Leu, M.-G.
Osaka J. Math.
45 (2008), 807–818

THE RESTRICTED NAGATA'S PAIRWISE ALGORITHM AND THE EUCLIDEAN ALGORITHM

Dedicated to Professor Takashi Ono on his eightieth birthday

MING-GUANG LEU

(Received August 16, 2007)

Abstract

In 1971, Samuel generalized Motzkin's idea to give a characterization of Euclidean rings. In this article we will show, from Motzkin and Samuel's point of view, that the concept of the restricted Nagata's pairwise algorithm should exist in the world of mathematics much earlier than the Euclidean algorithm.

1. Introduction

A Euclidean ring is a ring with a kind of Euclidean algorithm. There are several definitions of Euclidean rings which are mutually different (see [6]). In Section 2 we will introduce a definition of Euclidean rings due to Samuel [9]. In [9], Samuel generalized Motzkin's idea [4] to give an 'internal' characterization of Euclidean rings (see Proposition 2.1). In Section 3 we will introduce the concept of the pairwise algorithm due to Nagata [7]. In his papers, Nagata [7, 8] constructed a pairwise algorithm for $\mathbb{Z}[\sqrt{14}]$, the ring of integers of $\mathbb{Q}(\sqrt{14})$, but he did not mention much about the relation between pairwise algorithms and Euclidean algorithms. Inspired by the paper [9] of Samuel, Chen and Leu [1] derived some properties of a ring with a pairwise algorithm. In Section 4 we will build an unexpected genetic relation between pairwise algorithms and Euclidean algorithms so that, from Motzkin and Samuel's point of view, the concept of the restricted Nagata's pairwise algorithm is not only a generalization but also a longtime undiscovered ancestor of the Euclidean algorithm. In Section 5 we propose problems which are related to the class number of a number field and the k-stage Euclidean algorithm respectively.

In this article, a ring E means a commutative ring with identity 1_E.

2. The Euclidean algorithm

In this article we adopt the following definition of Euclidean rings due to Samuel [9].

2000 Mathematics Subject Classification. Primary 13F07; Secondary 11R04.

This research is supported in part by grant NSC 94-2115-M-008-006 of the National Science Council of the Republic of China (Taiwan).

DEFINITION 1. Given a ring E, a Euclidean algorithm in E is a map ϕ of $E \setminus \{0\}$ into a well-ordered set W such that for any $a, b \in E$ with $b \neq 0$, there exist q and r in E such that

$$a = qb + r \quad \text{with either} \quad r = 0 \quad \text{or} \quad \phi(r) < \phi(b).$$

We say that E is Euclidean if it admits a Euclidean algorithm ϕ.

NOTE. For a Euclidean algorithm ϕ on a ring E to be compatible with a Nagata's pairwise algorithm defined in Section 3, it is a good idea to define $\phi(0) > \phi(b)$ for all non-zero b in E.

Proposition (Samuel [9]). *Let E be a Euclidean ring for a Euclidean algorithm ϕ. Then*
(1) *E is a principal ideal ring.*
(2) *ϕ_1 is a Euclidean algorithm on E and $\phi_1(ac) \geq \phi_1(a)$ for $ac \neq 0$, where ϕ_1 is defined by $\phi_1(a) = \inf_{b \in aE \setminus \{0\}} \phi(b)$ for all non-zero a in E.*

REMARK 1. The above proposition shows that Samuel's definition of a Euclidean ring is a generalization of classical definitions of Euclidean rings.

REMARK 2. Nagata [5] constructed a Euclidean ring E with the properties: (1) E is an integral domain; (2) there does not exist a Euclidean algorithm of $E \setminus \{0\}$ into the set of natural numbers. Thus, Nagata constructed an integral domain E which satisfies Samuel's definition of a Euclidean ring, but E does not satisfy the classical definitions of Euclidean rings.

In [9], Samuel generalized Motzkin's idea [4] to introduce the transfinite construction of the Motzkin sets:

DEFINITION 2. Let E be a ring, and W an ordinal such that $\text{card}(E) < \text{card}(W)$. We set $E_0 = \{0\}$. For $\alpha > 0$ in W, we define the Motzkin set E_α by transfinite induction as follows: the set $E_\alpha{}' = \bigcup_{\beta<\alpha} E_\beta$ is already defined and E_α is the union of $\{0\}$ and the set of all $b \in E$ such that the canonical map $E_\alpha{}' \to E/bE$ is surjective. Define $E_W = \bigcup_{\alpha \in W} E_\alpha$.

Proposition 2.1. *A ring E is Euclidean if and only if $E_W = E$, where W is an ordinal such that* $\text{card}(E) < \text{card}(W)$.

