Ark. Mat., **31** (1993), 297–305


# On the asymptotic behaviour of the number of distinct factorizations into irreducibles

Franz Halter-Koch

**Abstract.** For an integral domain $R$ and a non-zero non-unit $a \in R$ we consider the number of distinct factorizations of $a^n$ into irreducible elements of $R$ for large $n$. Precise results are obtained for Krull domains and certain noetherian domains. In fact, we prove results valid for certain classes of monoids which then apply to the above-mentioned classes of domains.

**1.** Throughout this paper, a *monoid* $H$ is a multiplicative commutative and cancellative semigroup with unit element $1 \in H$. For any $a_1, \ldots, a_m \in H$, we denote by $[a_1, \ldots, a_m]$ the submonoid of $H$ generated by $a_1, \ldots, a_m$. We denote by $H^\times$ the group of invertible elements of $H$, and we use the notions of divisibility theory in $H$ as introduced in [6], § 6 or [9], ch. 2.14. A monoid $H$ is called *reduced* if $H^\times = \{1\}$. By a *factorization* of an element $a \in H \setminus H^\times$ we mean a relation of the form $a \sim u_1 \cdot \ldots \cdot u_r$ where $u_i \in H$ are irreducible elements. Two such factorizations, say $a \sim u_1 \cdot \ldots \cdot u_r$ and $a \sim u'_1 \cdot \ldots \cdot u'_{r'}$, are called *not essentially different* if $r = r'$ and $u_{\sigma(i)} \sim u'_i$ for some permutation $\sigma \in \mathfrak{S}_r$ and all $i \in \{1, \ldots, r\}$. We denote by $\mathbf{f}(a)$ the number of essentially different factorizations of $a$. We shall be concerned with the behaviour of $\mathbf{f}(a^n)$ as $n \to \infty$. The corresponding question concerning merely the lenghts of factorizations of $a^n$ as $n \to \infty$ has been dealt with in [1] and [5].

A monoid $H$ is called an FF-*monoid* (*finite factorization monoid*) if $1 \le \mathbf{f}(a) < \infty$ for all $a \in H \setminus H^\times$; see [8] for a detailed discussion. Our main results are the following two theorems.

**Theorem 1.** *Let $H$ be an* FF-*monoid, $a \in H \setminus H^\times$, and suppose that there exist (up to associates) only finitely many irreducible elements $u_1, \ldots, u_m \in H$ dividing some power $a^n$ of $a$. Let $r$ be the maximal number of $\mathbf{Q}$-linearly independent vectors $(k_1, \ldots, k_m) \in \mathbf{N}_0^m$ such that $u_1^{k_1} \cdot \ldots \cdot u_m^{k_m} \in [a]$. Then there exists a constant $A \in \mathbf{Q}_{>0}$ such that*

$$\mathbf{f}(a^n) = An^{r-1} + O(n^{r-2}).$$

**Theorem 2.** *Let $H$ be an* FF*-monoid, $a \in H \setminus H^{\times}$, and suppose that there exist infinitely many mutually non-associated irreducible elements $u \in H$ dividing some power $a^n$ of $a$. Then we have*

$$\mathbf{f}(a^n) \gg n^r$$

*for every $r \in \mathbf{N}$.*

The proofs of these two theorems will be given in Section 5. They are based on a general finiteness result for finitely generated monoids (Proposition 1) to be dealt with in Section 4. In the following two sections we discuss arithmetical applications.

**2**. Let us call a monoid $H$ an SFF*-monoid* (*strong finite factorization monoid*) if, for any $a \in H \setminus H^{\times}$, there exist (up to associates) only finitely many irreducible elements of $H$ dividing some power $a^n$ of $a$. Thus in an SFF-monoid $H$ Theorem 1 applies for all $a \in H \setminus H^{\times}$.

Every Krull monoid is an SFF-monoid. More generally, every saturated submonoid of a monoid with nearly unique factorization is an SFF-monoid (see [5], Proposition 2 and Corollary 1).

