Abstract

In this work, we study the factorization in $A[x]$, where A is an Artinian local principal ideal ring (briefly SPIR), whose maximal ideal, (t), has nilpotency h: this is not a Unique Factorization Ring, in fact its elasticity is infinity, but we can write, in quite a unique way, an element $x \in A[x]$ as the product of a nilpotent element, t^k, of a unit, u, and of a finite number, say r, of monic primary polynomials, $g_1, \ldots, g_r$.

Then, we extend this result to the case in which A is an Artinian principal ideal ring: to do this, we observe that such a ring can be written as a direct product of finitely many SPIR's, $A_1, \ldots, A_n$; using this result, we get that an element $(f_1, \ldots, f_n) \in A_1[x] \oplus \cdots \oplus A_n[x] \cong A[x]$, whose components are all non-zero, can be expressed as the product of a zerodivisor, of a unit, and of finitely many primary elements, and this product is quite unique.

Finally, we give the definition of *Unique Factorization Ring according to Fletcher*, briefly F-UFR, and we study the factorization in a polynomial ring over an F-UFR, B: and, using the fact that B is a direct product of finitely many UFD's and SPIR's, we get that an element in $B[x]$, whose components are all non-zero and non-units, can be expressed as the product of a unit, of finitely many F-irreducible elements, of finitely many primary elements, and of elements, whose components are units and zerodivisors.

Contents

Introduction

In this work, we deal with the factorization of polynomials over Artinian principal rings.
Our aim in the beginning was to generalize the result below to the case of a polynomial ring over an Artinian local principal ring.

Theorem 0.1 *([10], Prop 3.8) Each non-zero polynomial f in $\mathbb{Z}_{p^n}[x]$ can be written as*

$$f = p^k u f_1 f_2 \cdots f_r,$$

where $0 \leq k < n$, 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, $g_1, g_2, \ldots, g_r \in \mathbb{Z}_p[x]$, respectively .

Moreover, $k \in \mathbb{N}_n$ is unique, $u \in \mathbb{Z}_{p^n}[x]$ is unique modulo $p^{n-k}\mathbb{Z}_{p^n}[x]$, and also the polynomials $f_1, f_2, \ldots, f_r$ are uniquely determined (up to ordering) modulo $t^{n-k}\mathbb{Z}_{p^n}[x]$.

Where $\mu : \mathbb{Z}_{p^n}[x] \to \mathbb{Z}_p[x]$ is the natural extension of the canonical projection to the polynomial rings.
This theorem is proved in the Frei-Frisch's paper, *Non-unique factorization of polynomials over residue class rings of integers*, [10]. This paper deals with the factorization of polynomials over the residue class of the integers $\mathbb{Z}_{p^n}$, where p is a prime element of $\mathbb{Z}$. The authors found out that the ring $\mathbb{Z}_{p^n}[x]$ is not a unique factorization ring. Actually, they reminded the concept of *elasticity of a ring*, that intuitively can be described as a measure of how much the ring is not a unique factorization ring, and they found out that $\mathbb{Z}_{p^n}[x]$ has infinite elasticity. But, in this ring, each element can be factored in a unique way as the product of a power of p, p^k, of a unit u, and of finitely many monic primary coprime polynomials, $g_1, \ldots, g_m$, which have

the property that their canonical projections in the integral domain $\mathbb{Z}_p[x]$ are monic irreducible polynomials, as the above theorem says.

As $\mathbb{Z}_{p^n}$ is an Artinian, principal, local ring, it has only one maximal ideal, (p), that is nilpotent with nilpotency n. The structure of this ring is very interesting, because in it we can define a p-adic valuation, and we can also extend this map to the polynomial ring over $\mathbb{Z}_{p^n}$. For this reason, we have tried to extend the results contained in [10] to the general case of the polynomial ring $A[x]$, where A is an Artinian, principal, local ring, with maximal ideal (t). We note that such a ring, Artinian, local and principal ring, is also called Special Principal Ideal Ring, i.e. SPIR.

The second chapter of this work deals with the factorization in $A[x]$, where A is a SPIR. It starts with a brief description of A: there is only one maximal ideal, (t), whose nilpotency is h, i.e. h is the smallest integer such that $(t)^h = (0)$. Then, we have followed the same argument path as [10] and, after a generalization of each proposition and each theorem, we have got the same results that hold in $\mathbb{Z}_{p^n}[x]$, in particular we have found out that the elasticity of $A[x]$ is infinite, we have given an example that explain this fact and we have proved the following important result:

Theorem 0.2 *Each non-zero polynomial f in $A[x]$ is representable as*

$$f = t^k u f_1 f_2 \cdots f_r, \tag{1}$$

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, 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 $f_1, f_2, \ldots, f_r$ are unique modulo $t^{h-k}A[x]$.

Where K denotes the field $A/(t)$, and $\mu : A[x] \to K[x]$ is the natural extension of the canonical projection. This theorem shows us that the ring $A[x]$ has the same factorization features as $\mathbb{Z}_{p^n}[x]$.

The natural consequent step of this generalization work has been to study the factorization of polynomials over an Artinian principal ring, A.

Before doing it, we have tried to do a survey, contained in the first chapter, about the different definitions of unique factorization ring. We have studied especially three among the several definitions of unique factorization ring: each definition constitutes an attempt to generalize the concept of unique factorization domain to the rings with zerodivisors.
The first definition of unique factorization ring that we present in this work is the one created by Bouvier in [5]: the way in which he defines a unique factorization ring is very intuitive and close to the classical definition of UFD. In fact, a commutative ring with unity R is said to be a *unique factorization ring according to Bouvier*, or briefly B-UFR, if each non-zero and non-unit element can be written as a product of finitely many B-irreducible elements, and if a non-zero and non-unit element has two factorizations into B-irreducibles, then the numbers of the factors in the two factorizations are equal, and, after a suitable renumbering, the factors are associate.
We notice that in this definition, Bouvier uses a different concept of irreducible element, that is equivalent to the classical one in a class of rings, that we call *rings with only harmless zero-divisors*, that includes both UFD's and local rings. While the definition of associate elements that Bouvier uses is the classical one.
The other definition of UFR that we present is the one given by Galovich in [12]. Also the definition of *unique factorization ring according Galovich*, or briefly G-UFR, is very intuitive, in fact, it is equal to the one by Bouvier, apart from the definitions of irreducible element and of associates elements. Galovich uses the classical definition of irreducible element but he gives a stonger definition for associate elements.
These two definitions of UFR are very similiar, so we have done a comparison of them, finding out that a ring R is a B-UFR if and only if it is a G-UFR

and if and only if it is a SPIR or a UFD or a local ring with maximal ideal M, whose nilpotency is two.
The last definition of unique factorization ring, given in this work, is older than the first two and it was created by Fletcher in [8]. It is less intuitive than the other two, because it uses some new concepts, like the U-class and the U-decomposition of an element. Though the definition is not so easy, Fletcher gives a characterization of the *unique factorization rings according to Fletcher*, briefly F-UFR, in [9]: in fact, a ring is a F-UFR if and only if it is a direct product of SPIR's and of UFD's.
From these two characterization, it follows that the concept of F-UFR is independent of the concept of B-UFR, and it is also clear that an Artinian local principal ring is both an F-UFR and a B-UFR, while an Artinian principal ring is only an F-UFR.

The third chapter deals with the factorization of polynomials over an Artinian principal ring, B. We have achieved some new results that are very similiar to the ones contained in the second chapter, using especially two important theorems: an isomorphism theorem about Artinian rings, that we have used to write an Artinian principal ring as a direct product of finitely many artinan local principal rings; a simple isomorphism theorem about polynomial rings. So, we have proved that $B[x]$ is isomorphic to a direct product of finitely many polynomial rings over Artinian local PIR's, and that an element of $B[x]$, whose components are non-zero, can be factored in a unique way as the product of a unit, of finitely many primary elements, and of an element whose components are powers of the nilpotent elements that generate respectively the nilradicals of the rings, of which $B[x]$ is direct product.
So another theorem of the present work that we have achieved is the following:

Theorem 0.3 *Let $(f_1, \ldots, f_n)$ be a element in $B[x]$, such that $f_i \neq 0$ for each $i = 1, \ldots, n$, then there exist $k_1, \ldots, k_n \in \mathbb{N}$, $0 \leq k_i < h_i$, $i = 1, \ldots n$,*

n units $u_i \in B_i[x]$, $r_1, \ldots, r_n \in \mathbb{N}$, n sets of pairwise coprime, primary, monic polynomials $\{g_{i1}, \ldots, g_{ir_1}\} \subset B_i[x]$, where for each $j = 1, 2, \ldots, r_i$, $\mu_i(g_{ij}) \in K_i[x]$ is a power of a monic irreducible polynomial, such that

$$(f_1, \ldots, f_n) = (t_1^{k_1}, \ldots, t_n^{k_n})(u_1, \ldots, u_n)(g_{11}, 1, \ldots 1)(g_{1r_1}, 1, \ldots 1) \cdots$$
$$\cdots (1, g_{21} \ldots, 1) \cdots (1, g_{2r_2} \ldots, 1) \cdots (1, 1, \ldots g_{n1}) \cdots (1, 1, \ldots, g_{nr_n}).$$

The following step has been to study the factorization of polynomials over a ring B that is a F-UFR, i.e. that is a direct product of SPIR's and of UFD's. Let $B = U_1 \oplus \cdots \oplus U_n \oplus S_1 \oplus \cdots \oplus S_m$, where U_i is an UFD, for each $i = 1, \ldots, n$, and $(S_j, (t_j))$ is a SPIR, for each $j = 1, \ldots, m$.
We have taken an element $(f_1, \ldots, f_n, g_1, \ldots, g_m) \in B[x]$, whose components are all non-zero and non-units, and we have proved that it can be written as the product of $(1_{U_1}, \ldots, 1_{U_n}, t_1^{k_1}, \ldots, t_m^{k_m})$, of a unit $(1_{U_1}, \ldots, 1_{U_n}, u_1, \ldots, u_m)$, of some irreducible elements, and of some primary elements, and this factorization fulfills some uniqueness features.

Moreover, in the first chapter, we have also listed two attempts to generalize the concept of UFD to domains: the class of the Dedekind domains, that have the property that every proper ideal can be factored as the product of finitely many prime ideals in a unique way; the class of the Half-factorial Domains, in which two factorizations into irreducibles of an element have always the same lenght. We have also shown three characterizations of Dedekind domains, finding out that every Dedekind domain is an integral domain that is noetherian, integrally closed and one-dimensional. Moreover, we have given the definition of *class group* of a Dedekind domain, R, and of *class number* of R, in order to relate the concepts of Half-factorial domain and of Dedekind domain: in fact, let R be a Dedekind domain, with a finite class group in which every element contains a prime ideal, then R is an Half-factorial Domain if and only if the the class group has order 1 or 2.

1 Different definitions of UFR

1.1 UFD

In this section, we want to make a little survey of the main results about the structure of UFD, in such a way to present its generalization, the structure of UFR, in the next section, to give three different definitions of this new concept and to make clearer the differences between these definitions.

We start with some basic definitions: we now present the very important concepts of prime and irreducible element and also the concept of primary element, that will be central in the next chapters.

Definition 1.1 *Let R be a commutative ring with unity, we say that $r \in R$ is a prime element if*

$$r \mid ab \;\Rightarrow\; r \mid a \text{ or } r \mid b.$$

We say that $r \in R$ is an irreducible element if

$$r = ab \;\Rightarrow\; a \text{ is a unit or } \; b \text{ is a unit.}$$

We say that two elements, $a, b \in R$, are associates if $(a) = (b)$.
We say that an ideal I is primary if, from the fact that $xy \in I$ and that $x \notin I$, it follows that $y \in \sqrt{I}$. And an element x is primary if and only if (x) is such an ideal.

We notice that if r is a prime element, then the principal ideal (r) is prime.

Definition 1.2 *Let R be an integral domain, R is said to be an* UFD *if:*

- *each non-zero and non-unit element of R is a product of irreducible elements;*

- *if* $0 \neq r_1 \cdots r_m = s_1 \cdots s_n$ *are two factorizations into irreducibles, then* $n = m$ *and, after a suitable reordering,* r_i *and* s_i *are associates for each* $i = 1, \ldots, n$.

Definition 1.3 *An integral domain* R *is said to be a* PID *if each ideal of* R *is principal.*

Here, we have five main results about the features of UFD's and PID's: the first four are simple and standard results, so we only announce them.

Proposition 1.4 *Let* R *be a PID, then* R *is a UFD.*

Proposition 1.5 *If* A *is a UFD, then* $A[x]$ *is a UFD.*

Proposition 1.6 *In a UFD, if* x *is an irreducible element, then it is a prime element.*

Proposition 1.7 *In an integral domain* R *a factorization in prime elements is unique up to associate factorizations.*

The following proposition is one of the most important characterizations of UFD. There are many versions of this result, one is due to Krull and in the proof many important results about Noetherian rings are used (see [17]). The following version has a very general proof, in fact it holds in a arbitrary domain.

Proposition 1.8 *Let* R *be a domain, then* R *is a UFD if and only if all primes of height* 1 *are principal.*

Proof

$\Rightarrow$ Let R be a UFD, and let P be a prime ideal of height one. In P there is an irreducible element, $r \neq 0$. So we have:

$$P \supseteq (r) \supseteq (0).$$

We notice that $(r), (0)$ are prime ideals, so, by hypothesis, we must have that $P = (r)$.
$\Leftarrow$ Let us define

$$S = \{x \in R |\ x \text{ is } \text{ a product of finitely many prime elements and units}\}$$

We note that S is a multiplicatively closed set, and it is also saturated, i.e. if $yz \in S$, then y and z belong to S.
It is very easy to prove that it is a multiplicatively closed set. Let us prove that it is a saturated set. If $yz \in S$, then, if yz is a unit, we are done, otherwise, if we can write $yz = up_1p_2 \cdots p_m$, where p_j is a prime element $\forall\, j = 1, \ldots, m$ and u is a unit, then we could of course have that $y = ap_1 \cdots p_t$ and that $z = bp_{t+1} \cdots p_m$, after a suitable reordering of the prime factors; but R is a domain, so $ab = u$, i.e. a, b are units, and then we have that y and z are in S.

We now prove that $R\backslash\{0\} = S$ by contradiction. First we claim that if S is a saturated multiplicatively closed set, then $R\backslash S$ is union of prime ideals. Assuming that the claim is already proved, suppose that $S \subsetneq R\backslash\{0\}$, in $R\backslash S$ there is a prime ideal, P, that contains a prime ideal of height 1, which is principal, by hypothesis: here we have a contradiction, because we have found a prime element outside S.
Now, we prove the claim: let $x \notin S$, since S is saturated, $(x) \cap S = \emptyset$. Let us consider the image of (x) in $S^{-1}R$. We want to prove that $S^{-1}(x) \subsetneq S^{-1}R$, this is because, if $ax/v = w/w$, for some $w, v \in S$ and $a \in R$, then there would be $u \in S$ such that $axuw = uwv$, a contradiction. Because we have proved that $S^{-1}(x)$ still remains a proper ideal in $S^{-1}R$, we can consider the maximal prime ideal of $S^{-1}R$ that contains it. The inverse image in R of this prime ideal is a prime ideal disjoint from S. Because we can repeat this procedure for each element not in S, we have proved the claim.

By the Proposition 1.7, we get the uniqueness of factorization into prime elements, that are, in every domain, also irreducible elements.

□

There is a deep link between these algebraic concepts and Algebraic Geometry, and the two examples below show us it.

Example

An affine variety is the zero-set, $V(\mathbf{p})$, where $\mathbf{p}$ is a prime ideal of the polynomial ring $k[x_1, \ldots, x_n]$, with k field.
A subvariety, $V(\mathbf{q})$, is the zero-set of a prime ideal $\mathbf{q}$ in $R = k[x_1, \ldots, x_n]/\mathbf{p}$.

By definition of codimension and of dimension of a variety, we have that $\operatorname{codim}(V(\mathbf{q})) = 1$ if and only if $\operatorname{height}(\mathbf{q}) = 1$. Then, using Proposition 1.8, we get that if R is a UFD, the subvarieties of codimension one are defined by one equation, because $\mathbf{q}$ is a principal ideal. □

Example

Let k be a field, $k[t^2, t^3] \cong k[x, y]/(x^3 - y^2)$ is not a UFD. In this ring, the ideal (x, y) is a prime of height one, but it is not principal, which corresponds to the fact that the subvariety $\{(0, 0)\}$ of codimension one is defined by two equations. We notice that we easily have an example of non-unique factorization of an element in this ring, since $x^3 = y^2$, and x, y are irreducible elements. □

1.2 Dedekind domains: a survey

The present section deals with Dedekind domains. While in UFD's it is possible to factor, in a unique way, an element into the product of irreducible elements, in Dedekind domains, as we are going to see, it is possible to factor an ideal into prime ideals, and this factorization is also unique. So, in a certain way, Dedekind domains constitute a generalization of the concept of Unique Factorization Domain.

