Turkish Journal of Mathematics

Volume 21 | Number 4 Article 2

1-1-1997

Unique Factorisation for Commutative Rings Without Identity

A. G. AĞARGÜN

C.R. FLETCHER

Tr. J. of Mathematics
21 (1997) , 401 – 408.

UNIQUE FACTORISATION FOR COMMUTATIVE RINGS WITHOUT IDENTITY

A.G. Ağargün & C.R. Fletcher

Abstract

This paper concerns the unique factorisation property in commutative rings not necessarily with identity. We give a new definition of irreducibility and associates in a commutative ring with 1 (crw1), and define a UFR R in terms of a monomorphism from R into a crw1. This becomes equivalent to the definition in [3] when R has an identity. We generalize results on direct sums and direct summands. By our definition we have new members of the family of UFR's.

Keywords and phrases: Irreducibility, associates, unique factorisation.

1. Introduction

It is well known that a straightforward transfer of definitions from $\boldsymbol{Z}$ to a subring will lose the property of uniqueness of factorisation into primes. But one useful way to deal with rings not containing an identity is to embed them into a ring with identity. With a subring of $\boldsymbol{Z}$ this could lead us back to $\boldsymbol{Z}$ or not as we chose. Back in $\boldsymbol{Z}$, if we took that road, we could adopt the usual factorisations for our elements.

Suppose then that R is a commutative ring, perhaps without identity. R' is a commutative ring with identity, and $\theta : R \to R'$ is a monomorphism. We then consider factorisations of elements of R via the factorisation of the elements of $\theta(R)$ in R'. Two fundamental ways in which to construct an appropriate ring containing an identity are as follows.

(i) Form $R \times Z$ with the usual addition, and with multiplication defined by

$$(a,n)\cdot(b,m) = (ab + ma + nb, mn).$$

Then $R \times Z$ is a commutative ring with identity $(0,1)$ and $\theta : R \to R \times Z$ is a monomorphism where $\theta(r) = (r,0)$.

(ii) Form the ring of fractions R_S where S contains no zero-divisor, then $\theta_S : R \to R_S$ is a moromorphism where

$$\theta_S(r) = [rs, s].$$

We could define uniqueness of factorisation absolutely in terms of one or both of these, but it seems more sensible to define the concept relatively and talk of a unique factorisation ring with respect to a particular monomorphism. Incidentally, the subrings of Z do not give unique factorisation rings under construction (i). For example, in $2Z \times Z$ we have the different U-decompositions

$$(\ )((2,0)(2,0)(2,0)(2,1)) = (\ )((2,2)(2,0)(2,1))$$

(see below for the definitions).

2. Definitions

Let R be a crw1. A non-unit element $p \in R$ is said to be *irreducible* if whenever $p = a_1 \cdots a_n$, then for some $i, a_i = aa_i'$, $a, b \in R$ are said to be *associate* if a divides b and b divides a. We write $a \sim b$ if a and b are associates.

We recall that $U(r)$, the U-class of $r \in R$, is given by

$$U(r) = \{\alpha \in R \mid \exists\, \beta \in R \quad \text{where} \quad r = \alpha\beta r\}$$

and a U-decomposition of $r \in R$ is a factorisation of r, written in the form

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

where all the factors are irreducible, the factors of the first bracket are in $U(p_1 \cdots p_n)$, and $p_i \notin U(p_1 \cdots \hat{p}_i \cdots p_n)$ for each i, the hat signifying omission.

Then R, a commutative ring with identity (crw1), is a unique factorisation ring (UFR) if every non-unit element has a U-decomposition, and if for two such U-decompositions

$$a = (p_1' \cdots p_k')(p_1 \cdots p_n) = (q_1' \cdots q_\ell')(q_1 \cdots q_m),$$

we have $m = n$ and p_i, q_i are associate after a suitable renumbering of the qs.

But now we require the following generalisation of the definition of irreducibility. Let R be a crw1, then a non-unit element $p \in R$ is said to be a *neo-irreducible* if whenever

$$yp = ya_1 \cdots a_n$$

for any $y \in R$, then $ya_i \sim yp$ for some i. This corresponds to the usual definition for integral domains, but if zero divisors are present, the number of irreducibles may be reduced. For example (50, -1) is an irreducible but not a neo-irreducible in $5Z \times Z$ since

$$(5,0)(50,-1) = (5,0)(5,2)(5,2)$$

and

$$(5,0)(5,2) \neq (5,0)(50,-1)(5k,\ell).$$

However, as we shall see, the definitions of irreducible and neo-irreducible are equivalent for rings with unique factorisation. And for a crw1, a UFR remains a UFR for the identity monomorphism.

