Factorization of a non-zero polynomial over an Artinian, local, principal ideal ring

Ornella Greco

Abstract

In this work, we study the factorization in $A[x]$, where A is an Artinian local principal ideal ring, whose maximal ideal, (t), has nilpotency h.
This is not a unique factorization ring, indeed its elasticity is infinity, but in this ring some uniqueness properties about factorization hold: in fact, we prove that a non-zero polynomial in $A[x]$ can be written in quite a unique way as the product of a power of t, of a unit, and of finitely many primary, monic, pairwise coprime polynomials.

1 Non-unique Factorization in $A[x]$, where A is an Artinian, principal and local ring.

The aim of this work has been to investigate the non-unique factorization of polynomials in $A[x]$ into irreducible elements, where $(A, \underline{m})$ is an Artinian, principal and local ring, that is not a domain.
Let us denote by $\mu : A[x] \to K[x]$, where $K = A/\underline{m}$, the natural extension to the polynomial rings of the canonical projection. We will use this notation throughout the paper.

An Artinian, local, principal ideal ring is just the same as a special PIR (*SPIR*), which is a principal ideal ring, with a single nilpotent prime ideal: for this reason, throughout the paper we will not distinguish between these two kinds of ring.

Let us notice that the ring A is principal and local, so there is a $t \in A$ such that $\underline{m} = (t)$, moreover, because of the fact that A is Artinian, there exists an $h \in \mathbb{N},\ h > 0$, such that $t^h = 0$.
From these facts, we deduce that each non-zero and non-unit element $a \in A$, $a \neq 0$, can be represented in a unique way as

$$a = ut^k, \text{ where } u \text{ is a unit and } k \in \mathbb{N},\ k < h. \tag{1}$$

We have also that the factorization of $a = ut^k$ is unique, because of the fact that t^k is the greatest power of t that divides a.

Let $(\mathbb{N}_h; +; \leq)$ be the ordered monoid with elements $0, 1, \ldots, h-1, \infty$ obtained factoring $(\mathbb{N}_0 \cup \{\infty\}; +; \leq)$ by the congruence relation that identifies all numbers greater and equal to h, including ∞. Let us define $v : A \to \mathbb{N}_h$ by putting $v(a) = k \in \mathbb{N}_h$, if $a \neq 0$, and $v(0) = \infty$.
This map is called *t-adic valuation*, since it behaves as a valuation.
We now announce some simple properties of this map.

Remark 1.1 *The following statements hold:*

1. $v(a) = \infty \ \Leftrightarrow a = 0$;
2. $v(a+b) \geq \min\{v(a), v(b)\}$;
3. $v(ab) = v(a) + v(b)$.

We notice that the previous map can be naturally extended to a map, that we will denote by v, by abuse of notation, defined in $A[x]$, by putting:

$$v(f(x)) = v(\sum_{i=0}^{s} a_i x^i) = \min_{i=0,\ldots,s} v(a_i).$$

We notice that also this extended map behaves as a valuation, namely we have the following properties.

Remark 1.2 *The following statements hold:*

1. $v(f) = \infty \ \Leftrightarrow f = 0$;

2. $v(f+g) \geq \min\{v(f), v(g)\}$;

3. $v(fg) = v(f) + v(g)$.

So v is a t-adic valuation in $A[x]$. The following remark underlines the relationship between the t-adic valuation in $A[x]$ and the non-zerodivisors of this ring.

Remark 1.3 *If $f \in A[x]$, the following statements are equivalent:*

1. $v(f) > 0$, *i.e. all the coefficients of f are divisible by t in A;*

2. *f is nilpotent;*

3. *f is a zerodivisor.*

In the following, we will maintain the just introduced notation.

1.1 Nilpotent elements, regular elements, zerodivisors

In this section, we want to list some useful properties of the ring $A[x]$, and in particular we want to show that, even if many different definitions for irreducible element can be given, in this case they coincide.

