Mathematical Forum
Vol.XVIII, 2005-2006

FACTORIZATION IN Γ- INTEGRAL DOMAINS

By
*Md. Sabur Uddin and **A. C. Paul
* Department of Mathematics,
Carmichacl College, Rangpur Bangladesh.
**Department of Mathematics, University of Rajshahi,
Rajshahi-6205, Bangladesh.

Abstract

In this paper we work on factorization in Γ-integral domains, factorization in Γ-unique factorization domains and factorization in Γ-principal ideal domains. We have developed some characterizations of these above domains.

1. Introduction

V. Sahai and V. Bist [6] worked on factorization in integral domains. They have developed some characterizations. Haram Paley and Paul M. Weichsel [5] characterized factorization in unique factorization domains and principal ideal domains.

In this paper we generalize the above mentioned works in gamma rings due to Barnes [1]. The main theorems we have proved are the following : A non-unit element a of a Γ-PID has a factorization into primes and every Γ-PID is a Γ-UFD. Some other characterizations are studied in this note.

2. Preliminaries.

2.1 Definitions

Gamma Ring : Let M and Γ be two additive abelian groups. Suppose that there is a mapping from $M\times \Gamma \times M \to M$ (sending (x, α, y) into $x\alpha y$) such that

(i) $$(x+y)\alpha z = x\alpha z + y\alpha z$$
$$x(\alpha+\beta)z = x\alpha z + x\beta z$$
$$x\alpha(y+z) = x\alpha y + x\alpha z$$

(ii) $$(x\alpha y)\beta z = x\alpha(y\beta z),$$

where $x, y, z \in M$ and $\alpha, \beta \in \Gamma$. Then M is called a Γ-ring. This definition is due to Barnes [1].

Ideal of Γ-rings : A subset A of the Γ-ring M is a left (right) ideal of M if A is an additive subgroup of M and $M\Gamma A = \{c\alpha a \mid c \in M, \alpha \in \Gamma, a \in A\}(A\Gamma M)$ is contained in A. If A is both a left and a right ideal of M, then we say that A is an ideal or two-sided ideal of M.

If A and B are both left (respectively right or two-sided) ideals of M, then $A+B = \{a+b \mid a \in A, b \in B\}$ is clearly a left (respectively right or two-sided) ideal, called the sum of A and B. We can say every finite sum of left (respectively right or two-sided) ideal of a Γ-ring is also a left (respectively right or two-sided) ideal.

It is clear that the intersection of any number of left (respectively right or two sided) ideal of M is also a left (resprectively right or two-sided) ideal of M.

If A is a left ideal of M, B is a right ideal of M and S is any non-empty subset of M, then the set, $A\Gamma S = \left\{\sum_{i=1}^{n} a_i \gamma s_i \mid a_i \in A, \gamma \in \Gamma, s_i \in S, n \text{ is a positive integer}\right\}$ is a left ideal of M and $S\Gamma B$ is a right ideal of M. $A\Gamma B$ is a two-sided ideal of M.

If $a \in M$, then the principal ideal generated by a denoted by $\langle a \rangle$ is the intersection of all ideals containing a and is the set of all finite sum of elements of the form $na + x\alpha a + a\beta y + u\gamma a\mu v$, where n is an integer x, y, u, v are elements of M and $\alpha, \beta, \gamma, \mu$ are elements of Γ. This is the smallest ideal generated by a. Let $a \in M$. The smallest left (right) ideal generated by a is called the principal left (right) ideal $\langle a | (| a \rangle)$.

Identity element of a Γ-ring : Let M be a Γ-ring. M is called a Γ-ring with identity if there exists an element $e \in M$ such that

$$a\gamma e = e\gamma a = a \text{ for all } a \in M \text{ and some } \gamma \in \Gamma.$$

We shall frequently denote e by 1 and when M is a Γ-ring with identity, we shall often write $1 \in M$. Note that not all Γ-rings have an identity. When a Γ-ring has an identity, then the identity is unique.

Commutative Γ-ring : Let M be a Γ-ring. M is called a commutative Γ-ring if $a\gamma b = b\gamma a$ for all $a, b \in M$ and $\gamma \in \Gamma$.

Zero Divisor : Let M be a Γ-ring. An element $a \neq 0$ in M is called a left zero divisor if there exists an element $b \neq 0$ in M such that $a\gamma b = 0$ for some $\gamma \in \Gamma$. Similarly, an element $b \neq 0$ in M is called a right zero divisor if there exists an element $a \neq 0$ in M such that $a\gamma b = 0$ for some $\gamma \in \Gamma$. A zero divisor is an element that is either a left or a right zero divisor. If M is a commutative Γ-ring, then the concepts of left and right zero divisor coincide.

Γ-integral domain : Let M be a commutative Γ-ring such that $1 \in M$. If M has no zero divisors, then we call M a Γ-integral domain.

