UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede amministrativa: Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

CORSO DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

CURRICOLO MATEMATICA

CICLO XXIX

Factorizations of invertible matrices into products of elementary matrices and of singular matrices into products of idempotent matrices

Coordinatore: Ch.mo Prof. Martino Bardi

Supervisore: Ch.mo Prof. Paolo Zanardo

Dottoranda: Laura Cossu

SUNTO

In questa tesi si considerano due problemi classici, originati rispettivamente da un lavoro di P. Cohn del 1966 e da uno di J.A. Erdos del 1967, inerenti la fattorizzazione di matrici quadrate a coefficienti in un arbitrario dominio di integrità: caratterizzare i domini di integrità R che soddisfano la proprietà

(GE_n), ogni matrice invertibile $n \times n$ a valori in R è prodotto di matrici elementari;

e quelli che soddisfano la proprietà

(ID_n), ogni matrice singolare $n \times n$ a valori in R è prodotto di matrici idempotenti.

Vi è una stretta correlazione tra le proprietà (GE_n) e (ID_n). Un importante risultato di Ruitenburg (1993) mostra che esse sono equivalenti nei domini di Bézout (cioè domini integrali in cui ogni ideale finitamente generato è principale). Inoltre, se R è un dominio di Bézout, allora R soddisfa (GE_n) per ogni $n \geq 2$ se e solo se vale la (GE_2), se e solo se vale la (ID_2), se e solo se verifica la (ID_n) per ogni $n \geq 2$. In questo caso è quindi sufficiente considerare le matrici di dimensione 2.

La trattazione si sviluppa attorno allo studio di due congetture, tanto naturali quanto difficili da dimostrare in generale.

La prima, proposta da Salce e Zanardo (2014) e ispirata da importanti risultati sui campi di numeri algebrici, è la seguente: "*un dominio a ideali principali R soddisfa la proprietà (GE_2) se e solo se è Euclideo*".

A supporto di tale congettura, nella tesi viene dimostrata la sua validità in due importanti classi di PID non Euclidei: (i) gli anelli delle coordinate di

speciali curve algebriche non singolari definite su un campo perfetto k, tra cui l'anello delle coordinate delle coniche prive di punti razionali su k e quello delle curve ellittiche aventi il punto all'infinito come unico punto razionale; (ii) i PID non Euclidei costruiti da D.D. Anderson in un lavoro del 1988. I casi (i) e (ii) richiedono differenti dimostrazioni, basate su delicati lemmi tecnici. Da tali risultati si evince che la congettura sembra essere verificata da tutti i PID non Euclidei apparsi in letteratura.

La seconda congettura studiata nella tesi è legata alla fattorizzazione di matrici singolari in idempotenti: "*un dominio R avente la proprietà (ID_2) deve essere necessariamente un dominio di Bézout*".

I domini a fattorizzazione unica, quelli projective-free, e i domini PRINC, introdotti da Salce e Zanardo nel 2014, soddisfano la congettura. Nella tesi si è trovato un esempio di dominio PRINC che non è né UFD né projective-free. Si è inoltre provato che se un dominio R soddisfa la proprietà (ID_2), allora R è un dominio di Prüfer (i.e. gli ideali finitamente generati sono invertibili); la seconda congettura può essere quindi studiata limitandosi alla classe dei domini di Prüfer. Si è dimostrato che se un qualunque dominino di integrità R verifica la proprietà (ID_2), allora verifica anche la (GE_2). Utilizzando tale risultato e applicando opportunamente differenti risultati di Cohn (1966), a sostegno della congettura si è trovata una classe di anelli coordinati di curve non singolari che sono domini di Dedekind non PID che non soddisfano la proprietà (ID_2); si è inoltre provato che neanche l'anello $\mathrm{Int}(\mathbb{Z})$ dei polinomi a valori interi verifica tale proprietà.

ABSTRACT

In this thesis we consider two classical problems, originated respectively by a 1966 paper by P. Cohn and by a 1967 one by J.A. Erdos, concerning the factorization of square matrices with entries in an arbitrary domain: we want to characterize integral domains R satisfying property

(GE_n), every $n \times n$ invertible matrix over R is a product of elementary matrices;

and those satisfying property

(ID_n), every $n \times n$ singular matrix over R is a product of idempotent matrices.

There is a deep relationship between properties (GE_n) and (ID_n). An important result by Ruitenburg (1993) shows that they are equivalent for Bézout domains (i.e. integral domains whose finitely generated ideals are principal). Moreover, if R is a Bézout domain, then R satisfies (GE_n) for any $n \geq 2$ if and only if it satisfies (GE_2) if and only if it satisfies (ID_2) if and only if it satisfies (ID_n) for any $n \geq 2$. Thus, in this case, it is enough to consider matrices of dimension 2.

The thesis investigates two conjectures, as natural as hard to prove in general.

The first one, due to Salce and Zanardo (2014) and suggested by important results on number fields, is the following: "*a principal ideal domain R satisfies the property (ID_2) if and only if it is Euclidean*".

In support of this conjecture, in this thesis we prove that it is valid in two important classes of non-Euclidean PID's: (i) the coordinate rings of special

non-singular algebraic curves defined over a perfect field k, among them the coordinate rings of conics without k-rational points and the coordinate rings of elliptic curves having the point at infinity as unique k-rational point; (ii) the class of non-Euclidean PID's constructed by D.D. Anderson in a 1988 paper. The cases (i) and (ii) require different proofs, based on delicate technical lemmas. From these results we get that the conjecture seems to be verified by every non-Euclidean PID appeared in the literature.

The second conjecture studied in this thesis is related to the factorization of singular matrices into idempotent ones: "*an integral domain R verifying (GE_2) must be a Bézout domain*".

Unique factorization domains, projective-free domains and PRINC domains, introduced by Salce and Zanardo in 2014, satisfy the conjecture. In the thesis we exhibit an example of PRINC domain which is neither UFD nor projective-free. We also prove that if an integral domain R satisfies the property (ID_2), then it is a Prüfer domain (i.e. finitely generated ideals of R are invertible); thus in order to study the second conjecture we can confine ourselves to the class of Prüfer domains. Moreover, we show that if any integral domain R satisfies property (ID_2), then it satisfies also property (GE_2). Using this result and properly applying some results by Cohn (1996), in support of the conjecture we find a class of coordinate rings of smooth algebraic curves that are not PID's and that do not satisfy property (ID_2); moreover we prove that also the ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials does not verify this property.

ACKNOWLEDGMENTS

I would like to express my deep gratitude to my supervisor, Professor Paolo Zanardo, for guiding me during these years with so much dedication and professionalism. His constant support and his advices have been very important to me.

I thank Professor Umberto Zannier (Scuola Normale Superiore) for his proof of Theorem 2.1.4 and some related examples.

I also wish to thank all the professors, the Ph.D students and the staff of the *Dipartimento di Matematica "Tullio Levi-Civita" dell'Università degli Studi di Padova* for creating a really nice and stimulating research environment.

A special thanks goes also to my family, to my boyfriend Luigi and to all my friends for their constant support and love.

INTRODUCTION

The main motivation for this thesis comes from two classical problems concerning the factorization of square matrices over an integral domain R.

The first problem is to characterize integral domains R that satisfy the property

(GE_n): Every $n \times n$ *invertible* matrix over R can be written as a product of *elementary* matrices.

The second problem, somehow symmetric to the previous one, is to characterize integral domains R satisfying the property

(ID_n): Every $n \times n$ *singular* matrix over R can be written as a product of *idempotent* matrices.

The main impulse to investigate integral domains satisfying (GE_n), for all $n > 0$, was given by the fundamental 1966 paper by Cohn [15], who called these domains *generalized Euclidean* (GE-rings, for short), due to the fact that Euclidean domains provide the second instance, after the fields, of rings satisfying (GE_n), for all $n > 0$. When R is a field, Gauss Elimination produces a factorization into elementary matrices of any invertible matrix with entries in R. One of Cohn's main achievements in paper [15] was the proof that the rings of integers of imaginary quadratic number fields that are not Euclidean are not even generalized Euclidean. Thus, among the rings of algebraic integers of $\mathbb{Q}(\sqrt{-d})$, with $d > 0$, those with $d = 19, 43, 67, 163$ are examples of PID's that fail to be generalized Euclidean.

In the same year, 1966, Howie proved in [32] that every transformation of a finite set that is not a permutation can be written as a composition of

idempotents. Generalizing Howie's result to linear maps of a finite dimensional vector space, in 1967 Erdos [20] proved that every singular matrix with entries in a field is a product of idempotent matrices, thus initiating the research on the second problem.

An alternative proof and a slight refinement of Erdos'result may be found in Dawlings [19], where it is shown that any singular linear endomorphism of an n-dimensional vector space is a product of *at most* n idempotent linear maps of rank $n-1$. Other further generalizations of the above results to self-maps of infinite sets and to linear endomorphisms over any vector space can be found respectively in [33] and [50].

In 1983 [38], Laffey showed that also Euclidean domains satisfy (ID_n), for all $n > 0$. A crucial argument of his proof was a reduction, obtained by induction, from any dimension $n > 0$ to dimension 2.

Laffey's reduction argument was immediately adapted by Bhaskara Rao (cf. [5]) to principal ideal domains, and by Salce and Zanardo (cf. [53]) to Bézout domains, i.e. integral domains in which every finitely generated ideal is principal. It follows that *every* 2×2 *singular matrix with entries in a Bézout domain is a product of idempotent matrices if and only if every* $n \times n$ *singular matrix with entries in the same domain is a product of idempotent matrices, for any positive integer* n. Therefore, to study property (ID_n) in a Bézout domain R, it is enough to consider 2×2 matrices.

We recall that an analogous result holds also for the property (GE_n). By Kaplansky's Theorem 7.1 in [34], *if* R *is a Bézout domain, every* 2×2 *invertible matrix over* R *is a product of elementary matrices if and only if every* $n \times n$ *invertible matrix over* R *is product of elementary matrices, for any positive integer* n.

The property (ID_n) was studied in the class of principal ideal domains by John Fountain in the 1991 paper [22]. Extending the results by Erdos and Dawlings, Fountain introduced some properties equivalent to (ID_n) in PID's, by proving the following theorem, slightly rephrased as in [53]:

Theorem 0.0.1 (Fountain [22])**.** *Let* R *be a principal ideal domain and* $n \geq 2$ *an integer. The following properties are equivalent to the property* (ID_n)*:*

(H_n) *For any endomorphism* α *of* R^n *of rank* $n-1$*, there exists an endomorphism* β *with* $Ker(\beta) = Ker(\alpha)$ *and* $Im(\beta) = Im(\alpha)^*$*, such that* β *is a product of idempotent endomorphisms of rank* $n-1$*.*

(SC_n) *For any pair of pure submodules* A, B *of the free* R*-module* R^n*, of ranks* $n-1$ *and* 1 *respectively, and such that* $A \cap B = 0$*, there is a sequence of direct decompositions of* R^n*, with* $A = A_1$ *and* $B = B_k$*:*

$$R^n = A_1 \oplus B_1 = A_2 \oplus B_1 = A_2 \oplus B_2 = \cdots = A_k \oplus B_{k-1} = A_k \oplus B_k.$$

In condition (H_n), $\mathrm{Im}(\alpha)^*$ denotes the pure closure of the submodule $\mathrm{Im}(\alpha)$ in R^n. The proof of Fountain's theorem makes use of the fact that, if R is a PID, then $M_n(R)$ has the structure of abundant semigroup.

Using the new characterizations in Theorem 0.0.1, he proved that discrete valuation rings and the ring of integers $\mathbb{Z}$ satisfy property (ID_n) for all $n > 0$.

As observed by Fountain in Section 1 of [22], O'Meara [47] and Hannah and O'Meara [29] characterized the products of idempotents in some classes of (von Neumann) regular rings, getting some results yielding those of Erdos, Dawlings, Reynolds and Sullivan as special cases. However, their techniques could not be applied to the case of principal ideal domains since, when R is a PID, $M_n(R)$ is not a regular ring.

In 1993, Ruitnburg extended in [52] Fountain's result to Bézout domains. The main theorem of Ruitemburg's paper is a crucial result for our investigation. In fact it shows a deep relationship between the two problems we are considering, by establishing a connection of the three properties in Theorem 0.0.1 with the property (GE_n).

Theorem 0.0.2 (Ruitenburg [52])**.** *For a Bézout domain R the following conditions are equivalent:*

(i) for any assigned integer $n \geq 2$, (ID_m) holds for every $m \leq n$;

(ii) for any assigned integer $n \geq 2$, (H_m) holds for every $m \leq n$;

(iii) for any assigned integer $n \geq 2$, (SC_m) holds for every $m \leq n$;

(iv) (GE_n) holds for every integer $n > 0$.

Therefore, a Bézout domain R satisfies property (ID_n) for all $n > 0$ if and only if it satisfies property (GE_n) for all $n > 0$. Moreover, by the generalization to Bézout domains of Laffey's reduction argument (cf. [53, Prop. 2.4]) and by Kaplansky's theorem [34, Th. 7.1], in order to investigate these properties it is enough to consider the case $n = 2$.

It is worth noting that the equivalence in Ruitenburg's theorem is no longer valid outside the class of Bézout domains. Cohn proved in [15] that local domains always satisfy property (GE_2) and Salce and Zanardo proved in [53] that local domains satisfy property (ID_2) if and only if they are also valuation domains; thus, local domains that are not valuation domains (or equivalently that are not Bézout domains), like for instance the ring $R = k[\![X, Y]\!]$ of power series in two indeterminates over a field k, satisfy (GE_2) but not (ID_2).

Ruitenburg's theorem was extended in [53] by the introduction of two new conditions, (HF_n) and (SFC_n), that generalize (H_n) and (SC_n) to a general domain R:

(HF_n) For any free direct summand A, B of the free R-module R^n, of ranks r and $n-r$ respectively ($1 \leq r \leq n$), there exists an endomorphism β of R^n with $\mathrm{Ker}(\beta) = B$ and $\mathrm{Im}(\beta) = A$, that is a product of idempotent endomorphisms of rank r.

(SFC_n) For any free direct summand A, B of the free R-module R^n, of ranks r and $n-r$ respectively ($1 \leq r \leq n$), there exist direct decompositions of R^n:

$$R^n = A_1 \oplus B_1 = A_2 \oplus B_1 = A_2 \oplus B_2 = \cdots = A_k \oplus B_{k-1} = A_k \oplus B_k,$$

with $A = A_1$ and $B = B_k$.

In [53, Th.3.4] the authors proved the equivalence over any domain R of properties (GE_n), (HF_n) and (SFC_n), for all $n > 0$. However, since for Bézout domains the property (HF_n) coincides with (H_n) and the property (SFC_n) with (SC_n), the generalization of Ruitenburg's theorem leads to the main achievement of the original result, that is the equivalence of (GE_n) and (ID_n) over Bézout domains.

The study of factorizations of square invertible and singular matrices over an integral domain R into elementary and idempotent factors respectively, is related to the generalizations of the notion of Euclidean domain.

In the paper [16], G. Cooke generalized the notion of Euclidean domain, and applied it to the rings of integers in quadratic number fields in [17]. Several papers have followed his research, see, e.g., [41], [12], [27] and [28].

Following [53], we say that an integral domain R *admits a weak (Euclidean) algorithm*, if for any $a, b \in R$ there exists a (finite) sequence of divisions that starts with a, b and ends with last remainder zero. We refer to Chapter 1 for the precise definitions. Such an R is necessarily a Bézout domain. A non-discrete valuation domain is a typical example of a non-Euclidean domain that admits a weak algorithm.

A nice connection between domains with a weak algorithm and property (GE_n) was found by O'Meara in his 1965 paper [48]. In fact, in [48, Th.14.3], he proved that a PID admits a weak algorithm if and only if it satisfies (GE_2) (hence, equivalently, it satisfies (GE_n) and (ID_n), for every $n > 0$, by Kaplansky's result, Ruitenburg's theorem and Laffey's reduction argument). It was observed by Salce and Zanardo in [53] that O'Meara's proof extends *verbatim* to Bézout domains.

However, somehow surprisingly, an example of a non-Euclidean PID that does satisfy (GE_2) was not found up to now. In view of O'Meara's result, the problem to find such an example is equivalent to find a non-Euclidean PID that admits a weak algorithm.

It is worth noting that there is no hope to find such example in the natural environment of the rings of integers in algebraic number fields. As a matter of fact, the classical examples of non-Euclidean PID's, namely the special rings of integers in imaginary quadratic number fields $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67, 163$, were exhibited for the purpose of showing that not every PID satisfy (GE_2) (cf. [15]). Moreover, Weinberger [63] has proved, under the Generalized Riemann Hypothesis, that every ring of integers R which is a PID is also an Euclidean domain (not necessarily with respect to the usual norm), except in case that R is imaginary quadratic. More recently, Harper and Murty [30] proved the same result without assuming GRH, but with the additional hypothesis that the unit rank of R is greater than 3.

Note that even the example of non-Euclidean PID constructed by Bass in [4] does not satisfy property (GE_2).

Due to the above results, Salce and Zanardo [53] were led to formulate the following conjecture

> "A principal ideal domain R satisfies property (GE_n) for all $n > 0$ if and only if R is Euclidean".

In Cohn's terminology, the conjecture states that a PID R is generalized Euclidean if and only if it is Euclidean.

Actually, in what follows we will consider the conjecture in the following equivalent form

(C) "A non-Euclidean principal ideal domain R does not satisfy property (GE_n) for some $n > 0$".

Within this thesis we add consistency to the above conjecture, by showing that it is valid for two important classes of PID's that are not Euclidean.

The first class involves special smooth algebraic curves whose coordinate rings are non-Euclidean PID's. Examples of curves satisfying this requirement may be found in the literature. Indeed, in Section 6 of [56], Samuel gives some hints on how to find this kind of examples in the case of genus ≥ 1, and characterizes the case of genus zero in Proposition 19 [56]. Samuel does not provide any explicit example. In Theorem 2.1.4 we give a direct proof (due to U. Zannier) that, if E_0 is an affine elliptic curve over a field k such that the point at infinity is the unique rational point of the curve, then the coordinate ring $k[E_0]$ of E_0 is a non-Euclidean PID. In Remark 3 we observe that, under strong hypotheses, other non-Euclidean PID's may be found generalizing Theorem 2.1.4. Let us observe that Brown in [6] and [7] investigated the rings of algebraic curves that are Euclidean, hence satisfying property (GE_n) for all $n > 0$, while, in the same area of research,

Markanda [44] studied when a localization of the ring of an algebraic curve becomes an Euclidean ring. Actually, in Brown's Theorem 1.1 of [7] we can find four examples of principal ideal domains that are not Euclidean. These rings were firstly found and examined in [43] by MacRae, who, however, in his paper did not specify that they are not Euclidean. Three of them turn out to be rings of elliptic curves over finite fields, the fourth one is hyperelliptic over $\mathbb{F}_2$, hence not a smooth curve (see Remark 4 in Chapter 2).

The second class of non-Euclidean PID's consists of the rings constructed by D.D. Anderson in [1]. We refer to Theorem 2.2.2 in Chapter 2 for the details. We call *Anderson's PID* any non-Euclidean domain constructed as in [1].

In Theorems 2.3.5 and 2.3.11 we consider the coordinate rings $R = k[\mathcal{C}_0]$ of an affine smooth curve $\mathcal{C}_0$ over a field k. A series of lemmas allows us to use a result by Cohn in [15] to prove that, if $\mathcal{C}_0$ is a conic and R is a k-ring (i.e., the set of units of R coincide with k^*), then this coordinate ring does not satisfy property (GE_2). As a corollary, when $\mathcal{C}_0$ is a conic, we show that its coordinate ring R is a non-Euclidean PID if and only if $\mathcal{C}_0$ has no rational points, if and only if R does not satisfy (ID_2), i.e., there exist 2×2 singular matrices with entries in R that do not factorize as products of idempotent matrices. The first equivalence was essentially proved in Proposition 19 of Samuel's paper [56]; see Corollary 2.1.2. When $\mathcal{C}_0$ has a unique point at infinity, the condition for R to be a k-ring is automatic, and we do not even need to assume that the curve is plane. Under this simple hypotesis, we prove that $R = k[\mathcal{C}_0]$ does not satisfy property (ID_2). Finally, in Remark 4 we show that the four examples of PID's found by MacRae in [43], and reconsidered by Brown [7], do not satisfy (ID_2). Actually, only the example with the hyperelliptic curve needs examination, since it involves a curve with a singular point; we just observe that our techniques may be adapted also to this special case.

In Theorem 2.3.17 we prove that also any Anderson's PID does not satisfy property (ID_2). Then, by O'Meara's Theorem 14.3 of [48] and Ruitenburg's Theorem in [52], both classes of rings do not satisfy (GE_2), and the conjecture holds. It is worth noting that the case of an Anderson's PID is harder to establish than that of the coordinate ring of a smooth affine curve.

We point out that the classical examples of non-Euclidean PID's in number fields, Bass'example and the two classes mentioned above seem to be the only examples of non-Euclidean principal ideal domains that may be found in the literature. Thus, from the results above it follows that the conjecture **(C)** is verified for all non-Euclidean PID's appeared in the literature up to now.

As recalled above, fields, Euclidean domains, DVR's and the ring of integers $\mathbb{Z}$ satisfy property (ID_n) for all $n > 0$; moreover, the results in [5, 38, 52] characterize the property of factorization into idempotent matrices of singular matrices with entries in a Bézout domain.

These results suggested to Salce and Zanardo another natural conjecture proposed in [53]:

(D) "If an integral domain R satisfies property (ID_2), then it should be a Bézout domain".

While working on adding likelihood to this conjecture, the authors of [53] were led to introduce a suitable property of a domain R, called (princ).

We will say that an integral domain R satisfies the property (princ) if every ideal generated by two nonzero elements $a, b \in R$ that form an *idempotent pair*, i.e. such that either $a(1-a) \in bR$ or $b(1-b) \in aR$, is principal. In this case we will say that R is a PRINC domain. Unique factorization domains and projective-free domains (in particular local domains) are examples of PRINC domains.

