Tr. J. of Mathematics
19 (1995) , 291 – 399.

EUCLIDEAN RINGS

A. G. Ağargün, C. R. Fletcher

Abstract

In this paper, after a short survey of the Euclidean concept the possible definitions of Euclidean rings in which zero-divisors can appear are given. The connections between these definitions are shown. The Euclidean algorithms defined over a well-ordered set W and over $Z^+ \cup \{0\}$ are studied. The structure theorem for Euclidean rings defined over $Z^+ \cup \{0\}$ and some examples are given.

1. Introduction

In general terms van der Waerden defined a Euclidean ring to be an integral domain in which the division algorithm property is satisfied. Formally, an integral domain R is a Euclidean ring if there exists a mapping $\phi : R\backslash\{0\} \to Z^+ \cup \{0\}$ satisfying the two properties:

(i) $\phi(ab) \geq \phi(b)$ for all non-zero elements a, b, ab.

(ii) For $a, b \in R$, there exist $q, r \in R$ such that $a = bq + r$ where $r = 0$ or $\phi(r) < \phi(b)$[12].

Then Z is a Euclidean ring with respect to the mapping ϕ defined by $\phi(n) = |n|$; $Q[X]$ is a Euclidean ring under $\phi(f) = degf$; and $Z[i]$ is a Euclidean ring under the mapping $\phi(a + bi) = a^2 + b^2$. But not under $\phi(a + bi) = |a + bi|$.

Since the pioneering work of van der Waerden, the definition of Euclidean ring has suffered numerous alterations, some of substance, some not so. Our aim is to investigate this multitude of definitions and to provide a map for the lonely reader through this confusing landscape.

In 1951 Jacobson defined a Euclidean ring to be an integral domain R and a mapping $\phi : R\backslash\{0\} \to Z^+ \cup \{0\}$ satisfying.

(i) $\phi(a) = 0$ if and only if $a = 0$,

(ii) $\phi(ab) = \phi(a) \cdot \phi(b)$,

(iii) given $a, b \in R, b \neq 0$, there exist elements $q, r \in R$ such that

$$a = bq + r \text{ where } \phi(r) < \phi(b)[3].$$

Then Z is a Euclidean ring with respect to the usual mapping $\phi(n) = |n|$, and $Z[i]$ is a Euclidean ring for $\phi(a + bi) = a^2 + b^2$ but $Q[X]$ is not a Euclidean ring for $\phi(f) = \deg f$ because of the equality in (ii). Jacobson however does not lose this stock example because he may take instead the mapping $\phi(f) = 2^n$ where $n = \deg f$ and $\phi(0) = 0$.

In 1958 Zariski and Samuel reverted to van de Waerden's inequality in their Commutative Algebra [13].

In 1974 Jacobson went further and dropped completely any condition connecting $\phi(ab)$ and $\phi(b)$[4]. Now the mapping $\phi : R \to Z^+ \cup \{0\}$ was simply required to satisfy

(i) given $a, b \in R, a, b \neq 0$, there exist elements $q, r \in R$ such that

$$a = bq + r \text{ where } \phi(r) < \phi(b).$$

There is a slight wobble here because a is also taken to be non-zero, but in fact this does not widen the scope of the definition. For take $m \in R$ where $\phi(m)$ is minimum, then the condition $\phi(r) < \phi(m)$ implies that $m = 0$. For $a = 0, b \neq 0$ we have $0 = b.0 + 0$ where $\phi(0) < \phi(b)$.

In the meantime there were some further developments. In 1949 Motzkin had provided a necessary and sufficient condition for an integral domain to be a Euclidean ring [7]. This condition concerned the empty intersection of an infinite number of sets defined directly from R, with no mappings ϕ involved whatsoever. Motzkin's paper was a veritable tour de force. One can prove a domain is Euclidean by exhibiting a mapping which satisfies the appropriate properties, but a proof that a domain is not Euclidean cannot be found by proving that "all" mappings do not satisfy some property or other. Motzkin was able to make use of his criterion immediately by proving that the ring of algebraic integres of $Q[\sqrt{-19}]$ is not Euclidean.

Two generalisations of the original van der Waerden definition came in 1969 and 1971. Firstly, Fletcher defined the Euclidean property for a commutative ring with identity in which divisors of zero may appear [2]. Then Samuel postulated whether a mapping ϕ into a general well-ordered set would increase the number of Euclidean rings [11]. This idea had already occurred to Motzkin. The Fletcher and Samuel definitions are as follows.

