JOURNAL OF ALGEBRA 19, 282–301 (1971)

About Euclidean Rings

PIERRE SAMUEL

University of Colorado and Harvard University

Communicated by D. A. Buchsbaum

Received August 14, 1970

1. INTRODUCTION

In this article all rings are commutative with unit, all modules are unitary. Given a ring A, its multiplicative group of units (i.e. invertible elements) is denoted by A^*.

The customary definition of a Euclidean ring is that it is a domain A together with a map $\varphi : A \to \mathbf{N}$ (the nonnegative integers) such that

(1) $\varphi(ab) \geq \varphi(a)$ for $a, b \in A - (0)$;

(2) given $a, b \in A$, $b \neq 0$, there exist q and r in A such that $a = bq + r$ and $\varphi(r) < \varphi(b)$.

The main interest of a Euclidean ring A is that it is principal: given any nonzero ideal $\mathfrak{b}$ in A, take a nonzero element b in $\mathfrak{b}$ with the smallest possible value for $\varphi(b)$; then, for any $a \in \mathfrak{b}$, (2) shows that $a = bq + r$ with $r = 0$, whence b generates $\mathfrak{b}$. In this proof, (1) has not been used, and any well-ordered set W could replace $\mathbf{N}$ as the range of φ. This has already been noticed by Th. Motzkin [7]. On the other hand the hypothesis that A is a domain does not seem to be essential.

We therefore give the following definition:

DEFINITION 1. *Given a ring A, a Euclidean algorithm (or an algorithm) in A is a map φ of A into a well-ordered set W such that*

(E). *Given $a, b \in A$, $b \neq 0$, there exist q and r in A such that $a = bq + r$ and $\varphi(r) < \varphi(b)$.*

We say that A is Euclidean if it admits an algorithm φ, and, for precision's sake, we then say that A is Euclidean for φ.

In fact the proof that A is principal would work as well if W were a partially ordered set with descending chain condition. But we will see that this is not

an essential generalization (see Section 4, Prop. 11). On the other hand, I do not know whether, for domains, the passage from $\mathbf{N}$ to a well ordered set W enlarges the class of euclidean rings.

After some easy preliminaries and examples, we will show, as already noticed by Th. Motzkin, that a Euclidean ring admits a smallest algorithm. In various cases this algorithm can be explicitly computed, but its structure seems to be rather complicated in general (e.g. for $\mathbf{Z}[\sqrt{-2}]$).

The determination of the imaginary quadratic fields for which the ring of integers is Euclidean is easy (see Section 5). For real ones, there might be fields for which this ring is Euclidean, but not for the norm.

The case of the coordinate ring of an affine curve over any field can be completely treated if the genus is 0; furthermore the smallest algorithm is explicitly determined when the ground field is infinite. For this a strange theorem about finitely generated commutative subgroups of a linear group is needed.

We will see that many problems in the theory of euclidean rings are open.

2. Elementary Properties of Euclidean Rings

In what follows, A is a Euclidean ring, W a well-ordered set, and $\varphi : A \to W$ an algorithm.

Proposition 1. *For $b \in A$, $b \neq 0$, we have $\varphi(b) > \varphi(0)$, so that $\varphi(0)$ is the smallest element of $\varphi(A)$.*

By (E), we write $0 = bq + b_1$ with $\varphi(b_1) < \varphi(b)$. We inductively define a sequence $b, b_1, \ldots, b_n$ of elements of A by the following rule: if $b_n = 0$ we stop; if $b_n \neq 0$ we write $0 = b_n + b_{n+1}$ with $\varphi(b_{n+1}) < \varphi(b_n)$. Since $(\varphi(b_n))$ is a strictly decreasing sequence of elements of a well-ordered set, it must be finite. Hence there exists $n \geqslant 1$ such that $b_n = 0$. Thus $\varphi(0) = \varphi(b_n) < \varphi(b)$.

Proposition 2. *An element $b \in A$ such that $\varphi(b)$ is the smallest element of $\varphi(A) - \varphi(0)$ is a unit in A.*

By hypothesis we have $b \neq 0$. For any a in A, we have $a = bq + r$ with $\varphi(r) < \varphi(b)$, whence $r = 0$. Therefore $A = Ab$ and b is a unit.

Proposition 3. *Every ideal $\mathfrak{b}$ of the Euclidean ring A is principal.*

We may assume $\mathfrak{b} \neq (0)$. Then take, among the nonzero elements of $\mathfrak{b}$, an element b with smallest value for φ. For any $a \in \mathfrak{b}$, we write $a = bq + r$ with $\varphi(r) < \varphi(b)$. Since $r = a - bq \in \mathfrak{b}$, we necessarily have $r = 0$, whence $\mathfrak{b} = Ab$.

An algorithm φ on an Euclidean ring A does not necessarily satisfy the divisibility condition (1) of Section 1.

EXAMPLE 1. Let $A = \mathbf{Z}$, $\varphi(n) = |n|$ for $n \neq 5$, and $\varphi(5) = 13$. For any $n \neq 0$ in Z such that either $|n| \leqslant 5$ or $|n| \geqslant 14$, the representatives $r = 0, 1, \ldots, |n| - 1$ of the classes mod n satisfy $\varphi(r) < \varphi(n)$. For $6 \leqslant |n| \leqslant 13$ we replace the representative 5 by $5 - |n|$, which still satisfies $\varphi(5 - |n|) < \varphi(n)$. Hence (E) holds. But we have $\varphi(5) > \varphi(10)$ and $\varphi(5) > \varphi(-5)$, contradicting (1).

However a Euclidean ring A admits algorithms satisfying (1). More precisely,

PROPOSITION 4. *If $\varphi : A \to W$ is an algorithm on an Euclidean ring A, then φ_1, defined by $\varphi_1(0) = \varphi(0)$ and $\varphi_1(a) = \inf_{b \in Aa-(0)} \varphi(b)$ for $a \neq 0$, is an algorithm such that*

(a) $\varphi_1(ac) \geqslant \varphi_1(a)$ *for* $ac \neq 0$,

(b) $\varphi_1(ac) = \varphi_1(a)$ *iff* $Aac = Aa$,

(c) $\varphi_1(a) \leqslant \varphi(a)$ *for all* $a \in A$.

In fact φ_1 is well defined since W is well ordered. Properties (a) and (c) follow from the definition of φ_1, and also the "if" part of (b). For proving that φ_1 is an algorithm, let us consider $b \neq 0$ in A and a in A; by definition we have $\varphi_1(b) = \varphi(bc)$ for a suitable c in A; by (E) we can write $a = bcq + r$ with $\varphi(r) < \varphi(bc)$; therefore we have $a \equiv r \bmod Ab$ and $\varphi_1(r) \leqslant \varphi(r) < \varphi(bc) = \varphi_1(b)$. Finally we prove the "only if" part of (b): if $\varphi_1(ac) = \varphi_1(a)$, we write $a = acq + r$ with $\varphi_1(r) < \varphi_1(a)$; since $r = a(1 - cq)$, (a) implies that $r = 0$, whence $Aac = Aa$. Q.E.D.

COROLLARY 1. *If φ_1 is as in Prop. 4, and if u is a unit A, then $\varphi(u)$ is the smallest element β of $\varphi(A) - \varphi(0)$* (converse to Prop. 2)

By Proposition 2, there exists a unit u' with value β. Since u is an associate of u', it has also value β by (b).

Remark. The conclusion of Corollary 1 does not necessarily hold in general. Take $A = \mathbf{Z}$, $\varphi(n) = |n|$ for $n \neq 1$, $\varphi(1) = 2$ (use 0 and -1 as representatives mod 2).