Definition 1.4 *Let R be a commutative ring, let $Nil(R)$ be the nilradical of R, $J(R)$ be the Jacobson radical of R, $Z(R)$ be the set of all zerodivisors in R, and $U(R)$ be the group of all the units.*

Definition 1.5 *Let R be a commutative ring, let $c \in R$, c is a regular element if c is not a zerodivisor.*

Proposition 1.6 *(see [2]) We have that*

$$x \in J(R) \iff 1 - xy \text{ is a unit } \ \forall\, y \in R.$$

Proposition 1.7 *We have that:*

$$Nil(A[x]) = Z(A[x]) = J(A[x]) = (t)A[x] = \underline{m}[x].$$

Proof
From Remark 1.3, we have that $Nil(A[x]) = Z(A[x]) = (t)$. Now we prove that the maximal ideals of $A[x]$ are precisely the ideals (t, f), where $\mu(f) \in \frac{A}{\underline{m}}[x]$ is irreducible, so we have that $J(A[x]) = (t)$.
It is easy to prove that (t, f) is a maximal ideal of $A[x]$; conversely, suppose that N is a maximal ideal of $A[x]$, $N \cap A = (t)$ because it is a prime ideal of A, so $t \in N$, now we have that

$$\frac{A[x]}{N} \cong \frac{\frac{A[x]}{\underline{m}[x]}}{\frac{N}{\underline{m}[x]}} \cong \frac{\frac{A}{\underline{m}}[x]}{\frac{N}{\underline{m}[x]}}$$

but the first ring is a field, so $N/\underline{m}[x]$ is a maximal ideal in $(A/\underline{m})[x]$, so there is an irreducible ideal $\overline{f}$ such that $N/\underline{m}[x] = (\overline{f})$. $\square$

Observation 1.8 *In paper [4], we have introduced and compared three different definitions of irreducible element, finding out that they are equivalent in a particular class of ring, i.e. the rings with only harmless zerodivisors. We now notice that because of Proposition 1.6 and Proposition 1.7 we have that*

$$Z(A[x]) \subseteq 1 - U(A[x]),$$

so this polynomial ring, by definition, is a ring with only harmless zerodivisors, and this implies that we do not have to specify the definition of irreducible element we are using.

1.2 Factorization of arbitrary polynomials into regular elements

Now, we start a path, given by three steps, in order to generalize the results found in the paper by Frei and Frisch (see [3]).
The first step is to study the factorization of non-zero polynomials in $A[x]$ into regular elements.

Lemma 1.9 *Let f be in $A[x]$, the following statements are equivalent*

(i) $f = tu$, for some unit $u \in A[x]$;

(ii) *f is prime;*

(iii) *f is irreducible and a zerodivisor.*

Proof

(i) $\Rightarrow$ *(ii)* Let $v : A[x] \to \mathbb{N}_h$ be the t-adic valuation, since $v(t) = 1$, and $v(ab) = v(a) + v(b)$, if t divides ab in $A[x]$, then $v(a) + v(b) \geq 1$, so t divides a or b, i.e. t is prime in $A[x]$, and so is every associated to t.
(ii) $\Rightarrow$ *(iii)* Prime elements of $A[x]$ are irreducible. Since (f) is prime, it contains $\mathrm{Nil}(A[x]) = (t)$, so $f|t$. As t is a zerodivisor, so is f: in fact, t is irreducible, i.e. the relation $t = fz$ implies that z is a unit and not a zero divisor, hence f is a zerodivisor.
(iii) $\Rightarrow$ *(i)* Since f is a zerodivisor, $f \in \mathrm{Z}(A[x]) = (t)$, i.e. $f = tv$, for some v. And from the irreducibility of f, we deduce that v is a unit. □

The following proposition is very important in order to factor non-zero polynomials into regular polynomials.

