UNIQUE FACTORIZATION MONOIDS AND DOMAINS

R. E. JOHNSON

ABSTRACT. It is the purpose of this paper to construct unique factorization (uf) monoids and domains. The principal results are: (1) The free product of a well-ordered set of monoids is a uf-monoid iff every monoid in the set is a uf-monoid. (2) If M is an ordered monoid and F is a field, the ring $F[[M]]$ of all formal power series with well-ordered support is a uf-domain iff M is naturally ordered (i.e., whenever $b < a$ and $aM \cap bM \neq \emptyset$, then $aM \subset bM$).

By a monoid, we shall always mean a cancellative semigroup with identity element. All rings are assumed to have unities, and integral domains and fields are not assumed to be commutative. If R is an integral domain, then the multiplicative monoid of nonzero elements is denoted by $R^\times$. For any ring or monoid A , $U(A)$ will denote its group of units.

A monoid M is called a *unique factorization monoid* (uf-monoid) iff for every $m \in M - U(M)$, any two factorizations of m have a common refinement. That is, if $m = a_1 a_2 \cdots a_r = b_1 b_2 \cdots b_s$, then the a 's and b 's can be factored, say $a_1 = c_1 \cdots c_i$, $a_2 = c_{i+1} \cdots c_j$, $\cdots$, $b_1 = d_1 \cdots d_k$, $b_2 = d_{k+1} \cdots d_p$, $\cdots$, in such a way that $c_n = d_n$ for all n . An integral domain R is called a *unique factorization domain* (uf-domain) iff $R^\times$ is a uf-monoid.

A monoid M with relation $<$ is said to be *ordered* by $<$ iff $<$ is a transitive linear ordering such that whenever $a < b$ then $ac < bc$ and $ca < cb$ for all $c \in M$. We call M a *positive monoid* iff M equals its positive cone $M^+ = \{a \in M \mid a \geq 1\}$. An ordered monoid M is said to be *naturally ordered* (see [4, p. 154]) iff whenever $aM \cap bM \neq \emptyset$ and $b < a$, then $aM \subset bM$.

It is the purpose of this paper to show ways of constructing uf-monoids and uf-domains. The two principal results are as follows.

THEOREM 1. *The free product of a well-ordered set of monoids is a uf-monoid iff every monoid in the set is a uf-monoid.*

THEOREM 2. *Let M be an ordered monoid and F be a field. The ring $F[[M]]$ of all formal power series with well-ordered support is a uf-domain iff M is naturally ordered.*

Received by the editors April 27, 1970.

AMS 1970 subject classifications. Primary 16A02, 20M25; Secondary 06A50.

Key words and phrases. Free products of monoids, unique factorization monoids, unique factorization domains, noncommutative power series rings.

Copyright © 1971, American Mathematical Society

1. Unique factorization monoids. Another characterization of a uf-monoid is given by the following proposition.

PROPOSITION 1. *A monoid M is a uf-monoid iff for all $a, b \in M$ such that $aM \cap bM \neq \emptyset$, either $aM \subset bM$ or $bM \subset aM$.*

PROOF. If M is a uf-monoid and $aM \cap bM \neq \emptyset$, then $aa' = bb'$ for some $a', b' \in M$ and $a = c_1 \cdots c_i$, $a' = c_{i+1} \cdots c_n$, $b = c_1 \cdots c_j$, $b' = c_{j+1} \cdots c_n$ for some $c_i \in M$. Hence, $aM \subset bM$ if $i \geq j$ and $bM \subset aM$ if $i \leq j$.

To prove the converse, let $m \in M$ have factorizations $m = a_1 a_2 \cdots a_r = b_1 b_2 \cdots b_s$. Then $a_1 M \cap b_1 M \neq \emptyset$ and $a_1 = b_1 b'_1$ (or $b_1 = a_1 a'_1$) for some $b'_1 \in M$. Hence, $m_1 = b'_1 a_2 \cdots a_r = b_2 \cdots b_s$. The desired conclusion now follows by induction on $r + s$.

In view of the result above, every naturally ordered monoid is a uf-monoid.

If an element m of a uf-monoid M can be factored into primes, say $m = p_1 p_2 \cdots p_n$, then the only other possible way to factor m into primes is

$$m = (p_1 u_1) (u_1^{-1} p_2 u_2) \cdots (u_{n-1}^{-1} p_n)$$

where $u_1, u_2, \dots, u_{n-1}$ are units. This follows readily from Proposition 1.