For an integral domain $R$, we denote by $R^{\bullet} = R \setminus \{0\}$ its multiplicative monoid; we study the arithmetic of $R$ by means of the monoid $R^{\bullet}$. We call $R$ an SFF*-domain* if $R^{\bullet}$ is an SFF-monoid. In an SFF-domain, every non-zero non-unit satisfies the assumptions of Theorem 1.

If $R$ is a Krull domain, then $R^{\bullet}$ is a Krull monoid (cf. [7], Satz 5), and therefore $R$ is an SFF-domain. In general, a noetherian domain need not be an SFF-domain; see the subsequently discussed example $R = \mathbf{Z}[\sqrt{-7}]$. Criteria for a noetherian domain to be an SFF-domain may be found in [5], Theorems 4, 5 and Corollary 2.

**3**. In this section we present four examples, two for each theorem.

*Example* 1. Let $K$ be an algebraic number field, $R$ its ring of integers, and assume that the ideal class group $G$ of $R$ is an elementary abelian 2-group of rank $N \geq 2$. Let $\mathfrak{c}_1, \dots, \mathfrak{c}_N$ be a basis of $G$, and let $\mathbf{p}_0 \in \mathfrak{c}_1 \cdot \ldots \cdot \mathfrak{c}_N, \mathbf{p}_1 \in \mathfrak{c}_1, \dots, \mathbf{p}_N \in \mathfrak{c}_N$ be prime ideals. Then there exist elements $u$, $u_0$, $u_1, \dots, u_N \in R$ such that $(u) = \mathbf{p}_0 \mathbf{p}_1 \cdot \ldots \cdot \mathbf{p}_N$ and $(u_i) = \mathbf{p}_i^2$ for $0 \leq i \leq n$. Obviously, $u$, $u_0, \dots, u_N$ are irreducible elements of $R$, and they are (up to associates) the only irreducible elements of $R$ dividing some power $u^n$ of $u$. From the unique factorization into prime ideals we see that all factorizations of $u^n$ are of the form

$$u^n \sim u^{\alpha} u_0^{\beta} u_1^{\beta} \cdot \ldots \cdot u_N^{\beta}, \quad \text{where } n = \alpha + 2\beta.$$

This implies

$$\mathbf{f}(u^n) = \left[\frac{n}{2}\right] + 1 = \frac{n}{2} + O(1),$$

and indeed, $r=2$ is the maximal number of linearly independent vectors in the system

$$\{(\alpha,\beta,\dots,\beta)\in\mathbf{N}_0^{N+2}\,|\,\alpha,\beta\in\mathbf{N}_0\}.$$

*Example* 2. Let $K$ be an algebraic number field, $R$ its ring of integers, and assume that the ideal class group $G$ of $R$ is cyclic of order $N\geq 2$. Let $\mathfrak{c}$ be a generating class of $G$, and let $\mathbf{p}_1,\dots,\mathbf{p}_N\in\mathfrak{c}$ be distinct prime ideals. Let $\mathcal{A}$ be the set of all vectors $\boldsymbol{\alpha}=(\alpha_1,\dots,\alpha_N)\in\mathbf{N}_0^N$ such that $N=\alpha_1+\dots+\alpha_N$. For any $\boldsymbol{\alpha}\in\mathcal{A}$, there is an irreducible element $u_{\boldsymbol{\alpha}}\in R$ such that $(u_{\boldsymbol{\alpha}})=\mathbf{p}_1^{\alpha_1}\cdot\ldots\cdot\mathbf{p}_N^{\alpha_N}$. We set $a=u_{(1,\dots,1)}\in R$, and we use Theorem 1 to determine the asymptotic behaviour of $\mathbf{f}(a^n)$. Obviously, $\{u_{\boldsymbol{\alpha}}\,|\,\boldsymbol{\alpha}\in\mathcal{A}\}$ is a complete system of mutually not associated irreducible elements of $R$ dividing some power $a^n$ of $a$. The factorizations of $a^n$ are of the form

$$a^n\sim\prod_{\boldsymbol{\alpha}\in\mathcal{A}}u_{\boldsymbol{\alpha}}^{k(\boldsymbol{\alpha})},$$

where the exponent vectors $(k(\boldsymbol{\alpha}))_{\boldsymbol{\alpha}\in\mathcal{A}}\in\mathbf{N}_0^{\mathcal{A}}$ satisfy the relations

$$\sum_{\boldsymbol{\alpha}\in\mathcal{A}}k(\boldsymbol{\alpha})\alpha_i=n\quad\text{for all } i\in\{1,\dots,N\}.$$