Principal ideal : An ideal A of a Γ-integral domain M is called a principal ideal of M if A is generated by a single element $a \in M$, that is, $A = a\gamma M$ for all $\gamma \in \Gamma$.

Γ-Principal ideal domain : A Γ-ring M is called a Γ-principal ideal domain (Γ-PID for short) if M is Γ-integral domain and every ideal of M is a principal ideal.

Prime ideal : Let M be a commutative Γ-ring. An ideal K in M is called a prime ideal if whenever $a\gamma b\in K$, $a\in M$, $b\in M$ and some $\gamma\in\Gamma$, then either $a\in K$ or $b\in K$.

Maximal ideal : An ideal R in a Γ-ring M is called a maximal ideal in M if (i) $R\subset M$ and (ii) whenever L is an ideal in M such that $R\subseteq L\subseteq M$, then either $L = R$ or $L = M$.

Division gamma ring : Let M be a Γ-ring. Then M is called a division Γ-ring if it has an identity element and its only non-zero ideal is itself. A commutative division Γ-ring is called a Γ-field.

Multiplicatively closed sub set of a Γ-ring : A non empty sub set S of a Γ-ring M is said to be multiplicatively closed if $x\gamma y\in S$ whenever x, $y\in S$ and some $\gamma\in\Gamma$.

We need the following three Theorems due to V. Sahai and V. Bist [6] in ring theory. We modify these theorems in gamma rings which are needed to our next works.

2.2 Theorem : Let M be a commutative Γ-ring with identity and let A be an ideal of M. If S is a multiplicatively closed subset of M with $A\cap S$ is empty, then the family F of all ideals B of M which contain A and $B\cap S$ is empty possesses a maximal element; and such a maximal element is a prime ideal of M.

2.3 Theorem : Let M be a commutative Γ-ring with identity. An ideal K of M is prime if and only if M/K is a Γ-integral domain.

2.4 Theorem : Let M be a commutative Γ-ring with identity. Let K be maximal ideal in M. Then K is a prime ideal.

The proof of the above three theorems are similar to that of the ring theories.

3. Some Factorization in Γ-integral Domains

3.1 Definition : Let M be a Γ-integral domain. If m and s are elements of M, then we say m divides s (in symbols $m|s$) if there exists an element $t\in M$ such that $s = m\gamma t$ for some $\gamma\in\Gamma$. In this case m is called a factor or a divisor of s.

3.2 Definition : Let M be a Γ-integral domain. An element $a \in M$ is called a **unit** in M if there exists $b \in M$ such that $a\gamma b = 1$ for some $\gamma \in \Gamma$.

3.3 Definition : Let M be a Γ-integral domain. Non-zero elements a and b are called **associates** if $a|b$ and $b|a$. Note that $1|m$ for every m in M. Also, if u is a unit in M, then u and 1 are associates.

3.4 Theorem : Let a and b non-zero elements in a Γ-integral domain. Then

(i) a divides b if and only if $\langle b \rangle \subseteq \langle a \rangle$

(ii) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$

(iii) a is a unit in M if and only if $\langle a \rangle = M$.

Proof: (i) If $a|b$, then $b = a\gamma x$ for some $x \in M$ and $\gamma \in \Gamma$. Thus $b \in \langle a \rangle$ and so $\langle b \rangle \subseteq \langle a \rangle$. Conversely, if $\langle b \rangle \subseteq \langle a \rangle$, then $b \in \langle a \rangle$ and so $b = a\gamma x$ for some $x \in M$ and $\gamma \in \Gamma$, that is, $a|b$.

(ii) follows easily from the definition **3.3** and (i)

(iii) follows from (ii) as a and 1 are associates and $\langle a \rangle = M$.

3.5 Theorem : Let a and b be non-zero elements in a Γ-integral domain M. Then a and b are associates if and only if there exist a unit u in M such that $b = a\gamma u$ for some $\gamma \in \Gamma$.

Proof : Suppose that a and b are associates. Then $a|b$ and $b|a$, there exist u, v in M such that $b = a\gamma u$ and $a = b\gamma v$ for some $\gamma \in \Gamma$. Now,

$$\begin{aligned} a &= b\gamma v \\ &= (a\gamma u)\gamma v \\ &= a\gamma(u\gamma v) \end{aligned}$$

So, $a - a\gamma(u\gamma v) = 0$.

Thus $a\gamma(1 - u\gamma v) = 0$.

This implies that $1\text{-}u\gamma v = 0$, since $a \neq 0$. Hence $u\gamma v = 1$. Therefore u is a unit.

Conversely, let $b = a\gamma u$ for some $\gamma \in \Gamma$, where u is a unit in M. Then we have $a|b$.

Therefore,

$$b\gamma u^{-1} = (a\gamma u)\gamma u^{-1}$$

$$\Rightarrow b\gamma u^{-1} = a\gamma(u\gamma u^{-1})$$

$$\Rightarrow b\gamma u^{-1} = a\gamma 1$$

$\Rightarrow b\gamma u^{-1} = a$. Hence $a = b\gamma u^{-1}$.Thus $b|a$. Hence a and b are associates. Thus the theorem is proved.