COROLLARY 2. *Assume that the well-ordered set W contains $\mathbf{N}$ as an initial segment, and that the Euclidean ring A is a domain. Let $(v_p)_{p \in P}$ be the set of all*

normalized valuations of A (corresponding to the prime elements of A). Then, for any algorithm φ on A, we have

$$\varphi(x) \geqslant 1 + \sum_{p \in P} v_p(x) \qquad \text{for any} \quad x \neq 0 \text{ in } A. \tag{2.1}$$

We may replace φ by φ_1 as in Prop. 4, since $\varphi(x) \geqslant \varphi_1(x)$ for any x in A. Now, if x' is a strict multiple of x, we have $\varphi_1(x') > \varphi_1(x)$. Then (2.1) is proved by induction on $\sum v_p(x)$, the starting case $\sum v_p(x) = 0$ being the case of a unit x for which $\varphi(x) \geqslant 1$.

3. Examples of Euclidean Rings. Stability Properties

It is well known that $\mathbf{Z}$ is Euclidean for the algorithm $\varphi(n) = |n|$, and that the polynomial ring $k[X]$ (k: a field) is Euclidean for $\varphi(P(X)) = 1 + d^0(P(X))$; notice that, if k is algebraically closed, we then have $\varphi(P(X)) = 1 + \sum v_p(P(X))$ (cf. Sec. 2, Cor. 2 to Prop. 4).

Proposition 5. *A principal ideal domain with a finite number of maximal ideals, $Ap_1, \ldots, Ap_n$ is Euclidean for the algorithm*

$$\varphi(x) = 1 + \sum_{i=1}^{n} v_i(x) \ (x \neq 0), \quad \varphi(0) = 0,$$

(where v_i denotes the normalized p_i-adic valuation of A).

Let b be any nonzero element of A and $\bar{x}$ an element of A/Ab. We have to find a representative x of $\bar{x}$ in A such that $\varphi(x) < \varphi(b)$. For $\bar{x} = 0$ we take $x = 0$. For $\bar{x} \neq 0$, let x' be any representative of $\bar{x}$. There exist indices i such that $v_i(x') < v_i(b)$ (otherwise $x' \in Ab$ and $\bar{x} = 0$); for such an index i, we have $v_i(x) = v_i(x') < v_i(b)$ for every representative x of $\bar{x}$. For an index j such that $v_j(x') \geqslant v_j(b)$, we can write $x' \equiv z_j b \bmod Ap_j^{1+v_j(b)}$ with $z_j \in A$ well defined mod Ap_j. The chinese remainder theorem [8] provides us with an element z of A such that $z \equiv 1 - z_j \bmod Ap_j$ for all such indices j. Then $x = x' + bz$ is a representative of $\bar{x}$ and is congruent to b mod $Ap_j^{1+v_j(b)}$. Hence $v_j(x) = v_j(b)$ for all these indices j. Since $v_i(x) < v_i(b)$ for the other indices i, we get $\sum_{i=1}^{n} v_i(x) < \sum_{i=1}^{n} v_i(b)$, whence $\varphi(x) < \varphi(b)$. Q.E.D.

Corollary. *The ring of a discrete valuation v is Euclidean for $\varphi(x) = 1 + v(x) (x \neq 0)$.*

Proposition 6. *A product of a finite number of Euclidean rings is euclidean.*

By induction we are reduced to the case of a product of two factors, $A = A_1 \times A_2$. Let A_i be Euclidean for $\varphi_i : A_i \to W_i$ $(i = 1, 2)$. Let $W' = W_1 \times W_2$ lexicographically ordered ($(\alpha_1, \alpha_2) < (\beta_1, \beta_2)$ means either $\alpha_1 < \beta_1$, or $\alpha_1 = \beta_1$ and $\alpha_2 < \beta_2$). Call W the "ordinal sum" of two copies of W': this is a well-ordered set together with order-preserving injections $h', h'' : W' \to W$ such that $h'(\lambda) < h''(\mu)$ for all $\lambda, \mu \in W'$. We define $\varphi : A_1 \times A_2 \to W$ as follows ($x_1 \in A_1$, $x_2 \in A_2$):

(i) If none or both of x_1, x_2 are 0, $\varphi(x_1, x_2) = h'((\varphi_1(x_1), \varphi_2(x_2)))$,

(ii) If just one of x_1, x_2 is 0, $\varphi(x_1, x_2) = h''((\varphi_1(x_1), \varphi_2(x_2)))$.

We now show that φ is an algorithm on $A_1 \times A_2$. Consider $b = (b_1, b_2) \neq 0$ in $A_1 \times A_2$, and $a = (a_1, a_2) \in A_1 \times A_2$. We try to write $a = bq + r$ with $\varphi(r) < \varphi(b)$.

Suppose first that $b_1 \neq 0$, $b_2 \neq 0$ and write $a_i = b_i q_i + r_i$ with $\varphi(r_i) < \varphi_i(b_i)$ for $i = 1, 2$. If none or both of r_1, r_2 are 0, we have

$$\varphi(r_1, r_2) = h'((\varphi_1(r_1), \varphi_2(r_2))) < h'((\varphi_1(b_1), \varphi_2(b_2))) = \varphi(b)$$

so that we may take $r = (r_1, r_2)$, $q = (q_1, q_2)$. If $r_1 = 0$ and $r_2 \neq 0$ we write $a_1 = b_1(q_1 - 1) + b_1$, $a_2 = b_2 q_2 + r_2$, and take $r = (b_1, r_2)$, $q = (q_1 - 1, q_2)$; then $\varphi(r) = h'((\varphi_1(b_1), \varphi_2(r_2))) < h'((\varphi_1(b_1), \varphi_2(b_2))) = \varphi(b)$. The case $r_1 \neq 0$, $r_2 = 0$ is treated in a similar way.

Suppose now that $b_1 = 0$, $b_2 \neq 0$. If $a_1 \neq 0$, we write $a_2 = b_2 q_2 + r_2$ with $r_2 \neq 0$ (this is possible if we exclude the trivial case in which A_2 is the zero ring); taking $r = (a_1, r_2)$ and $q = (0, q_2)$, we then have $\varphi(r) \in h'(W')$, $\varphi(b) \in h''(W')$, whence $\varphi(r) < \varphi(b)$. If $a_1 = 0$, we write $a_2 = b_2 q_2 + r_2$ with $\varphi_2(r_2) < \varphi_2(b_2)$, and take $r = (0, r_2)$, $q = (0, q_2)$; then

$$\varphi(r) = h''((\varphi_1(0), \varphi_2(r_2))) < h''((\varphi_1(0), \varphi_2(b_2))) = \varphi(b).$$

The case $b_1 \neq 0$, $b_2 = 0$ is treated in a similar way Q.E.D.

Remarks. (1) A principal ideal ring is known to be a finite product of principal ideal domains and of principal ideal rings with a unique and nilpotent maximal ideal Ap (11, Chap. IV, Sec. 15, Thm. 33). Every nonzero element x of such a ring can be written as $x = p^{v(x)} \cdot u$ (u : a unit), where $v(x)$ is uniquely determined by x, so that $1 + v(x)$ is an algorithm (as in Prop. 5), and the corresponding ring is Euclidean. Thus the question as to whether a principal ideal ring is Euclidean boils down to the same question for principal ideal domains. This might explain why euclidean rings with zero-divisors did not receive much attention.

(2). The use of transfinite valued algorithms, as in the proof of Prop. 6, is unavoidable in the case $A = \mathbf{Z} \times \mathbf{Z}$. In fact, we more generally notice:

(F). *If A is Euclidean for φ, if A^* is finite and if n is an ordinary integer, then $A_n = \varphi^{-1}(\{n\})$ is finite.*

Proof. By induction on n, $A_n' = A_0 \cup \ldots \cup A_{n-1}$ is finite; if $\varphi(b) = n$ $A_n' \to A/Ab$ is surjective. Using Prop. 13 of Section 5, we see that the ideal Ab can take only a finite number of values. Hence the element b also since A^* is finite.

This being so, suppose that $\varphi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{N}$ is an algorithm, and set $\varphi((1, 0)) = n$. Then, as above in (F), $A_n' = A_0 \cup \ldots \cup A_{n-1}$ is finite and $A_n' \to (\mathbf{Z} \times \mathbf{Z})/((1, 0))$ is surjective. This is impossible since this last ring, isomorphic to $\mathbf{Z}$, is infinite.