Proof. See Proposition 10 and p.289 of Samuel [9] for a proof. □

NOTE. In Section 4 we will show that there exists surprisingly an analog of Proposition 2.1 for the restricted Nagata's pairwise algorithm (see Corollary 4.9).

3. The Nagata's pairwise algorithm

The following definition of a pairwise algorithm is equivalent to the one given by Nagata [7] (cf. [1, Proposition 2]):

DEFINITION 3. Let E be a ring and W a well-ordered set. We say that a mapping ρ from $E \times E$ into W gives E a Nagata's pairwise algorithm if and only if ρ satisfies the following conditions:
(1) If $a, b \in E$ and $u, v \in E^*$, then $\rho(au, bv) = \rho(a, b)$, where E^* is the unit group of E.
(2) If $b \in aE$ and $b \notin aE^* = \{ae \mid e \in E^*\}$, then $\rho(a, a) < \rho(b, b)$.
(3) If $b - c \in aE$, then $\rho(a, b) = \rho(a, c)$.
(4) For each pair (a, b) in $E \times E$, there are $q, r \in E$ so that $b = qa + r$ with either $r = a$ or $\rho(r, a) < \rho(a, b)$.

The following Remarks 3 and 4 are due to Nagata [7].

REMARK 3. If a ring E admits a Nagata's pairwise algorithm, then E is a principal ideal ring.

REMARK 4. If E is a Euclidean ring under a Euclidean algorithm ϕ to a well-ordered set W, then one can give a Nagata's pairwise algorithm ψ on E by defining that $\psi(a, b) = \min\{\phi(au) \mid u \in E^*\}$.

REMARK 5. It is known that a principal ideal ring is a finite product of principal ideal domains and of principal ideal rings with a unique and nilpotent maximal ideal (cf. [12, Chapter 4, Section 15, Theorem 33]). Further, by [9, p.286], a principal ideal ring with a unique and nilpotent maximal ideal is a Euclidean ring. Therefore, by Theorem 4.10 below, we need only to focus our attention on principal ideal domains.

Proposition 3.1. *Let $\rho\colon E \times E \to W$ be a Nagata's pairwise algorithm on a ring E. Then $\rho(1_E, 1_E) < \rho(a, b)$ for $a \notin E^*$ and $b \in E$.*

Proof. By Lemma 1 of [1] and the definition of a Nagata's pairwise algorithm, we have that $\rho(1_E, 1_E) = \min\{\rho(x, y) \mid x, y \in E\}$ and $\rho(1_E, 1_E) < \rho(a, a) = \rho(a, b)$ for $a \notin E^*$ and $b \in aE$. For the case $b \notin aE$, there exist $q, r \in E$, $r \neq 0$ such that $b = qa + r$ and $\rho(r, a) < \rho(a, b)$, thus $\rho(1_E, 1_E) \leq \rho(r, a) < \rho(a, b)$.
The proposition is proved. □

4. The restricted Nagata's pairwise algorithm

To point out that Nagata's pairwise algorithms have deep relation to Euclidean algorithms, let us consider the following special case of the Nagata's pairwise algorithm:

DEFINITION 4. Let E be a ring and W a well-ordered set. We say that a mapping ρ from $E \times E$ into W gives E a restricted Nagata's pairwise algorithm if and only if ρ is a Nagata's pairwise algorithm on E satisfying an extra condition:
(5) For b coprime to a, $\rho(a, b) = \rho(a, 1_E)$. (Note that, in a principal ideal ring E, a greatest common divisor of $\{a, b\}$ always exists.)

REMARK 6. If E is a Euclidean ring for ϕ, then the Nagata's pairwise algorithm ψ, induced by ϕ as in Remark 4, is a restricted Nagata's pairwise algorithm on E.

Proposition 4.1. *Let E, A, and B be rings such that $E = A \times B$. If A and B admit a restricted Nagata's pairwise algorithm respectively, then E admits a restricted Nagata's pairwise algorithm.*

Proof. If $\rho_1 : A \times A \to W_1$ and $\rho_2 : B \times B \to W_2$ give A and B a restricted Nagata's pairwise algorithm respectively, then, by Propositions 2 and 5 of [1], the mapping $\rho((a_1, b_1), (a_2, b_2)) = (\rho_1(a_1, a_2), \rho_2(b_1, b_2))$ for $(a_1, b_1), (a_2, b_2) \in E$ induces a restricted Nagata's pairwise algorithm on E. □

REMARK 7. Later in Proposition 4.8 we will prove that the converse of Proposition 4.1 also holds.

