ACTA ARITHMETICA
123.4 (2006)

δ-rings and factorial sequences preservation

by

Youssef Fares (Amiens)

1. Introduction. For every subset E of $\mathbb{Z}$, and more generally of a Dedekind domain D, Bhargava [2] introduced a notion of generalized factorials associated to E which preserves the classical properties of factorials. Proving a conjecture of Gilmer and Smith [8], we showed in [7] that if a polynomial $f \in \mathbb{Q}[X]$ maps an infinite subset E of $\mathbb{Z}$ onto a subset $f(E)$ which has the same factorials as E, then f is of degree 1. This proof extends easily to the imaginary quadratic number fields but not to all number fields since the group of units may be infinite. The aim of this paper is to give a proof for all number fields. In fact, we prove a stronger result: if a rational function φ with coefficients in a number field K transforms an infinite subset E of O_K into a subset $\varphi(E)$ which has the same factorials as E, then φ is a homographic function (Proposition 26).

These questions have strong links with integer-valued polynomials and integer-valued rational functions.

Notation. In this paper, D denotes an infinite domain with quotient field F and E denotes a subset of D.

Recall [4] that the ring of *integer-valued polynomials on E with respect to D* is

$$\mathrm{Int}(E,D) = \{f \in F[X] \mid f(E) \subseteq D\}$$

and that the ring of *integer-valued rational functions on E with respect to D* is the ring

$$\mathrm{Int}^{\mathrm{R}}(E,D) = \{\varphi \in F(X) \mid \varphi(E) \subseteq D\}.$$

When $E = D$, one writes $\mathrm{Int}(D)$ and $\mathrm{Int}^{\mathrm{R}}(D)$ instead of $\mathrm{Int}(D,D)$ and $\mathrm{Int}^{\mathrm{R}}(D,D)$.

Definition 1 ([2]). The nth *factorial ideal of E with respect to D*, denoted by $(n!)_E^D$, is the conductor in D of the fractional ideal formed by the coefficients of the polynomials of $\mathrm{Int}(E,D)$ with degree n.

2000 *Mathematics Subject Classification*: 11B65, 13F05, 13F20.

Thus, if $\mathrm{Int}(E,D) = \mathrm{Int}(f(E),D)$, then E and $f(E)$ have the same sequence of factorial ideals and it is easy to see that, if $f(E) \subseteq E$, the converse is true. It is in terms of the rings $\mathrm{Int}(E,D)$ and $\mathrm{Int}(f(E),D)$ that Gilmer and Smith proposed their conjecture: does the equality $\mathrm{Int}(f(E),D) = \mathrm{Int}(E,D)$ imply that f is of degree 1?

NOTATION. In this paper, K denotes a number field and O_K the ring of integers of K. Let U_K be the unit group of K.

It is known [4] that for every number field K,

$$\mathrm{Int}^{\mathrm{R}}(O_K) = \mathrm{Int}(O_K).$$

In other words, an integer-valued rational function on O_K is in fact an integer-valued polynomial. We say that O_K is a d-ring (Definition 2 below). In particular,

$$\mathrm{Int}^{\mathrm{R}}(\mathbb{Z}) = \mathrm{Int}(\mathbb{Z}).$$

This property remains true if we replace $\mathbb{Z}$ by an infinite subset $E \subseteq \mathbb{Z}$:

$$\mathrm{Int}^{\mathrm{R}}(E,\mathbb{Z}) = \mathrm{Int}(E,\mathbb{Z}).$$

This equality is easy to check: if $\varphi = g/f \in \mathrm{Int}^{\mathrm{R}}(E,\mathbb{Z})$, $g = qf + r$ where $\deg r < \deg f$, and $a \in \mathbb{Z}$ is such that $aq \in \mathbb{Z}[X]$, then the rational function $ar/f = a\varphi - aq$ is integer-valued on E while $\lim_{|x|\to\infty} ar(x)/f(x) = 0$. Consequently, $r = 0$ and φ is a polynomial.

In order to extend this property to arbitrary number fields, we introduce a property similar to that of d-rings but for infinite subsets E; it is the notion of δ-ring (Definition 6) which we will study in the following section. We will then show in Section 3 that, for every number field K, the ring O_K is a δ-ring (Corollary 18). Lastly, we will use this result to show that if φ is a rational function and E is an infinite subset of O_K such that E and $\varphi(E)$ have the same factorial sequence, then φ is a homographic function (Proposition 26). In particular, if φ is a polynomial, then $\deg \varphi = 1$.

2. δ-rings. Let us recall the definition of a d-ring introduced independently by Brizolis [3] and Gunji and McQuillan [9].

DEFINITION 2. Let D be an infinite integral domain with quotient field F. One says that D is a *d-ring* when, for every $\varphi \in F(X)$, $\varphi(x) \in D$ for almost all $x \in D$ implies $\varphi \in F[X]$.