A commutative ring R with identity is said to be Euclidean if to each non-zero $r \in R$ is assigned a non-negative integer $\phi(r)$, with the property that for any $a, b \in R, b \neq 0$, there exist elements $q, r \in R$ such that

$$a = bq + r \text{ where } r = 0 \text{ or } \phi(r) < \phi(b).$$

A commutative ring R with identity is said to be Euclidean if there exists a well-ordered set W and a mapping $\phi : R \to W$ with the property that for any $a, b \in R, b \neq 0$, there exist elements $q, r \in R$ such that

$$a = bq + r \text{ where } \phi(r) < \phi(b).$$

The element 0 is beginning to be a bit of a nuisance. Do we define $\phi(0)$? And do we insert "$r = 0$" as part of the condition? We return to these questions later. On the other hand, the condition "$\phi(ab) \geq \phi(b)$" has vanished, never to reappear. This is no loss for two reasons. Firstly, Motzkin had proved in 1949 that any Euclidean ring had a "fastest algorithm" which satisfied the inequality, and this proof happens to be valid for commutative rings (see $[2, p.79]$). Secondly, given any algorithm ϕ mapped into $Z^+ \cup \{0\}$, we may define a new mapping $\bar{\phi}$ defined by

$$\bar{\phi}(a) = \min\{\phi(\bar{a})\}$$

where $\bar{a}$ runs over all associate elements of a. In other words, a divides $\bar{a}$ and $\bar{a}$ divides a in R. Then $\bar{\phi}$ is an algorithm satisfying "$\bar{\phi}(ab) \geq \bar{\phi}(b)$" for all $a, b \in R$ where $ab \neq 0$.

In 1971 Samuel also asked the questions as to the outcome if, in the definition of Euclidean ring, The well-ordered set be replaced by a partially ordered set with descending chain condition. He answered his own question by showing that the class of Euclidean rings is unchanged. Finally, in this short survey of the twists and turns of the Euclidean concept, we mention the definition of Nagata in 1985 [9]. The algorithm ϕ maps the non-zero elements of R into a partially ordered set with descending chain condition. The criterion is that for $a, b \in R, b \neq 0$, there exist elements $q, r \in R$ such that

$$a = bq + r \text{ where } r = 0 \text{ or } \phi(r) < \phi(b).$$

This does not affect the class of Euclidean rings, but it has the advantage that we may write down $a = bq + r$ where $\phi(r)$ is always defined.

2. A Dozen Definitions

The above historical outline has shown that there are four possible areas for alternatives in the definition of Euclidean ring. One of these is the question whether we take $Z^+ \cup \{0\}$ or general welll-ordered set. For the moment we assume the existence of some well-ordered set W, and a mapping ϕ into W. The other three areas for choice are

(i) $\phi : R\backslash\{0\} \to W$ or $\phi : R \to W$,
(ii) b any element of R or $b \neq 0$,
(iii) $a = bq + r$ where $r = 0$ or $\phi(r) < \phi(b)$,
or $r = b$ or $\phi(r) < \phi(b)$,
or $\phi(r) < \phi(b)$.

That gives us twelve possible definitions in all, but some of these cannot exist in the wild.

Definition 1. $\phi : R\backslash\{0\} \to W, b \neq 0, r = 0$ *or* $\phi(r) < \phi(b)$[6].

Definition 2. $\phi : R\backslash\{0\} \to W, b \neq 0, r = b$ *or* $\phi(r) < \phi(b)$[9].

Definition 3. $\phi : R \to W, b \neq 0, r = 0$ *or* $\phi(r) < \phi(b)$[1].

Definition 4. $\phi : R \to W, b \neq 0, r = b$ *or* $\phi(r) < \phi(b)$.

Definition 5. $\phi : R \to W, b \neq 0, \phi(r) < \phi(b)$[6].

Definition 6. $\phi : R \to W$, *any* $b, r = 0$ *or* $\phi(r) < \phi(b)$[6].

Definition 7. $\phi : R \to W$, *any* $b, r = b$ *or* $\phi(r) < \phi(b)$[5] *and* [10].

Definition 8. $\phi : R \to W$, *any* $b, \phi(r) < \phi(b)$.

Definition 9. $\phi : R\backslash\{0\} \to W, b \neq 0, \phi(r) < \phi(b)$.