P. M. Cohn calls an integral domain R with unity *rigid* [2] iff every nonzero, nonunit element of R has unique factorization into primes. As he shows, a rigid domain R is local (i.e., $R - U(R)$ is an ideal). In general, we have:

PROPOSITION 2. *If R is a uf-domain, then R is local.*

PROOF. If $a, b \in R^\times$ and $a - b$ is a unit, then $aR + bR = R$ and hence $aR \cap bR \neq 0$. Therefore, $aR \subset bR$ or $bR \subset aR$ and either a or b is a unit. Hence, R is a local ring.

There are many examples of uf-monoids. Trivially, a group or a free monoid is a uf-monoid. A valuation ring is a uf-domain according to Proposition 1. If $F[x, y]$ is the polynomial ring in noncommuting indeterminates x and y over a field F , then the set H of homogeneous polynomials in $F[x, y]$ is a uf-monoid.

Given a well-ordered set $\{M_i \mid i \in \Gamma\}$ of monoids, we can form their *direct product* $\prod_\Gamma M_i$, their *restricted direct product* $\prod'_\Gamma M_i = \{a \in \prod_\Gamma M_i \mid \text{card}\{i \in \Gamma \mid a(i) \neq 1\} < \infty\}$, and their *free product* $\prod_\Gamma^* M_i$.

Each $a \in \prod_\Gamma^* M_i$, $a \neq 1$, has a unique normal form

$$a = a_{i_1} a_{i_2} \cdots a_{i_n}, \quad a_k \in M_k,$$

where all $a_{i_j} \neq 1$ and $i_j \neq i_{j+1}$ for each j . Evidently a is a unit iff each a_{i_j} is a unit in M_{i_j} . If a is a nonunit, then a can be expressed uniquely in the form $a = a'u$ where $a' = a_{i_1} \cdots a_{i_r}$, $u = a_{i_{r+1}} \cdots a_{i_n}$, a_{i_r} is not a unit in M_{i_r} , and u is a unit. We call a' *right unit-free*. If $r = n$, then $a' = a$ and $u = 1$. Similarly, $a = va''$ for some unit v and some *left unit-free* $a'' \in \prod_r^* M_i$. We are now ready to prove Theorem 1.

PROOF OF THEOREM 1. If some M_i in $\{M_i | i \in \Gamma\}$ is not a uf-monoid, then it is clear by Proposition 1 that $M = \prod_r^* M_i$ is not a uf-monoid. Next, assume that all M_i are uf-monoids and that $a, b \in M$ with $aM \cap bM \neq \emptyset$. Clearly $aM \subset bM$ or $bM \subset aM$ if either a or b is a unit, so let us assume a and b are nonunits. Then $a = a'u$ and $b = b'v$ for some units u, v and some right unit-free elements a', b' . Let a' and b' have normal forms $a' = a_{i_1} \cdots a_{i_n}$ and $b' = b_{j_1} \cdots b_{j_m}$, and assume $m \leq n$. Since a' and b' are right unit-free and $a'M \cap b'M \neq \emptyset$, necessarily $i_k = j_k$ for $k \leq m$ and $a_{i_k} = b_{j_k}$ for $k < m$. If $m < n$, $a_{i_m} \in b_{j_m} M_{j_m}$ and hence $a'M \subset b'M$. If $m = n$, then $a_{i_n} M_{i_n} \cap b_{j_n} M_{j_n} \neq \emptyset$ and either $a_{i_n} M_{i_n} \subset b_{j_n} M_{j_n}$ or $b_{j_n} M_{j_n} \subset a_{i_n} M_{i_n}$. Therefore, always $a'M \subset b'M$ or $b'M \subset a'M$. Since $aM = a'M$ and $bM = b'M$, we have proved that M is a uf-monoid.

PROPOSITION 3. *Let M be an ordered uf-monoid. Then M is naturally ordered iff $M - M^+ \subset U(M)$.*

PROOF. If M is naturally ordered and $a < 1$, then $1M \subset aM$ and a is a unit. If $M - M^+ \subset U(M)$ and $a, b \in M$ with $aM \cap bM \neq \emptyset$ and $b < a$, then either $bM \subset aM$ or $aM \subset bM$. If $bM \subset aM$, then $b = ac$ for some $c < 1$ and $bM = aM$ since c is a unit. In either case, $aM \subset bM$. Hence, M is naturally ordered.

