PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 57 (71), 1995, 124–134
Đuro Kurepa memorial volume

ON EUCLIDEAN ALGORITHMS WITH SOME PARTICULAR PROPERTIES

Gojko Kalajdžić

Dedicated to the memory of Profesor Đuro Kurepa

Abstract. Making use the notion of generalized Euclidean algorithm (as in [**1**] or [**5**]) we describe Euclidean rings whose algorithms satisfy the conditions (T), (N) or (Z) below.

In this paper every ring has a unit-element (denoted by *1*) and at least two elements. The units group of a given ring A will be denoted by $A^* = U(A)$. If $S \subset A$, then: $S^0 = S \setminus \{0\}$, $S_0 = S \cup \{0\}$, $K = U(A)_0$.

Right Euclidean algorithm of a ring A is each mapping $\phi: A \to W$ of a ring A into some well ordered set W so that the following is valid: for any $a \in A$ and $b \in A^0$, there exist $q, r \in A$ such that

$$a = bq + r, \qquad \phi(r) < \phi(b).$$

Besides $\phi(0) = \min \phi(A)$ holds. A right Euclidean algorithm ϕ is *monotone* if, for each $a, b \in A$ $(ab \neq 0)$, $\phi(ab) \geq \phi(a)$ is valid. *Left* (monotone) Euclidean algorithm of a ring A is similarly defined. If ϕ is a right and a left Euclidean algorithm of a ring A we say that ϕ is *Euclidean algorithm* of that ring. An Euclidean algorithm ϕ of a ring A is *finite*, if the *type* of the well ordered set $\phi(A)$ is not greater than ω; otherwise algorithm $\phi: A \to W$ is said to be *transfinite* ([**2**] or [**5**]).

A ring A is a *right* (*left*) *Euclidean ring* if it has at least one right (left) Euclidean algorithm ϕ. In that case the ordered pair (A, ϕ) is called a *right Euclidean pair*. Right Euclidean pairs (A, ϕ) and (B, ψ) are *isomorphic* if there is at least one ring isomorphism $f: A \to B$ and at least one ordered isomorphism $h: \phi(A) \to \psi(B)$, such that $h \circ \phi = \psi \circ f$ (Samuel [**4**], for $A = B$ and $f = \mathrm{Id}_A$).

Since isomorphic Euclidean pairs have the same properties, we can limit ourselves to Euclidean algorithms whose codomains are certain *ordinals*. Each right

AMS Subject Classification (1991): Primary 13 F 07

Euclidean pair (A, ϕ) is isomorphic to some right Euclidean pair (A, ψ) with monotone Euclidean algorithm ψ. If ϕ is a monotone right Euclidean algorithm of domain A, then for each $a, x \in A^0$ the following is valid:

$$\phi(0) < \phi(a), \qquad \phi(1) = \min \phi(A^0), \qquad \phi(ax) = \phi(a) \;\Leftrightarrow\; x \in A^*. \tag{1}$$

Let η be an ordinal and $\tilde{\eta} = \{-\infty\} \cup \eta$ (with the usual meaning and the properties of the symbol $-\infty$). Each right Euclidean algorithm $\phi: A \to \tilde{\eta}$ of a given ring A satisfying the conditions

$$\phi(a+b) \le \max\{\phi(a),\, \phi(b)\} \qquad (a, b \in A) \tag{M}$$

$$\phi(a \cdot b) = \phi(a) + \phi(b) \qquad (a, b \in A), \tag{L}$$

is called the *degree algorithm* of the ring. Ring A having at least one degree algorithm is an integral domain, and $K = U_0(A)$ is an subfield of a ring A. From the conditions (L) it follows that each degree algorithm is right (and left) monotone. If a ring A has at least one finite right Euclidean degree-algorithm ϕ, then for $K = U_0(A)$, there exists $X \in A \setminus K$ such that $A = K[X, f, \delta]$, where f is a monomorphism, and δ is a right f-derivation of field K. Then $\phi(a)$ is just *degree* of a (as a right polynomial with respect to X, with coefficients from K) (Cohn [**1**]). A similar assertion is valid if the condition (L) is substituted by the condition of monotoneity of algorithm ϕ (which is weaker than (L)). In the present paper we will deal more with the right Euclidean algorithms $\phi: A \to \tilde{\eta}$ (η being an ordinal) satisfying some of the conditions:

$$\phi(a+b) \le \phi(a) + \phi(b), \tag{T}$$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b), \tag{N}$$

$$\phi(a) = \phi(b) \;\Leftrightarrow\; (\exists e \in A^*)(a = be), \tag{Z}$$

where $+$ and $\cdot$ at the right-hand sides in (T) and (N) denote the *sum* and *product* of ordinals. It is obvious that for each right Euclidean algorithm ϕ the condition (T) follows from the condition (M). The example of ring $\mathbb{Z}$ shows that integral domain A can have an Euclidean algorithm satisfying all the conditions (T), (N) and (Z), and have not Euclidean algorithm satisfying the condition (M) (because $U(\mathbb{Z})_0$ is not a subfield of the ring $\mathbb{Z}$).

LEMMA 1. *Let $\phi: A \to W$ be a monotone right Euclidean algorithm, and $a \in A$ right regular element of a ring A. If $\phi(1) < \phi(a)$, then the sequence $\phi(a^n)$ is strictly increasing.*

Proof. Let $x = a^n$ and $q \in A$ so that $\phi(x - xaq) < \phi(xa)$. Then $c = 1 - aq$ is not 0 and monotoneity of algorithm ϕ implies: $\phi(xa) > \phi(xc) \ge \phi(x)$. □

LEMMA 2. *Let A be a domain and let $\phi: A \to W$ be a monotone right Euclidean algorithm satisfying the condition* (M). *Then for each $a, b \in A$ and $c \in A^0$ we have:*

1° *$K = U(A)_0$ is a subfield of the ring A,*

$2^\circ \quad \phi(a) < \phi(b) \;\Rightarrow\; \phi(ca) < \phi(cb).$

Proof. From (1) it follows that $K = \{a \in K\colon \phi a < \phi 1\}$, and for $a, b \in K$ we have $\phi(a-b) \le \max\{\phi a, \phi b\}$, i.e. $a - b \in K$, so that K is a subfield of the ring A.