PROPOSITION 7. *Let A be a Euclidean domain, and $S \subset A$ a multiplicatively closed set (such that $0 \notin S$). Then $S^{-1}A$ is Euclidean.*

Let φ be an algorithm on A such that $y \in Ax$, $y \neq 0$ implies $\varphi(x) \leqslant \varphi(y)$ (Sec. 2, Prop. 4). By saturating S, we may assume it is generated by some prime elements of A and by the units. Then every element x of $S^{-1}A$ can be written as $x = (s/t)\, x'$ with $s, t \in S$ and $x' \in A$ prime to all elements of S; then x' is uniquely determined up to units by x. We set $\varphi'(x) = \varphi(x')$ and show that φ' is an algorithm on $S^{-1}A$.

First we note that, for $s, s' \in S$ and $x \in S^{-1}A$, we have $\varphi'(s) = \varphi(1)$ and $\varphi'(sx/s') = \varphi'(x)$. Consider $a, b \in S^{-1}A$ with $b \neq 0$, and write $b = (s/t)\, b'$ as above. Since the prime ideals of A containing b' are all maximal, the canonical map $A/Ab' \to S^{-1}A/S^{-1}Ab$ is an isomorphism. Thus there exists $a' \in A$ such that $(t/s)a \equiv a' (\mathrm{mod} \cdot S^{-1}Ab)$, whence $a \equiv (s/t)\, a' \ (\mathrm{mod}\ S^{-1}Ab)$. We can write $a' = b'q + r$ with $q, r \in A$ and $\varphi(r) < \varphi(b')$. Therefore $a \equiv (s/t)r \ (\mathrm{mod}\ S^{-1}Ab)$, and we have $\varphi'((s/t)r) = \varphi'(r) \leqslant \varphi(r) < \varphi(b') = \varphi(b)$.

PROPOSITION 8. *If A is a Euclidean ring, then $A' = A[[X]][X^{-1}]$ is Euclidean.*

Let φ be an algorithm on A. The elements of A' are power series $\sum_{n \geqslant n_0} a_n X^n (a_n \in A)$ with, possibly, a finite number of terms with negative exponents. For $s \in A'$, $s \neq 0$, let $a(s)$ be the coefficient of the lowest degree term of s, $s = a(s)\, X^q + a_{q+1} X^{q+1} + \cdots$. We set $\varphi'(s) = \varphi(a(s))$ $\varphi'(0) = \varphi(0)$, and prove that φ' is an algorithm. Consider $s \in A'$, $s \neq 0$ so that $s = a(s)\, X^\alpha + \cdots$ with $a(s) \neq 0$. For each $t = a(t)\, X^\beta + \cdots$ in A' we write $a(t) = a(s)b + c$ with $b, c \in A$, $\varphi(c) < \varphi(a(s))$, and set $t' = t - bX^{\beta-\alpha}s = cX^\beta +$ higher degree terms. If $c \neq 0$, we stop since $\varphi'(t') = \varphi(c) < \varphi(a(s)) = \varphi'(s)$. If $c = 0$ we similarly construct $t'' = t' - b'X^{\beta'-\alpha}s$ ($\beta' =$ order of t'), and so on. If the process stops after a finite number of steps, we get a $t^{(n)} \equiv t \bmod A$'s such that $\varphi'(t^{(n)}) < \varphi'(s)$. Otherwise the infinite sum

$u = bX^{\beta-\alpha} + b'X^{\beta'-\alpha} + \cdots + b^{(n)}X^{\beta(n)-\alpha} + \cdots$ makes sense (the sequence $(\beta^{(n)})$ being strictly increasing), and we have $t = us + 0$ with evidently $\varphi'(0) < \varphi'(s)$. Q.E.D.

4. The Smallest Algorithm

Two algorithms $\varphi : A \to W, \varphi' : A \to W'$ on a ring A are said to be *isomorphic* if there exists an order-isomorphism $h : \varphi(A) \to \varphi'(A)$ such that $\varphi' = h \circ \varphi$. Isomorphic algorithms have obviously the same properties. Thus, since all well-ordered sets with cardinal $\leqslant \mathrm{card}(A)$ are order isomorphic to initial segments of any well ordered set W such that $\mathrm{card}(W) > \mathrm{card}(A)$, all the algorithms on the ring A may be construed to take their values in the fixed ordered set W. For precision sake, we may assume that W is an ordinal, with elements customarily denoted by 0, 1, 2, 3,..., ω, $\omega + 1$,..., 2ω,...

Proposition 9. *If $\varphi_\alpha : A \to W$ is any nonempty family of algorithms on an Euclidean ring A, then $\varphi = \inf_\alpha \varphi_\alpha$ is also an algorithm.*

Consider $a, b \in A$, $b \neq 0$. Since W is well ordered, there exists an index α such that $\varphi(b) = \varphi_\alpha(b)$. We can write $a = bq + r$ with $q, r \in A$ and $\varphi_\alpha(r) < \varphi_\alpha(b)$. Then $\varphi(r) \leqslant \varphi_\alpha(r) < \varphi_\alpha(b) = \varphi(b)$, proving that φ is an algorithm.

Proposition 9 shows that the Euclidean ring A admits a *smallest algorithm* θ (i.e. the infimum of all algorithms). By Prop. 4(c) of Section 2, θ enjoys the properties described in Prop. 4 and in its corollaries. Moreover we have

$$\theta(x) = 0 \Leftrightarrow x = 0, \text{ (Prop. 1);} \tag{4.1}$$

$$\theta(x) = 1 \Leftrightarrow x \text{ is a unit, (Prop. 2 and Cor. 1. to Prop. 4).} \tag{4.2}$$

Proposition 10. *Let $\theta : A \to W$ be the smallest algorithm on an Euclidean ring A. For $\alpha \in W$ set $A_\alpha = \{x \in A \mid \theta(x) \leqslant \alpha\}$ and $A_\alpha' = \{x \in A \mid \theta(x) < \alpha\}$. Then A_α is the union of $\{0\}$ and the set of all $b \in A$ such that the canonical map $A_\alpha' \to A/Ab$ is surjective (i.e. representatives of the classes* mod *Ab can be found in A_α').*

If $b \in A_\alpha$, and if $a + Ab (a \in A)$ is any class mod Ab, then, by writing $a = bq + r$, we find a representative r of this class such that $\theta(r) < \theta(b) \leqslant \alpha$, i.e. $r \in A_\alpha'$. Conversely consider $b \neq 0$ such that $A_\alpha' \to A/Ab$ is surjective, and suppose that $\theta(b) > \alpha$. Now define $\theta_1 : A \to W$ by $\theta_1(b) = \alpha$ and $\theta_1(x) = \theta(x)$ for $x \neq b$. I claim that θ_1 is an algorithm: in fact for the relations $a = bq + r$ in which b acts as the divisor, we know that each class $a + Ab$ has a representative $r \in A_\alpha'$ i.e. such that $\theta_1(r) < \alpha = \theta_1(b)$; on the other hand,

in a relation $a = cq + b$ in which b acts as a remainder, we have $\theta_1(b) = \alpha < \theta(b) < \theta(c) = \theta_1(c)$. This contradicts the fact that θ is the smallest algorithm. Therefore $\theta(b) \leqslant \alpha$. Q.E.D.

Proposition 10 shows that the smallest algorithm can be constructed by *transfinite induction*, since the set A_α' determines A_α in a simple way.

EXAMPLE. $\theta(x) = 2$ means that A/Ax admits a system of representatives made of 0 and of units. Such an x is necessarily a prime element of A (every nonzero element of A/Ax being invertible, A/Ax is a field).