What we are presenting now is a summary of the treatment of Dedekind domains contained in [19].

Definition 1.9 *A ring R is a* Dedekind domain *if it is an integral domain in which every ideal can be written as a product of finitely many prime ideals.*

We want to prove that in a Dedekind domain the factorization of an ideal in prime ideals is unique. To achieve this result, we have to give some definitions and propositions about fractionary and invertible ideals.

Definition 1.10 *Let R be a domain, K be its quotient field and $\underline{b}$ be an R-module of K, we say that $\underline{b}$ is a* fractionary ideal of R *if the elements of $\underline{b}$ admit a common denominator $d \neq 0$ in R, i.e. there exists $d \in R, d \neq 0$, such that $d\underline{b} \subseteq R$. Hence, if $\underline{b}$ is a fractionary ideal of R, there is an ideal $\underline{a}$ of R, such that $\underline{b} = (\frac{1}{d})\underline{a}$.*

We notice that, in contrast, the ordinary ideals of R, that are factionary ideals with $d = 1$, are called *integral ideals.*

An example of fractionary ideal is a *principal fractionary ideal*, which is equal to xR, where $x = \frac{a}{b}$, $b \neq 0$, is an element of K.

In the following observation, we describe the behaviour of the set of all the fractionary ideals of R towards the ideal thoretic operations $+$, $\cdot$ and $\cap$.

Observation 1.11 *The set of all fractionary ideals of R is closed under the ideal operations $\cdot, +$, and $\cap$: in fact, these operations have already been defined for submodules, furthermore, if $\underline{b} \subseteq (1/d)R$ and $\underline{b'} \subseteq (1/d')R$, it is clear* *that $\underline{b}+\underline{b'} \subseteq (1/dd')R$, that $\underline{b}\cdot\underline{b'} \subseteq (1/dd')R$ and that $\underline{b}\cap\underline{b'} \subseteq (1/d)R$. The set $(\underline{b}:\underline{b'})$ is defined as the set of all the $x \in K$ such that $x\underline{b'} \subseteq \underline{b}$. The set $\mathcal{I}$ of all the fractionary ideals of R is a partally ordered set by inclusion: R is a fractionary ideal and it is the identity element of $\mathcal{I}$; we also say that a fractionary ideal $\underline{a} \in \mathcal{I}$ is* invertible, *if there exists $\underline{a'} \in \mathcal{I}$, such that $\underline{a}\cdot\underline{a'} = R$; we notice that if Rx, with $x \neq 0, x \in K$ is a principal fractionary ideal, then it is an invertible fractionary ideal and its inverse is Rx^{-1}.*

We will still denote with $\mathcal{I}$ the set of all the fractionary ideals of an integral domain R and with the small underlined letters the elements of $\mathcal{I}$.

The lemmas below deal with fractionary and invertible ideals and describe some important properties that are useful to prove that in a Dedekind domain the factorization of an ideal into prime ideals is unique.

Lemma 1.12 *If $\underline{a}$ is invertible, then it has a unique inverse that is equal to $R:\underline{a}$. Hence, a necessary and sufficient condition for $\underline{a}$ to be invertible is: $\underline{a}\cdot(R:\underline{a}) = R$.*

Proof

If $\underline{aa'} = R$, then $\underline{a'} \subseteq R:\underline{a}$. On the other hand, $\underline{a}\cdot(R:\underline{a}) \subseteq R$, hence, if $\underline{a'}$ is an inverse of $\underline{a}$, we have that $(R:\underline{a}) = \underline{a'}\cdot\underline{a}\cdot(R:\underline{a}) \subseteq \underline{a'}\cdot R = \underline{a'}$. □

Lemma 1.13 *If every integral and non-zero ideal of R is invertible, then the set $\mathcal{I}$ is a group under multiplication.*

Proof

Every fractional ideal $\underline{a}$ may be written as $(1/d)\underline{b}$, where $\underline{b}$ is an integral ideal and d is a non-zero element of R. Since, there exists the inverse $\underline{b}^{-1}$ of $\underline{b}$, the inverse of $\underline{a}$ is $d\underline{b}^{-1}$. Furthermore, the multiplication of ideals is associative and there exists in $\mathcal{I}$ the identity element, then $\mathcal{I}$ is a group. □

Lemma 1.14 *An invertible ideal $\underline{a}$, considered as an R-module, has a finite basis.*

Proof

Let $\underline{a'}$ be the inverse of the ideal $\underline{a}$, i.e. $\underline{a} \cdot \underline{a'} = R$. Then there are two finite families $\{x_i\}_{i \in I} \subset \underline{a}$ and $\{x'_i\}_{i \in I} \subset \underline{a'}$, such that $\sum_{i \in I} x_i x'_i = 1$. For every $x \in \underline{a}$, $x = \sum_{i \in I} x x'_i x_i$, i.e. $\{x_i\}_{i \in I}$ is the finite basis for $\underline{a}$, since, by the assumption, $x x'_i \in R$, for each i. □

Lemma 1.15 *If a finite family $\{\underline{a}_i\}_{i \in I}$ of integral ideals of R is such that the product $\underline{b} = \prod_{i \in I} \underline{a}_i$ is invertible, then each $\underline{a}_i$ is invertible. In particular, if a product of integral ideals is principal, then each factor is invertible.*

Proof

From $\underline{b}^{-1} \cdot \prod_{i \in I} \underline{a}_i = R$, we deduce that $\underline{a}_i \cdot (\underline{b}^{-1} \cdot \prod_{j \neq i} \underline{a}_j) = R$, i.e. $\underline{a}_i$ is invertible. □

Lemma 1.16 *For a product of invertible prime integral ideals, the factorization into prime ideals is unique.*

Proof

Let $\underline{a} = \prod_{i=1}^{n} \underline{p}_i$ be a product of invertible prime ideals and suppose that we also have $\underline{a} = \prod_{j=1}^{m} \underline{q}_j$, where each $\underline{q}_j$ is a prime ideal. Now, we take a minimal element in the family of ideals $\{\underline{p}_i\}_{i=1,\ldots,n}$, say $\underline{p}_1$. Since $\prod_{j=1}^{m} \underline{q}_j$ is contained in $\underline{p}_1$, some $\underline{q}_j$, say $\underline{q}_1$, is contained in $\underline{p}_1$. Similarly, there is some $\underline{p}_j \subseteq \underline{q_1} \subseteq \underline{p}_1$. Then, from the minimality of $\underline{p}_1$, we deduce that $\underline{p}_r$ such that $\underline{p}_j = \underline{q}_1 = \underline{p}_1$. Multiplying the relation $\prod_{i=1}^{n} \underline{p}_i = \prod_{j=1}^{m} \underline{q}_j$ by $\underline{p}_1^{-1}$, we get $\prod_{j \neq 1} \underline{p} = \prod_{j \neq 1} \underline{q}$. The Lemma follows by induction on n, since the case $n = 1$ is trivial. □

Theorem 1.17 *In a Dedekind domain R, every proper prime ideal is invertible and maximal.*

Proof

We first show that every invertible proper prime ideal, $\underline{p}$, is maximal. Let us consider $a \notin \underline{p}$ and the ideals $\underline{p} + Ra$ and $\underline{p} + Ra^2$. As R is a Dedekind ring, we have that

$$\underline{p} + Ra = \prod_{i=1}^{n} \underline{p}_i;$$
$$\underline{p} + Ra^2 = \prod_{j=1}^{m} \underline{q}_j,$$

where each $\underline{p}_i$ and each $\underline{q}_j$ are prime ideals.
Let us consider the ring $\overline{R} = R/\underline{p}$ and let $\overline{a}$ be the residue class of a in this ring. We get that $\overline{R}\overline{a} = \prod_{i=1}^{n}(\underline{p}_i/\underline{p})$ and that $\overline{R}\overline{a}^2 = \prod_{j=1}^{m}(\underline{q}_j/\underline{p})$, where the ideals $\underline{p}_i/\underline{p}$ and $\underline{q}_i/\underline{p}$ are prime and, by Lemma 1.15, are also invertible. Thus, since $\overline{R}\overline{a}^2 = (\overline{R}\overline{a})^2 = \prod_{i=1}^{n}(\underline{p_i}/\underline{p})^2$, Lemma 1.16 shows that the ideals $\underline{q}_j/\underline{p}$ are the ideals $\underline{p}_i/\underline{p}$, each repeated twice, i.e., we have that $m = 2n$ and that we can renumber the $\underline{q}_j$ in such a way that $\underline{q}_{2i}/\underline{p} = \underline{q}_{2i-1}/\underline{p} = \underline{p}_i/\underline{p}$. Thus, $\underline{q}_{2i} = \underline{q}_{2i-1} = \underline{p}_i$, and we have that $\underline{p}^2 + Ra = (\underline{p} + Ra)^2$, and this implies that $\underline{p} \subset (\underline{p} + Ra)^2 \subset \underline{p}^2 + Ra$. Then, we may write every element $x \in \underline{p}$ as $y + za$, where $y \in \underline{p}^2$ and $z \in R$, and we have also that $za \in \underline{p}$ and, since $a \notin \underline{p}$, $z \in \underline{p}$: in other words, we get that $\underline{p} \subseteq \underline{p}^2 + \underline{p}a$, and, because the other inclusion is trivial, the equality holds. Now, by multiplying the following equality by $\underline{p}^{-1}$, $\underline{p} = \underline{p}(\underline{p} + Ra)$, we get the relation, $R = \underline{p} + Ra$, which holds for each element $a \notin \underline{p}$. This proves the maximality.

Now, to prove the theorem, we need only to prove that every proper prime ideal $\underline{p}$ of R is invertible. Let b be a non-zero element of $\underline{p}$, let us consider the ideal Rb, since R is a Dedekind domain, there exist finitely many prime ideals, $\underline{p}_1, \ldots, \underline{p}_m$, such that $Rb = \prod_{i=1}^{m} \underline{p}_i$. Since $\underline{p}$ contains Rb, there is some

$\underline{p}_j$, say $\underline{p}_1$ such that $\underline{p}_1 \subseteq \underline{p}$. But by Lemma 1.15, every $\underline{p}_i$ is invertible. Thus every $\underline{p}_i$ is maximal, by the first part of the proof. Then, from $\underline{p}_1 \subseteq \underline{p}$, we deduce that $\underline{p}_1 = \underline{p}$ and this prove the result. □

Using the above results, we finally get the main result: if in a integral domain we suppose that every ideal is a product of prime ideals, then we have also the uniqueness of this factorization.

Corollary 1.18 *In a Dedekind domain the factorization of any ideal into prime ideals is unique.*

Proof

This follows from Theorem 1.17, from Lemma 1.16, and also from the fact that the ring is a Dedekind domain. □

In order to achieve some useful and important characterizations of Dedekind domains, we announce some technical results about fractionary ideals in Dedekind domains without proofs.

Theorem 1.19 *([19]) Let R be a Dedekind domain, every non-zero fractionary ideal of R, $\underline{a}$, is invertible and can be written, in a unique way, in the form*

$$\underline{a} = \prod_{\underline{p},prime} \underline{p}^{n_{\underline{p}}(\underline{a})}, \tag{2}$$

where $n_{\underline{p}}(\underline{a}) \in \mathbb{Z}$ are non-zero, for given $\underline{a}$, only for a finite number of $\underline{p}$. In order that $\underline{a} \subseteq \underline{b}$, it is necessary and sufficient that $n_{\underline{p}}(\underline{a}) \geq n_{\underline{p}}(\underline{b})$ for every $\underline{p}$. We have also the relations:

$$n_{\underline{p}}(\underline{a} + \underline{b}) = \min(n_{\underline{p}}(\underline{a}), n_{\underline{p}}(\underline{b})), \tag{3}$$

$$n_{\underline{p}}(\underline{a} \cap \underline{b}) = \max(n_{\underline{p}}(\underline{a}), n_{\underline{p}}(\underline{b})), \tag{4}$$

$$n_{\underline{p}}(\underline{a} \cdot \underline{b}) = n_{\underline{p}}(\underline{a}) + n_{\underline{p}}(\underline{b}). \tag{5}$$

The ideals $\underline{a} : \underline{b}$ and $\underline{a} \cdot \underline{b}^{-1}$ are equal, and we have that

$$n_{\underline{p}}(\underline{a} : \underline{b}) = n_{\underline{p}}(\underline{a} \cdot \underline{b}^{-1}) = n_{\underline{p}}(\underline{a}) - n_{\underline{p}}(\underline{b}). \tag{6}$$

After this description, we want to study two important characterizations of this kind of rings: the first has a theoretical nature, while the second one is very useful as a method to recognize a Dedekind domain.

Theorem 1.20 (First characterization of Dedekind domains) *Let R be an integral domain. R is a Dedekind domain if and only if the set $\mathcal{I}$ of fractionary ideals of R is a group under multiplication.*

Proof

$\Rightarrow$ It is clear since every fractionary ideal of a Dedekind domain is invertible by the above theorem, and the set $\mathcal{I}$ needs only this property to be a group.
$\Leftarrow$ By Lemma 1.14, every ideal in R has a finite basis, and so it is noetherian. Now, our aim is to prove that every proper ideal of R is a product of maximal ideals, and this will complete the proof. Assuming, by contradiction, that the set of the non-zero proper ideals that are not product of maximal ideals is not empty, and let $\underline{a}$ be the maximal ideal of this set (there exists one such ideal since R is noetherian). Since $\underline{a}$ is not a maximal ideal, it is strictly contained in a maximal ideal $\underline{m}$. Since $\mathcal{I}$ is a group, there is in $\mathcal{I}$ the ideal $\underline{m}^{-1}\underline{a}$, and this ideal is an integral ideal that strictly contains $\underline{a}$: in fact, from $\underline{m}^{-1}\underline{a} = \underline{a}$, we would deduce that $\underline{m}\ \underline{a} = \underline{a}$, in contradiction with Nakayama's Lemma. Therefore, $\underline{m}^{-1}\underline{a}$ is product of maximal ideals, in virtue of the maximality of $\underline{a}$, and then also $\underline{a} = \underline{m}\ \underline{m}^{-1}\underline{a}$ is product of maximal ideals. This is a contradiction. □

Finally, we prove the other characterization of Dedekind domains that constitutes a good method of checking whether a given domain is or is not a Dedekind domain. To prove this theorem we need the following lemma, that we only announce, about prime ideals of principal ideals.

Lemma 1.21 *([19]) Let R be a noetherian integrally closed domain and $\underline{p}$ be a non-zero maximal ideal of R. If $\underline{p}$ is a prime ideal of a principal ideal (y), then $\underline{p}$ is invertible.*

Theorem 1.22 (Second characterization of Dedekind domains) *Let R be an integral domain, R is a Dedekind domain if and only if it satisfies the following conditions:*

1. *R is noetherian;*

2. *every proper prime ideal of R is maximal;*

3. *R is integrally closed.*

Proof

$\Rightarrow$ The fact that R is noetherian follows from Theorem 1.17 and from Lemma 1.14.

From Theorem 1.17, it follows that every proper ideal is a maximal ideal.

Finally, we have to prove that R is integrally closed. Let us consider $x \in K$, where K is the quotient field of R, which is integral over R. We can find a common denominator $d \neq 0$ in R, such that $dx^n \in R$ for every $n \geq 0$. Then, for every prime ideal $\underline{p} \subseteq R$, we have $v_{\underline{p}}(dx^n) = v_{\underline{p}}(d) + nv_{\underline{p}}(x)$ for every n. But $v_{\underline{p}}(d)$ and $v_{\underline{p}}(x)$ are integers and n is arbitrary, so $v_{\underline{p}}(x) \geq 0$, and then $v_{\underline{p}}(Rx) \geq 0$ for each prime ideal $\underline{p}$, i.e. $x \in R$. Thus R is integrally closed.