Let us prove the implication 2°. Clearly, 2° is valid for $a = 0$ and each $b \in A$ and $c \in A^0$. Let us assume that 2° is valid for each $x \in A$ for which $\phi(x) < \alpha$ ($\alpha > 0$ is the given element from W), and let $a, b, c \in A$ such that $\phi(a) = \alpha$ and $\phi(a) < \phi(b)$, $c \ne 0$. There exist $q, r \in A$ such that $b = aq + r$ and $\phi(r) < \phi(a)$. Since $\phi(r) < \alpha$, we have $\phi(cr) < \phi(ca)$, and therefore

$$cb = caq + cr, \qquad \phi(cr) < \phi(ca). \tag{2}$$

It must be $q \ne 0$ (because on the contrary it would be $\phi b < \phi a$). Further, from $\phi a < \phi b$ it follows $\phi(a+b) \le \phi(b)$ and

$$\phi(b) \;=\; \phi(a+b-a) \;\le\; \max\bigl\{\phi(a+b),\, \phi(a)\bigr\},$$

so that $\phi(a+b) = \phi(b)$. In other words, the implication

$$\phi(a) < \phi(b) \;\Rightarrow\; \phi(a+b) = \phi(b) \tag{P}$$

is valid. Since ϕ is right monotone, it will be $\phi(caq) \ge \phi(ca) > \phi(cr)$, and thus $\phi(caq + cr) = \phi(caq)$, which together with (2) yields $\phi(cb) \ge \phi(ca)$. If $\phi(cb) = \phi(ca)$, then from $\phi(caq) = \phi(ca)$ would follow $q \in A^*$, and thereby $\phi(b) = \phi(aq + r) = \phi(aq) = \phi(a)$, which is contrary to $\phi(a) < \phi(b)$. Summing up, we have: $\phi(cb) > \phi(ca)$. $\square$

If $\phi\colon A \to W$ is a right Euclidean algorithm of a ring A and $x \in A$, let us denote by $A(x, \phi)$ the subset of A determined by:

$$a \in A(x,\phi) \quad \Leftrightarrow \quad (\exists n \in \mathbb{N})\,\bigl[\phi(a) \le \phi(x^n)\bigr].$$

So, for example, if K is a field and ϕ a degree algorithm of the ring $A = K[X]$, then we have $A(1, \phi) = K$, $A(X, \phi) = A$. Similarly we have $\mathbb{Z}(1, \nu) = \{-1, 0, 1\}$ and $\mathbb{Z}(2, \nu) = \mathbb{Z}$, where $\nu(m) = |m|$ is the *standard* Euclidean algorithm of the ring $\mathbb{Z}$.

LEMMA 3. *Let $\phi\colon A \to W$ be a monotone right Euclidean algorithm of a domain A satisfying the condition (M), and let x be any element from $A \setminus K$ such that $B = \{b \in A : \phi b < \phi x\}$ is a subring of the ring A. Then $A(x, \phi)$ is a subring of the ring A, and $a \in A$ belongs to the set $A(x, \phi)$ if and only if it is uniquely expressible in the form*

$$a \;=\; x^n a_n + \cdots + x a_1 + a_0 \qquad (a_i \in B). \tag{3}$$

Proof. Let us put $V = A(x, \phi)$ and let us prove first that each $a \in V$ has (at least one) decomposition of the form (3). It is obvious that it is true for $a \in B$. If $a \in V \setminus B$, then for some $n \in \mathbb{N}$ we have

$$\phi(x^n) \le \phi(a) < \phi(x^{n+1}). \tag{4}$$

There exist $c, a_0 \in A$ such that $a = xc + a_0$ and $\phi a_0 < \phi x$. Since ϕ satisfies the condition (P), from $xc = a - a_0$ and $\phi a_0 < \phi x \leq \phi a$ it follows $\phi(xc) = \phi(a)$, as well as $a_0 \in B$. If we prove that $\phi(c) < \phi(x^n)$, then the assertion will follow directly by induction with respect to n for which (4) holds. Let $c = x^n q + r$, $\phi(r) < \phi(x^n)$. If $q \neq 0$, then we have

$$\phi(x^{n+1}q) \geq \phi(x^{n+1}) > \phi(a).$$

On the other hand, by Lemma 2, from $\phi r < \phi x^n$ it follows $\phi(xr) < \phi(x^{n+1})$, and since ϕ also satisfies the condition (P), multiplying the equality $c = x^n q + r$ from the left-hand side by x, we get

$$\phi(xc) = \phi(x^{n+1}q + xr) = \phi(x^{n+1}q) \geq \phi(x^{n+1}),$$

i.e. $\phi(xc) > \phi(a)$, which is contrary to $\phi(xc) = \phi(a)$. Hence $q = 0$, and thereby $\phi(c) = \phi(r) < \phi(x^n)$. Therefrom c has a decomposition the form (3), so that from $a = xc + a_0$ and $a_0 \in B$ it follows that a is expressible in the form (3).