By Theorem 1 we obtain

$$\mathbf{f}(a^n)=An^{r-1}+O(n^{r-2}),$$

where $A\in\mathbf{Q}_{>0}$, and $r$ is the maximal number of linearly independent vectors

$$(k(\boldsymbol{\alpha}))_{\boldsymbol{\alpha}\in\mathcal{A}}\in\mathbf{N}_0^{\mathcal{A}}$$

satisfying the relations

$$\sum_{\boldsymbol{\alpha}\in\mathcal{A}}k(\boldsymbol{\alpha})(\alpha_i-\alpha_1)=0,\quad(i=2,\dots,N).$$

These $N-1$ relations are linearly independent: Indeed, if $\lambda_2,\dots,\lambda_N\in\mathbf{Q}$ are such that

$$\sum_{i=2}^{N}\lambda_i(\alpha_i-\alpha_1)=0\quad\text{for all }\boldsymbol{\alpha}\in\mathcal{A},$$

then the vectors $\boldsymbol{\alpha}=(0,\dots,0,N,0,\dots,0)\in\mathcal{A}$ show that $\lambda_2=\dots=\lambda_N=0$. This implies

$$r=\#\mathcal{A}-N+1=\binom{2N-1}{N}-N+1.$$

*Example* 3. We consider the multiplicative monoid $H=\{1\}\cup 2\mathbf{N}$. The irreducible elements of $H$ are the numbers $u\equiv 2 \mod 4$, $H$ is an FF-monoid, and any two factorizations of an element $a\in H\setminus\{1\}$ have the same length. For an odd prime number $p$, we consider the element $a=2p$. The irreducible elements of $H$ dividing some power $a^n$ of $a$ are the elements $u_\alpha=2p^\alpha$ for $\alpha\in\mathbf{N}_0$, and the factorizations of $a^n$ are of the form

$$a^n=\prod_{i=1}^{n}(2p^{\alpha_i}),\quad \text{where } n=\alpha_1+\ldots+\alpha_n,$$

whence they correspond bijectively to the partions of $n$, which implies

$$\mathbf{f}(a^n)=p(n)\sim\frac{1}{4n\sqrt{3}}\exp\left\{\pi\sqrt{\frac{2n}{3}}\right\};$$

see [11], Theorem 6.10 and [12], §2.7.

*Example* 4. We consider the ring $R=\mathbf{Z}[\sqrt{-7}]$ which is the simplest example of a noetherian domain not being an SFF-domain. We shall prove the estimate

$$\mathbf{f}(2^n)\gg\frac{1}{n^2}\exp\left\{\pi\sqrt{\frac{2n}{3}}\right\},$$

which is substantially stronger than Theorem 2.

For $i\geq 1$, the elements

$$u_i=2\left(\frac{1+\sqrt{-7}}{2}\right)^i \quad\text{and}\quad \bar{u}_i=2\left(\frac{1-\sqrt{-7}}{2}\right)^i$$

are irreducible in $\mathbf{Z}[\sqrt{-7}]$, and the elements 2, $u_i$, $\bar{u}_i (i\geq 1)$ are (up to associates) the only irreducible elements of $\mathbf{Z}[\sqrt{-7}]$ which divide some power $2^n$ of 2 in $R$ (to see this, consider the factorial ring $\mathbf{Z}[(1+\sqrt{-7})/2]$, where $2=(1+\sqrt{-7})/2\cdot(1-\sqrt{-7})/2)$. The factorizations of $2^n$ in $\mathbf{Z}[\sqrt{-7}]$ are of the form

