PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

C. R. FLETCHER

Equivalent Conditions for Unique Factorization

Publications du Département de Mathématiques de Lyon, 1971, tome 8, fascicule 1
, p. 13-22
<http://www.numdam.org/item?id=PDML_1971__8_1_13_0>

Publications du
Département de
Mathématiques
Lyon 1971 t. 8-1

EQUIVALENT CONDITIONS FOR UNIQUE FACTORIZATION

by C.R. FLETCHER

University College of Wales, Aberystwyth.

1 - INTRODUCTION.

This paper forms the main part of an address given at the University of Lyon in May 1971. Results on Euclidean rings, which were also stated, will shortly be appearing in the Journal of the London Mathematical Society (see (3)), and will not be repeated here. The terminology used in the sequel was defined in (1) and (2). All rings are commutative and have identity elements.

In (2) we showed that if R is a pseudo-domain having the property that every non-unit element has an irreducible decomposition, then R is a unique factorization ring (UFR) if and only if every irreducible element is prime. This résult we now generalize, and we also consider the generalization of other equivalent conditions from the theory of UFD's.

2 - MAIN RESULT.

THEOREM 1. - *R is a ring in which every non-unit element has an irreducible decomposition. Then R is a UFR if and only if every irreducible is prime.*

PROOF. - One way rond is trivial. For suppose R is a UFR, then from (2), $R \cong R_1 \oplus \cdots \oplus R_n$ where R_i is a UFPD for $i = 1,\ldots,n$. If p is irreducible in R and $p|ab$, then p is of the form $(u_1,\ldots,p_i,\ldots,u_n)$ where p_i is irreducible in R_i and u_j $(j\neq i)$ is a unit in R_j , and $p_i|a_ib_i$ with an obvious notations. The result from (2) mentioned above proves that p_i is prime in R_i , and hence $p_i|a_i$ or $p_i|b_i$. Therefore $p|a$ or $p|b$ and p is prime in R.

To prove the converse we require some further results.

PROPOSITION 2. - *If R is a ring in which every non-unit element has an irreducible decomposition, and if every irreducible element of R is prime, then the factors of the relevant part of each U-decomposition of 0 are unique up to associativity, i.e. if*

$$0 = (\ )(\alpha_1^{m_1}\cdots\alpha_n^{m_n}) = (\ )(\beta_1^{k_1}\cdots\beta_\ell^{k_\ell})$$

where α_i and α_j are not associate for $i\neq j$, and β_r and β_s are not associate for $r\neq s$, then $n = \ell$ and α_i and β_i are associate for $i = 1,\ldots,n$ after a suitable renombering of the β's. (At this stage $m_i \neq k_i$ necessarily).

PROOF. - $\alpha_i | \beta_1^{k_1} \cdots \beta_\ell^{k_\ell}$ and since α_i is irreducible and hence prime we have $\alpha_i | \beta_j$ say. Similarly $\beta_j | \alpha_1^{m_1} \cdots \alpha_n^{m_n}$ and $\beta_j | \alpha_k$ say. Therefore $\alpha_i | \alpha_k$, and either α_i and α_k are associate or $\alpha_i \epsilon U(\alpha_k)$. In both cases we have $i=k$ and α_i and β_j are associate. Thus taking each factor in turn we get α_1 and $\beta_{j_1}, \cdots, \alpha_n$ and β_{j_n} are associate. Now if β_{j_s} are associate, then α_r and α_s are associate and $r=s$. Hense $\beta_{j_1}, \cdots, \beta_{j_n}$ represent distinct associativity classes, and $\ell \geqslant n$. Similarly, starting with the β's we may prove that $n \geqslant \ell$, which implies $n=\ell$. We have also proved that α_i and β_i are associate for $i=1,\ldots,n$ after a suitable renumbering of the β's.

In the sequel $0 = (\ )(\alpha_1^{m_1} \cdots \alpha_n^{m_n})$ will always be a U-decomposition of 0 where α_i is not an associate of α_j for $i \neq j$.

PROPOSITION 3. - *R is a ring in which every non-unit element has an irreducible decomposition and every irreducible element is prime. If* $0 = (\ )(\alpha_1^{m_1} \cdots \alpha_n^{m_n})$ then

(i) $\alpha_i \notin U(\alpha_1^{m_1} \cdots \alpha_i^{d_i} \cdots \alpha_n^{m_n})$ *where* $0 \leqslant d_i < m_i$ *for* $i=1,\ldots,n$.