PROPOSITION 3 ([3], [4], [9], [10]). *Let D be an infinite integral domain with quotient field F and unit group $U(D)$. The following assertions are equivalent*:

(1) *D is a d-ring.*
(2) *For all $f, g \in F[X]$, if $f(x)$ divides $g(x)$ for almost all $x \in D$, then f divides g in $F[X]$.*

(3) *For every non-constant* $f \in D[X]$, *there exists* $a \in D$ *such that* $f(a) \notin U(D)$.
(4) *For every non-constant* $f \in D[X]$, *there exists a maximal ideal* $\mathfrak{M}$ *of* D *such that* f *admits a root in* D *modulo* $\mathfrak{M}$.

Proposition 3 shows that, as soon as $U(D)$ is finite, D is a d-ring. In fact, both propositions below proved by Gunji and McQuillan [9] may be used for any ring of integers of a number field.

Proposition 4. *Let* D *be a* d*-ring and let* B *be a domain containing* D. *If* B *is integral over* D *or if* B *is a finitely generated ring over* D, *then* B *is a* d*-ring.*

Proposition 5. *If the group of units* $U(D)$ *of* D *is of finite type and* $D \neq F$, *then* D *is a* d*-ring.*

Thus, the ring O_K of integers of a number field K is a d-ring. When $U(D)$ is infinite, there are infinite subsets E of D such that $\mathrm{Int}^{\mathrm{R}}(E, D) \neq \mathrm{Int}(E, D)$. Indeed, for every $a \in D$, every subset E contained in $a + U(D)$ and every $n \in \mathbb{N}$, $1/(X-a)^n \in \mathrm{Int}^{\mathrm{R}}(E, D)$. Since we have to take this example into account, we introduce the following definition:

Definition 6. One says that D is a *δ-ring* if for every infinite subset $E \subseteq D$, $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, D)$ implies that φ admits at most one pole (in an algebraic closure of K).

Examples 7.

(1) $\mathbb{Z}$ and every ring of integers of an imaginary quadratic number field are δ-rings.
(2) A non-algebraically closed field F is not a δ-ring. Indeed, there exists $f \in F[X]$ of degree ≥ 2 without any root in F. Let $\varphi(X) = 1/f(X)f(X+1)$. The inclusion $\varphi(F) \subseteq F$ implies that F is not a δ-ring.

Remarks 8. Assume that D is a δ-ring.

(1) A priori, the poles of $\varphi \in F(X)$ belong to an algebraic closure of F, but if φ has only one pole it is an element of F.
(2) For a fixed infinite subset E of D, the poles of all the rational functions $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, D)$ are equal to a unique element e of F. Indeed, if $\varphi_1, \varphi_2 \in \mathrm{Int}^{\mathrm{R}}(E, D)$, then $\varphi_1\varphi_2(E) \subseteq D$ and $\varphi_1\varphi_2$ has at most one pole.
(3) The Jacobson radical $J(D)$ of D is equal to (0). Indeed, let $a \in J(D)$ and let $\varphi(X) = 1/(1+aX)(1+a^2X)$. Then $\varphi(D) \subseteq U(D)$. Thus $a^2 = a$. Since $a \neq 1$, $a = 0$.
(4) For every polynomial $f \in F[X]$ and every infinite subset E of D, $f(E) \subseteq U(D)$ implies that f is of the form $\lambda(X-e)^n$ where $\lambda, e \in F$

and $n \in \mathbb{N}$ ($\mathbb{N}$ is the set of non-negative integers); we then say that f is a *monomial* of $F[X]$.

PROPOSITION 9. *A δ-ring is a d-ring.*

Proof. Suppose that D is a δ-ring. Let $f \in F[X]$ be such that $f(x) \in U(D)$ for almost every x in D. Then $f(X) = \lambda(X-e)^n$. Let E be an infinite subset of D such that $f(x), f(x+1) \in U(D)$ for any $x \in E$. Such a subset exists because D is infinite. Then $\varphi_1(X) = 1/f(X)f(X+1)$ is such that $\varphi(E) \subseteq U(D)$ and consequently has at most one pole. This implies that $n = 0$ and f is a constant. Thus, D is a d-ring. ∎

It is interesting to give for δ-rings a proposition similar to Proposition 3. For that, we make an additional assumption on D. Let us recall:

DEFINITION 10. The ring D is a *FFD* (finite factorization domain) if every non-zero element of D has only a finite number of non-associate divisors.

Thus, Krull domains are FFD (see [1]) and in particular, Dedekind domains are FFD. More generally, every Noetherian domain with finite residue fields is a FFD. It is the case of orders of number fields.