In Theorem 3.1.5 we give a direct proof that if D is a PRINC domain, Q is its fraction field and X is an indeterminate, then also $R = D + XQ[\![X]\!]$ is a PRINC domain. Therefore, PRINC domains can be easily produced via pullbacks. This result allows us to provide an example of PRINC domain that is neither factorial nor projective free: $R = D + XQ[\![X]\!]$, where $D = \mathbb{R}[X, Y, Z]/\langle X^2 + Y^2 + Z^2 - 1\rangle$ is the real coordinate ring of the 2-dimensional sphere. Another example of this kind of domain, much more complicate, can be found in [45, Remark p.189].

The main result of [53] on PRINC domains is that a PRINC domain satisfying (ID_2) must be a Bézout domain, thus PRINC domains satisfy the conjecture **(D)**. The fact that local domains that are not valuation domains do not satisfy (ID_2) is a consequence of this fact.

After their introduction in [53], the study of PRINC domains has been continued in [49]. In this paper it is proved, among the other results, that a Dedekind domain is a PRINC domain if and only if it is a PID. In view of this fact it is natural to ask if any Prüfer domain that satisfies (princ) is also a Bézout domain. We note that the answer is positive for Prüfer domains of finite character (cf. [49, Cor. 1.7]) and for Prüfer domains that are also CFD's (cf. [45, Cor. 1.9]). While investigating this question, we considered an interesting family of Prüfer domains, that we called Prüfer - Schülting domains, since they were first introduced by Schülting in his 1979 paper [57], in which he provided the first example of Prüfer domain having a 3-generated ideal. In Section 3.2, following the notations in [21], we define this class of

domains and we recall their principal properties. Moreover, we prove that a particular subfamily of Schülting domains has an ideal generated by an idempotent pair that cannot be principal (see Theorem 3.2.6 and Corollary 3.2.7). These domains are then Prüfer domains that are neither Bézout nor PRINC domains and this result gives a further hint that a PRINC Prüfer domain must be Bézout.

As recalled above, whenever a UFD, a projective-free domain or a PRINC domain satisfies property (ID_2), then it is also a Bézout domain. Thus, these three classes of domains verify **(D)**. Part of this thesis is dedicated to adding consistency to this conjecture.

Our main result in this direction is Corollary 4.1.2, where we prove that if an integral domain R satisfies property (ID_2), then R is a Prüfer domain. This can be obtained as a direct consequence of Proposition 4.1.1: if every matrix of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b two nonzero elements of an integral domain R is a product of idempotent matrices, then the ideal $\langle a, b \rangle$ is invertible.

It follows that, when dealing with conjecture **(D)**, we can restrict our attention to Prüfer domains. Moreover, in view of this result, we can give an equivalent formulation of conjecture **(D)**:

(D') "If R is a Prüfer domain that is not a Bézout domain, then it does not satisfy property (ID_2)".

We also find a new relation between properties (ID_2) and (GE_2) over any integral domain R. Namely, in Corollary 4.2.4 we prove that if any singular 2×2 matrix over any integral domain R is a product of idempotent matrices, then every invertible 2×2 matrix over R is a product of elementary matrices.

In this environment, we find a large class of algebraic plane non-singular curves whose coordinate rings satisfy **(D')**. Applying in a suitable way the same result by Cohn used to prove Theorem 2.3.5, in Theorem 4.2.7 we prove that the coordinate ring R of an affine plane curve $\mathcal{C}_0$ over a field k, with degree ≥ 2 and all the points at infinity conjugate by elements of the Galois group $G_{\bar{k}/k}$, does not satisfy property (GE_2). Then, as an immediate consequence we get that if R is a PID, then R is a non-Euclidean PID satisfying the conjecture **(C)**, if it is not a PID, then it is a Dedekind domain (so also a Prüfer domain) for which the conjecture **(D')** is verified.

Properly applying some results by Cohn on discretely ordered rings (cf. [15, Section 8]), in Theorem 4.2.16 and in its Corollary, we also prove that the ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials, one of the most known examples of Prüfer domain that is not Bézout , verifies the conjecture **(D')** by showing that it does not satisfy property (ID_2).

This thesis is organized as follows. In Chapter 1 we fix the notation and recall some preliminary results. In Chapter 2 we focus on the conjecture **(C)**. In particular, we present the two classes of non-Euclidean PID's metioned above, i.e. the coordinate rings $k[\mathcal{C}_0]$ of special affine smooth curves $\mathcal{C}_0$ over a perfect field k and the family of Anderson's PID's, and we prove that they verify the conjecture. Chapter 3 is dedicated to PRINC domains. We recall there the main results of [53] and [49] on this topic. Moreover, as an answer (or a partial answer) to some open questions raised in these two papers, we give an example of a PRINC domain which is non-UFD and non-projective-free and of a Prüfer domain non-Bézout and non-PRINC. We also analyze the deep relationship, observed in [49], between the notion of PRINC domain and the notion of UCFD, unique comaximal factorization domain, introduced in [45]. In Chapter 4 we discuss our results in support of the second conjecture considered in this thesis, the conjecture **(D)**. We prove that every integral domain satisfying (ID_2) must be a Prüfer domain and that it must satisfy property (GE_2). Moreover, we give the equivalent formulation **(D')** of **(D)** and we show that the coordinate rings of a wide class of curves and the ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials verify **(D')**.

The results contained in Chapter 2 are part of an article recently submitted for the publication, [18].

CONTENTS

CHAPTER 1

PRELIMINARIES

In this chapter we fix the notation and introduce some preliminary results that will be used in the sequel.

In what follows every ring considered will be a commutative integral domain. We will use the standard symbols PID to denote a principal ideal domain, and UFD to denote a unique factorization domain. For any assigned ring A we will denote by A^* its multiplicative group of units. An integral domain R will be called local if it contains a unique maximal ideal, we do not require noetherianity in the definition. Recall that R is said to be a Bézout domain if every finitely generated ideal of R is principal, a Prüfer domain if every finitely generated ideal of R is invertible and a Dedekind domain if every fractional ideal of R is invertible.

For unexplained notions and results in commutative ring theory we refer to Kaplansky's book [36].

1.1 Matrices over an integral domain

As usual, we will denote the R-algebra of the $n \times n$ matrices with entries in R by $M_n(R)$. A matrix $\mathbf{M} \in M_n(R)$ is said to be *singular* if $\det(\mathbf{M}) = 0$; it is said to be *invertible* if $\det(\mathbf{M}) \in R^*$. The *general linear group* and the *special linear group* of degree n over R, i.e. the set of all invertible matrices in $M_n(R)$ and the set of all matrices in $M_n(R)$ having determinant equal to 1, will be denoted by $GL_n(R)$ and $SL_n(R)$ respectively.

Definition 1.1.1. An *elementary matrix* is an element of $M_n(R)$ obtained by applying *elementary transformations* to the identity matrix $\mathbf{I}_n$. There

exist three different types of elementary matrices, corresponding respectively to three different types of elementary row transformations (or equivalently, column transformations):

- *transpositions* $\mathbf{P}_{ij}$, with $i \neq j$, obtained from $\mathbf{I}_n$ by exchanging row i and row j;
- *dilations* $\mathbf{D}_i(u)$, obtained from $\mathbf{I}_n$ by multiplying row i by the unit $u \in U(R)$;
- *transvections* $\mathbf{T}_{ij}(r)$, with $i \neq j$ and $r \in R$, obtained from $\mathbf{I}_n$ by adding to row i, r times row j. It turns out that $\mathbf{T}_{ij}(r)$ is nothing but the identity matrix with r in the ij position.

All these matrices are invertible since their determinants are units of R, and we have

$$\begin{aligned}\mathbf{P}_{ij}^{-1} &= \mathbf{P}_{ij},\\ \mathbf{D}_i(u)^{-1} &= \mathbf{D}_i(u^{-1}),\\ \mathbf{T}_{ij}(r)^{-1} &= \mathbf{T}_{ij}(-r).\end{aligned}$$

Moreover, for 2×2 elementary matrices, it can be easily verified by a direct computation, that the following relations we will need later hold for any $u, w \in R^*$ and for any $r \in R$:

$$\mathbf{E}(u,r) := \begin{pmatrix} 0 & u \\ -u^{-1} & r \end{pmatrix} = \mathbf{T}_{12}(u)\mathbf{T}_{21}(-u^{-1})\mathbf{T}_{12}(u(1-r)); \tag{1.1}$$

$$\mathbf{D}(w) := \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} = \mathbf{E}(u,-w^{-1})\mathbf{E}(u,-w)\mathbf{E}(u,-w^{-1}). \tag{1.2}$$

In particular, $\mathbf{E}(1,r) = \begin{pmatrix} 0 & 1 \\ -1 & r \end{pmatrix} = \mathbf{T}_{12}(1)\mathbf{T}_{21}(-1)\mathbf{T}_{12}(1-r)$, $\mathbf{D}(w) = \mathbf{E}(1,-w^{-1})\mathbf{E}(1,-w)\mathbf{E}(1,-w^{-1})$ and $\mathbf{D}(1) = \mathbf{I}_2$.

Definition 1.1.2. An *idempotent* matrix is a matrix $\mathbf{M} \in M_n(R)$ such that $\mathbf{M}^2 = \mathbf{M}$.

The following proposition provides a standard form for 2×2 non-identity idempotent matrices. We omit its straightforward proof.

Proposition 1.1.3. *Let* $\boldsymbol{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be a non-zero and non-identity* 2×2 *matrix over the integral domain* R. *Then* $\boldsymbol{M}$ *is idempotent if and only if* $d = 1 - a$ *and* $a(1-a) = bc$.

We will call $GE_n(R)$ the subgroup of $GL_n(R)$ containing all matrices that can be written as a product of elementary matrices, and we will denote as $ID_n(R)$ the set of matrices of dimension n over R that are products of non-identity idempotent matrices. Therefore, an integral domain R satisfies property (GE_n) if $GL_n(R) = GE_n(R)$, and it satisfies property (ID_n) if the subset of the singular matrices of $M_n(R)$ coincides with $ID_n(R)$.

Definition 1.1.4. A matrix $\mathbf{M} \in M_2(R)$ is called *column-row* if there exist $a, b, x, y \in R$ such that

$$\mathbf{M} = \begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} xa & xb \\ ya & yb \end{pmatrix}.$$

Proposition 1.1.5. *Let $\boldsymbol{M}$ be a singular matrix in $M_2(R)$. If the ideal generated by the elements of its first row is principal, then $\boldsymbol{M}$ is a column-row matrix.*

Proof. Let $\mathbf{M} = \begin{pmatrix} \bar{a} & \bar{b} \\ c & d \end{pmatrix}$ with $\langle \bar{a}, \bar{b} \rangle = xR$. Then there exist $a, b \in R$ such that $\bar{a} = xa$, $\bar{b} = xb$, and $\langle a, b \rangle = R$. Say $\alpha a + \beta b = 1$ for some $\alpha, \beta \in R$. Moreover, from $\bar{a}d = \bar{b}c$ we get $ad = bc$ and, therefore $c = \alpha ac + \beta bc = a(\alpha c + \beta d)$. If we set $y = c/a \in R$, then we readily get $c = ya$ and $d = cb/a = yb$. So $\mathbf{M} = \begin{pmatrix} xa & xb \\ ya & yb \end{pmatrix}$ is column-row. □

1.2 Weak Euclidean algorithm

As observed in the introduction, the study of properties (GE_n) and (ID_n) of factorization of invertible and singular matrices into elementary and idempotent ones, is related to the study of the generalizations of the Euclidean algorithm. In this section we introduce the notion of weak Euclidean algorithm and present its connection with our factorization properties.

In the paper [48], O'Meara examined the notion of *Euclidean chain condition* for Dedekind domains. Here we extend O'Meara's definition to a generic domain; the Dedekind condition is indeed irrelevant (cf. [53]).

Definition 1.2.1. Let a and b be two non-zero elements of an integral domain R. We say that a, b satisfy a *weak (Euclidean) algorithm* if there exists a finite sequence of divisions

$$r_i = q_{i+1} r_{i+1} + r_{i+2}, \quad r_i, q_i \in R,\ 1 \leq i \leq n,$$

such that $a = r_1$, $b = r_2$, $r_{n+1} \neq 0$ and $r_{n+2} = 0$. If this happens for any pair of non-zero elements of R, we say that R admits a weak (Euclidean) algorithm

and we will call R a *weakly Euclidean* domain (in O'Meara's terminology, R satisfies the Euclidean chain condition).

Remark 1. We recall that in the paper [16], G. Cooke generalized the notion of Euclidean domain, and applied it to the rings of integers in quadratic number fields in [17]. In Cooke's terminology (see [16]), a domain R that satisfies a weak algorithm is an ω-stage Euclidean domain, if we consider the trivial norm N on R defined by $N(0) = 0$ and $N(a) = 1$ for $0 \neq a \in R$.

We collect some easy results on weak algorithms in the following Proposition.

Proposition 1.2.2.

(i) *Any weakly Euclidean domain R is also a Bézout domain.*

(ii) *If either a divides b or b divides a, then $a, b \in R$ admit a weak algorithm.*

(iii) *Any valuation domain satisfies a weak algorithm.*

(iv) *If $a, b \in R$ satisfy a weak algorithm, then, for any $u, w \in R^*$, also ua and wb do.*

(v) *If R admits a weak algorithm, then the localization R_S of R to any multiplicative subset S of R admits a weak algorithm.*

Proof.

(i) For any pair of non-zero elements $a, b \in R$, the weak algorithm implies that $aR + bR = r_{n+1}R$.

(ii) If $b|a$, then $a = cb$ with $0 \neq c \in R$. If $a|b$, then $b = da$ for some $0 \neq d \in R$, and we have the following sequence of relations

$$\begin{aligned} a &= b + (a - b), \\ b &= -(a - b) + a, \\ (a - b) &= a(1 - d). \end{aligned}$$

(iii) Given two non-zero elements a and b of a valuation domain R, either $a|b$ or $b|a$. Then the result follows from (ii).

(iv) It can be checked by an easy computation that, if there exists a finite sequence of relations

$$r_i = q_{i+1}r_{i+1} + r_{i+2},$$

with $r_i, q_i \in R$ and $1 \leq i \leq n$, such that $a = r_1$, $b = r_2$, $r_{n+1} \neq 0$ and $r_{n+2} = 0$, then there is also a sequence

$$R_i = Q_{i+1}R_{i+1} + R_{i+2},$$

such that $ua = R_1$, $wb = R_2$, $R_i = ur_i$ and $Q_i = wu^{-1}q_i$ for i odd, and $R_i = wr_i$ and $Q_i = uw^{-1}q_i$ for i even.

(v) The elements of S are units of R_S, then the thesis follows from (iv).

□

The link between the notion of weak algorithm and the property (GE_2) is given by a nice result by O'Meara [48], that we state and prove using our terminology.

Theorem 1.2.3 (Th.14.3 in [48])**.** *A principal ideal R admits a weak Euclidean algorithm if and only if R satisfies property (GE_2).*

Proof. Assume first that R is a weakly Euclidean domain and let

$$\mathbf{A} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

be an invertible matrix over R. We can assume, up to a multiplication by a suitable dilation, that $\mathbf{A} \in SL_2(R)$, i.e. $\det(\mathbf{A}) = a_1b_2 - a_2b_1 = 1$. We want to express $\mathbf{A}$ as a product of elementary matrices. We distinguish two cases.

1. If either a_1 or a_2 is zero, then either a_2 or a_1 is a unit of R. In particular, if $a_1 = 0$ we get $\mathbf{A} = \mathbf{E}(-a_2^{-1}, b_2)$ while, if $a_2 = 0$, then $\mathbf{A} = \mathbf{D}(a_1)\mathbf{T}_{12}(a_1^{-1}b_1)$. In both cases $\mathbf{A}$ is a product of transvections (see 1.1 and 1.2).

2. If both a_1 and a_2 are different from 0, then there exists a sequence of relations of the form

$$\begin{aligned} a_1 &= q_2a_2 + r_3, \\ a_2 &= q_3r_3 + r_4, \\ r_3 &= q_4r_4 + r_5, \\ &\dots \\ r_n &= q_{n+1}r_{n+1}. \end{aligned}$$

Premultiplying $\mathbf{A}$ by $\mathbf{T}_{12}(-q_2)$, then by $\mathbf{T}_{21}(-q_3)$, then by $\mathbf{T}_{12}(-q_4)$, and so on, we ultimately obtain a new invertible matrix of the form

$\begin{pmatrix} r_{n+1} & \alpha \\ 0 & \beta \end{pmatrix}$ or $\begin{pmatrix} 0 & \gamma \\ r_{n+1} & \delta \end{pmatrix}$, with $\alpha, \beta, \gamma, \delta \in R$. Since this new matrix has again determinant equal to 1, then the result follows now from point (1).

Conversely, assume that R satisfies property (GE_2) and let a_1, a_2 be two non-zero elements of R. We want to prove that they admit a weak algorithm. We can assume without loss of generality, that $\langle a_1, a_2 \rangle = R$. In fact, since R is a principal ideal domain, there exists $\alpha \in R$, the greatest common divisor of a_1 and a_2, such that $\langle a_1, a_2 \rangle = \alpha R$, but if a_1/α and a_2/α have a weak algorithm, then we have one also for a_1 and a_2. It follows that there exist $b_1, b_2 \in R$ such that

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in SL_2(R),$$

and, by assumption, we have $q_2, \ldots, q_k \in R$ such that

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_3 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ q_k & 1 \end{pmatrix}.$$

We observe that, in order to get the above factorization, it might be necessary to introduce some terms with $q_i = 0$. Define

$$\begin{aligned} r_3 &= a_1 - a_2 q_2, \\ r_4 &= a_2 - r_3 q_3, \\ r_{i+2} &= r_i - ri + 1 q_{i+1} \qquad \text{for} \qquad i = 3, \ldots, k-1. \end{aligned}$$

Then, premultiplying $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ by $\mathbf{T}_{21}(-q_2)$, then by $\mathbf{T}_{21}(-q_3)$ and so on, we get from the matrix equation above that

$$\begin{pmatrix} r_k & * \\ r_{k+1} & * \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore there exists a finite sequence of relations of the form

$$r_i = q_{i+1} r_{i+1} + r_{i+2}, \quad \text{with } i = 1, \ldots, k-1$$

such that $r_1 = a_1$, $r_2 = a_2$ and $r_{k+1} = 0$. So R admits a weak Euclidean algorithm. □

We remark that the theorem above was proved by O'Meara for principal ideal domains but, as observed by Salce and Zanardo in [53], its proof extends *verbatim* to Bézout domains. Moreover, Kaplansky's Theorem 7.1 in [34] allows to lift the previous result to (GE_n), for all $n > 0$. Therefore we can state O'Meara's theorem in a more general form:

Theorem 1.2.4 (O'Meara)**.** *A Bézout domain R admits a weak Euclidean algorithm if and only if it satisfies the property (GE_n), for all $n > 0$.*

From Ruitenburg's Thorem 0.0.2 and Proposition 1.2.2 (i) it also follows that an integral domain R satisfying a weak Euclidean algorithm, satisfies also property (ID_n), for all $n > 0$.

The next result was proved in [53, Th.6.2] without using Ruitenburg's Theorem.

Theorem 1.2.5 (Th.6.2 in [53])**.** *If an integral domain R admits a weak Euclidean algorithm, then it satisfies property (ID_n), for all $n > 0$.*

Proof. Let R be a weakly Euclidean domain. By Proposition 1.2.2, R is a Bézout domain then, by Laffey's reduction argument, it is enough to consider the 2×2 case. Moreover, by Proposition 1.1.5, any singular 2×2 matrix $\mathbf{M}$ over R is column-row i.e.

$$\mathbf{M} = \begin{pmatrix} xa & xb \\ ya & yb \end{pmatrix}$$

for suitable $a, b, x, y \in R$. This matrix can be written as $\mathbf{M} = \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ and it is a product of idempotent matrices whenever the matrices $\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$ and $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ are products of idempotents. Since the transposition of a 2×2 idempotent matrix is again an idempotent matrix, then the transposition of a product of idempotents is again a product of idempotents. Therefore to prove that R satisfies property (ID_2) is enough to show that every matrix of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ lies in $ID_2(R)$. Cases $a = 0$ and $b = 0$ are trivial, so we assume that both a and b are non-zero elements of R. By assumption, there exists a finite sequence of relations $r_i = q_{i+1}r_{i+1} + r_{i+2}$ with $i = 1, \ldots, n$ such that $r_1 = a$, $r_2 = b$, $r_{n+1} \neq 0$ and $r_n + 2 = 0$. At the first step, we get $a = bq_2 + r_3$ and we get the following relation of similarity:

$$\begin{pmatrix} 1 & 0 \\ q_2 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q_2 & 1 \end{pmatrix} = \begin{pmatrix} r_3 & b \\ q_2 r_3 & q_2 b \end{pmatrix}.$$

Therefore it suffices to show that $\begin{pmatrix} r_3 & b \\ q_2 r_3 & q_2 b \end{pmatrix}$, similar to $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, is product of idempotents. But

$$\begin{pmatrix} r_3 & b \\ q_2 r_3 & q_2 b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ q_2 & 0 \end{pmatrix} \begin{pmatrix} r_3 & b \\ 0 & 0 \end{pmatrix},$$

then it is enough to show that $\begin{pmatrix} r_3 & b \\ 0 & 0 \end{pmatrix} \in ID_2(R)$. At the second step of the algorithm we get $b = q_3 r_3 + r_4$ and

$$\begin{pmatrix} 1 & q_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_3 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} r_3 & r_4 \\ 0 & 0 \end{pmatrix}.$$

Hence $\begin{pmatrix} r_3 & b \\ 0 & 0 \end{pmatrix}$ is similar to $\begin{pmatrix} r_3 & r_4 \\ 0 & 0 \end{pmatrix}$ and it suffices to prove that this latter matrix is product of idempotents. Repeating this procedure, after n steps, it remains to prove that $\begin{pmatrix} r_{n+2} & r_{n+1} \\ 0 & 0 \end{pmatrix} \in ID_2(R)$ or that $\begin{pmatrix} r_{n+1} & r_{n+2} \\ 0 & 0 \end{pmatrix} \in ID_2(R)$. Since $r_{n+2} = 0$, we get in the first case

$$\begin{pmatrix} 0 & r_{n+1} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & r_{n+1} \\ 0 & 1 \end{pmatrix},$$

and in the second case

$$\begin{pmatrix} r_{n+1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 - r_{n+1} & 0 \end{pmatrix}.$$

Finally, we conclude that $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in ID_2(R)$. □

Remark 2. Using this result, we can avoid the use of Ruitenburg's theorem in the following discussion. Actually, in Theorems 2.3.11 and 2.3.17 we prove that two classes of principal ideal domains do not satisfy property (ID_2) in order to conclude that they are non-Euclidean PID's that do not satisfy (GE_2). These facts can be deduced using only Theorem 1.2.5 and Theorem 1.2.3.