Two Nagata's pairwise algorithms $\rho : E \times E \to W$, $\rho' : E \times E \to W'$ on a ring E are said to be isomorphic if there exists an order-isomorphism h: $\rho(E \times E) \to \rho'(E \times E)$ such that $\rho' = h \circ \rho$. It is easy to see that isomorphic Nagata's pairwise algorithms have the same properties. Thus, since all well-ordered sets with cardinal $\leq \text{card}(E \times E)$ are order isomorphic to proper initial segments of any well-ordered set W such that $\text{card}(W) > \text{card}(E \times E)$ (see Corollary 7.1.1 (d) and Theorem 7.1.2 of [10]), all the Nagata's pairwise algorithms on the ring E may be constructed to take their values in the fixed well-ordered set W. For precision sake, we may assume that W is an ordinal, with elements customarily denoted by $0, 1, 2, 3, \ldots, \omega, \omega + 1, \ldots, 2\omega, \ldots$, and $\text{card}(E \times E) < \text{card}(W)$.

As an immediate consequence of Proposition 4 of [1], we have the following proposition.

Proposition 4.2. *If $\rho_\alpha : E \times E \to W$ is any nonempty family of restricted Nagata's pairwise algorithms on a ring E, then $\rho = \inf_\alpha \rho_\alpha$ is also a restricted Nagata's pairwise algorithm on E.*

Proposition 4.2 shows that if a ring E admits a restricted Nagata's pairwise algorithm, then E admits a smallest restricted Nagata's pairwise algorithm θ (i.e. the infimum of all restricted Nagata's pairwise algorithms).

Theorem 4.3. *Let $\theta\colon E \times E \to W$ be the smallest restricted Nagata's pairwise algorithm on a ring E. For $\alpha \in W$ set $\hat{E}_\alpha = \hat{E}_{-1} \cup \{a \in E \setminus \{0\} \mid \theta(a, 1_E) \leq \alpha\}$, $\hat{E}'_\alpha = \hat{E}_{-1} \cup \{a \in E \setminus \{0\} \mid \theta(a, 1_E) < \alpha\}$ and $\tilde{E}_\alpha$ be the union of $\tilde{E}_{-1}$ and the set of all $a \in E \setminus \{0\}$ such that $(E/aE)^* \subseteq \pi_a(\tilde{E}'_\alpha)$, where $(E/aE)^*$ is the unit group of E/aE, $\hat{E}_{-1} = \tilde{E}_{-1} = \{0\}$, $\tilde{E}'_\alpha = \bigcup_{\beta<\alpha} \tilde{E}_\beta$ (set $-1 < \alpha$ for every $\alpha \in W$ and $\beta \in \{-1\} \cup W$), and $\pi_a\colon \tilde{E}'_\alpha \to E/aE$ is the canonical map. Then $\hat{E}_\alpha = \tilde{E}_\alpha$ for all $\alpha \in W$.*

Proof. By Proposition 3.1, we know that $\hat{E}_0 = \tilde{E}_0 = \{0\} \cup E^*$. For $\alpha \neq 0$ in W, assuming $\hat{E}_\beta = \tilde{E}_\beta$ for all $\beta < \alpha$ in W, we want to prove that $\hat{E}_\alpha = \tilde{E}_\alpha$.

For nonzero nonunit $a \in \hat{E}_\alpha$, if $b + aE$ is any coprime residue class modulo aE, then, by writing $b = qa + r$, we find a representative r of this class such that $\theta(r, a) < \theta(a, b) = \theta(a, 1_E) \leq \alpha$, thus $r \in \hat{E}'_\alpha = \bigcup_{\beta<\alpha} \hat{E}_\beta = \tilde{E}'_\alpha$. This implies that $\hat{E}_\alpha \subseteq \tilde{E}_\alpha$. Conversely consider nonzero nonunit $a \in \tilde{E}_\alpha$ and suppose that $\theta(a, 1_E) > \alpha$. Now define $\theta_1\colon E \times E \to W$ by

$$\theta_1(x, y) = \begin{cases} \alpha, & \text{if } \ x \in aE^* \text{ and } y \text{ coprime to } x; \\ \theta(x, y), & \text{otherwise.} \end{cases}$$

We claim that θ_1 is a restricted Nagata's pairwise algorithm: It is obvious that θ_1 satisfies the conditions (1), (2), (3) and (5) of Definitions 3 and 4. As for the condition (4) of Definition 3, we divide the arguments into three cases.

CASE 1. For $y \in E$ and y coprime to a. Since $a \in \tilde{E}_\alpha$, so there exist q in E and nonzero r in $\tilde{E}'_\alpha$ such that $y = qa + r$ and $\theta_1(r, a) = \theta(r, a) < \alpha = \theta_1(a, y)$.

CASE 2. For $y \in E$ and y not coprime to a. Then there exist q and r in E such that $y = qa + r$ with either $r = a$ or $\theta_1(r, a) = \theta(r, a) < \theta(a, y) = \theta_1(a, y)$.