Following the innovation in the definition of neo-irreducible we define a pair of associate elements similarly in terms of subset T of R. We say that $a, b \in R$ are $ass(T)$ if for each $y \in T$ $ya \sim yb$ and we write $a \sim_T b$. $\sim_T$ is an equivalence relation which reduces to the usual relation if $1 \in T$.

We may now define what we mean by a commutative ring, not necessarily containing an identity, being a UFR with respect to a monomorphism.

Definition. *Let R be a commutative ring and R' a crw1, and suppose $\theta : R \to R'$ is a monomorphism with $\theta(R)$ an ideal of R'. Then R is said to be a UFR with respect to (w.r.t) $\theta : R \to R'$ if the following properties are satisfied.*

UFR1. Every non-unit element of the form $\theta(a)$ in R' has U-decompositions into neo-irreducibles in R'.

UFR2. If $\theta(a) = (p'_1 \cdots p'_k)(p_1 \cdots p_n) = (q'_1 \cdots q'_\ell)(q_1 \cdots q_m)$ are two such U-decompositions of a non-unit $\theta(a) \in \theta(R)$, then $m = n$, and $p_i \sim_{\theta(R)} q_i$ for $i = 1, \ldots n$ after a suitable renumbering of the q' s.

Since every product of neo-irreducibles may be turned into a U-decomposition the property UFR1 is equivalent to 'every non-unit element of the form $\theta(a)$ in R' may be expressed as a product of neo-irreducibles in R'.

3. Equivalence of Definitions

We may now substantiate our claim that in the case of a crw1 the new definition of UFR is equivalent to the old definition in the following sense.

Theorem 1. *Let R be a crw1. Then R is a UFR if and only if R is a UFR w.r.t $1 : R \to R$.*

It is helpful first to show that the definitions of neo-irreducibility and irreducibility are equivalent when we have uniqueness of factorisation.

Lemma 2. Let R be a crw1.

(i) If R is a UFR then every irreducible in R is neo-irreducible;

(ii) If R is a UFR w.r.t $1 : R \to R$ then every irreducible in R is neo-irreducible.

Proof. (i) Suppose q is irreducible in R, and for any $y \in R$ let

$$yq = ya_1 \cdots a_n. \tag{1}$$

We have to show that yq divides ya_i for some i. If y is a unit or zero this is the case. If y is non-zero and non-unit then it has an irreducible decomposition $y_1 \cdots y_s$. Suppose that $q \in U(y_1 \cdots y_s)$ then $y = q\alpha y$ and $ya_i = yq(\alpha a_i)$ for each of the elements a_i. The case when $q \notin U(y_1 \cdots y_s)$ involves chasing elements round two U-decompositions. Write each side of (1) as a U-decomposition

$$(y_{t+1} \cdots y_s)(y_1 \cdots y_t q) = (y_j \cdots p_j \cdots)(y_i \cdots p_i \cdots),$$

where on the right hand side the p elements are irreducible factors of the a elements. Since R is a UFR, q is an associate of either y_i or p_i. If the latter then $p_i = q\beta$ and $a_i = q\beta'$ giving $ya_i = yq\beta'$. The former possibility is a little more complicated and requires another split into two cases. Suppose $t+1 \leq i \leq s$ then $y_i \in U(y_i \cdots y_t q)$ and

$$y_1 \cdots y_t q = y_i \gamma y_1 \cdots y_t q.$$

But if q and y_i are associate then $y_i = q\delta$ and

$$y_1 \cdots y_t y_i = y_1 \cdots y_t y_i \gamma \delta q.$$

Hence

$$ya_i = yq(\gamma \delta a_i).$$

Finally, suppose that $1 \leq i \leq t$. Then

$$(y_{t+1} \cdots y_s)(y_1 \cdots y_i \cdots y_t q) = (y_j \cdots p_j \cdots)(y_i \cdots p_i \cdots).$$

The two $y_i s$ can be paired off leaving q an associate of some other y_k, and the process can be repeated. Eventually we reach a case which we have dealt with previously. Hence q is a neo-irreducible.

(ii) The proof of the second part starts off differently but soon falls into a similar pattern. Suppose q is irreducible in R, and for any $y \in R$ let

$$yq = ya_1 \cdots a_n. \tag{2}$$

Once again we have to show that yq divides ya_i for some i. Express both sides of (2) as products of neo-irreducibles in the UFR w.r.t $1 : R \to R$. We do not know that q is neo-irreducible; this in fact is what we are trying to prove:

$$y_1 \cdots y_s \cdot q_1 \cdots q_k = y_1 \cdots y_s \cdot p_i \cdots, \tag{3}$$

where p_i is a neo-irreducible factor of a_i. Since q is irreducible in R we have $q_1 = q\sigma$ say, and $q_2 \cdots q_k \in U(q_1)$. Now consider U-decompositions of both sides of (3).