Proposition 1.10 *Let f be a non-zero polynomial in $A[x]$.*

1. *There exist a regular element $g \in A[x]$ and an integer k, with $0 \leq k < h$, such that $f = t^k g$. Furthermore, k is uniquely determined by $k = v(f)$, and g is unique modulo $t^{h-k}A[x]$;*

2. *In every factorization of f into irreducibles, exactly $v(f)$ of the irreducible factors are associates of t.*

Proof

1. follows from Remark 1.3 and from the definition of t-adic valuation: in fact, if f is a zerodivisor, then let t^k be the largest power of t that divides f, so $\exists$ g such that $f = t^k g$, where $t \nmid g$, i.e. g is a regular polynomial. Therefore, we notice that $k = v(f)$, so k is uniquely determined.
2. follows from *1.* and from the fact that t is prime in $A[x]$, in fact, if $f = a_1 a_2 \cdots a_m$ is a factorization of f into irreducibles, using part *1.*, we have that $f = t^{v(f)}g$, with g regular polynomial, and $a_i = t^{v(a_i)}a_i'$, for each $i = 1, \ldots, m$, and with a_i' regular element, so we get the following relation

$$f = t^{v(f)}g = t^{v(a_1)+\cdots+v(a_m)}a_1' \cdots a_m',$$

hence, using the fact that t is prime and that $g - a'_1 \cdots a'_m$ is a regular polynomial, we obtain that $v(f) = v(a_1) + \cdots + v(a_m)$. $\square$

Remark 1.11 *Let f_1 and f_2 be two polynomials $\in A[x]$. Then f_1 and f_2 are coprime in $A[x]$ if and only if $\mu(f_1)$ and $\mu(f_2)$ are coprime in $K[x]$.*

In order to do the second step of this path, we need a simple form of the Hensel's Lemma and also one corollary. The proofs of the following three results are the generalizations of some result contained in [5].

Lemma 1.12 (Hensel's Lemma) *Let $f \in A[x]$ and $\mu(f) = \overline{g}_1\overline{g}_2 \cdots \overline{g}_n$, where $\overline{g}_i$ are pairwise coprime. Then there exist $g_1, g_2, \ldots, g_n \in A[x]$ such that:*

1. *$g_1, \ldots, g_n$ are pairwise coprime;*
2. *$\mu(g_i) = \overline{g}_i,\ 1 \leq i \leq n$;*
3. *$f = g_1 \cdots g_n$.*

<u>*Proof*</u>
We first study the case $n = 2$. From $\mu(f) = \overline{g}_1\overline{g}_2$ and from the fact that μ is surjective, we deduce that there exist $h_1,\ h_2 \in A[x]$ such that $\mu(h_1) = \overline{g}_1$ and $\mu(h_2) = \overline{g}_2$, and there is $v \in \underline{m}[x]$, such that $f = h_1h_2 + v$. Since $\overline{g}_1$ and $\overline{g}_2$ are coprime, there exist $\lambda_1, \lambda_2 \in A[x]$ such that $\lambda_1 h_1 + \lambda_2 h_2 = 1$.
Now we put

$$h_{11} = h_1 + \lambda_2 v, \quad h_{21} = h_2 + \lambda_1 v$$

and we have

$$h_{11}h_{21} = h_1h_2 + v(\lambda_1 h_1 + \lambda_2 h_2) + \lambda_1\lambda_2 v^2 = h_1h_2 + v + \lambda_1\lambda_2 v^2 = f + \lambda_1\lambda_2 v^2,$$

so $f = h_{11}h_{21} \bmod(v^2)$ where $\mu(h_{i1}) = \mu(h_i)\ \forall\ i = 1, 2$.
We can repeat the procedure because of the fact that h_{11} and h_{21} are coprime, so $\forall\ t \in \mathbb{N}$ there are h_{1t} and h_{2t} in $A[x]$ such that

$$f = h_{1t}h_{2t} \bmod(v^{2t}) \ \text{ and } \ \mu(h_{it}) = \mu(h_i) \text{ for } i = 1, 2,$$

but $v \in \underline{m}[x]$, so it is nilpotent, then there is $t \in \mathbb{N}$ such that $f = h_{1t}h_{2t}$, and this concludes the case $n = 2$.
The result follows by induction by observing that if h_1 is coprime to h_i, $2 \le i \le n$, then h_1 and $h_2 \cdots h_n$ are coprime. $\square$

The following result is a corollary of Hensel's Lemma that is very important to prove that a regular element can be factored in a unique way into monic polynomials.