A natural problem that arises after the definition of weak Euclidean algorithm is to establish which integral domains admit a weak algorithm. It is easy to see that Bézout domains with stable range 1 (see [23, V.8]) admit a weak algorithm. Let us recall that R is said to have stable range 1 if for any $a, b \in R$ satisfying $aR + bR = R$, there exists $y \in R$ such that $a + by$ is a unit. Moreover, if $V_1, \ldots, V_n$ are valuation domains of the same field Q, the ring $R = \bigcap_{i=1}^{n} V_i$ is Bézout and semi-local hence, since semi-local domains have stable range 1 (for these notions see [46] and [23, V.8.2]), it is weakly Euclidean. Salce and Zanardo constructed in [53] a large class of weakly Euclidean domains obtained as an infinite intersection of valuation domains. Moreover, they proved that the pull-back $R = D + XQ[\![X]\!]$ of an integral domain D admitting a weak algorithm (where Q is the field of fraction of D and X indeterminate) admits a weak algorithm as well, providing a natural method to construct weak Euclidean domains. Other classes of domains with a weak algorithm have been exhibited in [12].

1.3 Algebraic curves

In this section we recall some results on algebraic curves we will need in the following. For full details, more general definitions and proofs we refer to [24, 42, 59, 60]. We also fix some notations that will stand throughout the thesis.

Let k be a perfect field, i.e., every algebraic extension of k is separable, and $\bar{k}$ its algebraic closure.

We consider a projective curve $\mathcal{C} \subset \mathbb{P}^n$ over k. We denote as $\mathcal{C}(k)$, $\mathcal{C}(\bar{k})$ the sets of points of $\mathcal{C}$ with coordinates in k, $\bar{k}$, respectively. Let us choose a canonical embedding ϕ_i of $\mathbb{A}^n$ in $\mathbb{P}^n$ and identify $\mathbb{A}^n$ with its image. As it is well known from the theory of affine and projective varieties, $\mathcal{C} \cap \mathbb{A}^n$ is an affine curve (i.e. an affine variety of dimension 1) and either $\mathcal{C} \cap \mathbb{A}^n = \emptyset$ or $\mathcal{C} = \overline{\mathcal{C} \cap \mathbb{A}^n}$, where $\overline{\mathcal{C} \cap \mathbb{A}^n}$ denotes the projective closure of $\mathcal{C} \cap \mathbb{A}^n$. There is at least one i such that $\mathcal{C} \cap \phi_i \mathbb{A}^n \neq \emptyset$, and we denote by $\mathcal{C}_0$ the affine curve $\mathcal{C} \cap \mathbb{A}^n \neq \emptyset$, called a *nonempty affine part* of $\mathcal{C}$. We denote by $\mathcal{C}_\infty$ the finite set $\mathcal{C} \setminus \mathcal{C}_0$. The elements of $\mathcal{C}_\infty$ are called *points at infinity* on $\mathcal{C}$.

The *function field* (or *field of rational functions*) of $\mathcal{C}$ over k is denoted by $k(\mathcal{C})$, and it is defined as the quotient ring of the affine coordinate ring $k[\mathcal{C}_0]$. It is worth recalling that $k(\mathcal{C})$ is independent on the choice of the affine part $\mathcal{C}_0$ of $\mathcal{C}$.

The affine coordinate ring of $\mathcal{C}_0$ and the function field of $\mathcal{C}$ can be defined in the obvious way over $\bar{k}$. It can be checked that $k[\mathcal{C}_0]$ and $k(\mathcal{C})$ are, respectively, the subsets of $\bar{k}[\mathcal{C}_0]$ and $\bar{k}(\mathcal{C})$ fixed by the Galois group $G_{\bar{k}/k}$.

In what follows, by curve we will mean a projective variety of dimension 1.

1.3.1 Local rings at smooth points of a curve

In this section we recall the main results on the local ring of a curve $\mathcal{C}$ over k at a smooth point $P \in \mathcal{C}$.

Definition 1.3.1. Let P be a point of the projective curve $\mathcal{C}$, choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $P \in \mathbb{A}^n$, and set $\mathcal{C}_0 = \mathcal{C} \cap \mathbb{A}^n$. The *local ring of* $\mathcal{C}$ *at* P, denoted by $k[\mathcal{C}]_P$, is the subset of $k(\mathcal{C})$ defined as

$$k[\mathcal{C}]_P = \{F \in k(\mathcal{C}) \mid F = f/g \text{ for some } f, g \in k[\mathcal{C}_0] \text{ with } g(P) \neq 0\}.$$

It is easy to see that $k[\mathcal{C}]_P$ is the localization of $k[\mathcal{C}_0]$ at the maximal ideal $\mathfrak{M}_P = \{f \in k[\mathcal{C}_0] \mid f(P) = 0\}$.

A function $F \in k(\mathcal{C})$ that lies in $k[\mathcal{C}]_P$ is said to be *regular* at P since in this case it makes sense to evaluate F at P.

The *residue field* of P is defined as $k[\mathcal{C}]_P/\mathfrak{M}_P$ and it is the smallest extension field $k(P)$ of k such that $P \in \mathbb{P}^n(k(P))$. The degree of P is defined as $\deg(P) = [k(P) : k]$ and it is equal to the order of the Galois orbit $G_{\bar{k}/k}P$.

With this terminology the coordinate ring of the affine curve $\mathcal{C}_0$ over k, $k[\mathcal{C}_0]$, is the ring of the rational functions on $\mathcal{C}$ which are regular at $\mathcal{C}_0$, i.e.

$$k[\mathcal{C}_0] = \bigcap_{P \in \mathcal{C}_0} k[\mathcal{C}]_P.$$

Definition 1.3.2. Let $\mathcal{C}$ be a projective curve over k, $P \in \mathcal{C}$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. We will say that P is a *non-sigular smooth* point of $\mathcal{C}$ if it is a smooth point of $\mathcal{C}_0 = \mathcal{C} \cap \mathbb{A}^n$. A curve $\mathcal{C}$ is said to be *non-singular* or *smooth* if every point of $\mathcal{C}$, i.e. every element of $\mathcal{C}(\bar{k})$, is non-singular.

Proposition 1.3.3. *Let $\mathcal{C}$ be a curve and $P \in \mathcal{C}$ a smooth point. Then $k[\mathcal{C}]_P$ is a DVR. In particular $k[\mathcal{C}]_P$ is integrally closed in $k(\mathcal{C})$.*

It follows that if $\mathcal{C}$ is a smooth curve, then, the coordinate ring $k[\mathcal{C}_0]$ of any affine part $\mathcal{C}_0$ of $\mathcal{C}$ is a Dedekind domain.

Definition 1.3.4. Let $\mathcal{C}$ be a curve and $P \in \mathcal{C}$ a smooth point. The *(normalized) valuation* on $k[\mathcal{C}]_P$ is given by the correspondence

$$\mathrm{ord}_P : k[\mathcal{C}]_P \to \mathbb{N} \cup \{\infty\},$$

defined by:

$$\mathrm{ord}_P(f) = \max\{d \in \mathbb{Z} \mid f \in \mathfrak{M}_P^d\}.$$

Using the relation $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, we can extend ord_P to $k(\mathcal{C})$:

$$\mathrm{ord}_P : k(\mathcal{C}) \to \mathbb{Z} \cup \{\infty\}.$$

A *uniformizer* for $\mathcal{C}$ at P is a function $t \in k(\mathcal{C})$ such that $\mathrm{ord}_P(t) = 1$ (i.e. a generator for $\mathfrak{M}_P$).

Let P_1 and P_2 be smooth points of $\mathcal{C}$. Then $\mathrm{ord}_{P_1} = \mathrm{ord}_{P_2}$ if and only if $P_1 \in G_{\bar{k}/k}P_2$, i.e. if and only if there exists $g \in G_{\bar{k}/k}$ such that $P_1 = gP_2$.

Definition 1.3.5. Let $\mathcal{C}$ and P be as above and let $F \in k(\mathcal{C})$. We will call $\mathrm{ord}_P(F)$ the *order* of F at P.

Proposition 1.3.6. *Let $\mathcal{C}$ be a curve, $P \in \mathcal{C}$ a smooth point, and $F \in k(\mathcal{C})$. Then if*

(i) $ord_P(F) > 0$, *then* F *has a zero at* P *whose multiplicity is* $ord_P(F)$;

(ii) $ord_P(F) < 0$, *then* F *has a pole at* P *whose multiplicity is* $-ord_P(F)$; *and if*

(iii) $ord_P(F) \geq 0$, *then* F *is regular at* P *and we can evaluate* $F(P)$.

Proposition 1.3.7. *Let* $\mathcal{C}$ *be a smooth curve and* $F \in k(\mathcal{C})$. *Then there are only finitely many points of* $\mathcal{C}$ *at which* F *has a pole or a zero. Moreover, if* F *has no poles, then* $F \in k$.

For a proof we refer to [31, Ch. I and II].

Let $\mathcal{C}$ be a curve defined over k, and let $k(\mathcal{C})$ be its function field.

Definition 1.3.8. A *place* $\mathfrak{p}$ of the function field $k(\mathcal{C})$ is the maximal ideal of some discrete valuation ring $O_\mathfrak{p}$ of $k(\mathcal{C})$ having $k(\mathcal{C})$ as field of fractions. Set $\mathbb{P}_{k(\mathcal{C})} = \{\mathfrak{p} \,|\, \mathfrak{p} \text{ is a place of } k(\mathcal{C})\}$.

To a place $\mathfrak{p} \in \mathbb{P}_{k(\mathcal{C})}$ we associate a discrete valuation $v_\mathfrak{p} : k(\mathcal{C}) \to \mathbb{Z} \cup \{\infty\}$ defined as follows: for $F \in k(\mathcal{C})^* \cap O_\mathfrak{p}$ we set $v_\mathfrak{p}(F) = \sup\{d \in \mathbb{Z} \,|\, F \in \mathfrak{p}^d\}$, while for $F \in k(\mathcal{C})^* \setminus O_\mathfrak{p}$ we set $v_\mathfrak{p}(F) = -v_\mathfrak{p}(1/F)$; $v_\mathfrak{p}(0) = \infty$. We have then that

$$O_\mathfrak{p} = \{F \in k(\mathcal{C}) \,|\, v_\mathfrak{p}(F) \geq 0\};$$

$$O_\mathfrak{p}^* = \{F \in k(\mathcal{C}) \,|\, v_\mathfrak{p}(F) = 0\};$$

$$\mathfrak{p} = \{F \in k(\mathcal{C}) \,|\, v_\mathfrak{p}(F) > 0\}.$$

The *degree* of a place $\mathfrak{p}$ of $k(\mathcal{C})$ is defined as $\deg \mathfrak{p} = [O_\mathfrak{p}/\mathfrak{p} : k]$.

It is straightforward that we can define a correspondence between the set of Galois orbits of non-singular points of $\mathcal{C}$ and the set $\mathbb{P}_{k(\mathcal{C})}$ of places of $k(\mathcal{C})$, associating to $G_{\bar{k}/k}P = \{gP \,|\, g \in G_{\bar{k}/k}\}$ with P smooth point of $\mathcal{C}$, the place $\mathfrak{p} = \{F \in k(\mathcal{C}) \,|\, \mathrm{ord}_P(F) > 0\}$. Clearly $O_\mathfrak{p} = k[\mathcal{C}]_P$.

If $\mathcal{C}$ is smooth, this correspondence is even a bijection. Given a place $\mathfrak{p} \in \mathbb{P}_{k(\mathcal{C})}$, there exist points $P_1, \ldots, P_n \in \mathcal{C}(\bar{k})$ such that $O_\mathfrak{p} = k[\mathcal{C}]_{P_i}$ and the P_i's form an orbit under $G_{\bar{k}/k}$ (cf. [42, Prop. 6.9]).

If $\mathfrak{p}$ is a place of degree 1, then we may associate to $\mathfrak{p}$ a point P of the smooth curve $\mathcal{C}$ which is defined over k.

1.3.2 Divisors

The *(k-rational) divisor group* $\mathrm{Div}_k(\mathcal{C})$ of a curve $\mathcal{C}$, defined over the perfect field k, is the free abelian group generated by the places of $k(\mathcal{C})$.

Therefore any divisor $D \in \mathrm{Div}_k(\mathcal{C})$ is a formal sum

$$D = \sum_{\mathfrak{p} \in \mathbb{P}_{k(\mathcal{C})}} n_{\mathfrak{p}} \mathfrak{p},$$

with $n_{\mathfrak{p}} \in \mathbb{Z}$ and $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p} \in \mathbb{P}_{k(\mathcal{C})}$.

Recall that, when $\mathcal{C}$ is smooth, to each place $\mathfrak{p} \in \mathbb{P}_{k(\mathcal{C})}$ corresponds a conjugacy class of $\mathcal{C}(\bar{k})/G_{\bar{k}/k}$. Hence D can also be given in the form

$$D = \sum_{P \in \mathcal{C}} n_P P$$

with $n_P \in \mathbb{Z}$, almost all $n_P = 0$, and $n_P = n_Q$ if $P = gQ$ for some $g \in G_{\bar{k}/k}$.

Since in what follows we will be concerned only in smooth curves defined over the perfect field k, from now on we will use the notation above, i.e.

$$\mathrm{Div}_k(\mathcal{C}) = \{D = \sum_{P \in \mathcal{C}} n_P P \,|\, n_P \in \mathbb{Z},\ \text{a. a. } n_P = 0,\ n_P = n_Q \text{ if } P \in G_{\bar{k}/k} Q\}.$$

We can define a partial order on $\mathrm{Div}_k(\mathcal{C})$ saying that a divisor $D = \sum_{P \in \mathcal{C}} n_P P$ is *positive* (or *effective*) if $n_P \geq 0$ for every $P \in \mathcal{C}$. In this case we will write $D \geq 0$. Analogously, for any two divisors D_1, D_2, writing $D_1 \geq D_2$ means that $D_1 - D_2$ is positive.

For $D \in \mathrm{Div}_k(\mathcal{C})$, let $Z = \{P \in \mathcal{C} \,|\, n_P > 0\}$ and $N = \{P \in \mathcal{C} \,|\, n_P < 0\}$, and define

$$D_0 = \sum_{P \in Z} n_P P \qquad \text{and} \qquad D_\infty = \sum_{P \in N} -n_P P.$$

Then $D = D_0 - D_\infty$, and both D_0 and D_∞ are positive.

The *degree* of a divisor $D = \sum_{P \in \mathcal{C}} n_P P$ is defined as

$$\deg(D) = \sum_{P \in \mathcal{C}} n_P.$$

The divisors of degree 0 form a subgroup of $\mathrm{Div}_k(\mathcal{C})$,

$$\mathrm{Div}_k^0(\mathcal{C}) = \{D \in \mathrm{Div}_k(\mathcal{C}) \,|\, \deg(D) = 0\}.$$

Let us define the action of the Galois group $G_{\bar{k}/k}$ on a divisor D as follows: for $g \in G_{\bar{k}/k}$, $gD = \sum_{P \in \mathcal{C}} n_P(gP)$.

It is immediate to see that for any $D \in \mathrm{Div}_k(\mathcal{C})$ $gD = D$ for all $g \in G_{\bar{k}/k}$ and we will say that the divisors $D \in \mathrm{Div}_k(\mathcal{C})$ are *defined over* k or k*-rational*.

Now consider a rational function $F \in k(\mathcal{C})^*$. We can associate to F a divisor,

$$\mathrm{div}(F) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(F)P.$$

Since F has only a finite number of poles and zeroes, and $\mathrm{ord}_P = \mathrm{ord}_Q$ whenever P and Q are conjugate points of $\mathcal{C}$, $\mathrm{div}(F)$ is a well-defined divisor moreover, since each ord_P is a valuation, then

$$\mathrm{div} : k(\mathcal{C})^* \to \mathrm{Div}_k(\mathcal{C})$$

is a homomorphism of abelian groups.

We can write $\mathrm{div}(F)$ as

$$\mathrm{div}(F) = \mathrm{div}(F)_0 - \mathrm{div}(F)_\infty;$$

the points occurring in $\mathrm{div}(F)_0$ (resp. $\mathrm{div}(F)_\infty$) are *zeroes* (resp. *poles*) of F.

Definition 1.3.9. A divisor $D \in \mathrm{Div}_k(\mathcal{C})$ is said to be *principal* if it has the form $D = \mathrm{div}(F)$ for some $F \in k(\mathcal{C})^*$. The set of principal divisors is a subgroup of $\mathrm{Div}_k(\mathcal{C})$ and it is usually denoted as $\mathrm{Princ}_k(\mathcal{C})$

Definition 1.3.10. The *divisor class group* or *Picard group* of the curve $\mathcal{C}$, denoted by $\mathrm{Pic}(\mathcal{C})$ is defined as the quotient of $\mathrm{Div}_k(\mathcal{C})$ by the subgroup of principal divisors.

$$\mathrm{Pic}(\mathcal{C}) = \mathrm{Div}_k(\mathcal{C})/\mathrm{Princ}_k(\mathcal{C}).$$

Two divisors $D_1, D_2 \in \mathrm{Div}_k(\mathcal{C})$ are in the same class if there exists $F \in k(\mathcal{C})$ such that $\mathrm{div}(F) = D_1 - D_2$.

Proposition 1.3.11. *Let $\mathcal{C}$ be a smooth curve and $F \in k(\mathcal{C})^*$. Then:*

(i) $div(F) = 0$ *iff* $F \in k^*$.

(ii) $deg(div(F)) = 0$.

It follows from Proposition 1.3.11 (ii) that the principal divisors form a subgroup of $\mathrm{Div}_k^0(\mathcal{C})$.

Proposition 1.3.12. *Let $\mathcal{C}$ be a smooth curve and $F \in k(\mathcal{C}) \setminus k$. The degree $deg(F)$ of F, defined as $[k(\mathcal{C}) : k(F)]$ is the number of poles of F counted with their multiplicity:*

$$deg(F) = [k(\mathcal{C}) : k(F)] = deg(div(F)_\infty).$$

For a proof of these last two propositions we refer to [13], Corollary of Theorem 4, pag.18, [60], Theorem 1.4.11, or to [62], Theorem 3.2.7.

Since $\mathrm{div}(F)_0 = \mathrm{div}(F^{-1})_\infty$ and $[k(\mathcal{C}) : k(F)] = [k(\mathcal{C}) : k(F^{-1})]$, from Proposition 1.3.12, we also get that $[k(\mathcal{C}) : k(F)] = \deg(\mathrm{div}(F)_0)$.

Definition 1.3.13. We define the *degree-0 part of the divisor class group* of a smooth curve $\mathcal{C}$ defined over k to be the quotient of $\mathrm{Div}_k^0(\mathcal{C})$ by the subgroup of principal divisors. It is usually denoted as $\mathrm{Pic}_k^0(\mathcal{C})$:

$$\mathrm{Pic}_k^0(\mathcal{C}) = \mathrm{Div}_k^0(\mathcal{C})/\mathrm{Princ}_k(\mathcal{C}).$$

Canonical divisors

In this section we focus on differential forms on a smooth curve $\mathcal{C}$ defined over k and introduce the notion of canonical divisor.

Definition 1.3.14. The *space of differential forms* on $\mathcal{C}$, $\Omega_\mathcal{C}$, is the $k(\mathcal{C})$-vector space generated by the elements dx, with $x \in k(\mathcal{C})$, with the relations:

1. $d(x + y) = dx + dy$ for all $x, y \in k(\mathcal{C})$;
2. $d(xy) = xdy + ydx$ for all $x, y \in k(\mathcal{C})$;
3. $d(\alpha) = 0$ for all $\alpha \in k$

In the following proposition we define the order of a differential form on a curve at a point of the curve.

Proposition 1.3.15. *Let $\mathcal{C}$ be a curve, $P \in \mathcal{C}$ and $t \in k(\mathcal{C})$, a uniformizer for $\mathcal{C}$ at P, i.e. $ord_P(t) = 1$. For every $\omega \in \Omega_\mathcal{C}$ there exists a unique $F \in k(\mathcal{C})$ such that $\omega = Fdt$. F will be denoted by ω/dt. Moreover, for any non-zero $\omega \in \Omega_\mathcal{C}$, the value $ord_P(\omega/dt)$ is independent on the choice of the uniformizer t. This value is called the* order of ω at P *and it is denoted by $ord_P(\omega)$.*

Definition 1.3.16. Let $\omega \in \Omega_\mathcal{C}$. The *divisor* of ω $\mathrm{div}(\omega)$ is defined as

$$\mathrm{div}(\omega) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(\mathcal{C}).$$

A divisor D of $\mathcal{C}$ of the form $D = \mathrm{div}(\omega)$ for some $\omega \in \Omega_\mathcal{C}$, is called a *canonical divisor*.

1.3.3 The Riemann-Roch Theorem

We recall in this section one of the main and most celebrated results in the theory of algebraic curves, the Riemann-Roch Theorem. We recall, in particular, one of its corollaries, that will be useful in the sequel.