3.6 Definition : Let M be a Γ-integral domain.

(i) An element a of M is irreducible if a is a non-zero, non-unit element and if $a = x\gamma y$ for some $\gamma \in \Gamma$, then either x or y is unit.

(ii) An element k of M is prime if k is a non-zero, non-unit element and if $k|x\gamma y$ for some $\gamma \in \Gamma$, then $k|x$ or $k|y$.

It follows immediately from the above definition that every associate of a prime (respectively irreducible) element is also prime (respectively irreducible).

3.7 Theorem : Let k be a non-zero element of a Γ-integral domain M. Then k is a prime if and only if $\langle k \rangle$ is prime ideal.

Proof : Let k be prime, then k is a non-zero non-unit. So $\langle k \rangle \neq 0$ and $\langle k \rangle \neq M$. If $x,y \in M$ such that $x\gamma y \in \langle k \rangle$ for some $\gamma \in \Gamma$, then $k|x\gamma y$ and so $k|x$ or $k|y$. Thus $x \in \langle k \rangle$ or $y \in \langle k \rangle$. Therefore $\langle k \rangle$ is a prime ideal.

Conversely, let $\langle k\rangle$ be a prime ideal, since $k \neq 0$ and $\langle k\rangle \neq M$, so k is not a unit. If $k|x\gamma y$ for some $\gamma \in \Gamma$, then $x\gamma y \in \langle k\rangle$ and so $x \in \langle k\rangle$ or $y \in \langle k\rangle$. Hence $k|x$ or $k|y$. Therefore k is a prime element of M. Thus the theorem is proved.

3.8 Theorem : Let M be a Γ-integral domain.

(i) If k is a prime element of M and $k|(a_1\gamma a_2\gamma \ldots\gamma a_t)$ for some $\gamma \in \Gamma$, then $k|a_r$ for some index r.

(ii) Every prime element is irreducible.

(iii) If $k_1\gamma k_2\gamma \ldots\gamma k_s = q_1\gamma q_2\gamma \ldots\gamma q_t$ for some $\gamma \in \Gamma$, where elements k_i and q_j are primes, then s = t. Further, there exists a permutation $\sigma \in S_t$ such that k_i and $q_{\sigma(i)}$ are associates. This means that the decomposition into primes is unique upto rearrangement of factors or multiplication of factors by units.

Proof : (i) By induction on t. The case $t = 2$ is trivial. Now $k|(a_1\gamma a_2\gamma \ldots\gamma a_{t-1})\gamma a_t$ implies that $k|(a_1\gamma a_2\gamma \ldots\gamma a_{t-1})$ or $k|a_t$. If $k|a_t$, then we have proved the statement; other wise $k|a_1\gamma a_2\gamma \ldots\gamma a_{t-1}$ and so by induction hypothesis $k|a_r$ for some r = 1, 2, . . ., t-1.

(ii) Let $k \in M$ be a prime. If $k = a\gamma b$ for some $\gamma \in \Gamma$, then $k|a$ or $k|b$. Without any loss we can assume that $k|b$. Then $b = k\gamma x$ for some $x \in M$. Therefore,

$$a\gamma b = a\gamma k\gamma x$$
$$\Rightarrow k = a\gamma k\gamma x$$
$$\Rightarrow k - a\gamma k\gamma x = 0$$
$$\Rightarrow k - k\gamma a\gamma x = 0, \text{ since M is commutative}$$
$$\Rightarrow k\gamma(1 - a\gamma x) = 0$$

$\Rightarrow 1 - a\gamma x = 0$, since $k \neq 0$.Thus $a\gamma x = 1$. Hence a is a unit. Thus k is irreducible.

(iii) Without any loss we can assume that $s \leq t$. Suppose first that $s < t$. Then $k_1\gamma k_2\gamma \ldots \gamma k_s = q_1\gamma q_2\gamma \ldots \gamma q_t$ for some $\gamma \in \Gamma$ with $s < t$. Since each k_i divides $q_1\gamma q_2\gamma \ldots \gamma q_t$ by (i) there exists q_{r_1} such that $k_i | q_{r_1}$ and so $q_{r_1} = k_i\gamma x_i$ for some $x_i \in M$ and $\gamma \in \Gamma$. Therefore

$$k_1\gamma\, k_2\gamma \ldots \gamma\, k_s = (k_1\gamma\, k_2\gamma \ldots \gamma\, k_s)\gamma\, (x_1\gamma\, x_2\gamma \ldots \gamma\, x_s)\gamma q'$$

where q' is product of remaining primes from $\{q_1, q_2, \ldots, q_t\}$. But then it implies that $(x_1\gamma\, x_2\gamma \ldots \gamma\, x_s)\gamma\, q' = 1$, that is, q' is a unit. This is a contradiction. Hence $s = t$.