If $m, n \in \mathbb{N}_0$, then for $m > n$ and any elements $p \in B^0$, $q \in B$ we have $\phi(x^{m-n}p) \geq \phi(x) > \phi(q)$, and thereby $\phi(x^m p) > \phi(x^n q)$ the (by Lemma 2). Besides ϕ satisfies the condition (P), so that for each $a \in A$ of form (3) it holds $\phi(a) = \phi(x^n a_n)$. Particularly, in (3) for $a = 0$ we have $a_i = 0$ for each $i \geq 0$.

Let a be given by (3) and let $a = x^n b_n + \cdots + b_0$ be valid for some $b_i \in B$. If we put $c_i = a_i - b_i$, it will be $0 = x^n c_n + \cdots + c_0$. But, since B is a subring of the ring A, together with $a_i, b_i \in B$ we have $c_i \in B$, so that from the last equality it follows that it must be $c_i = 0$, and thereby $a_i = b_i$ for each $1 \leq i \leq n$. On the other side, since $\phi(c) < \phi(x)$ $(c \in B)$, by Lemma 2 we conclude that $\phi(x^n c) < \phi(x^{n+1})$ for each $c \in B$ and $n \in \mathbb{N}_0$. Hence for each a of the form (3) it follows $\phi(a) = \phi(x^n a_n) < \phi(x^{n+1})$, and therefore $a \in V$. Thus $V = A(x, \phi)$ is a right B-modul (in a natural way) with the basis $\{x^n :\ n \in \mathbb{N}_0\}$.

Finally, let us prove that V is a subring of the ring A, i.e. that $ab \in V$ for each $a, b \in V$. Let at first be $b = x$. There exist $q, r \in A$ such that $x = aq + r$, $\phi(r) < \phi(a)$. Then $\phi(x) = \phi(aq)$. If $\phi(q) > \phi(x)$, then by Lemma 2 we have $\phi(x) = \phi(aq) > \phi(ax)$, and thus $ax \in V$. In the case $\phi(q) = \phi(x)$, let us put $q = xu + s$, $\phi(s) < \phi(x)$. From $\phi(q) = \phi(x) > \phi(s)$ it follows that $u \neq 0$, so that $\phi(xu) > \phi(s)$, and thereby $\phi(q) = \phi(xu) = \phi(x)$. Hence $u \in A^*$, and since $\phi(s) < \phi(x)$ implies $\phi(as) < \phi(ax) \leq \phi(axu)$ (Lemma 2), we have

$$\phi(x) = \phi(aq) = \phi(axu + as) = \phi(axu) = \phi(ax),$$

and thereby $ax \in V$. At the end, if it were $\phi(q) < \phi(x)$, i.e. $q \in B$, then, together with $a, q, r \in B$, it would be $x = aq + r \in B$, a contradiction. Thus $ax \in V$ for each $a \in B$. Hence, by induction on n, we have $ax^n \in V$ $(a \in V,\ n \in \mathbb{N}_0)$. Hence, for any elements $a = x^r a_r + \cdots + a_0$ and $b = x^s b_s + \cdots + b_0$ $(a_i, b_i \in B)$ from V. the product ab is the sum of a finitely many summands of form $x^m(ux^n)v$ with $u, v \in B$, and thus $ab \in V$. □

If, with the assumption and symbolism of Lemma 2, $B = K \neq A$ and x is any element from $A \setminus K$ such that $\phi(x) = \min \phi(A \setminus K)$, then $V = A(x, \phi)$ is a subring of the ring A. If, besides the algorithm ϕ is finite (which will certainly be if the ring A is commutative), then it will be $a(x,\phi) = A$. Similarly to Cohn [**1**], we infer that for some monomorphism f and right f-derivation δ of field K we have $A(x,\phi) = K[x,f,\delta]$. Besides that, if ψ is the restriction of ϕ on V, and σ degree algorithm of the ring $K[x,f,\delta]$, then the right Euclidean pair (V,ψ) is isomorphic to the right Euclidean pair $\big(K[x,f,\delta],\sigma\big)$. In general, for the ring $V = A(x,\phi)$ from Lemma 2 it follows that there exist an endomorphism f and a right f-derivation δ of the domain B such that $V = K[x,f,\delta]$ and $f(B) \subset K$.

Lemma 4. *If a right Euclidean algorithm $\phi: A \to \eta$ of a ring A satisfies the conditions* (N) *and* (T)*, then it satisfies the condition* (M)*, iff $U(A)_0$ is a subfield of the ring A.*

Proof. Since ϕ satisfies the condition (N), it is clear that A is an integral domain, that the algorithm ϕ is monotone, and that $\phi(0) = 0$, $\phi 1) = 1$ (η is some ordinal). It is obvious that the *condition* is necessary. Let us prove that it is sufficient. If $K = U(A)_0$ is a subfield of the ring A, then for each $a,b \in A$ we have

$$\phi(a) \le \phi(b) \qquad \Rightarrow \qquad \phi(a+b) \le \phi(b). \tag{5}$$

Let at first, $\phi(a) = 1$, and thus $a \in K^0$. Since ϕ satisfies the condition (N), we have $\phi(a+b) = \phi(a(1+a^{-1}b)) = \phi(a)\,\phi(c)$, with $c = a^{-1}b$, and thereby $\phi(c) = \phi(a^{-1})\,\phi(b) = \phi(b)$. Hence for $\phi(a) = 1$ the implication (5) reduces to $1 \le \phi(c) \;\Rightarrow\; \phi(1+c) \le \phi(c)$ $(c \in A^0)$. Since K is a field, we have $k1 \in K$, and thereby $\phi(kc) = \phi(k1)\,\phi(c) \le \phi(c)$ for each $k \in \mathbb{N}$. Besides, ϕ satisfies the condition (T) too, so: $(1+c)^n = \sum \binom{n}{r} c^r$ and

$$\big[\phi(1+c)\big]^n = \phi\big[(1+c)^n\big] \le \sum \phi(c)^r. \tag{6}$$

for any $n \in \mathbb{N}$ and each $c \in A^0$. Let us put $\phi(c) = \lambda$. Then $\lambda \ge 1$. If $\lambda < \omega$, then from (6) it follows that for each $c \in A^0$ and $n \in \mathbb{N}$ we have $\phi(1+c) \le (1+n)^{1/n}$ (for $\lambda = 1$) and

$$\phi(1+c) \le \left(\frac{\lambda^{n+1}-1}{\lambda-1}\right)^{1/n} \qquad (\text{for } \lambda \ne 1).$$