Definition 1.3.17. Let $D = \sum_{P \in \mathcal{C}} n_P P$ be a k-rational divisor of the curve $\mathcal{C}$. We can associate to D the set of functions

$$\mathcal{L}(D) = \{F \in k(\mathcal{C})^* \,|\, \mathrm{div}(F) \geq -D\} \cup \{0\}.$$

Equivalently

$$\mathcal{L}(D) = \{F \in k(\mathcal{C})^* \,|\, ord_P(F) \geq -n_P \text{ for all } P \in \mathcal{C}\} \cup \{0\}.$$

It can be proved that $\mathcal{L}(D)$ is a finite-dimensional k-vector space, and we denote its dimension by $\ell(D)$.

The *Riemann-Roch Thoerem* provides a very important relation that connects $\deg(D)$ with $\ell(D)$.

Theorem 1.3.18 (Riemann-Roch)**.** *Let $\mathcal{C}$ be a smooth projective curve defined over k, and let W be a canonical divisor on $\mathcal{C}$. There is an integer $g \geq 0$, called the* genus *of $\mathcal{C}$, such that, for every $D \in Div_k(\mathcal{C})$*

$$\ell(D) = deg(D) + 1 - g + \ell(W - D).$$

For a proof we refer to [60, Th. 1.5.15] or to the Weil's proof given in the first chapter of [40].

Corollary 1.3.19. *In the above notation we have that :*

(a) $\ell(W) = g$*;*

(b) $deg(W) = 2g - 2$*;*

(c) for all $D \in Div_k(\mathcal{C})$ such that $deg(D) > 2g - 2$, then

$$\ell(D) = deg(D) + 1 - g.$$

To any projective non-singular curve $\mathcal{C}$ of genus g over the field k can be associated in a "functorial" way a g-dimensional abelian variety, called the *Jacobian* of $\mathcal{C}$ and denoted as $J_{\mathcal{C}}$. We are interested, for our purposes, only in the set of points of this variety having coordinates in k.

Definition 1.3.20. The set of k-rational points of the Jacobian of a curve $\mathcal{C}$ is defined as

$$J_{\mathcal{C}}(k) \cong \mathrm{Pic}^0_k(\mathcal{C}).$$

Now we give a characterization of the field of rational functions of our curve $\mathcal{C}$. For more details see [60, Prop. 1.6.3].

Definition 1.3.21. We will say that a curve $\mathcal{C}$ defined over k is *rational* if the field of rational functions of $\mathcal{C}$, $k(\mathcal{C})$, is rational, i.e. $k(\mathcal{C}) = k(x)$ for some x trascendental over the field k.

Proposition 1.3.22. *Let $\mathcal{C}$ be a non-singular projective curve over the field k. The following conditions are equivalent:*

(a) $k(\mathcal{C})$ is rational;

(b) $\mathcal{C}$ has genus 0 and there is some divisor $D \in Div_k(\mathcal{C})$ with $deg(D) = 1$.

As an immediate consequence we get that every smooth projective curve having genus ≥ 1 can not be a rational curve.

We conclude with the *genus-degree* formula that relates the genus g of a smooth *plane* curve $\mathcal{C} \subset \mathbb{P}^2$ and its degree d, i.e. the degree of its defining polynomial.

Proposition 1.3.23 (Genus-degree)**.** *Let $F(X, Y, Z) \in k[X, Y, Z]$ be a homogeneous polynomial of degree $d \geq 1$ and assume that $\mathcal{C} \subset \mathbb{P}^2$ is a non-singular plane curve defined by the equation $F = 0$. Then, the genus g of $\mathcal{C}$ is given by the following relation:*

$$g = \frac{(d-1)(d-2)}{2}.$$

1.3.4 Class group of coordinate rings

Let $\mathcal{C}$ be a non-singular projective curve defined over the perfect field k, given by the disjoint union $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_\infty$, where $\mathcal{C}_0$ is an affine smooth part of $\mathcal{C}$ and $\mathcal{C}_\infty = \mathcal{C} \setminus \mathcal{C}_0$ is the finite set of the points at infinity of $\mathcal{C}$.

Let us call $\mathrm{Div}_k(\mathcal{C}_0)$ the subgroup of $\mathrm{Div}_k(\mathcal{C})$ generated by the places of $k(\mathcal{C})$ *at finite*, i.e. corresponding to the conjugacy classes of the points of $\mathcal{C}_0$, and $\mathrm{Div}_k(\mathcal{C}_\infty)$ the subgroup of $\mathrm{Div}_k(\mathcal{C})$ generated by the places of $k(\mathcal{C})$

at infinity, i.e. corresponding to the conjugacy classes of the points of $\mathcal{C}_\infty$. Namely,

$$\mathrm{Div}_k(\mathcal{C}_0) = \{D = \sum_{\mathfrak{p}\in\mathcal{C}_0} n_\mathfrak{p}\mathfrak{p}\};$$

$$\mathrm{Div}_k(\mathcal{C}_\infty) = \{D = \sum_{\mathfrak{p}\in\mathcal{C}_\infty} n_\mathfrak{p}\mathfrak{p}\};$$

where, with a slight abuse of notation, we denoted the set of places at finite (resp. at infinity) as $\mathcal{C}_0$ (resp. $\mathcal{C}_\infty$).

As usual we denote by $\mathrm{Princ}_k(\mathcal{C})$ the group of principal divisors of $\mathcal{C}$.

For our purposes it will be more convenient to adopt this notation throughout all this section.

Let $R = k[\mathcal{C}_0] = \bigcap_{\mathfrak{p}\in\mathcal{C}_0} O_\mathfrak{p}$ be the affine coordinate ring of $\mathcal{C}_0$. As it is well known R is a Dedekind domain.

We want to explain the relation between the ideal class group of $R = k[\mathcal{C}_0]$ and the group $\mathrm{Div}_k(\mathcal{C})$ of k-rational divisors of $\mathcal{C}$.

For any $f \in R = k[\mathcal{C}_0]$ we define

$$\mathrm{div}_0(f) = \sum_{\mathfrak{p}\in\mathcal{C}_0} v_\mathfrak{p}(f)\mathfrak{p} \in \mathrm{Div}_k(\mathcal{C}_0) \subset \mathrm{Div}_k(\mathcal{C}).$$

The generalization of this definition at any $F \in k(\mathcal{C}_0)$ is obvious.

For I an ideal of $R = k[\mathcal{C}_0]$, we define

$$\mathrm{div}_0(I) = \sum_{\mathfrak{p}\in\mathcal{C}_0} n_\mathfrak{p}(I)\mathfrak{p} \in \mathrm{Div}_k(\mathcal{C}_0) \subset \mathrm{Div}_k(\mathcal{C}),$$

where, for each $\mathfrak{p} \in \mathcal{C}_0$,

$$n_\mathfrak{p}(I) = \inf\{v_\mathfrak{p}(z) : z \in I\}.$$

Note that $\mathrm{div}_0(f)$, with $f \in R$, and $\mathrm{div}_0(I)$ are both positive in the partial order of divisors.

As a matter of fact, by the definition it is not immediate that $\sum_{\mathfrak{p}\in\mathcal{C}_0} n_\mathfrak{p}(I)\mathfrak{p}$ is a finite sum. However, the finiteness of the sum is a trivial consequence of the next result.

Proposition 1.3.24. *In the above notation $f \in I$ if and only $div_0(f) \geq div_0(I)$.*

Proof. Assume that $\mathrm{div}_0(f) \geq \mathrm{div}_0(I)$. Since R is a Dedekind domain, I is invertible and two-generated, say $I = \langle z_1, z_2\rangle$. It follows that $n_\mathfrak{p}(I) = v_\mathfrak{p}(z_i)$ where i is either 1 or 2, hence for all $\mathfrak{p} \in \mathcal{C}_0$ there is $i \in \{1, 2\}$ such that

$v_{\mathfrak{p}}(f) \geq v_{\mathfrak{p}}(z_i)$. Moreover, since I is invertible, there exist $\alpha_1, \alpha_2 \in I^{-1}$ such that $1 = \alpha_1 z_1 + \alpha_2 z_2$, with $\alpha_j z_i \in R$ for $i, j \in \{1, 2\}$. Then $v_{\mathfrak{p}}(\alpha_j z_i) \geq 0$ for any $\mathfrak{p} \in \mathcal{C}_0$ and i, j. Thus, $v_{\mathfrak{p}}(\alpha_j f) \geq v_{\mathfrak{p}}(\alpha_j z_i) \geq 0$ for all $\mathfrak{p} \in \mathcal{C}_0$ and $j \in \{1, 2\}$, and $f\alpha_1, f\alpha_2 \in R$. It follows that

$$f = (f\alpha_1)z_1 + (f\alpha_2)z_2 \in I.$$

The reverse implication is immediate. □

Proposition 1.3.25. *In the above notation $I = rR$ ($r \in R$) if and only if there exists $\eta \in Div_k(\mathcal{C}_\infty)$ such that $div(r) = div_0(I) + \eta$.*

Proof. Let us assume that $\mathrm{div}(r) = \mathrm{div}_0(I) + \eta$. Then $v_{\mathfrak{p}}(r) = n_{\mathfrak{p}}(I)$ for every $\mathfrak{p} \in \mathcal{C}_0$. Take any $z \in I$. By definition $v_{\mathfrak{p}}(z) \geq n_{\mathfrak{p}}(I)$ for every $\mathfrak{p} \in \mathcal{C}_0$. Hence, for every $\mathfrak{p} \in \mathcal{C}_0$, we get $v_{\mathfrak{p}}(z) \geq v_{\mathfrak{p}}(r)$ and then $v_{\mathfrak{p}}(z/r) \geq 0$, so $z/r \in R$, i.e. $z \in rR$. We conclude that $I \subseteq rR$. The reverse implication $rR \subseteq I$ follows from the preceding proposition. Since $\mathrm{div}_0(r) = \mathrm{div}_0(I)$, then $r \in I$.

Conversely, let us verify that $I = rR$ yields $\mathrm{div}(r) = \mathrm{div}_0(I) + \eta$, for some divisor at infinity η, or, equivalently, $\mathrm{div}_0(r) = \mathrm{div}_0(I)$. This is clear, since, for all $\mathfrak{p} \in \mathcal{C}_0$, $z \in rR$, say $z = rx$ for some $x \in R$, implies $v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}(r) + v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(r)$, hence $v_{\mathfrak{p}}(r) = \inf\{v_{\mathfrak{p}}(z) : z \in I\} = n_{\mathfrak{p}}(I)$. □

Proposition 1.3.26. *In the above notation, for every $D \in Div_k(\mathcal{C})$ there exist an ideal I of $R = k[\mathcal{C}_0]$, a principal divisor $div(F) \in Princ_k(\mathcal{C})$ and a divisor at infinity $\eta \in Div_k(\mathcal{C}_\infty)$ such that $D = div_0(I) + div(F) + \eta$.*

Proof. Recall that, from the Corollary 1.3.19 (c) of the Riemann-Roch Theorem, $\ell(D) = \deg(D) + 1 - g$, for every divisor D of degree $> 2g - 2$.

Clearly, in the proof of our assertion, we may assume that $D \in \mathrm{Div}_k(\mathcal{C}_0)$, say $D = \sum_{i=1}^{m} a_i \mathfrak{p}_i$, with $\mathfrak{p}_i \in \mathcal{C}_0$ and $a_i \in \mathbb{Z}$. We may also assume that each a_i is strictly positive: it suffices to take $F \in k(\mathcal{C})$ such that $\mathrm{div}_0(F) + D > 0$ and replace D with $\mathrm{div}_0(F) + D$.

Let us take a divisor at infinity $\eta \in \mathrm{Div}_k(\mathcal{C}_\infty)$ of suitably large degree such that $B = \eta - D$ has degree $\geq 2g + M - 1$, with $M = \max\{m_i = \deg \mathfrak{p}_i \,|\, i \in \{1, \ldots, m\}\}$. For each $i \leq m$ let

$$B_i = B - \mathfrak{p}_i = \eta - D - \mathfrak{p}_i.$$

Since $\deg(B_i) = \deg(B) - \deg \mathfrak{p}_i \geq 2g + M - 1 - m_i \geq 2g - 1$, we get $\ell(B_i) = \ell(B) - m_i$, and then $\ell(B) - \ell(B_i) = m_i \geq 1$. Therefore, for $1 \leq i \leq m$, we may take $z_i \in \mathcal{L}(B) \setminus \mathcal{L}(B_i)$. From $z_i \in \mathcal{L}(B)$ we get that $v_{\mathfrak{p}_i}(z_i) \geq a_i$, but, since $z_i \notin \mathcal{L}(B_i)$, then $v_{\mathfrak{p}_i}(z_i) < a_i + 1$, so that $v_{\mathfrak{p}_i}(z_i) = a_i$. Moreover, by definition of $\mathcal{L}(B)$, $v_{\mathfrak{p}_j}(z_i) \geq a_j$ for any $j \neq i$. We may also assume that

$v_{\mathfrak{p}}(z_i) = 0$ for every $\mathfrak{p} \in \mathcal{C}_0 \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. In particular, $z_i \in R$ for every $1 \leq i \leq m$. Now a direct check shows that the ideal $I = \langle z_1, \ldots, z_m \rangle$ of R is such that $\mathrm{div}_0(I) = D$. The desired conclusion follows. □

Let us recall that a *fractional ideal* J of R is a finitely-generated R-submodule of $k(\mathcal{C})$ such that $rJ \subseteq R$ for some non-zero $r \in R$. A fractional ideal J of R is said to be *principal* if there exists $F \in k(\mathcal{C})^*$ such that $J = FR$.

Let $J \subset k(\mathcal{C})$ be a fractional ideal of R and assume that rJ is an ideal of R for some non-zero $r \in R$. Then we can define

$$\mathrm{div}_0(J) = \sum_{\mathfrak{p} \in \mathcal{C}_0} n_{\mathfrak{p}}(J)\mathfrak{p} \in \mathrm{Div}_k(\mathcal{C}_0),$$

where $n_{\mathfrak{p}}(J) = \inf\{v_{\mathfrak{p}}(F) \,|\, F \in J\}$. Moreover, it can be easily checked that

$$\mathrm{div}_0(J) = \mathrm{div}_0(rJ) - \mathrm{div}(r) + \zeta$$

for a suitable $\zeta \in \mathrm{Div}_k(\mathcal{C}_\infty)$.

Theorem 1.3.27. *Let $C(R) = \mathcal{I}/\mathcal{P}$ be the ideal class group of the Dedekind domain R (or Picard group of R), where $\mathcal{I}$ is the group of fractional (invertible) ideals and $\mathcal{P}$ is the subgroup of the principal ones. Then the assignments $\phi : J \cdot \mathcal{P} \mapsto div_0(J) + Princ_k(\mathcal{C}) + Div_k(\mathcal{C}_\infty)$ define an isomorphism $\phi : C(R) \to Div_k(\mathcal{C})/(Princ_k(\mathcal{C}) + Div_k(\mathcal{C}_\infty))$.*

Proof. One can check directly that ϕ is well defined, and that ϕ is a homomorphism from the multiplicative group $C(R)$ to the additive group $\mathrm{Div}_k(\mathcal{C})/(\mathrm{Princ}_k(\mathcal{C}) + \mathrm{Div}_k(\mathcal{C}_\infty))$. Namely, if $J \sim H$, then $\phi(J \cdot \mathcal{P}) = \phi(H \cdot \mathcal{P})$ and, given $J \cdot \mathcal{P}, H \cdot \mathcal{P} \in C(R)$, then $\phi(JH \cdot \mathcal{P}) = \mathrm{div}_0(J) + \mathrm{div}_0(H) + \mathrm{Princ}_k(\mathcal{C}) + \mathrm{Div}_k(\mathcal{C}_\infty)$.

Generalizing Proposition 1.3.25 we can easily get that a fractional ideal J of R is principal, say $J = FR$ ($F \in k(\mathcal{C})^*$), if and only if there exists $\beta \in \mathrm{Div}_k(\mathcal{C}_\infty)$ such that $\mathrm{div}_0(J) = \mathrm{div}(F) + \beta$. It follows that $\ker(\phi) = \{J \cdot \mathcal{P} \in C(R) \,|\, \mathrm{div}_0(J) \in \mathrm{Princ}_k(\mathcal{C}) + \mathrm{Div}_k(\mathcal{C}_\infty)\} = \{1 \cdot \mathcal{P}\}$, and then ϕ is a monomorphism. Moreover, it is surjective by the preceding Proposition 1.3.26. □

CHAPTER 2

FACTORIZATION PROPERTIES ON NON-EUCLIDEAN PID'S

As recalled in the introduction, the classical examples of non-Euclidean principal ideal domains, namely the rings of integers of $\mathbb{Q}\sqrt{-d}$, with $d = 19, 43, 67, 163$, and the example constructed by Bass [4], were exhibited in order to show that not every PID satisfies property (GE_2) (cf. [15] and [4]). Actually, up to now, there is no example of a non-Euclidean PID that is also generalized Euclidean. Moreover, in view of the results by Weinberger [63], Harper and Murty [30], it is clear that this example cannot be found in the natural class of number fields.

Since, by O'Meara's theorem (cf. Theorem 1.2.3), every PID satisfying (GE_2) must admit a weak Euclidean algorithm, the above results suggested a natural conjecture, due to Salce and Zanardo [53]: any non-Euclidean PID cannot satisfy property (GE_2).

In this chapter we verify this conjecture for two important classes of non-Euclidean principal ideal domains: the coordinate rings of special algebraic curves, among them the conics without rational points and the elliptic curves having only one rational point, and the non-Euclidean PID's constructed by a fixed procedure, described in Anderson's 1988 paper [1].

The results in this chapter have been gathered in a paper [18] recently submitted for the publication.

2.1 The coordinate rings of special curves.

In this section we deal with the coordinate rings of special curves, that turn out to be non-Euclidean PID's. The notation is the same as that in Section 3 of Chapter 1.

With $\mathcal{C}$ we will denote a smooth projective curve of $\mathbb{P}^n$ over a perfect field k, by C_∞ the finite set of the points at infinity of $\mathcal{C}$, and as $\mathcal{C}_0 = \mathcal{C} \setminus \mathcal{C}_\infty$ an affine part of $\mathcal{C}$.

We recall that a k- rational divisor on $\mathcal{C}$ is a formal sum $D = \sum_{P \in \mathcal{C}} n_P P$, with almost all $n_P = 0$ and $n_P = n_Q$ whenever $P \in G_{\bar{k}/k} Q$.

Now we use Proposition 19 of Samuel's paper [56] to find the curves of genus zero whose coordinate rings are non-Euclidean PID's. Following [56], for an assigned curve $\mathcal{C}$ over k, we define the integers δ to be the g.c.d. of the degrees of the rational divisors of $\mathcal{C}$ and δ' the g.c.d. of the degrees of the rational divisors at infinity (i.e., rational and generated by the points at infinity of $\mathcal{C}$). Let us remark that $\delta = \delta'$ whenever $R = k[\mathcal{C}_0]$ is a PID; in fact, the group $\delta\mathbb{Z}/\delta'\mathbb{Z}$ is a homomorphic image of the Picard group $C(R)$ of R, defined as in Theorem 1.3.27 (see Section 6 of [56]), and, as it is well-known, since R is a Dedekind domain, R is a PID if and only if its Picard group vanishes.

We have the following

Proposition 2.1.1 (Proposition 19 in [56])**.** *Let $\mathcal{C}_0$ be an affine curve of genus zero over k, and $R = k[\mathcal{C}_0]$ its coordinate ring. Then*

(a) if $\delta = 1$, R is a PID if and only if R is Euclidean if and only if $\delta' = 1$.

(b) if $\delta = 2$, R is a PID if and only if $\delta' = 2$, and R is never Euclidean.

Samuel does not give examples, nor he characterizes the curves that satisfy condition (b) above. So it is worth stating the following

Corollary 2.1.2. *Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane smooth curve of genus zero over k, $\mathcal{C}_0$ the affine part of $\mathcal{C}$ and $R = k[\mathcal{C}_0]$ the affine coordinate ring of $\mathcal{C}_0$. Then R is a non-Euclidean PID if and only if $\mathcal{C}$ has no rational points.*

Proof. We recall that a curve $\mathcal{C}$ of genus 0 over the field k admits a rational divisor of odd degree if and only if the curve has rational points over k, i.e. $\mathcal{C}(k) \neq \emptyset$ (cf. [58, Prop. 4.91] or [2, Th. 7 pag. 304]). By the genus-degree Proposition 1.3.23, since $\mathcal{C}$ is a smooth plane curve of genus 0, then it is defined by a homogeneous polynomial of $k[X, Y, Z]$ of degree one or two. Therefore the corresponding affine plane curve $\mathcal{C}_0$ has equation $f(x, y) = 0$, for a suitable polynomial $f \in k[x, y]$ of degree one or two. If the degree is one, then $\mathcal{C}$ has rational points and $R \cong k[x]$ is Euclidean. Assume that the

degree of f is two. If $\mathcal{C}$ has a rational point, say P, then the divisor $1 \cdot P$ is rational and has degree one, so $\delta = 1$. Then Proposition 2.1.1 (a) shows that R is Euclidean, whenever it is a PID. Conversely, let us assume that $\mathcal{C}$ has no rational points. Then every rational divisor of $\mathcal{C}$ has even degree. Moreover, if P_1, P_2 are the points at infinity of $\mathcal{C}$ (not rational but conjugates), the divisor at infinity $P_1 + P_2$ is rational and it has degree two, so $\delta = \delta' = 2$. Thus Proposition 2.1.1 (b) shows that R is a non-Euclidean PID. □

Example 2.1.3. The coordinate ring of the conic over $\mathbb{R}$ with equation $x^2 + y^2 + 1 = 0$ is a non-Euclidean PID. Moreover, the coordinate ring of the conic over $\mathbb{Q}$ with equation $x^2 - 3y^2 + 1 = 0$ is a non-Euclidean PID over $\mathbb{Q}$ but not over $\mathbb{R}$. In fact this conic has no points with coordinates in $\mathbb{Q}$, since the equation

$$X^2 + Z^2 = 3Y^2 \tag{2.1}$$

has no solutions in $\mathbb{Z}$. To see this, assume that there exist $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Y, Z) = 1$, satisfying the equation above. Then $X^2 + Z^2 \equiv 0$ modulo 3 and, since -1 is not a square modulo 3, we get $X \equiv Z$ modulo 3. Hence, X^2 and Z^2 are divisible by 3^2 and from 2.1 we get that 3 also divides Y, contradicting the assumption $\gcd(X, Y, Z) = 1$.