(ii) $\alpha_i \epsilon U(\alpha_i^{m_i})$ *for* $i=1,\ldots,n$.

PROOF. - *(i)* Immediate.

(ii) Suppose $i=1$ and put $\alpha_1 = \alpha$, $m_1 = m$. If $n=1$ then $0 = (\ )(\alpha^m)$ and $\alpha \epsilon U(\alpha^m)$. If $n>1$ then $0 = \alpha^m(\alpha - (\alpha - \alpha_2^{m_2} \cdots \alpha_n^{m_n}))$. Suppose $\alpha - \alpha_2^{m_2} \cdots \alpha_n^{m_n} = u$ a unit, then $\alpha^{m+1} = \alpha^m u$ and $\alpha \epsilon U(\alpha^m)$.

$\alpha-\alpha_2^{m_2}\cdots\alpha_n^{m_n}$ is a non-unit then it has an irreducible décomposition $d_1\cdots d_g$ and $\alpha^{m+1} = \alpha^m d_1\cdots d_g$. Since d_i is irreducible it is prime and $d_i|\alpha$, $i=1,\ldots,g$. Then either d_i and α are associate or $d_i\in U(\alpha)$. If the former then $\alpha_2^{m_2}\cdots\alpha_n^{m_n} = \alpha-d_1\cdots d_g$ implies that $\alpha|\alpha_j$ for some $j\geqslant 2$, and either α and α_j are associate or $\alpha\in U(\alpha_j)$.

Contradiction from the U-decomposition of 0. Therefore $d_i\in U(\alpha)$ and $d_1\cdots d_g\in U(\alpha)$. Hence $\alpha = d_1\cdots d_g r\alpha$ and $\alpha^m = d_1\cdots d_g r\alpha^m = r\alpha^{m+1}$, which gives $\alpha\in U(\alpha^m)$.

COROLLARY. - 0 has unique factorization.

PROFF. - Suppose $0 = (\ )(\alpha_1^{m_1}\cdots\alpha_n^{m_n}) = (\ )(\beta_1^{k_1}\cdots\beta_\ell^{k_\ell})$ then from Proposition 2, $\ell=n$ and α_i and β_i are associate i.e. $0 = (\ )(\alpha_1^{m_1}\cdots\alpha_n^{m_n}) = (\ )(\alpha_1^{k_1}\cdots\alpha_n^{k_n})$. If for some i $m_i>k_i$, then $\alpha_i\in U(\alpha_1^{m_1}\cdots\alpha_i^{m_i-1}\cdots\alpha_n^{m_n})$ and $\alpha_i\in U(\alpha_i^{k_i})$ from above. But $U(\alpha_1^{m_1}\cdots\alpha_i^{m_i-1}\cdots\alpha_n^{m_n})\supsetneq U(\alpha_i^{k_i})$ and we have a contradiction. Therefore $m_i = k_i$ for $i=1,\ldots,n$.

It is immediate that every zero-divisor irreducible in R has α_i as an associate for some i. Also we see that the U-decomposition of the product $\alpha_1^{d_1}\cdots\alpha_n^{d_n}$ is $(\alpha_1^{x_1}\cdots\alpha_n^{x_n})(\alpha_1^{y_1}\cdots\alpha_n^{y_n})$ where if $d_i\geqslant m_i$ then $x_i = d_i-m_i$ and $y_i = m_i$, and if $d_i<m_i$ then $x_i = 0$ and $y_i = d_i$.

We are now able to complete the proof of our main result.

PROOF of THEOREM 1. - Suppose r is a non-zero element of R with irreducible decompositions:

$$r = p_1\cdots p_k\beta_{11}\cdots\beta_{1k_1}\beta_{21}\cdots\beta_{nk_n} = q_1\cdots q_\ell\gamma_{11}\cdots\gamma_{1\ell_1}\gamma_{21}$$

$\cdots\gamma_{n\ell_n}$, where the p's and q's are regular and where β_{ij} and γ_{ij} are associate to α_i . Substituting we have :

$$r = u_{11}\cdots u_{nk_n} p_1\cdots p_k\alpha_1^{k_1}\cdots\alpha_n^{k_n} = v_{11}\cdots v_{n\ell_n} q_1\cdots q_\ell\alpha_1^{\ell_1}\cdots\alpha_n^{\ell_n}.$$