$\Leftarrow$ We notice that in the proof of Theorem 1.20 the assumption that every ideal of R is invertible has been used only to establish that R is noetherian, while the rest of the proof was based on the fact that R is noetherian and on the assumption that every prime ideal is invertible. Since, now we are assuming that R is noetherian, in order to prove that R is a Dedekind domain, we have only to show that every proper prime ideal $\underline{p}$ of R is invertible. We note that if y is a non-zero element of $\underline{p}$, then $\underline{p}$ must contain some prime ideal of the principal ideal (y), but, since all proper prime ideals in R are maximal, $\underline{p}$ itself must be a prime ideal of (y). The theorem follows easily from Lemma 1.21. □

After the above theorem, we are very close to another characterization of Dedekind domains: in fact, a noetherian 1-dimensional domain, R, is a Dedekind domain if and only if the localization $R_{\underline{p}}$ is a discrete valuation ring for each prime $\underline{p}$.
To achieve this result, we first announce two propositions.

Proposition 1.23 *Let B be a ring and A a subring of B, then the following sentences are equivalent:*

1. *$x \in B$ is integral over A;*
2. *$A[x]$ is a finitely generated A-module;*
3. *$A[x]$ is contained in a subring C of B, such that C is a finitely generated A-module;*
4. *There exists a faithful $A[x]$-module M, i.e. $\mathrm{Ann}_{A[x]}(M) = (0)$ which is finitely generated.*

The other proposition that is very useful to prove the third characterization of Dedekind domain is a local property.

Proposition 1.24 *Let A be an integral domain, then the following sentences are equivalent:*

1. *A is integrally closed;*
2. *$A_{\underline{p}}$ is integrally closed for each prime ideal $\underline{p}$;*
3. *$A_{\underline{m}}$ is integrally closed for each maximal ideal $\underline{m}$.*

Theorem 1.25 (Third characterization of Dedekind domains) *Let R be a noetherian one-dimensional domain, then R is a Dedekind domain if and only if, for each prime ideal $\underline{p}$, the local ring $R_{\underline{p}}$ is a DVR.*

Proof

$\Rightarrow$ Using Theorem 1.22, we know that R is also integrally closed. Then, by Proposition 1.24, for each prime ideal $\underline{p}$, the local ring $R_{\underline{p}}$ is integrally closed too. In order to prove that $R_{\underline{p}}$ is a DVR, we need to prove that the only maximal ideal, $M = \underline{p}R_{\underline{p}}$, is principal, since we already know that $R_{\underline{p}}$ is noetherian and local.

In order to simplify the notation, let A be the local, noetherian ring, $R_{\underline{p}}$. We first note that each non-zero ideal, I, of A is M-primary, i.e. it is a primary ideal and $\sqrt{I} = M$; in fact, since A is noetherian, I can be written as the intersection of finitely many primary ideals, that have to be M-primary, because of the fact that R is one-dimensional and then the only prime non-zero ideal of A is M.

Let $a \in M$ a non-zero element, because of the previous observation, we have that there exists $n \in \mathbb{N}$ such that $M^n \subseteq (a)$ but $M^{n-1} \nsubseteq (a)$. Let b be an element in $M^{n-1} \backslash (a)$ and let us consider $x = a/b \in K$, where K is the fraction field of A. Since $b \notin (a)$, $x^{-1} \notin A$ and then, since A is integrally closed, $x^{-1}$is not integral over A. Now we prove that $x^{-1}M \nsubseteq M$, in fact, if we suppose the contrary, M would be a faithful $A[x^{-1}]$-module that is also finitely generated and then x^{-1} would be integral over A, because of Proposition 1.23. But, on the other hand, $x^{-1}M \subseteq M$, since $a \in M$, and it is an ideal of A not contained in the only maximal ideal of A, then we must have that $A = x^{-1}M$, and so $M = xA = (x)$.

$\Leftarrow$ The converse is very simple, in fact, in order to get that R is a Dedekind domain, it is sufficient to prove that R is integrally closed. But this is true by hypothesis and by Proposition 1.24. □

Here, we have an application of the last two characterizations of Dedekind domains to Algebraic Geometry.

Observation 1.26 *Let us consider $V = V(f)$ be an irreducible plane curve and let $\Gamma[V] = K[x,y]/(f)$, where K is a field, be its coordinate ring. A well-known geometrical result tells us that: V is smooth if and only if the local ring $\mathcal{O}_P(V)$ is a Discrete Valuation Ring, for each point $P \in V$ (see [11]).*
We now apply the above characterization of Dedekind domains to our case: $\Gamma[V]$ is a noetherian, one-dimensional domain, since V is an irreducible curve; $\mathcal{O}_P(V)$, where $P = (a,b) \in V$, is the localization of the coordinate ring in the maximal ideal $(x-a, y-b)$. So, using Theorem 1.22 and Theorem 1.25, we have that V is smooth if and only if $\Gamma[V]$ is integrally closed, since it is already one-dimensional and noetherian.

Finally, we want to prove an important result about Dedekind domains that shows how much they are close to PID's: in fact we will show that a basis of a non-zero ideal of a Dedekind domain R is constituted by two elements.

Lemma 1.27 *Let us consider a Dedekind domain R and a proper ideal $\underline{a}$, then $R/\underline{a}$ is a PIR.*

Proof
Let $\underline{a} = \prod_i \underline{p}_i^{n(i)}$ be the factorization of $\underline{a}$ into prime ideals. Then, $R/\underline{a}$ is isomorphic to the direct product of the rings $R/\underline{p}_i^{n(i)}$. So, it is sufficient to prove that $R/\underline{p}_i^{n(i)}$ is a PIR, to get that $R/\underline{a}$ is itself a PIR.
We can suppose that $\underline{a}$ is a power of a prime ideal, say $\underline{p}^n$.
The only proper ideals of $R/\underline{p}^n$ are $\underline{p}/\underline{p}^n$, $\underline{p}^2/\underline{p}^n$, $\dots$, $\underline{p}^{n-1}/\underline{p}^n$, since all ideals in R are product of prime ideals, and the only prime ideal containing $\underline{p}^n$ is $\underline{p}$.
Since R is noetherian, because of the fact that it is a Dedekind domain,

$\underline{p}^2 \subsetneq \underline{p}$, so we can fix an element t which is in $\underline{p}$ but not in $\underline{p}^2$. Since $Rt + \underline{p}^n \neq \underline{p}^k$, for each $k > 1$, otherwise we would have that $t \in \underline{p}^2$, we must have $\underline{p} = Rt + \underline{p}^n$. This implies that, in $R/\underline{p}^n$, $\underline{p}/\underline{p}^n = (t)/\underline{p}^n$, and then all the powers of this ideal are principal ideals too, i.e. all the ideals of $R/\underline{p}^n$ are principal.

□

Here we have another way to prove the above lemma, using the following result.

Proposition 1.28 *Let $(R, \underline{m})$ be a noetherian local ring, whose only ideals are powers of the maximal ideal. Then R is a PIR.*

Proof

Let x be a non-zero element in $\underline{m}$ but not in $\underline{m}^2$ (this is possible since R is a local noetherian ring). Then, the following equality must hold, $(x) = \underline{m}$. □
The Lemma 1.27 is a corollary of the above proposition, since $R/\underline{p}^n$ is a local noetherian ring whose only ideals are powers of the maximal ideal.

Theorem 1.29 *In a Dedekind domain R, very proper ideal $\underline{a}$ has a basis consisting of two elements.*

Proof

We take a non-zero element a in $\underline{a}$. As R/Ra is a PIR, by Lemma 1.27, the ideal $\underline{a}/Ra$ is principal, let b be an element of $\underline{a}$, whose residue class generates $\underline{a}/Ra$. Then $\{a, b\}$ is the basis of $\underline{a}$.

□

We notice that in the proof of the previous theorem the first element a of the basis of $\underline{a}$ is an arbitrary non-zero element of R.

1.3 Half-Factorial Domains

This section deals with a new kind of generalization of the concept of UFD, the Half-factorial Domain, or briefly HFD. Here we explain the relation between this new concept and the one of Dedekind domain, described in the above section. But, first we have to define the concept of *atomic ring* and to give some of its properties.

Definition 1.30 *Let R an integral domain. R is called* atomic *if every non-zero, non-unit is a product of irreducible elements.*

Proposition 1.31 *An integral domain R which is also noetherian is atomic.*

Proof

The proof is very simple and it uses only the fact that the ACC (Ascending Chain Condition) holds in R.

In fact, let us consider the set S of those non-units and non-zero that do not factor into irreducible elements. By contradiction, let us suppose that there is $x \in S$: x is not irreducible, then there are two non-zero and non-units a, b such that $x = ab$; at least one of these two elements is in S, say a, otherwise x would be product of irreducible elements, i.e. $x \notin S$. Since, $a \mid x$, but $x \nmid a$, we have that $(x) \subsetneq (a)$; by iteration, we get an infinite ascending chain, against the assumption that R is noetherian. □

We notice that, by Theorem 1.22, every Dedekind domain is atomic, since it is a noetherian domain.

Now, we give two important notions: the *Half-factorial Domain* and the *Class Group* of a Dedekind domain.

Definition 1.32 *An atomic domain R is an* Half-factorial Domain *(HFD), if the following equality*

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m,$$

where, for each i, j, α_i, β_j are irreducible, implies that $n = m$.

Let us consider a Dedekind domain, R, by Theorem 1.20, we have that the set of all the fractionary ideals of R, $\mathcal{I}$, is a group under multiplication, in particular it is an abelian group, generated by prime ideals, by Theorem 1.19. Let us denote with $\mathcal{H}$ the normal subgroup of $\mathcal{I}$ made of the principal fractionary ideals.

Definition 1.33 *The* class group *of R is the quotient group $\mathcal{G} = \mathcal{I}/\mathcal{H}$. Its elements are equivalence classes, and two fractional ideals, I, J, belong to the same class if there is $x \in K\backslash\{0\}$, where K is the quotient field of R, such that $I = xJ$.*
If the class group of R is finite, then its order, n, is the class number *of K.*

Here we have an example of Dedekind domain, whose class group is finite.
Example
Let K a finite extension of the rationals. The *ring of integers*, R, of K, is the integral closure of $\mathbb{Z}$ in K. Then, R is a Dedekind domain (see [4], p. 144), and the class group of R is finite (see [14]). This group has also the property that each class contains a prime ideal (see [13]). □

Now, we have a theorem that relates the HFD's and the subclass of those Dedekind domains whose class group is finite and such that each class contains a prime ideal.

Theorem 1.34 *Let R be a Dedekind domain with finite class group, and K its quotient field. Let us suppose that each class in $\mathcal{G}$ contains a prime ideal. Then, R is an HFD if and only if K has class number* 1 *or* 2.

Proof
⇒ Let us suppose, by contradiction, that $|\mathcal{G}| > 2$. We have to distinguish between two cases.
First, there is an element $g \in \mathcal{G}$, such that $o(g) = n > 2$. In this case, we

consider the two different classes g and g^{-1}: by hypothesis, there is a prime ideal $P \in g$ and a prime ideal $Q \in g^{-1}$. Then, since the order of g and of g^{-1} is n, we have that $P^n = (a)$, $Q^n = (b)$ and $PQ = (c)$, where $a, b, c \in R$ are non-zero and irreducible: in fact, if there are two non-unit elements, $a_1, a_2 \in R$, such that $a = a_1 a_2$, using the fact that R is a Dedekind domain, we have that

$$(a) = P^n = (a_1)(a_2) = \prod_i P_i \prod_j Q_j,$$

where P_i and Q_j are prime ideals, and, so, by the uniqueness of the factorizations into prime ideals, we must have that $P_i = P$ and $(a_1) = P^k$ and that $Q_j = P$ and $(a_j) = P^{n-k}$, with $k \geq 1$, but this is a contradiction, because, since the order of g is n, P^k and P^{n-k} cannot be principal ideals; in similiar ways, we can prove that also b and c are irreducible.

Now, $(a)(b) = (PQ)^n = (c^n)$ implies that there is a unit $u \in R$ such that $ab = uc^n$, this is a contradiction, because $n > 2$ and R is supposed to be an HFD.

Second case, each element $g \in \mathcal{G}$ has order 2. We consider, since $|\mathcal{G}| > 2$, g_1 and g_2, different from unity, such that $g_1 \neq g_2$, and we take g_3 to be $(g_1 g_2)^{-1}$. By hypothesis, there are three prime ideals, $P \in g_1$, $Q \in g_2$ and $S \in g_3$, and we have that $P^2 = (a)$, $Q^2 = (b)$, $S^2 = (c)$ and $PQS = (d)$, where $a, b, c, d \in R$ are irreducible elements, let us prove, for instance, that a is irreducible: if, by contradiction, $a = a_1 a_2$, with a_1, a_2 non-units, then we have that

$$(a) = P^2 = (a_1)(a_2) = \prod_i P_i \prod_j Q_j,$$

where P_i and Q_j are prime ideals, and, by the uniqueness of the factorizations into prime ideals, this implies that $(a_1) = P = (a_2)$, but this contradicts the fact that g_1 has order two.

Now, we have that $(d^2) = (PQS)^2 = (a)(b)(c)$ and, so, there is an unit u such that $d^2 u = abc$, and so we get a contradiction, since R is an HFD.

$\Leftarrow$ Let us suppose that $|\mathcal{G}| \leq 2$.
If $|\mathcal{G}| = 1$, then $\mathcal{I} = \mathcal{H}$, i.e. R is an UFD.
If $|\mathcal{G}| = 2$, then $\mathcal{G}$ is made of two classes, the unity $\mathcal{H}$ and $Q\mathcal{H}$, where Q is a fixed prime non-principal ideal, whose existence is guaranteed by the facts that R is not a PID and that R is a Dedekind domain.
Now, in order to prove that R is an HFD, we consider two factorizations into irreducibles of an element in R and we show that they have the same lenght. In particular, let us consider the following equality

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{7}$$

where α_i, β_j are irreducible. Without loss of generality we can assume that all these factors are not prime, otherwise we can factor out the prime elements.
First, we notice that the product of two non-principal ideals, Qh_1 and Qh_2, with $h_1, h_2 \in \mathcal{H}$, is a principal ideal: in fact, $Qh_1 \cdot Qh_2 = Q^2 h_1 h_2 \in \mathcal{H}$, since $Q\mathcal{H}$ has order two.
Now, we prove that (a), with a irreducible but not prime, is the product of two non-principal prime ideals: it has to be the product of an even number of non-principal prime ideals, otherwise it would not be principal; moreover, if it is product of $2n$, with $n > 1$, prime non-principal ideals, then, as we have noticed, it is the product of $n > 1$ principal ideals, against the assumption that a is irreducible.
Using this fact, we can consider the principal ideals (α_i) and (β_j) and write them as products of two non-principal prime ideals. In this way, we get the following equality:

$$(P_{11}P_{12}) \cdots (P_{n1}P_{n2}) = (Q_{11}Q_{12}) \cdots (Q_{m1}Q_{m2});$$

finally, since R is a Dedekind domain, the factorization into prime ideals is unique, so $2n = 2m$. $\square$

1.4 BG-UFR

In this section, we want to present two different definitions of Unique Factorization Rings, and to draw a comparison of them.

Bouvier defined his own concept of unique factorization ring, briefly B-UFR, in the paper, *Structure des anneaux à factorisation unique*, written in 1974, [5], in a very intuitive way: in fact the Bouvier's definition of unique factorization ring is very close to the definition of unique factorization domain, although he used a different concept of irreducible element.

Galovich in 1978, in the paper, *Unique factorization rings with zerodivisors* ([12]), tried to extend the concept of UFD to rings with zerodivisors, by defining the unique factorization ring according to Galovich, briefly G-UFR. Like Bouvier's definition, the Galovich's one is still intuitive and similiar to the concept of UFD, even if he used a different definition for associate elements.

Throughout this section, R is a commutative ring with unity and with zerodivisors.

1.4.1 Bouvier's definition

At first we give the definitions of irreducible element and of associate elements adopted by Bouvier in [5]. They make the difference, since, otherwise, the concepts of B-UFR and of UFD would be equal.

Definition 1.35 *Let r be a non-zero and non-unit element in R, we say that it is* B-irreducible *if the ideal (r) is a maximal element in the set of the principal proper ideals of R, ordered by the inclusion relation.*

Definition 1.36 *We say that $a, b \in R$ are* associates *if $(a) = (b)$, and we write $a \approx b$.*

Definition 1.37 *We say that R is* B-UFR *(unique factorization ring, according to Bouvier) if:*

- *each non-zero, non-unit element of R is a product of B-irreducible elements;*
- *if $0 \neq a_1 \cdots a_n = b_1 \cdots b_m$, where a_i, b_j are B-irreducible, then $n = m$, and, after renumbering, if necessary, $a_i \approx b_i$, $\forall\ i = 1, \ldots, n$.*

1.4.2 Galovich's definition

As we have done defining Bouvier's UFR, we now describe the concepts, respectively, of irreducible element and of associate elements chosen by Galovich.