PROPOSITION 11. *Suppose D is a FFD. Then D is a δ-ring if and only if, for every infinite subset E of D, all polynomials $f \in F[X]$ such that $f(E) \subseteq U(D)$ are monomials.*

Proof. The necessity results from Remark 8(4). Conversely, suppose that, for every infinite subset $E \subseteq D$ and for every $f \in F[X]$, $f(E) \subseteq U(D)$ implies that f is a monomial. Fix an infinite subset E of D and a non-zero rational function $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, D)$. Write $\varphi(X) = g/f$ with $f, g \in D[X]$ relatively prime in $F[X]$. By Bézout, there exist $u, v \in D[X]$ and a non-zero $d \in D$ such that $uf + vg = d$. Since $f(x)$ divides $g(x)$ for every $x \in E$, $f(x)$ divides d for every $x \in E$. Since d has only finitely many non-associate divisors, there exists an infinite subset $E_0 \subseteq E$ such that the ideals $(f(x))$ and $(f(y))$ are equal for all $x, y \in E_0$. Fix $x_0 \in E_0$ and let $\lambda = f(x_0)$. Then $f_0(X) = (1/\lambda)f(X)$ is such that $f_0(E_0) \subseteq U(D)$. Thus, f_0 is a monomial and φ admits at most one pole. ∎

COROLLARY 12. *When D is a FFD, the following assertions are equivalent*:

(1) *D is δ-ring.*
(2) *For every $f \in F[X]$ which is not a monomial and every infinite subset E of D, there exists $x \in E$ such that $f(x) \notin U(D)$.*
(3) *For every infinite subset E of D and for every $f \in F[X]$, if $(f(x)) = (f(y))$ for all $x, y \in E$, then f is a monomial.*

PROPOSITION 13. *Let D be a FFD with a finite group of units, E be an infinite subset of D and $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, D)$. Then φ is a polynomial. In particular, D is a δ-ring.*

Proof. Let $\varphi(X) = g(X)/f(X)$ with $f, g \in F[X]$ relatively prime in $F[X]$. By Bézout, there exist $d \in D$ and $u, v \in D[X]$ such that $uf + vg = d$. Since $f(x)$ divides $g(x)$ for every $x \in E$, $f(x)$ divides d for every $x \in E$. Since D is a FFD and $U(D)$ is finite, the set of divisors of d in D is finite. Hence, f is a constant. ∎

PROPOSITION 14. *Assume that D is a δ-ring and let E be a fixed infinite subset of D. Then the elements of the group of units*

$$U(\mathrm{Int}^{\mathrm{R}}(E, D)) = \{\varphi \in F(X) \mid \varphi(E) \subseteq U(D)\}$$

are of the form

$$u\varphi_0(X)^k \quad \textit{where} \quad u \in U(D),\ k \in \mathbb{Z} \textit{ and } \varphi_0(X) = \lambda_0(X - e)^{n_0}.$$

Proof. Let $\varphi \in U(\mathrm{Int}^{\mathrm{R}}(E, D))$. Then $\varphi, 1/\varphi \in \mathrm{Int}^{\mathrm{R}}(E, D)$ imply that $\varphi(X) = \lambda(X - e)^n$ where $e \in F$ and $n \in \mathbb{Z}$. Let n_0 be the least positive integer for which there exist $\lambda_0 \in F$ such that $\varphi_0(X) = \lambda_0(X - e)^{n_0} \in U(\mathrm{Int}^{\mathrm{R}}(E, D))$. Let $n = kn_0 + r$ with $0 \le r < n_0$. Then $\varphi(X) = (\varphi_0(X))^k \cdot \lambda_0^{-k}\lambda(X - e)^r$. Consequently, $\lambda_0^{-k}\lambda(X - e)^r \in U(\mathrm{Int}^{\mathrm{R}}(E, D))$, and hence, $r = 0$ and $\lambda_0^{-k}\lambda \in U(D)$. ∎

PROPOSITION 15. *Let D be an integrally closed δ-ring and let E be an infinite subset of D. If there exists $f \in F[X]$ of degree ≥ 1 such that $f(E) \subseteq U(D)$, then there exists a polynomial $h \in F[X]$ of degree one such that $E \subseteq h(U(D))$ and $f(h(x)) \in U(D)$ for every $x \in U(D)$.*

Proof. If $f(E) \subseteq U(D)$, then $f(X) = \lambda(X - e)^n$ with $\lambda, e \in F$ and $n \in \mathbb{N}$, $n \neq 0$. Write $e = \alpha/\beta$ where $\alpha, \beta \in D$. Let $x_0 \in E$. For all $x \in E$, one has

$$\left(\frac{\beta x - \alpha}{\beta x_0 - \alpha}\right)^n \in U(D).$$

In particular, since D is integrally closed, $(\beta x - \alpha)/(\beta x_0 - \alpha) \in U(D)$. Thus, for every $x \in E$, there exists $u \in U(D)$ such that $\beta x - \alpha = u(\beta x_0 - \alpha)$ and $x = u(x_0 - \alpha/\beta) + \alpha/\beta$. Let $h(X) = (x_0 - \alpha/\beta)X + \alpha/\beta$; on the one hand $E \subseteq h(U(D))$, on the other hand $f(h(U(D))) \subseteq U(D)$. ∎