A consequence of this proposition is that a positive uf-monoid is naturally ordered.

If $\{M_i | i \in \Gamma\}$ is a well-ordered set of ordered monoids, then their orders can be extended to $M' = \prod_r^* M_i$, possibly in many different ways. One way is called the Γ -ordering: $a < b$ iff there exists $k \in \Gamma$ such that $a(i) = b(i)$ for all $i < k$ and $a(k) < b(k)$.

If $(M, <_1)$ and $(N, <_2)$ are ordered monoids and $M \xrightarrow{\theta} N$ is a homomorphism, then an ordering $<_3$ can be defined in M by: $a <_3 b$ iff either $\theta(a) <_2 \theta(b)$ or $\theta(a) = \theta(b)$ and $a <_1 b$. Clearly $(M, <_3)$ is an ordered monoid. For example, let $M' = \prod_r^* M_i$ where each $M_i = \{x_i^m | m \in I\}$ and I is $\mathbb{Z}$ or $\mathbb{Z}^+$. Then $M' \xrightarrow{\deg} \mathbb{Z}$ is a homomorphism ($\deg = \text{degree}$) and M' has the $(\Gamma, \deg)$ -ordering defined by: $a < b$ iff $\deg a < \deg b$ or $\deg a = \deg b$ and $a < b$ in the Γ -ordering.

If $\{M_i | i \in \Gamma\}$ is a well-ordered set of ordered monoids, then the orderings in the M_i can also be extended to an ordering in $\prod_{\Gamma}^* M_i$ [5]. In fact, the ordering in $\prod_{\Gamma}^* M_i$ can be chosen as an extension of any ordering in $\prod_{\Gamma} M_i$ in the sense that the natural epimorphism $\prod_{\Gamma}^* M_i \rightarrow \prod_{\Gamma} M_i$ will be order-preserving. We shall assume, henceforth, that whatever ordering we choose in $\prod_{\Gamma}^* M_i$, it preserves the ordering in every M_i . Hence, if all the M_i are positive monoids, then $\prod_{\Gamma}^* M_i$ is also positive. It follows from Theorem 1 and Proposition 3 that a free product of positive uf-monoids is naturally ordered, no matter which order we choose in $\prod_{\Gamma}^* M_i$.

An example to show that the free product might be naturally ordered even if some of the monoids are not positive is as follows: Let $M_1 = \{x^n | n \in \mathbb{Z}^+\}$, M_2 be an ordered group, and $M = M_1 * M_2$. If M is ordered by an extension of this (1, 2)-ordering in $M_1 \times M_2$, then each $a \in M$, $a < 1$, is in M_2 and hence is a unit. Thus, M is naturally ordered by Theorem 1 and Proposition 3. If the (2, 1)-ordering is used in $M_1 \times M_2$ and $a \in M_2$, $a < 1$, then $ax < 1$. Since ax is not a unit, M is not naturally ordered according to Proposition 3, although both M_1 and M_2 are naturally ordered.

For each monoid M , let $W_0(M)$ denote the set of all finite subsets of M ; and if M is ordered, let $W(M)$ denote the set of all well-ordered subsets of M . If M is ordered and $A \subset M$, let $\inf A$ denote the least element of A , if it exists. As usual, for any $A \subset M$ and $B \subset M$, we let $AB = \{ab | a \in A, b \in B\}$. The following result is proved in [3, Lemma 1].

PROPOSITION 4. *Let M be an ordered monoid. For all $B, C \in W(M)$ and $d \in M$, $B \cup C$ and BC are in $W(M)$ and $\{b \in B | d = bc \text{ for some } c \in C\}$ is in $W_0(M)$.*

The following result is proved for ordered groups in [4, p. 135]. Since the proof does not seem to carry over readily to monoids, we have supplied a new proof.