Definition 1.38 *Let $r \in R$ be a non-unit, and non-zero element. We say that r is* G-irreducible*, or simply* irreducible *if*

$$r = ab \ \Rightarrow\ a \text{ is a unit or } b \text{ is a unit.}$$

Definition 1.39 *We say that $a, b \in R$ are* G-associates *if there exists a unit u in R such that $a = ub$, and we write $a \approx_G b$.*

Definition 1.40 *We say that R is* G-UFR *(unique factorization ring, accor ding to Galovich) if:*

- *each non-zero, non-unit element of R is a product of G-irreducible elements;*
- *if $0 \neq a_1 \cdots a_n = b_1 \cdots b_m$, where a_i, b_j are B-irreducible, then $n = m$, and, after renumbering, if necessary, $a_i \approx_G b_i$, $\forall\ i = 1, \ldots, n$.*

1.4.3 Comparing B-UFR with G-UFR

Since the two definitions of UFR given above are both similiar to the definition of UFD, we want to draw a comparison of them and also of the different concepts of irreducible element and of associate elements adopted by the two authors.

We start by comparing the concept of B-irreducible element with the classical one.

Proposition 1.41 *Let $r \in R$ be a non-unit, non-zero element, and suppose that it is G-irreducible, then r is B-irreducible.*
The converse is not true.

Proof

By contradiction, let (s) be a proper, principal ideal of R, and let $(r) \subsetneq (s)$. So there is $a \in R$, such that $r = as$, but s is not a unit and r is G-irreducible, hence a must be a unit. It follows that $(r) = (s)$, against assumption.

For the second part of the proof, we give an example of a ring, in which there is a B-irreducible element that is not G-irreducible. Let us consider $R = \mathbb{Z}_6$, and $r = \overline{3}$: the ideal $(\overline{3})$ is maximal among the principal proper ideals of R, but $\overline{3} = \overline{3} \cdot \overline{3}$, so we have that $\overline{3}$ is B-irreducible, but it is not G-irreducible.

□

In the above proposition, we have found out that the concept of B-irreducible element is stronger than the one of G-irreducible element, but there is a class of rings, that we will call *rings with only harmless zerodivisors*, in which these two concepts are the same. In particular, this holds also in local rings and in UFD, as they are rings with only harmless zerodivisors.

Proposition 1.42 *In a local ring (R, M), every B-irreducible element is G-irreducible.*

Proof

In fact, let us consider a non zero non unit element r, that is G-reducible and B- irreducible: by hypothesis, there are two non unit elements, $a, b \in R$, such that $ab = r$, and (r) is a maximal element in the set of the principal proper ideals of R. Hence, $a, b \in M$, because of the fact that R is local, and $(r) = (a) = (b)$. So, there exist some $c, d \in R$, such that $a = rc$ and $b = rd$. Then we have the relation $r(rcd - 1) = 0$, but $rcd \in M$ and R is local, so we get that $rcd - 1$ is a unit and $r = 0$, and here there is a contradiction. □

Let us denote with $Z(R)$ the set of all the zerodivisors of R, and with $U(R)$ the group of units of R.

Definition 1.43 *Let R be a commutative ring, we say that $r \in R$ is an* harmless zero-divisors *if $r \in Z(R)$ and there exists a unit u such that $a = 1 - u$.*

Proposition 1.44 *Let R be a ring with only harmless zerodivisors, then every B-irreducible element is G-irreducible.*

Proof

By contradiction, suppose that there is a non-zero, non-unit element x in R that is B-irreducible, but not G-irreducible. Then, the principal ideal generated by it is a maximal element in the set of the principal and proper ideals of R; in the other hand, there are two non-unit elements, $a, b \in R$, such that $x = ab$ Since x is B-irreducible, we have that $(r) = (a) = (b)$, so we get the relation $x(xcd - 1) = 0$, for some c, d. We now distinguish between two cases: first, if x is not a zerodivisor, then $xcd = 1$, and so x is a unit, here we have a contradiction; second, if x is a zerodivisor, then xcd is still a zerodivisor, and, by hypothesis, $1 - xcd$ is a unit, and $x = 0$, a contradiction. □

Now, we compare the two different definitions of associate elements used by Bouvier and Galovich, respectively, in their papers. In the following propositions we prove the these two concepts, that in a general case are not the same, are equivalent in rings with only harmless zerodivisors.

Proposition 1.45 *Let $a, b \in R$ be G-associates, then they are also associates. The converse is not true.*

<u>*Proof*</u>
The first part of this Proposition is trivial, because, if $a = bu$, for such unit u, then $(a) = (b)$.

We give an example of a ring in which there are two elements that are associates, but not G-associates. Let R be $k[x, y, z]/(x - xyz)$, where k is a field. Let us consider $\overline{x}$ and $\overline{x}\ \overline{y}$: these two elements are associates, because we have that $\overline{x} = \overline{x}\ \overline{y}\ \overline{z}$, but they are not G-associated because $\overline{x} \neq \overline{x}\ \overline{y}\ \overline{u}$, for any unit $\overline{u} \in R$.
We notice that in the ring R there are zerodivisors that are not harmless: for instance, $1 - \overline{y}\ \overline{z}$ is a zerodivisor, but it cannot be harmless because $\overline{y}$ and $\overline{z}$ are not unit, so we cannot write $1 - \overline{y}\ \overline{z}$ as $1 - u$, where u is a unit. □

Proposition 1.46 *Let (R, M) be a local ring, then if $a, b \in R$ are associates, they are also G-associates.*

<u>*Proof*</u>
Let us suppose that a, b are non-unit, non-zero elements, and that they are associates, i.e. $(a) = (b)$, i.e. there are $c, d \in R$ such that $a = cb$ and $b = da$. We now distinguish between two cases: if one or both c and d are units, then we get the result; otherwise, $cd \in M$ and $cd - 1$ is a unit, hence we deduce from the relation $acd = a$ that $a = 0$, and here we get the contadiction. □

As we have done with Proposition 1.42, we could generalize the last result.

Proposition 1.47 *Let R be a ring with only harmless zerodivisors, then if two elements a, b are B-associates, they are also G-associates.*

Proof

Let us suppose that a, b are non-unit and non-zero elements. Since they are G-associates, there are $c, d \in R$ such that $a = cb$ and $b = da$, then $a(1 - cd) = 0$, and, by hypothesis, $1 - cd = 1 - u$ for some unit u. Hence, we have that $cd = u$, so both c and d are unit. □

Finally, we prove that the two definitions of UFR, B-UFR and G-UFR, given in this section, are equivalent.

Definition 1.48 *A commutative ring with unity R is said to be a special PIR (SPIR), if it is a principal ideal ring, with a single prime nilpotent ideal.*

Theorem 1.49 *The following sentences are equivalent:*

(i) R is a G-UFR;

(ii) R is a B-UFR;

(iii) R is an UFD, or a SPIR, or a local ring (R, M) with $M^2 = (0)$.

To achieve this Theorem, we start with some results from Galovich (cf. [12]).

Lemma 1.50 *Let R be a G-UFR with zerodivisors, then there exists an irreducible zerodivisor.*

Proof

Let $x \in R$ be a zerodivisor. Let us consider a factorization of x into irreducibles:

$$x = x_1 x_2 \cdots x_n;$$

we claim that at least one of the irreducible factors of x is a zerodivisor: by hypothesis $\exists\ y \neq 0$, such that $xy = 0$, so $x_1 x_2 \cdots x_n y = 0$; if x_1 is a zerodivisor, we have the result, otherwise, $x_2 \cdots x_n y = 0$; if x_2 is a zerodivisor, we have the thesis, otherwise $x_3 \cdots x_n y = 0$, and so on. Hence we must find among $x_1, x_2, \ldots x_n$ at least one element that is a zerodivisor.

□

Lemma 1.51 *Let R be a G-UFR which contains zerodivisors, the following statements hold:*

1. *every irreducible element is prime;*
2. *every irreducible in R is a zerodivisor;*
3. *every irreducible element in R is nilpotent.*

Proof

1. Let r be an irreducible element in R. Suppose that $r|\ ab$, with $ab \neq 0$. Then, $ry = ab$ for some $y \in R$. Factoring y, a and b into irreducibles, we get
$$ry_1 \cdots y_d = a_1 \cdots a_e b_1 \cdots b_f.$$
Since R is G-UFR, r is a G-associate of one of the a_i, or one of the b_j, so we have that either $r|a$, or $r|b$.

2. By contradiction, suppose that r is an irreducible element, which is not a zerodivisor. By Lemma 1.50, there exists an element s, which is irreducible and zerodivisor, i.e. there is $x \in R$ non-zero such that $sx = 0$.
Let $t = r + s$, since r does not divide s (otherwise it would be a

zerodivisor), r does not divide t.

We have that

$$tx = rx + sx = rx \neq 0.$$

Then, factoring into irreducibles both t and x, we get

$$t_1 \cdots t_n x_1 \cdots x_m = r x_1 \cdots x_m,$$

so by uniqueness of factorization, $n = 1$ and r divides $t_1 = t$, here we get a contradiction.

3. Let r be irreducible, by 2., we know that $rx = 0$, for some $x \neq 0$. Putting $r = r_1$, and factoring x into irreducibles, $x = r_2 \cdots r_m$, we get

$$r_1 r_2 \cdots r_m = 0;$$

We can rewrite this relation in the form

$$s_1^{a_1} \cdots s_n^{a_n} = 0,$$

where $r = s_1$, s_i and s_j are non-G-associate irreducibles if $i \neq j$, and a_i are positive integers.

If $n = 1$, we get that r is nilpotent, otherwise, let $t = s_1^{a_1} + s_2^{a_2} \cdots s_n^{a_n}$. Note that, since $x \neq 0$, $s_2^{a_2} \cdots s_n^{a_n} \neq 0$. The irreducible element r does not divide t, otherwise it must divide $s_2^{a_2} \cdots s_n^{a_n}$, but, by 1., r is prime, hence r must divide s_i for some $i > 1$. But, we have that $s_1^{a_1} t = s_1^{2a_1} + s_1^{a_1} \cdots s_n^{a_n} = s_1^{2a_1}$, which violates unique factorization unless $s_1^{2a_1} = r^{2a_1} = 0$.

□

The proposition below is very important not only because it is useful to prove the equivalence between the two definitions of UFR, but also because it assures us of the fact that every G-UFD is a local ring.

Proposition 1.52 *Let R be a G-UFR and let M be the set of non-units of R. Then (R, M) is a local ring.*

Proof

By Lemma 1.51, we have that every non-unit in R is nilpotent, in fact, suppose that x is a non-unit and non-zero element, we can write it as a product of irreducible elements, which are nilpotent, so x is a nilpotent element.
So we have that M is equal to the nilradical of R, i.e. it is an ideal. M is the only maximal ideal of R: it is clear that it is maximal, since the elements that are not in M are units; it is also the only one, because it is the nilradical of R. □

Theorem 1.53 *Any G-UFR with zerodivisors is a local ring whose maximal ideal M is the set of all non-units. In such a case, either M is principal, or $rs = 0$ for all irreducibles r and s (not necessarily distinct).*

Proof

If M is principal, we get the result. Otherwise, let us suppose that there are two irreducible elements $r, s \in R$, which are not G-associates, we now prove that $rs = 0$. By contradiction, suppose that $rs \neq 0$, and choose the least integers n, m such that $r^n = s^m = 0$. Then $rs = r(r^{n-1} + s)$, and by Lemma 1.51(1.), we conclude that s divides $r^{n-1} + s$, so s divides r, which is a contradiction.

□

Before proving the main theorem of this section, we want to prove some simple lemmas that describe the structure of SPIR's and that will be also very useful in the generalization of the second chapter of this work.

Lemma 1.54 *Let R be a SPIR, then it is a ring in which each non-zero element can be written in a unique way as*

$$s = ur^m \quad \textit{where } u \textit{ is a unit and } \; 0 \leq m < n,$$

where r is the element that generates the only prime ideal, P, of R, and n is its nilpotency.

Proof

It is a principal ideal ring, in which there is a single prime ideal P such that $P^n = (0)$, for some n. Because of these facts, there is $r \in R$ such that $P = (r)$ and $r^n = 0$. First, we prove that each non-zero, non-unit $s \in R$ can be written in the following way

$$s = ur^m \text{ where } u \text{ is a unit and } 0 \leq m < n.$$

Since s is not a unit, we have that

$$\exists\ k_1 \text{ such that } s = br^{k_1};$$

if b is a unit, we have the result, otherwise we have that

$$\exists\ k_2 \text{ such that } b = cr^{k_2};$$

so we obtain the following ascending sequence

$$(s) = (br^{k_1}) \subseteq (b) = (cr^{k_2}) \subseteq (c) \subseteq \cdots$$

that must end because of the condition $r^n = 0$, and of the fact that s is not zero.

We have also that the factorization of $s = ur^m$ is unique, because of the fact that r is the greatest power of r that divides s. □

Proposition 1.55 *A SPIR is just that same of a local Artinian PIR.*

Proof

We already know that an Artinian local PIR is a SPIR: in fact, it is a local ring, it is a PIR, and its maximal ideal is nilpotent, because of the fact that the ring is Artinian and so the terminal condition about descending chains holds.

Vive versa, let $(R, (r))$ be a SPIR, then by the reasoning done in Lemma 1.54, each non zero element a in R can be written as ur^n, where u is a unit and $0 \leq n < m$, and m is the nilpotency of (r). So the ideals of R are precisely $(0), (r)^n$, with $0 \leq n < m$. Then, we have that our ring is also Artinian and by hypothesy it is local and PIR. □

Now we are ready to prove the following result.

Theorem 1.56 *The following sentences are equivalent:*

(i) R is a G-UFR;

(ii) R is an UFD, or a SPIR, or a local ring (R, M) with $M^2 = (0)$.

Proof

(i)⇒(ii) Let us suppose that R is a G-UFR.
We distinguish between two cases: first, R is an integral domain; second, R is a G-UFR with zerodivisors.

In the first case, R is a UFD, because in a domain the concepts of G-UFR and UFD are the same.

In the second case, we use Theorem 1.53: let M be the only maximal ideal of R, we know that it is the set of all nilpotent of R; we know also from the last theorem, that either M is principal, or $rs = 0$ for all irreducibles r and s (not necessarily distinct).
If M is principal, there is an element $s \in M$ such that $M = (s)$, but s is a nilpotent, so there exists an integer n such that $(s)^n = 0$. From the fact that M is principal, we deduce also that R is a PIR, because every proper ideal of R is contained in M. Hence, R is a SPIR.
Otherwise, the fact that $rs = 0$ for all irreducibles r and s is equivalent to

$M^2 = (0)$, so, in this case, we have that (R, M) is a local ring with $M^2 = (0)$. (ii)$\Rightarrow$(i) If R is a UFD, it is also a G-UFR.

Let us suppose that R is a SPIR, then by Lemma 1.54 each non-zero element s has a unique factorization into irreducibles, $s = ur^m$, for some unit u and some m.

Let us suppose that (R, M) is a local ring with $M^2 = (0)$: if s is a non-unit, non-zero, then $s \in M$ and s is irreducible, otherwise $s = ab$ with a, b non-unit, but $a, b \in M$, so $ab = 0$, a contradiction; the second condition is also guaranteed.

□

Now we want to obtain a similiar result using Bouvier's definition of UFR.

Theorem 1.57 *The following sentences are equivalent:*

(i) R is a B-UFR;

(ii) R is an UFD, or a SPIR, or a local ring (R, M) with $M^2 = (0)$.

Proof

If R is a UFD, it is also a B-UFR, because in domains we have that B-irreducible is equivalent to irreducible.

Let us suppose that R is a SPIR: it is a principal ideal ring, in which there is a single prime ideal P such that $P^n = (0)$, for such n. Because of these facts, there is $r \in R$ such that $P = (r)$ and $r^n = 0$. We want to prove the two conditions contained in the definition of B-UFR. First, as we have done in Theorem 1.56, we have that each non-zero, non-unit $s \in R$ can be written in the following way

$$s = ur^m \quad \text{where } u \text{ is a unit and } \ 0 \leq m < n,$$

so this is the factorization into irreducibles of s, so, by Proposition 1.41, it is also the factorization into B-irreducibles of s.