We recall that the *degree* $\deg(F)$ of a rational map $F \in k(\mathcal{C})$ is the number of poles of F, counted with their multiplicities.

Now we focus on the case of the elliptic curves. Let k be a perfect field, $\bar{k}$ its algebraic closure, and $f \in k[x]$ a cubic polynomial without multiple roots. Then the equation $y^2 = f(x)$ defines an affine smooth curve E_0 over k. Its projective completion in $\mathbb{P}_2$ has a unique (smooth) point at infinity O and thus it defines an elliptic curve E with origin O.

Let $R = k[x, y] = k[E_0]$ be the coordinate ring over k of our curve. It is the ring of rational functions on E regular on E_0, i.e., defined over k, and with no poles over $\bar{k}$ outside O. We will denote by $\bar{R}$ the coordinate ring of E_0 over $\bar{k}$.

Let us observe that, since $\deg(x) = 2$ and $\deg(y) = 3$, then there is no element in R having degree 1. In fact any element $\eta \in R$ can be written in a canonical form as

$$\eta(x, y) = \alpha(x) + y\beta(x),$$

hence, if η is a non-unit of R, we must have $\deg(\eta) \geq 2$.

As usual $E(k)$ denotes the set of k-rational points of E. Then we have the following result, whose proof is due to U. Zannier.

Theorem 2.1.4 (Zannier)**.** *The ring $R = k[E_0]$ is a PID if and only if the point at infinity is the unique rational point of E. The ring is never Euclidean.*

Proof. We start by observing that the group R^* of the units of R is precisely k^*: in fact, any possible zero of a unit u would be a pole of u^{-1}, hence O, and thus u would have poles different from O.

Also, $x - c$ is irreducible (as an element of R) for any $c \in k$: in fact, this function has degree 2 on E, hence every possible non-unit factor in R would have O as a simple pole; since functions in R have no other pole, such a factor would have degree 1, impossible.

Now, suppose first that there is a point $(a, b) \in E_0(k)$, so $b^2 = f(a)$. Then $x - a$ lies in R and divides $f(x) - f(a) = (y + b)(y - b)$. However, we have already observed that $x - a$ is irreducible and does not divide any of $y \pm b \in R$, so R is not a UFD in this case.

Conversely, suppose $E(k) = \{O\}$, and take an ideal I of R. We want to show that I is principal. Since $\bar{R}$ is a Dedekind domain, the extended ideal $\bar{I}$ is a product of maximal ideals of $\bar{R}$, say $\bar{I} = \prod_i \mathfrak{M}_i$, where each $\mathfrak{M}_i$ is associated to a point P_i of $E_0(\bar{k})$. Let us consider the effective divisor $D = \sum_i (P_i)$ on E, supported outside O. Then $\mathrm{div}_0(I) = D$ and $u \in I$ if and only if $\mathrm{div}_0(u) \geq D$ (see 1.3.4).

Recall now that the degree-0 Picard group of an elliptic curve is canonically isomorphic to the group of the points of the curve, i.e. $\mathrm{Pic}^0_k(\mathcal{C}) \cong E(k)$ (cf. [59, Ch.X, Th.3.8]).

Let us take the point $Q := \sum P_i$ on E (this last sum being with respect to the group law on E). Since $\bar{I}$ is generated by elements of R, it is invariant by Galois conjugation over k. It follows that also Q is invariant by Galois conjugation, hence it lies in $E(k)$, hence is O. Then, by the above recalled isomorphism, the divisor of degree 0 given by $D - \deg(D) \cdot (O)$ is principal, equal to $\mathrm{div}(v)$ for some $v \in \bar{R}$. We conclude that $\bar{I} = v\bar{R}$.

Take any element $g \in G = G_{\bar{k}/k}$; since $g\bar{I} = \bar{I}$, we get $g(v) = u_g v$ for some unit of $\bar{R}$, i.e., $u_g \in \bar{k}^*$. But $\{u_g : g \in G\}$ is a 1-cocycle, since $u_{gh} = u_g g(u_h)$, so, by Hilbert's Theorem 90, we get $u_g = u/g(u)$, for a suitable $u \in \bar{k}$ (independent on the choice of $g \in G$). It follows that $g(uv) = uv$ for every $g \in G$, hence $uv \in R$. Then $I = \bar{I} \cap R = (uv\bar{R}) \cap R = uvR$ is a principal ideal. (Reversing this argument would also supply another proof for the converse.)

As to the last part of the theorem, if R were Euclidean, by Samuel's criterion on page 289 of [56] we would have $R = \bigcup_{n=0}^{\infty} R_n$, where the sets R_n are defined inductively by $R_0 = \{0\}$ and $R_{n+1} = \{x \in R \mid R = R_n + xR\} \cup \{0\}$, for $n \geq 0$. This definition yields $R_1 = R^* \cup \{0\} = k$. Let us prove that $R_2 = k$, as well. Assume, for a contradiction, that $u \in R_2 \setminus k$. Then $R = k + uR$, which entails $\bar{k}[x, y] = \bar{k} + u\bar{k}[x, y]$. The function u, being non constant, has degree ≥ 2, whence it has either at least two distinct zeros $P, Q \in E(\bar{k})$ or at least a double zero P. The first (respectively second) case

yields $z(P) = z(Q)$ (respectively $\mathrm{d}z(P) = 0$) for all $z \in \bar{k}[x, y]$, which is impossible. It follows that $R_2 = R_1$, and recursively $R_n = R_1 = k$ for all $n \geq 1$, so $\bigcup_{n=0}^{\infty} R_n = k \neq R$, hence R in fact is not Euclidean, finally proving the theorem. □

In [56], Remark (1) page 300, it is observed that the proof of Proposition 19 (b) may be adapted to show that the coordinate ring of a curve with one rational point is never Euclidean. For the sake of completeness, we have given a direct proof of this fact for the case of elliptic curves.

Remark 3 (Zannier)**.** (i) One can easily generalize the preceding result, replacing E by a smooth curve X over k of genus $g \geq 1$, with a rational point $O \in X(k)$, setting $X_0 = X \setminus \{O\}$ and considering $R = k[X_0]$. The condition for R being a PID becomes that the Jacobian of X has only O as a rational point over k (This is a fairly strong condition, especially for $g > 1$, as it implies e.g. that $(2g - 2) \cdot O$ is a canonical divisor.)

(ii) It seems that the above results are part of the "folklore". One can also give more elementary and explicit arguments, at least for the case of elliptic curves.

Example 2.1.5. We recall that there are several known examples of elliptic curves over $\mathbb{Q}$ with only one rational point. For instance, in the book by Cassels [10], Lemma 2, page 86, one may find the example of the curve $\mathcal{C}$ with equation

$$y^2 = x^3 - 2^8 3^5 5^2.$$

The proof that $\mathcal{C}$ has no rational points other than $O = (0, 1, 0)$ is far from being easy.

Example 2.1.6 (Zannier)**.** We give an easy example of an elliptic curve $\mathcal{C}$, defined over the field of rational functions $\mathbb{C}(t)$, that has only one rational point. Namely, let $\mathcal{C}$ have equation

$$y^2 = x^3 + t.$$

Let us show that the point at infinity $O = (0, 1, 0)$ is the unique rational point of $\mathcal{C}$. Assume, for a contradiction, that $(x(t), y(t))$ is a point of the curve, with $x(t), y(t) \in \mathbb{C}(t)$. Then the substitution $t = u^6$ shows that $(x(u^6)/u^2, y(u^6)/u^3)$ is a rational point of the curve $y^2 = x^3 + 1$, defined over $\mathbb{C}(u)$. Since the latter curve is not rational, it follows that the functions $x(u^6)/u^2$, $y(u^6)/u^3$ must be constant, which is impossible.

2.2 Anderson's PID's

The main purpose of Anderson's paper [1] was to provide an easy way to construct an abundance of principal ideal domains that are not Euclidean. To fix the ideas, we give a pair of standard examples, based on the results in [1].

Example 2.2.1. Let K be a field, X, Y indeterminates, and consider the maximal ideal $\mathfrak{M} = \langle X, Y \rangle$ of $K[X, Y]$; let $R = K[X, Y]_{\mathfrak{M}}$ be the localization at $\mathfrak{M}$. Let f be any prime element of R that lies in $\mathfrak{M}^2$ (for instance, take $f = X^2 + Y^3$), and define $R_f = R[1/f]$. Then $R[1/f]$ is a PID which is not Euclidean. In a similar way, if we take the ring of formal power series $K[[X, Y]]$, then the ring $K[[X, Y]][1/f]$, where $f = X^2 + Y^3$, is a non-Euclidean PID. Note that this second example is always uncountable, while the first one is countable, when K is countable.

Following [1], for an assigned UFD R and any prime element f of R, we consider the UFD $R[1/f]$, that will always be denoted by R_f.

It is easily seen that any $r \in R_f$ may be uniquely written as $r = f^k b$, for some $b \in R \setminus fR$ and $k \in \mathbb{Z}$. In particular, r is a unit of R_f if and only if a is a unit of R.

The following theorem, due to Anderson, derives from the theorem on page 1222 of [1]. We state it in a slightly less general way, more suitable for our purposes.

Theorem 2.2.2. *(Anderson, [1]) Let R be a two-dimensional UFD, and let f be a prime element contained in the Jacobson radical $J(R)$. Then $R_f = R[1/f]$ is always a PID, and it is Euclidean if and only if R/Rf is Euclidean. Moreover, if R_f is Euclidean, then R is regular and $f \notin \mathfrak{M}^2$ for every maximal ideal $\mathfrak{M}$ of R. Otherwise, R_f is a non-Euclidean PID.*

It is important to remark that, in the above theorem, the case when R_f is non-Euclidean was solved using the celebrated characterization by Samuel (Proposition 9 of [56]), which does not exclude the possible existence of weak algorithms.

A non-Euclidean PID of the form $R_f = R[1/f]$, as in Theorem 2.2.2 (i.e. such that R is a non-regular two-dimensional UFD, or such that $f \in \mathfrak{M}^2$ for some maximal ideal $\mathfrak{M}$ of R), will be called *Anderson's PID*.

2.3 The conjecture on non-Euclidean PID's

In this section we examine the following conjecture, proposed in [53] in the equivalent form recalled in the introduction:

(C) If a principal ideal domain R is not Euclidean, then R does not satisfy (GE_n), for some $n > 0$.

As discussed in the introduction, by the results of O'Meara [48] and Ruitenburg [52] it follows that **(C)** is equivalent to the following

(C_1) If a principal ideal domain R is not Euclidean, then R does not satisfy (GE_2).

(C_2) If a principal ideal domain R is not Euclidean, then R does not satisfy (ID_2).

(C_3) If a principal ideal domain R satisfies (ID_n) for every $n > 0$, then R is Euclidean.

(C_4) If a principal ideal domain R admits a weak algorithm, then R is Euclidean.

Our aim is to prove that the conjecture is valid when R is either a special coordinate ring as in Section 2.1, or an Anderson's PID. In fact, we will show that such R does not satisfy property (ID_2), thus proving the validity of (C_2), equivalent to **(C)**.

For convenience, we recall that by Proposition 1.1.3, $\mathbf{T} \in M_2(R)$ is a non-zero non-identity idempotent matrix if and only if $\mathbf{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$, where $a, b, c \in R$ and $a(1-a) = bc$.

The following technical property and the next lemma will be crucial for our discussion.

Let x, y, ω_1, ω_2 be elements of an integral domain R. We will say that x and y satisfy property **(NU)** if

$$\omega_1 x + \omega_2 y = 1 \Longrightarrow \omega_1, \omega_2 \text{ are not units of } R. \qquad (\mathbf{NU})$$

Lemma 2.3.1. *Let R be a UFD, x and y two coprime non-zero elements of R satisfying property **(NU)**, and $\boldsymbol{M} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in M_2(R)$. If $\boldsymbol{M} = \boldsymbol{S} \cdot \boldsymbol{T}$, with $\boldsymbol{S} = \begin{pmatrix} x' & y' \\ z & t \end{pmatrix}$ a singular matrix and $\boldsymbol{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ an idempotent matrix over R, then $\boldsymbol{S}$ has the form $\boldsymbol{S} = \begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix}$ with $x' \neq 0$. Moreover, there exist $\lambda, \mu \in R$ such that $\lambda x + \mu y = 1$ and $\lambda x' + \mu y' = 1$.*

Proof. By assumption

$$\mathbf{M} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x' & y' \\ z & t \end{pmatrix} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} = \begin{pmatrix} ax' + cy' & bx' + (1-a)y' \\ az + ct & bz + (1-a)t \end{pmatrix}, \tag{2.2}$$

where, by singularity,

$$x't = y'z, \tag{2.3}$$

$$a(1-a) = bc. \tag{2.4}$$

Moreover, by (2.2), we get

$$x = ax' + cy', \tag{2.5}$$
$$y = bx' + (1-a)y', \tag{2.6}$$
$$az + ct = 0, \tag{2.7}$$
$$bz + (1-a)t = 0. \tag{2.8}$$

Assume by contradiction that $z \neq 0$. Therefore, from (2.5), (2.7) and (2.3), we have

$$zx = azx' + czy' = -ctx' + czy' = -c(tx' - zy') = 0,$$

and hence it must be $x = 0$, contradiction. Therefore it must be $z = 0$, and the previous conditions become

$$x't = 0, \tag{2.9}$$
$$ct = 0, \tag{2.10}$$
$$(1-a)t = 0. \tag{2.11}$$

Assume now $t \neq 0$. Then, from (2.9) we obtain $x' = 0$ and, from (2.10) we get $c = 0$. Therefore, using (2.5), we get again the contradiction $x = 0$. It follows that it must be $t = 0$.

Thus the factorization in (2.2), becomes

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} = \begin{pmatrix} ax' + cy' & bx' + (1-a)y' \\ 0 & 0 \end{pmatrix}, \tag{2.12}$$

It is worth noting that the previous construction is valid for any integral domain R and for any non-zero $x, y \in R$. The next step is to prove that $x' \neq 0$ (here the assumption that R is factorial is used). If $x' = 0$ and $y' = 0$,

we immediately get $x = y = 0$, impossible. If $x' = 0$ and $y' \neq 0$, then $x = cy'$ and $y = (1-a)y'$, hence the coprimality of x, y yields $y' \in R^*$. Thus, $c = x/y'$, $1-a = y/y'$, and then (2.4) becomes $bx = (1-y/y')y$. Since y and x are coprime, it follows that $y \mid b$, say $b = y\gamma$. Then, since x and y satisfy property **(NU)**, we get a contradiction from $1 = \gamma x + y/y'$. We conclude that $x' \neq 0$. (Let us remark that, in fact, condition **(NU)** is needed only to show that $x' \neq 0$).

Now let $p \in R$ be the greatest common divisor of a and b, say $a = pa'$ and $b = pb'$ with $\mathrm{GCD}(a', b') = 1$. Using (2.5), (2.6) and (2.4), it is easy to see that $bx = ay$, hence

$$b'x = a'y. \tag{2.13}$$

Since x, y and a', b' are coprime, it readily follows that $a' = ux$ with u a unit of R, hence (2.13) yields $b' = uy$. Moreover, from $a'(1-a) = b'c$ and a', b' coprime we get $c = \alpha a' = \alpha u x$, for some $\alpha \in R$. Thus the idempotent matrix $\mathbf{T}$ becomes

$$\mathbf{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} = \begin{pmatrix} pa' & pb' \\ c & 1-pa' \end{pmatrix} = \begin{pmatrix} pux & puy \\ \alpha ux & 1-pux \end{pmatrix}.$$

To simplify the notation, set $pu = \mu$ and $\alpha u = \lambda$, hence

$$\mathbf{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} = \begin{pmatrix} \mu x & \mu y \\ \lambda x & 1-\mu x \end{pmatrix}. \tag{2.14}$$

The condition of idempotence (2.4) leads to the equation

$$\mu x + \lambda y = 1.$$

Moreover, from (2.12) and (2.14) we get

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} (x'\mu + y'\lambda)x & x'\mu y + y'(1-\mu x) \\ 0 & 0 \end{pmatrix}$$

so that

$$\mu x' + \lambda y' = 1.$$

□

2.3.1 The case of the coordinate rings

Let us start this section with a definition. Following Cohn [15] we will say that a commutative ring R, containing a field k as a subring, is a k-ring if the group of units of R, R^*, coincides with k^*.

Dealing with coordinate rings that are non-Euclidean PID's, we will distinguish the cases of plane curves $\mathcal{C}$ over the field k such that $k[\mathcal{C}_0]$ is a k-ring and with at least two points at infinity, and that of general curves that have only one point at infinity.

When the plane curve has at least two points at infinity, using a result by Cohn [15], we will directly show that its coordinate ring R does not satisfy property (GE_2), provided R is a k-ring. Recall that (GE_2) is equivalent to (ID_2) when R is a PID.

Let k be a field, R a commutative ring containing k. Following Cohn [15], we consider a map $d : R \to \mathbb{N} \cup \{-\infty\}$ such that, for $a, b \in R$,

(d1) $d(a) = -\infty$ if and only if $a = 0$,

(d2) $d(a) = 0$ if and only if $a \in k^*$,

(d3) $d(a + b) \leq \max\{d(a), d(b)\}$,

(d4) $d(ab) = d(a) + d(b)$.

Cohn called this map *pseudo-valuation* in [14] and *degree function* in [15]. We prefer to call this map d-function to avoid confusion with the concepts of valuation and of degrees for divisors and for rational functions on curves.

Note that (d2) and (d4) show that $R^* = k^*$, hence R is a k-ring; moreover, by (d1) and (d4), R cannot contain non-trivial zero-divisors, hence it is an integral domain.

Let R be a k-ring with a d-function d. Two elements $a, b \in R$ are said to be *R-independent* if for any non-zero $c \in R$ we have

$$d(a + bc) \geq d(a), \quad d(b + ac) \geq d(b).$$

We say that a pair of elements $a, b \in R$ form a *regular row* if the couple (a, b) is the first row of a suitable 2×2 invertible matrix with entries in R.

We recall the following result by Cohn:

Proposition 2.3.2 (Proposition 7.3 of [15])**.** *Let R be a k-ring with a d-function d that satisfies the property (GE_2), and let a, b be elements of R such that $d(a) = d(b)$. If a, b form a regular row, then they cannot be R-independent.*

This result was used by Cohn to show that the ring $k[X, Y]$ of polynomials in two indeterminates over a field k does not satisfy property (GE_2).

In fact, take as a d-function on $k[X, Y]$ the total degree in X and Y, since for any non-zero polynomial $a \in k[X, Y]$,

$$d((1+XY)-aX^2) > 2 \quad \text{and} \quad d(aX^2) \geq 2,$$

then $(1+XY, X^2)$ is a regular row consisting of two elements of the same degree that are not R-dependent.

Now we focus on coordinate rings of algebraic curves. Take a smooth projective curve $\mathcal{C}$ over the perfect field k, an affine part $\mathcal{C}_0$ of $\mathcal{C}$ and the corresponding set of the points at infinity $\mathcal{C}_\infty$. For $z \in k[\mathcal{C}_0]$, let us define

$$d(z) = -\sum_{P \in C_\infty} \mathrm{ord}_P(z).$$

Lemma 2.3.3. *In the above notation, let us assume that k^* is the set of units of $R = k[\mathcal{C}_0]$ and that the points at infinity are conjugate by elements of $G_{\bar{k}/k}$. Then the map $d : R \to \mathbb{N} \cup \{-\infty\}$ is a d-function on R that satisfies the further condition* (d3') *: $d(a+b) = \max\{d(a), d(b)\}$ whenever $d(a) \neq d(b)$.*

Proof. Since the points at infinity are conjugate, the valuation $v = \mathrm{ord}_P$ on $k(\mathcal{C})$ does not depend on the choice of $P \in \mathcal{C}_\infty$: if $\mathcal{C}_\infty = \{P_1, \ldots, P_m\}$, then $\mathrm{ord}_{P_1}(F) = \cdots = \mathrm{ord}_{P_m}(F)$ for any $F \in k(\mathcal{C})$. Then the map d on R coincides with $-mv$, where $m = |\mathcal{C}_\infty|$. It is straightforward to show that $d = -mv$ satisfies properties (d1) and (d4). Indeed, the properties (d3) and (d3') hold since d is the opposite of a valuation, (d2) holds since R is a k-ring. To conclude we remark that the map d actually takes values in $\mathbb{N} \cup \{-\infty\}$. Any element $z \in k[\mathcal{C}_0] \setminus \{0\}$ has no poles outside $\mathcal{C}_\infty$, therefore $\mathrm{ord}_P(z) \geq 0$ for all $P \in \mathcal{C}_0$. Then, from Proposition 1.3.11, it follows that $d(z) = -\sum_{P \in \mathcal{C}_\infty} \mathrm{ord}_P(z) = \sum_{P \in \mathcal{C}_0} \mathrm{ord}_P(z) \geq 0$ for any non-zero $z \in k[\mathcal{C}_0]$. □

Lemma 2.3.4. *Let $R = k[\mathcal{C}_0]$ be the coordinate ring of the smooth curve $\mathcal{C}$ of genus $g = 0$ over the field k. Then R is a k-ring if and only if all the points at infinity of $\mathcal{C}$ are conjugate by elements of the Galois group $G_{\bar{k}/k}$.*

Proof. Let R be a k-ring. We firstly assume, for a contradiction, that the set $\mathcal{C}_\infty$ of the points at infinity has two distinct conjugate classes, say C_1 and C_2, containing m_1, m_2 points respectively. Then the k-rational divisor at infinity $D = m_2 \sum_{P \in C_1} P_1 - m_1 \sum_{Q \in C_2} Q$ has degree zero. Since $\mathcal{C}$ has genus zero, its Jacobian is 0 and, as a consequence, $\mathrm{Pic}^0_k(\mathcal{C})$ vanishes and we get that every k-rational divisor of degree zero is a principal divisor. Therefore, there exists $z \in k(\mathcal{C}_0)$ such that $\mathrm{div}(z) = D$. Then the zeroes of z lie in $\mathcal{C}_\infty$, hence z is a unit of R since z^{-1} has poles in $\mathcal{C}_\infty$ and thus $z^{-1} \in R$. However, z cannot lie in k, since $\mathrm{div}(z) \neq 0$. We reached a contradiction.