Definition 10. $\phi : R\backslash\{0\} \to W$, *any* $b, r = 0$, *or* $\phi(r) < \phi(b)$.

Definition 11. $\phi : R\backslash\{0\} \to W$, *any* $b, r = b$, *or* $\phi(r) < \phi(b)$.

Definition 12. $\phi : R\backslash\{0\} \to W$, *any* $b, \phi(r) < \phi(b)$.

We note that Lenstra is considering a module rather than a ring, Nagata is mapping R into a partially ordered set with minimum condition, Kanemitsu and Yoshida also require $\phi(a) \leq \phi(0)$ for all $a \in R$, but this follows automatically by taking $b = 0$ and $a \neq 0$.

We may immediately eliminate the last three definitions by taking $a = 1$ and $b = 0$. Similarly definitions 8 and 9 lead nowhere simply by choosing b where $\phi(b)$ is minimal. The remaining seven possibilities however can be taken as the basis for Euclidean ring definition.

But are any two of them equivalent? Before we can answer such a questions we have to make it more precise since there are several different interpretations of the word "equivalent". Do we mean that if R is a Euclidean ring with respect to one definition then it will be a Euclidean ring with respect to the other? Or do we mean that if R is a Euclidean ring with respect to one definition and a given W then it will be a Euclidean ring with respect to the other definition but the same W? Or are we taking about the some W and the same ϕ? The answer is that we may take one or all of these possibilities, and indeed we start off with a fourth notion of equivalence. The zero element is seemingly a problem child for a Euclidean algorithm, so first we consider the connections between these seven definitions keeping the same W and the same ϕ apart perhaps from $\phi(0)$.

Theorem 1. *Definitions 1,2,3 and 4 are equivalent with respect to a fixed well-ordered set W, and a mapping ϕ fixed on the non-zero elements of R.*

Proof. Definitions 1 and 3 are identical apart from the definition or non-definition of $\phi(0)$. The same is true for Definitions 2 and 4. Clearly also 1 and 2 are the same since $a = bq + 0$ if and only if $a = b(q-1) + b$.

A similar argument will prove the following. □

Theorem 2. *Definitions 6 and 7 are equivalent with respect to a fixed well-ordered set W, and a mapping ϕ fixed on the non-zero elements of R.*

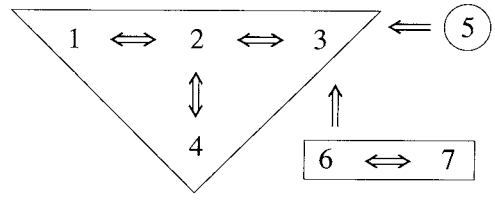
The following theorem is immediate

Theorem 3.

(i) *If $\phi : R \to W$ satisfies Definition 5, then it satisfies Definition 3.*

(ii) *If $\phi : R \to W$ satisfies Definition 6, then it satisfies Definition 3.*

The picture of implications for a given W, and ϕ fixed on the non-zero elements, shows three distinct subsets of equivalent definitions.



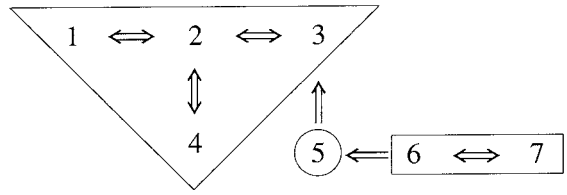
Note that:
for Definitions 1 and 2, $\phi(0)$ is not defined;
for Definitions 3 and 4, $\phi(0)$ is defined but satisfies no extra conditions;
for Definition 5, $\phi(0) < \phi(b)$ for all non-zero $b \in R$;
for Definitions 6 and 7, $\phi(r) < \phi(0)$ for all non-zero $r \in R$.

If we allow ϕ to change while W remains constant, the three distinct subsets of equivalent definitions remain the same, but there is an extra implication connecting two of them.

Theorem 4. *If R is a Euclidean ring according to Definition 6 with respect to a well-ordered set W and a mapping $\phi : R \to W$, then there exists a mapping $\bar{\phi} : R \to W$ satisfying Definition 5.*

The only change we have to make is to switch the image of 0 from the unique maximum $\phi(0)$ to the unique minimum $\bar{\phi}(0)$. Informally, we move the images up one step and slot in $\bar{\phi}(0)$ at the bottom.

