η is a ring ismorphism, and that if $\theta = \eta^{-1}$, $a, b \in \mathbf{Z}$, then $a * b = \theta^{-1}(\theta(a) + \theta(b))$.

References

1. R.A. Beaument and R.J. Wisner, *Rings with additive group which is torsion-free of rank* 2, Acta Sci Math. Szeged, **20**, (1959), pp. 105–116.

2. P.M. Cohn, *Unique factorization domains*, Amer. Math. Monthly, **80**, #1, (1973) 1–18.

3. L. Fuchs, *Infinite Abelian Groups*, Vol. II. Academic Press, 1973.
4. S. Lang, *Algebra*, Addison-Wesley, 1965.
5. M.D. Larsen and P.J. McCarthy, *Multiplicative Theory of Ideals*, Academic Press, 1971.
6. D.A. Marcus, *Number Fields*, Springer-Verlag Universitext, 1977.
7. S. Ulam, *Sets, Numbers and Universes*, MIT Press, 1974.

UNIVERSITY OF CALGARY, DEPARTMENT OF MATHEMATICS, CALGARY, ALBERTA, CANADA T2N 1N4