$$2^n=2^\alpha\cdot\prod_{i=1}^{n-2}(u_i\bar{u}_i)^{\alpha_i},$$

where $\alpha,\ \alpha_1,\ldots,\alpha_{n-2}\in\mathbf{N}_0$ are the solutions of the equation

$$(*)\qquad n=\alpha+\sum_{i=1}^{n-2}(i+2)\alpha_i\,;$$

consequently, $\mathbf{f}(2^n)$ is the number of solutions $(\alpha, \alpha_1, \ldots, \alpha_{n-2}) \in \mathbf{N}_0^{n-1}$ of (*). The partition function $p(n)$ counts the number of solutions $(\alpha, \alpha_0, \ldots, \alpha_{n-2}) \in \mathbf{N}_0^n$ of the equation

$$n = \alpha + 2\alpha_0 + 3\alpha_1 + \ldots + n\alpha_{n-2}$$

(see [11], Lemma 6.12), and therefore

$$p(n) = \sum_{i=0}^{[n/2]} \mathbf{f}(2^{n-2i}) \leq n\mathbf{f}(2^n),$$

which implies

$$\mathbf{f}(2^n) \geq \frac{p(n)}{n} \gg \frac{1}{n^2} \exp\left\{\pi\sqrt{\frac{2n}{3}}\right\}$$

by [11], Theorem 6.10 and [12], §2.7.

**4.** The following finiteness result is of interest in itself

**Proposition 1.** *Let $H = [a_1, \ldots, a_t]$ be a finitely generated torsion-free monoid and $F: H \to \mathbf{N}_0$ a function with the following properties:*
*(1) $F(xy) = F(x) + F(y)$ for all $x, y \in H$;*
*(2) $1 = F(a_1) \leq F(a_2) \leq \ldots \leq F(a_t)$.*
*For $n \in \mathbf{N}_0$, we set*

$$A_n = \#F^{-1}(n) = \#\{x \in H \mid F(x) = n\}.$$

*Let*

$$r = \dim_{\mathbf{Q}} \mathbf{Q} \otimes \mathcal{Q}(H) \geq 1$$

*be the torsion-free rank of a quotient group $\mathcal{Q}(H)$ of $H$. Then we have*

$$\sum_{n=0}^{\infty} A_n t^n = \frac{f(t)}{(1-t)(1-t^{d_2}) \cdot \ldots \cdot (1-t^{d_r})},$$

*where $f(t) \in \mathbf{Q}[t]$, $f(1) \neq 0$ and $d_2, \ldots, d_r \in \mathbf{N}$. In particular, there is a constant $A \in \mathbf{Q}_{>0}$ such that*

$$A_n = An^{r-1} + O(n^{r-2}).$$

The proof of Proposition 1 depends on two Lemmata; the first one belongs to commutative algebra, the second one is of combinatorial nature.

**Lemma 1.** *Let*

$$R=\bigoplus_{n\geq 0} R_n=k[x_1,\ldots,x_t]$$

*be a graded domain, where* $R_0=k$ *is a field,* $x_1,\ldots,x_t\in R$ *are homogeneous elements,* $0\neq x_1\in R_1$ *and* $r=\mathrm{tr.deg}(R/k)\geq 1$. *Then there exist homogeneous elements* $x_2',\ldots,x_r'\in R$ *such that* $x_1, x_2',\ldots,x_r'$ *is a transcendence basis of* $R/k$, *and* $R$ *is integral over* $k[x_1,x_2',\ldots,x_r']$. *The Poincaré series of* $R$ *is of the form*

$$\sum_{n=0}^{\infty}(\dim_k R_n)t^n=\frac{f(t)}{(1-t)(1-t^{d_2})\cdot\ldots\cdot(1-t^{d_r})},$$

*where* $f(t)\in\mathbf{Q}[t]$, $f(1)\neq 0$ *and* $d_2,\ldots,d_r\in\mathbf{N}$.