CASE 3. For $x, y \in E$ and $x \notin aE^*$. Then there exist q and r in E such that $y = qx + r$ with either $r = x$ or $\theta(r, x) < \theta(x, y) = \theta_1(x, y)$. For the case $r \neq x$, we divide the arguments into three subcases.

SUBCASE 3.1. $r \notin aE^*$. Then $\theta_1(r, x) = \theta(r, x) < \theta(x, y) = \theta_1(x, y)$.

SUBCASE 3.2. $r \in aE^*$ and x coprime to r. In this case we still have $\theta_1(r, x) = \alpha < \theta(r, x) < \theta(x, y) = \theta_1(x, y)$.

SUBCASE 3.3. $r \in aE^*$ and x not coprime to r. Then $\theta_1(r, x) = \theta(r, x) < \theta(x, y) = \theta_1(x, y)$.

Thus θ_1 is indeed a restricted Nagata's pairwise algorithm on E. This contradicts the fact that θ is the smallest restricted Nagata's pairwise algorithm. Therefore we have $\theta(a, 1_E) \leq \alpha$, that is $a \in \hat{E}_\alpha$. We conclude that $\hat{E}_\alpha = \tilde{E}_\alpha$. □

REMARK 8. Theorem 4.3 on restricted Nagata's pairwise algorithms is an analog of Proposition 10 of [9] on Euclidean algorithms.

The transfinite construction described in Theorem 4.3 may be performed in any ring E. More precisely,

The transfinite construction. Let E be a ring and W an ordinal such that $\mathrm{card}(E \times E) < \mathrm{card}(W)$. We set $\tilde{E}_{-1} = \{0\}$ and $-1 < \alpha$ for every α in W. For α in W, we define $\tilde{E}_\alpha$ by transfinite induction as follows: the set $\tilde{E}'_\alpha = \bigcup_{\beta<\alpha} \tilde{E}_\beta$ (where $\beta \in \{-1\} \cup W$) is already defined and $\tilde{E}_\alpha$ is the union of $\{0\}$ and the set of all $a \in E$ such that $(E/aE)^\circ \subseteq \pi_a(\tilde{E}'_\alpha)$, where $\pi_a\colon \tilde{E}'_\alpha \to E/aE$ is the canonical map and $(E/aE)^\circ$ is the set of all distinct cosets $b + aE$ with b coprime to a.

It is clear that the sequence $(\tilde{E}_\alpha)_{\alpha\in W}$ is increasing and $\bigcup_{\alpha\in W} \tilde{E}_\alpha \supseteq \bigcup_{\alpha\in W} E_\alpha$. To experience the relation between $\tilde{E}_\alpha$ and the Motzkin set E_α, let $E = \mathbb{Z}/8\mathbb{Z} = \{[0], [1], [2], \ldots, [7]\}$ be the ring of $\mathbb{Z}$ modulo $8\mathbb{Z}$. Then $\tilde{E}_{-1} = E_0 = \{[0]\}$, $\tilde{E}_0 = E_1 = \{[0]\} \cup E^*$, $\tilde{E}_1 = E \supsetneqq E_2 = E \setminus \{[4]\}$, $E_3 = E$. The advantage of $\tilde{E}_\alpha$ revealed in this simple example is one step earlier than the Motzkin set E_α to exhaust the ring E.

Back to $\tilde{E}_\alpha$, as a consequence of Theorem 4.3, we have:

Corollary 4.4. *If a ring E admits a restricted Nagata's pairwise algorithm, then the sequence $(\tilde{E}_\alpha)_{\alpha\in W}$ exhausts the ring E.*

Proof. For nonzero a in E, say $\theta(a, 1_E) = \alpha$, where θ is the smallest restricted Nagata's pairwise algorithm from $E \times E$ into W. Then, by Theorem 4.3, $a \in \tilde{E}_\alpha$, whence $E = \bigcup_{\alpha\in W} \tilde{E}_\alpha$. □

Theorem 4.5. *Let E be a unique factorization domain (UFD). Then E admits a restricted Nagata's pairwise algorithm if and only if the sequence $(\tilde{E}_\alpha)_{\alpha\in W}$ exhausts the ring E, where W is an ordinal such that* $\mathrm{card}(E \times E) < \mathrm{card}(W)$.

Proof. If E admits a restricted Nagata's pairwise algorithm, then, by Corollary 4.4, $E = \bigcup_{\alpha\in W} \tilde{E}_\alpha$.

Conversely if $E = \bigcup_{\alpha\in W} \tilde{E}_\alpha$, then we define a map $\rho\colon E \times E \to W$ as follows:

(i) For α in W, if $a \in \tilde{E}_\alpha \setminus \tilde{E}'_\alpha$ and $b \in E$, which is coprime to a, we define $\rho(a, b) = \alpha$.