The transfinite construction described in Prop. 10 may be performed in any ring. More precisely,

The transfinite construction. Let A be a ring, and W an ordinal such that $\operatorname{card}(A) < \operatorname{card}(W)$. *We set $A_0 = \{0\}$. For $\alpha > 0$ in W, we define A_α by transfinite induction as follows: the set $A_\alpha' = \bigcup_{\beta<\alpha} A_\beta$ is already defined and A_α is the union of $\{0\}$ and of the set of all $b \in A$ such that $A_\alpha' \to A/Ab$ is surjective.*

It is clear that the sequence $(A_\alpha)_{\alpha \in W}$ is increasing. The ring A is *Euclidean iff this sequence exhausts* the ring A. In this case the smallest algorithm θ on A is defined by

$$\theta(x) = \alpha \in W \Leftrightarrow x \in A_\alpha - A_\alpha'. \tag{4.3}$$

Otherwise the sequence stops increasing before exhausting A. At any rate we have

$$A_0 = \{0\}, \tag{4.4}$$

$$A_1 - A_0 = A_1 - A_1' = \text{set of units } A^*, \tag{4.5}$$

$$A_2 - A_1 = A_2 - A_2' = \{b \in A \mid A/Ab \text{ admits a system of representatives made of 0 and of units}\}. \tag{4.6}$$

The set $A_2 - A_1$ may very well be empty (see the example of imaginary quadratic fields in Section 5); in this case A is not euclidean, unless it is a field.

EXAMPLES. (1) For $A = \mathbf{Z}$, we have $A_2' = A_1 = \{-1, 0, +1\}$ and this set contains three consecutive integers. Thus it provides representatives for the classes mod 2 and mod 3, so that $A_3' = A_2 = \{-3, -2, -1, 0, 1, 2, 3,\}$. Here we have seven consecutive integers, so that $A_4' = A_3$ is the interval $[-7, +7]$, consisting of 15 consecutive integers. An easy induction shows that *the smallest algorithm θ on $\mathbf{Z}$ is given by*

$$\theta(n) = \textit{number of binary digits of } |\, n \,|.$$

(2) Let k be a field, and A the polynomial ring in one variable $A = k[X]$. Since $A^* = k^*$ we have $A_2' = A_1 = k$. Thus the elements of A_2 are 0 and the polynomials p such that $k[X]/(p)$ is a vector space of dimension $\leqslant 1$ over k; these are the polynomials of degree $\leqslant 1$, and they form a two-dimensional vector space over k. By induction we see that $A'_{n+1} = A_n$ is the n-dimensional vector space of polynomials with degree $\leqslant n-1$. Therefore *the smallest algorithm* θ on $k[X]$ *is the usual algorithm*

$$\theta(q) = 1 + d^0(q) \quad (q \neq 0)$$

(3) Let A be a principal ideal domain with a finite number of maximal ideals $Ap_i (i = 1,..., n)$, and let v_i be the normalized p_i-adic valuation of A. It follows from Prop. 5 (Sec. 3) and Cor. 2 to Prop. 4 (Sec. 2) that the smallest algorithm θ on A is given by

$$\theta(x) = 1 + \sum_{i=1}^{n} v_i(x) \ (x \neq 0).$$

(4) Let A be a Euclidean domain, θ its smallest algorithm, and S a multiplicative subset of $A (0 \notin S)$. The algorithm θ' on $S^{-1}A$ deduced from θ as in Prop. 7 (Sec. 3) is not necessarily the smallest algorithm on $S^{-1}A$. For example if A is $\mathbf{Z}$ and if S is the set of integers prime to 6, we have $\theta'(4) = 3 < \theta'(9) = 4$ (Example 1), whereas, for the smallest algorithm φ on $S^{-1}\mathbf{Z}$, we have $\varphi(4) = \varphi(9) = 3$.

(5) If A is a Euclidean ring of integers in an imaginary quadratic number field, the sets A_n of the transfinite construction are finite (since A^* is finite; see (F) in Sec. 3, Remark 2), and can be explicitly determined one after another. I did it until $n = 9$ for $A = \mathbf{Z}[\sqrt{-1}]$ and $A = \mathbf{Z}[\sqrt{-2}]$, and these sets seem to be very irregular; for $\mathbf{Z}[\sqrt{-2}]$ their cardinalities are 1, 3, 9, 21, 35, 61, 99, 153, 227, 327.

We are now ready to show that algorithms with values in partially ordered sets with descending chain condition are not really needed.

PROPOSITION 11. *Let A be a ring, T a partially ordered set with descending chain condition and $\varphi : A \to T$ a mapping such that, given any a and $b \neq 0$ in A, there exist $q, r \in A$ such that $a = bq + r$ and $\varphi(r) < \varphi(b)$. Then A is Euclidean.*

Proof. Let (A_α) be the transfinite construction on A and $A' = \bigcup_\alpha A_\alpha$. If $A' \neq A$, choose $b \in A' - A$ such that $\varphi(b)$ is minimal. Then $\varphi(r) < \varphi(b)$ implies $r \in A'$, so that $A' \to A/Ab$ is surjective. But this implies $b \in A'$, a contradiction. Therefore $A = A'$, and A is Euclidean. Q.E.D.

If finite valued, the smallest algorithm satisfies an inequality. More generally,

PROPOSITION 12. *Let A be a ring, $(A_n)_{n\in\mathbf{N}}$ the beginning of its transfinite construction, and $A' = \bigcup_{n=0}^{\infty} A_n$. We set $\theta(x) = n$ for $x \in A_{n+1} - A_n$ (thus $\theta(unit) = 0$, $\theta(0) = -1$). If a, b are nonzero elements of A such that $ab \in A'$, then $a, b \in A'$ and $\theta(ab) \geqslant \theta(a) + \theta(b)$.*

For some n, $A_n \to A/Aab$ is surjective, thus $A_n \to A/Aa$ is also surjective. This proves that $a \in A'$, and similarly $b \in A'$.

For proving $\theta(ab) \geqslant \theta(a) + \theta(b)$, we fix b, and suppose that there exist nonzero elements a of A such that $\theta(ab) < \theta(a) + \theta(b)$. Among these elements we choose an a such that

(1) The difference $\theta(ab) - \theta(a)$ takes its minimum value, say h;

(2) Among the elements a' such that $\theta(a'b) - \theta(a') = h$, a has the smallest value for θ.

Notice that a is not a unit (otherwise $\theta(ab) = \theta(a) + \theta(b) = \theta(b)$ is true). Then there exists a coset $c + Aa$ containing an element $x_0 \in A'$ such that $\theta(x_0) = \theta(a) - 1$ and that $\theta(x) \geqslant \theta(a) - 1$ for every $x \in A_n' \cap (c + Aa)$. Consider the coset $cb + Aab$. Since $ab \in A'$, this coset contains an element $y \in A'$ such that $\theta(y) < \theta(ab)$, i.e. $\theta(y) \leqslant \theta(ab) - 1$. We have $y = xb$ with $x \in c + Aa$, whence $x \in A'$ according to our first statement, i.e. $x \in A_n' \cap (c + Aa)$. If $\theta(x) = \theta(a) - 1$, we have $\theta(xb) - \theta(x) \leqslant \theta(ab) - 1 - (\theta(a) - 1) = h$, and this contradicts (2) since $\theta(x) < \theta(a)$. Otherwise we have $\theta(x) \geqslant \theta(a)$, whence $\theta(xb) - \theta(x) \leqslant \theta(ab) - 1 - \theta(a) = h - 1$, in contradiction with (1). Thus $\theta(ab) < \theta(a) + \theta(b)$ is impossible. Q.E.D.

5. DOMAINS WITH FINITE RESIDUE FIELDS

Let A be a noetherian one-dimensional domain (e.g. a Dedekind or a principal ideal domain) for which all the residue fields are finite. Then, if $\mathfrak{b}$ is a nonzero ideal of A, it is well known that $A/\mathfrak{b}$ is a finite ring. More generally we define the *norm* $n(\mathfrak{b})$ of an ideal $\mathfrak{b}$ in a ring A as the cardinal number $\mathrm{card}(A/\mathfrak{b})$; the norm $n(b)$ of an element $b \in A$ is by definition $n(Ab)$. For $b, b' \in A$, b' not a zero divisor, the isomorphism $A/Ab \to Ab'/Abb'$ shows that

$$n(bb') = n(b)\, b(b').$$

The word "norm" is justified by the following result: If A is an *order* of a number field K (i.e. a finite $\mathbf{Z}$-algebra having K as a field of fractions), then, for $b \in A$, $b \neq 0$, we have

$$n(b) = | N_{K/\mathbf{Q}}(b) |$$

([10, p. 62–63]).