The second condition is also satisfied, because the factorization of $s = ur^m$ is unique.

Let us suppose that (R, M) is a local ring with $M^2 = (0)$: if s is a non-unit, non-zero, then $s \in M$ and s is irreducible, otherwise $s = ab$ with a, b non-unit, but $a, b \in M$, so $ab = 0$, a contradiction, again because of Proposition 1.41, s is B-irreducible; the second condition is also guaranteed.

To obtain the converse, we have to repeat the proofs of Lemma 1.51, of Theorem 1.53, and finally of Theorem 1.56, in which we have to replace G-UFD with B-UFD. So we get the same results also for B-UFD rings.

□

We will use the term BG-UFR (Bouvier-Galovich unique factorization ring) for the equivalent unique factorization rings introduced by Bouvier and Galovich.

1.5 Fletcher's definition

There is another way to extend the notion of UFD to rings with zerodivisors. In fact, Fletcher, in the paper *Unique Factorization Rings*, ([8]), defined the F-UFR's (unique factorization rings according to Fletcher) using a new concept of irreducible element, and also the concepts of U-class and U-decomposition of an element. So this definiton is surely less intuitive than the other two. Although, Fletcher gave also a characterization of F-UFR's in another paper, *The structure of unique factorization rings*, ([9]), that is very useful to draw a comparison with the BG-UFR's.

Let us consider a commutative ring with unity, R.

Definition 1.58 *Let $r = a_1 \cdots a_n$ be a factorization of $r \in R$. A* refinement *of this factorization is obtained by factoring one or more of the factors.*

Definition 1.59 *A non-unit element $r \in R$ is said to be* F-irreducible *if each factorization of r has a refinement containing r, as one of the new factors.*

This definition can be formulated in another, more intuitive, way, because of the following proposition.

Proposition 1.60 *The following sentences are equivalent:*

1. *$r \in R$ is an F-irreducible element;*
2. *if $r = ab$, then $a \in (r)$ or $b \in (r)$;*
3. *if $r = ab$, then $(r) = (a)$ or $(r) = (b)$.*

Proof
1. $\Rightarrow$ 2. If $r = ab$, since r is F-irreducible, there is a refinement of this factorization that contains r as one of the new factors, so we must have that either $a = a'r$ or $b = b'r$.
2. $\Rightarrow$ 3. It is trivial.
3. $\Rightarrow$ 1. Let $r = a_1 \cdots a_n$ be an arbitrary factorization of r, we want to prove that this factorization has a refinement that contains r as one of the new factors, i.e. we have to prove that there exist at least one i such that $a_i \in (r)$. We proceed by induction. If $n = 2$, the result is ensured from the hypothesis. Let us suppose that the thesis holds for $n - 1$ and let us prove it when the number of factors is n: if $r = a_1 \cdots a_n$, then we have that either $a_1 \in (r)$ or $a_2 \cdots a_n \in (r)$, if the second case holds, we apply induction hypothesis to get our result. □

Definition 1.61 *The U-class of an element $r \in R$ is the following set*

$$U(r) = \{a \in R |\ abr = r \text{ for some } b \in R\}.$$

Now, we want to underline the features of the U-class of an element in R and to descover the relationship between the definition of irreducible element given by Bouvier in Section 1.4.1 and the above definition given by Fletcher.

Proposition 1.62 *The U-class of an element $r \in R$. $U(r)$ is a multiplicatively closed and saturated set.*

Proof

Let a, b be two elements of $U(r)$, then there are $c, d \in R$ such that $acr = r$ and $bdr = r$, so we have that

$$r = acr = ac(bdr) = (ab)(cd)r,$$

hence $ab \in U(r)$.

If $ab \in U(r)$, there exists $c \in R$ such that $abcr = r = a(bc)r = b(ac)r$, hence, because of the fact that $ac \in R$ and $bc \in R$, both a and b are elements of $U(r)$. □

Proposition 1.63 *Let R be a commutative ring and $r \in R$, then the following sentences are equivalent:*

1. *$a \in U(r)$;*
2. *$(a) + (0 : r) = (1)$;*
3. *a is a unit in the quotient $R/(0 : r)$.*

Proof

1. $\Rightarrow$ 2. By definition, there is $b \in R$, such that $(ab - 1)r = 0$, then $c = ab - 1 \in (0 : r)$ and we have that $1 = ab - c \in (a) + (0 : r)$.

2. $\Rightarrow$ 3. It is trivial.

3. $\Rightarrow$ 1. If there is some $b \in R$ such that $ab = 1 + c$, where $c \in (0 : r)$, then

$0 = cr = (ab - 1)r$, and so $a \in U(r)$. □

In the following we prove that Fletcher's definition of irreducible element is a more general concept of Bouvier's one.

Proposition 1.64 *If $r \in R$ is B-irreducible element, then it is a F-irreducible element.*

Proof

Suppose that $r = a_1 a_2 \cdots a_m$ and, for instance, let $a_1, a_2, \ldots, a_s$ be non-units, hence $(r) \subseteq (a_i)$, for each $i = 1, 2, \ldots, s$, and, by hypothesis, we must have that $(r) = (a_i)$ for those i, i.e. there is a refinement of the given factorization that contains r, then, because we have taken an arbitrary factorization, r is F-irreducible. □

But, this two concepts are equivalent in the case of a ring with only harmless zerodivisors, and in particular, in the local case.

Proposition 1.65 *Let R be a ring with only harmless zerodivisors, if $r \in R$ is a non-zero, F-irreducible element, then it is also a B-irreducible element.*

Proof

By contradiction, let us suppose that $r \in R$ is F-irreducible, but B-reducible, then there exists a non unit $a \in R$ such that $(r) \subsetneq (a)$, i.e. there is a non unit element $b \in R$ such that $r = ab$. Since r is F-irreducible, we have that $a \in (r)$ or $b \in (r)$: in the first case, we get a contradiction, because we obtain that $(r) = (a)$; in the second case, we have that $b = cr$ and that $r(1-ac) = 0$, but $r \neq 0$, then we get that $1 - ac = 1 - u$, where u is a unit, and that a is a unit, and here we have the contradiction. □

Corollary 1.66 *In UFD's and in local rings, the F-irreducible elements are also B-irreducible.*

Proof

This result is true, since UFD's and local rings are rings with only harmless zerodivisors. □

Because of Proposition 1.65 and of Proposition 1.41, in a ring with only harmless zerodivisors the three concepts of irreducible element, given respectively, by Galovich, Bouvier and Fletcher, are just the same.

To be ready to define the Fletcher's UFR, we have to talk about U-decompositions.

Definition 1.67 *A* U-decomposition *of an element $r \in R$ is a factorization of r*

$$r = (p'_1 \cdots p'_k)(p_1 \cdots p_n),$$

where
1. p'_i, p_j are F-irreducible, $i = 1, \ldots, k$ and $j = 1, \ldots, n$;
2. $p'_i \in U(p_1 \cdots p_n)$, $i = 1, \ldots, k$;
3. $p_j \notin U(p_1 \cdots \widehat{p_j} \cdots p_n)$, $j = 1, \ldots, n$.
where $\widehat{}$ denotes that the term is omitted.
In a U-decomposition $p_1, \ldots p_n$ are said to be the relevant part, $p_1 \cdots p_n$ is said the relevant element, and $p'_1, \ldots p'_k$ are said to be the non-relevant part.

Proposition 1.68 *If r has a factorization into F-irreducibles, then r has a U-decomposition.*

Definition 1.69 *Two element $a, b \in R$ are said* F-associates *(or simply associates), if $(a) = (b)$.*

Proposition 1.70 *The relevant element of a U-decomposition of $r \in R$ is an associate of r.*

Definition 1.71 *Two U-decomposition of $r \in R$*

$$r = (p'_1 \cdots p'_k)(p_1 \cdots p_n) = (q'_1 \cdots q'_l)(q_1 \cdots q_m)$$

are said to be associate *if $n = m$ and, after a suitable renumbering of the factors, the elements p_i and q_i are associate for each $i = 1, \ldots, n$.*

Definition 1.72 *A ring R is a* F-UFR*, i.e. a unique factorization ring, according to Fletcher, if:*

1. *every non-unit element of R has a U-decomposition;*
2. *any two U-decompositions of a non-unit element of R are associate.*

Here we have an important result: in domains, the two notions of F-UFR and of UFD are just the same. We notice that this result is not so easy to be proved: in fact the definition of F-UFR is not so intuitive and so close to the one of UFD's as the other two definitions of UFR are, so we need to spend few words more.

Theorem 1.73 *An integral domain R is a F-UFR if and only if it is a UFD.*

<u>*Proof*</u>
Suppose first that R is a F-UFR, and consider only non-zero, non-unit elements of R. Each U-class is the class of units, since R is an integral domain. So, if we consider the U-decomposition of a non-zero, non-unit element, the non-relevant part has to be empty, because it is constituted by elements that are at the same time F-irreducible and units. Hence, R is a UFD.

Conversely, if R is a UFD, then every non-zero, non-unit element r has a unique factorization into irreducibles, and, in a integral domain, an element is irreducible if and only if it is F-irreducible, but by Proposition 1.68 r has a U-decomposition. And also 0 has a unique factorization, because $U(0) = R$

and $0 \in U(r)$ for any $r \neq 0$, hence a U-decomposition of 0 is of the form $(p'_1 \cdots p'_k)0$. So R is a F-UFR.

□

In the following, we announce some important results that give a description of the structure of F-UFR. and finally, we will find out that each F-UFR is a finite direct product of SPIR's and UFD's.
For instance, we will obtain that each Artinian, local, PIR is a F-UFR, and that also a finite direct product of such rings is a F-UFR, hence every Artinian PIR is a F-UFR, because it can be written as a finite product of Artinian local PIR's (see 3.4).

Theorem 1.74 *If R and S are F-UFR's, then $R \oplus S$ is a F-UFR. Hence, the direct sum of finitely many F-UFR's is a F-UFR.*

Let us prove a kind of converse of the theorem above, in which we suppose to have a ring that is a direct product of two rings.

Proposition 1.75 *Let R be the direct product of two rings, A, B, and let us suppose that R is a F-UFR, then both A and B are F-UFR's.*

Proof

For instance, we prove that A is a F-UFR, since the proof that B is a F-UFR is just the same.
Let $a \in A$ be a non-unit element of A and let us consider the element of R, $(a, 1_B)$, which is not a unit since a is not a unit. We know, by hypothesis, that R is a F-UFR, so we can consider the U-decomposition of $(a, 1_B)$:

$$(a, 1_B) = [(p'_1, q'_1) \cdots (p'_n, q'_n)][(p_1, q_1) \cdots (p_m, q_m)].$$

Since every factor of this product is F-irreducible, we must have, by Proposition 1.80, that one and only one of the two components is F-irreducible,

while the other component is a unit. So, because of the fact that $1_B = (q'_1 \cdots q'_m)(q_1 \cdots q_m)$, each p'_i and each p_j must be F-irreducible. Moreover, the other two conditions for $(p'_1 \cdots p'_m)(p_1 \cdots p_m)$ are satisfied, since they hold for the U-decomposition of $(a, 1_B)$. Then, we have found an U-decomposition for a, where a is an arbitrary non-unit element of A.
The fact that two U-decomposition of a non-unit element of A are associate follows from the fact that R is a F-UFR. □

Theorem 1.76 *If R is a SPIR, then R is a F-UFR.*

Theorem 1.77 *Every PIR is a finite direct sum of PID's and of SPIR's.*

Corollary 1.78 *A PIR is a F-UFR.*

Theorem 1.79 (Characterization of F-UFR's) *Every F-UFR is a finite direct sum of UFD's and of SPIR's.*

The following examples show us that the concept of F-UFR is independent of the notion of BG-UFR.

Example

An example of a ring that is a BG-UFR but not a F-UFR is the following:

$$R = \frac{k[x,y]}{(x^2, y^2, xy)},$$

where k is a field. It is a local ring with maximal ideal, (x, y), which is nilpotent with nilpotency 2. Then, by Theorem 1.56, it is a BG-UFR. It cannot be a F-UFR, because it is not a SPIR or a UFD, and, since it is local, it cannot be a direct product of finitely many (two or more) SPIR's and UFD's. □

Example

Conversely, it is easy to prove that $\mathbb{Z}_n$, where $n$is not a power of a prime element, is a F-UFR but not a BG-UFR. Infact, it is a direct product of SPIR's. But, it is neither an UFD nor a local ring, so it can be a BG-UFR. We also observe that this is an example of a ring that is a PIR, but not a BG-UFR). □

1.5.1 Cartesian Product and F-irreducible elements

In the following we want to list some useful properties about the beaviour of F-irreducible elements in the cartesian product of two rings.

Proposition 1.80 *Let A, B be two commutative rings with unity. If $(a, b) \in A \times B$ is an F-irreducible element (so, it is a non-zero, non-unit element), then a is a unit and b is an F-irreducible element or vice versa.*

Proof

Let us consider the following factorization

$$(a, b) = (a, 1_B) \cdot (1_A, b),$$

since, by hypothesis, (a, b) is F-irreducible, we have that either $(a, 1_B) \in ((a, b))$, i.e. b is a unit in B, or $(1_A, b) \in ((a, b))$, i.e. a is a unit in A. We notice that we cannot have that both a and b are units, since (a, b) is not a unit in $A \times B$. □

Proposition 1.81 *Let us consider the direct product of n commutative rings with unity, $B = A_1 \times \cdots \times A_n$, and let $(a_1, \ldots, a_n) \in B$ be a non-unit, non-zero element, if $(a_1, \ldots, a_n)$ is an F-irreducible element, then $\exists\ i = 1, \ldots, n$ such that a_i is F-irreducible and a_j is a unit for each $j \neq i$.*

Proof

Let us consider the factorization

$$(a_1, a_2, \dots, a_n) = (a_1, 1, \dots, 1) \cdots (1, 1, \cdots, a_n),$$

but $(a_1, \dots, a_n)$ is F-irreducible, so, by definition, this factorization has a refiniment that contains $(a_1, \dots, a_n)$ as one of the new factors, i.e. there is $i \in \{1, \dots, n\}$, such that $(1, \dots, 1, a_i, 1, \dots, 1) \in ((a_1, \dots, a_n))$. This means that a_j is a unit for each $j \neq i$, and that a_i is an F-irreducible element, since, if it had a factorization without refiniment that contains it, we could easily find such a factorization for $(a_1, \dots, a_n)$, against the assumption of the F-irreducibility. □

Corollary 1.82 *Let A, B be two commutative rings with unity. If the concept of F-irreducible is equivalent to the concept of B-irreducible in A and in B, then the same occurs in $A \times B$.*

Proof

We already know that in every commutative ring with unity the concept of B-irreducible implies the concept of F-irreducible.

We now prove the converse: if (a, b) is an F-irreducible element in $A \times B$, we know from Proposition 1.80 that a is a unit and b an F- irreducible element, or vice versa. Let us suppose, for instance, that the first case occurs, then, by hypothesis, b is a B-irreducible element. From these facts, it is easy to deduce that the ideal generated by (a, b) is a maximal element among the principal ideals of $A \times B$, i.e., (a, b) is, by definition, a B-irreducible element. □

Corollary 1.83 *Let $A_1, A_2, \dots, A_m$ be commutative rings with unity. If the two concept of irreducible elements, given, respectively, by Bouvier and by*

Fletcher, are equivalent in each A_i, for $i = 1, \dots, m$, then they are equivalent also in the ring $A_1 \times \cdots \times A_m$.

Proof

This result follows directly from the above corollary, by induction. □

Corollary 1.84 *If R is a F-UFR, then the concepts of F-irreducible element and of B-irreducible element are the same.*

Proof

We know, from Theorem 1.79, that every F-UFR is a direct product of finitely many UFD's and SPIR's. Finally, using Corollary 1.66 and Corollary 1.83, we get the result. □

1.6 Some results about rings with only harmless zerodivisors

At first, we want to remind the definition of harmless zerodivisor.

Definition 1.85 *Let R be a commutative ring with unity, we say that $r \in R$ is a harmless zerodivisor, if it is a zerodivisor and it may be written as $r = 1 - u$, where u is a unit.*

In the following, we want to enounce some propositions about rings with only harmless zerodivisors, that we have already proved in the previous sections.

