BULLETIN *of the*
MALAYSIAN
MATHEMATICAL
SCIENCES
SOCIETY

Bull. Malaysian Math. Sc. Soc. (Second Series) **27** (2004) 87–90

An Addendum to the Paper "Arithmetic Functions Over Rings with Zero Divisors", Bull. Malaysian Math. Sc. Soc. 24 (2001), 81–91

[1]WŁADYSŁAW NARKIEWICZ ,[2]PATTIRA RUENGSINSUB AND [2]VICHIAN LAOHAKOSOL
[1]Institute of Mathematics, Wrocław University, Wrocław, Poland
[2]Department of Mathematics, Kasetsart University, Bangkok 10900, Thailand
[1]e-mail: narkiew@math.uni.wroc.pl and [2]e-mail: fscipar@ku.ac.th, fscivil@ku.ac.th

2000 Mathematics Subject Classification: 13F15, 11A25.

A commutative ring *R*, with unity and zero divisors, is a unique factorization ring, UFR for short, if for every non-zero non-unit $r \in R$, there exist irreducible elements $r_1, \cdots, r_n$ such that $r = r_1 \cdots r_n$ and whenever $r = r_1 \cdots r_n = s_1 \cdots s_m$ (where $r_1, \cdots, r_n, s_1, \cdots, s_m$ are irreducibles), then $n = m$ and the s_j can be renumbered so that r_i is associated to $s_i (i = 1, \cdots, n)$. Denote the set of arithmetic functions over a ring *R* by A_R, i.e. $A_R = \{f : \mathbb{N} \to R\}$, and let $R_\omega = R[[x_1, x_2, \cdots]]$ and $R_m = R[[x_1, \cdots, x_m]]$ be the rings of formal power series in $\mathbb{N}_0$, respectively, m indeterminates. It is well-known that A_R and R_ω are isomorphic.

All UFR's considered here throughout are assumed to have nonempty sets of zero divisors.

In the cited paper, several results have been proved based on the hypothesis that "R_j is a UFR". As observed by the first author, this hypothesis is void, as we now prove.

Lemma 1. *If R is a UFR , then every non-zero element of R is either a unit or a zero divisor.*

Proof. Since R is a UFR, then by Theorem 1 of [2], *R* satisfies the weak cancellation law, i.e., if $ab = ac \neq 0$, then b and c differ by a unit factor. We first show that every zero divisor in *R* is divisible by every element of *R* which is not a zero divisor. Let $a \neq 0$ be an arbitrary zero divisor in *R*. Then there exists $0 \neq b \in R$ such that $ab = 0$. Let c be an arbitrary element of R which is not a zero divisor. Then $(c - a)b = cb \neq 0$, so $c - a = uc$ for some unit $u \in R - \{1\}$. Thus $a = (1 - u)c$, so a is divisible by c. Next we prove that every irreducible element in R is a zero divisor. Suppose r is an irreducible element in R which is not a zero divisor. Then r would divide every zero divisor and this implies that every zero divisor is reducible. Since the set of non-zero divisors is closed under multiplication, this implies that R does not have zero divisors. This contradiction implies that no such element r exists in R.

Since any non-zero multiple of a zero divisor is again a zero divisor, we obtain that every non-zero element of a UFR is either a unit or a zero divisor, as asserted.

An alternative proof of part of this statement can also be found in Galovich [1, Lemma 2].

Corollary. *If R is a UFR, then none of the rings $R_1, R_2, \cdots, R_\omega$ can be a UFR.*

Proof. It suffices to observe that although $R_j\,(j = 1, 2, \cdots, \omega)$ has zero divisors inherited from R, the element x_1 is neither a unit, nor a zero divisor.