3. Rings of integers of number fields. Let K be a number field with ring of integers O_K. Denote by $\mathrm{Max}(O_K)$ the set of ideals of O_K. Let $S = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_s\}$ be a finite subset of $\mathrm{Max}(O_K)$ with cardinality s. Denote by $O_{K,S}$ the set formed by the S-units of K, that is,

$$O_{K,S} = \{x \in K \mid v_{\mathfrak{M}}(x) \ge 0\ \forall \mathfrak{M} \notin S\},$$

and by $U_{K,S}$ the group of units of $O_{K,S}$, that is,

$$U_{K,S} = \{x \in K \mid v_{\mathfrak{M}}(x) = 0 \ \forall \mathfrak{M} \notin S\}.$$

Then $O_{K,S}$ is a Dedekind domain. Let us recall the following result of Evertse [6]:

THEOREM 16. *Let K be a number field of degree n. Let $S = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_s\}$ be a finite subset of $\mathrm{Max}(O_K)$ with cardinality s and let a and b be two non-zero elements of K. Then the number of solutions $(x, y) \in U_{K,S}^2$ of the equation $ax + by = 1$ is less than $N(n, s) = 3.7^{n+2s}$.*

As a consequence, we have:

THEOREM 17. *Let K be a number field of degree n. Let $S = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_s\}$ be a finite subset of $\mathrm{Max}(O_K)$. Then, for every $f \in O_{K,S}[X]$ of degree r and leading coefficient a, there exists $N = N(n, s, r, a)$ such that, for every $E \subseteq O_{K,S}$ of cardinality $> N$, $f(E) \subseteq U_{K,S}$ implies that f is a monomial of $K[X]$, that is, $f(X) = a(X - e)^r$ with $e \in K$.*

Proof. Let $f = a_r X^r + \cdots + a_1 X + a_0 \in O_{K,S}[X]$. Let L be the spliting field of f over K and let T be the set of maximal ideals of O_L either lying over a maximal ideal of S, or containing a_r. Then we can write $f(X) = a_r(X - \alpha_1) \cdots (X - \alpha_r)$ with $\alpha_1, \ldots, \alpha_r \in O_{L,T}$. Let $E \subseteq O_{K,S}$ be such that $f(E) \subseteq U_{K,S}$. For every $x \in E$, one has $f(x) = a_r(x - \alpha_1) \cdots (x - \alpha_r) \in U_{K,S} \subseteq U_{L,T}$. Therefore, $x - \alpha_i \in U_{L,T}$ for $i = 1, \ldots, r$. Suppose that there exist $1 \leq i < j \leq r$ such that $\alpha_i \neq \alpha_j$. Then for every $x \in E$ the element $(\alpha_i - x, x - \alpha_j)$ of $U_{L,T}^2$ is a solution of the equation $bx_1 + bx_2 = 1$ with $b = 1/(\alpha_i - \alpha_j) \in L$. Therefore, there exist at least $\mathrm{card}(E)$ solutions. However, according to Theorem 16, this number is less than $N(m, t) = 3.7^{m+2t}$ where $m = [L : \mathbb{Q}]$ and t is the cardinality of T. Thus, if $\mathrm{card}(E) > N(m, t)$, then $\alpha_1 = \cdots = \alpha_r$ and f is of the form $a_r(X - e)^r$. ∎

Note that m and t only depend on n, s, r and a: $m = [L : \mathbb{Q}] \leq nr!$ and $t \leq (s + s')^{r!}$ where s' is the number of maximal ideals of $O_{K,S}$ containing a.

COROLLARY 18. *For every number field K and every finite set S of maximal ideals of O_K, $O_{K,S}$ is a δ-ring.*

Proof. Let $f \in K[X]$ and let E be an infinite subset of $O_{K,S}$ such that $f(E) \subseteq U_{K,S}$. Let $d \in O_K$ be such that $df \in O_K[X]$ and let S_1 be the finite set of maximal ideals of O_K containing d. Let $S_2 = S \cup S_1$; then $f \in O_{K,S_2}[X]$. Theorem 17 shows that f is a monomial of $K[X]$ and thus $O_{K,S}$ is a δ-ring according to Proposition 11. ∎

REMARK 19. Let S and T be two finite subsets of $\mathrm{Max}(O_K)$. Let E be an infinite subset of K such that $E \subseteq O_{K,S}$ and $E \subseteq O_{K,T}$. Let $\varphi, \psi \in K(X)$ be such that $\varphi(E) \subseteq U_{K,S}$ and $\psi(E) \subseteq U_{K,T}$. Then $(\varphi.\psi)(E) \subseteq O_{K,S \cup T}$.

