Journal of Mathematical Extension
Vol. 5, No. 1 (2010), 41-48

Homorooty in Rings

M. H. Hooshmand*
Islamic Azad University-Shiraz Branch

R. Poorjafary
Islamic Azad University-Estahban Branch

Abstract. The topic of "Homorooty" (for integer numbers) has been introduced and studied in [2]. There are some applications of the homorooty in studying and solving some Diophantine equations and systems, as an interesting and useful elementary method. As a continuation of the Homorooty, we consider it for arbitrary rings and will study its properties in different rings, especially UFD and homorooty rings (which will be introduced). At last we shall state some applications of homorooty in studying some equations over homorooty rings.

AMS Subject Classification: 11A99; 11D25; 11D09; 11D72.
Keywords and Phrases: Diophantine equation, homorooty, homoroot integers, homorooty inequality, homorooty lemma, homorooty ring, indeterminate equation and system, quartic equation, UFD.

1. Introduction

In [1] the homoroot integer numbers have been introduced and studied. The topic of Homorooty has some applications in studying and solving some Diophantine equations and systems (specially the quartic equations discussed in [2]).
Two integer numbers a, b are called homoroot if there exist integer numbers r_1, r_2 (the root of a, b) such that $a = r_1 + r_2$ and $b = r_1 r_2$. Two homoroot integer numbers a, b will be denoted by $< a, b > \rightarrow \mathbb{Z} < r_1, r_2 >$

Received May 2010; Final Revised October 2010
*Corresponding author

or simply by $< a, b >\to \mathbb{Z}$. By $< a, b >\to \mathbb{N}$ we mean $< a, b >\to \mathbb{Z} < r_1, r_2 >$ and $\{a, b, r_1, r_2\} \subseteq \mathbb{N}$. Thus if $a, b \in \mathbb{N}$ and $< a, b >\to \mathbb{Z}$, then $< a, b >\to \mathbb{N}$. It is shown that the following properties hold (see [2]).
(I)

$$< a, a+b >\to \mathbb{Z} \Longleftrightarrow < a-2, b+1 >\to \mathbb{Z},$$

$$< a, -a+b >\to \mathbb{Z} \Longleftrightarrow < a+2, b+1 >\to \mathbb{Z}.$$

(II) (The homorooty inequalities) Let b be a non-zero integer. Then
(a) $< a, b >\to \mathbb{Z} \Longrightarrow |a| \leqslant |b+1|$.
(b) If $< a, b >\to \mathbb{Z}$ and $|a| \neq |\frac{b}{i} + i|$, for $i = 1, \cdots, n \leqslant \sqrt{|b|}$, then $|a| < |\frac{b}{n} + n|$.
(c) moreover if $a, b \in \mathbb{N}$, then
$< a, b >\to \mathbb{N} \Longrightarrow 2\sqrt{b} \leqslant a \leqslant b+1$.
$< a, a+b >\to \mathbb{N} \Longrightarrow a \leqslant b+4$.
$< a, -a+b >\to \mathbb{Z} \Longrightarrow a \leqslant b$.

(III) (The homorooty lemma for integers) For every integers a, b with $b \neq 0$, the following statements are equivalent:
(a) $< a, b >\to \mathbb{Z}$,
(b) The equation $x^2 - ax + b$ has an integer root,
(c) $< \lambda a, \lambda^2 b >\to \mathbb{Z}$ for every integer $\lambda \neq 0$,
(d) $a = r + \frac{b}{r}$ for some integer r such that $r|b$ and $1 \leqslant |r| \leqslant \sqrt{|b|}$,
(e) $< \lambda_0 a, \lambda_0^2 b >\to \mathbb{Z}$ for some integer $\lambda_0 \neq 0$,
(f) $a^2 - 4b$ is a square integer,
(g) $< -a, b >\to \mathbb{Z}$.

(IV) We have $< a, a-1 >\to \mathbb{Z}$, $< a, 0 >\to \mathbb{Z}$ and $< 0, -a^2 >\to \mathbb{Z}$, for every $a \in \mathbb{Z}$.

2. Homoroot Elements of Rings

Considering the properties of elements of a ring, it is induced that the homorooty can be defined and studied in any arbitrary ring. Hence, in this section we consider the homorooty in arbitrary rings and study its properties in various kinds of rings.

Definition 2.1. *Let* $(R,+,.)$ *be a ring, we say that the elements* a,b *of* R *are homoroot if there exist elements* r_1 *and* r_2 *of* R *such that* $a=r_1+r_2, b=r_1.r_2$ *(the elements* r_1 *and* r_2 *are called 'the roots of* a,b*').*

Two homoroot elements a,b will be denoted by $<a,b>\rightarrow R<r_1,r_2>$ or simply by $<a,b>\rightarrow R$. It is easy to see that the following properties hold.