Theorem 1.86 *Let R be a ring with only harmless zerodivisors. Then, the following different concepts of irriducible element are equivalent:*

1. *G-irreducible;*

2. B-irreducible;

3. F-irreducible.

Proof

The equivalences follow from Proposition 1.41, from Proposition 1.64 and from Proposition 1.65. □

Because of Theorem 1.86, in the next chapters, we will not distinguish among the three different concepts of irreducibility.

Lemma 1.87 *Let A and B be rings with only harmless zerodivisors, then $A \times B$ is still a ring with only harmless zerodivisors.*

Proof

We first notice that $(a, b) \in A \times B$ is a zerodivisor if and only if a, b are zerodivisors; the same holds for units.

We know that, since A, B are, by hypothesis, rings with only harmless zerodivisors, $Z(A) \subseteq 1_A - U(A)$ and that $Z(B) \subseteq 1_B - U(B)$, where $U(A)$ and $U(B)$ denote the groups of units respectively of A and B. Then we have that

$$Z(A\times B) \subseteq Z(A)\times Z(B) \subseteq (1_A - U(A)) \times (1_B - U(B)) \subseteq 1_{A\times B} - U(A\times B),$$

i.e. $A \times B$ is a ring with only harmless zerodivisors. □

Proposition 1.88 *If R is an integral domain, or a local ring with maximal ideal M, then it is a ring with only harmless zerodivisors.*

Proof

It is trivial to prove that an integral domain is a ring with only harmless zerodivisors, because it has not zerodivisors.

Let us prove that if (R, M) is a local ring, it has only harmless zerodivisors:

we know that $Z(R) \subseteq J(R) = M$; therefore, in every commutative ring with unity, we have that $J(R) \subseteq 1_R - U(R)$; then we have that $Z(R) \subseteq 1_R - U(R)$ and this completes the proof.

□

Example

Now, we show an example of a ring with only harmless zerodivisors, that is neither an integral domain nor a local ring.

Let A be a SPIR, then $A[x]$ is such a ring.

If (t) is the only maximal ideal of A, then, as we will prove in Fact 2.9, we have that

$$(t) = J(A[x]) = Z(A[x]),$$

and so, as we have done in the proof of the previous proposition, we have that $A[x]$ is a ring with only harmless zerodivisors.

$A[x]$ is not an integral domain, for $Z(A[x])$ is not empty. Furthermore, $A[x]$ is not a local ring, as it is proved in Fact 2.9. □

Theorem 1.89 *If $A_1, A_2, \ldots, A_n$ are rings with only harmless zerodivisors, then in $A_1 \times A_2 \times \cdots \times A_n$ the concepts of B-irreducibility, F-irreducibility and G-irreducibility are equivalent .*

Proof

This result follows, by induction, from Theorem 1.86 and from Lemma 1.87.

□

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

We want now to generalize the paper *Non-unique factorization of polynomials over residue class rings of the integers* (cf. [10]), investigating the non-unique factorization of polynomials in $A[x]$ into irreducible, where $(A, \underline{m})$ is an Artinian, principal and local ring.

At first we want to 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 and from Lemma 1.54 and Proposition 1.55, we deduce that each element $a \in A$, $a \neq 0$, can be represented in the following way

$$a = ut^k,\ \text{where } u \text{ is a unit and } k \in \mathbb{N},\ k < h. \tag{8}$$

We denote by $\mu : A[x] \to K[x]$, where $K = A/\underline{m}$, the canonical projection. We will use the notation just introduced throughout the paper.

2.1 t-adic Valuation

We want to introduce the concept of t-adic valuation. First, we denote with $(\mathbb{N}_h, +, \leq)$ 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 ∞.

Definition 2.1 *Let $v : A \to \mathbb{N}_h$ be the map defined by putting*

$$v(a) = \max\{n \ :\ t^n \mid a\} \quad \text{with } a \neq 0$$
$$v(0) = \infty$$

This map is called t-adic valuation, where $v(a)$ is the natural number that occurs in (8).

Remark 2.2 *The following statements hold:*

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

Definition 2.3 *The previous map can be naturally extended to a map, that we will denote with v, by abuse of notation, $v : A[x] \to \mathbb{N}_h$, where we put*

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

Remark 2.4 *The following statements hold:*

1. $v(f) = \infty \;\Leftrightarrow f = 0$;
2. $v(f + g) \geq \min\{v(f), v(g)\}$;
3. $v(fg) = v(f) + v(g)$.

<u>*Proof*</u>
1. Let $f = \sum_{i=0}^{s} a_i x^i$, $v(f) = \min_{i=0,\dots,s}(v(a_i)) = \infty$ if and only if $v(a_i) = \infty,\;\; i = 0, \dots, s$, for the properties of t-adic valuation of the ring A, we have that this holds if and only if $a_i = 0,\; i = 0, \dots, s$.
2. Let $f = \sum_{i=0}^{s} a_i x^i$ and $g = \sum_{j=0}^{r} b_j x^j$, for instance let $s \leq r$, then $v(f + g) = \min\{v(a_i + b_i), v(b_j) |\, i = 0, \dots, s;\; j = s+1, \dots, r\} \geq \min\{v(a_i),\, v(b_j)| i = 0, \dots s;\; j = 0, \dots, r\} \geq \min\{v(f), v(g)\}$, because of the fact $v(a_i + b_i) \geq \min\{v(a_i), v(b_i)\}$.
3. Let $f = \sum_{i=0}^{s} a_i x^i$ and $g = \sum_{j=0}^{r} b_j x^j$, $v(fg) = v(\sum_{i=0,\dots s;\; j=0,\dots r} a_i b_j x^{i+j}) = \min\{v(a_i b_j)|\; i = 0, \dots s;\; j = 0, \dots r\} = \{v(a_i) + v(b_j)|\; i = 0, \dots s;\; j = 0, \dots r\} = v(f) + v(g)$. □

Fact 2.5 *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 zero-divisor.*

Proof

1. ⇒ 2. If $f = tg$, certainly $f^h = 0$.
2. ⇒ 3. It's trivial.
3. ⇒ 1. By contradiction, let $v(f)$ be equal to 0, i.e. not-every coefficient of f is divisible by t, by the hypothesis $\exists\ g \neq 0$ such that $fg = 0$, then, using Remark 2.4, we obtain that $v(g) = \infty$, here we have a contradiction. □

2.2 Nilpotent elements, regular elements, zerodivisors

Definition 2.6 *Let R be a commutative ring, let $Nil(R)$ be the intersection of all primes in R, $J(R)$ be the intersection of all maximal ideals in R, $Z(R)$ be the set of all zero-divisors in R, and $U(R)$ be the group of all the units.*

Definition 2.7 *Let R be a commutative ring, let $c \in R$, it is a regular element if it is not a zero-divisor.*

Proposition 2.8 *We have that*

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

Proof

⇒ Let $x \in R$ and suppose that $\exists\ y \in R$ such that $1 - xy$ is not a unit, then there exists a maximal ideal M such that $1 - xy \in M$, but $x \in M$ because it is in $J(R)$, so we must have $1 \in M$, and this is a contradiction.

$\Leftarrow$ By contradiction, suppose that $x \notin J(R)$, hence there exists a maximal ideal M of R such that $x \notin M$. So we have that $R = M + (x)$, then there are $m \in M$ and $n \in R$ such that $1 = m + nx$, i.e. $1 - nx = m$, but, by hypothesis, this element is a unit, and here we have the contradiction. □

Fact 2.9 *We have that:*

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

Proof

From 2.5, 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 $\frac{N}{\underline{m}[x]}$ is a maximal ideal in $\frac{A}{\underline{m}}[x]$, so there is an irreducible ideal $\overline{f}$ such that $\frac{N}{\underline{m}[x]} = (\overline{f})$. □

The following results are easy to prove.

Proposition 2.10 *Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, then:*

1. *The following statements are equivalent:*

   (a) *f is a unit;*

   (b) *$\mu(f)$ is a unit;*

   (c) *a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent.*

2. *The following statements are equivalent:*

   (a) f *is nilpotent;*

   (b) $\mu(f) = 0$ *;*

   (c) $a_0, a_1, \ldots, a_n$ *are nilpotent.*

3. *The following statements are equivalent:*

   (a) f *is regular;*

   (b) $(a_0, a_1, \ldots, a_n) = A$ *;*

   (c) $\exists\ i\ :\ a_i$ *is a unit ;*

   (d) $\mu(f) \neq 0$.

Proof

1. (a)⇒(b) It is trivial.
   (b)⇒(c) If $\mu(f) = \sum_{i=0}^{n} \mu(a_i)x^i$ is a unit in $K[x]$, we have that $\mu(a_i) = 0$ for each $i > 0$, and $\mu(a_0) \neq 0$, so $a_i \in \underline{m}\ \forall\ i > 0$, i.e. a_i is nilpotent, and $a_0 \notin \underline{m}$, so it is a unit.
   (c)⇒(a) If $f = a_0 + g$ with a_0 a unit and all coefficients of g in the intersection of all primes of A, then g is in every prime ideal of $A[x]$ and hence $f = a_0 + g$ is in no prime ideal of $A[x]$, and therefore is a unit of $A[x]$..

2. (a)⇒(b) $\exists\ m$ such that $f^m = 0$, we have that $(\mu(f))^m = 0$ in $K[x]$, that is a domain, so $\mu(f) = 0$.
   (b)⇒(c) $\mu(f) = \sum_{i=0}^{n} \mu(a_i)x^i = 0$ if and only if $a_i \in \underline{m}$ for each $i = 0, \ldots, n$, i.e. a_i is nilpotent.
   (c)⇒(a) We have that $a_i x^i$ is nilpotent for each $i = 0, \ldots, n$, but the sum of nilpotent elements is nilpotent.

3. (a)$\Rightarrow$(b) By contradiction, suppose that $(a_0, a_1, \ldots, a_n)$ is a proper ideal of R, then it is contained in $\underline{m}$, but this implies that $a_0, a_1, \ldots, a_n$ are nilpotent, i.e. that f is nilpotent, against the assumption.

   (b)$\Rightarrow$(c) and (c)$\Rightarrow$(d) are trivial.

   (d)$\Rightarrow$(a) By contradiction, we suppose that f is a zero-divisor, so we must have $f \in (t)$, i.e. each a_i is divisible by t, but this is a contradiction because by hypothesis there exists such i such that $a_i \notin (t)$.

□

2.3 Factorization of arbitrary polynomials into regular elements

Lemma 2.11 *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, i.e. if* $f|gh$*, then* $f|g$ *or* $f|h$*;*

(iii) f *is irreducible and zerodivisor.*

Proof

(i) $\Rightarrow$ *(ii)* Let $v : A[x] \to \mathbb{N}_h$ be the t-adic valutation, 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. □

Proposition 2.12 *Let f be a non-zero polynomial in $A[x]$.*

1. *There exist a regular element $g \in A[x]$, and $0 \leq k < h$, 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.*

<u>*Proof*</u>
1. follows from Fact 2.5 and from the definition of t-adic valutation: 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. Therefor, 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 $v(f) = v(a_1) + \cdots + v(a_m)$. □

Fact 2.13 *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 $K[x]$.*

Proof

Assume that $\mu(f_1)$ and $\mu(f_2)$ are coprime in $K[x]$. Then there are β_1 and β_2 in $A[x]$ such that

$$\mu(\beta_1)\mu(f_1) + \mu(\beta_2)\mu(f_2) = 1.$$

Thus,

$$\beta_1 f_1 + \beta_2 f_2 = 1 + tk, \text{where } k \in A[x]. \tag{9}$$

Let

$$l = \sum_{i=0}^{s-1} (-tk)^i$$

Then multiplying (9), we obtain that $1 = l\beta_1 f_1 + l\beta_2 f_2$, so f_1 and f_2 are coprime in $A[x]$.

The converse is trivial. □

Lemma 2.14 (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 $g_1, g_2, \dots, g_n \in A[x]$ such that:*

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

Proof

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

$$h_{11}h_{21} = h_1h_2 + v(\lambda_1h_1 + \lambda_2h_2) + \lambda_1\lambda_2v^2 = h_1h_2 + v + \lambda_1\lambda_2v^2 = f + \lambda_1\lambda_2v^2,$$

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, $2 \leq i \leq n$, then h_1 and $h_2 \cdots h_n$ are coprime. □

Lemma 2.15 *Let f be a regular polynomial in $A[x]$. Then there exists a sequence $\{f_j\}$ of monic polynomials in $A[x]$ with*

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

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

$$b_jf = f_j + g_jf_j \mod(\underline{m}^j).$$

<u>*Proof*</u>
Let $f = \sum_{i=0}^{n} b_ix^i$, where $b_n \neq 0$; if $\deg(\mu(f)) = u \leq n$, b_u is a unit. Choose $g_1 = 0$ and $f_1 = b_u^{-1}(b_0 + b_1x + \cdots + b_ux^u)$.
We now proceed by induction. Assume that $\{f_i\}_{i=1}^{j}$ satisfies the Lemma; then $b_jf = f_j + g_jf_j + h$ where $h \in \underline{m}^j[x]$. Since f_j is monic, we may select q and r in $A[x]$, such that $h = f_jq + r$, 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 $h = 0 \bmod(\underline{m}^j)$ 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 $r = h - qf_j \in \underline{m}^j[x]$.

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

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

□

Theorem 2.16 *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* $\deg(\mu(f))$.

Proof

Let β be the nilpotency of $\underline{m}$, i.e. $\underline{m}^\beta = (0)$. Using the Lemma 2.15, we have that $f = b_\beta^{-1}(1 + g_\beta)f_\beta$, where $g = f_\beta$ is monic and its degree is the degree of $\mu(f)$, and b_β is a unit, and because of the fact that $g_\beta \in \underline{m}[x]$, also $1 + g_\beta$ is a unit.

The uniqueness follows from Proposition 2.10.

□

Theorem 2.17 *Let $f \in A[x]$ be a non-zero regular polynomial, and u and g 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 $d_1, \dots, d_k \in A[x]$ and units $v_1, \dots, v_k \in A[x]$ 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.

2.4 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 remind that an element $f \in A[x]$ is said to be primary if the principal ideal (f) is a 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 2.18 *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 PID $K[x]$, 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.

□

Using the Lemma 2.14, we want to prove the following theorem.

Theorem 2.19 *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

$$f = f_1 \cdots f_r = h_1 \cdots h_s \tag{10}$$

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 2.14 , 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 Fact 2.13, even the

polynomials g_i are coprime.

(ii) From the equation (10), 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, $1 \leq k_i \leq r$, 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, $1 \leq l_j \leq s$ 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 Fact 2.13, 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 $s \leq r$. Similarly, $r \leq s$, 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 Fact 2.13, 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 Fact 2.13, $f_2 \cdots f_r$ 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

$$f_1 = cf_1 f_2 \cdots f_r + df_1 h_1 = ch_1 h_2 \cdots h_r + df_1 h_1,$$

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

$$f = t^k u f_1 f_2 \cdots f_r, \tag{11}$$

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 $t^{h-k}A[x]$.

Proof

We use at first Proposition 2.12, 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 valutation, so k is uniquely determined, and g is unique modulo $t^{h-k}A[x]$.

Then we apply Theorem 2.16 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 2.19 to the equivalence class of the monic polynomial $\overline{h}$ in the ring $t^{h-k}A[x]$.

The fact that u is unique modulo $t^{h-k}A[x]$ follows from Theorem 2.16 and also from the presence of the factor t^k in the equation (11), for the same reason the polynomials f_i are unique modulo $t^{h-k}A[x]$.

□

2.5 Non-uniqueness of factorization in $A[x]$

Now, we want to give an example of non-unique factorization in $A[x]$.
We already know that $t^h = 0$, let us suppose that $h > 3$: if h is even, then we put $k = h/2$ in order to have that $t^{2k} = 0$; if h is odd, then we put $k = (h+1)/2$, and we still have that $t^{2k} = 0$. If k is odd, we do not change it, otherwise we replace it with $k+1$. After the choice of k we want to prove that $x^2 + t^k$ is irreducible, otherwise, there exist $a, b \in A$ such that

$$x^2 + t^k = (x+a)(x+b).$$

So we must have: $a = -b$, and $-a^2 = t^k$ and here we get a contradiction, since k is odd.
If $h = 3$ we take $k = 1$.
We also have that

$$(x^2 + t^k)^m = x^{2m-1}(x + mt^k)$$

so this polynomial can be written as a product of m irreducible factors and also as the product of almost $2m$ factors.

Let us define a new concept that can be considered as the measure of how much the ring is not a unique factorization ring.