PROPOSITION 5. *Let M be an ordered monoid, $B \in W(M)$, $\bar{B} = \bigcup_{n=1}^{\infty} B^n$, and $Z_a = \{k \in \mathbb{Z}^+ | a \in B^k\}$ for each $a \in M$. If $\inf B > 1$, then $\bar{B} \in W(M)$ and $\text{card } Z_a < \infty$ for every $a \in \bar{B}$.*

PROOF. Assume that $\bar{B} \notin W(M)$, so that $\bar{B}$ contains infinite descending chains, and let S be the set of all such chains in $\bar{B}$. Also, let $A = \{a \in \bar{B} | a^n > C \text{ for some } C \in S \text{ and some integer } n > 0\}$, where $a^n > C$ means $a^n > c$ for every $c \in C$. Finally, let b be the least element of A and r be the least positive integer such that $b^r > C$ for some $C \in S$.

If $b^r > C$, where $C = \{c_k\}$ and $c_1 > c_2 > \dots$, then each $c_k = b_{k1}b_{k2} \dots b_{kn_k}$ for some $b_{ki} \in B$. Let $b_k = \max\{b_{ki} \mid i=1, \dots, n_k\}$. Since $b_k^{n_k} \geq c_k > c_{k+1} > \dots$, evidently each $b_k \in A$. Thus, $b_k \geq b$ for every k . We note that $r > 1$; for if $b > c_k$ for each k , then $b > c_k \geq b_k$ since $\inf B > 1$. Now each c_k has the form $c_k = p_k b_k q_k$ for some $p_k, q_k \in \bar{B} \cup \{1\}$. Since $\{p_k\} \{b_k\} \{q_k\}$ is not well-ordered, either $\{p_k\}$ or $\{q_k\}$ is not well-ordered. Assume that $\{p_k\}$ is not well-ordered. Then $D \subset \{p_k\}$ for some $D \in S$. Since $b^r > c_k = p_k b_k q_k \geq p_k b_k \geq p_k b$, $b^{r-1} > p_k$ for every k . Thus, $b^{r-1} > D$ contrary to the minimality of r . Hence, $\bar{B} \in W(M)$.

Assume that $\text{card } Z_a = \infty$ for some $a \in \bar{B}$, and let a be the least such element of $\bar{B}$. By assumption, $a = b_{k1}b_{k2} \dots b_{kn_k}$ for some integers $2 \leq n_1 < n_2 < \dots$ and some $b_{ki} \in B$. We can assume, without loss of generality, that $b_{11} \leq b_{21} \leq b_{31} \leq \dots$. If we let $a_k = b_{k2} \dots b_{kn_k}$, then $a > a_1 \geq a_2 \geq a_3 \geq \dots$. Hence, there exists an integer m such that $a_m = a_{m+1} = a_{m+2} = \dots$. Then $\text{card } Z_{a_m} = \infty$ contrary to the choice of a . Therefore $\text{card } Z_a < \infty$ for every $a \in \bar{B}$.

2. Ordered-monoid rings. In this section, F is taken to be a ring with unity. Given a monoid M , an expression of the form

$$f = \sum_{a \in M} \alpha_a a, \quad \alpha_a \in F,$$

is called a *formal power series* in M over F . As usual, the *support* of f is defined by $\text{supp } f = \{a \in M \mid \alpha_a \neq 0\}$. The set

$$F[M] = \left\{ f = \sum \alpha_a a \mid \text{supp } f \in W_0(M) \right\}$$

becomes a ring if we define: for $f = \sum \alpha_a a$, $g = \sum \beta_a a$, $f+g = \sum (\alpha_a + \beta_a)a$, $fg = \sum \gamma_a a$, where $\gamma_a = \sum_{b,c; bc=a} \alpha_b \beta_c$. Then $F[M]$ is the usual monoid ring.

When we further assume M is ordered, then we can also form the power series ring

$$F[[M]] = \left\{ f = \sum \alpha_a a \mid \text{supp } f \in W(M) \right\}$$

with operations as defined above. That $F[[M]]$ is a ring follows from Proposition 4 and the fact that $\text{supp } (f+g) \subset \text{supp } f \cup \text{supp } g$ and $\text{supp } fg \subset (\text{supp } f)(\text{supp } g)$. Clearly we can consider $F \subset F[M] \subset F[[M]]$. If F is an integral domain, then so are $F[M]$ and $F[[M]]$. For if we define $\inf f$ to be $\inf \text{supp } f$ whenever it exists, then it is

clear that for all nonzero $f, g \in F[[M]]$, $\inf fg = (\inf f)(\inf g)$ and hence $fg \neq 0$.