Allowing that $n \to \infty$ we get $\phi(1+c) \le \lambda$. Hence $\phi(a+b) \le \phi(b)$ for each $a \in K$ and each $b \in A$ for which $1 \le \phi(b) < \omega$. If $\phi(b) = \lambda \ge \omega$, it will be $1 + \lambda = \lambda$, so that we have directly: $\phi(a+b) \le \phi(a) + \phi(b) = 1 + \lambda = \lambda = \phi(b)$.

Suppose now that (5) is valid for each $a \in A$ such that $\phi(a) < \alpha$ (α is a fixed ordinal, $\alpha > 1$), and let a be any element from A for which $\phi(a) = \min\{\phi(c): c \in A,\ \phi(c) \ge \alpha\}$. There exist $q,r \in A$ such that $b = aq + r$ and $\phi(r) < \phi(a)$. Hence $a + b = r + c$ with $c = a(1+q)$. If $1 + q \ne 0$, then we have $\phi(c) = \phi(a)\phi(1+q) \ge \phi(a) > \phi(r)$. Besides, since $\phi(r) < \alpha$, it will be $\phi(r+c) \le \phi(c)$, and for $q \ne 0$ we have $\phi(a+b) \le \phi(r+c) \le \phi(c)$ and $\phi(c) = \phi(a)\phi(1+q) \le \phi(a)\phi(q) = \phi(aq) = \phi(b-r)$, Finally, if $\phi(a) \le \phi(b)$, we have $\phi(r) < \phi(b)$, and then $\phi(a+b) \le \phi(b)$. $\square$

Lemma 5. *Let A be an integral domain which is not a field, $\phi: A \to \eta$ a right Euclidean algorithm satisfying the conditions* (N) *and* (T)*, $K = U(A)_0$ and*

x any element from $A \setminus K$ such that $\phi(x) = \min \phi(A \setminus K)$. Then each element $a \in A$ is expressible in the form

$$a = x^n a_n + \cdots + x a_1 + a_0 \qquad (a_r \in K,\ n \in \mathbb{N}_0). \tag{7}$$

Besides, $a = 0$ has exactly one decomposition of the form (7), and it is valid for each $a \in A$ provided that K is a subfield of A.

Proof. Let $\phi(a) = \alpha > 1$ and $a = xb + c$, $\phi(c) < \phi(x)$. Then $c \in K$. Since ϕ satisfies the conditions (N) and (T), we have $\phi(xb) = \phi(a - c) \le \phi(c) + \phi(a) \le 1 + \alpha$. Hence

$$\phi(x)\phi(b) \le 1 + \alpha. \tag{8}$$

If $\phi(b) \ge \alpha$, then $\phi(x)\phi(b) \ge (1+1)\alpha > 1 + \alpha$, a contradiction. Thus $\phi(b) < \alpha$. Now by (transfinite) induction on $\alpha = \phi(a)$ it follows that each $a \in A$ is expressible in the form (7). Besides, for each $n \in \mathbb{N}_0$ and $a_r \in K$ we have

$$\phi(\alpha_0 + \cdots + x^n a_n) < \phi(x^{n+1}). \tag{9}$$

Namely, if K is a field, then (9) follows directly by Lemma 4. If K is not a field, then $1 < \phi(u + v) \le \phi(u) + \phi(v) \le 2$ for some $u, v \in K$. Hence $\phi(x) = 2$, so that we have

$$\phi(\alpha_0 + \cdots + x^n a_n) \le 1 + \phi(x) + \cdots + \phi(x)^n < 2^{n+1}, \tag{10}$$

and thus (13) is proved. Now, by (10), for $a = 0$, from (7) it follows $\phi(-x^n a_n) < \phi(x^n)$. Hence $a_n = 0$, and similarly $a_r = 0$ for each $0 \le r \le n$. If K is a field, then the remaining part of the assertion follows by lemmas 3, 4. □

By Lemma 5, each right Euclidean algorithm ϕ of a ring A, satisfying the conditions (N) and (T), is finite. Therefore for such algorithms we may restrict our attention to the case $\phi(A) \subset \mathbb{N}_0$.

THEOREM 1. *If a ring A has a right Euclidean algorithm $\phi: A \to \mathbb{N}_0$ satisfying the conditions (N) and (T), then for $K = U(A)_0$ we have*

1° *If K is a subfield of A, then either $A = K$, or, for some monomorphism f and some right f-derivation δ of the field K, the right Euclidean pair (A, ϕ) is isomorphic to the right Euclidean pair (B, σ), where σ is a degree algorithm of the ring $B = K[X, f, \delta]$;*

2° *If K is not a subfield of A, then the right Euclidean pair (A, ϕ) is isomorphic to the Euclidean pair $(\mathbb{Z}, \nu)$, with $\nu(m) = |m|$.*

Proof. 1° It is clear that A is a domain, that algorithm ϕ is monotone and that $\phi(0) = 0$, $\phi(1) = 1$. Since K is a subfield of A, by Lemma 4 the algorithm ϕ satisfies the condition (M), as well. Now by Lemma 3, $\phi(A) \subset \mathbb{N}_0$ implies that $A = K$ or $A = A(x, \phi)$, so the assertion follows directly by Lemma 3.