Let us suppose that $k_1<m_1$. Then if $k_1<\ell_1$ we may multiply through by $\alpha_1^{r_1}\alpha_2^{m_2}\cdots\alpha_n^{m_n}$ where $r_1 = \max(0,m_1-\ell_1)$ to obtain :

$$u_{11}\cdots u_{nk_n} p_1\cdots p_k\alpha_1^{k_1+r_1}\alpha_2^{k_2+m_2}\cdots\alpha_n^{k_n+m_n}$$

$$= v_{11}\cdots v_{n\ell_n} q_1\cdots q_\ell\alpha_1^{\ell_1+r_1}\alpha_2^{\ell_2+m_2}\cdots\alpha_n^{\ell_n+m_n} .$$

The right hand side is zero since $\ell_1+r_1\geqslant m_1$. Therefore

$$\alpha_1^{r_1}\alpha_2^{m_2}\cdots\alpha_n^{m_n}\beta_{11}\cdots\beta_{nk_n} = 0$$

since the p's are regular. Transforming to U-decomposition using Proposition 3 we have

$$(\beta_{21}\cdots\beta_{nk_n})(\beta_{11}\cdots\beta_{1k_1}\alpha_1^{r_1}\alpha_2^{m_2}\cdots\alpha_n^{m_n}) = 0,$$

which implies that $\beta_{11}\cdots\beta_{1k_1}\alpha_1^{r_1}\alpha_2^{m_2}\cdots\alpha_n^{m_n} = 0$ from Proposition 3 of (1). Hence $\alpha_1^{k_1+r_1}\alpha_2^{m_2}\cdots\alpha_n^{m_n} = 0$ which is impossible since $k_1+r_1<m_1$. We have thus proved that in this case $k_1 = \ell_1$. Similarly if $\ell_1<k_1$ we may prove the same result.

Now suppose that $k_1\geqslant m_1$. If $\ell_1<m_1$ the above proof may be repeated with k_1 and ℓ_1 interchanged. Hence we suppose $k_1,\ell_1\geqslant m_1$.

We transform the original irreducible decompositions to U-decompositions using Proposition 3 and noting that in any statement $a \in U(b)$ or its negative, we may replace either element by an associate. Hence in both U-decompositions there will be exactly m_1 elements associate to α_1 in the relevant part. Now considering the elements associate to $\alpha_2, \cdots, \alpha_n$ we see that we have proved the uniqueness of the non-regular factors of r.

Turning to the regular factors, suppose p_1 is in the relevant part. Then $p_1 | r$ and therefore $p_1 | q_1$, or $p_1 | \gamma_{11}$ say. If latter holds then $p_1 \in U(\gamma_{11})$ (Proposition 1 of (2)) and $p_1 \in U(\beta_{11})$. Contradiction. Hence p_1 and q_1 are associate since $p_1 \notin U(q_1)$ = {units}. Now q_1 is also in the relevant part because otherwise $q_1 \in U(\gamma_{11} \cdots \gamma_{n\ell_n})$ which implies $p_1 \in U(\beta_{11} \cdots \beta_{nk_n})$ a contradiction as before. By cancellation we immediately see that the number of associates of p_1 equals the number of associates of q_1 , considering relevant parts only. Arguing in a like manner we prove that all regular factors in the relevant part are unique.

Putting the two results together we have proved that r has unique factorization and therefore R is a UFR.

3 - EQUIVALENT CONDITIONS.

The result in the previous section may lead one to suppose that a complete generalization of the usual equivalent conditions for a UFD is possible, but one is soon disillusioned. However we have the following.

THEOREM 4. - *The following conditions on a ring* R *are equivalent.*

(i) R *is a* UFR.

(ii) R *satisfies the maximum condition for principal ideals, and every irreducible element is prime.*

(iii) *Every non-unit element of* R *has a factorization into primes.*

PROOF. - *(i)* $\Rightarrow$ *(ii)*. - If R is a UFR then every irreducible is prime (Theorem 1). From the structure theorem (2), $R \cong R_1 \oplus \cdots \oplus R_n$ where each R_i is either a UFD or a special PIR. Hence each R_i satisfies the maximum condition on principal ideals, and it is a simple matter to show that R does also.

(ii) $\Rightarrow$ *(iii)*. - Consider the set of principal ideals generated by non-unit elements not having an irreducible decomposition. The existence of the maximum gives the contradiction (see (1) Theorem 7). Then every non-unit has an irreducible decomposition and hence a prime decomposition.