(ii) For nonzero nonunit element a in E and $b \in aE$, write $a = p_1 p_2 \cdots p_t$, where $p_1, p_2, \ldots, p_t$ are irreducible. We define $\rho(a, b) = t$.

(iii) We define

$$\rho(0, b) = \begin{cases} \omega, & \text{if} \quad b = 0; \\ t + 1, & \text{if} \quad b = uq_1 \cdots q_t, \end{cases}$$

where ω denotes the first transfinite ordinal, $u \in E^*$ and $q_1, \ldots, q_t$ irreducible elements of E. If $b \in E^*$, then $\rho(0, b) = 1$.

(iv) For nonzero elements a, b in E, which have a greatest common divisor s, we define $\rho(a, b) = \rho(a', b') + \rho(s, s)$, where $a', b' \in E$ such that $a = a's$ and $b = b's$. (For α, not a last, in W, $\alpha + 1$ is the immediate successor of α.)

Now we claim that ρ is a restricted Nagata's pairwise algorithm: First it is easy to verify that ρ satisfies the conditions (1), (2), (3) of Definition 3 and the condition (5)

of Definition 4. To verify that ρ satisfies the condition (4) of Definition 3, we divide the arguments into four cases.

For each pair (a, b) in $E \times E$:

CASE 1. If $b \in aE$, then $b = qa + a$ for some $q \in E$.

CASE 2. If $a = 0$ and $b \neq 0$, then we have $b = 0 + b$ with $\rho(b, 0) < \rho(0, b)$.

CASE 3. If a is a nonzero nonunit element, b coprime to a, and $a \in \tilde{E}_\alpha \setminus \tilde{E}'_\alpha$, then there exist $q, r \in E$ such that $b = qa + r$ with nonzero $r \in \tilde{E}'_\alpha$, whence we have $\rho(r, a) < \alpha = \rho(a, b)$.

CASE 4. If a is a nonzero nonunit element, and $s \notin aE^*$, a greatest common divisor of $\{a, b\}$, then $a = a's$ and $b = b's$ for some a', b' in E, which are relatively prime. Thus, as in Case 3, there exist $q, r' \in E$ such that $b' = qa' + r'$ and $\rho(r', a') < \rho(a', b')$. This implies that $\rho(r's, a's) = \rho(r', a') + \rho(s, s) < \rho(a', b') + \rho(s, s) = \rho(a, b)$. Hence there exist $q, r = r's$ in E such that $b = b's = qa's + r's$ with $\rho(r, a) = \rho(r's, a's) < \rho(a, b)$.

Indeed, ρ is a restricted Nagata's pairwise algorithm on E. □

Proposition 4.6. *Let E, A, and B be rings such that $E = A \times B$, W an ordinal such that* $\mathrm{card}(E \times E) < \mathrm{card}(W)$. *Then $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$ implies $A = \bigcup_{\alpha \in W} \tilde{A}_\alpha$ and $B = \bigcup_{\alpha \in W} \tilde{B}_\alpha$.*

Proof. Let $p_A : A \times B \to A$ given by $p_A(a, b) = a$ be the canonical projection. Set $\bar{A}_\beta = p_A(\tilde{E}_\beta)$ for all $\beta \in \{-1\} \cup W$. Then it is clear that the sequence $(\bar{A}_\alpha)_{\alpha \in W}$ is increasing. Since $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$, it is obvious that $A = \bigcup_{\alpha \in W} \bar{A}_\alpha$.

We claim by induction that $\bar{A}_\alpha \subseteq \tilde{A}_\alpha$ for every $\alpha \in W$. For $\alpha = 0$, it is clear that $\bar{A}_0 = \tilde{A}_0 = \{0\} \cup A^*$, where A^* is the unit group of A. For $\alpha \neq 0$ in W, assume that $\bar{A}_\beta \subseteq \tilde{A}_\beta$ for all $\beta < \alpha$. We want to prove that $\bar{A}_\alpha \subseteq \tilde{A}_\alpha$. Set $\bar{A}'_\alpha = \bigcup_{\beta < \alpha} \bar{A}_\beta$. For $a \neq 0$ in $\bar{A}_\alpha$, there exists $x \in B$ such that $(a, x) \in \tilde{E}_\alpha$. That means $\pi_{(a,x)}(\tilde{E}'_\alpha) \supseteq (E/(a, x)E)^\circ = (A/aA)^\circ \times (B/xB)^\circ$. This implies that $\pi_a(\bar{A}'_\alpha) \supseteq (A/aA)^\circ$. Since $\bar{A}'_\alpha \subseteq \tilde{A}'_\alpha = \bigcup_{\beta < \alpha} \tilde{A}_\beta$, we obtain that $\pi_a(\tilde{A}'_\alpha) \supseteq (A/aA)^\circ$, whence $a \in \tilde{A}_\alpha$. Thus $\bar{A}_\alpha \subseteq \tilde{A}_\alpha$. We conclude that $A = \bigcup_{\alpha \in W} \tilde{A}_\alpha$.