2° Since K is not a subfield of A, there exist u, v from K such that $1 < \phi(u + v) \le \phi(u) + \phi(v) \le 2$. Hence for $e = u^{-1}v$ we have $u + v = u(1 + e)$, $e \in K^0$ and $2 = \phi(u + v) = \phi(u)\phi(1 + e) = \phi(1 + e)$. It particularly means that $\phi(1 + e) = 2$ at least for one $e \in K^0$. For such an $e \in K$ let us put

$$a = 1 + e, \qquad b = 1 - e, \qquad c = 1 + e^2. \tag{11}$$

Then $\phi(a) = 2$, $\phi(a^2) = \phi(a)^2 = 4$, $\phi(c) \le \phi(1) + \phi(e^2) = 2$. Since $a^2 = c + 2e$, it will be $4 = \phi(a^2) \le \phi(c) + \phi(2e) \le 2 + \phi(2e)$. Hence $\phi(2e) = \phi(c) = 2$. Further, for each $u \in K^0$ it holds $2u = (2e)v$ with $v = e^{-1}u$, so that

$$\phi(2u) = 2, \qquad (u \in K^0). \tag{12}$$

Particularly, $\phi(1 + 1) = \phi(2 \cdot 1) = 2$. Hence $1 \ne -1$. Let us prove that

$$K = \{-1, 0, 1\} \quad \text{and} \quad K^0 = \{-1, 1\}. \tag{13}$$

Let $e \in K^0$ and a, b, c be elements from A given by (11). Then from $ab = 1 - e^2$ it follows $\phi(a)\phi(b) = \phi(ab) = \phi(1 - e^2) \le 2$. Hence $\phi(a) \le 2$ or $\phi(b) \le 2$. Let us prove that $a = 0$ or $b = 0$. If it were $\phi(a) = \phi(b) = 1$, because of (12) and $a^2 - b^2 = 4e = (2 \cdot 1)^2 e$ we would have $4 \le \phi(a^2 - b^2) \le \phi(a^2) + \phi(b^2) \le 2$, a contradiction. Suppose that $\phi(a) = 2$. Then $\phi(b) \le 1$. From $a^2 = c + 2e$ it follows $4 \le \phi(c) + 2 \le 4$. Thus $\phi(c) = 2$. Since $abc = 1 - e^4$ we have $\phi(a)\phi(b)\phi(c) = \phi(1 - e^4) \le 2$. Besides, $\phi(a) = \phi(c) = 2$. Hence $4\phi(b) \le 2$, and thereby $b = 0$. Similarly, if $\phi(b) = 2$, then $a = 0$. Thus (13) is valid.

We denote the sum $r1 = 1 + \cdots + 1$ by $\bar{r}$ $(r \in \mathbb{N})$. By (12), holds

$$\phi(\bar{r}) = r \tag{14}$$

for $r = 2$. Let us prove that (14) is valid for any $r \in \mathbb{N}$. Let $n > 1$ be a given natural number and suppose that (14) is true for each $r < n$. If $n = pq$ $(1 < p, q < n)$, then it will be $\bar{n} = \bar{p}\bar{q}$. Hence $\phi(\bar{n}) = \phi(\bar{p})\phi(\bar{q}) = pq$. Let now n be a prime and $n > 2$. Then $n - 1 = 2p$ and $n + 1 = 2q$ for some natural numbers $p, q < n$. If $m = n^2 - 1$, then $\bar{m} = 4\bar{p}\bar{q}$, $\phi(\bar{p}) = p$, $\phi(\bar{q}) = q$, $\phi(\bar{4}) = \phi(\bar{2})\phi(\bar{2}) = 4$ and $\phi(\bar{n}) \le n$. For $\phi(\bar{n}) < n$, it follows that $\phi(\bar{4})\phi(\bar{p})\phi(\bar{q}) = \phi(\bar{n}^2 - \bar{1}) \le 1 + \phi(\bar{n})^2 \le 1 + (n-1)^2$, that is $n^2 - 1 \le 1 + (n-1)^2$, a contradiction. Thus $\phi(\bar{n}) = n$, and thereby $\phi(m1) = |m|$ for any $m \in \mathbb{Z}$. Hence the characteristic of the ring A is 0.

Finally, let us prove that

$$\phi(a) = r \;\Rightarrow\; a = \pm\bar{r} \tag{15}$$

is valid for each $a \in A$. For $r = 1$ (15) is equivalent to (16). Let $n > 1$ and suppose that (15) holds for any $r < n$. There exist $b, c \in A$ such that $a = \bar{n}b + c$, $\phi(c) < \phi(\bar{n}) = n$. Since $\phi(c) = r < n$, it will be $c = \bar{r}$ or $c = -\bar{r}$. On the other hand, we have $n\phi(b) = \phi(\bar{n})\phi(b) = \phi(nb) = \phi(a - c) \le \phi(a) + \phi(c) = n - r$, that is $\phi(b) \le 1$. If $b = 0$, then $a = c$, i.e. $n = \phi(a) = \phi(c)$, a contradiction. Hence $\phi(b) = 1$, so that from (13) and $a = \bar{n}b + c$ it follows $a = \pm\bar{n} \pm \bar{r}$, that is $n = \phi(a) = |\pm n \pm r|$, and thereby $r = 0$. Thus, we have $a = \bar{n}$ or $a = -\bar{n}$. Hence, by $f(m) = m1$ a ring isomorphism $f \colon \mathbb{Z} \to A$ is defined. Since $\phi \colon f = \nu$, the (right) Euclidean pair (A, ϕ) is isomorphic to the Euclidean pair $(\mathbb{Z}, \nu)$. $\square$