(I) In an arbitrary ring R we have

(i) $<a,0>\rightarrow R, <0,-a^2>\rightarrow R$, for every $a\in R$.

(ii) $<a,b>\rightarrow R \Longleftrightarrow <-a,b>\rightarrow R$.

(iii) $<a,b>\rightarrow R \Longleftrightarrow b=ar-r^2$, for some $r\in R$.

(II) Let R be a ring with identity. Then for every $a,b\in R$ we have

(i) $<a,a-1>\rightarrow R$.

(ii) $<a,a+b>\rightarrow R \Longleftrightarrow <a-2,b+1>\rightarrow R$.

(iii) $<a,-a+b>\rightarrow R \Longleftrightarrow <a+2,b+1>\rightarrow R$.

(III) Let R be a commutative ring. Then

(i) $<a,b>\rightarrow R \Longrightarrow <\lambda a,\lambda^2 b>\rightarrow R$, for every $\lambda\in R$.

(ii) $<a,b>\rightarrow R \Longrightarrow a^2-4b=c^2$, for some $c\in R$.

(iii) $a^2-4b=c^2 \Longrightarrow <2a,4b>\rightarrow R$.

(IV) Let R be a commutative ring with identity. Then $<a,a>\rightarrow R$ if and only if there exists an invertible element u such that $a=u+u^{-1}+2$. Therefore

(i) $<a,a>\rightarrow \mathbb{Q} \Longleftrightarrow a=\frac{(m+n)^2}{mn}$, for some $m,n\in\mathbb{Z}\setminus\{0\}, (m,n)=1$.

(ii) $<a,a>\rightarrow \mathbb{Z} \Longleftrightarrow a=0,4$.

(V) Let R be a commutative ring with no zero divisors. If $<a,b>\rightarrow R$, then the roots of a,b are unique (i.e, $<a,b>\rightarrow R<r_1,r_2>, <a,b>\rightarrow R<t_1,t_2>$, then $r_1=t_1, r_2=t_2$ or $r_1=t_2, r_2=t_1$).

Assume that $S\subseteq R$. By the notation $<a,b>\rightarrow S$ we mean $<a,b>\rightarrow R<r_1,r_2>$ and $\{a,b,r_1,r_2\}\subseteq S$.

2.1 Homorooty Rings

There exists a vast class of rings in which important properties of homorooty, including the homorooty lemma, hold. Now we introduce these rings.

Definition 2.2. *Let R be an arbitrary ring. For an integer n and $a \in R$, $n|a$ means that there exists an element $b \in R$ such that $a = nb$ (note that if $1 \in R$, then $n|a$ if and only if $n1_R|a$, in the sense of dividing for two elements of a ring). We say that n is prime with respect to R if for any $r_1, r_2 \in R, n|r_1r_2$ implies that $n|r_1$ or $n|r_2$.*

Definition 2.3. *Let R be a commutative ring with no element of additive order 2. Then R is called a homorooty ring if we have*

$$\forall r_1, r_2 \in R \;(2|r_1 + r_2, 4|r_1r_2 \Longrightarrow 2|r_1, 2|r_2)\;.$$

Example 2.4. Assume R to be a commutative ring such that or $\mathrm{Ord}(r) \neq 2$ (for every $r \in R$). If the integer number 2 or 4 is prime with respect to R or if $1 \in R$ and 2 or 4 is a unit element, then R is homorooty ring. The field F for which $\mathrm{Char}(F) \neq 2$ is another type of the homorooty rings.

Lemma 2.5. *The Gaussian domain is a homorooty ring.*

Proof. Consider the elements $r_1 = a + bi, r_2 = c + di$ of $\mathbb{Z}[i]$, so $r_1r_2 = (ac - bd) + (ad + bc)i$. If $4|r_1r_2$, then $4|ac - bd$ and $4|ad + bc$, therefore

$$4|a(c^2 + d^2), 4|c(a^2 + b^2), 4|d(a^2 + b^2).$$

If $a^2 + b^2$ is odd, then $4|c, 4|d$ so $2|c + di = r_2$.
Let $a^2 + b^2$ be even. If a and b are even, then $2|a + bi + r_1$ and if a and b are odd, then $4|c^2 + d^2$ so $2|c$ and $2|d$ and hence $2|c + di = r_2$. Therefore, we have proved that "$4|r_1r_2 \Longrightarrow 2|r_1$ or $2|r_2$", and this proves our claim. $\square$

Lemma 2.6. *Let R be a commutative ring such that $\mathrm{Ord}(r) \neq 2$, for every $r \in R$. If $4|a^2 - c^2$ implies $2|a + c$ (for any $a, c \in R$), then R is a homorooty ring and vice versa.*

Proof. If $2|r_1 + r_2$ and $4|r_1r_2$, then $r_1 - r_2 = -2a$, for some $a \in R$. thus $4|a^2 - (r_2 - a)^2 = -r_1r_2$ and so $2|a + (r_2 - a) = r_2$ and $2|r_1$, clearly. Conversely, let R be a homorooty ring. If $4|a^2 - c^2$ then $4|(a + c)(a - c)$ and $2|(a + c) + (a - c)$. Therefore $2|a + c$. $\square$

Lemma 2.7. *(The homorooty Lemma) Let R be a homorooty ring. Then*

$$< a, b >\rightarrow R \Longleftrightarrow a^2 - 4b = c^2,$$

for some c.