Conversely, let us assume that the points at infinity are conjugate. Then any nonzero rational divisor at infinity has the form $m \sum_{P \in \mathcal{C}_\infty} P$, for some

$m \in \mathbb{Z} \setminus \{0\}$. Let a be a unit of R. Then a has no zeroes in $\mathcal{C}_0$, otherwise $a^{-1} \in R^*$ would have poles in $\mathcal{C}_0$, impossible. Hence $\mathrm{div}(a)$ is a divisor at infinity which is also k-rational. Then $\deg(\mathrm{div}(a)) = 0$ implies $\mathrm{ord}_P(a) = 0$ for every $P \in \mathcal{C}_\infty$ i.e. $\mathrm{div}(a) = 0$, hence $a \in k^*$. □

The preceding lemmas allow us to use Cohn's result (Proposition 2.3.2) to prove the following theorem.

Theorem 2.3.5. *Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane smooth curve of genus $g = 0$ over the field k having two points at infinity, and assume that its coordinate ring R is a k-ring. Then R does not satisfy property (GE_2).*

Proof. Since R is a k-ring, by Lemma 2.3.4, the points at infinity are conjugate by elements of the Galois group $G_{\bar{k}/k}$ and no one of them is rational over k. Therefore we can apply Lemma 2.3.3 and show that the map $d = -\sum_{i=1}^{2} \mathrm{ord}_{P_i}$ is a d-function.

Let $F(x, y) = 0$ be the defining equation of $\mathcal{C}_0$, where $F \in k[x, y]$ is a polynomial of degree 2; we assume, without loss of generality, that $F(0, 0) \neq 0$. Let $F_2(x, y)$ be the homogeneous component of F of degree 2. Since the points at infinity are conjugate and not rational, it follows that $F_2(X, Y) = c\prod_{i=1}^{2}(Y - \alpha_i X)$, where $c \in k$, $\alpha_i \in \bar{k} \setminus k$, and $P_i = (1, \alpha_i, 0)$, with $i \in \{1, 2\}$, are the points at infinity. Now we consider the elements x, y of R. Since $F(0, 0) \neq 0$, it is clear that x, y form a regular row. Taking homogeneous coordinates, it is straightforward to verify that $d(x) = d(y)$. Let us verify that x, y are R-independent. Take any nonzero $c \in R$. If $c \notin k^*$, than $d(c) > 0$ and so $d(x + yc) > d(x), d(y + xc) > d(y)$ by the properties of the d-function. If $c \in k^*$, it is easily seen that $d(x + yc) = d(x) = d(y) = d(y + xc)$. We are in the position to apply Proposition 2.3.2, hence we conclude that R does not satisfy property (GE_2). □

Corollary 2.3.6. *Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane smooth curve of genus zero over k, such that its coordinate ring $R = k[\mathcal{C}_0]$ is a non-Euclidean PID. Then R does not satisfy property (GE_2).*

Proof. By Corollary 2.1.2, $\mathcal{C}$ has no rational points, hence the two points at infinity are necessarily conjugate. Then R is a k-ring by Lemma 2.3.4, and we conclude by Theorem 2.3.5. □

Now we focus on the case of genus ≥ 1. In the notation of Section 2, we have to prove that the non-Euclidean PID $R := k[x, y] = k[E_0]$, with $E(k) = O$, does not satisfy property (ID_2).

Actually, we will prove a more general result, namely, for every smooth curve $\mathcal{C}$ of genus ≥ 1 and with a unique point at infinity, if the coordinate

ring $R = k[\mathcal{C}_0]$ is a PID, then R does not satisfy property (ID_2). In this way we will also cover the cases mentioned in Remark 3.

We will need a preliminary lemma, that follows from a corollary of the Riemann-Roch Theorem. We give the proof for the sake of completeness.

Lemma 2.3.7. *Let $k(\mathcal{C})$ be the field of functions of an affine smooth curve $\mathcal{C}_0$ over the field k. If P_∞ is a rational point at infinity of the corresponding projective curve $\mathcal{C}$, then, for every positive integer m large enough, there exists $z \in k(\mathcal{C})$ such that $ord_{P_\infty}(z) = -m$.*

Proof. Say P_∞ is the rational point at infinity of the curve. As usual, for D a k-rational divisor over $\mathcal{C}$, we denote by $l(D)$ the dimension of the k-vector space $L(D) = \{z \in F : \mathrm{div}(z) + D \geq 0\} \cup \{0\}$. By Corollary 1.3.19 (c) of the Riemann-Roch Theorem, we know that there exists an integer $c \geq 0$ such that $l(D) = \deg(D) + 1 - g$, whenever $\deg(D) > c$. Let us take any positive integer m such that $m - 1 > c$, and consider the divisors $D_1 = (m-1)P_\infty$ and $D_2 = mP_\infty$. Both D_1 and D_2 have degrees $> c$, then $\ell(D_1) = \ell(D_2) - 1$. Hence $L(D_1)$ is a proper subspace of $L(D_2)$, and we may take $z \in L(D_2) \setminus L(D_1)$. It follows that $\mathrm{ord}_{P_\infty}(z) \geq -m$. On the other hand, $\mathrm{ord}_{P_\infty}(z) < -m-1$, otherwise $\mathrm{div}(z) + D_1 \geq 0$, impossible, since $z \notin L(D_1)$. We conclude that $\mathrm{ord}_{P_\infty}(z) = -m$. □

Now we consider any smooth curve $\mathcal{C}$ over k of genus $g \geq 1$ and with a unique point at infinity, say P_∞. Let R and $k(C)$ be, respectively, the coordinate ring and the function field of the affine curve $\mathcal{C}_0$. Since $\mathcal{C}$ has a unique point at infinity, an argument as the one that opens the proof of Theorem 2.1.4, shows that R is a k-ring. Therefore by Lemma 2.3.3 the function $d : k(\mathcal{C}_0)^* \to \mathbb{Z}$, defined by $d(z) = -\mathrm{ord}_{P_\infty}(z)$, satisfies properties (d3), (d3') and (d4). Note that, if $\eta \in R$, the degree of η as a rational function coincides with $d(\eta)$, and if $\eta \notin k$ then $d(\eta) = \deg(\eta) > 1$, since $\mathcal{C}$ is not a rational curve.

Lemma 2.3.8. *Let $\mathcal{C}$ be a smooth curve of genus ≥ 1, with a unique point at infinity, R and $k(\mathcal{C})$ the coordinate ring and the field of functions of the affine curve $\mathcal{C}_0$, respectively. Then there exist $\eta, \xi \in R$ such that $d(\eta) = d(\xi) + 1$. If R is a PID, then η, ξ may be chosen to be coprime.*

Proof. The point at infinity, say P_∞, is rational since it is unique. By Lemma 2.3.7, there exist $m > 0$ and $z, z' \in F$ such that $\mathrm{ord}_{P_\infty}(z) = -m$ and $\mathrm{ord}_{P_\infty}(z') = -m - 1$. Say $z = \xi/t$, $z' = \eta/t$, for suitable $\eta, \xi, t \in R$. Then $\mathrm{ord}_{P_\infty}(\eta) = \mathrm{ord}_{P_\infty}(\xi) - 1$, hence $d(\eta) = d(\xi) + 1$, since $d = -\mathrm{ord}_{P_\infty}$, under the present hypotheses.

The last statement is obvious. □

Lemma 2.3.9. *Let the notation be as above. If η and ξ are elements of R such that $|d(\eta) - d(\xi)| = 1$, then they satisfy property* **(NU)**.

Proof. We firstly observe that $\eta, \xi \notin k$. In fact η and ξ are both nonzero, and, if $d(\eta) = 0$, say, then we get $d(\xi) = 1$, impossible. By symmetry, we may assume $d(\eta) = m$ and $d(\xi) = m + 1$, with m positive integer greater than 1.

Assume by contradiction that there exist $\alpha \in k^*$ and $\omega \in R$ such that $\alpha\eta + \omega\xi = 1$. Therefore it must be $d(\alpha\eta + \omega\xi) = 0$, but this is impossible by (d3'), since $d(\alpha\eta + \omega\xi) = \max\{d(\alpha\eta), d(\omega\xi)\} = d(\omega\xi) \geq m + 1$.

On the other hand, if there exist $\alpha \in k^*$ and $\omega \in R$ such that $\omega\eta + \alpha\xi = 1$, then from $d(\omega\eta + \alpha\xi) = 0$, and (d3') we get $d(\omega) = 1$, again impossible. □

Lemma 2.3.10. *Let $\eta, \xi, \mu, \lambda, \eta', \xi'$ be elements of R such that:*

(a) $\mu\eta + \lambda\xi = 1$;

(b) $\mu\eta' + \lambda\xi' = 1$.

If $|d(\eta) - d(\xi)| = 1$, then also $|d(\eta') - d(\xi')| = 1$. In particular, η' and ξ' satisfy property **(NU)**.

Proof. It is not restrictive to assume that $d(\xi) = d(\eta) + 1$. By properties (d3') and (d4), from (a) we readily get $d(\mu) = d(\lambda) + 1$, so that, from (b), we derive $d(\xi') = d(\eta') + 1$. The last statement follows from Lemma 2.3.9. □

Finally we can prove the following

Theorem 2.3.11. *Let $\mathcal{C}$ be a smooth curve of genus ≥ 1 with a unique point at infinity. If the coordinate ring $R = k[\mathcal{C}_0]$ of the affine curve $\mathcal{C}_0$ is a PID, then R does not satisfy property (ID_2).*

Proof. Assume, for a contradiction, that R satisfies property (ID_2) and let

$$\mathcal{A} = \{(\eta, \xi) \in R \times R : \eta \text{ and } \xi \text{ are coprime and } |d(\eta) - d(\xi)| = 1\}.$$

By Lemma 2.3.8 we get $\mathcal{A} \neq \emptyset$. For every $(\eta, \xi) \in \mathcal{A}$ we consider the singular matrix $S_{\eta,\xi} = \begin{pmatrix} \eta & \xi \\ 0 & 0 \end{pmatrix}$. It is worth noting that $S_{\eta,\xi}$ could be idempotent only if $\eta = 1$, so that $d(\xi) = 1$. Since R has no elements of degree one, it follows that no matrix $S_{\eta,\xi}$ is idempotent.

We define the *length of factorization* of $S_{\eta,\xi}$ as the minimum number of idempotent matrices into which $S_{\eta,\xi}$ can be factorized. Let $m \geq 2$ be the

smallest integer in the set of the length of the factorizations of these matrices, and assume that $S_{\eta,\xi}$ has length of factorization m. Hence we may write

$$\begin{pmatrix} \eta & \xi \\ 0 & 0 \end{pmatrix} = \mathbf{T}_1 \cdot \cdots \cdot \mathbf{T}_{m-1} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}, \tag{2.15}$$

where $\mathbf{T}_1, \ldots, \mathbf{T}_{m-1}$ and $\mathbf{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ are idempotent matrices on R. Let $\mathbf{S} = \mathbf{T}_1 \cdot \cdots \cdot \mathbf{T}_{m-1} = \begin{pmatrix} \eta' & \xi' \\ \sigma & \tau \end{pmatrix}$. With this notation, we can rewrite (2.15) as

$$\begin{pmatrix} \eta & \xi \\ 0 & 0 \end{pmatrix} = \mathbf{S} \cdot \mathbf{T} = \begin{pmatrix} \eta' & \xi' \\ \sigma & \tau \end{pmatrix} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix} \tag{2.16}$$

where $\mathbf{S}$ is singular. It follows from Lemma 2.3.1 that $\mathbf{S} = \begin{pmatrix} \eta' & \xi' \\ 0 & 0 \end{pmatrix}$, with $\eta' \neq 0$, and there exist $\lambda, \mu \in R$ such that

$$\mu\eta + \lambda\xi = 1, \tag{2.17}$$

and

$$\mu\eta' + \lambda\xi' = 1. \tag{2.18}$$

It follows from Lemma 2.3.10 and (2.17), (2.18), that η' and ξ' are coprime elements of R such that $|d(\eta') - d(\xi')| = 1$. Therefore $(\eta', \xi') \in \mathcal{A}$ and the length of factorization of $S_{\eta',\xi'}$ is $\leq m-1$. We reached a contradiction, since m was minimum. □

By Theorem 2.3.11 and O'Meara result in [48] (see Theorem 1.2.3), we immediately get the following

Corollary 2.3.12. *In the above notation, if $R = k[\mathcal{C}_0]$ is a PID, then it does not admit a weak algorithm; in particular, it is never Euclidean.*

The above corollary automatically shows that, in the case of the affine elliptic curve E_0 without rational points, the PID $k[E_0]$ cannot be Euclidean. So the last part of the proof of Theorem 2.1.4 should not be necessary, *a priori*.

Remark 4. In Brown's paper [7], statement of Theorem 1.1, one finds a list of four principal ideal domains that are not Euclidean, namely

$$R_1 = \mathbb{F}_2[X,Y]/(Y^2 + Y + X^3 + X + 1) \ ; \ R_2 = \mathbb{F}_3[X,Y]/(Y^2 - X^3 + X + 1);$$

$$R_3 = \mathbb{F}_4[X,Y]/(Y^2 + Y + X^3 + \eta) \ ; \ R_4 = \mathbb{F}_2[X,Y]/(Y^2 + Y + X^5 + X^3 + 1),$$

where η is a generator of $\mathbb{F}_4^*$. Recall that the above rings were firstly found and examined by MacRae in [43]. MacRae in his paper proved that these rings are unique factorization domains, but he did not specify that they are not Euclidean. Since R_1–R_3 are the rings of smooth curves with genus 1 and a unique point at infinity, they do not satisfy property (ID_2), by Theorem 2.3.11. On the other hand, the curve $\mathcal{C}_4$ of equation $y^2 + y + x^5 + x^3 + 1 = 0$ on $\mathbb{F}_2$ has a singular point at infinity, so we cannot directly apply the above arguments to the coordinate ring R_4. However, we can fix this case defining a d-function d on R_4. We just set $d(x) = 2$, $d(y) = 5$, $d(1) = 0$ and extend in the obvious way these assignments to any $f(x, y) \in R_4$. A straightforward computation shows that R_4 is a $\mathbb{F}_2$-ring, and that d satisfies the conditions (d1)–(d4) and (d3'). Then $d(y) = d(x^2)+1$, and, by an immediate adaptation of Lemmas 2.3.9 and 2.3.10, the proof of Theorem 2.3.11 shows that also R_4 does not satisfy property (ID_2).

2.3.2 The case of Anderson's PID's

Our final aim is to prove that an Anderson's PID does not satisfy property (ID_2). Equivalently, by Ruitenburg's results in [52], it does not satisfy property (GE_2).

So we take any Anderson's PID, say $D_f = D[1/f]$, where D is a two-dimensional UFD, and f is a prime element of D contained in the Jacobson radical $J(D)$.

We start showing that it is not restrictive to assume D to be local, i.e. a maximal ideal $\mathfrak{M}$ of D to be the unique maximal ideal of D. Note that, since $f \in J(D)$, then f remains a prime element of the localization $D_{\mathfrak{M}}$.

Lemma 2.3.13. *In the above notation, if the PID $D_{\mathfrak{M}}[1/f]$ does not satisfy (ID_2), then also D_f does not satisfy (ID_2).*

Proof. We have

$$D_f \setminus \{0\} = \{f^k r : k \in \mathbb{Z}, r \in D, r \notin fD\}$$

and

$$D_{\mathfrak{M}}[1/f] \setminus \{0\} = \{f^k a/b : k \in \mathbb{Z}, a, b \in D, a \notin fD, b \notin \mathfrak{M}\}.$$

Then it is readily seen that $D_{\mathfrak{M}}[1/f] = (D_f)_S$, where $S = D \setminus \mathfrak{M}$.

Now let us assume, for a contradiction, that D_f satisfies (ID_2). Equivalently, it satisfies (GE_2). Then Theorem 1.2.3 shows that D_f admits a weak algorithm. Since $D_{\mathfrak{M}}[1/f] = (D_f)_S$ is a localization of D_f, we infer that also $D_{\mathfrak{M}}[1/f]$ admits a weak algorithm. It follows that $D_{\mathfrak{M}}[1/f]$ satisfies (GE_2), again by Theorem 1.2.3, hence it satisfies (ID_2), impossible. □

In view of Lemma 2.3.13, in the remainder of this section D will denote a local two-dimensional UFD, with maximal ideal $\mathfrak{M}$, and f a prime element of D. We will assume that D_f is an Anderson's PID, which means that either D is regular and $f \in \mathfrak{M}^2$, or D is not regular (see Theorem [1]). It follows that $\mathfrak{M}$ cannot be a principal ideal of D, otherwise we should get $\mathfrak{M} = fD$, since f is a prime element. Then D, being a local UFD, is actually a DVR, so D is one-dimensional, against our assumption.

Let us verify that there exist $X, Y \in \mathfrak{M} \setminus \mathfrak{M}^2$ such that

$$\alpha X + \beta Y \notin fD \tag{2.19}$$

whenever either α or β is a unit of D.

We distinguish the cases where $f \in \mathfrak{M}^2$, and $f \notin \mathfrak{M}^2$ (the latter case is possible only when D is not regular).

Let $f \in \mathfrak{M}^2$. Since $\mathfrak{M}$ is not a principal ideal, by Nakayama's Lemma we get $\dim_{D/\mathfrak{M}}(\mathfrak{M}/\mathfrak{M}^2) \geq 2$. So we may take $X, Y \in \mathfrak{M}$ such that $\{X + \mathfrak{M}^2$, $Y + \mathfrak{M}^2\}$ are linearly independent in $\mathfrak{M}/\mathfrak{M}^2$. Then $\alpha X + \beta Y \in fD \subset \mathfrak{M}^2$ yields $\alpha, \beta \in \mathfrak{M}$.

Now we assume that $f \notin \mathfrak{M}^2$, so D is not regular, hence a set of generators of $\mathfrak{M}$ has at least three elements. We may take $X \in \mathfrak{M} \setminus \mathfrak{M}^2$ such that the ideal $\langle f, X\rangle$ is not principal. Then $\{X+\mathfrak{M}^2$, $f+\mathfrak{M}^2\}$ are linearly independent in $\mathfrak{M}/\mathfrak{M}^2$. Since $\mathfrak{M}$ is not two-generated, we may take $Y \in \mathfrak{M} \setminus \mathfrak{M}^2$ such that $Y \notin \langle f, X\rangle$. Let us pick $\alpha, \beta \in R$ such that $\alpha X + \beta Y \in fD$. Then, necessarily, $\beta \in \mathfrak{M}$, since $Y \notin \langle f, X\rangle$, and therefore also $\alpha \in \mathfrak{M}$, since f, X are linearly independent modulo $\mathfrak{M}^2$.

Recall that any element r of D_f may be uniquely written as $r = f^k a$, where $k \in \mathbb{Z}$ and $a \in D$ is coprime with f, as elements of D. Moreover, $r \in D_f^*$ if and only if $a \in D^*$. We consider the f-adic valuation v_f on the field $Q = \mathrm{Frac}(D_f) = \mathrm{Frac}(D)$, and focus on its restriction to D_f. Under the present notation, we have $v_f(r) = v_f(f^k a) = k$.

Definition 2.3.14. Let $x, y, \in D_f$ and $\tilde{\omega}_1, \tilde{\omega}_2 \in D$. We will say that x and y satisfy property **(*)** if:

(a) x, y are non-units of D_f,

(b) $v_f(x) = v_f(y)$,

(c) $v_f(\tilde{\omega}_1 x + \tilde{\omega}_2 y) > v_f(x) \Rightarrow \tilde{\omega}_1, \tilde{\omega}_2 \in \mathfrak{M}$.

It is worth noting that condition (c) is equivalent to

(c') $v_f(\tilde{\omega}_1 x + \tilde{\omega}_2 y) = v_f(x) = v_f(y)$, when either $\tilde{\omega}_1$ or $\tilde{\omega}_2$ is a unit of D.

The proof of our final Theorem 2.3.17 is based on two crucial lemmas.

Lemma 2.3.15. *In the above notation, if $x, y \in D_f$ satisfy property* (*)*, then they also satisfy property* **(NU)**.

Proof. Assume that x, y satisfy property (*), and let

$$\omega_1 x + \omega_2 y = 1, \tag{2.20}$$

with $\omega_1, \omega_2 \in D_f$. To verify that **(NU)** holds, we must show that $\omega_1, \omega_2 \notin D_f^*$. Set $x = f^k\tilde{x}$, $y = f^k\tilde{y}$, $\omega_1 = f^h\tilde{\omega}_1$, $\omega_2 = f^l\tilde{\omega}_2$, with $k, h, l \in \mathbb{Z}$, $\tilde{x}, \tilde{y} \in \mathfrak{M} \setminus fD$ and $\tilde{\omega}_1, \tilde{\omega}_2 \in D \setminus fD$.
Considering the valuation v_f on (2.20), we obtain

$$0 \geq \min\{h + k, l + k\}$$

and we can analyze all the possible cases:

(1) $h + k = 0$, $l + k > 0$.
This case is impossible since it leads to the contradiction $\tilde{\omega}_1\tilde{x} + f^{l+k}\tilde{\omega}_2\tilde{y} = 1 \in \mathfrak{M}$.

(2) $l + k = 0$, $h + k > 0$.
Here we get $f^{h+k}\tilde{\omega}_1\tilde{x} + \tilde{\omega}_2\tilde{y} = 1 \in \mathfrak{M}$, contradiction.

(3) $h + k = l + k = 0$.
Analogously to the previous cases, we get a contradiction since (2.20) becomes $\tilde{\omega}_1\tilde{x} + \tilde{\omega}_2\tilde{y} = 1 \in \mathfrak{M}$.