THEOREM 2. *Let $\phi \colon A \to \mathbb{N}_0$ be a monotone right Euclidean algorithm of an integral domain A, satisfying the conditions* (T) *and* (Z). *If $K = U(A)_0$ and $\phi(1) = 1$, then*

1° *If K is not a subfield of the ring A, then the (right) Euclidean pair (A,ϕ) is isomorphic to the Euclidean pair $(\mathbb{Z},\nu)$;*

2° *If K is a subfield of the ring A with at least three elements, then $A=K$;*

3° *If K is a subfield of the ring A with two elements, and algorithm ϕ is two side monotone, then either $A=K$, or the ring A is isomorphic to the ring $B=K[X]$. Besides, the Euclidean pairs (A,ϕ) and (B,σ) are not isomorphic.*

Proof. 1° Since K is not subfield of A, there exist units $u,v\in K^0$ such that $1<\phi(u+v)\le\phi(u)+\phi(v)=2$, that is $\phi(u+v)=2$. Let us put $e=vu^{-1}$ and $a=1+e$, $b=1-e$, $c=1+e^2$. Then $2=\phi(u+v)=\phi[(1+e)u]$, i.e. $\phi(1+e)=\phi(a)$, $\phi(b)\le 2$, $\phi(c)\le 2$. Let us prove that $\phi(2e)=2$. From $\phi(1)<\phi(a)$, by Lemma 1, it follows $2=\phi(a)<\phi(a^2)$. For $2e=0$ we have $a^2=1+e^2$, and thereby $\phi(a^2)\le 2$, a contradiction. Suppose now that $\phi(2e)=1$. Then $3\le\phi(a^2)=\phi(c+2e)\le 1+\phi(c)\le 3$, i.e. $\phi(c)=3$. Since $acb=1-e^4$, we have $\phi(acb)\le 1+\phi(e^4)=2$. For $\phi(acb)=2=\phi(a)$, by the condition (Z), there exists a unit $u\in K^0$ such that $acb=au$. Hence $c\in K^0$, which is contrary to $\phi(c)=2$. Since $\phi(a)=2$, then $\phi(acb)\ne\phi(1)$. Finally, if $\phi(acb)=0$, that is $acb=0$, then $b=0$ since $ac\ne 0$. Hence $e=1$. Then $2=\phi(a)=\phi(2e)$, which is contrary to $\phi(2e)=1$. Thus $\phi(2e)=2$. Let now $u\in K^0$ be any unit of the ring A. If $w=u^{-1}e$, we have $w\in K^0$ and $\phi(2u)=\phi(2uw)=\phi(2e)=2$ for any $u\in K^0$.

Let us put $x=1+1$. Then $\phi(x)=2=\min\phi(A\setminus K)$. Let us prove that it must be $\phi(x^2)=4$. Indeed, since $2=\phi(x)<\phi(x^2)$ and $x^2=1+1+1+1$, we have $3\le\phi(x^2)\le 4$. If $\bar m=m1$ $(m\in\mathbb{Z},\ 1\in A)$, it will be $x^2=\bar 4$. Then $\phi(\bar 3)\le 3$. Since $\phi(\bar 3)\le 1$ implies $\phi(x^2)=\phi(\bar 3+\bar 1)\le 1+1=2$, we conclude that $\phi(\bar 3)\ge 2$. But, if $\phi(\bar 3)=2$, i.e. $\phi(\bar 3)=\phi(\bar 2)$, then there exist a $u\in K^0$ such that $\bar 3=\bar 2u$, i.e. $1=x(u-1)$, which is contrary to $\phi(x)=2$. Hence $\phi(\bar 3)=3$. Analogously we conclude that $\phi(\bar 4)\ne\phi(\bar 3)$. Thus $\phi(x^2)=4$.

Let us prove now that $K^0=\{-1,1\}$. Primarily, $\bar 2\ne 0\ \Rightarrow\ -1\ne 1$. For arbitrary $e\in K^0$ we put: $a=1+e$, $b=1-e$, $c=1+e^2$. Then $a=0$ or $b=0$, and thereby $e=1$ or $e=-1$. Namely, at first $\phi(a),\phi(b),\phi(c)\le 2$. Since $4=\phi(\bar 4)=\phi(4e)=\phi(a^2-b^2)\le\phi(a^2)+\phi(b^2)$, we conclude that $\phi(a)\ne 1$ or $\phi(b)\ne 1$. If $\phi(a)=\phi(b)=2$, then $b=au$ for some $u\in K^0$, and thereby $1-e^2=ab=a^2u$. It means that $\phi(a^2)=\phi(a^2u)=\phi(1-e^2)\le 2$, which is contrary to $\phi(a^2)>\phi(a)=2$. Finally, assume that $\phi(a)=2$ and $\phi(b)\le 1$. Then, for some u from K^0 we have $a=\bar 2u=2u$, so that $\phi(a^2)=\phi(4u^2)=\phi(\bar 4)=\phi(x^2)=4$. Hence $4=\phi(a^2)=\phi(c+2e)\le\phi(c)+\phi(2e)=2+\phi(c)\le 4$. Thus $\phi(c)=2)$. On the other hand we have $\phi(acb)=\phi(1-e^4)\le 2$. If $\phi(acb)=2=\phi(a)$, then there exists $u\in K^0$ such that $acb=au$, that is $c\in K^0$, which is contrary to $\phi(c)=2$. Similarly, $\phi(a)=2)$ implies that $\phi(acb)\ne 1$. Hence $acb=0$, that is $b=0$ (because of $ac\ne 0$). Thus $e=1$. Similarly, for $\phi(a)\le 1$ and $\phi(b)=2$ we have $e=-1$, so that $K^0=\{-1,1\}$.