Thus φ and ψ have the same pole. In other words, the pole of all the rational functions $\varphi \in K(X)$ such $\varphi(E) \subseteq U_{K,S}$ does not depend on S.

We also have

THEOREM 20. *Let K be a number field, S be a finite subset of* $\mathrm{Max}(O_K)$ *of cardinality s, and $\varphi \in K(X)$. Then there exists $M = M(\varphi, s)$ such that, for every subset $E \subseteq O_{K,S}$, if* $\mathrm{card}(E) > M$ *and $\varphi(E) \subseteq O_{K,S}$, then φ has at most one pole (in an algebraic closure of K).*

Proof. Let $\varphi(x) = g(x)/f(x)$ where f and g are relatively prime in $K[X]$. By Bézout, there exist $d \in O_K$ and $u, v \in O_K[X]$ such that $uf + vg = d$. Let $E \subseteq O_{K,S}$ be such that $\varphi(E) \subseteq O_{K,S}$. Then, for all $x \in E$, $f(x)$ divides d. Let m be the number of non-associated divisors of d in O_K. Let $f(X) = a_r X^r + \cdots + a_1 X + a_0$ and $n = [K : \mathbb{Q}]$. If $\mathrm{card}(E) > mN(n, s, r, a_r)$, then there exist a divisor d_0 of d in $O_{K,S}$ and a subset $E_0 \subseteq E$ of cardinality $\geq N(n, s, r, a_r)$ such that $f(x)/d_0 \in U_{K,S}$ for every $x \in E_0$. According to Theorem 17, φ has at most one pole (in an algebraic closure of K). ∎

REMARKS 21. Let K be a number field and let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$.

(1) Let $\varphi(X) = g(X)/f(X) \in \overline{\mathbb{Q}}(X)$ with f and g relatively prime in $\overline{\mathbb{Q}}[X]$. Proposition X.1.4 of [4] shows that, if E is an infinite subset of $O_{K,S}$ such that $\varphi(E) \subseteq O_{K,S}$, then $\varphi \in K(X)$. In fact, this assertion remains true for every finite subset E of $O_{K,S}$ such that $\mathrm{card}(E) > \deg f + \deg g$.

(2) Let $\varphi \in K(X)$ be a rational function such that 0 is not a unique pole of φ. Let E be a subset of O_K, $M \in \mathbb{N}$ and $E(M) = \{z \in E : |N_{K/\mathbb{Q}}(z)| \leq M\}$. Theorem 3 of [5] shows that there are two constants $M_0 > 0$ and $\kappa > 0$ depending on φ such that, if $M > M_0$ and $\mathrm{card}(E(M)) > \kappa \log(M)^{r_1+r_2-1}$, then $\varphi(E) \subseteq O_K$ implies $\varphi \in K[X]$, where r_1 and r_2 denote the numbers of real and complex isomorphisms of K into $\mathbb{C}$. Note that, unlike Theorem 20, this theorem does not allow to affirm that $\varphi \in K[X]$ as soon as $\varphi(E) \subseteq O_K$ for some infinite subset E.

4. Application to the preservation of factorial sequences. The notion of generalized factorial was recalled in the introduction:

$$(n!)_E^D = \{y \in D \mid yf \in D[X] \ \forall f \in \mathrm{Int}(E, D), \deg f = n\}.$$

When the ring D is Noetherian, this notion behaves well under localization [4]: For every maximal ideal $\mathfrak{M}$ of D, one has $\mathrm{Int}(E, D)_{\mathfrak{M}} = \mathrm{Int}(E, D_{\mathfrak{M}})$, so that

$$(n!)_E^{D_{\mathfrak{M}}} = (n!)_E^D D_{\mathfrak{M}}$$

and consequently,

$$(n!)_E^D = \bigcap_{\mathfrak{M}\in \mathrm{Max}(D)} (n!)_E^{D_{\mathfrak{M}}}.$$

When D is a Dedekind domain, one is thus led to the case of a discrete valuation domain. Let us recall Bhargava's definition [2]:

Let V be the ring of a discrete valuation v and E be a non-empty subset of V. A sequence $(a_n)_{n\geq 0}$ of elements of E is a *v-ordering* of E if, for all $0 \leq n \leq N$, one has

$$v\Big(\prod_{k=0}^{n-1}(a_n - a_k)\Big) = \inf_{x\in E} v\Big(\prod_{k=0}^{n-1}(x - a_k)\Big).$$