PROPOSITION 13. *In a noetherian ring A, the number of ideals having a given finite norm is finite.*

Let n be this norm. The number of isomorphism classes of rings with n elements being finite, it is sufficient to show that, if R is a given finite ring, the family $(\mathfrak{b}_i)_{i\in I}$ of ideals $\mathfrak{b}_i \subset A$ with $A/\mathfrak{b}_i \sim R$ is finite. Let $\mathfrak{b} = \bigcap_{i\in I} \mathfrak{b}_i$. We have an *injective* homomorphism $A/\mathfrak{b} \to \prod_i A/\mathfrak{b}_i = R^I$. Now let $\mathfrak{m}_j (j = 1,..., r)$ be the maximal ideals of R; set $q_j = \operatorname{card}(R/\mathfrak{m}_j)$, and let s be an exponent such that $(\mathfrak{m}_1 ,..., \mathfrak{m}_r)^s = 0$. We then have, for every x in R

$$P(x) = \prod_{j=1}^{r} (x^{q_j} - x)^s = 0. \tag{5.1}$$

This relation holds also for every x in R^I, whence for every element of $B = A/\mathfrak{b}$.

Now B is noetherian, and there is a monic polynomial $P(X)$ over $\mathbf{Z}$ such that $P(b) = 0$ for every $b \in B$. Since a nonzero polynomial has only a finite number of roots in an integral domain, we see that $B/\mathfrak{p}$ is finite for every prime ideal $\mathfrak{p}$ of B. In particular $B/\mathfrak{p}$ is a field, $\mathfrak{p}$ is maximal and B is Artinian. Since its residue fields are finite, and since B has finite length, B is a finite ring. The correspondence between the ideals of $B = A/\mathfrak{b}$ and the ideals of A containing $\mathfrak{b}$ shows that the latter ones form a finite set. Hence the family $(\mathfrak{b}_i)_{i\in I}$ is finite. Q.E.D.

Given an Euclidean domain A with finite residue fields, one can ask whether the norm is an algorithm on A.

EXAMPLES. (1) For $x \in \mathbf{Z}$, $n(x) = |x|$, so that the usual algorithm on $\mathbf{Z}$ is the norm.

(2) Let k be a finite field with q elements; for any nonzero polynomial $b \in k[X]$ we have $n(b) = q^{d^0(b)}$, so that the norm in $k[X]$ is isomorphic with the usual algorithm.

(3) Let A be a principal ideal domain with a finite number of maximal ideals $Ap_1 ,..., Ap_q$, such that A/Ap_i is a finite field with q_i elements. If v_i denotes the normalized p_i-adic valuation of A, we have

$$n(x) = \prod_{i=1}^{r} q_i^{v_i(x)} (x \in A,\ x \neq 0).$$

Given $b \in A$, $b \neq 0$, we have found in the proof of Prop. 5 (Sec. 3) representatives x for the nonzero classes mod Ab such that $v_i(x) \leqslant v_i(b)$ for all i, one at least of the inequalities being strict. Thus $n(x) < n(b)$ for such a representative x, so that the norm is an algorithm on A.

(4) Let A be an Euclidean domain with finite residue fields, S a multiplicative subset of A ($0 \notin S$), and suppose that the norm n is an algorithm on A. We have seen in Prop. 7 (Sec. 3) that, if we write each $x \in S^{-1}A$, $x \neq 0$ under the form $x = (s/t)\,x'$ with $s, t \in S$ and $x' \in A$ prime to all elements of S, then the mapping n' defined by $n'(x) = n(x')$ is an algorithm on $S^{-1}A$. Since $A/Ax' \to S^{-1}A/S^{-1}Ax$ is an isomorphism, we see that the algorithm n' is actually the norm on $S^{-1}A$.

(5) When mathematicians have studied which rings of integers in number fields are Euclidean, they usually meant to find out whether these rings are *Euclidean for the norm.* This problem has been settled for quadratic fields, there are five imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$,

$$d = -1, -2, -3, -7, -11$$

and sixteen real quadratic fields,

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

for which the ring of all algebraic integers is Euclidean for the norm [5].

One can tackle the more general problem of finding out the number fields for which the ring of integers is Euclidean (for some algorithm, not necessarily the norm). The answer is quite simple for imaginary quadratic fields, due to the scarcity of units.

PROPOSITION 14. *The only imaginary quadratic fields* $\mathbf{Q}(\sqrt{-d})$ *for which the ring* A *of integers is Euclidean are the ones for which* $d = 1, 2, 3, 7, 11$. *These rings are even Euclidean for the norm.*

Except for $d = 1$ and $d = 3$, the only units in A are $+1$ and -1. We exclude these two cases and we use the transfinite construction of Section 4, so that $A_1 = \{, 0, 1, -1\}$ (with the notation of this construction). Thus $A_2 - A_1$ consists of elements with norm 2 or 3. Now, for $-d \equiv 2$ or $3 \pmod 4$, we have $A = \mathbf{Z} + \mathbf{Z}\sqrt{-d}$ and the norm of $x = a + b\sqrt{-d} (a, b \in \mathbf{Z})$ is $a^2 + b^2 d$; the equation $a^2 + b^2 = 2$ or 3 has solutions only if $d \leqslant 3$. For $d \equiv 1 \pmod 4$ the ring of integers A is $\mathbf{Z} + \{(1 + \sqrt{-d})/2\}\mathbf{Z}$, the equation to be solved in ordinary integers is $(2a + b)^2 + ab^2 = 8$ or 12, and has solutions only if $d \leqslant 12$, i.e. only if $d = 7$ or 11 (since $-d \equiv 1 \pmod 4$). Thus, if A is Euclidean, $A_2 - A_1$ is nonempty, and the only possible values for d are 2, 7, 11 (and also 1 and 3). But, in each five cases, A is known to be Euclidean for the norm.

Remarks. (1) The fact that the ring of integers of $\mathbf{Q}(\sqrt{-d})$ is known to be principal also for $d = 19, 43, 67, 163$ gives examples of P. I. D's which are not Euclidean for any algorithm (should one say "which ain't Euclidean for no algorithm?"). Other examples are given in Section 6.

(2) One should not conclude from the proof of Prop. 14 that, if a ring A is not Euclidean, its transfinite construction stops with the units. In fact, in $A = \mathbf{Z}[\sqrt{10}]$, the elements $3 + 2\sqrt{10}$ and $9 + 2\sqrt{10}$ generate prime ideals $\mathfrak{p}_i (i = 1, 2)$, of norms 31 and 41, for which the class of the fundamental unit $3 + \sqrt{10}$ of A generates the multiplicative group $(A/\mathfrak{p}_i)^*$ (i.e. $3 + \sqrt{10}$ is a primitive root mod $\mathfrak{p}_i$). Thus the nonzero cosets mod $\mathfrak{p}_i$ are represented by units, and the elements $3 + 2\sqrt{10}$, $9 + 2\sqrt{10}$ (and their associates) belong to the stage A_2 of the transfinite construction of A. However $\mathbf{Z}[\sqrt{10}]$ is surely not Euclidean, since it is not even principal (its class number is 2).

Concerning *real quadratic fields*, the ones for which the ring of integers is Euclidean are not known. Even one does not know whether there exists such a field for which the ring of integers is Euclidean without being Euclidean for the norm (i.e. a field outside the above list of sixteen).

A possible candidate might be the ring $A = \mathbf{Z}[\sqrt{14}]$. This is known to be principal. Its fundamental unit is $15 + 4\sqrt{14}$, whence its units have the form $a + b\sqrt{14}$ with b even. The elements of the coset $1 + \sqrt{14} + 2A$ cannot thus be units, whence none of them can have a norm $< N(2) = 4$ since 3 is not a norm in A (the ideal $3A$ is prime). This shows that A is not Euclidean for the norm. However I was able to show, by direct computation, that all elements of A up to norm 31 are in some A_n of the transfinite construction (in fact in A_6, the two last ones to be caught being $6 + 2\sqrt{14}$, norm 20, in A_5 and 4, norm 16, in A_6). Many more primes (of norms 43, 47, 67, 101, 103, 107) are in A_2, i.e., the fundamental unit $15 + 4\sqrt{14}$ is a primitive root modulo these elements. We are thus very close to the hard problem of getting some information about the set of primes modulo which a given element is a primitive root (there is a famous conjecture of E. Artin about the ordinary prime numbers for which 2 is a primitive root; see [3, introduction]).