If $f \in F[[M]]$ and $\inf f > 1$, then we see as in [4, p. 135] that $g = \gamma_1 f + \gamma_2 f^2 + \dots$ is a well-defined element of $F[[M]]$ for any $\gamma_i \in F$. Thus, if $f^n = \sum \alpha_{na} a$, we take $g = \sum \beta_a a$ where $\beta_a = \sum_{n=1}^{\infty} \gamma_n \alpha_{na}$. Since $\text{supp } g \subset \bigcup \text{supp } f^n \subset \bigcup (\text{supp } f)^n$, $g \in F[[M]]$ by Proposition 5.

PROPOSITION 6. *Let M an ordered monoid, $f = \sum \alpha_a a$ be a nonzero element of $F[[M]]$, and $d = \inf f$. Then f is a unit iff d is a unit of M and α_d is a unit of F .*

PROOF. If f has an inverse $f^{-1} = \sum \beta_a a$ and $c = \inf f^{-1}$, then $dc = cd = 1$ and $\alpha_d \beta_c = \beta_c \alpha_d = 1$. Hence, $d \in U(M)$ and $\alpha_d \in U(F)$. Conversely, if $d \in U(M)$ and $\alpha_d \in U(F)$ then we can express f in the form $f = \alpha_d d(1 - h)$ for some $h \in F[[M]]$ with $\inf h > 1$. Then $k = h + h^2 + h^3 + \dots \in F[[M]]$ and we verify that $(1 - h)(1 + k) = 1$ in the usual way. Therefore, f has $(1 + k)\alpha_d^{-1}d^{-1}$ as a right inverse. A similar argument shows f also has a left inverse.

If F is a field and M is an ordered group, then this proposition is the well-known result [4, p. 137] that $F[[M]]$ is a field.

We are now in a position to prove Theorem 2.

PROOF OF THEOREM 2. Assume that $R = F[[M]]$ is a uf-domain and $a, b \in M$ with $a < b$ and $aM \cap bM \neq \emptyset$. Then $aR \cap bR \neq 0$ and hence $a = bc$ or $b = ac$ for some $c \in M$. If $a = bc$, then $c < 1$. Since R is local by Proposition 2 and $(-c + 1) + c \in U(R)$, either c or $-c + 1$ is a unit. In either case, c is a unit of M by Proposition 6. Therefore $b = ac^{-1}$ and always $bM \subset aM$. Hence, M is naturally ordered.

Now assume M is naturally ordered and $f, g \in R$ with $fR \cap gR \neq 0$ and $\inf f = c \leq d = \inf g$. Then $fg' = gf' \neq 0$ for some $f', g' \in R$, and $\inf f' = c' \leq d' = \inf g'$. If c' is a unit, then f' is a unit by Proposition 6 and $gR \subset fR$. If c' is not a unit, then let $A = \{a \in \text{supp } f' \mid Ma \cap Mc' \neq \emptyset\}$ and $B = \{a \in \text{supp } g' \mid Ma \cap Mc' \neq \emptyset\}$. We can express $f' = f'_1 + f'_2$ and $g' = g'_1 + g'_2$, where $\text{supp } f'_1 = A$, $\text{supp } f'_2 = (\text{supp } f') - A$, $\text{supp } g'_1 = B$, and $\text{supp } g'_2 = (\text{supp } g') - B$. Since $c' \leq a$ for all $a \in A \cup B$ and M is naturally ordered, we must have $Ra \subset Rc'$ for all $a \in A \cup B$. Thus, $f'_1 = hc'$ and $g'_1 = kc'$ for some $h \in U(R)$, $k \in R$. Now $fk'c' + fg'_2 = ghc' + gf'_2$, with $Rc' \cap Ra = 0$ for all $a \in (\text{supp } fg'_2) \cup (\text{supp } gf'_2)$. Therefore, $fk'c' = ghc'$, $fkh^{-1} = g$, and $gR \subset fR$. This proves the theorem.

If $M_i = \{x_i^n \mid n \in \mathbb{Z}^+\}$ and $M = \prod_{i \in \Gamma} M_i$, the free monoid with generators $\{x_i \mid i \in \Gamma\}$, then M is naturally ordered for any ordering in M . Hence, by Theorem 2, the ring $R = F[[M]]$ is a uf-domain for any field F . Clearly every nonzero nonunit $f \in R$ can be factored into

primes, since $\inf f$ has only a finite number of factors in M .