Proof. Suppose that $a^2 - 4b = c^2$ so $< 2a, 4b >\rightarrow R$, by (III), therefore

$$2a = t_1 + t_2, 4b = t_1t_2 \Longrightarrow 2|t_1 + t_2, 4|t_1t_2 \Longrightarrow 2|t_1, 2|t_2 \Longrightarrow t_1 = 2r_1, t_2 = 2r_2$$

So $2a = 2(r_1 + r_2)$, $4b = 4r_1r_2$ and then $a = r_1 + r_2$, $b = r_1r_2$. $\square$

Corollary 2.8. *Let F be a field for which $\mathrm{Char}(F) \neq 2$. Then $g \in F[X]$ is reducible (i.e.g can be expressed as the product of two non-trivial factors in $F[X]$) if and only if there exists $f \in F[X]$ such that $\deg(f) < \deg(g)$ and $f^2 - 4g$ is a square element.*

Proof. If $f^2 - 4g$ is a square element, then $< f, g >\rightarrow F[X]$, by the homorooty lemma. So, there exist two polynomials $r_1 = r_1(x)$, $r_2 = r_2(x)$ such that $g = r_1r_2$ and $\deg(r_1 + r_2) < \deg(r_1r_2)$. Thus $\deg(r_1), \deg(r_2) \geqslant 1$ and so g is reducible. The converse is trivial. $\square$

We note that $\sqrt{a}$ $(a/2)$ is every element r of R such that $r^2 = a$ $(2r = a)$. Here we call r a second root of a.

Theorem 2.9. *(a) In every homorooty ring the formula $\frac{a+\sqrt{a^2-4b}}{2}$ gives us all roots of $x^2 - ax + b$ and the set of all roots of this polynomial is the set of all values of $\frac{a+\sqrt{a^2-4b}}{2}$.*
(b) Consider the indeterminate equation $x^2 - dy = z^2$ over a homorooty ring R, where d is a constant element of R or $\mathbb{Z}$. Then the general solution of the (d-homorooty equation) is

$$(x, y, z) = (\frac{r_1 + r_2}{2}, \frac{r_1r_2}{d}, \frac{r_1 - r_2}{2}) \text{ for all } r_1, r_2 \in R \text{ with } 2|r_1 + r_2\ ,\ d|r_1r_2.$$

If $d = 4$ (homorooty equation), then $(x = r_1 + r_2, y = r_1r_2, z = r_1 - r_2)$ is its general solution, where r_1, r_2 run over R.

Proof. If R is a commutative ring and r is a root of $x^2 - ax + b$, then there exists a second root t, of $a^2 - 4b$ such that $r = \frac{a+t}{2}$. This is because $r^2 - ar + b = 0$ implies

$$(2r - a)^2 = a^2 - 4b \Longrightarrow 2r - a = \sqrt{a^2 - 4b} \Longrightarrow 2r = a + \sqrt{a^2 - 4b}.$$

But if t is a second root of $a^2 - 4b$, then it is no more necessary for $r = \frac{a+t}{2}$ to be a root of $x^2 - ax + b$ (even it is possible that $r = \frac{a+t}{2}$ does not make sense). Now assume that R is a homorooty ring and $a^2 - 4b = t^2$, for some $r \in R$, then $2|a + t$ (by Lemma 3.6) so $\frac{a+t}{2} = r \in R$ thus

$$2r - a = t \Longrightarrow (2r - a)^2 = t^2 = a^2 - 4b \Longrightarrow 4(r^2 - ar + b) = 0,$$

therefore $r^2 - ar + b = 0$.
The part (b) is gotten from the homorooty lemma and this fact that $x_0^2 - dy_0 = z_0^2$ implies $< 2x_0, dy_0 >\to R$. $\square$

2.2 Homorooty Properties in UFD's

In this section we assume that R is a UFD. and F is the quotient field of R.

