PROCEEDINGS OF THE
Cambridge Philosophical Society

VOL. 65 MAY 1969 PART 3

*Proc. Camb. Phil. Soc.* (1969), 65, 579
PCPS 65–59
*Printed in Great Britain*

# Unique factorization rings

BY C. R. FLETCHER
*University College of Wales, Aberystwyth*

*In memory of Professor W. B. Pennington*

(*Received* 23 *February* 1968)

1. *Introduction.* The concept of a unique factorization domain (UFD) has been defined for commutative (e.g. (4) page 21) and non-commutative (1) integral domains. We take the theory a stage further here by defining a unique factorization ring (UFR), where throughout, a ring is understood to mean a commutative ring with identity, possibly containing proper zero-divisors.

A UFR is a ring in which each non-unit element has a unique (in a certain sense) irreducible decomposition. The zero element is included since proper zero-divisors exist in general. We could also consider irreducible decompositions of units if we took the (natural?) step of allowing units to be irreducibles. The subsequent work would still be valid, for the 'relevant part' (see prior to Proposition 3) of the decomposition of a non-unit (unit) element would contain no unit (merely one unit). However, we have taken the traditional path and do not allow unit irreducibles.

We first show that we have a true generalization of a UFD by proving that an integral domain is a UFR if and only if it is a UFD. We then see that the direct sum of a finite number of UFR's is a UFR, and in particular, the direct sum of a finite number of UFD's is a UFR. Not all UFR's are of this second type however (e.g. the ring of integers modulo $q^m$, $q$ prime and $m > 1$). Finally we prove that a principal ideal ring is a UFR.

2. *Definition of a UFR.* All elements introduced are members of a ring $R$ unless otherwise stated.

DEFINITION 1. *A refinement of a factorization* $r = a_1 \dots a_n$ *is obtained by factorizing one or more of the* $a_i$*'s* $(i = 1, \dots, n)$.

DEFINITION 2. *A non-unit element* $p \in R$ *is said to be irreducible if and only if each factorization of* $p$ *has a refinement containing* $p$. If $R$ is a domain, the above definition is equivalent to the standard definition, except that here the zero element is irreducible.



https://doi.org/10.1017/S0305004100003352 Published online by Cambridge University Press

DEFINITION 3. *The $U$-class of an element $r \in R$, denoted by $U(r)$, is given by*

$$U(r) = \{\beta \in R | \beta\gamma r = r \quad \text{for some} \quad \gamma \in R\}.$$

The following results are easily proved.

PROPOSITION 1. (i) *If $\beta, \gamma \in U(r)$ then $\beta\gamma \in U(r)$.*
(ii) *If $\beta \in U(rs)$ and $r \in U(s)$ then $\beta \in U(s)$.*
(iii) *$U(rs) \supseteq U(r)$.*
(iv) *$U(ar) = U(r)$ for a non-zero-divisor $a$.*

DEFINITION 4. *A $U$-decomposition of an element $r \in R$ is a factorization of $r$*

$$r = (p_1' \dots p_k')(p_1 \dots p_n),$$

*such that*
(i) *$p_i'$, $p_j$ are irreducible $i = 1, \dots, k$, $j = 1, \dots, n$.*
(ii) *$p_i' \in U(p_1 \dots p_n)$ $(i = 1, \dots, k)$.*
(iii) *$p_j \notin U(p_1 \dots \hat{p}_j \dots p_n)$ $j = 1, \dots, n$,*

*where $\hat{}$ denotes that the term is omitted.*

The two brackets will always be written in the above order. If the first bracket is empty we write $r = (\ )(p_1 \dots p_n)$. A necessary and sufficient condition for a $U$-decomposition of an element to exist is that it has an irreducible decomposition. This condition is clearly necessary.

PROPOSITION 2. *If $r \in R$ has an irreducible decomposition then $r$ has a $U$-decomposition.*

*Proof.* Suppose $r = p_1 \dots p_n$, where $p_i$ is irreducible $i = 1, \dots, n$. Then either $r = (\ )(p_1 \dots p_n)$ and $r$ has a $U$-decomposition, or $p_i \in U(p_1 \dots \hat{p}_i \dots p_n)$ for some $i$. If the latter, suppose $p_1$ has this property, and similarly choose $p_2$ say, where $p_2 \in U(p_3 \dots p_n)$. Perform this operation repeatedly, choosing $p_1, p_2, \dots, p_k$ until no further $p_i$ has this property. We claim that $r = (p_1 \dots p_k)(p_{k+1} \dots p_n)$ is a $U$-decomposition. From the construction $p_j \notin U(p_{k+1} \dots \hat{p}_j \dots p_n)$ $j = k+1, \dots, n$, and $p_i \in U(p_{i+1} \dots p_n)$ $i = 1, \dots, k$. By repeated application of Proposition 1 (ii) the proof is completed.