If $q_1 \in U(y_1 \cdots y_s)$ then $y = q_1 \alpha y = yq(\sigma\alpha)$ and $ya_i = yq(\sigma\alpha a_1)$. If $q_1 \notin U(y_1 \cdots y_s)$ then the U-decompositions will take the forms

$$(y_{t+1} \cdots y_s q_2 \cdots q_k)(y_1 \cdots y_t q_1) = (y_j \cdots p_j \cdots)(y_i \cdots p_i \cdots)$$

and the proof procedes as before. □

Proof of Theorem 1. Suppose first that R is a UFR. Then each element has a U-decomposition into irreducibles and this becomes a U-decomposition of neo-irreducibles with respect to $1 : R \to R$. Therefore UFR1 is satisfied. Since pairs of associate elements are clearly $ass(R)$ it immediately follows that UFR2 is satisfied, and hence R is a UFR w.r.t $1 : R \to R$. For the converse suppose R is a UFR w.r.t $1 : R \to R$, then a U-decomposition of neo-irreducibles becomes a U decomposition of irreducibles and UFR1 follows. Finally, suppose an element has two U-decompositions of irreducibles.

$$(p'_1 \cdots p'_k)(p_1 \cdots p_n) = (q'_1 \cdots q'_\ell)(q_1 \cdots q_m).$$

Then these become U-decompositions of neo-irreducibles and any pair of elements which are $ass(R)$ must also be associate. Thus UFR2 holds and R is a UFR. □

4. Examples

We may illustrate these ideas by considering subrings of Z, and by answering the question whether nZ is a UFR w.r.t $\theta : nZ \to nZ \times \mathbf{Z}$. We consider first the case where n is prime. For convenience the term 'prime' will encompass the negative prime numbers.

Proposition 3. *Let p be prime in $\mathbf{Z}$, then the neo-irreducible of $p\mathbf{Z} \times \mathbf{Z}$ are as follows.*

(i) $(-\rho \pm 1, \rho)$, *where ρ is prime in $\mathbf{Z}$ and* $\rho \equiv \pm 1 (\mathrm{mod} p)$.

(ii) $(\rho \mp 1, \pm 1)$, *where ρ is prime in $\mathbf{Z}$ and* $\rho \equiv \pm 1 (\mathrm{mod} p)$;

(iii) $(\rho - \tau, \tau)$, *where ρ, τ are prime in $\mathbf{Z}$ and* $\sigma \not\equiv \pm 1 (\mathrm{mod} p)$, $\sigma \equiv \tau (\mathrm{mod} p)$;

(iv) $(0, \pm p), (\pm p, 0), (\pm 2p, \mp p)$;

(v) $(\pm p, \mp p)$.

The proof of this proposition is long but trivial and so it is omitted. From it, however, we can see that $p\mathbf{Z}$ is a UFR w.r.t θ: $p\mathbf{Z} \to p\mathbf{Z} \times \mathbf{Z}$. We note in passing that the only neo-irreducibles we need from the above list to factor elements of $\theta(p\mathbf{Z})$ are $(\rho \mp 1, \pm 1), (0, \sigma)$ *and* $(\pm p, 0)$. *For let* $pr = p^k r_1 \cdots r_1 s_1 \cdots s_m$ *be a prime factorisation where* $r_i \equiv \pm 1 (\mathrm{mod} p)$ *and* $s_\gamma \not\equiv \pm 1 (\mathrm{mod} p)$. *Then*

$$(pr, 0) = (p, 0)^k \ (r_1 \mp 1, \pm 1) \cdots (r_\ell \mp 1, \pm 1)(0, s_1) \cdots (0, s_m).$$

Proposition 4. *Let p be prime in $\mathbf{Z}$. Then $p\mathbf{Z}$ is a UFR w.r.t $\theta : p\mathbf{Z} \to p\mathbf{Z} \times \mathbf{Z}$ where $\theta(pr) = (pr, 0)$.*