Pushing slightly forward the method applied in the proof of Lemma 1 we can obtain an easy elementary proof of the following characterization of UFR's:

Theorem. *If R is a UFR, then either for all irreducible elements $r, s \in R$ we have $rs = 0$, or all irreducible elements of R are associated, and thus every non-zero element of R is of the form ur^n, where u is invertible, r is a fixed irreducible and $n = 0, 1, \cdots, k - 1$ with a fixed integer k. Moreover, $r^k = 0$.*

We need two simple lemmas:

Lemma 2. *If R is a UFR then either for all irreducibles r, s we have $rs \neq 0$ or for all irreducibles r, s we have $rs = 0$.*

Proof. If the assertion is false, then there are irreducibles r, s, t, u with $rs = 0$ and $tu \neq 0$. Then $r(t + s) = rt$, therefore either $tr = 0$ or $t + s = \alpha t$ with a unit α. In the second case t divides s, hence it must be associated with s, and we get $rt = \beta rs = 0$ for some unit β. So in all cases $tr = 0$. Now $t(u + r) = tu \neq 0$ and thus $u \mid r$, showing that r and u are associated, i.e. $u = \gamma r$ with a unit γ, but this forces $tu = \gamma tr = 0$, contrary to our assumption.

Lemma 3. *If R is a UFR and there exist in R irreducibles with non-zero product, then the following holds:*

(i) *If $Z(a) = \{b \neq 0 : ab = 0\}$ and r, s are irreducibles, then $Z(r) = Z(s)$.*

(ii) *Irreducible elements are uniformly nilpotent, i.e., for some $k > 0$ one has $r^k = 0$ for each irreducible r.*

Proof.
(i) Let $br = 0, b \neq 0$ and assume $bs \neq 0$. Then we have $b(r+s) = bs \neq 0$, hence s divides r and we see that r and s are associated and therefore $bs = 0$, contrary to our assumption.
(ii) Let r be irreducible. Choose $a \in Z(r)$ and let b a non-unit with $br \neq 0$. Such b exists, since our assumption and Lemma 2 imply $r^2 \neq 0$. Now $r(a+b) = br \neq 0$ and this leads to $b \mid a$. Therefore , the set of non-associated elements b lying outside $Z(r)$ is finite. Let the complement of $Z(r)$ be $\{b_1, \cdots, b_m\}$ and put $N = \max_j \Omega(b_j)$, where $\Omega(x)$ denotes the number of irreducible factors counted with multiplicity of $x \in R$. Note that $Z(r)$ and its complement do not depend on r in view of (i). Finally we obtain $r^{N+1} \in Z(r)$, thus $r^{N+2} = 0$, and we may take $k = N + 2 \geq 2$.

Modifying the proof of (ii) by separating the cases $r^2 = 0$ and $r^2 \neq 0$, Lemma 3 remains valid without the non-zero product of irreducibles condition. Yet to prove our main Theorem, Lemma 3 suffices.

Proof of Theorem. If there are irreducible elements with non-zero product, then by Lemma 2 every pair of irreducibles has a non-zero product. Now choose k occuring in Lemma 3 (ii) and let r, s be non-associated irreducibles. Then $r^{k-1} \neq 0$, $r^k = 0$, and so

$$(s + r^{k-1})r = sr \neq 0.$$

Hence $s \mid r^{k-1}$, i.e. $s \mid r$ and we see that s and r are associated.

Observe that both situations can occur: the first arises when R is the ring of residue classes mod 4, where 2 is the only irreducible, and we have $2 \cdot 2 = 0$, and for the second case consider any ring of residue classes mod p^n, where p is a prime and $n \geq 2$, with the exception of the case $p = n = 2$. Here every irreducible is of the form αp (with p not dividing α), thus is associated with p.

References

1. S. Galovich, Unique factorization rings with zero divisors, *Math. Magazine* **51** (1978), 276–283.
2. R. Ruangsinsap, V. Laohakosol, and P. Udomkavanich, Arithmetic functions over rings with zero divisors, *Bull. Malaysian Math. Sc. Soc*. **24** (2001), 81–91.