Similarly, we also have that $B = \bigcup_{\alpha \in W} \tilde{B}_\alpha$. □

Corollary 4.7. *Let E, A, and B be rings with A being a UFD, but not a PID, such that $E = A \times B$, W an ordinal such that* $\mathrm{card}(E \times E) < \mathrm{card}(W)$. *Then $E \neq \bigcup_{\alpha \in W} \tilde{E}_\alpha$.*

Proof. If $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$, then, by Proposition 4.6, Theorem 4.5 and Remark 3, A is a principal ideal domain (PID), which is a contradiction. Hence we have $E \neq \bigcup_{\alpha \in W} \tilde{E}_\alpha$. □

Now we are ready to prove the converse of Proposition 4.1.

Proposition 4.8. *Let E, A, and B be rings such that $E = A \times B$. If E admits a restricted Nagata's pairwise algorithm, then A and B admit a restricted Nagata's pairwise algorithm respectively.*

Proof. By Remark 3 we know that E is a principal ideal ring, whence A and B are also principal ideal rings. Let W be an ordinal such that $\mathrm{card}(E \times E) < \mathrm{card}(W)$. Then, by Corollary 4.4 and Proposition 4.6, we have $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$, $A = \bigcup_{\alpha \in W} \tilde{A}_\alpha$ and $B = \bigcup_{\alpha \in W} \tilde{B}_\alpha$ respectively. Now following the steps indicated in order by Remarks 5 and 6, Proposition 4.6, Theorem 4.5, and Proposition 4.1, we obtain that A and B admit a restricted Nagata's pairwise algorithm respectively. □

From the proof of Proposition 4.8 and by Corollary 4.4, we obtain immediately the following 'internal' characterization of a ring admitting a restricted Nagata's pairwise algorithm.

Corollary 4.9. *Let E be a principal ideal ring and W an ordinal such that $\mathrm{card}(E \times E) < \mathrm{card}(W)$. Then $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$ if and only if E admits a restricted Nagata's pairwise algorithm.*

Bringing Propositions 4.1 and 4.8 together and applying induction, we have the following:

Theorem 4.10. *Let $E, A_1, \ldots, A_n$ be rings such that $E = A_1 \times \cdots \times A_n$. Then E admits a restricted Nagata's pairwise algorithm if and only if A_i admits a restricted Nagata's pairwise algorithm for $i = 1, 2, \ldots, n$.*

To determine which rings of integers in imaginary quadratic fields admit a restricted Nagata's pairwise algorithm, we need the following lemma.

Lemma 4.11. *Let E be a PID and a, b nonzero nonunit elements in E. If $\pi_{ab}(E') \supseteq (E/abE)^*$, then $\pi_a(E') \supseteq (E/aE)^*$, where E' is a subset of E and $\pi_x\colon E' \to E/xE$ is the canonical map.*

Proof. For $r \in E$ and $r + aE \in (E/aE)^*$, if r and b are relatively prime, then $r + abE \in (E/abE)^*$, whence $r + aE \in \pi_a(E')$. If r and b are not relatively prime with a greatest common divisor d. Write $d = q_1^{n_1} \cdots q_t^{n_t}$ with nonassociate irreducible elements q_i in E and $n_i \in \mathbb{N}$ for $i = 1, 2, \ldots, t$. Express $b = q_1^{s_1} \cdots q_t^{s_t} p_1^{m_1} \cdots p_k^{m_k}$ as a product of nonassociate irreducible elements q_i, p_j and $s_i, m_j \in \mathbb{N}$, where integers $t > 0$ and $k \geq 0$. (Note that $p_0 = 1_E$ if $k = 0$.) It is clear that $r + ap_1 \cdots p_k$ and b are relatively prime, whence $r + ap_1 \cdots p_k$ and ab are relatively prime. Hence, by assumption, there exists $c \in E'$ such that $c + abE = (r + ap_1 \cdots p_k) + abE$. This implies that $c + aE = r + aE$.

We conclude that $\pi_a(E') \supseteq (E/aE)^*$. □

Theorem 4.12. *The only imaginary quadratic fields $\mathbb{Q}(\sqrt{-l})$ for which the ring E of integers admits a restricted Nagata's pairwise algorithm are the ones for which $l = 1, 2, 3, 7, 11$.*

Proof. By Proposition 14 of [9], we know that the rings E of integers of $\mathbb{Q}(\sqrt{-l})$ for $l = 1, 2, 3, 7, 11$ are Euclidean. Hence they admit a restricted Nagata's pairwise algorithm respectively.