Proof. We have seen how to obtain a neo-irreducible decomposition of $\theta(pr)$. To prove uniqueness, we first see that the only neo-irreducibles in $U(pr,0)$, with $r \neq 0$, are the set $\{(-\rho \pm 1, \rho)\}$. Then if

$$((-\rho \pm 1, \rho)\cdots)((\rho_1 \mp 1, \pm 1)\cdots \\ (\rho_h \mp 1, \pm 1)(\sigma_1 - \tau_1, \tau_1)\cdots(\sigma_k - \tau_k, \tau_k)\cdots(0, \pm p)^\ell(\pm p, 0)^m(\pm 2, \mp p)^n)$$

is a U-decomposition of $(pr, 0)$ we have

$$pr = \rho_1 \cdots \rho_h \sigma_1 \cdots \sigma_k (\pm p)^\ell (\pm p)^m (\pm p)^n,$$

where $\rho_i \equiv \pm 1(\bmod p)$ and $\sigma_i \not\equiv \pm 1(\bmod p)$. So h and k are unique, and so is $\ell+m+n$. Therefore we have UFR2 satisfied since the neo-irreducibles in the separate sections (ii), (iii) and (iv) of Proposition 3, corresponding to h, k and $\ell + m + n$, are all $ass(\theta(p\ \mathbf{Z}))$. In the case of $r = 0$, then $(0,0)$ has always a U-decomposition as:

$$(0,0) = (\text{some irreducibles of finite number })((\pm p, \mp p)(\pm p, 0)).$$

Clearly, in $\{(\pm p, \mp p)(\pm p, 0)\}$ every pair of elements of form $(\pm p, \mp p)$ and every pair elements of form $(\pm p, 0)$ are $ass(\theta(p\mathbf{Z}))$ respectively. So $p\mathbf{Z}$ is a UFR w.r.t $\theta : p\mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}$. □

On the other hand, this result does not hold for a non-prime integer.

Proposition 5. *Suppose that n is non-unit and non-prime in $\mathbf{Z}$. Then $n\mathbf{Z}$ is not a UFR w.r.t $\theta : n\mathbf{Z} \to n\mathbf{Z} \times \mathbf{Z}$ where $\theta(nr) = (nr, 0)$.*

Proof. The element $\theta(n) = (n, 0)$ is not a unit. Neither is it a neo-irreducible since if $n = n_1 n_2$ where $1 < n_1,\ n_2 < n$, we have $(y,0)(n,0) = (y,0)(0,n_1)(0,n_2)$, but $(y,0)(n,0)$ does not divide $(y,0)(0,n_1)$ or $(y,0)(0,n_2)$. And any factorisation of $(n,0)$ must include $(\pm n, 0)$. So UFR1 does not hold, and $n\mathbf{Z}$ is not a UFR w.r.t $\theta : n\mathbf{Z} \to n\mathbf{Z} \times \mathbf{Z}$. □

As an example, 2 $\mathbf{Z}$, 3 $\mathbf{Z}$ and 5 $\mathbf{Z}$ are UFRs w.r.t. the mapping given in Proposition 4. The element 120 is a member of each of these rings and we have the following three neo-irreducible decompositions of the image of 120.

$$\begin{aligned}(120,0) &= (2,0)(2,0)(2,0)(4,-1)(6,-1) \text{ in } 2\mathbf{Z} \times \mathbf{Z},\\ &= (3,0)(3,-1)(3,-1)(3,-1)(6,-1) \text{ in } 3\mathbf{Z} \times \mathbf{Z},\\ &= (5,0)(5,-3)(5,-3)(5,-3)(5,-2) \text{ in } 5\mathbf{Z} \times \mathbf{Z}.\end{aligned}$$

5. Direct Sums and Direct Summands

We show finally that the operation of talking direct sums and direct summands sends UFRs to UFRs. This generalises the result for crw1s. The following proposition is easily proved.

Proposition 6. *Let R' and S' be crw1s. Then (r,s) is a neo-irreducible in $R' \oplus S'$ if and only if r is a neo-irreducible in R' and s is a unit in S', or r is a unit in R' and s is a neo-irreducible in S'.*

The main theorems follow from this.

Theorem 7. *Let R and S be UFRs w.r.t $\theta_1 : R \to R'$ and $\theta_1 : S \to S'$ respectively. Then $R \oplus S$ is a UFR w.r.t $\theta : R \oplus S \to R' \oplus S'$ given by $\theta(r,s) = (\theta_1(r), \theta_2(s))$.*

Proof. θ is a monomorphism and $\theta(R \oplus S)$ is an ideal of $R' \oplus S'$. Given $(r,s) \in R \oplus S$ we have neo-irreducible decompositions

$$\theta_1(r) = r_1 \cdots r_k \quad \text{and} \quad \theta_2(s) = s_1 \cdots s_n.$$

Hence $(r,s) = (r_1,1) \cdots (r_k,1)(1,s_1) \cdots (1,s_n)$ and UFR1 is satisfied.