Lemma 2.10. *Let $a, b \in R$. Then $< a, b >\to F$ if and only if $< a, b >\to R$ and moreover the roots of a, b in F belong to R.*

Proof. By the Gaussian lemma, the polynomial $x^2 - ax + b$ is reducible over F if and only if it is reducible over R, so by (I), the first part of the lemma is proved, but if $< a, b >\to F$ then $< a, b >\to R$ and so the roots of a, b in F are the same as the roots of a, b in R. $\square$

Corollary 2.11. *Let a, b, c, d, λ belong to R and $bd \neq 0$. Then*
(i)

$$bd|ad + bc, bd|ac \Longleftrightarrow b|a, d|c.$$

(ii)

$$\lambda|a + c, \lambda^2|ac \Longleftrightarrow \lambda|a, \lambda|c.$$

Proof. Put $r_1 = a/b, r_2 = c/d, s = r_1 + r_2 = ad + bc/bd, p = ac/bd$ so $s, p \in R$ (up to isomorphism) since $< s, p >\rightarrow F$, we have $< s, p >\rightarrow R$ and $r_1, r_2 \in R$ (by Lemma 3.10), therefore $b|a$, $d|c$. (ii) is a conclusion of (i), by putting $\lambda = b = d \neq 0$ in (i) (if $\lambda = 0$, then it is clear). $\square$

Corollary 2.12. *Every UFD with no characteristic* 2 *is a homorooty ring.*

Proof. It is enough to consider $\lambda = 2$ in the above corollary. $\square$

Lemma 2.13. *If* $0 \neq \lambda \in R$, *then*

$$< \lambda a, \lambda^2 b >\rightarrow R \Longleftrightarrow < a, b >\rightarrow R.$$

Proof. Suppose $\lambda a = r_1 + r_2, \lambda^2 b = r_1 r_2$ so $\lambda | r_1 + r_2, \lambda^2 | r_1 r_2$ thus $\lambda | r_1$ and $\lambda | r_2$ (corollary 3.2) so r_1/λ and r_2/λ belong to R. Since we have $a = r_1 + r_2/\lambda, b = r_1 r_2/\lambda^2$, then we have $a = (r_1/\lambda) + (r_2/\lambda), b = (r_1/\lambda)(r_2/\lambda)$ so $< a, b >\rightarrow R$. $\square$

Lemma 2.14. *Let* $< a, b >\rightarrow R < r_1, r_2 >$. *Then* (a, b) *and* (r_1, r_2) *are associated if and only if* $(a, b)^2 | b$ *(where* (a, b) *is the greatest common divisor of* a *and* b*).*

Proof. Assume $(a, b)^2 | b$, so $(a, b) | r_1 + r_2, (a, b)^2 | r_1 r_2$ thus $(a, b) | r_1, (a, b) | r_2$ therefore $(a, b) | (r_1, r_2)$, also clearly $(r_1, r_2) | (a, b)$. Now if $(a, b) | (r_1, r_2)$, then $(a, b)^2 | r_1 r_2 = b$. $\square$

Lemma 2.15. *Let* m, n, p, q *belong to* R. *Then*

$$< \frac{m}{n}, \frac{p}{q} >\rightarrow F \Longleftrightarrow < qm, pqn^2 >\rightarrow R.$$

Proof. Suppose $< \frac{m}{n}, \frac{p}{q} >\rightarrow F$ so there exist $\alpha, \beta, \gamma, \lambda$ in R such that

$$\frac{m}{n} = \frac{\alpha}{\beta} + \frac{\gamma}{\lambda} \quad , \quad \frac{p}{q} = \frac{\alpha}{\beta} \frac{\gamma}{\lambda}.$$

so

$$mq = nq\tfrac{\alpha}{\beta} + nq\tfrac{\gamma}{\lambda}, pqn^2 = (nq\tfrac{\alpha}{\beta})(nq\tfrac{\gamma}{\lambda}) \Longrightarrow < mq, pqn^2 > \to F$$
$$\Longrightarrow < mq, pqn^2 > \to R,$$

(by Lemma 3.10). Now assume $< qm, pqn^2 > \to R$, then

$$qm = r_1 + r_2, pqn^2 = r_1 r_2 \Longrightarrow \tfrac{m}{n} = \tfrac{r_1}{qn} + \tfrac{r_2}{qn}, \tfrac{p}{q} = \tfrac{r_1}{qn}\tfrac{r_2}{qn}$$
$$\Longrightarrow < \tfrac{m}{n}, \tfrac{p}{q} > \to F. \quad \square$$

References

[1] M. H. Hooshmand, Homoroot integer numbers, *Acta Math. Univ. Comen.,* 1 (2010), 65-72.

[2] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

Mohammad Hadi Hooshmand
Department of Mathematics
Assistant Professor of Mathematics
Islamic Azad University-Shiraz Branch
Shiraz, Iran
E-mail: hadi.hooshmand@gmail.com

Reza Poorjafary
Department of Mathematics
Assistant Professor of Mathematics
Islamic Azad University-Estahban Branch
Estahban, Iran
E-mail: poorjafaryreza@yahoo.com