If we take the $(\Gamma, \deg)$ -ordering in $M' = \prod_{\Gamma} M_i$ and extend it to M , then R consists of all formal power series in the x_i over F having only a finite number of terms of each degree. If the Γ -ordering is used in M' and extended to M , then we get a different ring R of formal power series. While every $f \in R$ has only a finite number of terms of each degree, not all power series of this form are in R . For example, if $\Gamma = \mathbb{Z}^+$ and $f = x_1 + x_2^2 + x_3^3 + \cdots$, $g = x_1 + x_1^2 + x_1^3 + \cdots$, then $g \in R$ but $f \notin R$.

Another possible ordering in M' is the (dual Γ , $\deg$)-ordering $<_a: a <_a b$ iff $\deg a < \deg b$ or $\deg a = \deg b$ and $b < a$ in the Γ -ordering. Clearly $<_a$ is an extension of the ordering in each M_i , and hence $<_a$ can be extended to an ordering in M .

The monoid $(M', <_a)$ is well-ordered. For if $S \subset M'$, $m = \min_{a \in S} (\deg a)$, and $T = \{a \in S \mid \deg a = m\}$, then the least element of T , if it exists, is the least element of S . Thus, we need only show that if $\deg S = m$ (i.e., $\deg a = m$ for all $a \in S$) then S has a least element. If $m = 0$ then $S = \{1\}$ and S has a least element. Assume that every set T of degree m has a least element, and let S be any set of degree $m+1$. If i is the least element of Γ such that $a(i) \neq 1$ for some $a = \prod_{\Gamma} a(i) \in S$ and $T = \{a \in S \mid a(i) \neq 1\}$, then the least element of T , if it exists, is the least element of S . Let $U = \{x_i^{-1}a \mid a \in T\}$, so that $U \subset M'$ and $\deg U = m$. Now U has a least element b by the induction assumption. Clearly $x_i b$ is the least element of S . We conclude that $(M', <_a)$ is well-ordered. Then M , with any ordering which is an extension of $<_a$, is also well-ordered. If $R = F[[M]]$, then R is the set of all power series $\sum \alpha_a a$. Thus, R is the power series domain considered by Cohn in [1].

The three different orderings in $M = \prod_{\Gamma}^* M_i$ considered above lead to three different power series rings $R = F[[M]]$. Each of these rings is a uf-domain for any field F by Theorem 2. In particular, if the ordering $<_a$ is used we have another proof of Cohn's result in [1] that R is rigid.

The example given above, $M = M_1 * M_2$, where $M_1 = \{x^n \mid n \in \mathbb{Z}^+\}$, M_2 is any ordered group, and the $(1, 2)$ -ordering is taken in $M = M_1 \times M_2$, is naturally ordered. Hence, $R = F[[M]]$ is a uf-domain. Evidently R is also rigid. If the $(2, 1)$ -ordering is taken in M , the resulting ring $P = F[[M]]$ is not a uf-domain since M is not naturally ordered. Actually, P is not even local. For if $a \in M_2$, $a < 1$, and $b = -ax + 1$, $c = ax$, then $b + c$ is a unit in P although neither b nor c is a unit since $\inf b = \inf c = ax$ is not a unit.

BIBLIOGRAPHY

1. P. M. Cohn, *Factorization in non-commutative power series rings*, Proc. Cambridge Philos. Soc. **58** (1962), 452–464. MR **25** #2092.
2. ———, *Hereditary local rings*, Nagoya Math. J. **27** (1966), 223–230. MR **33** #5663.
3. P. Conrad, *Generalized semigroup rings*, J. Indian Math. Soc. **21** (1957), 73–95. MR **20** #887.
4. L. Fuchs, *Partially ordered algebraic systems*, Pergamon Press, New York; Addison-Wesley, Reading, Mass., 1963. MR **30** #2090.
5. R. E. Johnson, *Free products of ordered semigroups*, Proc. Amer. Math. Soc. **19**(1968), 697–700. MR **37** #2864.

UNIVERSITY OF NEW HAMPSHIRE, DURHAM, NEW HAMPSHIRE 03824