Suppose now (r,s) has the two U-decompositions

$$\begin{aligned}&((r_1', s_1') \cdots (r_k', s_k'))((r_1, s_1) \cdots (r_m, s_m)) \\ &\quad = ((a_1', t_1') \cdots (a_\ell', t_1') \cdots (a_\ell', t_\ell'))((a_1, t_1) \cdots (a_n, t_n)).\end{aligned}$$

Then $(r_i', s_i') \in U((r_1, s_1) \in U((r_1, s_1) \cdots (r_m, s_m))$ and it follows that $r_i' \in U(r_1 \cdots r_m)$, $s_i' \in U(s_1 \cdots s_m)$. Also since $(r_j, s_j) \notin U((r_1, s_1) \cdots \widehat{(r_j, s_j)} \cdots (r_m, s_m))$, the previous proposition shows that we have exactly one of $r_j \notin U(r_1 \cdots \hat{r}_j \cdots r_m)$ and $s_j \notin U(s_1 \cdots \hat{s}_j \cdots s_m)$. Suppose $r_j \in U(r_1 \cdots \hat{r}_j \cdots r_m)$ for $j = 1, \ldots, g$ and $r_j \notin U(r_1 \cdots \hat{r}_j \cdots r_m)$ for $j = g+1, \ldots, m$. Then $s_j \notin U(s_1 \cdots \hat{s}_j \cdots s_m), s_j$ is not a unit and r_j is a unit for $j = 1, \ldots, g$. Similarly s_j is a unit for $j = g+1, \ldots, m$. Let $u = r_1 \cdots r_g$ and $v = s_{g+1} \cdots s_m$ then ur_{g+1} is neo-irreducible in R' and $s_g v$ is neo-irreducible in S'. Therefore

$$\theta_1(r) = (r_1' \cdots r_k')(ur_{g+1} \cdots r_m)$$

and

$$\theta_2(s) = (s_1' \cdots s_k')(s_1 \cdots s_g v)$$

are U-decompositions. Similarly, we have the two other U-decompositions

$$\begin{aligned}\theta_1(r) &= (a_1' \cdots a_\ell')(\mu a_{h+1} \cdots a_n) \\ \theta_2(s) &= (t_1' \cdots t_\ell')(t_1 \cdots t_h \gamma),\end{aligned}$$

where $\mu = a_1 \cdots a_h$ and $\gamma = t_{h+1} \cdots t_n$ are units.

Since R and S are UFRs it is immediate that $m-g=n-h$ and $g=h$. Hence $m=n$. Also $r_j \sim_{\theta_1(R)} a_j$ for $j=g+1,\ldots,m$ and $s_j \sim_{\theta_2(S)} t_j$ for $j=1,\ldots,g$. Hence $(r_j,s_j) \sim_{\theta(R\oplus S)} (a_j,t_j)$ for $j=1,\ldots,m$. Then $R\oplus S$ is a UFR w.r.t $\theta : R\oplus S \to R'\oplus S'$. □

There is a similar result for direct summands.

Theorem 8. *Suppose* $R \cong R_1 \oplus \cdots \oplus R_n$ *and* R *is a UFR w.r.t* $\theta : R \to R'$. *Define* $\theta_i : R_i \to R'$ *by* $\theta_i(r_i) = \theta(0,\ldots,r_i,\ldots,0)$. *Then if* $\theta_i(R_i)$ *is an ideal of* R' *it follows that* R_i *is a UFR w.r.t* $\theta_i : R_i \to R_i'$.

References

[1] Ağargün, A.G.: Some factorisation problems in rings, Ph.D. thesis, 1993, University of Wales.

[2] Anderson, D.D. and Valdes-Leon, S.: Factorisation in commutative rings with zero divisors, *Rocky Mountain Journal of Mathematics*, **26** (1996), 439-480.

[3] Fletcher, C.R.: Unique factorization rings, *Proc. Cambridge Philos. Soc.*, **65** (1969), 579-83.

[4] Fletcher, C.R.: The structure of unique factorisation rings, *Proc. Cambridge Philos. Soc.*, **67** (1970), 535-40.

Ahmet Göksel AĞARGÜN
Yıldız Technical University,
Faculty of Art and Sciences,
Department of Mathematics
Şişli, İstanbul-TURKEY

Colin Robert FLETCHER
Department of Mathematics,
University of Wales,
Aberystwyth-UK

Received 04.04.1996