DEFINITION 5. *Two elements $a, b \in R$ are said to be associate if and only if $a$ divides $b$ and $b$ divides $a$ in $R$.*

This condition is not equivalent to '$a = ub$ for some unit $u \in R$'. For example let $R = F[x, y, z]/(x - xyz)$, where $F$ is a field. Then $\bar{x}$ and $\overline{xy}$ are associates in $R$, but $\bar{x} \neq \overline{xyu}$ for any unit $\bar{u} \in R$.

In a $U$-decomposition $r = (p_1' \dots p_k')(p_1 \dots p_n)$ we call the factorization $p_1 \dots p_n$ the relevant part, the element $s = p_1 \dots p_n$ the relevant element, and the set $\{p_1', \dots, p_k'\}$ the non-relevant set.

PROPOSITION 3. *The relevant element of a $U$-decomposition of $r \in R$ is an associate of $r$.*

*Proof.* Suppose

$$r = (p_1' \dots p_k')(p_1 \dots p_n).$$

Then $$p_i' \in U(p_1 \dots p_n) \quad \text{for} \quad i = 1, \dots, k,$$

and from Proposition 1 (i)

$$p_1' \dots p_k' \in U(p_1 \dots p_n).$$

Hence $r$ and $p_1 \dots p_n$ are associate.

https://doi.org/10.1017/S0305004100003352 Published online by Cambridge University Press

It follows immediately that the relevant elements of two $U$-decompositions of $r \in R$ are associate.

DEFINITION 6. *Two $U$-decompositions of $r \in R$*

$$r = (p_1' \dots p_k')(p_1 \dots p_n) = (q_1' \dots q_l')(q_1 \dots q_m)$$

*are said to be associate if and only if* (i) $m = n$, (ii) *after a suitable change in the numbering of the factors of the second $U$-decomposition, the elements $p_i$ and $q_i$ are associate $i = 1, \dots, n$.*

DEFINITION 7. *A ring $R$ is called a unique factorization ring* (UFR) *if and only if* (UFR 1) *every non-unit element of $R$ has a $U$-decomposition,* (UFR 2) *any two $U$-decompositions of a non-unit element of $R$ are associate.*

An element in $R$ having a $U$-decomposition and satisfying UFR 2 is said to have unique factorization. From Proposition 2 UFR 1 is satisfied whenever every non-unit element of $R$ has an irreducible decomposition. We first show that in the domain case the definitions of UFR and UFD are equivalent. We assume the definition of UFD given in (4), page 21.

THEOREM 4. *An integral domain $R$ is a UFR if and only if $R$ is a UFD.*

*Proof.* Suppose first that $R$ is a UFR and consider only non-zero, non-unit elements of $R$. Then each $U$-class is the class of units, and each non-relevant set is empty. Clearly $R$ is a UFD. Conversely if $R$ is a UFD then every non-zero, non-unit element of $R$ has unique factorization. Since $U(O) = R$ and $O \notin U(s)$ for any $s \neq 0$, a $U$-decomposition of the zero element is of the form $(p_1' \dots p_k')(O)$. Hence $O$ has unique factorization and $R$ is a UFR.

3. *The direct sum of UFR's.* We prove that the direct sum of two UFR's is a UFR. Induction may be used to extend the result to include a finite number of rings.

THEOREM 5. *If $R$ and $S$ are UFR's, then $R \oplus S$ is a UFR.*

*Proof.* We may easily see that the irreducibles of $R \oplus S$ are all elements of the form $(u, q)$ and $(p, v)$, where $u, v$ are units and $p, q$ are irreducibles in $R$ and $S$ respectively. Consider any non-unit element $(r, s) \in R \oplus S$, where both $r$ and $s$ are not units. We shall suppose that neither is a unit, but the proof is similar if this is not the case. Then $r$ and $s$ have $U$-decompositions

$$r = (p_1' \dots p_k')(p_1 \dots p_n) \quad \text{and} \quad s = (q_1' \dots q_l')(q_1 \dots q_m).$$

Therefore $(r, s)$ has the irreducible decomposition

$$(p_1', 1) \dots (p_n, 1)(1, q_1') \dots (1, q_m),$$

and UFR 1 is satisfied.

Now suppose $(r, s)$ has the two $U$-decompositions

$$((r_1', s_1') \dots (r_l', s_l'))((r_1, s_1) \dots (r_m, s_m)) = ((\rho_1', \sigma_1') \dots (\rho_k', \sigma_k'))((\rho_1, \sigma_1) \dots (\rho_n, \sigma_n)).$$

Then $$(r_i', s_i') \in U((r_1, s_1) \dots (r_m, s_m)) \quad (i = 1, \dots, l)$$

and $$r_i' \in U(r_1 \dots r_m), \quad s_i' \in U(s_1 \dots s_m).$$

Also $$(r_i, s_i) \notin U((r_1, s_1) \dots \widehat{(r_i, s_i)} \dots (r_m, s_m)) \quad (i = 1, \dots, m),$$

and exactly one of $$r_i \notin U(r_1 \dots \hat{r}_i \dots r_m) \quad \text{and} \quad s_i \notin U(s_1 \dots \hat{s}_i \dots s_m)$$



https://doi.org/10.1017/S0305004100003352 Published online by Cambridge University Press

occurs. Suppose that

$$r_i \in U(r_1 \dots \hat{r}_i \dots r_m) \quad \text{for} \quad i = 1, \dots, g$$

and

$$r_j \notin U(r_1 \dots \hat{r}_j \dots r_m) \quad \text{for} \quad j = g+1, \dots, m.$$