Lemma 1.13 *Let f be a regular polynomial in $A[x]$. Then there exists a sequence $\{f_j\}$ of monic polynomials in $A[x]$ with*

$$\begin{aligned} \deg(f_j) &= \deg(\mu(f)) \\ f_j &= f_{j+1} \mod(\underline{m}^j) \end{aligned}$$

and for some $g_j \in \underline{m}[x]$ and unit $b_j \in A$

$$b_j f = f_j + g_j f_j \mod(\underline{m}^j).$$

<u>*Proof*</u>
Let $f = \sum_{i=0}^{n} b_i x^i$, where $b_n \neq 0$; if $\deg(\mu(f)) = u \le n$, b_u is a unit. Choose $g_1 = 0$ and $f_1 = b_u^{-1}(b_0 + b_1 x + \cdots + b_u x^u)$.
We now proceed by induction. Assume that $\{f_i\}_{i=1}^{j}$ satisfies the Lemma; then $b_j f = f_j + g_j f_j + h$ where $h \in \underline{m}^j[x]$. Since f_j is monic, we may select q and r in $A[x]$, such that $h = f_j q + r$, where $\deg(r) < \deg(f_j) = \deg(\mu(f)))$, or $r = 0$.
Set $f_{j+1} = f_j + r$ and $g_{j+1} = g_j + q$. Now we prove that $g_{j+1} \in \underline{m}[x]$ and $r \in \underline{m}^j[x]$.
If $r = 0$, the proof is trivial; otherwise suppose $f_j = a_0 + a_1 x + \cdots + a_{u-1}x^{u-1} + x^u$ and $q = c_0 + c_1 x + \cdots + c_s x^s$. In the product $f_j q$, the coefficient of x^{s+u} is c_s, of x^{s+u-1} is $c_{s-1} + a_{u-1}c_s$, etc. Since $h = 0 \mod(\underline{m}^j)$ and $\deg(r) < \deg(f_j) = u$, $c_s \in \underline{m}^j$, so also $c_{s-1} \in \underline{m}^j$, etc, and consequently $q \in \underline{m}^j[x]$.
Then $g_{j+1} \in \underline{m}[x]$ and $r = h - q f_j \in \underline{m}^j[x]$.

This ends the proof, because with this choice of f_{j+1} and g_{j+1} we have

$$\begin{aligned} b_j f &= f_j + g_j f_j + h \\ &= (f_j + r) + (g_j + q)(f_j + r) - r g_j - r q \\ &= f_{j+1} + g_{j+1} f_{j+1} - r(g_j + q) \\ &= f_{j+1} + g_{j+1} f_{j+1} \quad \mathrm{mod}(\underline{m}^j). \end{aligned}$$

□

Theorem 1.14 *Every regular polynomial $f \in A[x]$ is uniquely representable as $f = ug$, with u unit and g monic in $A[x]$. Therefore, the degree of g is* $\deg(\mu(f))$.

<u>*Proof*</u>
We already know that h is the nilpotency of the ideal $\underline{m}$. Using the Lemma 1.13, we have that $f = b_h^{-1}(1 + g_h) f_h$, where $g = f_h$ is monic and its degree is the degree of $\mu(f)$, and b_h is a unit, and because of the fact that $g_h \in \underline{m}[x]$, also $1 + g_h$ is a unit.
The uniqueness follows from the fact that the only monic unit in $A[x]$ is 1, since a polynomial $a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ is a unit if and only if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent.

□

Theorem 1.15 *Let $f \in A[x]$ be a non-zero regular polynomial, and let u and g be the unique unit and monic polynomial, respectively, in $A[x]$ such that $f = ug$. For every factorization into irreducibles $f = c_1 \cdots c_k$, there exist uniquely determined monic irreducible $d_1, \ldots, d_k \in A[x]$ and units $v_1, \ldots, v_k \in A[x]$ such that $c_i = v_i d_i$, $u = v_1 \cdots v_k$ and $g = d_1 \cdots d_k$.*

By the last Theorem we have reduced the question of factoring regular elements of $A[x]$ into irreducibles to the question of factoring monic polynomials into monic irreducibles. In the next section we will go another step forward.