The picture for fixed W becomes:



The single implications cannot be reversed because of the different properties of $\phi(0)$, e.g.
$\phi : Z_2 \to \{0\}$ satisfies Definition 3 but not Definition 5.
$\phi : Z \to Z^+ \cup \{0\}$ defined by $\phi(n) = |n|$ satisfies Definition 5 but not Definition 6.

Next we allow W to change. We could allow ϕ to change as well, but this is unnecessary apart perhaps from redefining $\phi(0)$.

Theorem 5. *Let R be a Euclidean ring according to definition 3 with respect to a well ordered set W and a mapping $\phi : R \to W$. Then there exists a well-ordered set $\bar{W}$ and a mapping $\bar{\phi} : R \to \bar{W}$ for which R is a Euclidean ring according to Definition 6.*

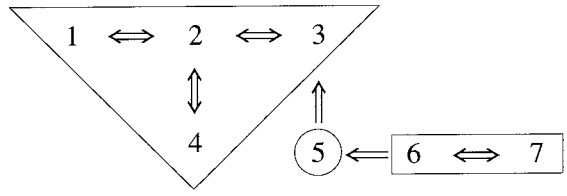
Proof. Put $\bar{W} = W \cup \{t\}$ where $t \notin W$ and define $w < t$ for all $w \in W$. Define $\bar{\phi} : R \to \bar{W}$ by

$$\bar{\phi}(0) = t$$
$$\bar{\phi}(r) = \phi(r) \text{ for } r \neq 0.$$

So the seven definitions of a Euclidean ring are equivalent provided that we may choose both W and ϕ. □

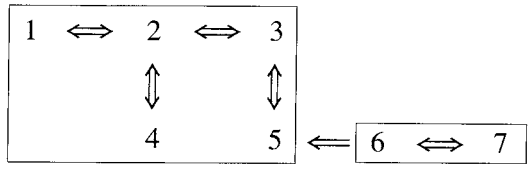
3. Euclidean Rings and the Non-Negative Integers

It remains to determine what sort of restriction would ensue if the well-ordered is taken to be $Z^+ \cup \{0\}$. We are back to the case of fixed W and variable ϕ, and the pictorial implications are



But for the particular case of $Z^+ \cup \{0\}$ we can do a little better than this, for Definition 3 implies Definition 5 by using the method of Theorem 4, moving everything up one place

and putting $\bar{\phi}(0)$ at the bottom. This gives us two classes of Euclidean rings if we use the non-negative integers.



The difference between the two classes is that for Definitions 6 and 7, $\phi(0)$ is the unique maximum element of the image of ϕ, hence the range of values of ϕ is bounded. So the concept of a bounded Euclidean ring has entered the theory naturally from a study of possible definitions. These rings had already made an appearance in [2] with the proof of the following structure theorem.

Theorem 6.

(i) A Euclidean ring defined over $Z^+ \cup \{0\}$ is either an integral domain or a direct sum of bounded Euclidean rings.

(ii) If R is a Euclidean ring defined over $Z^+ \cup \{0\}$ and

$$R = R_1 \oplus \cdots \oplus R_n \text{ where } n > 1$$

then each R_i is a bounded Euclidean ring for $i = 1, \cdots, n$.

We have already seen examples of such integral domains, $Z, Q[X], Z[i]$. For a nondomain we may take Z_{12} and define $\phi : Z_{12} \to Z^+ \cup \{0\}$ as follows.

r	0	1	2	3	4	5	6	7	8	9	10	11
$\phi(r)$	3	0	1	1	2	0	2	0	2	1	1	0

An example of a Euclidean ring which is not bounded is given by Z. The usual mapping defined by $\phi(r) = |n|$ is clearly not bounded, but this by itself is not sufficient for the proof. In fact every integral domain which is a bounded Euclidean ring is a field (see [2], p. 80). So Z, $Q[X]$ and $Z[i]$ are all non-bounded.

4. Conclusion

We have seen that there are fundamentally three types of Euclidean ring R.

(I): Defined with respect to a well-ordered set W and a mapping $\phi : R \to W$.

(II): Defined with respect to $Z^+ \cup \{0\}$ and a mapping $\phi : R \to Z^+ \cup \{0\}$.

(III): Defined with respect to $Z^+ \cup \{0\}$ and a mapping $\phi : R \to Z^+ \cup \{0\}$, where the set $\{\phi(r) | r \in R\}$ is bounded.