It is easy to see that $v(\prod_{k=0}^{n-1}(a_n - a_k))$ does not depend on the sequence $(a_n)_{n\geq 0}$ because of the equality

$$(n!)_E^V = \prod_{k=0}^{n-1}(a_n - a_k)V.$$

Using v-orderings, we showed in [7] that, if E is an infinite subset of a Dedekind domain D with finite residue fields and a finite unit group, then for all $f \in \mathrm{Int}(E, D)$ the equalities $(n!)_E^D = (n!)_{f(E)}^D$ for all $n \in \mathbb{N}$ imply that f is of degree 1. Such a result, in the case of number fields, applies only to $\mathbb{Q}$ and the imaginary quadratic fields. Here, we are going to extend it on the one hand to the rings of integers of any number field, on the other hand to rational functions instead of polynomials. Recall first the following result of [7]:

Proposition 22. *Let V be the ring of a discrete valuation v, E be a precompact subset of V and $\varphi : E \to V$ a contracting map ($\forall x, y \in E$, $v(\varphi(x) - \varphi(y)) \geq v(x - y)$). The following assertions are equivalent*:

(1) $(n!)_E^V = (n!)_{\varphi(E)}^V$ *for all* $n \in \mathbb{N}$.

(2) φ *is an isometry of* E *onto* $\varphi(E)$.

Thus, for a polynomial $f \in V[X]$, the equalities $(n!)_E^V = (n!)_{f(E)}^V$ for all $n \in \mathbb{N}$ are characterized by $v(f(x) - f(y)) = v(x - y)$ for all $x, y \in E$.

From now on, we assume that K is a number field. Let E be an infinite subset of O_K and $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, O_K)$. Using Theorem 20, we will show that, if E and $\varphi(E)$ have the same factorial sequence, then φ is a homographic function. We start with the case of polynomials.

Proposition 23. *Let K be a number field, E be an infinite subset of O_K and $f \in \mathrm{Int}(E, O_K)$. If $((n!)_E^{O_K})_{\mathfrak{M}} = (n!)_{f(E)}^{O_{K,\mathfrak{M}}}$ for all $n \in \mathbb{N}$ and all maximal ideals $\mathfrak{M}$ of O_K but a finite number, then f is of degree* 1.

Proof. For every maximal ideal $\mathfrak{M}$ of O_K, denote by $v_{\mathfrak{M}}$ the corresponding valuation of K. Assume that $(n!_E^{O_K})_{\mathfrak{M}} = (n!)_{f(E)}^{o_{K,\mathfrak{M}}}$ for all $n \in \mathbb{N}$ and all $\mathfrak{M} \notin \{\mathfrak{M}_1, \dots, \mathfrak{M}_r\}$. Let $d \in O_K$ be such that $df \in O_K[X]$. Let S_1 be the set of maximal ideals of O_K containing d and let $S = S_1 \cup \{\mathfrak{M}_1, \dots, \mathfrak{M}_r\}$. According to Proposition 22, one has $v_{\mathfrak{M}}(f(x) - f(y)) = v_{\mathfrak{M}}(x - y)$ for all $x, y \in E$ and all $\mathfrak{M} \notin S$. Let $df(X) - df(Y) = (X - Y)h(X, Y)$. Then $v_{\mathfrak{M}}(h(x, y)) = 0$ for all $x, y \in E$ with $x \neq y$ and all $\mathfrak{M} \notin S$.

Let $a \in E$. Then $h(x, a)$ is a unit of $O_{K,S}$ for every $x \in E$ distinct from a. Since $O_{K,S}$ is a δ-ring, there exist e independent of a (Remarks 8) and $\lambda \in K$ such that $h(X, a) = \lambda(X - e)^n$. In particular, $f(X) - f(a) = \lambda(X - a)(X - e)^n$ where $n + 1$ is the degree of f. If $n \neq 0$, then $f(a) = f(e)$ for every $a \in E$ and f would be a constant. Thus, $n = 0$ and $\deg f = 1$. ∎

Corollary 24. *Let K be a number field, E be an infinite subset of O_K and $f \in \mathrm{Int}(E, O_K)$. The subsets E and $f(E)$ have the same factorial sequence if and only if $f(X) = uX + b$ where $u \in U_K$ and $b \in O_K$.*

Proof. If E and $f(E)$ have the same factorial sequence, then the preceding proposition implies $f(X) = uX + b$. Since $(n!)_{f(E)}^{O_K} = u^n (n!)_E^{O_K}$ for $n \in \mathbb{N}$, we have $u \in U_K$. Finally, for $x \in E$, one has $ux \in O_K$ and $ux + b \in O_K$; consequently, $b \in O_K$.