Definition 2.21 *Let $(M, \cdot)$ be a cancellative monoid. Let k be ≥ 2, we define $\rho_k(M)$ to be the supremum of those $m \in \mathbb{N}$, for which there is a product of k irreducible elements that can be also be written as a product of m irreducible elements. We also define the* elasticity *of M to be $\sup_{k\geq 2}(\rho_k(M)/k)$.*

We notice that the set, M, of the regular elements of $A[x]$ is a cancellative monoid, so we can talk about the elasticity of $A[x]$.

We want to give another example in order to show 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 2.11, 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.

3 Non-unique Factorization in $B[x]$, where B is an Artinian PIR

3.1 Structure Theorem of Artinian PIR

In the following, we will present a few of the main results about Artinian and noetherian rings.

Proposition 3.1 *Let B be a commutative ring with a unity, then:*

- *if I, J are ideals of B, we have that $\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$;*
- *if I is an ideal of B, $\sqrt{I} = A$ if and only if $I = A$.*

Proposition 3.2 *If B is an Artinian ring, then there is an $h \in \mathbb{N}$, such that $Nil(B)^h = (0)$*

Theorem 3.3 (Chinese Remainder Theorem) *Let B be a commutative ring with unity. Let $I_1, I_2, \dots, I_n$ be ideals of B. Let us consider the ring homomorphism*

$$\begin{array}{rcl} \varphi : B & \longrightarrow & \dfrac{B}{I_1} \times \cdots \times \dfrac{B}{I_n}, \\ \textit{where} \;\; b & \longmapsto & (b + I_1, \dots, b + I_n), \end{array}$$

then:

1. $\mathrm{Ker}(\varphi) = \cap_{i=0}^{n} I_i$;
2. *if I_i, I_j are coprime ideals $\forall\ i \neq j$, then $\cap_{i=0}^{n} I_i = \prod_{i=0}^{n} I_i$;*
3. *φ is surjective if and only if I_i and I_j are coprime $\forall i \neq j$.*

Theorem 3.4 (Structure of Artinian rings) *Let B be an Artinian ring, then B is isomorphic to a direct product of finitely many Artinian local rings.*

Proof

Since B is an Artinian ring, it has finitely many prime (maximal) ideals, $M_1, M_2, \dots, M_n$. Let us consider $Nil(B) = J(B) = \cap_{i=1}^n M_i$. By Proposition 3.2, there is $h \in \mathbb{N}$ such that $Nil(B)^h = M_1^h \cap \dots \cap M_n^h = (0)$. Furthermore, by Proposition 3.1, we have that M_i^h and M_j^h are coprime ideals for each $i \neq j$. Hence, we have that $\cap_{i=1}^n M_i = \prod_{i=1}^n M_i = (0)$, where the first equality is ensured from the Chinese Remainder Theorem. Using again the Chinese Remainder Theorem, we obtain that the following ring homomorphism is an isomorphism:

$$\begin{array}{rcl} \varphi : B & \longrightarrow & \dfrac{B}{M_1^h} \times \dots \times \dfrac{B}{M_n^h}, \\ \text{where } \; b & \longmapsto & (b + M_1^h, \dots, b + M_n^h). \end{array}$$

Finally, we want to prove that $B_i = B/M_i^h$ is an Artinian local ring for each $i = 1, \dots, n$.

It is Artinian, for B is Artinian.

It is local, since M_i is the only maximal ideal containing M_i^h. □

3.2 An Isomorphism Theorem

Theorem 3.5 *Let A, B be two commutative rings with unity. Then*

$$(A \oplus B)[x] \simeq A[x] \oplus B[x].$$

Proof

We want to find a ring isomorphism between these rings. So let us define the following map

$$\begin{aligned} &\psi : (A \oplus B)[x] \longrightarrow A[x] \oplus B[x], \\ &\text{where } \; \psi\left((a_0, b_0) + (a_1, b_1)x + \dots + (a_m, b_m)x^m\right) = \\ &= (a_0 + a_1 x + \dots + a_m, b_0 + b_1 x + \dots + b_m x^m). \end{aligned}$$

Now we prove that this is a ring isomorphism.
Surely, it is a ring homomorphism, because the sum and product in the direct product is defined component by component.
It is also injective and surjective: if $\psi\left((a_0,b_0)+(a_1,b_1)x+\cdots+(a_m,b_m)x^m\right)=(0,0)$, then we must have that $a_0=\cdots=a_m=0_A$, and $b_0=\cdots=b_m=0_B$; it is surjective, because the element $(f(x),g(x))\in A[x]\oplus B[x]$, where

$$f(x)=a_0+a_1x+\cdots+a_mx^m;$$
$$g(x)=b_0+b_1x+\cdots+b_nx^n,$$

and $n\leq m$ is the image of ψ of the following element

$$(a_0,b_0)+(a_1,b_1)x+\cdots+(a_n,b_n)x^n+(a_{n+1},0_B)x^{n+1}+\cdots+(a_m,0_B)x^m$$

that belongs to $(A\oplus B)[x]$. □

Corollary 3.6 *Let $A_1,A_2,\ldots A_m$ be commutative rings with unity, then*

$$(A_1\oplus A_2\oplus\cdots\oplus A_m)[x]\simeq A_1[x]\oplus A_2[x]\oplus\cdots\oplus A_m[x].$$

Proof
It follows, by induction, from the above theorem. □

3.3 Factorization in $B[x]$, where B is an Artinian PIR

In the last two sections, we have found some good results, we will use them to get some information about factorization in $B[x]$, with B Artinian, PIR.

Using Theorem 3.4, we know that B can be written as a finite direct product of artinan local rings, $B_1,B_2,\ldots,B_m$. Since B is a PIR, the rings, $B_1,B_2,\ldots,B_m$ are PIR's too. Then we have written B as finite direct product of Artinian local PIR's. So we want to use what we know about the

factorization in the polynomial rings with coefficients in these rings to get some new results.
Using Theorem 3.5, we know also that

$$B[x] \simeq B_1[x] \oplus \cdots \oplus B_m[x].$$

At first, we want to study the factorization in a polynomial ring, with coefficients in an Artinian PIR which can be written as a product of only two SPIR's, then we will extend the results to the general case by induction.

3.3.1 Factorization of a non-zero element in $B[x]$, where B is a direct product of two SPIR's.

Let us suppose that $B = B_1 \oplus B_2$, where B_1 and B_2 are Artinian local PIR's. Let (t_1) be the only maximal ideal of B_1, $h_1 \in \mathbb{N}$ be its nilpotency; in the same way, let (t_2) be the only maximal ideal of B_2 and $h_2 \in \mathbb{N}$ be its nilpotency. Let v_1 and v_2 be respectively the t_1-adic valuation and the t_2-adic valuation; and let us consider the fields $K_1 = B_1/(t_1)$ and $K_2 = B_2/(t_2)$, and also the canonical projections $\mu_1 : B_1[x] \to K_1[x]$ and $\mu_2 : B_2[x] \to K_2[x]$.

Now, we want to repeat the long path done in the Chapter 2. We begin by studying the factorization of a non-zero element in $B[x]$, and easily, applying the known results, we get the following proposition.

Proposition 3.7 *Let $(f_1, f_2) \in B[x]$ be a non-zero element, where both f_1 and f_2 are non-zero elements, then there exist two regular elements, $g_1 \in B_1[x]$ and $g_2 \in B_2[x]$, and $k_1, k_2 \in \mathbb{N}$, with $0 \leq k_1 < h_1$ and $0 \leq k_2 < h_2$, such that*

$$(f_1, f_2) = (t_1^{h_1} g_1, t_2^{h_2} g_2) = (t_1^{h_1}, t_2^{k_2})(g_1, g_2).$$

Moreover, we have that k_1, k_2 are uniquely determined and that g_i is unique modulo $(t_i)^{h_i - k_i} B_i[x]$, $i = 1, 2$.

Proof

As f_1 and f_2 are non-zero elements respectively in $B_1[x]$ and $B_2[x]$, we can use Proposition 2.12, so we can say that there exist g_1, g_2 regular elements, and $k_1, k_2 \in \mathbb{N}$, with $0 \leq k_1 < h_1$ and $0 \leq k_2 < h_2$, such that

$$f_1 = t_1^{k_1} g_1 \quad \text{and} \quad f_2 = t_2^{k_1} g_2,$$

from these equalities easily follows the main result.
We notice that, as g_1 and g_2 are regular elements, $(g_1, g_2) \in B[x]$ is a regular element too. □

We continue the path by studying the problem of factoring an element in $B[x]$ whose components are both regular.

Proposition 3.8 *Let us consider $(g_1, g_2) \in B[x]$, where g_1, g_2 are both regular. Then, it can be written uniquely in the following way*

$$(g_1, g_2) = (u_1, u_2)(d_1, d_2),$$

where $u_1 \in B_1[x]$ and $u_2 \in B_2[x]$ are units, $d_1 \in B_1[x]$ and $d_2 \in B_2[x]$ are monic polynomials, such that $deg(d_i) = deg(\mu_i(g_i))$, $i = 1, 2$.

Proof

We directly apply Theorem 2.16. We notice that (u_1, u_2) is a unit in $B[x]$. □

From Theorem 2.17, easily we deduce the following result.

Theorem 3.9 *Let $f = (f_1, f_2) \in B[x]$ be a non-zero element, with f_1, f_2 regular polynomial respectively in $B_1[x]$ and in $B_2[x]$, and $u = (u_1, u_2)$ and $g = (g_1, g_2)$ the unique unit and couple of monic polynomials, respectively, in $B[x]$ such that $f = ug$. For every factorization into irreducibles $f = c_1 \cdots c_k$, there exist uniquely determined monic irreducibles $d_1, \ldots, d_k \in B[x]$ and units $v_1, \ldots, v_k \in B[x]$ such that $c_i = v_i d_i$, $u = v_1 \cdots v_k$ and $g = d_1 \cdots d_k$.*

Now, we want to apply Theorem 2.19 to our case in order to find out some factorization results about couples in $B[x]$, whose components are both monic polynomials.

Theorem 3.10 *Let $f = (f_1, f_2) \in B[x]$ be a couple of monic polynomials, whose degrees are both ≥ 1. Then f can be factorized in the following way*

$$(f_1, f_2) = (g_{11}, 1) \cdots (g_{1s}, 1)(1, g_{21}) \cdots (1, g_{2r}),$$

where $\{g_{11}, \ldots, g_{1s}\}$ is a set of pairwise coprime, monic, primary polynomials in $B_1[x]$, $\{g_{21}, \ldots, g_{2r}\}$ is a set of pairwise coprime, monic, primary polynomials in $B_2[x]$, and for each $i = 1, 2, \ldots s$, for each $j = 1, 2, \ldots r$, $\mu_1(g_{1i}) \in K_1[x]$ and $\mu_2(g_{2j}) \in K_2[x]$ are powers of monic irreducible polynomials. Moreover, the elements, $g_{11}, \ldots, g_{1s}$ are uniquely determined, the same holds for $g_{21}, \ldots, g_{2r}$.

Proof

This is a direct corollary of Theorem 2.19. □

Observation 3.11 *Let us consider the ring $A_1 \oplus A_2$, if I_1 is a primary ideal of A_1, then $I_1 \oplus A_2$ is a primary ideal of $A_1 \oplus A_2$: in fact, let us suppose that $(x_1 y_1, x_2 y_2) \in I_1 \oplus A_2$, but $(x_1, x_2) \notin I_1 \oplus A_2$, i.e. we must have that $x_1 \notin I_1$, using the fact that I_1 is a primary ideal, by definition, we get that $y_1 \in \sqrt{I_1}$, on the other hand $y_2 \in \sqrt{A_2} = A_2$, then we have the thesis.*

Using Proposition 3.7, Proposition 3.8 and Theorem 3.10, we get the following result.

Theorem 3.12 *Let (f_1, f_2) be a non-zero element in $B[x]$, with both components non-zero, then there exist $k_1, k_2 \in \mathbb{N}$, $0 \leq k_i < h_i$, $i = 1, 2$, two units $u_1 \in B_1[x]$ and $u_2 \in B_2[x]$, two sets of pairwise coprime, primary, monic* *polynomials* $\{g_{11}, \ldots, g_{1s}\} \subset B_1[x]$ *and* $\{g_{21}, \ldots, g_{2r}\} \subset B_2[x]$*, where for each* $i = 1, 2, \ldots s$*, for each* $j = 1, 2, \ldots r$*,* $\mu_1(g_{1i}) \in K_1[x]$ *and* $\mu_2(g_{2j}) \in K_2[x]$ *are powers of monic irreducible polynomials, such that*

$$(f_1, f_2) = (t_1^{k_1}, t_2^{k_2})(u_1, u_2)(g_{11}, 1) \cdots (g_{1s}, 1)(1, g_{21}) \cdots (1, g_{2r}).$$

Proof

As f_1, f_2 are non-zero elements, using Proposition 3.7, there are $k_1, k_2 \in \mathbb{N}$, two regular elements, g_1, g_2, such that $(f_1, f_2) = (t_1^{k_1}, t_2^{k_2})(g_1, g_2)$, where k_1, k_2 are uniquely determined, and g_1, g_2 are unique modulo, respectively, $(t_1)^{h_1-k_1}B_1[x]$ and $(t_2)^{h_2-k_2}B_2[x]$. Then, using Proposition 3.8, we have that there are two units $u_1 \in B_1[x], u_2 \in B_2[x]$ and two monic polynomials $d_1 \in B_1[x], d_2 \in B_2[x]$, such that (g_1, g_2) is uniquely representable as $(u_1, u_2)(d_1, d_2)$. Finally, we can use Theorem 3.10 to factor the element (d_1, d_2) into the product of the elements $(g_{11}, 1), \ldots (g_{1s}, 1), (1, g_{21}), \ldots (1, g_{2r})$. We notice that the couples of monic, primary polynomials that we are considering are uniquely determinated when g_1, g_2 are given, because the elements $g_{11} \ldots g_{1s},$, and $g_{21}, \ldots g_{1r}$ are uniquely determined.

Moreover, we notice that, by Observation 3.11, the $r + s$ factors, $(g_{1s}, 1)$, $(1, g_{21}), \ldots,$ $(1, g_{2r})$ are primary. □

3.3.2 Factorization of a non-zero element in $B[x]$, where B is an Artinian PIR.

We want to extend the results that we have found out in the above subsection to the general case using an induction proof.

We have already proved that $B[x] \cong B_1[x] \oplus \cdots \oplus B_n[x]$, where $B_1, \ldots B_n$ are SPIR's. As we have done in the last subsection, for each $i = 1, \ldots n$, let (t_i) be the only maximal ideal of B_1 and $h_i \in \mathbb{N}$ be its nilpotency. Then, let us consider the field $K_i = B_i/(t_i)$ and let $\mu_i : B_i[x] \to K_i[x]$ be the natural extension of the canonical projection; let $v_i : B_i[x] \to \mathbb{N}_{h_i}$ be the t_i-valuation. As we have done for the case of the product of only two SPIR's, we can easily prove the following results.

Proposition 3.13 *Let $(f_1, \dots, f_n) \in B[x]$ be an element, such that $f_i \neq 0$ for each $i = 1, \dots, n$, then there exist n regular elements, $g_i \in B_i[x]$, $i = 1, \dots n$, and $k_i \in \mathbb{N}$, with $0 \leq k_i < h_i$, $i = 1, \dots n$, such that*

$$(f_1, \dots, f_n) = (t_1^{h_1} g_1, \dots, t_n^{h_n} g_n) = (t_1^{h_1}, \dots, t_n^{k_n})(g_1, \dots, g_n).$$

Moreover, we have that k_i, $i = 1, \dots n$, is uniquely determined and that g_i is unique modulo $(t_i)^{h_i - k_i} B_i[x]$, $i = 1, \dots n$.

Proof

The proof is just the same as the one of Proposition 3.7. □

Proposition 3.14 *Let us consider $(g_1, \dots, g_n) \in B[x]$, where $g_1, \dots, g_n$ are regular. Then, it can be written uniquely in the following way*

$$(g_1, \dots, g_n) = (u_1, \dots u_n)(d_1, \dots, d_n),$$

where $u_i \in B_i[x]$ is a unit and $d_i \in B_i[x]$ is a monic polynomial such that $deg(d_i) = deg(\mu_i(g_i))$ for each $i = 1, \dots, n$.

Finally, we get the main result.