Now we prove by iduction on t that if $k_1\gamma k_2\gamma \ldots \gamma\, k_t = q_1\gamma q_2\gamma \ldots \gamma q_t$, then there exists $\sigma \in S_t$ so that k_i and $q_{\sigma(i)}$ are associates. If $t = 1$, then the hypothesis is clearly true. Suppose that the hypothesis is true for all $r < t$. Now if $k_1\gamma k_2\gamma \ldots \gamma k_t = q_1\gamma q_2\gamma \ldots \gamma q_t$, then $k_t | q_1\gamma q_2\gamma \ldots \gamma q_t$. Thus $k_t | q_h$ for some index h and so $q_h = u\gamma k_t$ for some $u \in M$. Since q_h is prime and so irreducible, u is a unit in M. Therefore q_h and k_t are associates. Now

$$k_1\gamma k_2\gamma \ldots \gamma k_{t-1}\gamma k_t = q_1\gamma q_2\gamma \ldots \gamma q_{h-1}\gamma\, q_h\gamma\, q_{h+1}\gamma \ldots \gamma q_t$$

$$\Rightarrow k_1\gamma k_2\gamma \ldots \gamma k_{t-1}\gamma k_t = q_1\gamma q_2\gamma \ldots \gamma q_{h-1}\gamma\, (u\gamma k_t)\gamma\, q_{h+1}\gamma \ldots \gamma q_t$$

$$\Rightarrow k_1\gamma k_2\gamma \ldots \gamma k_{t-1}\gamma k_t = u\gamma q_1\gamma q_2\gamma \ldots \gamma q_{h-1}\gamma k_t\gamma q_{h+1}\gamma \ldots \gamma q_t,$$

since M is commutative. Dividing by k_t on both sides, we get.

$$k_1\gamma\, k_2\gamma \ldots \gamma\, k_{t-1} = u\gamma q_1\gamma q_2\gamma \ldots \gamma\, q_{h-1}\, \gamma\, q_{h+1}\gamma \ldots \gamma q_t$$

By induction hypothesis, there exists a one-one and onto mapping σ from $\{1, 2, \ldots, t\}$ to $\{1, 2, \ldots h-1, h+1, \ldots, t\}$ such that k_i and $q_{\sigma(i)}$ are associates. Now define $\sigma(t) = h$, to obtain the claim. Thus the theorem is proved.

3.9 Theorem : Let k be a prime in a Γ-integral domain. If q is an associate of k, then q is a prime.

The proof is obvious.

4. Factorization in Γ-Unique Factorization domains

4.1 Definition : A Γ-integral domain M is a Γ-unique factorization domain (Γ-UFD) if it satisfies followin conditions :

(i) every non-zero, non-unit element a of M can be written as $a = k_1\gamma k_2\gamma \ldots \gamma k_n$ for some $\gamma \in \Gamma$, where $k_1, k_2, \ldots, k_n$, are irreducible elements in M and

(ii) if $a = k_1\gamma k_2\gamma \ldots \gamma k_n$ and $a = q_1\gamma q_2\gamma \ldots \gamma q_t$ for some $\gamma \in \Gamma$, where $k_1, k_2, \ldots, k_n$, $q_1, q_2, \ldots, q_t$ are irreducibles, then $n = t$ and for some permutation $\sigma \in S_t$ each q_i is an associate of $k_{\sigma(i)}$.

If we define a relation $\sim$ on a Γ-integral domain M by $a \sim b$, if a is an associate of b, then $\sim$ is an equivalence relation. Since a is associate of b if and only if $\langle a \rangle = \langle b \rangle$ (by Theorem **3.4**). Also we have a is an associate of b if and only if $a = u\gamma b$ for some unit u in M and some $\gamma \in \Gamma$ (by Theorem **3.5**). Thus if $\bar{a}$ denotes the equivalence class of a, then $\bar{a} = \{u\gamma b \mid u \text{ is a unit in } M \text{ and some } \gamma \in \Gamma\}$.

Let M be a Γ-UFD. If a is a non-zero non-unit in M, then by part (i) of the above definition we have $a = c_1\gamma c_2\gamma \ldots \gamma c_t$ for some $\gamma \in \Gamma$, where $c_1, c_2, \ldots, c_t$ are irreducibles in M. If we collect all associates of these irreducibles together, then it is easy to see that we can write a as $a = u\gamma(k_1\gamma)^{m1} k_1\gamma(k_2\gamma)^{m2} k_2\gamma \ldots \gamma(k_n\gamma)^{m_n} k_n$, where u is a unit, $k_1, k_2, \ldots, k_n$ are irreducibles such that no two of these are associates. More precisely, $\bar{k}_1, \bar{k}_2, \ldots, \bar{k}_n$ are distinct equivalence classes. Further, part (ii) of the above definition says that these equivalence classes and positive integers $m_1, m_2, \ldots, m_n$ are uniquely determined by a. Thus if also $a = v\gamma(q_1\gamma)^{s1} q_1\gamma(q_2\gamma)^{s2} q_2\gamma \ldots \gamma(q_h\gamma)^{s_h} q_h$ with v, a unit and $\bar{q}_1, \bar{q}_2, \ldots, \bar{q}_h$ distinct equivalence classes, then $h = n$ and for some $\sigma \in S_n$ we have $\bar{k}_i = \bar{q}_{\sigma(i)}$ for all $i = 1, 2, \ldots, n$.