Then $s_i \notin U(s_1 \dots \hat{s}_i \dots s_m)$, $s_i$ is not a unit, and $r_i$ is a unit. Similarly $s_j$ is a unit. Put $u = r_1 \dots r_g$ and $v = s_{g+1} \dots s_m$, then $ur_{g+1}$ is irreducible in $R$ and $s_g v$ is irreducible in $S$. Hence

$$r = (r_1' \dots r_l')(ur_{g+1} \dots r_m) \quad \text{and} \quad s = (s_1' \dots s_l')(s_1 \dots s_g v)$$

are $U$-decompositions of $r$ and $s$ respectively. Similarly

$$r = (\rho_1' \dots \rho_k')(\mu\rho_{h+1} \dots \rho_n) \quad \text{and} \quad s = (\sigma_1' \dots \sigma_k')(\sigma_1 \dots \sigma_h \nu),$$

where $\mu = \rho_1 \dots \rho_h$ and $\nu = \sigma_{h+1} \dots \sigma_n$ are units, are $U$-decompositions of $r$ and $s$ respectively. Therefore $m-g = n-h$ and $g = h$, i.e. $m = n$. $r_j$ and $\rho_j$ are associate for $j = g+1, \dots, n$ and $s_i$ and $\sigma_i$ are associate for $i = 1, \dots, g$, after a suitable change in the numbering of the factors. Thus $(r_i, s_i)$ is an associate of $(\rho_i, \sigma_i)$ for $i = 1, \dots, n$ and $R \oplus S$ is a UFR.

COROLLARY. *If $R_i$ is a UFR for $i = 1 \dots n$ then $R_1 \oplus \dots \oplus R_n$ is a UFR.*

In particular a finite direct sum of UFD's is a UFR. The converse is not true, i.e. not every UFR may be expressed as a direct sum of UFD's. For consider the ring of integers modulo $q^m$, $q$ prime and $m > 1$. This is principal and hence is a UFR (Theorem 7, Corollary), but is not a direct sum of domains (proved by counting the number of elements in a direct sum and equating characteristics).

4. *Principal ideal rings.* It is well known that a principal ideal domain is a UFD. In the non-commutative case one can also obtain a unique factorization theorem ((2), p. 34). We now show that a principal ideal ring (PIR) is a UFR. This extends the work of Serbin (3) in the particular instance of a commutative ring. From (4), p. 245 we have the following definition and result.

DEFINITION 8. *A PIR is called special if it has only one prime ideal $P \neq R$ and if $P$ is nilpotent, that is $P^m = (O)$ for some integer $m > 0$.*

THEOREM 6. *Every PIR is a (finite) direct sum of principal ideal domains and of special PIR's.*

Hence from Theorem 5, Corollary, we need only show that a special PIR is a UFR.

THEOREM 7. *If $R$ is a special PIR then $R$ is a UFR.*

*Proof.* UFR 1 may be verified by considering the principal ideals generated by elements not having an irreducible decomposition. This class has a maximal member $Ra$, where $a$ is not irreducible. Therefore $a = a_1 \dots a_n$ where $a$ does not divide $a_i$ and $Ra \subset Ra_i$ for all $i$ (strict inclusion). Every $a_i$ thus has an irreducible decomposition, and so does $a$. Contradiction. Suppose now that $R$ has the unique prime ideal $P$ with $P^m = (O)$. If $m = 1$ then $R$ is a field, and in particular is a UFR. If $m > 1$ put $P = R\alpha$. Then $\alpha$ is the only irreducible in $R$ up to associativity, all elements not in $R\alpha$ are units, and every non-unit non-zero $r \in R$ has the form $r = u\alpha^k$, where $u$ is a unit and $k < m$ is unique (4). Therefore $R$ is a UFR.

COROLLARY. *A PIR is a UFR.*

https://doi.org/10.1017/S0305004100003352 Published online by Cambridge University Press

The author would like to express his thanks to the referee for communicating the example which follows Definition 5.

## REFERENCES

(1) Cohn, P. M. Noncommutative unique factorization domains. *Trans. Amer. Math. Soc.* **109** (1963), 313–331.
(2) Jacobson, N. *The theory of rings* (Amer. Math. Soc. 1943).
(3) Serbin, H. Factorization in principal ideal rings. *Duke Math. J.* **4** (1938), 656–663.
(4) Zariski, O. and Samuel, P. *Commutative algebra*, vol. 1 (Princeton 1958).

https://doi.org/10.1017/S0305004100003352 Published online by Cambridge University Press