Observation 3.15 *In a ring A that is direct product of n rings, $A_1, \dots A_n$, if I_1 is a primary ideal of A_1, then $I_1 \oplus A_2 \oplus \cdots \oplus A_n$ is a primary ideal of A. The proof is just the same as the proof given in Observation 3.11.*

Theorem 3.16 *Let $(f_1, \dots, f_n)$ be a element in $B[x]$, such that $f_i \neq 0$ for each $i = 1, \dots, n$, then there exist $k_1, \dots k_n \in \mathbb{N}$, $0 \leq k_i < h_i$, $i = 1, \dots n$, n units $u_i \in B_i[x]$, $r_1, \dots r_n \in \mathbb{N}$, n sets of pairwise coprime, primary, monic polynomials $\{g_{i1}, \dots, g_{ir_1}\} \subset B_i[x]$, where for each $j = 1, 2, \dots r_i$, $\mu_i(g_{ij}) \in K_i[x]$ is a power of a monic irreducible polynomial, such that*

$$\begin{aligned}&(f_1, \dots, f_n) = (t_1^{k_1}, \dots, t_n^{k_n})(u_1, \dots, u_n)(g_{11}, 1, \dots 1)(g_{1r_1}, 1, \dots 1) \cdots \\ &\cdots (1, g_{21} \dots, 1) \cdots (1, g_{2r_2} \dots, 1) \cdots (1, 1, \dots g_{n1}) \cdots (1, 1, \dots, g_{nr_n}).\end{aligned}$$

Proof

For each component, f_i, we use is sequence Proposition 3.7, Proposition 3.8 and Theorem 3.10, to obtain that there exist a unit $u_i \in B_i[x]$, an integer $k_i \in \mathbb{N}$, and a set of pairwise coprime, primary, monic polynomials $\{g_{i1}, \dots, g_{ir_i}\}$, such that $f_i = t_i^{k_i} u_i g_{i1} \cdots g_{ir_i}$, where $\mu_i(g_{ij}) \in K_i[x]$ is a monic irreducible polynomial, for each $j = 1, \dots r_i$.

Then, we can factor $(f_1, f_2 \dots, f_n)$ in the following way:

$$\begin{aligned}&(f_1, f_2 \dots, f_n) = (t_1^{k_1}, t_2^{k_2}, \dots, t_n^{k_n})(u_1, u_2 \dots, u_n) \cdot \\ &\cdot (g_{11} \cdots g_{1r_1}, g_{21} \cdots g_{2r_2}, \dots, g_{n1} \cdots g_{nr_n});\end{aligned}$$

so we have factored the element $(f_1, \dots, f_n)$ in the product of $(t_1^{k_1}, \dots t_n^{k_n})$, of a unit $(u_1, \dots, u_n)$, and, by Observation 3.15, of $r_1 + r_2 + \cdots + r_n$ primary elements; we also notice that the integers $k_1, \dots k_n$ are uniquely determined, the units u_i is uniquely determined modulo $(t_i)^{h_i - k_i} B_i[x]$, and also the elements $g_{i1} \dots, g_{ir_i}$ are uniquely determined modulo $(t_i)^{h_i - k_i} B_i[x]$. □

4 Factorization in $B[x]$, where B is a F-UFR

We are now considering the problem of factoring a non-zero element in the polynomial ring, $B[x]$, where B is a F-UFR. To do this, we need first to remind some results about F-UFR's and F-irreducible elements and to announce some classical theorems about UFD's.

Theorem 4.1 (Characterization of F-UFR's) *Every F-UFR is a finite direct sum of UFD's and of SPIR's.*

Then, if B is a F-UFR, there exist a finite number, say n_1, of UFD's, $U_1, U_2, \dots, U_{n_1}$, and a finite number n_2 of SPIR's, $S_1, S_2, \dots, S_{n_2}$, such that

$$B = U_1 \oplus U_2 \oplus \cdots U_{n_1} \oplus S_1 \oplus S_2 \oplus \cdots S_{n_2}.$$

Moreover, using Theorem 3.5, we get the following useful information

$$B[x] = U_1[x] \oplus U_2[x] \oplus \cdots U_{n_1}[x] \oplus S_1[x] \oplus S_2[x] \oplus \cdots S_{n_2}[x].$$

Now, we make use of the results gained in the second chapter of this work and of one of the Gauss'results about UFD's to get some information about factorization in $B[x]$.

Theorem 4.2 (Gauss' Lemma) *Let R be an UFD, then $R[x]$ is a UFD.*

At first let us study a simplier case, the factorization in a F-UFR, that is a direct product of precisely an UFD, U, and of a SPIR, S. Then ,we are going to examine the way in which an element in $U[x] \oplus S[x]$, whose components are both non-zero, can be factored.
Let (z) be the maximal ideal of S, and let h be its nilpotency.
Let us consider $(f, g) \in U[x] \oplus S[x]$, with f, g non-zero and non-unit elements.

Since U is an UFD and because of the Gauss' Lemma, there are a finite number, say n, of irreducible elements in $U[x]$, $r_1, r_2, \ldots, r_n$, such that

$$f = r_1 r_2 \cdots r_n, \tag{12}$$

and this factorization is unique, up to associate ones.
Then, we apply the main theorem about the polynomial rings over a SPIR. In order to make the argument clearer, we announce it again.

Theorem 4.3 *(see Prop. 2.20) Each non-zero polynomial f in $A[x]$, where A is a SPIR and (t) is its maximal ideal, is representable as*

$$f = t^k u f_1 f_2 \cdots f_r,$$

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, 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 $f_1, f_2, \ldots, f_r$ are unique modulo $t^{h-k}A[x]$.

Where K denotes the field $A/(t)$, and $\mu : A[x] \to K[x]$ is the natural extension of the canonical projection.

So, if we take the non-zero element $g \in S[x]$, we can surely find a number $0 \leq k < h$, a unit $u \in S[x]$, and m monic primary polynomials, $g_1, \ldots, g_m$, such that their projections in $S/(z)[x]$ are powers of irreducible, pairwise distinct polynomials, such that

$$g = z^k u g_1 g_2 \cdots g_m \tag{13}$$

Using the equalities (12) and (13), we get the following result,

$$(f, g) = (1_U, z^k)(1_U, u)(r_1, 1_S) \cdots (r_n, 1_S) \cdot (1_U, g_1) \cdots (1_U, g_m) \tag{14}$$

We, now, wonder which is the nature of the factors in the previous equation.

- $(1_U, z^k)$ is a zero-divisors, if $k > 0$, since $(1_U, z^k)(0, z^{h-k}) = (0, 0)$, but not a unit, since z^k is not a unit in $S[x]$.
- The element $(1_U, u)$ is of course a unit, because both components are units.
- The elements, $(r_i, 1_S)$, for $i = 1, \dots, n$, are F-irreducible elements, since, as we have seen in Proposition 1.80, in a direct product of two rings, an element (a, b) is an F-irreducible element if and only if a is F-irreducible and b is a unit, or vice versa, and, we notice, in a UFD, the concept of irreducible element and of F-irreducible element are just the same.
- The elements $(1_U, g_j)$, $j = 1, \dots, m$, are primary, because of Observation 3.11.

Naturally, a question arises:
what about the uniqueness features of the equation (14)?

We can certainly say that $k \in \mathbb{N}$ is unique and that u is unique modulo $z^{h-k}S[x]$. Since $U[x]$ is an UFD, the factorization $(r_1, 1_S) \cdots (r_n, 1_S)$ is unique, up to associate ones. More precisely, we mean that, if there are two such factorizations,

$$(r_1, 1_S) \cdots (r_n, 1_S) = (s_1, 1_S) \cdots (s_{n'}, 1_S),$$

we must have that $n = n'$ and, after a suitable reordering of the factors, $(r_i, 1_S)$ and $(s_i, 1_S)$ are associates.
Moreover, using Theorem 2.20, we have that the product $g_1 \cdots g_m$ is unique modulo $z^{h-k}S[x]$, and, after the choise of a representant in the equivalence class, the elements $g_1, \dots, g_m$, and, then, also, the elements $(1_U, g_1), \dots, (1_U, g_m)$ are uniquely determined.

The above argument is the proof of the following theorem.

Theorem 4.4 *Let U be an UFD and S be a SPIR, and let $(f, g) \in U[x] \oplus S[x]$ be an element, whose components are non-zero and non-units. Then, there exist a integer $0 \leq k < h$, a unit $u \in S[x]$, n irreducible elements in $U[x]$, $r_1, \ldots, r_n$, m primary monic polynomials in $S[x]$, $g_1, \ldots, g_m$, such that*

$$(f, g) = (1_U, z^k)(1_U, u)(r_1, 1_S) \cdots (r_n, 1_S) \cdot (1_U, g_1) \cdots (1_U, g_m),$$

where $(1_U, u)$ is a unit, $(r_i, 1_S)$ is F-irreducible $\forall$ i, $(1_U, g_j)$ is primary $\forall$ j, in $U[x] \oplus S[x]$.

Moreover, k is uniquely determined, while u is unique modulo $(z)^{h-k}S[x]$, $r_1, \ldots, r_n$ are uniquely determined up to associates, the product $g_1 \cdots g_m$ is unique modulo $(z)^{h-k}S[x]$, and the elements $(1_U, g_1), \ldots, (1_U, g_m)$ are uniquely determined modulo $U \oplus (z)^{h-k}S[x]$.

The next aim is to study the general case. Before starting it, we have to make the following observation.

Observation 4.5 *Let us suppose that U_1, U_2 are UFD's, and let us consider their product. If we take $(a, b) \in U_1 \oplus U_2$, where a, b are both non-zero and non-units, there are $r_1, \ldots, r_n \in U_1$ and $s_1, \ldots s_m \in U_2$, irreducible elements, such that:*

$$(a, b) = (r_1, 1_{U_2}) \cdots (r_n, 1_{U_2}) \cdot (1_{U_1}, s_1) \cdots (1_{U_1}, s_m),$$

and this factorization is unique, up to associates.
By an induction argument, we can prove easily that this holds for the product of more than two UFD's.

Now, we prove the main result, but first we need some notations.
Let us consider the ring

$$B[x] \cong U_1[x] \oplus U_2[x] \oplus \cdots U_{n_1}[x] \oplus S_1[x] \oplus S_2[x] \oplus \cdots S_{n_2}[x],$$

where U_i is an UFD, for each i, S_j is a SPIR, for each j. We already know that every polynomial ring over an F-UFR can be written in this form. Moreover, let us suppose that $n_1, n_2 \geq 1$, since in the above observation and in the previous chapters, we have studied the factorizations in rings that are direct products of only UFD's or of only SPIR's. Let (t_i) be the only maximal ideal of S_i, for $i = 1, \ldots, n_2$, and let $h_i \in \mathbb{N}$ be its nilpotency.

Theorem 4.6 *Let $\gamma = (f_1, \ldots, f_{n_1}, g_1, \ldots, g_{n_2})$ be an element of this ring, whose components are all non-zero and non-units. Then, there is a zerodivisor, z, a unit u, a finite set of primary distinct elements, $\{p_1, \ldots, p_\beta\}$, a finite set of irreducible elements, $\{q_1, \ldots, q_\alpha\}$, such that*

$$\gamma = z \cdot u \cdot (p_1 \cdots p_\beta) \cdot (q_1 \cdots q_\alpha).$$

Moreover, this factorization fulfills some uniqueness features that we will explain in the proof.

Proof

If we consider $f_i \in U_i[x]$, for each $i = 1, \ldots, n_1$, there is a finite set of irreducible elements, $\{r_{i1}, \ldots, r_{ia_i}\}$, such that $f_i = \prod_{j=1}^{a_i} r_{ij}$, and this factorization is unique up to associates. In the same way, if we consider g_l, for each $l = 1, \ldots, n_2$, then there is a unique integer k_l, a unit u_l, that is unique modulo $(t_l)^{h_l - k_l} S_l[x]$, a finite set of primary distinct monic polynomials, $\{s_{l1}, \ldots, s_{lb_l}\}$ that are uniquely determined modulo $(t_l)^{h_l - k_l} S_l[x]$, such that $g_l = t_l^{k_l} u_l s_{l1} \cdots s_{lb_l}$.

Now, let us put:

- $\beta = \sum_{l=1}^{n_2} b_l$, $\alpha = \sum_{i=1}^{n_1} a_i$;
- $p_1 = (1_{U_1}, \ldots, 1_{U_{n_1}}, s_{11}, 1_{S_2}, \ldots, 1_{S_{n_2}})$, $p_2 = (1_{U_1}, \ldots, 1_{U_{n_1}}, s_{12}, 1_{S_2}, \ldots, 1_{S_{n_2}})$, and, so on, untill $p_\beta = (1_{U_1}, \ldots, 1_{U_{n_1}}, 1_{S_1}, \ldots, 1_{S_{n_2 - 1}}, s_{n_2 b_{n_2}})$;
- $q_1 = (r_{11}, 1_{U_2}, \ldots, 1_{U_{n_1}}, 1_{S_1}, \ldots, 1_{S_{n_2}})$, $q_2 = (r_{12}, 1_{U_2}, \ldots, 1_{U_{n_1}}, 1_{S_1}, \ldots, 1_{S_{n_2}})$, untill $q_\alpha = (1_{U_1}, \ldots, 1_{U_{n_1 - 1}}, r_{n_1 a_{n_1}}, 1_{S_1}, \ldots, 1_{S_{n_2}})$;

- $z = (1_{U_1}, \ldots, 1_{U_{n_1}}, t_1^{k_1}, \ldots, t_{n_2}^{k_{n_2}})$ and $u = (1_{U_1}, \ldots, 1_{U_{n_1}}, u_1, \ldots, u_{n_2})$.

We notice that p_i is a primary element, $\forall\ i = 1, \ldots, \beta$, because of the Observation 3.15, and that $p_i \neq p_j$ for each $j \neq i$.
As in UFD's an irreducible element is F-irreducible, using Proposition 1.81, we have that q_i, $\forall\ i = 1, \ldots, \alpha$, is an F-irreducible element. Actually, it is an irreducible element, since the three concepts of irreducibility, given in the first chapter, are the same in rings with only harmless zerodivisors, like the ours.
Moreover, u is clearly a unit, and z is a zerodivisor, since $zy = 0_{B[x]}$, with $y = (0_{U_1}, \ldots, 0_{U_{n_1}}, t_1^{h_1-k_1}, \ldots, t_{n_2}^{h_{n_2}-k_{n_2}})$.

Furthermore, we have already noticed that the integer k_i is uniquely determined, and that the unit u_i and the primary monic polynomials, $s_{i1}, \ldots, s_{ib_i}$, are uniquely determined modulo $(t_i^{h_i-k_i})S_i[x]$. We have also that, for each $j = 1, \ldots, n_1$, the irreducible elements, $r_{j1}, \ldots, r_{ja_j} \in U_j[x]$, are uniquely determined, up to associates.
This completes the proof. □

References

[1] A. G. Aḡargün, D. D. Anderson, S. Valdes-Leon, *Factorization in commutative rings with zerodivisors*, Rocky Mountain J. Math. 31, 2001.

[2] D.D. Anderson and R. Markanda, *Unique factorization rings with zero-divisors*, Houston J. Math 11, pp 15-30, 1985.

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

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

[5] A. Bouvier, *Structure des anneaux à factorisation unique*, Publ. Dép. Math. (Lyon) 11, pp 39-49, 1974.

[6] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11**, 1960.

[7] S. T. Chapman, J. Coykendall, *Half-factorial Domains: a survey*, Non-Noetherian Commutative Ring Theory, 2001.

[8] C.R. Fletcher, *Unique Factorization Rings*, Proc. Cambridge Philos. Soc. 65, 1969.

[9] C.R. Fletcher, *The structure of unique factorization rings*, Proc. Cambridge Philos. Soc. 67, 1970.

[10] 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.

[11] W. Fulton, *Algebraic Curves*, W.A. Benjamin, Inc., Mathematic Lecture Note Series, 1969.

[12] S. Galovich, *Unique factorization rings with zerodivisors*, Mathematical Magazines 5, pp. 276-283, 1978.

[13] E. Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen Zahlkörper*, Nachr. Akad. Wiss. Göttingen, 1917.

[14] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag New York, pp. 171-179, 1990.

[15] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, pp. 71-91, 1986.

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

[17] P. Samuel, *Unique factorization*, Amer. Math. Monthly 75, pp. 945-952, 1968.

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

[19] O. Zariski, P. Samuel, *Commutative Algebra*, D. Van Norstrand Company, 1967.