*Proof.* See [13], § 6. □

**Lemma 2.** *Let* $d_1,\ldots,d_r$ *be positive integers such that* $\gcd(d_1,\ldots,d_r)=1$ *and* $\mathrm{lcm}(d_1,\ldots,d_r)=d\in\mathbf{N}$. *Let* $f(t)\in\mathbf{Q}[t]$ *be a polynomial,* $f(1)\neq 0$, *and set*

$$\frac{f(t)}{(1-t^{d_1})\cdot\ldots\cdot(1-t^{d_r})}=\sum_{n=0}^{\infty}A_nt^n\in\mathbf{Q}\,[\![t]\!].$$

*Then there exist polynomials* $P_0,\ldots,P_{d-1}\in\mathbf{Q}[z]$, *all of degree* $r-1$ *and with leading coefficient* $f(1)[d_1\cdot\ldots\cdot d_r(r-1)!]^{-1}$ *such that* $A_n=P_\nu(n)$ *for all sufficiently large* $n\equiv\nu \mod d$ *and* $0\leq\nu<d$. *In particular,*

$$\lim_{n\to\infty}\frac{A_n}{n^{r-1}}=\frac{f(1)}{d_1\cdot\ldots\cdot d_r(r-1)!}.$$

*Proof* (following a suggestion of R. Tichy; a weaker result is in [3], 2.6). We start with a preliminary remark of general nature. For $\alpha\in\mathbf{C}$ and $m\in\mathbf{N}$, we consider the binomial series

$$(1-\alpha t)^{-m}=\sum_{n=0}^{\infty}\binom{n+m-1}{m-1}\alpha^nt^n\in\mathbf{C}\,[\![t]\!].$$

For a polynomial $g(t)=c_0+c_1t+\ldots+c_st^s\in\mathbf{Q}[t]$ we obtain

$$\frac{g(t)}{(1-\alpha t)^m}=\sum_{n=0}^{\infty}B_nt^n,$$

where, for $n \geq s$,

$$B_n = \sum_{\nu=0}^{s} c_\nu \binom{n-\nu+m-1}{m-1} \alpha^{n-\nu} = Q(n)\alpha^n$$

and

$$Q(z) = \frac{g(\alpha^{-1})}{(m-1)!} z^{m-1} + \ldots \in \mathbf{C}[z].$$

Now we are well prepared for the proof of Lemma 2. We set

$$(1-t^{d_1}) \cdot \ldots \cdot (1-t^{d_r}) = (1-t)^r \cdot \prod_{j=1}^{s} (1-\xi_j^{-1} t)^{r_j},$$

where $1, \xi_1, \ldots, \xi_s \in \mathbf{C}$ are distinct $d$-th roots of unity, and $1 \leq r_j < r$ for all $j \in \{1, \ldots, s\}$, since $\gcd(d_1, \ldots, d_r) = 1$. We use the partial fractions decomposition in the form

$$\frac{f(t)}{(1-t^{d_1}) \cdot \ldots \cdot (1-t^{d_r})} = \frac{f_0(t)}{(1-t)^r} + \sum_{j=1}^{s} \frac{f_j(t)}{(1-\xi_j^{-1} t)^{r_j}},$$

where $f_0(t) \in \mathbf{Q}[t]$, $f_0(1) \neq 0$ and $f_1(t), \ldots, f_s(t) \in \mathbf{C}[t]$. Now we expand the fractions into power series and obtain from the formulas derived above:

$$A_n = Q_0(n) + \sum_{j=1}^{s} Q_j(n) \xi_j^{-n}$$

for all sufficiently large $n$, where

$$Q_0(z) = \frac{f_0(1)}{(r-1)!} z^{r-1} + \ldots \quad \text{and} \quad Q_j(z) = \frac{f_j(\xi_j)}{(r_j-1)!} z^{r_j-1} + \ldots \in \mathbf{C}[z].$$