We mentioned, in the introduction, the following problem: Are transfinite valued algorithms really needed for Euclidean domains? Since extremely nice Euclidean rings admit transfinite valued algorithms (e.g. $\varphi(2^j(2n + 1)) = j\omega + n + 1$ in $\mathbf{Z}$, for $n \geqslant 0$, ω denoting the first transfinite ordinal), the problem should be stated as: given a Euclidean domain, is its smallest algorithm finite valued? I do not know the answer in general. However,

PROPOSITION 15. *In a Euclidean domain A with finite residue fields, the smallest algorithm θ is finite valued.*

Proof. Otherwise there is an element $b \in A$ such that $\theta(b) = \omega$. Every coset $c_i + Ab$ admits a representative r_i with $\theta(r_i) < \omega$, i.e. $\theta(r_i) = n_i$ finite. By the hypothesis A/Ab is finite, thus $n = 1 + \sup_i (n_i)$ is an ordinary integer. By definition of the smallest algorithm, we thus have $\theta(b) \leqslant n$, a contradiction. Q.E.D.

6. Rings of Affine Curves

Since the rings we are interested in are principal, and therefore integrally closed, we will restrict ourselves to *normal* affine curves. Such curves are obtained from complete (i.e., projective) normal curves by removing a finite number of points ("the points at infinity"). In a more algebraic way let k be a field, K a finitely generated extension of k with transcendence degree 1, and $(v_\alpha)_{\alpha\in P}$ the set of all valuations of K that are trivial on k; as is well known, these valuations are discrete, and we may suppose they are normalized. Let $P = I \cup F$ be a partition of P in which I is finite nonempty, and let V_α be the valuation ring of v_α; then $A = \bigcap_{\alpha\in F} V_\alpha$ is the ring of an affine normal curve, and all such rings can be obtained in this way. For convenience's sake, we assume that K is a *regular extension* of k, i.e. that K is separable over k and that k is algebraically closed in K; in particular $\bigcap_{\alpha\in P} V_\alpha = k$. For the reader's convenience, we first recall or make explicit some more or less known results.

It is well known that A is a Dedekind ring. To any fractionary ideal $\mathfrak{A}$ of A corresponds a divisor $d(\mathfrak{A}) = \sum_{\alpha\in F} n(\alpha)\cdot\alpha$ "at finite distance" (where $n(\alpha) = \inf_{x\in\mathfrak{A}} v_\alpha(x)$). The ideal $\mathfrak{A}$ is principal, say $\mathfrak{A} = Aa$, iff the divisor $(a) = \sum_{\alpha\in P} v_\alpha(a)\alpha$ of a in K is equal to $\mathfrak{d}(\mathfrak{A})$ + (divisor at infinity), i.e. iff $d(\mathfrak{A})$ is congruent to a principal divisor of K modulo a divisor at infinity. If we call D the group of all divisors of K ($D = \mathbf{Z}^{(P)}$), D_F the group of divisors at finite distance ($D_F = \mathbf{Z}^{(F)}$), D_I the group of divisors at infinity ($D_I = \mathbf{Z}^I$) and D_f the group of divisors of functions, we have thus seen that the class group $C(A)$ of A is given by

$$C(A) \simeq D/(D_f + D_I). \tag{6.1}$$

Now D_f is a subgroup of the group D_0 of divisors of degree 0, and D_0/D_f is the *Jacobian variety* J of the complete curve $\bar{C}$ corresponding to K (more precisely, J denotes here the group of rational points over k of this Jacobian variety). Let δ (resp. δ') be the g.c.d. of the degrees of the divisors of K (resp. of the divisors at infinity); in other words $\delta\mathbf{Z}$ (resp. $\delta'\mathbf{Z}$) is the image of D (resp. D_F) by the degree map $\mathfrak{d} \to d^0(\mathfrak{d})$. Then $D/(D_f + D_I)$ admits as quotient group the group $D/(D_0 + D_I) \simeq \delta\mathbf{Z}/\delta'\mathbf{Z}$ which is a finite cyclic group. The corresponding subgroup is $(D_0 + D_I)/(D_f + D_I)$ and is clearly isomorphic with $D_0/D_0 \cap (D_f + D_I)$, i.e. with a quotient group of the Jacobian J. We thus have proved

Proposition 16. *With the above notations, we have the exact sequence*

$$0 \to D_0/D_0 \cap (D_f + D_I) \to C(A) \to \delta Z/\delta' Z \to 0$$

in which $\delta\mathbf{Z}/\delta'\mathbf{Z}$ *is a finite cyclic group, and* $D_0/D_0 \cap (D_f + D_I)$ *is the quotient group of the Jacobian* J *by the finitely generated subgroup* $(D_0 \cap (D_f + D_I))/D_f$.

This last group is the image in J of the divisors at infinity which have degree 0.

It is 0 if there is only one valuation at infinity.

COROLLARY. *Suppose* k *algebraically closed. Then* A *is principal iff the genus* g *of* C *is* 0.

In fact we have $\delta = \delta' = 1$ since k is algebraically closed. If $g = 0$, we have $J = 0$, whence $c(A) = 0$. If $g > 0$, the Jacobian J is not a finitely generated group (e.g. it carries points of arbitrarily high order), whence

$$D_0/D_0 \cap (D_f + D_I) \neq 0.$$

If k is not algebraically closed, it may happen that J is a finitely generated group (e.g. when k is finitely generated over the prime field, according to the Mordell–Weil–Severi–Neron theorem). Then the valuations at infinity of K may be chosen in such a way that A be principal (i.e. D_I must contain a divisor of degree δ and $D_I \cap D_0$ must contain representatives of a finite set of generators of J).

PROPOSITION 17. *The group of units* A^* *of* A *is the direct product of* k^* *and of a free Abelian group of rank* $\leqslant \mathrm{card}(I) - 1$.

In fact an element x of K^* belongs to A^* iff its divisor (x) is in D_I , i.e. in $D_I \cap D_0$. Whence a homomorphism φ of A^* into $D_I \cap D_0$, which is a free group of rank $\mathrm{card}(I) - 1$, and the kernel of φ is k^* since $\bigcap_{\alpha \in P} V_\alpha = k$.

PROPOSITION 18. *Let* K *be an infinite field,* L *a finite dimensional vector-space over* K, W *a proper subspace of* L *and* Γ *a finitely generated Abelian subgroup of* $\mathrm{Aut}(L)$. *Then* $\Gamma W \neq L$ (*i.e. the transforms of* W *by the elements of* Γ *do not fill* L).

First we get rid of the case in which K is algebraic over a finite field. Then $\mathrm{Aut}(L)$ (considered as a matrix group) is a union of finite groups (namely the groups of matrices with entries in finite subfields of K), and all its elements are of finite order. Thus Γ is a torsion group, whence a finite group. Hence ΓW is a finite union of proper subspaces, and does not fill L since K is infinite.