For $l > 12$, the only units in E (the ring of integers of imaginary quadratic field $\mathbb{Q}(\sqrt{-l})$ of class-number one) are $+1$ and -1. We use the transfinite construction, so that $\tilde{E}_0 = \{0, 1, -1\}$ (with the notation of this construction). By Lemma 4.11, if a is in $\tilde{E}_1$, then every prime factor of a is in $\tilde{E}_1$. We recall that for $b \in E \setminus \{0\}$ the norm of b is the cardinal number of the set E/bE. Thus the norms of prime elements in $\tilde{E}_1 \setminus \tilde{E}_0$ are 2 or 3. Now, for $-l \equiv 2$ or 3 (mod 4), we have $E = \mathbb{Z} + \mathbb{Z}\sqrt{-l}$ and the norm of $x = a + b\sqrt{-l}$ $(a, b \in \mathbb{Z})$ is $a^2 + b^2 l$; the equation $a^2 + b^2 l = 2$ or 3 has no solution for $l > 12$. For $-l \equiv 1$ (mod 4) the ring E of integers of $\mathbb{Q}(\sqrt{-l})$ is $\mathbb{Z} + \mathbb{Z}\{(1 + \sqrt{-l})/2\}$, the equation to be solved in ordinary integers is $(2a + b)^2 + b^2 l = 8$ or 12, and has no solution for $l > 12$. Thus, $\tilde{E}_1 \setminus \tilde{E}_0 = \emptyset$ for $l > 12$.

Hence, by Theorem 4.5, the theorem is proved. □

REMARK 9. By Proposition 14 of [9] and Theorem 4.12, we obtain that the ring E of integers of an imaginary quadratic field is Euclidean if and only if E admits a restricted Nagata's pairwise algorithm. Thus the rings of integers of $\mathbb{Q}(\sqrt{-l})$ for $l = 19, 43, 67, 163$ give examples of principal ideal domains which are neither Euclidean nor admitting a restricted Nagata's pairwise algorithm. Furthermore, by applying Theorem 4.10, there exist more examples of principal ideal rings (not domains) which do not admit a restricted Nagata's pairwise algorithm.

Finally, to close this section, we prove that for the ring E of integers in a number field if it admits a restricted Nagata's pairwise algorithm, then its smallest restricted Nagata's pairwise algorithm is finite valued on $E \times E \setminus \{(0, 0)\}$.

Theorem 4.13. *Let E be an integral domain such that all the residue fields are finite. If E admits a restricted Nagata's pairwise algorithm, then the smallest restricted Nagata's pairwise algorithm θ is finite valued on $E \times E \setminus \{(0, 0)\}$.*

Proof. By Remark 3 and Theorem 4.5, we have $E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$, where W is an ordinal such that $\mathrm{card}(E \times E) < \mathrm{card}(W)$. Let ρ: $E \times E \to W$ be the restricted Nagata's pairwise algorithm defined in the proof of Theorem 4.5. If ρ is not finite valued on $E \times E \setminus \{(0, 0)\}$, then there is an element $a \in \tilde{E}_\omega \setminus \tilde{E}'_\omega$, where ω denotes the first transfinite ordinal. We have $\rho(a, b) = \omega$ for any element b coprime to a. Every coset

$c_i + aE$ with c_i coprime to a admits a representative r_i with $\rho(r_i, a) < \rho(a, c_i) = \omega$, thus $\rho(r_i, a) = n_i$ for some finite value n_i. By the hypothesis E/aE is finite, whence $n = 1 + \sup_i(n_i)$ is an ordinary integer. By the transfinite construction of E and the definition of ρ, we have $a \in \tilde{E}_n$, thus $\rho(a, 1_E) \leq n$, a contradiction. Hence ρ is finite valued on $E \times E \setminus \{(0,0)\}$. Therefore the smallest restricted Nagata's pairwise algorithm θ is finite valued on $E \times E \setminus \{(0, 0)\}$. □

5. Remarks and Problems

In appearance the definition of a restricted Nagata's pairwise algorithm is more complicated than the definition of a Euclidean algorithm. But from Motzkin and Samuel's point of view, as we analyze in Sections 2 and 4, the job to see the existence of a restricted Nagata's pairwise algorithm on a principal ideal ring E is easier than to make sure the existence of a Euclidean algorithm on E. As an example, in 1987, Nagata introduced the concept of pairwise algorithms and constructed a pairwise algorithm on $\mathbb{Z}[\sqrt{14}]$. Actually, the pairwise algorithm he constructed on $\mathbb{Z}[\sqrt{14}]$ is an algorithm now called a restricted Nagata's pairwise algorithm here. But, for the existence of a Euclidean algorithm on $\mathbb{Z}[\sqrt{14}]$, one had to wait until recently Harper [3] succeeded in proving, by means of Motzkin and Samuel's characterization of Euclidean rings, that $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain.