Since $\xi_j^d = 1$, the factors $\xi_j^{-n}$ depend only on the residue class of $n$ modulo $d$. Observing $r_j < r$, $A_n \in \mathbf{Q}$ and

$$f_0(1) = \lim_{t \to 1} \frac{f(t)(1-t)^r}{(1-t^{d_1}) \cdot \ldots \cdot (1-t^{d_r})} = \frac{f(1)}{d_1 \cdot \ldots \cdot d_r},$$

the assertion follows. □

*Proof of Proposition* 1. Since $H$ is torsion-free, the monoid ring $R = \mathbf{Q}[H]$ is a domain by [6], Theorem 8.1, and clearly $r = \operatorname{tr.deg}(R/\mathbf{Q})$. We make $R$ into a graded ring by setting

$$R = \bigoplus_{n \geq 0} R_n, \quad \text{where } R_n = \bigoplus_{x \in F^{-1}(n)} \mathbf{Q}x\,;$$

since $A_n = \#F^{-1}(n) = \dim_{\mathbf{Q}} R_n$, the result follows from Lemma 1 and Lemma 2. □

Next we show how Proposition 1 implies factorization properties.

**Proposition 2.** *Let $H=[u_1,\dots,u_m]$ be a finitely generated reduced monoid, $1\notin\{u_1,\dots,u_m\}$ and $1\neq a\in H$. For $n\in\mathbf{N}_0$, we set*

$$A_n=\#\{(k_1,\dots,k_m)\in\mathbf{N}_0^m \mid u_1^{k_1}\cdot\ldots\cdot u_m^{k_m}=a^n\}.$$

*Let $r$ be the maximal number of $\mathbf{Q}$-linearly independent vectors $(k_1,\dots,k_m)\in\mathbf{N}_0^m$ such that $u_1^{k_1}\cdot\ldots\cdot u_m^{k_m}\in[a]$. Then there exists a constant $A\in\mathbf{Q}_{>0}$ such that*

$$A_n=An^{r-1}+O(n^{r-2}).$$

*Proof.* For $m\in\mathbf{N}$, we write the elements of $\mathbf{N}_0^m$ in the form $\mathbf{k}=(k_1,\dots,k_m)$. For $\mathbf{k}$, $\mathbf{k}'\in\mathbf{N}_0^m$, we define $\mathbf{k}\leq\mathbf{k}'$ by $k_j\leq k_j'$ for all $j\in\{1,\dots,m\}$. Then $(\mathbf{N}_0^m,+,\leq)$ becomes an ordered additive monoid, and we shall use the fact that every non-empty subset $M\subset\mathbf{N}_0^m$ has only finitely many minimal points, cf. [2], Theorem 9.18. The set

$$\Gamma=\{\mathbf{k}\in\mathbf{N}_0^m \mid u_1^{k_1}\cdot\ldots\cdot u_m^{k_m}\in[a]\}$$

is a submonoid of $\mathbf{N}_0^m$ with the property that $\mathbf{m}$, $\mathbf{n}\in\Gamma$, $\mathbf{m}\geq\mathbf{n}$ implies $\mathbf{m}-\mathbf{n}\in\Gamma$. Therefore $\Gamma$ is generated by the minimal points of $\Gamma\setminus\{\mathbf{0}\}$, say $\mathbf{k}^{(1)},\dots,\mathbf{k}^{(t)}$. We define $F:\Gamma\to\mathbf{N}_0$ by

$$F(\mathbf{k})=n \quad \text{if } u_1^{k_1}\cdot\ldots\cdot u_m^{k_m}=a^n\,;$$

Proposition 1 implies the assertion. □

**5.** *Proof of Theorem* 1. Passing from $H$ to $H/H^\times$, we may assume that $H$ is reduced. Then there exist only finitely many irreducible elements $u_1,\dots,u_m$ in $H$ dividing some power $a^n$ of $a$. The result follows by applying Proposition 2 to $[u_1,\dots,u_m]$, since

$$\mathbf{f}(a^n)=\#\{(k_1,\dots,k_m)\in\mathbf{N}_0^m \mid u_1^{k_1}\cdot\ldots\cdot u_m^{k_m}=a^n\}.$$