The converse is obvious. ∎

Corollary 25. *Let K be a number field, E be an infinite subset of O_K and $f \in \mathrm{Int}(E, O_K)$. If $\mathrm{Int}(E, O_K) = \mathrm{Int}(f(E), O_K)$, then $f(X) = uX + b$ where $u \in U_K$ and $b \in O_K$.*

Proposition 26. *Let K be a number field, E be an infinite subset of O_K and $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, O_K)$. If $((n!)_E^{O_K})_{\mathfrak{M}} = ((n!)_{\varphi(E)}^{O_K})_{\mathfrak{M}}$ for all $n \in \mathbb{N}$ and all maximal ideals $\mathfrak{M}$ of O_K but a finite number, then*

$$\varphi = \frac{aX + b}{cX + d} \quad \text{where} \quad ad - bc \neq 0.$$

Proof. Write $\varphi(X) = g(X)/f(X)$ where f and g are polynomials of $O_K[X]$ relatively prime in $K[X]$. As O_K is a δ-ring, φ admits at most one pole. Thus, $f(X) = \lambda(X - e)^n$ where $\lambda, e \in K$ and $n = \deg f$. If $n = 0$, Proposition 23 allows us to conclude. Assume now that $n > 0$. By Bézout, there exist $d \in O_K$ and $u, v \in O_K[X]$ such that $uf + vg = d$. Let S_1 be the set of all maximal ideals $\mathfrak{M}$ of O_K such that $((n!)_E^{O_K})_{\mathfrak{M}} = ((n!)_{\varphi(E)}^{O_K})_{\mathfrak{M}}$ and let S_2 be the set of all maximal ideals $\mathfrak{M}$ containing d. Let $S = S_1 \cup S_2$.

For $x \in E$, $f(x)$ divides $g(x)$, therefore $f(x)$ divides d. Consequently, for $x \in E$ and $\mathfrak{M} \notin S_2$, $v_{\mathfrak{M}}(f(x)) = 0$. Thus for $x, y \in E$ and $\mathfrak{M} \notin S_2$,

$$v_{\mathfrak{M}}(\varphi(x) - \varphi(y)) = v_{\mathfrak{M}}(g(x)f(y) - f(x)g(y)) \geq v_{\mathfrak{M}}(x - y).$$

According to Proposition 22, for all $\mathfrak{M} \notin S$ and all $x, y \in E$, $x \neq y$, one has

$$v_{\mathfrak{M}}(g(x)f(y) - f(x)g(y)) = v_{\mathfrak{M}}(x - y).$$

Write $g(X)f(Y) - f(X)g(Y) = (X-Y)h(X,Y)$ where $h(X,Y) \in O_K[X,Y]$. Fix $y \in E \setminus \{e\}$. Then, for all $\mathfrak{M} \notin S$ and every $x \in E \setminus \{y\}$, one has $v_{\mathfrak{M}}(h(x,y)) = 0$. Since $O_{K,S}$ is a δ-ring (Corollary 18), one has $h(X,y) = \mu(X-e)^m$ where $\mu \in K$ and $m \in \mathbb{N}$. Then $(X-e)^{\inf(n,m)}$ divides $f(X)$ and $g(X)$. Consequently, $m = 0$ since $n > 0$, in other words $g(X)f(y) - f(X)g(y) = \mu(X-y)$. This equality implies $\deg f \leq 1$ and $\deg g \leq 1$. Indeed, let $g(X) = q(X)f(X) + r(X)$ where $\deg r < \deg f$; then

$$(q(X)f(y) - g(y))f(X) + f(y)r(X) = \mu(X-y)$$

shows that $\deg f \leq 1$.

Thus, $\varphi(X) = (aX+b)/(cX+d)$ where $ad - bc \neq 0$ because φ cannot be constant. ∎

Corollary 27. *Let E be an infinite subset of O_K and $\varphi \in \mathrm{Int}^{\mathrm{R}}(E, O_K)$. If $\mathrm{Int}(\varphi(E), O_K) = \mathrm{Int}(E, O_K)$, then $\varphi(X) = (aX+b)/(cX+d)$ where $ad - bc \neq 0$.*

One may omit the condition $E \subseteq O_K$ of the previous proposition by considering more general fractional subsets of K. Recall that a subset E of K is *fractional* if there exists a non-zero element $d \in O_K$ such that $dE \subseteq O_K$. Let E be such a subset of K. For every $f \in K[X]$, $f \in \mathrm{Int}(E, O_K)$ if and only if $f(X/d) \in \mathrm{Int}(dE, O_K)$. Thus, we have the formulas

$$(n!)_{dE}^{O_K} = d^n (n!)_E^{O_K} \quad \text{and} \quad (n!)_{E+\nu}^{O_K} = (n!)_E^{O_K}$$

for every $d \in K^*$ and $\nu \in K$.