For further study, it is natural to ask the following questions:

PROBLEM 1. Let E be a ring and W an ordinal such that $\text{card}(E \times E) < \text{card}(W)$. Is the statement "$E = \bigcup_{\alpha \in W} \tilde{E}_\alpha$ if and only if $E = \bigcup_{\alpha \in W} E_\alpha$" always true?

In the case E being the ring of integers of an imaginary quadratic field, by applying Proposition 14 of [9] and Theorem 4.12, the answer to Problem 1 is affirmative. Furthermore, by assuming a *GRH* (generalized Riemann hypothesis) and E_K having an infinite unit group, Weinberger [11] proved that E_K is Euclidean, where E_K denotes the ring of integers of a number field K of class number one. Thus, by assuming a *GRH*, the answer to Problem 1 is affirmative for every E_K of a number field K of class number one except $K = \mathbb{Q}(\sqrt{-l})$ for $l = 19, 43, 67, 163$.

Theoretically, to see if a given number field is of class number one, the set $\bigcup_{\alpha \in \mathbb{N}} \tilde{E}_\alpha$ takes less effort than the set $\bigcup_{\alpha \in \mathbb{N}} E_\alpha$, where $\mathbb{N}$ is the set of nonnegative integers.

PROBLEM 2. Given a number field K of class number > 1 and the ring E of integers of K, does there exist any connection between the set $\bigcup_{\alpha \in \mathbb{N}} \tilde{E}_\alpha$ and the class number of K?

In 1976, Cooke [2] introduced the concept of k-stage Euclidean rings: Let R be an integral domain. A sequence of equations (with $\alpha, \beta, \gamma_i, \rho_i \in R$)

$$\alpha = \beta\gamma_1 + \rho_1,$$
$$\beta = \rho_1\gamma_2 + \rho_2,$$
$$\dots$$
$$\rho_{k-2} = \rho_{k-1}\gamma_k + \rho_k$$

is called a k-stage division chain starting from the pair (α, β). We say that R is k-stage Euclidean with respect to f if we can find a function $f: R \to \mathbb{N}$ with the properties
(1) $f(\alpha) = 0 \iff \alpha = 0$,
(2) there is a $k \in \mathbb{N}$ such that for every pair $\alpha, \beta \in R \setminus \{0\}$ there exists an n-stage division chain for some $n \le k$ with $f(\rho_n) < f(\beta)$. Such f is called a k-stage Euclidean algorithm on R.

Clearly, the concept of k-stage Euclidean algorithms is a generalization of Euclidean algorithms, therefore we should also ask the following question:

PROBLEM 3. Is there a characterization of k-stage Euclidean rings which is an analog of Proposition 2.1 or Corollary 4.9?

References

[1] W.-Y. Chen and M.-G. Leu: *On Nagata's pairwise algorithm*, J. Algebra **165** (1994), 194–203.
[2] G.E. Cooke: *A weakening of the Euclidean property for integral domains and applications to algebraic number theory* I, J. Reine Angew. Math. **282** (1976), 133–156.
[3] M. Harper: $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canad. J. Math. **56** (2004), 55–70.
[4] Th. Motzkin: *The Euclidean algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
[5] M. Nagata: *On Euclid algorithm*; in C.P. Ramanujan—A Tribute, Tata Inst. Fund. Res. Studies in Math. **8**, Springer, Berlin, 1978, 175–186.
[6] M. Nagata: *On the definition of a Euclid ring*; in Commutative Algebra and Combinatorics (Kyoto, 1985), Adv. Stud. Pure Math. **11**, North-Holland, Amsterdam, 1987, 167–171.
[7] M. Nagata: *A pairwise algorithm and its application to* $\boldsymbol{Z}[\sqrt{14}]$; in Algebraic Geometry Seminar (Singapore, 1987), World Sci. Publishing, Singapore, 1988, 69–74.
[8] M. Nagata: *Pairwise algorithms and Euclid algorithms*; in Collection of Papers Dedicated to Prof. Jong Geun Park on His Sixtieth Birthday (Korean), Jeonbug, Seoul, 1989, 1–9.
[9] P. Samuel: *About Euclidean rings*, J. Algebra **19** (1971), 282–301.
[10] R.L. Vaught: Set Theory, Birkhäuser Boston, Boston, MA, 1985.
[11] P.J. Weinberger: *On Euclidean rings of algebraic integers*; in Analytic Number Theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, 321–332.
[12] O. Zariski and P. Samuel: Commutative Algebra, I, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1986.

Department of Mathematics
National Central University
Chung-Li 32054
Taiwan
e-mail: mleu@math.ncu.edu.tw