We take a basis of L over K containing a basis of W (so that $L = K^n$, $W = K^p$, $p < n$). Let (γ_s) be a finite system of generators of Γ, $(a_{s,i,j})(a'_{s,i,j})$ the matrices of γ_s and γ_s^{-1}. We can then replace K by the sufield generated by the elements $a_{s,i,j}$, $a'_{s,i,j}$, thus assume that K is finitely generated over the prime field. Then the Kroneckerian dimension of K is finite, and is $\geqslant 1$

since we have excluded the case in which K is algebraic over a finite field. The subring A of K generated by the elements $a_{s,i,j}$, $a'_{s,i,j}$ is not a field since, by a corollary of the Nullstellensatz, a finitely generated $\mathbf{Z}$-algebra which is a field is a finite field ([12, Chap. V, Sec. 3, no. 4, Cor. 1 du Thm 3]). If the Kroneckerian dimension d of K is $\geqslant 2$, we can find a discrete valuation ring R of K containing A such that the residue field K' of K has Kroneckerian dimension $d-1$. The matrices of the elements of Γ being invertible over R, the relation $\Gamma W = L$, i.e. $\Gamma K^p = K^n$, would imply $\Gamma R^p = R^n$. By the base change $R \to K'$ the image of Γ would be a finitely generated Abelian subgroup Γ' of $\mathrm{aut}(K'^n)$ such that $\Gamma' K'^p = K'^n$. By successive reductions, we may thus assume that K has Kroneckerian dimension 1, i.e. is a *number field or a function field in one variable over a finite field.*

We then proceed by induction on $\dim(L)$. For $\dim(L) = 1$, we have $W = \{0\}$, whence $\Gamma W = \{0\} \neq L$. If L admits a nontrivial subspace L_1 stable by Γ (i.e. $\Gamma L_1 = L_1$), two cases may occur. If $L_1 \not\subset W$, $L_1 \cap W$ is a proper subspace of L_1, and $\Gamma W = L$ would imply $\Gamma(L_1 \cap W) = L_1$ and contradict the induction hypothesis. If $L_1 \subset W$, W/L_1 is a proper subspace of L/L_1, Γ acts on L/L_1, $\Gamma W = L$ would imply $\Gamma(W/L_1) = L/L_1$, again in contradiction with the induction hypothesis. We are therefore reduced to the case in which L is a *simple* $K[\Gamma]$-module, i.e. is isomorphic to a field $K[\Gamma]/\mathfrak{m}$ ($\mathfrak{m}$: a maximal ideal). In other words L may be viewed as a finite extension of K, and Γ as a finitely generated subgroup of the multiplicative group L^*. We will use the following remark:

(R) We may replace W by αW for any $\alpha \in L^*$ (and keep the same Γ)

(In fact $\Gamma W = L$ implies $\Gamma \alpha W = \alpha \Gamma W = \alpha L = L$).

We first tackle the case in which L is *separable* over K. We may enlarge W and suppose it is a hyperplane. Since the bilinear form $\mathrm{Tr}(x \cdot y)$ on L is nondegenerate, W is defined by an equation of the form $\mathrm{Tr}(ax) = 0$ ($a \in L^*$). Replacing W by $a^{-1}W$ (by (R)) we may assume that W is defined by the equation $\mathrm{Tr}(x) = 0$. Let (γ_s) be a finite generating system of Γ. For almost all valuations w of L we have $w(\gamma_s) = w(\gamma_s^{-1}) = 0$, for every s, whence $w(\gamma) = 0$ for every $\gamma \in \Gamma$. On the other hand, if we call L' the Galois closure of L over K, the equipartition of the "Frobenius elements" in the Galois group of L' over K show that this element is the identity for infinitely many valuations of L, i.e. that infinitely many valuations of K are completely decomposed in L', whence also in L. Thus there exists a completely decomposed valuation v of K such that, for all the extensions $w_1, \ldots, w_n$ ($n = \dim(L)$) of v to L, we have $w_i(\Gamma) = \{0\}$. Now, if we call $\sigma_1, \ldots, \sigma_n$ the distinct K-isomorphisms of L in L', and w any fixed extension of v to L', we have $w_i = w \circ \sigma_i$ and $\mathrm{Tr}(x) = \sigma_1(x) + \cdots + \sigma_n(x)$ for any $x \in L$. Now the approximation theorem provides us with an element y of L such that the values $w_i(y)$ are all distinct.

Suppose that $L = \Gamma W$. Then we can write $y = \gamma x$ with $\gamma \in \Gamma$ and $x \in W$, i.e. $\mathrm{Tr}(x) = \sigma_1(x) + \cdots + \sigma_n(x) = 0$. This implies that for two distinct indices i, j, we have $w(\sigma_i(x)) = w(\sigma_j(x))$, i.e. $w_i(x) = w_j(x)$. Since $w_i(\gamma) = w_j(\gamma) = 0$ and $w_i(y) \neq w_j(y)$, the relation $y = \gamma x$ leads to a contradiction. Thus $L \neq \Gamma W$ in the separable case.

In the general case, let L_s be the separable closure of K in L. Since every element of L has a power in L_s, $\Gamma/\Gamma \cap L_s$ is a torsion group, whence a finite group. Let $\delta_1, \ldots, \delta_q \in \Gamma$ be representatives of the classes modulo $\Gamma \cap L_s$. Suppose that $L = \Gamma W$. Then every $x \in L_s$ may be written as $x = \gamma \delta_j w$ with $\gamma \in \Gamma \cap L_s$, $w \in W$ and a suitable j; here $\delta_j w \in \delta_j W \cap L_s$. By using (R) we may assume that all the $\delta_j W \cap L_s$ are proper subspaces of L_s: in fact take $a \in L$ such that $a \notin \delta_j W$ for every j; then $L_s \subset \delta_j a^{-1} W$ would imply $1 \in a^{-1}\delta_j W$, i.e. $a \in \delta_j W$. Thus each $\delta_j W \cap L_s$ is a hyperplane in L_s. Let H be a fixed hyperplane in L_s. Since $L_s{}^*$ acts transitively on the set of hyperplanes of L_s (note that $\mathrm{Hom}_K(L_s, K)$ is a one-dimensional vector space over L_s), we can write $\delta_j W \cap L_s = \alpha_j H$ with $\alpha_j \in L_s{}^*$. Let Γ^1 be the subgroup of $L_s{}^*$ generated by $\Gamma \cap L_s$ and the α_j. We then have $L_s = \Gamma^1 H$, in contradiction with the result proved in the separable case. Q.E.D.

I am indebted to P. Deligne for the idea of using the equipartition of the Frobenius elements.

COROLLARY. *If K' is a proper extension of an infinite field K, then the group K'^*/K^* is not finitely generated.*

The case of a transcendental extension is clear (there are infinitely many irreducible monic polynomials in $K[X]$). Thus we may suppose that K' is finite algebraic. Representatives in K'^* of a finite generating set of K'^*/K^* generate a subgroup Γ of K'^* such that $K' = \Gamma K$.

The fact that, for an infinite field K, the multiplicative group K^* and the additive group K are finitely generated, is true and very easy to prove.

Remark. The fact that infinitely many valuations of a field K are totally decomposed in a finite separable extension is also proved by Nagata in [9]. The above corollary has been proved by A. Brandis [4], who also uses Cebotarev density theorem.

We now consider curves of genus 0. Since the canonical divisors of the function field K have then degree -2, the g.c.d. δ of the degrees of the divisors is either 1 or 2. Let C be an affine normal curve with function field K, and A be the ring of C. For $a \in A$, $a \neq 0$, we define the *degree* of a as being the dimension of A/Aa over the ground field k; notation $d^0(a)$.