Now, by the condition (Z), for any $m,n\in\mathbb{Z}$ we have $\phi(\bar m)=\phi(\bar n)$ if and only if $\bar m=\bar n$ or $\bar m=-\bar n$. Hence: $\phi(\bar m)=\phi(\bar n)\ \Leftrightarrow\ m=n\vee m=-n$. Namely, the characteristic p of the ring A is not 2. If $p > 2$, then we have $x = 1 + 1 = 1^p + 1^p = (1+1)^p = x^p$, that is $x^{p-2}x = 1$, and thus $x \in K^0$, which is not true. Thus $p = 0$. Hence $\bar{m} = \bar{n} \Leftrightarrow m = n \vee m = -n$. Now, by induction on n, we conclude that $\phi(\bar{n}) = n$ $(n \in \mathbb{N})$ is valid. It is clear that for each $m \in \mathbb{Z}$ the following holds: $\phi(\bar{m}) = |m|$, i.e. $\phi(\bar{m}) = \nu(m)$.

Finally, let $a \in A$ and let us put $\phi(a) = n$. Since $\phi(\bar{n}) = n$, for some unit $u \in K^0$ then $a = \bar{n}u$. Hence $a = \bar{n}$ or $a = -\bar{n}$. Thus, by $f(m) = \bar{m}$ is defined a ring isomorphism $f\colon \mathbb{Z} \to A$, and since $\phi\colon f = \nu$ is valid, the (right) Euclidean pair (A, ϕ) is isomorphic to the Euclidean pair $(\mathbb{Z}, \nu)$.

2° Let 1 and e be different units of the ring A. Suppose that $A = K$ is not true. We denote by x any element from A such that $\phi(x) = \min \phi(A \setminus K)$. Since ϕ satisfies the condition (T), we have

$$\phi(1 + x) \leq 1 + \phi(x). \tag{14}$$

Assume that $\phi(1+x) = \phi(x)$. Then, by the condition (Z), for some $u \in K^0$ we have $1 + x = xu$. Hence $x(u-1) = 1$, that is $x \in K^0$, which is contrary to $x \in A \setminus K$. If $\phi(1+x) < \phi(x)$, then $\phi(1+x) \leq \phi(1)$, i.e. $1+x \in K$, which is not possible because of $x \notin K$. Thus $\phi(1+x) \geq \phi(x)$, which with (14) gives $\phi(1+x) = 1 + \phi(x)$. It is clear that $\phi(1+x) = 1 + \phi(xv)$ $(v \in K^0)$ is also valid. Hence for any $u \in K^0$ and $v = u^{-1}$ holds $u + x = (1 + xv)u$ and

$$\phi(u + x) \;=\; \phi(1 + xv) \;=\; 1 + \phi(xv) \;=\; 1 + \phi(x). \tag{15}$$

From (15) it follows that $\phi(1 + x) = \phi(e + x)$, that is $e + x = (1 + x)w$ for some $w \in K^0$. Since $1 \neq e$, we have $w \neq 1$. Hence $w - e \in K^0$, that is $x(1 + w) \in K^0$, which is contrary to $x \in A \setminus K$. Thus $A = K$.

3° From $K^0 = \{1\}$, by (Z), it follows that the mapping $\phi\colon A \to \mathbb{N}_0$ is an injection. Since $1 + 1 = 0$, the characteristic of the ring A is 2. Assume that $A \neq K$ and let $x \in A \setminus K$ such that $\phi(x) = \min \phi(A \setminus K)$. Similarly as in the proof of the assertion 2°, we conclude that

$$\phi(1 + x) = 1 + \phi(x). \tag{16}$$

Let $a \in A$. Then there exist $c, r \in A$ such that $a = cx + r$, $\phi(r) < \phi(x)$. From $\phi(r) < \phi(x)$ it follows that $r \in K$. Since the algorithm ϕ is two side monotone, we have

$$\phi(c) \;\leq\; \phi(xc) \;=\; \phi(a - r) \;\leq\; \phi(a) + \phi(r) \;\leq\; 1 + \phi(a).$$

Suppose that $\phi(a) \geq \phi(x)$. Then $c \neq 0$. If $\phi(c) = \phi(xc)$, it will be $c = xc$, that is $x = 1$, a contradiction. Hence $\phi(c) < \phi(xc) \leq 1 + \phi(a)$, i.e. $\phi(c) \leq \phi(a)$. Since $\phi(c) = \phi(a)$ implies $\phi(r) = \phi[(1 - xu)a] \geq \phi(a)$, we conclude that $\phi(c) < \phi(a)$. Thus, for any $a \in A^0$ there exist $c, r \in A$ such that $a = xc+r$, $r \in K$, $\phi(c) < \phi(a)$. Hence, by induction on $n = \phi(a)$, it follows that any element $a \in A$ is expressible in the form

$$a = x^n a_n + \cdots + x a_1 + a_0 \;\; (a_r \in K,\, n \in \mathbb{N}_0). \tag{17}$$