4.2 Theorem : Let M be Γ-UFD. An element a of M is prime if and only if it is irreducible.

Proof : By Theorem **3.8**, if a is a prime element of M, then it is also irreducible.

If 1 is the gcd of A, then we say that the set A is relatively prime. Note that any two gcd's of A are associates. Thus the gcd, if it exists, is well defined up to multiplication by a unit.

4.5 Theorem : Let M be a Γ-UFD and let A be a non-empty subset of $M\backslash\{0\}$. Then there exists a gcd of A.

Proof : Since M is a Γ-UFD, each $a\in A$ can be written in the form $a = u\gamma\left(c_1\gamma\right)^{h_1}c_1\gamma\left(c_2\gamma\right)^{h_2}c_2\gamma\ldots\gamma\left(c_r\right)^{h_r}c_r$ for some $\gamma\in\Gamma$, where u is a unit, $c_1, c_2, \ldots, c_r$ are irreducibles in M with no two of these irreducibles being associates and $h_i \geq 1$ for all $i = 1, 2, \ldots, r$. Define $D(a) = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_r\}$, where $\overline{c}$ is the equivalence class of c with equivalence relation $\sim$ on M defined by $a\sim b$ if and only if a is an associate of b. Clearly $D(a)$ is finite. Observe that $D(a)$ is empty if and only if a is a unit. Let $D = \cap\{D(a) | a \in A\}$. Since each $D(a)$ is finite, so D is a finite set.

If $a' \in A$ is a unit, then a gcd of A is 1. Since if $e \in M$ and $e|a$ for all $a \in A$, then in particular $e|a'$ and so e is a unit. Thus $e|1$.

If all element of A are non-units, then $D(a)$ is non-empty for all $a\in A$. First assume that D is empty. In this case we claim that 1 is a gcd of A. For this, it is sufficient to show that if $e\in M$ and $e|a$ for all $a\in A$, then e is a unit. If e is not unit, then there exists an irreducible $c\in M$ such that $c|e$. Since $e|a$ for all $a\in A$, so $c|a$ for all $a\in A$. Thus $\overline{c} \in D$, a contradiction as D is empty.

Now assume that $D = \{\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_t\}$, a non-empty set with t distinct elements. Then to each $a\in A$, there exists positive integers $m_i(a)$ such that $(k_i\gamma)^{m_i(a)}k_i|a$ and $(k_i\gamma)^{m_i(a)+1}k_i$ does not divide a for all $i = 1, 2, \ldots, t$ and some $\gamma\in\Gamma$.

Clearly, then every $a\in A$ can be written as $a = (k_1\gamma)^{m_1(a)}k_1\gamma(k_2\gamma)^{m_2(a)}k_2\gamma\ldots\gamma(k_t\gamma)^{m_t(a)}k_t\gamma a'$ for some $\gamma\in\Gamma$, where $a' \in M$. Let m_i min $= \{m_i(a)|a\in A\}$ for $i = 1, 2, \ldots, t$ and

$d=(k_1\gamma)^{m_1} k_1\gamma (k_2\gamma)^{m_2} k_2\gamma ...\gamma (k_t\gamma)^{m_t} k_t$ for some $\gamma\in\Gamma$. Then $d|a$ for all $a\in A$. Now we will show that d is a gcd of A. Let $e\in M$ and $e|a$ for all $a\in A$. If e is a unit, then clearly $e|d$. If e is a non-unit, then $e=v\gamma(q_1\gamma)^{s_1} q_1\gamma (q_2\gamma)^{s_2} q_2\gamma ...\gamma (q_n\gamma)^{s_n} q_n$ for some $\gamma\in\Gamma$, where v is a unit, $q_1, q_2, \ldots, q_n$ are irreducible such that no two of these are associates an $s_i \geq 1$ for $i = 1, 2, \ldots, n$. Since $q_j|e$ so $q_j|a$ for all $a\in A$. Thus $\overline{q}_j \in D$ for all $j = 1, 2, \ldots, n$. Therefore, $\{\overline{q}_1, \overline{q}_2, ..., \overline{q}_n\}\subseteq D$ so $n\leq t$. Also, it shows that each q_j is an associate of some k_{i_j}. Thus $q_j = u_j\gamma k_{i_j}$ for some unit u_j in M and $\gamma\in\Gamma$.