1.3 Factorization of monic polynomials into primary monic polynomials

In the following section, we start by giving a characterization for a primary ideal that holds in $A[x]$. We recall that an element $f \in A[x]$ is said to be primary if the principal ideal (f) is primary. In the lemma above, we say that f is primary if and only if $\mu(f)$ is a power of an irreducible polynomial, which will be a very useful result.

Lemma 1.16 *Let $f \in A[x]$ be a non-zerodivisor, then (f) is a primary ideal if and only if $\mu(f)$ is a power of an irreducible polynomial.*

Proof

In the principal ideal domain $K[x]$, where $K = A/\underline{m}$, the non-trivial primary ideals are the principal ideals generated by powers of irreducible elements. So the projection μ induces a bijective correspondence between the primary ideals of $K[x]$ and the primary ideals of $A[x]$ containing (t).

An ideal in $A[x]$ in which there are non-zerodivisors is primary if and only if its radical is a maximal ideal (since the only non-maximal prime ideal of $A[x]$ is $(t) = \mathrm{Z}(A[x])$). Let $f \in A[x]$, since every prime ideal of $A[x]$ contains $(t) = \mathrm{Nil}(A[x])$, we have that the radical of (f) is equal to the radical of $\mu^{-1}(\mu(f)) = (f) + (t)$. So (f) is primary if and only if $(f) + (t)$ is primary, because of the fact that if (f) is primary, since f is a non-zerodivisor, $\sqrt{(f)}$ is maximal, then $\sqrt{(f) + (t)}$ is maximal too, and this implies that $(f) + (t)$ is primary, and conversely. The fact that $(f) + (t)$ is primary is equivalent to $\mu(f)$ being a primary element of $K[x]$, because of the bijective correspondence described above.

$\square$

Using Hensel's Lemma, we prove the following theorem, that constitutes the third step of the path, since in it we found out that a monic polynomial can be factored in a unique way into primary elements.
We notice that this theorem is the generalization of the Theorem 13.8 contained in [6].

Theorem 1.17 *Let $f \in A[x]$ be a monic polynomial, of degree ≥ 1. Then:*

(i) f can be factorized in the product of r coprime primary monic polynomials $f_1, f_2, \ldots, f_r \in A[x]$, and for each $i = 1, 2, \ldots, r$, $\mu(f_i)$ is a power of a monic irreducible polynomial over k;

(ii) Let

$$f = f_1 \cdots f_r = h_1 \cdots h_s \tag{2}$$

be two factorizations of f into products of pairwise coprime monic primary polynomials over A, then $r = s$ and after renumbering, $f_i = h_i,\ i = 1, 2, \ldots, r$.

Proof

(i) We can assume that $\mu(f) = h_1^{e_1} \cdots h_r^{e_r}$, where $h_1, \ldots, h_r$ are monic irreducible distinct polynomials, by the Lemma 1.12 , there exist $g_1, \ldots, g_r \in A[x]$, such that $f = g_1 \cdots g_r$ and $\mu(g_i) = h_i^{e_i}$ for each i. Moreover, because of the fact that the polynomials $h_i^{e_i}$ are coprime, using Remark 1.11, even the polynomials g_i are coprime.

(ii) From the equation (2), we deduce that $f_1 \cdots f_r \in (h_i)$ for each $i = 1, \ldots, s$. Since (h_i) is a primary ideal, there exist an integer k_i, $1 \le k_i \le r$, and a positive integer n_i, such that $f_{k_i}^{n_i} \in (h_i)$. We now prove that k_i is uniquely determined. Assume that there is another $k_i' \neq k_i$ and n_i' such that $f_{k_i'}^{n_i'} \in (h_i)$, since f_{k_i} and $f_{k_i'}$ are coprime in $A[x]$, there are $a, b \in A[x]$ such that $1 = af_{k_i} + bf_{k_i'}$. Then

$$1 = 1^{n_i + n_i' - 1} = (af_{k_i} + bf_{k_i'})^{n_i + n_i' - 1} \in (h_i)$$

and this is a contradiction.