(4) $0 > h + k = l + k$.
This is the only case that may actually happen. The equality (2.20) becomes $\tilde{\omega}_1\tilde{x} + \tilde{\omega}_2\tilde{y} = f^{-h-k}$, where $-h - k > 0$.

Therefore, $v_f(\omega_1) = v_f(\omega_2) = h < -k$ and (2.20) becomes $\tilde{\omega}_1 x + \tilde{\omega}_2 y = f^{-h}$, i.e. $v_f(\tilde{\omega}_1 x + \tilde{\omega}_2 y) = -h > k$. Since x and y satisfy property (*), from (c) we get $\tilde{\omega}_1, \tilde{\omega}_2 \in \mathfrak{M}$, and therefore $\omega_1, \omega_2 \notin D_f^*$, as required. □

Remark 5. It follows from condition (2.19) that, given any Anderson's PID D_f there always exist two elements X, Y of the maximal ideal $\mathfrak{M}$ that satisfy property (*) and then also property (NU).

Lemma 2.3.16. *In the above notation, let $x, y, \mu, \lambda, x', y'$ be elements of D_f such that:*

(i) $\mu x + \lambda y = 1$;

(ii) $\mu x' + \lambda y' = 1$.

If x and y satisfy property **(*)**, then also x' and y' do.

Proof. Assume that x and y satisfy property **(*)**. Since, by Lemma 2.3.15, they also have property (NU), from $\mu x + \lambda y = 1$ it follows that $\mu, \lambda \notin D_f^*$. Moreover, being $v_f(x) = v_f(y)$, it must be $v_f(\mu) = v_f(\lambda) < -v_f(x)$. Set $x = f^k\tilde{x}$, $y = f^k\tilde{y}$, $\mu = f^a\tilde{\mu}$, $\lambda = f^a\tilde{\lambda}$, with $\tilde{x}, \tilde{y}, \tilde{\mu}, \tilde{\lambda} \in \mathfrak{M} \setminus fD$ and $a < -k$. Condition (i) can be now rewritten as

$$\tilde{\mu}\tilde{x} + \tilde{\lambda}\tilde{y} = f^{-a-k}, \tag{2.21}$$

with $-a - k > 0$, so that

$$\tilde{\mu}\tilde{x} + \tilde{\lambda}\tilde{y} \equiv 0 \mod f. \tag{2.22}$$

Moreover, since $v_f(\mu) = v_f(\lambda)$, it follows from condition (ii), that $v_f(x') = v_f(y') < -v_f(\mu)$. If we set $x' = f^K\tilde{x}'$ and $y' = f^K\tilde{y}'$, with $\tilde{x}', \tilde{y}' \in D \setminus fD$, then we can rewrite condition (ii) as

$$\tilde{\mu}\tilde{x}' + \tilde{\lambda}\tilde{y}' = f^{-a-K}, \tag{2.23}$$

with $-a - K > 0$, i.e.

$$\tilde{\mu}\tilde{x}' + \tilde{\lambda}\tilde{y}' \equiv 0 \mod f. \tag{2.24}$$

We want to prove that x' and y' satisfy property (*). We already know that $v_f(x') = v_f(y') = K$, and now we want to show that if $v_f(\tilde{\omega}_1 x' + \tilde{\omega}_2 y') > K$, with $\tilde{\omega}_1, \tilde{\omega}_2 \in D$, then $\tilde{\omega}_1, \tilde{\omega}_2 \in \mathfrak{M}$.

Assume by contradiction that $\tilde{\omega}_1 \in D^* = D \setminus \mathfrak{M}$ and that $v_f(\tilde{\omega}_1 x' + \tilde{\omega}_2 y') > K$. This is equivalent to say that

$$\tilde{\omega}_1\tilde{x}' + \tilde{\omega}_2\tilde{y}' \equiv 0 \mod f$$

with $\tilde{\omega}_1 \in U(D)$, or that

$$\tilde{x}' + \tilde{\omega}\tilde{y}' \equiv 0 \mod f \tag{2.25}$$

with $\tilde{\omega} \in D$. Multiplying (2.25) by $\tilde{\mu}$ and using (2.22), we obtain

$$\tilde{y}'(-\tilde{\lambda} + \tilde{\omega}\tilde{\mu}) \equiv 0 \mod f$$

and, since $\tilde{y}' \notin fD$,

$$\tilde{\lambda} \equiv \tilde{\omega}\tilde{\mu} \mod f.$$

Consequently, (2.22) becomes

$$\tilde{\mu}(\tilde{x} + \tilde{\omega}\tilde{y}) \equiv 0 \mod f.$$

Since $\tilde{\mu} \notin fD$, then

$$\tilde{x} + \tilde{\omega}\tilde{y} \equiv 0 \mod f$$

and

$$v_f(x + \tilde{\omega}y) = k + v_f(\tilde{x} + \tilde{\omega}\tilde{y}) > k.$$

But this is a contradiction because, since x and y satisfy property (*), (c') shows that $v_f(x + \tilde{\omega}y) = k$. By symmetry, we find a contradiction also assuming $\omega_2 \in D_f^*$.

It remains to prove that $x', y' \notin D_f^*$. Assume by contradiction that $x' \in D_f^*$, the case $y' \in D_f^*$ is analogous. From condition (ii), multiplying by $(x')^{-1} = f^{-K}(\tilde{x}')^{-1}$, we get

$$\tilde{\mu} = f^{-a-K}(\tilde{x}')^{-1} - \tilde{\lambda}(\tilde{x}')^{-1}\tilde{y}'.$$

Multiplying by $\tilde{x}$ and using (2.21), we get

$$f^{-a-K}(\tilde{x}')^{-1}\tilde{x} - \tilde{\lambda}((\tilde{x}')^{-1}\tilde{y}'\tilde{x} - \tilde{y}) = f^{-a-k}, \tag{2.26}$$

with $-a - K > 0$ and $-a - k > 0$. It follows that $\tilde{\lambda}((\tilde{x}')^{-1}\tilde{y}'\tilde{x} - \tilde{y}) \in fD$. But x and y satisfy property (*), so $v_f((\tilde{x}')^{-1}\tilde{y}'\tilde{x} - \tilde{y}) = 0$, and, by definition, $v_f(\tilde{\lambda}) = 0$. We reached a contradiction. □

We state our last result in the most general form (i.e. D is not necessarily local), even though in the proof we will assume D to be local, by Lemma 2.3.13.

Theorem 2.3.17. *Let D be a two-dimensional UFD, that contains a prime element $f \in J(D)$. Then the Anderson's PID $D_f = D[1/f]$ does not satisfy property (ID$_2$).*

Proof. By Lemma 2.3.13, we may assume that D is local with maximal ideal $\mathfrak{M}$.

The argument is similar to the proof of Theorem 2.3.11. Assume by contradiction that D_f satisfies property (ID$_2$) and let

$$\mathcal{B} = \{(\alpha, \beta) \in D_f \times D_f : \alpha \text{ and } \beta \text{ are coprime and satisfy (*)}\}.$$

As observed in Remark 5, there always exist X and Y, coprime elements of D_f satisfying (*), thus $\mathcal{B} \neq \emptyset$.

For any $(x, y) \in \mathcal{B}$ consider the singular matrix $S_{x,y} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$. Note that $S_{x,y}$ is not idempotent, otherwise $x = 1$ and $y = 0$, while the couple $(1, 0) \notin \mathcal{B}$.

We define the *length of factorization* of $S_{x,y}$ as the minimum number of idempotent matrices into which $S_{x,y}$ can be factorized. Let $n \geq 2$ be the

smallest integer in the set of the length of the factorizations of these matrices, and assume that $S_{x,y}$ has length of factorization n. Hence we may write

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \mathbf{T}_1 \cdot \cdots \cdot \mathbf{T}_{n-1} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}, \tag{2.27}$$

where $\mathbf{T}_1, \ldots, \mathbf{T}_{n-1}$ and $\mathbf{T} = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ are idempotent matrices on D_f, and set $\mathbf{S} = \mathbf{T}_1 \cdot \cdots \cdot \mathbf{T}_{n-1} = \begin{pmatrix} x' & y' \\ s & t \end{pmatrix}$.

With this notation, we can rewrite (2.27) as

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \mathbf{S} \cdot \mathbf{T} = \begin{pmatrix} x' & y' \\ s & t \end{pmatrix} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}, \tag{2.28}$$

that, from Lemma 2.3.1 becomes

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \mathbf{S} \cdot \mathbf{T} = \begin{pmatrix} x' & y' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix},$$

with $x' \neq 0$. Moreover, there exist $\lambda, \mu \in D_f$ such that

$$\mu x + \lambda y = 1, \tag{2.29}$$

and

$$\mu x' + \lambda y' = 1. \tag{2.30}$$

It follows from Lemma 2.3.16 and (2.29), (2.30), that x' and y' are elements of D_f satisfying property **(*)**. Moreover, by (2.30), they are also coprime. Therefore $(x', y') \in \mathcal{B}$ and the length of factorization of $\mathbf{S} = S_{x',y'}$ is $\leq n-1$, a contradiction. □

As above, we remark that Theorem 2.3.17, together with Theorem 1.2.3, shows that an Anderson's PID cannot be Euclidean, with no need of Theorem 2.2.2.

CHAPTER 3

PRINC DOMAINS

In Section 4 of [53], the authors considered the problem to understand when the fact that any singular matrix over an integral domain R is a product of idempotents implies that R is a Bézout domain. While dealing with this subject, they were led to introduce the property (princ) and the notion of PRINC domain. Actually, they proved that any PRINC domain satisfying property (ID_2) must be a Bézout domain. Let us give the definitions.

Two elements $a, b \in R$ are said to form an *idempotent pair* if they can occur as a row, or as a column, of a 2×2 singular idempotent matrix. In view of Proposition 1.1.3, that gives the standard form of a 2-dimensional non-identity idempotent matrix over R, this is equivalent to say that $a, b \in R$ form an idempotent pair if and only if either $a(1-a) \in bR$ or $b(1-b) \in aR$.

We will say that an integral domain R satisfies the property *(princ)* if every ideal generated by an idempotent pair is principal. In this case we'll say, for short, that R is a *PRINC* domain.

In this chapter we recall the main results on PRINC domains contained in [53] and in the subsequent [49], and we answer, or give a partial answer, to some questions posed in these papers.

Moreover, we investigate how PRINC domains are related to the notion of *unique comaximal factorization domain* (UCFD) introduced in [45].

3.1 PRINC domains and the property (ID_2)

In this section, we present the main results of [53] on PRINC domains, that relate this new notion with the factorization property (ID_2), and we give an

example of PRINC domain that fails to be projective-free and factorial thus answering a question in [49].

Let us start by showing that unique factorization domains and projective-free domains, in particular local domains, are examples of integral domains satisfying (princ). For further details we refer to [53] and [49].

Lemma 3.1.1. *If $a, b \in R$ form an idempotent pair, then the ideal $\langle a, b\rangle$ is invertible.*

Proof. We can assume without loss of generality that $a(1-a) \in bR$, say $a(1-a) = bc$, with $c \in R$. Then, since

$$\langle a, b\rangle\langle 1-a, b\rangle = \langle bc, ab, b(1-a), b^2\rangle = b\langle c, a, 1-a, b\rangle = bR,$$

the ideal $\langle a, b\rangle$ is invertible. □

Recall that an integral domain R is said to be a *Bézout domain* if every finitely generated ideal of R is principal, and that R is called *projective-free* if every finitely generated projective R-module is free. We also recall that an R-module P is said to be projective if and only if it is the direct summand of a free R-module, i.e. if and only if there exist a free R-module F and another R-module M such that $F = P \oplus M$.

Proposition 3.1.2. *If R is either a Bézout domain, or a UFD, or a projective-free domain, then it is also a PRINC domain.*

Proof. A Bézout domain R is obviously a PRINC domain; since every finitely generated ideal of R is principal, so is every ideal generated by an idempotent pair. If R is a UFD, then its invertible ideals are free, hence principal (see [25], or, more explicitly [49, Lemma 1.2]). Thus R satisfies the property (princ) by Lemma 3.1.1. Finally, since an ideal of a domain R is projective (as R-module) if and only if it is invertible (see [51, Prop. 4.21] or [3, pag. 458]), if R is a projective-free domain, then every ideal I of R generated by an idempotent pair is principal. □

Corollary 3.1.3. *Every local domain R is a PRINC domain.*

Proof. Every local domain is projective-free (see [23, Th. 1.9, p. 198]). □

It is worth observing that there exist unique factorization domains that are not projective-free.

Example 3.1.4. The coordinate ring of the 2-dimensional real sphere

$$D = \frac{\mathbb{R}[X_1, X_2, X_3]}{\left\langle \sum_{i=1}^{3} X_i^2 - 1 \right\rangle},$$

where X_1, X_2, X_3 are indeterminates over the real numbers $\mathbb{R}$, is a factorial domain (cf. [55, Prop. 8.3]) that is not projective-free. This fact can be seen in the following way: let $F = \bigoplus_{i=1}^{3} De_i$, where the e_i's are the canonical basis vectors for D^3, and consider the D-epimorphism

$$\phi_0 : F \to D,$$

defined, as in [39, Ex. 2.10], by $\phi_0(e_i) = X_i$, with $i \in \{1, 2, 3\}$. If we set $P_0 = \mathrm{Ker}\phi_0$, then $F \cong P_0 \oplus D$ and P_0, as direct summand of a free module, is a finitely generated projective R-module of rank 2. It has been proved using different techniques (cf. [37, 61]) that P_0 is not a free module, and therefore D is not a projective-free domain.

A natural problem that arises from Proposition 3.1.2, and that was also proposed in [49], is to find an example of PRINC domain that is neither projective-free, nor factorial. An example of this kind of domain, as observed by the authors of [49], was exhibited for other purposes in Section 4 of [45].

We give now a simpler example of PRINC domain non-UFD and non-projective-free: a pull-back of the real coordinate ring of the 2-dimensional sphere D, as in example 3.1.4.

In order to get the proof, we will need some preliminary results.

In the following lemma, we give a direct proof that PRINC domains can be easily constructed via pull-backs.

Lemma 3.1.5. *Let D be a PRINC domain, Q its field of fractions and X an indeterminate. Then the pull-back $R = D + XQ[\![X]\!]$ is a PRINC domain.*

Proof. Let $J = XQ[\![X]\!]$ be the Jacobson radical of R and let r be any element of R. It can be easily verified that, if $r \in J$, then $r = qX^k u$ for suitable $q \in Q$, $k > 0$ and $u \in R^*$, while, if $r \notin J$, then $r = sw$, for suitable $s \in D$ and $w \in R^*$. Let us pick two elements $a, b \in R$ that form an idempotent pair, say $a(1-a) = br$ for a $r \in R$, and prove that the ideal that they generate is principal. We distinguish three cases.

Assume that $a \in J$ and $b \notin J$, or viceversa. Then one element divides the other, thus the ideal $\langle a, b \rangle$ is principal.

Assume that both a, b are elements of J, say $a = q_1 X^k u$ and $b = q_2 X^h w$ with $q_1, q_2 \in Q$, $h, k > 0$ and u, w units of R. If $k \neq h$, then one element

divides the other and we conclude as in the previous case. If $k = h$, then we have $a = q\bar{u}b$, with $q \in Q$ and $\bar{u} \in R^*$. Set $q = c/d$, with $c, d \in D$; then we get $da = c\bar{u}b$. Moreover, since $a \in J$, then $1 - a$ must be a unit of R, say $1 - a = \bar{w}$. Therefore, from $a(1 - a) = br$, we get multiplying by d that $dr = c\bar{u}\bar{w}$, and so that $c/d = r\bar{u}^{-1}\bar{w}^{-1}$ lies in R, in particular it lies in D. It follows then that $b|a$ and that $\langle a, b\rangle = bR$.

Assume now that $a, b \notin J$, say $a = a'u$ and $b = b'w$, with $a', b' \in D$ and $u, w \in R$. From the condition $a(1 - a) = br$, it follows that a' and b' form an idempotent pair in D, thus, being D a PRINC domain, there exists an element $d \in D$ such that $a'D + b'D = dD$. Finally, working in R, we obtain that $\langle a, b\rangle = \langle a', b'\rangle = dR$, thus concluding the proof. □

Recall that the *rank* of a module M over an integral domain R is the rank of a maximal free submodule of M, i.e. the maximal number of elements of M that are linearly independent over R. The rank is equal to the dimension of the Q-vector space $Q \otimes_R M$, where Q is the field of fraction of R. Then, $\operatorname{rank}_R M = \dim_Q (Q \otimes_R M)$. We will need the following

Lemma 3.1.6. *Let R be an integral domain and M a torsion-free n-generated R-module of rank n. Then M is a free R-module.*

Proof. Let M be a torsion-free n-generated R-module of rank n. So there exist $a_1, \ldots, a_n, \in M$ such that $M = \langle a_1, \ldots, a_n\rangle$, and $x_1, \ldots, x_n \in M$ linearly independent (over R). Moreover, the Q-vector space $Q \otimes_R M$ is such that $Q \otimes_R M = \langle a_1, \ldots, a_n\rangle = \langle x_1, \ldots, x_n\rangle$.

Assume by contradiction that $a_1, \ldots, a_n$ is a linearly dependent generating set of M. We can assume, without loss of generality, that there exist $r_1, \ldots, r_n \in R$, with $r_1 \neq 0$, such that

$$r_1 a_1 = \sum_{i=2}^{n} r_i a_i.$$

Then

$$a_1 = \sum_{i=2}^{n} \frac{r_i}{r_1} a_i$$

and $\dim_Q (Q \otimes_R M) < n$, absurd.

Hence, $a_1, \ldots, a_n$ must be a free set of generators of M. □

We are finally able to provide an example of PRINC domain which is neither UFD, nor projective free.

Proposition 3.1.7. *Let D be the coordinate ring of the 2-dimensional real sphere as in 3.1.4, Q its field of fractions, T an indeterminate and let*

$$R = D + TQ[\![T]\!] = \{f(T) = a + Tf'(T) |\, a \in D,\ f'(T) \in Q[\![T]\!]\}$$

be a pullback of D. Then R is a PRINC domain that is not factorial nor projective-free.

Proof. The coordinate ring D is a PRINC domain since it is a UFD, thus it follows from Lemma 3.1.5 that R is a PRINC domain.

Moreover it is not a UFD: let $a \in D \setminus D^*$ (in particular $a \in R \setminus R^*$); then $T/a^n \in R \quad \forall n > 0$, impossible in a UFD.

It remains to prove that it is not projective-free.

Let $M = \oplus_{i=1}^{3} Re_i$, where the e_i's are the vectors of the canonical basis of R^3 and define a R-homomorpism

$$\phi : M \to R,$$

by $\phi(e_i) = X_i$. Since $1 = \sum_{i=1}^{3} X_i^2 \in \mathrm{Im}\phi$, then ϕ is an epimorphism.

Let $P = \mathrm{Ker}\phi$. As in Example 3.1.4, we have $M \cong P \oplus R$ and P is a finitely generated projective R-module of rank 2.

We claim that P is not a free R-module.

Assume by contradiction that

$$P \cong R \oplus R,$$

in particular there exist $m, n \in M$, say $m = \sum_{i=1}^{3} f_i(T)e_i$ and $n = \sum_{i=1}^{3} g_i(T)e_i$ with $f_i(T), g_i(T) \in R$, such that

$$P = Rm \oplus Rn = R\left(\sum_{i=1}^{3} f_i(T)e_i\right) \oplus R\left(\sum_{i=1}^{3} g_i(T)e_i\right).$$

Since $P = \mathrm{Ker}\phi$, then $\phi\left(\sum_{i=1}^{3} f_i(T)e_i\right) = \sum_{i=1}^{3} f_i(T)X_i = 0$ and $\phi\left(\sum_{i=1}^{3} g_i(T)e_i\right) = \sum_{i=1}^{3} g_i(T)X_i = 0$. Therefore, if we set $T = 0$, we get $\sum_{i=1}^{3} f_i(0)X_i = 0$ and $\sum_{i=1}^{3} g_i(0)X_i = 0$ and then, since $f_i(0)$ and $g_i(0)$ are elements of D, $\sum_{i=1}^{3} f_i(0)e_i$, $\sum_{i=1}^{3} g_i(0)e_i \in \mathrm{Ker}\phi_0 = P_0$, where ϕ_0 and P_0 are defined as in example 3.1.4.

Moreover, since every element $r \in P_0 \subset F \subset M$ is also an element of P, there exist $\lambda(T), \mu(T) \in R$ such that

$$r = \lambda(T)\left(\sum_{i=1}^{3} f_i(T)e_i\right) + \mu(T)\left(\sum_{i=1}^{3} g_i(T)e_i\right) =$$
$$= \lambda(0)\left(\sum_{i=1}^{3} f_i(0)e_i\right) + \mu(0)\left(\sum_{i=1}^{3} g_i(0)e_i\right).$$

It follows that

$$P_0 = D\left(\sum_{i=1}^{3} f_i(0)e_i\right) + D\left(\sum_{i=1}^{3} g_i(0)e_i\right).$$

Then P_0 is 2-generated D-module of rank 2, hence by Lemma 3.1.6 it is free, contradiction. □

The main result in [53] concerning PRINC domains is the following

Theorem 3.1.8 (Th. 4.6 of [53])**.** *If R is a PRINC domain satisfying property (ID_2), then it must be a Bézout domain.*

The proof is based on the fact that every idempotent matrix with entries on a PRINC domain is a column-row matrix and that the entries of its first row generate a principal ideal (cf. [53, Prop.4.5]).

As a corollary we immediately get from Proposition 3.1.2, that unique factorization domains and projective-free domains satisfying property (ID_2), are Bézout domains.

It is worth noting that, for R projective-free, the above result was proved by Bhaskara Rao in [5] using different arguments.