We have also seen that (II) and (III) are distinct and lead to different classes of Euclidean rings. It remains to show that (I) is in fact a wider class than (II).

Theorem 7. *The direct sum $Z \oplus Z$ is a Euclidean ring of type (I) but not of type (II).*

Proof. Let W be the well-ordered set $Z^+ \cup \{t\}$, where $n < t$ for all $n \in Z^+$, then $Z \oplus Z$ is a Euclidean ring with respect to the well-ordered set $W \times W$ and the mapping $\phi : Z \oplus Z \to W \times W$ given by

$$\begin{array}{rcll} \phi(k,l) & = & (|k|,|l|) & k,l \neq 0, \\ \phi(0,l) & = & (t,|l|) & l \neq 0, \\ \phi(k,0) & = & (|k|,t) & k \neq 0, \\ \phi(0,0) & = & (t,t). & \end{array}$$

The order on $W \times W$ is given by

$$(a_1,a_2) < (b_1,b_2) \text{ if } a_1 < b_1 \text{ or } a_1 = b_1 \text{ and } a_2 < b_2.$$

Here the zero integer causes the problem, for without it we could simply use the division algorithm for Z on the separate components

$$(a_1,a_2) = (b_1,b_2)(q_1,q_2) + (r_1,r_2) \text{ where } |r_1| < |b_1| \text{ and } |r_2| < |b_2|.$$

When $b_1 = 0$ or $b_2 = 0$, we have to make other arrangements.

That $Z \oplus Z$ is not a Euclidean ring with respect to $Z^+ \cup \{0\}$, follows directly from the structure theorem, since Z is not a bounded Euclidean ring. □

References

[1] Amano, A.: A note on Euclidean rings, *Bull. Fac. Gen. Ed. Gifu Univ.*, no. 20, 13-15 (1985).

[2] Fletcher, C.R.: Euclidean rings, *J. London Math. Soc.* (2), 4, 79-82 (1971).

[3] Jacobson, N.: *Lectures in Abstract Algebra,* Van Nostrand, New York, 1951.

[4] Jacobson, N.: *Basic Algebra I,* W H Freeman & Co., San Francisco, 1974.

[5] Kanemitsu, M., Yoshiba, K.: Euclidean rings, *Bull. Fac. Sci.*, Ibaraki Univ., Math., No. 18, 1-5 (1986).

[6] Lenstra, H. W.: *Lectures on Euclidean rings,* Bielefeld, 1974.

[7] Motzkin, T.: The Euclidean algorithm, *Bull. Amer. Math. Soc.* 55, 1142-1146 (1949).

[8] Nagata, M.: On Euclid algorithm, *Stud. Math.* 8, Tata Inst. Fund. Res., 175-186 (1978).

[9] Nagata, M.: Some remarks on Euclid rings, *J. Math.,* Kyoto Univ. 25-3, 421-422 (1985).

[10] Nagata, M.: On the definition of a Euclid ring, *Adv. Stud. Pure Maths.* 11, 167-171 (1987).

[11] Samuel, P.: About Euclidean rings, *J. Alg.,* 19, 282-301 (1971).

[12] Waerden, B.L. van der: *Moderne Algebra*, Springer, Berlin, 1931.

[13] Zariski, O., Samuel, P.: *Commutative Algebra I*, Van Nostrand, New York, 1958.

EUCLID HALKALARI

Özet

Bu çalışmada Euclid halkası kavramı hakkında kısa bir tarihsel gelişim verildikten sonra halkanın sıfır bölensiz olma koşulunu kaldırarak mümkün Euclid halkalarının tanımları verilmiş ve bunlar arasındaki ilişkiler gösterilmiştir. Euclid algoritmasının iyi-sıralı bir W kümesi üzerine tanımlanmasıyla $Z^+ \cup \{0\}$ üzerine tanımlanması arasındaki farklılıklar incelenmiştir. $Z^+ \cup \{0\}$ üzerine tanımlanan Euclid halkaları için yapısal teorem ve örnekler verilmiştir.

Ahmet Göksel AĞARGÜN,
Yıldız Teknik Üniversitesi,
Fen-Edebiyat Fakültesi,
Matematik Bölümü,
Şişli, İstanbul-TURKEY
Colin Robert FLETCHER
University of Wales, Aberystwyth,
Department of Mathematics,
Aberystwyth, Wales, U.K.

Received 1.7.1994