PROPOSITION 19. *Let A be the ring of an affine normal curve C of genus* 0

(a) *Suppose that* $\delta = 1$. *Then the following assertions are equivalent*:

(i) *The* g.c.d. δ' *of the degrees of the divisors at infinity is* 1;

(ii) A *is principal*;

(iii) A *is Euclidean for the degree* (*more precisely for*

$$\theta(x) = 1 + [A/Ax : k],\ x \neq 0).$$

(b) *Suppose that* $\delta = 2$. *Then* A *is principal iff* $\delta' = 2$. *Furthermore,* A *is never Euclidean.*

Since the Jacobian variety J is 0, the exact sequence of Prop. 6 shows that $C(A)$ is isomorphic with $\delta\mathbf{Z}/\delta'\mathbf{Z}$. This proves the equivalence of (i) and (ii) in (a), and the first statement in (b). We now prove that (i) and (ii) imply (iii), and this will take care of (a). Consider $a \in A$, $a \neq 0$ and set $d = d^0(a)$. Hypothesis (i) shows the existence of a divisor $\mathfrak{b}$ at infinity with degree $d - 1$. As usual, set $L(\mathfrak{b}) = \{x \in K \mid (x) \geqslant -\mathfrak{b}\}$. By Riemann–Roch's theorem, $L(\mathfrak{b})$ is a vector space of dimension d over k. Since the elements of $L(\mathfrak{b})$ have no poles at finite distance, we have $L(\mathfrak{b}) \subset A$. Furthermore, for $x \in L(\mathfrak{b})$, $x \neq 0$, the part at finite distance of the divisor (x) is positive and its degree is $\leqslant d^0(\mathfrak{b}) = d - 1$; in other words we have $d^0(x) \leqslant d - 1$. Consider now the k-linear mapping $\varphi : L(\mathfrak{b}) \to A \to A/Aa$; for $x \neq 0$, $\varphi(x) = 0$ means that $x \in Aa$ and implies that $d^0(x) \geqslant d^0(a) = d$; we have just seen it is impossible, whence φ is injective. Since the vector spaces $L(\mathfrak{b})$ and A/Aa have the same finite dimension d, φ is surjective, so that each class mod Aa admits a representative $r \in L(\mathfrak{b})$ and we have $d^0(r) \leqslant d - 1 < d = d^0(a)$. In other words A is euclidean for the degree and (a) is proved.

Let us now prove the second statement in (b). Chevalley's theorem about finite fields being C_1 implies that a curve of genus 0 over a finite field k carries a rational point over k. Thus the hypothesis $\delta = 2$ implies that k is infinite. It also implies that the residue fields of A are proper extensions of k. If A were Euclidean, it would contain at least a prime element b such that the residue classes mod Ab can be represented by 0 or units (Sec. 4); in other words $A^* \to (A/Ab)^*$ would be surjective. Since A^*/k^* is a finitely generated group (Prop. 17), this would imply that $(A/Ab)^*/k^*$ is finitely generated and contradict corollary to Prop. 18. Therefore A cannot be Euclidean. Q.E.D.

Part of Prop. 19 had been obtained by J. V. Armitage [1, 2].

PROPOSITION 20. *As above let* A *be the ring of an affine normal curve* C *of genus* 0, *with* $\delta = \delta' = 1$. *Suppose that the ground field* k *is infinite. Then the smallest algorithm* φ *on* A *is* $\varphi(x) = 1 + [A/Ax : k]$ (*i.e. is the degree*).

We already know that $\theta(x) = 1 + [A/Ax : k]$ is an algorithm on A (Prop. 19). Thus $\varphi(x) \leqslant \theta(x)$. Suppose that $\varphi \neq \theta$, and let n be the smallest integer for which there exists $b \in A$ with $\varphi(b) = n$ and $\theta(b) > n$. Since both $\theta(x) = 1$ and $\varphi(x) = 1$ mean that x is a unit, we have $n \geqslant 2$. For any $x \neq 0$ such that $\varphi(x) < n$, we have $d = [A/Ax : k] = \varphi(x) - 1 < n - 1$. Then the "part of infinity" of the divisor (b) has degree $-d$, so that there exists a divisor $\mathfrak{A}$ at infinity of degree $n - 2$ such that (b) $\geqslant -\mathfrak{A}$, i.e. such that $b \in L(\mathfrak{A})$. Now, if $\mathfrak{A}_0$ denotes a fixed divisor of degree $n - 2$ at infinity, $\mathfrak{A}_0 - \mathfrak{A}$ is a principal divisor with zeros and poles at infinity, i.e. the divisor of a unit $u \in A^*$. In other words $L(\mathfrak{A}) = uL(\mathfrak{A}_0)$, so that the set of all $x \in A$ such that $\varphi(x) < n$ is $A^*L(\mathfrak{A}_0)$. Since $A^* = \Gamma k^*$, where Γ is a free Abelian group of finite rank, the above set is $\Gamma L(\mathfrak{A}_0)$. Now $L(\mathfrak{A}_0)$ is a vector space of dimension $n - 1$ over k, whereas A/Ab has, by hypothesis, a dimension $> n - 1$. Let Γ' and L' be the images of Γ and $L(\mathfrak{A}_0)$ in A/Ab. The fact that $\varphi(b) = n$ means that $A^*L(\mathfrak{A}_0) \to A/Ab$ is surjective, i.e., that $A/Ab = \Gamma' L'$. Since k is infinite, since L' is a proper subspace of A/Ab, and since the group Γ' is finitely generated, this contradicts Prop. 18. Q.E.D.

Remarks. (1) As was pointed out to me by Professor Robert MacRae, the method used for proving (b) in Prop. 19 shows that, if C is an affine curve without rational points over an infinite field k, then $k[C]$ cannot be Euclidean. As noticed by him, this conclusion holds also if C has only a finite number of rational points over k: remove these points from C by localizing $k[C]$ with respect to a suitable element, and apply Prop. 7 (Sec. 2).

(2) When k is a finite field, it has been proved by H. Hasse and his students that any nonconstant element of $k(C)$ is a primitive root modulo infinitely many primes [6]. Thus, if $A = k[C]$ is principal (this can be achieved for any function field $k(C)$ by sending enough points at infinity), infinitely many (prime) elements of A belong to the stage A_2 of the transfinite construction. Does this make A Euclidean?

At any rate, in genus 0 (in which case A is Euclidean by Prop. 19(a)), the smallest algorithm θ on A may very well be distinct from the degree (which, in this case, is an algorithm isomorphic to the norm). For example, let $A = \mathbf{F}_q[X, X^{-1}]$. The units are the elements aX^j, $a \in k^*$, $j \in \mathbf{Z}$. For a polynomial $P(X) \in \mathbf{F}_q[X]$ prime to X and of degree n, the relation $\theta(P(X)) = 2$ means that $P(X)$ is irreducible and that the class x of X in $\mathbf{F}_q[X]/(P(X)) \simeq \mathbf{F}_{q^n}$ generates the multiplicative group $\mathbf{F}_{q^n}^*$ modulo $\mathbf{F}_q^*$. Since $\mathbf{F}_{q^n}^*/\mathbf{F}_q^*$ is a cyclic group of order $(q^n - 1)/(q - 1)$, there are $(q - 1)\varphi\{(q^n - 1)/(q - 1)\}$ such elements in $\mathbf{F}_q^*$ (φ: Euler function). The number of corresponding polynomials $P(X)$ is thus $(q-1)^2/n\,\varphi\{(q^n-1)/(q-1)\}$. This gives some information about the set A_2. It would be interesting to describe the transfinite construction for A and its smallest algorithm, even in the simple case $q = 2$.

REFERENCES

1. J. V. ARMITAGE, Euclid's algorithm in certain algebraic function fields, *Proc. London Math. Soc.* **28** (1957), 498–509.
2. J. V. ARMITAGE, Euclid's algorithm in algebraic function fields, *J. London Math. Soc.* **38** (1963), 55–59.
3. E. ARTIN, "Collected Papers," (S. Lang and J. Tate, Eds.), Addison–Wesley, Reading, Mass., 1965.
4. A. BRANDIS, Über die multiplikative Struktur von Körpererweiterungen, *Math. Z.* **87** (1965), 71–73.
5. G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," Chap. XVI, Oxford Univ. Press, London, 1965.
6. H. HASSE, *Acta. Acad. Sci. Fenn. Series A,* 1952.
7. TH. MOTZKIN, On the Euclidean algorithm, *Bull. Amer. Math. Soc.* (1949).
8. MAO, TSE-TUNG, "Little Red Book".
9. M. NAGATA, T. NAKAYAMA, AND T. TUZUKU, On an existence lemma in valuation theory, *Nagoya Math. J.* **6** (1953), 59–62.
10. P. SAMUEL, "Theorie Algébrique des Nombres," Hermann, Paris, 1967.
11. O. ZARISKI AND P. SAMUEL, "Commutative Algebra," Vol. I, Van Nostrand, Princeton, N. J., 1958.
12. N. BOURBAKI, "Algèbre Commutative," Hermann, Paris, 1964.

Printed in Belgium