Similarly, for each $j = 1, \ldots, r$, there is a uniquely determined integer l_j, $1 \le l_j \le s$ and a positive integer m_j, such that $h_{l_j}^{m_j} \in (f_j)$. For every i, we have that $h_{l_{k_i}}^{m_{k_i} n_i} \in (h_i)$, then $\mu(h_{l_{k_i}})^{m_{k_i} n_i} \in (\mu(h_i))$. Since the polynomials h_i are coprime, using Remark 1.11, the polynomials $\mu(h_i)$ are coprime and so we must have $l_{k_i} = i$, for every $i = 1, \ldots s$. It follows that the map $i \mapsto k_i$ is well defined and injective, so we must have $s \le r$. Similarly, $r \le s$, i.e.

$r = s$. After renumbering, we may assume that $i = k_i$ for $i = 1, \ldots, r$, then $l_j = j$ for $j = 1, \ldots, r$. Thus, $f_i^{n_i} \in (h_i)$ and $h_i^{m_i} \in (f_i)$ for $i = 1, \ldots, r$.

Using Remark 1.11, for $j \neq 1$, f_j and f_1 are coprime, so also $\mu(f_j)$ and $\mu(f_1)$ are coprime, and this implies $\mu(f_j)$ and $\mu(f_1)^{n_1}$ are coprime. Hence, $\mu(f_2) \cdots \mu(f_r)$ and $\mu(f_1)^{n_1}$ are coprime. Using Remark 1.11, $f_2 \cdots f_r$ and $f_1^{n_1}$ are coprime. Since $f_1^{n_1} \in (h_1)$, $f_2 \cdots f_r$ and h_1 are coprime. Then, there exist $c, d \in A[x]$ such that

$$cf_2 \cdots f_r + dh_1 = 1.$$

Multiplying both sides of the above equality by f_1, we obtain

$$f_1 = cf_1f_2 \cdots f_r + df_1h_1 = ch_1h_2 \cdots h_r + df_1h_1,$$

which implies $h_1 | f_1$. Similarly, $f_1 | h_1$. Since both f_1 and h_1 are monic, $f_1 = h_1$. Similarly, $f_i = h_i$, $i = 2, \ldots, r$.

□

Now, we have the following results.

Proposition 1.18 *Each non-zero polynomial f in $A[x]$ can be written as*

$$f = t^k u f_1 f_2 \cdots f_r, \tag{3}$$

where $0 \leq k < h$, u is a unit, and $f_1, f_2, \ldots, f_r$ are monic polynomials, such that $\mu(f_1), \mu(f_2), \ldots, \mu(f_r)$ are powers of irreducible and pairwise distinct polynomials, $g_1, g_2, \ldots, g_r \in K[x]$, respectively .

Moreover, $k \in \mathbb{N}_h$ is unique, $u \in A[x]$ is unique modulo $t^{h-k}A[x]$, and also the polynomials $f_1, \ldots, f_r$ are uniquely determined modulo $t^{h-k}A[x]$.

<u>*Proof*</u>

We use at first Proposition 1.10, from which we deduce that $\exists\, g \in A[x]$, and $0 \leq k < h$, such that $f = t^k g$, where g is a non-zerodivisor and $k = v(f)$, with v t-adic valuation, so k is uniquely determined, and g is unique modulo $t^{h-k}A[x]$.

Then we apply Theorem 1.14 to g, and so we have that g is uniquely representable as $g = uh$, with u unit and h monic in $A[x]$.

Finally, we apply Theorem 1.17 to the equivalence class of the monic polynomial $\overline{h}$ modulo $t^{h-k}A[x]$.

The fact that u is unique modulo $t^{h-k}A[x]$ follows from Theorem 1.14 and also from the presence of the factor t^k in the equation (3), for the same reason the polynomials f_i are unique modulo $t^{h-k}A[x]$.

□

1.4 The elasticity of $A[x]$

The ring $A[x]$ is not a unique factorization ring and it easy to find an example to show it.
This ring is actually more than a not-unique factorization ring as we are going to see now.

In fact, we now present the concept of elasticity, that can be considered as the measure of how much the ring is not a unique factorization ring, and through an example we will show that the elasticity of this ring is infinite. This concepts also presented in [1].