Since K is subfield of the ring A, by (16) we conclude that each $a \in A$ is uniquely expressible in the form (17). Let $B = K[X]$. Hence by

$$F(a_0 + xa_1 + \cdots + x^n a_n) = a_0 + Xa_1 + \cdots + X^n a_n$$

is defined a ring isomorphism $F: A \to B$. However, the Euclidean pairs (A, ϕ) and (B, σ) are not isomorphic. Indeed, suppose that for some isomorphism $f: A \to B$ and some monomorphism h of the well ordered set $\phi(A)$ into the well ordered set $\sigma(B)$ we have $\sigma \circ f = h \circ \phi$. Since x is not a unit in the ring A, $p = f(x)$ is not a unit in the ring B. Hence for such a p we have $\sigma(1 + p) = \sigma(p)$, so that $(\sigma \circ f)(1 + x) = (\sigma \circ f)(x)$, i.e. $(h \circ \phi)(1 + x) = (h \circ \phi)(x)$. Since h is an injection, it follows that $\phi(1 + x) = \phi(x)$, which is contrary to (16). $\square$

Example 1. Let $K = \{0, 1\}$ be a field of two elements and $A = K[X]$. If $a \in K$, then let $\tilde{a}$ denote the integer 0 for $a = 0$, and the integer 1 for $a = 1$. Then the mapping $\phi: A \to \mathbb{N}_0$ defined by

$$\phi(a_0 + Xa_1 + \cdots + X^n a_n) = \tilde{a}_0 + 2\tilde{a}_1 + \cdots + 2^n \tilde{a}_n$$

is an Euclidean algorithm of the ring A, satisfying the conditions 3° of Theorem 2. Indeed, let σ be a degree algorithm of A. Since $\phi(a_0 + \cdots + X^n a_n) < 2^{n+1}$, then, for $a, b \in A$ we have $\phi(a) < \phi(b)$, if and only if $\sigma(a) < \sigma(b)$. Hence the function ϕ is also an Euclidean algorithm of A. Since each $m \in \mathbb{N}_0$ is uniquely expressible in the form $m = \tilde{a}_0 + \cdots + 2^n \tilde{a}_n$, where $\tilde{a}_r \in \{0, 1\}$, it follows that ϕ is an injection. Besides, $K^0 = \{1\}$, so the algorithm ϕ satisfies the condition (Z). Further, since for $u, v \in A$ and $w = u + v$ holds $\tilde{w} \le \tilde{u} + \tilde{v}$, we conclude that $\phi(a + b) \le \phi(a) + \phi(b)$ $(a, b \in A)$. Thus the algorithm ϕ also satisfies the condition (T).

THEOREM 3. *If for a ring A there exists a mapping $\phi: A \to \mathbb{N}_0$ satisfying the conditions* (T), (N) *and* (Z)*, then A is either field, or (A, ϕ) is an Euclidean pair isomorphic to Euclidean pair $(\mathbb{Z}, \nu)$.*

Proof. By the condition (Z) we have $\phi(0) \ne \phi(1)$, so that the mapping ϕ is not constant. Since $\phi(a) = \phi(a1) = \phi(a) \cdot \phi(1)$, it must be $\phi(1) = 1$. Now $\phi(0) = \phi(0)\phi(0)$ implies $\phi(0) = 0$, and hence $\phi(a) = 0 \Leftrightarrow a = 0$. Further, by the condition (Z) holds $\phi(a) = \phi(1) \Leftrightarrow a \in K^0$, where $K = U(A)_0$. Finally, since ϕ satisfies condition (N), we conclude that A is an integral domain, that $\phi(ab) \ge \phi(a), \phi(b)$, and that, $\phi(a^n) < \phi(a^{n+1})$ for $\phi(a) > 1$.

If K is subfield of A, then $A = K$. Namely, in the case that K has at least three elements, similarly as in the proof of Theorem 2 under 2°, we conclude that $A \setminus K = \varnothing$. Suppose now that $K = \{0, 1\}$ and $A \setminus K \ne \varnothing$. If $x \in A$ and $\phi(x) = \min \phi(A \setminus K)$, similarly as in the proof of Theorem 2 under 3° we get $\phi(1 + x) = 1 + \phi(x)$. Hence, by the condition (N), for $\phi(x) = n$ we have $\phi[(1 + x)^2] = [\phi(1 + x)]^2 = [1 + \phi(x)]^2 = (1 + n)^2$. On the other hand, by the condition (T), we have $\phi[(1 + x)^2] = \phi(1 + x^2) \le 1 + \phi(x^2) = 1 + n^2$. Hence $(1 + n)^2 \le 1 + n^2$, i.e. $\phi(x) = n = 0$, a contradiction. Thus $A = K$.

Suppose now that K is not a subfield of A. Similarly as in the proof of Theorem 1 we conclude that $K^0 = \{-1, 1\}$, with $-1 \ne 1$, and that $\phi(m1) = |m|$

for every $m \in \mathbb{Z}$. Hence for every $a \in A$ and $\phi(a) = n$ we have $\phi(a) = \phi(n1)$, so that $a = n1$ or $a = -n1$ by condition (Z). Therefore $A = \{m1\colon\ m \in \mathbb{Z}\}$, and since the characteristic of the ring A is 0, we conclude that the Euclidean pair (A, ϕ) is isomorphic to the Euclidean pair $(\mathbb{Z}, \nu)$. $\square$

REFERENCES

[1] P.M. Cohn, *On a generalization of the Euclidean algorithm*, Proc. Cambridge Phil. Soc. **57** (1961), 18–30.

[2] P.M. Cohn, *Ring with a transfinite weak algorithm*, Bull. London Math. Soc. **1** (1969), 55–59.

[3] P.M. Cohn, *Free Rings and their Relations*, London – New York, 1971.

[4] A.V. Jategaonkar, *Left Principal Ideal Rings*, Lecture Notes in Mathematics. No. 123, Springer-Verlag, Berlin, 1970.

[5] P. Samuel, *About Euclidean Rings*, J. Algebra **19** (1971), 282–301.

Matematički fakultet
Studentski trg 16
11000 Beograd, p.p. 550
Yugoslavia

(Received 01 02 1995)