*Proof of Theorem* 2. We may again assume that $H$ is reduced. Since $H$ is an FF-monoid, every power $a^n$ of $a$ is divisible by only finitely many irreducible elements of $H$. Therefore, by assumption, there exists a sequence $(u_i)_{i\geq1}$ of irreducible elements of $H$ and there exist sequences $1\leq m_1<m_2<\ldots$ and $1\leq n_1<n_2<\ldots$ such that $u_1,\dots,u_{m_i}$ are all irreducible elements of $H$ dividing $a^{n_i}$. For $i\geq1$, set

$$\Gamma_i=\{(k_1,\dots,k_{m_i})\in\mathbf{N}_0^{m_i} \mid u_1^{k_1}\cdot\ldots\cdot u_{m_i}^{k_{m_i}}\in[a]\},$$

and denote by $r_i$ the maximal number of $\mathbf{Q}$-linearly independent vectors in $\Gamma_i$ ; then we obtain

$$\mathbf{f}(a^n)\geq\#\{\mathbf{k}\in\Gamma_i \mid u_1^{k_1}\cdot\ldots\cdot u_{m_i}^{k_{m_i}}=a^n\}\gg n^{r_i-1}$$

by Proposition 2. If $(k_1, ..., k_{m_i}) \in \Gamma_i$, then $(k_1, ..., k_{m_i}, 0, ..., 0) \in \Gamma_{i+1}$; however, there exist elements $\mathbf{k} \in \Gamma_{i+1}$ such that $k_j \geq 1$ for some $m_j < j \leq m_{i+1}$, and therefore $r_{i+1} > r_i$. Now the assertion follows. □

*Remark.* It is possible to give a proof of Proposition 2 using geometrical methods instead of those of commutative algebra (Lemma 1). These geometrical proofs either rely upon [10], Ch. VI, §2, Theorem 2, or on the combinatorial ideas outlined in [4]. In both cases it is rather difficult to prove that $A$ is a rational (and not only a real) number and to give a precise description of the exponent $r$. However, we do not know of a proof of the (stronger) Proposition 1 without using commutative algebra.

## References


1. ANDERSON, D. F. and PRUIS, P., Length functions on integral domains, *Proc. Amer. Math. Soc.* **113** (1991), 933–937.
2. CLIFFORD, A. H. and PRESTON, G. B., *The Algebraic Theory of Semigroups. Vol. II*, Amer. Math. Soc. Providence, R. I., 1967.
3. COMTET, L., *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974.
4. EHRHART, E., Sur un problème de géometrie diophantienne linéaire I, *J. Reine Angew. Math.* **226** (1967), 1–29.
5. GEROLDINGER, A. and HALTER-KOCH, F., On the asymptotic behaviour of lengths of factorizations, *J. Pure Appl. Algebra* **77** (1992), 239–252.
6. GILMER, R., *Commutative Semigroup Rings*, Univ. of Chicago Press, Chicago, Ill., 1984.
7. HALTER-KOCH, F., Ein Approximationssatz für Halbgruppen mit Divisorentheorie, *Resultate Math.* **19** (1991), 74–82.
8. HALTER-KOCH, F., Finiteness theorems for factorizations, *Semigroup Forum* **44** (1992), 112–117.
9. JACOBSON, N., *Basic Algebra I*, Freeman, New York, 1974.
10. LANG, S., *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.
11. NARKIEWICZ, W., *Number Theory*, World Scientific, Singapore, 1983.
12. POSTNIKOV, A. G., *Introduction to Analytic Number Theory, Translations of Math. Monographs* **68**, Amer. Math. Soc., Providence, R.I., 1988.
13. SMOKE, W., Dimension and multiplicity for graded algebras, *J. Algebra* **21** (1972), 149–173.


*Received February 11, 1993*

Franz Halter-Koch
Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36/IV
A-8010 Graz
Österreich