Now $e=v\gamma(q_1\gamma)^{s_1} q_1\gamma ...\gamma (q_n\gamma)^{s_n} q_n = w\gamma(k_{i_1}\gamma)^{s_1} k_{i_1}\gamma (k_{i_2}\gamma)^{s_2} k_{i_2}\gamma ...\gamma (k_{i_n}\gamma)^{s_n} k_{i_n}$, where $w=v\gamma(u_1\gamma)^{s_1} u_1\gamma (u_2\gamma)^{s_2} u_2\gamma ...\gamma (u_n\gamma)^{s_n} u_n$, a unit in M. Now again as $(k_{i_j}\gamma)^{s_j} k_{i_j}|a$ for all $a\in A$ and $j = 1, 2, \ldots, n$, by definition of m_{i_j}, we get $s_j \leq m_{i_j}$. Therefore $e|d$. Hence the theorem is proved.

5. Factorization in G-Principal ideal domains

5.1 Theorem : Let c be a non-zero element in a Γ-PID M. Then c is irreducible if and only if $\langle c\rangle$ is a maximal ideal of M.

Proof : Let $c\in M$ is irreducible. Then $\langle c\rangle\neq 0$ and $\langle c\rangle\neq M$ as c is non-zero and nonunit. Now suppose that there exists a in M such that $\langle c\rangle\subseteq\langle a\rangle\subseteq M$ and $\langle c\rangle\neq\langle a\rangle$. Then $c = a\gamma x$ for some $x\in M$ and $\gamma\in\Gamma$. If x is a unit, then c and a are associates (by Theorem 3.4), so $\langle c\rangle=\langle a\rangle$, a contradiction. Hence a must be a unit. Therefore $\langle a\rangle = M$. Hence $\langle c\rangle$ is a maximal ideal of M.

Conversely, let $\langle c\rangle$ is a maximal ideal in M. Then c is not a unit. If $a\in M$ with $\langle c\rangle\subseteq\langle a\rangle\subseteq M$ and $\langle c\rangle\neq M$. Then $\langle c\rangle=\langle a\rangle$. Therefore $c = a\gamma u$ for some unit u in M and $\gamma\in\Gamma$ (by Theorem 3.5). Hence c is irreducible. Thus the theorem is proved.

5.2 Theorem : Let M be a Γ-PID and A be a non empty subset of $M\backslash\{0\}$.

(i) An element d of M is a gcd of A if and only if d is a generator of $\langle a \rangle$, an ideal of M generated by A.

(ii) If $A = \{a_1, a_2, \ldots, a_s\}$ is finite, then every gcd of A is of the form $m_1\gamma a_1 + m_2\gamma a_2 + \ldots m_s\gamma a_s$, where $m_1, m_2, \ldots, m_s \in M$ and some $\gamma \in \Gamma$.

Proof : (i) Suppose that d is generator of $\langle A \rangle$. Then for any $a \in A$, $d|a$. Also as $d \in \langle A \rangle$, so $d = m_1\gamma a_1 + m_2\gamma a_2 + \ldots m_t\gamma a_t$, for some $m_1, m_2, \ldots, m_t \in M$, $a_1, a_2 \ldots, a_t \in A$ and some $\gamma \in \Gamma$. Therefore, if $e|a$ for all $a \in A$ then $e|d$. Hence d is gcd of A.

Conversely, let d is gcd of A and $\langle A \rangle = \langle c \rangle$, then as $d|a$ for all $a \in A$ so $a \in \langle d \rangle$. Therefore $\langle A \rangle \subseteq \langle d \rangle$, that is, $\langle c \rangle \subseteq \langle d \rangle$. Now if $a \in A$, then as $a \in \langle A \rangle = \langle c \rangle$ so $c|a$. Since d is a gcd of A, we have $c|d$, that is, $\langle d \rangle \subseteq \langle c \rangle$. Therefore $\langle d \rangle = \langle c \rangle = \langle A \rangle$. Hence d is a generator of $\langle A \rangle$.

(ii) is a straightforward consequence of (i). Thus the theorem is proved.

5.3 Theorem : Let M be a Γ-PID. Then an element k of M is prime if and only if k is irreducible.

Proof : By Theorem 3.8, we get if k is prime then it is irreducible. By Theorem 5.1, we get if k is irreducible, then $\langle k \rangle$ is maximal. So, $M/\langle k \rangle$ is a Γ-field. In particular $M/\langle k \rangle$ is a Γ-intergral domain. Therefore $\langle k \rangle$ is a prime ideal (by Theorem **2.3**). By Theorem 3.7 we get, k is prime. Hence the theorem is proved.

5.4 Lemma : Let M be a Γ-PID. Let k be a prime and suppose that k does not divide a. Then there exist elements s and t in M such that $1 = s\gamma k + t\gamma a$ for some $\gamma \in \Gamma$.