Definition 1.19 *Let us consider a commutative ring with identity, R, and let M be the set of the regular elements of R. Let k be ≥ 2, we define $\rho_k(R)$ to be the supremum of those $m \in \mathbb{N}$, for which there is a product of k irreducible regular elements that can be also be written as a product of m irreducible regular elements. We also define the* elasticity *of R to be $\sup_{k\geq 2}(\rho_k(R)/k)$.*

We notice that the set, M, of the regular elements of A is a cancellative monoid, so it is also possible to consider the elasticity of a cancellative monoid, as it is done in [3].

Here we have the example that shows that the elasticity of the ring $A[x]$ is infinity.
Let us consider the polynomial

$$x^m + t;$$

we want to prove that this polynomial is irreducible in $A[x]$.
By contradiction, let us suppose that there are two non-unit polynomials,

$f(x), g(x) \in A[x]$, such that $x^m + t = f(x)g(x)$. Then, we can write it in the following way

$$
\begin{aligned}
&x^m + t = a_0 + a_1 x + \cdots a_m x^m = \\
&= (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s),
\end{aligned}
$$

where we can suppose that $b_r c_s \neq 0$.
Because of the Lemma 1.9, we have that t is prime. So, from $t = b_0 c_0$, it is ensured that either $t \mid b_0$ and $t \nmid c_0$ or $t \mid c_0$ and $t \nmid b_0$. Suppose that the first sentence occurs. We have that $t \nmid b_r$ and $t \nmid c_s$. because $b_r c_s = 1$ and $t \nmid 1$. Let b_n be the first coefficient of $f(x)$ such that $t \nmid b_n$, and let us note that

$$
\begin{aligned}
a_n &= c_0 b_n + c_1 b_{n-1} + \cdots + c_n b_0, \quad \text{if } n \leq s, \\
a_n &= c_0 b_n + c_1 b_{n-1} + \cdots + c_s b_{n-s}, \quad \text{if } n > s,
\end{aligned}
$$

and that in both cases t divides each term of this sum except the first, so $t \nmid a_n$, and then $a_n = 1$ and $n = m$. Here we get a contradiction, because we have that the following relations hold

$$n = m \leq r < m.$$

We have just proved that $x^m + t$ is an irreducible polynomial for each m. Let us consider $N > h$ and the following polynomial

$$
\begin{aligned}
&(x^m + t)^N = \sum_{i=0}^{N} \binom{N}{i} x^{m(N-i)} t^i = \binom{N}{0} x^{mN} + \\
&+ \binom{N}{1} x^{m(N-1)} t + \cdots + \binom{N}{h-1} x^{m(N-h+1)} t^{h-1} = \\
&= x^{m(N-h+1)} \left(x^{m(h-1)} + N x^{m(h-2)} t + \cdots + \binom{N}{h-1} t^{h-1} \right)
\end{aligned}
$$

So here we have given an example of a polynomial that has a factorization in N irreducible factors, on the left, and in more than $m(N-h+1)$ irreducible factors on the right, where N is arbitrary but greater than h and m is arbitrary: this proofs that $\rho_N(M) = \infty$ and so also $\rho_N(M)/N = \infty$.

Acknowledgments I would like to thank Professor Ralf Fröberg and Professor Christian Gottlieb for their useful help.

References

[1] D. F. Anderson, *Elasticity of Factorizations in Integral Domains: A Survey*, Lecture notes in Pure and Applied Mathematics, Marcel Decker Inc., 1997.

[2] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1961..

[3] C. Frei, S. Frisch, *Non-unique factorization of polynomials over residue class rings of integers*, arXiv:0907.0657v1, submitted on July 2009, to appear in Comm. Algebra.

[4] O. Greco, *Equivalence of three different definitions of irreducible element*, arXiv:1101.3977v1, January 2011.

[5] B. R. McDonald, *Finite rings with identity*, Marcel Dekker, 1974.

[6] Z. X. Wan, *Lectures on finite fields and Galois rings*, World Scientific, 2003.

Royal Institute of Technology, Department of Mathematics, 10044 Stockholm, Sweden.
E-mail address: `ogreco@kth.se`