(iii) $\Rightarrow$ *(i)*. - From Theorem 1 it is sufficient to prove that every irreducible element is prime. So suppose q is irreducible and $q = p_1 \cdots p_n$ where each p_i is prime. Then $q | p_i$ for some i, and q and p_i are associate. Therefore q is prime.

The next result gives conditions that are necessary but not sufficient.

THEOREM 5. - *If* R *is a* UFR *then the following conditions hold.*

(*i*) R *satisfies the maximum condition for principal ideals, and the intersection of any two principal ideals is principal* (*i.e. any two elements have an* l.c.m.).

(*ii*) R *satisfies the maximum condition for principal ideals, and the set of principal ideals containing any two principal ideals has a unique minimum* (*i.e. anay two elements have a* g.c.d.).

(*iii*) *Every non-zero prime ideal* ($\neq$R) *of* R *contains a non-zero principal prime ideal.*

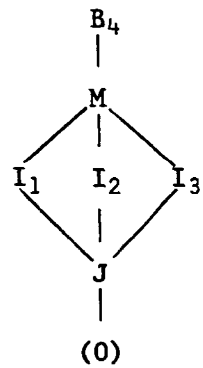
PROOF. - $R \cong R_1 \oplus \cdots \oplus R_n$ where each R_i is either a UFD or a special PIR. Hence conditions (*i*) and (*ii*) are satisfied for each R_i, and therefore also for R. Now suppose P is a prime ideal and $P \neq (0)$, R. Then there exists a non-zero, non-unit r P which has a prime decomposition $p_1 \cdots p_m$ from Theorem 4. Thus $(p_j) \subseteq P$ for some j.

To prove that no part of Theorem 5 has a converse we need two couter-examples. Both are constructed from the familiar example $Z[\sqrt{-3}]$ is domain theory. First consider $B_4 = \{(m,n) | m,n \in Z_4\}$ where

$$(m_1,n_1)+(m_2,n_2) = (m_1+m_2,n_1+n_2)$$

and $$(m_1,n_1)\cdot(m_2,n_2) = (m_1m_2+n_1n_2,m_1n_2+n_1m_2).$$

Then (i) and (ii) are satisfied since in pictorial form the ideals are



where $J = (2,2)B_4$, $I_1 = (2,0)B_4 = (0,2)B_4$, $I_2 = (1,3)B_4 = (3,1)B_4$, $I_3 = (3,3)B_4 = (1,1)B_4$, and M is the unique maximal ideal consisting of all non-units. However (2,0) is irreducible but not prime, since $(1,1)(1,1)\in I_1$. Therefore from Theorem 1 B_4 is not a UFR. We remark in passing that it is still an open question whether strengthening the hypothèses, so that the sum of principal ideals is principal, will ensure that the ring is a UFR.

The second counter-example is $R = B\oplus Z_4$ where $B = Z[\sqrt{-3}]$. R is not a UFR since B is not a UFD (see (2) Theorem 10). The prime elements of R are of the form (p,v) and (u,q) where p,q are prime and u,v are units in B and Z_4 respectively. 0 is prime in B and 2 is the only prime in Z_4. Suppose P ($\neq$ (0),R) is a prime ideal of R. Then not all elements of P are of the form (b,0) since $(0,2)(0,2)\in P$. If P has an element of the form (b,3) then $(b,3)(1,3) = (b,1)\in P$ and $(0,1)R\subseteq P$. Finally suppose $(b,2)\in P$.

Then $(b,2)(1,2) = (b,0) = (b,1)(1,0) \in P$. The case $(b,1) \in P$ has been dealt with. Suppose $(1,0) \in P$. Now $(b,2)(0,1) = (0,2) \in P$ and therefore $(1,0)+(0,2) = (1,2) \in P$. Hence $(1,2)R \subseteq P$. We have proved that every non-zero prime ideal of R contains a non-zero principal prime ideal.

It is perhaps surprising to find that a ring satisfying the maximum condition for principal ideals and having the additional property that every irreducible is prime is a UFR, whereas one with the additional property that every pair of elements has a g.c.d. is not a UFR in general. In the domain case of course the g.c.d. property implies that every irreducible is prime.

REFERENCES :

[1] FLETCHER, C.R. *Unique factorization rings*. Proc. Cambridge Philos. Soc. 65 (1969), 579-583.

[2] FLETCHER, C.R. *The structure of unique factorization rings*. Proc. Cambridge Philos. Soc. 67 (1970), 535-540.

[3] FLETCHER, C.R. *Euclidean rings*. J. London Math. Soc. (to appear).

Manuscrit rècu le24 juin 1971