Proof : Let A be the ideal generated by k and a, that is, $A = \{x\gamma k + y\gamma a | x \in M, y \in M \text{ and some} \gamma \in \Gamma\}$. Since A is a principal ideal, there exists $c \in A$ such that $A = \langle c \rangle$ and so we can find s and t such that $s\gamma k + t\gamma a = c$. Since $\langle k \rangle \subseteq A = \langle c \rangle$, by Lemma 3.4, $c|k$. Similarly $c|a$. Since k is a prime, c is either a unit or an associate of k. In the later case $c = u\gamma k$, u a unit for some $\gamma \in \Gamma$. Hence $c|a$ implies $k|a$. This is impossible, so c is a unit. Thus there exists $e \in A$ such that $e\gamma c = 1$. Now

$$(s\gamma k + t\gamma a) = c$$

Therefore, $$e\gamma(s\gamma k + t\gamma a) = e\gamma c$$

$$\Rightarrow e\gamma s\gamma k + e\gamma t\gamma a = e\gamma c$$

$$\Rightarrow (e\gamma s)\gamma k + (e\gamma t)\gamma a = 1$$

$\Rightarrow s\gamma k + t\gamma a = 1$, since e is the identity of M. Thus the lemma is proved.

5.5 Lemma : Let M be a Γ-PID. Let $\{A_n | n = 1, 2, \ldots\}$ be a chain of ideals in M, that is, $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$. Then there exists an integer t such that $A_s = A_t$ for all $s \geq t$.

Proof : Let $A_n = \langle a_n \rangle$ and let $A = \bigcup_{n=1}^{\infty} A_n$. Since $A_s \subseteq A_h, s \leq h$, we can prove easily that A is an ideal of M. For let $a, b \in A$. Then clearly there exists s such that $a \in A_s$ and $b \in A_s$. Since A_s is an ideal of M, $a\text{-}b \in A_s$. Hence $a\text{-}b \in A$. It is also easy to prove that if $a \in A$, $m \in M$ and $\gamma \in \Gamma$, then $m\gamma a$, $a\gamma m \in A$. Since A is an ideal of M, there exists an element $c \in A$ such that $A = \langle c \rangle$. But since A is the union of sets, $c \in A_t$ for some t. Thus $A \subseteq A_t$. Hence $A_s \subseteq A_t$ for all $s \geq t$. Since also $A_s \subseteq A_t$ for all $s \geq t$. Hence $A_s = A_t$ for all $s \geq t$. Thus the lemma is proved.

5.6 Lemma : Let M be a Γ-PID. Let B be an ideal of M, $B \neq M$. Then there exists a maximal ideal R of M such that $B \subseteq R$. Moreover, $R = \langle k \rangle$, where k is a prime.

Proof : Let $A_1 = B$. If B is not a maximal ideal, then there exists an ideal A_2 such that $A_1 \subseteq A_2 \subseteq M$. If A_2 is not maximal, then there exists and ideal A_3 such that $A_1 \subseteq A_2 \subseteq A_3 \subseteq M$. By Lemma 5.5, this process must stop after a finite number of steps. Thus there does not exist a maximal ideal R in M such that B $\subseteq R$. By Theorem 2.4, R is a prime ideal. Now let $R = \langle k \rangle$. If k is not a prime, then $k = a\gamma b$ for some non-zero non-units a and b and some $\gamma \in \Gamma$. Also $b \notin \langle k \rangle$, for if $b \in \langle k \rangle$, then $b = c\gamma k$, for some c. Therefore,

$$\begin{aligned} k &= a\gamma b \\ &= a\gamma(c\gamma k) \\ &= (a\gamma c)\gamma k \end{aligned}$$

Then $k - (a\gamma c)\gamma k = 0$

$$\Rightarrow (1 - a\gamma c)\gamma k = 0$$

$$\Rightarrow 1 - a\gamma c = 0, \text{ since } k \neq 0.$$

Hence $1 = a\gamma c$. Therefore a is a unit, a contradiction. Thus $b \notin \langle k \rangle$ and similarly $a \notin \langle k \rangle$. But this contradicts that $\langle k \rangle$ is a prime ideal. Thus k is a prime. Hence the lemma is proved.

5.7 Lemma : Let M be a Γ-PID. Let $a \in M$, $a \neq 0$, a not a unit. Then there exists a prime $k \in M$ such that $k | a$.

Proof : Since a is not a unit, $\langle a\rangle \subseteq M$. Hence by Lemma 5.6, $\langle a\rangle \subseteq \langle k\rangle$ for some ideal $\langle k\rangle$, where k is a prime. Then by Theorem 3.4(i), $k|a$. Hence the lemma is proved.

5.8 Theorem : Let M be a Γ-PID. Let $a\in M$, $a\neq 0$, a not a unit. Then a has a factorization into primes in M.

Proof : By Lemma 5.7, there exists a prime k_1 such that $k_1|a$, that is, $a = k_1\gamma a_1$ for some unique $\gamma\in\Gamma$.

If a_1 is a unit, then a is a prime by Theorem 3.9 and the proof is completed.

If a_1 is not a prime, by Lemma 5.7, there exists a prime k_2 such that $a_1 = k_2\gamma a_2$. Again if a_2 is a unit, then $k_2\gamma a_2$ is a prime. Hence $a = k_1\gamma(k_2\gamma a_2) = k_1\gamma k_2\gamma a_2$ is a product of primes.