It is known that a subset E of K is not fractional if and only if $\mathrm{Int}(E, O_K) = O_K$, and hence, $(n!)_E^{O_K} = O_K$ for every $n \geq 1$. Moreover, a subset E is of cardinality less than $n \in \mathbb{N}$ if and only if $(n)!_E^{O_K} = (0)$. Consequently, we have:

Lemma 28. *For every infinite fractional subset E of K and every $\varphi \in K(X)$ without any pole in E, if $(n!)_{\varphi(E)}^{O_K} = (n!)_E^{O_K}$ for every $n \in \mathbb{N}$, then $\varphi(E)$ is also an infinite fractional subset of K.*

Theorem 29. *Let K be a number field, E be an infinite fractional subset of K and $\varphi \in K(X)$. If $(n!)_E^{O_K} = (n!)_{\varphi(E)}^{O_K}$ for all $n \in \mathbb{N}$, then $\varphi(X) = (aX+b)/(cX+d)$ with $ad - bc \neq 0$.*

Proof. Let $\delta \in O_K$ be such that $\delta E = E' \subseteq O_K$ and $\delta\varphi(E) \subseteq O_K$. Since $(n!)_E^{O_K} = (n!)_{\varphi(E)}^{O_K}$ for all $n \in \mathbb{N}$, we have $(n!)_{E'}^{O_K} = (n!)_{\psi(E')}^{O_K}$ for all $n \in \mathbb{N}$ where $\psi(X) = \delta\varphi(X/\delta)$. According to Proposition 26, ψ and φ are homographic functions. ∎

REMARK 30. Let K be a number field and let $\varphi(X)=(aX+b)/(cX+d) \in K(X)$ with $ad-bc\neq 0$. Conversely, one may wish to know whether there exists an infinite fractional subset E such that $(n!)_E^{O_K} = (n!)_{\varphi(E)}^{O_K}$. There are two distinct cases:

(1) If $c=0$, then φ is a polynomial and the answer is affirmative if and only if a is an element of U_K (Corollary 24). In this case, we have $(n!)_E^{O_K} = (n!)_{\varphi(E)}^{O_K}$ for every infinite fractional subset E of K.

(2) If $c\neq 0$, again one distinguishes two cases:

   (a) The unit group U_K of O_K is finite. It follows from Proposition 13 that the answer is negative.

   (b) The unit group U_K of O_K is infinite. Let λ be a non-zero element of K, $E(\lambda)=U_K\cup\lambda U_K$ and $\psi(X)=\lambda/X$. Then $E(\lambda)$ is an infinite fractional subset of K and $\psi(E(\lambda))=E(\lambda)$. In particular, ψ preserves the factorial sequence of the infinite fractional subset $E(\lambda)$. Now write

$$\varphi(X)=\frac{bc-ad}{c^2}\,\frac{1}{X+d/c}+\frac{a}{c}.$$

   Then $\varphi(X)=f_2\circ\varphi_1\circ f_1(X)$ where $f_1(X)=X+d/c$,

$$\varphi_1(X)=\lambda/X \quad \text{with} \quad \lambda=\frac{bc-ad}{c^2}\,\frac{1}{X}$$

   and $f_2(X)=X+a/c$. Let $E=E(\lambda)-d/c$. Then φ preserves the factorial sequence of the infinite fractional subset E because $\varphi(E)=E(\lambda)+a/c$ and the translation obviously preserves the factorial sequence.The answer is then affirmative.

It would be interesting to characterize all the infinite fractional subsets of K whose factorial sequence is preserved by a given $\varphi(X)=(aX+b)/(cX+d) \in K(X)$ with $ad-bc\neq 0$ and $c\neq 0$.

We end with a proposition without proof because the previous proofs may be easily extended to the following case:

PROPOSITION 31. *Let D be a Dedekind domain with quotient field F and with finite residue fields. If, for every finite set S of maximal ideals of D, $D_S=\{x\in F \mid v_{\mathfrak{M}}(x)=0\ \forall \mathfrak{M}\notin S\}$ is a δ-ring, then Theorem 29 still holds with F and D instead of K and O_K.*

References

[1] D. Anderson and B. Mullins, *Finite factorization domains*, Proc. Amer. Math. Soc. 124 (1996), 389–396.

[2] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math. 490 (1997), 101–127.
[3] D. Brizolis, *Hilbert rings of integral-valued polynomials*, Comm. Algebra 3 (1975), 1051–1081.
[4] P. J. Cahen and J. L. Chabert, *Integer Valued Polynomials*, Math. Surveys Monogr. 48, Amer. Math. Soc., Providence, 1997.
[5] L. Denis et S. Dion, *Valeurs entières de fractions rationnelles*, Acta Arith. 117 (2005), 149–169.
[6] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.
[7] Y. Fares, *Factorial preservation*, Arch. Math. (Basel) 83 (2004), 497–506.
[8] R. Gilmer and W. Smith, *On the polynomial equivalence of subsets E and $f(E)$ of $\mathbb{Z}$*, ibid. 73 (1999), 355–365.
[9] H. Gunji and D. L. McQuillan, *On rings with a certain divisibility property*, Michigan Math. J. 22 (1975), 289–290.
[10] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Math. 1600, Springer, 1995.

LAMFA CNRS UMR 6140
Université de Picardie
80039 Amiens, France
E-mail: youssef.fares@u-picardie.fr

Received on 20.10.2005
and in revised form on 11.2.2006 (5082)