If a_2 is not a prime, we find that $a_2 = k_3\gamma a_3$, k_3 is a prime. Continuing, we find primes $k_1, k_2, \ldots, k_n, \ldots$ and elements $a_1, a_2, \ldots, a_n, \ldots$ such that $a_i|a_{i-1}$, $i = 2, 3, \ldots,$. Thus by Theorem 3.4(i), $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \ldots\ldots$.By Lemma 5.5, there exists an integer t such $\langle a_t\rangle = \langle a_{t+1}\rangle = \ldots$ .Thus $a_{t+1} = u\gamma a_t = u\gamma k_{t+1}\gamma a_{t+1}$. Hence $u\gamma k_{t+1} = 1$. Thus k_{t+1} is a unit, which contradicts that k_{t+1} is a prime. Therefore a_t must be a prime. Hence $a = k_1\gamma k_2\gamma \ldots\gamma k_t\gamma a_t$ is a factorization of a into primes for some unique $\gamma\in\Gamma$. Thus the theorem is proved.

5.9 Theorem : Every Γ-PID is Γ-UFD.

Proof : Let M be a Γ-PID. Theorem 5.8, established the existence of one prime factorization for an element $a\in M$, $a\neq 0$, a not a unit.

Suppose now that k is a prime and $k|a\gamma b$ for some $\gamma\in\Gamma$. If k does not divide a, by Lemma 5.4, we get $1 = s\gamma k + t\gamma a$ for some $s, t\in M$ and $\gamma\in\Gamma$. Then

$$1 = (s\gamma k + t\gamma a)$$

$$\Rightarrow 1\gamma b = (s\gamma k + t\gamma a)\gamma b$$

$$\Rightarrow b = s\gamma k\gamma b + t\gamma a\gamma b$$

$\Rightarrow b = s\gamma(b\gamma k) + t\gamma a\gamma b$, since M is commutative

$\Rightarrow b = (s\gamma b)\gamma k + t\gamma(a\gamma b)$. Since $k|(s\gamma b)\gamma k$ and $k|t\gamma(a\gamma b)$, $k|(s\gamma b)\gamma k + t\gamma(a\gamma b)$

Thus $k|b$.

Now let $a = k_1\gamma k_2\gamma \ldots \gamma k_m = q_1\gamma q_2\gamma \ldots \gamma q_n$ for some $\gamma \in \Gamma$ be two prime factorizations for a. Then $k_1|(q_1\gamma q_2 \ldots \gamma q_n)$ and so $k_1|q_i$ for some i. We may assume that i = 1. Since q_1 is a prime, k_1 and q_1 must be associates. The theorem now follows by induction. If $m = 1$, then a is a prime. Hence we have $n = 1$ and also $k_1 = q_1$. Thus, we may assume $m > 1$ and $n > 1$. Now it is clear that $k_1|(q_1\gamma q_2 \ldots \gamma q_n)$ and so by Theorem 3.8(i), $k_1|q_h$ for some h. But since q_h is a prime, $k_1 = q_h$. We may assume that the q_i's are so arranged that $h = 1$. Thus $k_1\gamma k_2\gamma \ldots \gamma k_m = k_1\gamma q_2\gamma \ldots \gamma q_n$.

Since $k_1 \neq 0$, we may cancel and get $k_2\gamma k_3\gamma \ldots \gamma k_m = q_2\gamma q_3\gamma \ldots \gamma q_n = a'$. But $1 < a' < a$ and by our induction hypothesis we may conclude (i) that m - 1 = n - 1 and (ii) that the factorization $k_2\gamma k_3\gamma \ldots \gamma k_m$ is just a rearrangement of q_i's i = 2, 3, . . ., m. Thus $m = n$ and γ is also unique, since $k_1 = q_1$, we have proved the theorem for m. Hence the expression $a = k_1\gamma k_2\gamma \ldots \gamma k_m$ into primes is unique. Therefore M is a Γ-UFD. Thus the theorem is proved.

References

[1] Barnes, W. E. (1966). "On the gamma rings of Nobusawa", Pacific J. Math 18 (1966) 411-422.

[2] Coppage, W. E. and Luh, J. (1971). "Radicals of gamma rings", J. Math. Soc. Japan, Vol 23, No. 1 (1971), 40-52.

[3] Jacobson, N. (1964). "Structure of Rings", revised Amer. Math. Soc. Colloquim oubl. 37, providence, 1964.

[4] Nobusawa, N. (1964). "On a generalization of the ring theory", Osaka J. Math. 1 (1964), 81-89.

[5] Paley, H. and Weichsel, P. M. (1996). "A First Course in Abstract Algebra", Holt, Rinehart and Winston, Inc. 1966.

[6] Sahai, V. and Bist, V. (1999). "Algebra", Narosa Publishing House, New Delhi. 1999.

***