Example 3.1.9. In Section 4 of [49], is proved that the rings $\mathbb{Z}(\sqrt{-3})$ and $\mathbb{Z}(\sqrt{-7})$ are PRINC domains. These rings are then PRINC domains that fail to be factorial or local, hence, by theorem 3.1.8 they cannot satisfy property (ID_2). We observe that a first proof that $\mathbb{Z}(\sqrt{-3})$ is a PRINC domain, that uses arguments different from those used in [49] was privately communicated by U. Zannier to the authors of [53]. This ring was mentioned in the paper as an example of PRINC that is not a UFD (cf. [53, Example 4.9.]).

However, in [49], it is also proved that $\mathbb{Z}(\sqrt{-3})$ and $\mathbb{Z}(\sqrt{-7})$ are projective-free. This is deduced from the fact that their invertible ideals are principal.

3.2 Prüfer domains and (princ) property

After their introduction in [53], the study of PRINC domains has been continued in [49]. The main achievement in this paper is the following theorem.

Theorem 3.2.1 (Corollary 2.6 of [49])**.** *A Dedekind domain R is a PRINC domain if and only if it is a PID.*

Example 3.2.2. The ring $R = \mathbb{Z}(\sqrt{-5})$ is an example of Dedekind domain that does not satisfy the property (princ). The elements 3 and $(1+\sqrt{-5})$, in fact, form an idempotent pair since $3(1-3) = (1+\sqrt{-5})(-1+\sqrt{-5})$, but the ideal they generate is not principal.

Since Prüfer domains are the generalization to a non-Noetherian context of Dedekind domains, a natural question that arises from Theorem 3.2.1 is the following:

(Q) *if R is a Prüfer domain that is PRINC, then is it also a Bézout domain?*

In view of the previous result and of [49, Cor. 1.5] and [45, Corollary 1.9], that gives a positive answer for Prüfer domains of finite character (i.e. such that each non-zero ideal is contained in finitely many maximal ideals), the expected answer to this question is yes. In support of this conjecture, we got a further result related to a particular Prüfer domain described in [21], that we will call *Prüfer - Schülting domain* . Let us recall that an integral domain R is said to be a Prüfer domain if every finitely generated ideal of R is invertible.

Let us start with some general results. Let v be a valuation on a field K. We denote by Γ_v the (totally) ordered group of the values of v.

Assume now that $K = F(\mathcal{X})$ where F is a field and $\mathcal{X}$ is a set of indeterminates, and take any subset $\mathcal{A} \subseteq \mathcal{X}$. We denote by $v_{\mathcal{A}}$ the valuation on K defined as follows.

If we set $F_1 = F(\mathcal{X} \setminus \mathcal{A})$, then $K = F_1(\mathcal{A})$ and any element $z \in K$ has the form $z = f/g$ where f, g are polynomials of $F_1[\mathcal{A}]$. Let us define $v_{\mathcal{A}}(f)$ as the minimal degree of the monomials of $f \in F_1[\mathcal{A}]$ and $v_{\mathcal{A}}(f/g) = v_{\mathcal{A}}(f) - v_{\mathcal{A}}(g)$. Then $v_{\mathcal{A}}$ is a valuation of K.

Let $V_{\mathcal{A}} = \{z \in K \mid v_{\mathcal{A}}(z) \geq 0\}$ be the valuation domain of $v_{\mathcal{A}}$ and $\mathfrak{M}_{\mathcal{A}} = \{z \in K \mid v_{\mathcal{A}}(z) > 0\}$ its maximal ideal. Take any $f/g \in V_{\mathcal{A}}$ with $f, g \in F_1[\mathcal{A}]$ and $g \notin \mathfrak{M}_{\mathcal{A}}$. Since any element of $\mathcal{A}$ lies in $\mathfrak{M}_{\mathcal{A}}$, we readily see that $f/g \equiv \alpha$ modulo $\mathfrak{M}_{\mathcal{A}}$ for a suitable $\alpha \in F_1$.

A special case we will be interested in is the following. Let $K = F(\mathcal{X})$ be as above, and consider the set $\mathcal{B} = \{1/X : X \in \mathcal{X}\}$. Then $K = F(\mathcal{B})$

and we may consider the valuation $v_{\mathcal{B}}$ on K, where $z \in K$ is regarded as a rational function in the indeterminates $1/X \in \mathcal{B}$. Under these circumstances if $f \in F[\mathcal{X}]$, then $v_{\mathcal{B}}(f) = -\deg(f)$, where $\deg(f)$ denotes the total degree of f as a polynomial in the indeterminates $X \in \mathcal{X}$.

If K is the quotient field of a unique factorization domain D and q is an irreducible element of D, we denote by v_q the valuation associated to the valuation domain $D_{(q)}$ of K, i.e. the localization of D at the principal prime ideal qD.

We now recall some definitions; see [21, ch.II] for further details and references.

A field K is said to be *formally real* if $a_1^2 + \cdots + a_n^2 + 1 \neq 0$ for any choice of $a_1, \ldots, a_n \in K$. The field $\mathbb{R}$ of real numbers and any subfield k of $\mathbb{R}$ are formally real fields. Moreover, an easy exercise shows that K is formally real if and only if $K(\mathcal{X})$ is formally real for any set $\mathcal{X}$ of indeterminates over K. Clearly, the field $\mathbb{C}$ of complex numbers and any field with characteristic $\neq 0$ are not formally real.

A valuation v on the field K is called *formally real* if the residue field of v is formally real. If V_v denotes the valuation domain of v and $\mathfrak{M}_v$ its maximal ideal, then v is formally real if and only if $r_1^2 + \cdots + r_n^2 + 1 \notin \mathfrak{M}_v$, for any choice of $r_1, \ldots, r_n \in V_v$. This is equivalent to say $a_1^2 + \cdots + a_n^2 + 1 \notin \mathfrak{M}_v$ for any choice of $a_1, \ldots, a_n \in K$. Under these circumstances, we also say that V_v is a *formally real valuation domain.*

We gather in a single lemma the properties of formally real valuations we will need in the remainder of the section. We denote by Q_K the set of the nonzero elements of K that are sum of squares.

Lemma 3.2.3. *Let K be a formally real field.*

(i) If v is a formally real valuation of K and $a_1, \ldots, a_n$ are arbitrary elements of K, then $v(a_1^2 + \cdots + a_n^2) = \min\{2v(a_1), \ldots, 2v(a_n)\}$. In particular, if $a \in Q_K$, then 2 divides $v(a)$ in Γ_v.

(ii) If $K = F(X)$, where X is an indeterminate, and f is an irreducible polynomial of $F[X]$, then v_f is formally real if and only if f is not a sum of squares of K.

Proof. (i) See Lemma 2.1.3 on page 15 of [21].

(ii) The assumption follows from point (i) and Lemma 2.1.6 on page 17 of [21].

□

It is worth noting that, for a formally real valuation v of K, $v(n) = 0$ for any $n \in \mathbb{N}$. In fact, since $n = 1^2 + \cdots + 1^2$, then by Lemma 3.2.3 (i),

$$v(n) = v(1^2 + \cdots + 1^2) = \min\{2v(1), \ldots, 2v(1)\} = 0. \tag{3.1}$$

We now give the crucial definitions following the notation of Chapter II of [21]. In the rest of the section, K will always denote a formally real field.

Let $\mathcal{T}$ be the set of all formally real valuations on K. We consider the integral domain

$$R_K = \bigcap_{v \in \mathcal{T}} V_v.$$

We call it the *Prüfer - Schülting domain* of K, since R_K was firstly investigated by Schülting in his 1979 paper [57].

There are some nice characterizations of R_K (cf. [21, Ch. II]), in particular, we recall that it coincides with the subring of K generated by the elements $1/(1+q)$, with $q \in Q_K$:

$$R_K = \langle \{1/(1+q) \,|\, q \in Q_K\} \rangle.$$

Using this characterization it can be easily seen that K is the quotient field of R_K (see [21, Th. 2.1.4]).

Let us observe that $u \in R_K$ is a unit if and only if $v(u) = 0$ for every formally real valuation v of K.

The following result provides a crucial property of R_K, that shows that every Prüfer - Schülting domain is a Prüfer domain. For the proof we refer to Lemma 2.1.5 on page 16 of [21].

Lemma 3.2.4. *Let $J = \langle a_1, \ldots, a_n \rangle$ be the R_K-module generated by the elements $a_1, \ldots, a_n$ of K. Then $J^2 = (a_1^2 + \cdots + a_n^2)R_K$. In particular, any finitely-generated ideal of R_K is invertible, hence R_K is a Prüfer domain.*

Since any formally real field K has characteristic 0, we may always assume that $\mathbb{R} \subseteq K$. The following result may be useful.

Proposition 3.2.5. *Every formally real valuation on $\mathbb{R}$ coincides with the trivial one, thus $R_{\mathbb{R}} = \mathbb{R}$.*

Proof. Let v be an arbitrary formally real valuation of $\mathbb{R}$. We must show that $v(a) = 0$ for any nonzero element $a \in \mathbb{R}$. For a contradiction, take $0 \neq a \in \mathbb{R}$ such that $v(a) \neq 0$. We may assume that $a > 0$ (as an element of $\mathbb{R}$) and that $v(a) > 0$ (otherwise, replace a with $1/a$). Let $n \in \mathbb{N}$ be such that $na = b > 1$. Then, by 3.1, $v(b) = v(n) + v(a) = v(a) > 0$. On the other hand $b = 1 + c^2$, for a suitable $c \in \mathbb{R}$, and $v(1 + c^2) > 0$ is impossible for any formally real valuation v. We reached a contradiction. □

Now we focus on a particular Prüfer - Schülting domain useful for our purposes. Take $K = F(X)$, where F is any formally real field and X is an indeterminate over F. We first show that the Prüfer - Schülting domain R_K is not a Bézout domain.

Theorem 3.2.6. *Let $K = F(X)$, where F is any formally real field and X is an indeterminate over F, and consider the Prüfer - Schülting domain $R = R_K$. Then, the fractional ideal of R $J = \langle 1, X\rangle$ is not principal.*

Proof. Let us assume for a contradiction, that $J = hR$ for a suitable $h \in K$. By Lemma 3.2.4, we get

$$J^2 = (1 + X^2)R = h^2R.$$

It follows that $1 + X^2 = uh^2$, where u is a unit of R. Since $D = F[X]$ is a unique factorization domain, we readily get from the preceding equality that

$$u = \frac{(1 + X^2)C^2}{H^2}$$

for suitable $H, C \in D$ coprime. To reach the required contradiction, we will find a formally real valuation v on K, such that $v(u) \neq 0$.

We firstly assume that C has an irreducible factor, say P, that is not a sum of squares. Then, by Lemma 3.2.3 (ii), the valuation v_P is formally real. Since C and H are coprime, we get $v_P(H) = 0$, hence $v_P(u) = v_P((1+X^2)C^2) > 0$. In a similar way, if H has an irreducible factor, say P', that is not in Q_K, then $v_{P'}((1 + X^2)C^2) = 0$ and $v_{P'}(u) = -v_{P'}(H) < 0$.

Therefore, we assume that C and H are both products of elements that are sum of squares. Then 4 divides the degrees of C^2 and H^2, say $\deg(C^2) = 4n$ and $\deg(H^2) = 4m$. Then $\deg((1+X^2)C^2) = 4n+2$ is different from $\deg(H^2)$. We consider now the formally real valuation $v_{1/X}$. We get

$$v_{1/X}(u) = v_{1/X}((1+X^2)C^2) - v_{1/X}(H^2) = -\deg((1+X^2)C^2) + \deg(H^2) \neq 0.$$

Therefore, in any case, there exists a formally real valuation v such that $v(u) \neq 0$ and we find a contradiction. □

As a corollary, it is easy to show that R_K is not a PRINC domain.

Corollary 3.2.7. *Let $K = F(X)$ be as above. The Prüfer - Schülting domain $R = R_K$ is not a PRINC domain. More precisely, if $a = 1/(1 + X^2)$ and $b = X/(1 + X^2)$, then a, b is an idempotent pair of R such that $\langle a, b\rangle$ is not a principal ideal.*

Proof. We start by verifying that a, b are elements of R. Let us consider any formally real valuation of K. By definition, $1 + X^2 \notin \mathfrak{M}_v$ and then $v(1 + X^2) \leq 0$. It follows that $v(a) \geq 0$ for any formally real valuation of K, i.e. $a \in R$. Let us examine b. If $v(X) > 0$, we immediately get $v(b) \geq 0$; if $v(X) \leq 0$, we get $v(1 + X^2) = \min\{2v(1), 2v(X)\} = 2v(X)$, hence $v(b) = v(X) - 2v(X) = -v(X) \geq 0$ and $b \in R$. We then conclude that both a and b lie in $R = R_K = \bigcap_{v \in \mathcal{T}} V_v$.

Now, by a direct computation, we get

$$a(1 - a) = \frac{1}{1 + X^2}\left(1 - \frac{1}{1 + X^2}\right) = \frac{X^2}{1 + X^2} = b,$$

hence a and b form an idempotent pair in R. Finally, since

$$\langle a, b\rangle = \frac{1}{1 + X^2}\langle 1, X\rangle$$

we conclude that $\langle a, b\rangle$ cannot be a principal ideal in view of theorem 3.2.6. □

These results provide an example of Prüfer domain that fails to be a Bézout domain and also to be a PRINC domain. Thus they add plausibility to the expected answer to the question **(Q)** in [49], yes.

We conclude this section with the following remark, that points out the real importance of Prüfer - Schülting domains.

Remark 6. It is well known that every ideal of a Dedekind domain requires at most two generators. Since Prüfer domains are the non-Noetherian counterpart of Dedekind domains, it is natural to ask if two is the minimal number of generators also for any finitely generated ideal of a Prüfer domain. Some early results (see [26,54]) led to think that the answer to the previous question might be yes. Using the construction of what we called a Prüfer - Schülting domain, Schülting was able to provide an example of Prüfer domain with a 3-generated finitely generated ideal, thus answering the question in negative (cf. [57], [21, II.2]). The example is the following: let $K = \mathbb{R}(X, Y)$ be the rational function field in two indeterminates over $\mathbb{R}$ and set $R = R_K$. A quite difficult proof shows that the fractional ideal $\langle 1, X, Y\rangle$ of R cannot be generated by two elements.

3.3 PRINC domains and UCFD's

At the beginning of the chapter we mentioned a relation between the notion of PRINC domain and the notion of UCFD, unique comaximal factorization domain, introduced in the 2002 paper [45] by McAdam and Swan.

In particular, we will see that a comaximal factorization domain R is a PRINC domain if and only if it is a unique comaximal factorization domain. Let us start with some definitions from [45].

Two elements $c, d \in R$ are said to be *comaximal* if the ideal $\langle c, d\rangle = R$.

A non-zero non-unit element b of an integral domain R is called *pseudo-irreducible* if it is impossible to factor b as $b = cd$ with c, d comaximal non-units of R.

We will call $b = b_1 b_2 \cdots b_m$ a *complete comaximal factorization* of b if the b_i's are pairwise comaximal pseudo-irreducible elements.

We will say that R is a *comaximal factorization domain* (CFD), if any non-zero non-unit $b \in R$ has a complete comaximal factorization. If this factorization in unique (up to order and units), then R is said to be a *unique comaximal factorization domain* (UCFD).

It is worth observing that comaximal factorization domains are very common. For instance, Noetherian domains are CFD's. We refer to [45, Lemma 1.1] for other characterizations of CFD's.

In order to understand when a CFD is also a UCFD, the authors of [45] use the concept of S-ideal as a fundamental tool.

A non-zero ideal I of R is called an S-ideal if there exist $a, c \in R$ such that $I = \langle a, c\rangle = \langle a^2, c\rangle$.

The following lemma will be useful.

Lemma 3.3.1. *Let $a, c \in R$. The following conditions are equivalent:*

(i) $\langle a, c\rangle = \langle a^2, c\rangle$.

(ii) There is an element b in R such that $\langle a, b\rangle = R$ with c dividing ab.

Proof. See Lemma 1.2 in [45]. □

The connection between PRINC domains and unique comaximal factorization domains is based on the following proposition.

Proposition 3.3.2. *A non-zero ideal I of R is an S-ideal if and only if it is generated by two elements that form an idempotent pair.*

Proof. Assume that I is an S ideal. Since, by definition, there exist $a, c \in R$ such that $I = \langle a, c\rangle = \langle a^2, c\rangle$, then there exist $\lambda, \mu \in R$ such that $a = \lambda a^2 + \mu c$. From this last equivalence we readily get that $\lambda a, c$ form an idempotent pair, in particular, $\lambda a(1 - \lambda a) = \lambda\mu c$. Clearly, $\langle \lambda a, c\rangle \subseteq I$ and $a \in \langle \lambda a, c\rangle$. Therefore, $I = \langle \lambda a, c\rangle$.

Assume now that $I = \langle a, c\rangle$, with a, c idempotent pair. Say $a(1-a) = cd$ with $d \in R$. If we set $b = 1 - a$, then $\langle a, b\rangle = R$ and $c|ab$, thus, from Lemma 3.3.1 we get $I = \langle a, c\rangle = \langle a^2, c\rangle$ and I is an S-ideal. □

Therefore, as a corollary we immediately get that

Corollary 3.3.3. *An integral domain R is a PRINC domain if and only if every S-ideal of R is principal.*

In [45, Th. 1.7] is proved that if R is a CFD, then R is a UCFD if and only if every S-ideal is principal. In view of Corollary 3.3.3 we get that

Theorem 3.3.4. *A CFD R is a UCFD iff it is a PRINC domain.*

In Section 3 of [45] it is proved that UCFD's are easily produced via pullbacks. We conclude this section by observing that, for comaximal factorization domains, Lemma 3.1.5 is a direct consequence of Theorem 3.6 on page 187 of [45].

CHAPTER 4

PROPERTY (ID_2) AND BÉZOUT DOMAINS

In this chapter we focus on the following conjecture, due to Salce and Zanardo (cf. [53]), and suggested by the results in [5, 38, 52]:

(D) If an integral domain R satisfies property (ID_2), then it is a Bézout domain.

In view of Laffey's reduction argument, if this conjecture would be true, then every domain satisfying property (ID_2) would satisfy property (ID_n) for any $n > 0$.

It is worth noting that the analogous assumption for the property (GE_2) is false. In fact, there exist non-Bézout generalized Euclidean domains, for instance, local non-valuation domains (cf. [53, Cor. 5.3], [15, Th. 4.1]).

Some classes of domains satisfying conjecture **(D)** have been shown in [53, Sect.4]: unique factorization domains, projective-free domains and PRINC domains; actually, the notion of PRINC domain was introduced in order to add consistency to **(D)**.

We present here some further results in support of conjecture **(D)**.

4.1 Prüfer domains and property (ID_2)

In this section we prove that an integral domain that satisfies (ID_2) must be a Prüfer domain, i.e. an integral domain in which every finitely generated ideal is invertible. Hence, when studying **(D)** we can confine ourselves to the class of Prüfer domains.

Proposition 4.1.1. *Let R be an integral domain and a, b two non-zero elements of R. If $I = \langle a, b\rangle$ is a non-invertible ideal of R, then $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ cannot be written as a product of idempotent matrices.*

Proof. Since I is a non-invertible ideal, in particular non-principal, then we must have:

(i) $a, b \notin R^*$,

(ii) $a \nmid b$ and $b \nmid a$.

Moreover, since the ideal generated by an idempotent pair is always invertible (see Lemma 3.1.1), we also assume that

(iii) a and b do not form an idempotent pair.

Assume by contradiction that

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x & y \\ z & 1-x \end{pmatrix}$$

where $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is a product of idempotent matrices and $\begin{pmatrix} x & y \\ z & 1-x \end{pmatrix}$ is a non-identity idempotent matrix.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is an idempotent matrix and $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, it is enough to assume

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \bar{p} & \bar{q} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & 1-x \end{pmatrix}$$

where $\begin{pmatrix} \bar{p} & \bar{q} \\ 0 & 0 \end{pmatrix}$ is a product of idempotent matrices and $\begin{pmatrix} x & y \\ z & 1-x \end{pmatrix}$ is a singular idempotent.

This leads to the equations

$$a = \bar{p}x + \bar{q}z \tag{4.1}$$

$$b = \bar{p}y + \bar{q}(1-x). \tag{4.2}$$

Moreover, we know that

$$x(1-x) = yz. \tag{4.3}$$

Then, multiplying (4.2) by x and using (4.3), we get from (4.1)

$$ay = bx. \tag{4.4}$$

Analogously, multiplying (4.2) by z and using (4.3), we get from (4.1)

$$a(1-x) = bz. \tag{4.5}$$

We now focus on the idempotent matrix $\begin{pmatrix} x & y \\ z & 1-x \end{pmatrix}$.

If $x \in R^*$, it follows from (4.4) that $a|b$, absurd. Therefore it must be $x \notin R^*$ and, analogously, $y \notin R^*$.

Using the same argument, by (4.5) it follows that it must be also $(1-x) \notin R^*$ and $z \notin R^*$.

In particular, $x \neq 1 \Leftrightarrow (1-x) \neq 0$ and $(1-x) \neq 1 \Leftrightarrow x \neq 0$. Therefore, since $x(1-x) = yz$, it must be $y \neq 0$ and $z \neq 0$.

It follows from (4.4) that

$$y\langle a, b\rangle = \langle ay, by\rangle = \langle bx, by\rangle = b\langle x, y\rangle.$$

Thus, since x, y is an idempotent pair and then $\langle x, y\rangle$ is invertible by Lemma 3.1.1, then $\langle a, b\rangle$ is also invertible, contradicting the hypothesis. □

A well known result by Robert Gilmer (cf. [25, Th. 22.1]) says that R is a Prüfer domain if and only if every two-generated ideal of R is invertible, hence we can conclude with the following corollary.

Corollary 4.1.2. *If R is an integral domain satisfying property (ID_2), then R is a Prüfer domain.*

Proof. Assume that R satisfies property (ID_2). Then, every matrix of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ with a, b non-zero elements of R, is a product of idempotent matrices. Thus, it follows from Proposition 4.1.1 that every two-generated ideal of R must be invertible, i.e. R must be a Prüfer domain. □

From this result we get an equivalent formulation of the conjecture **(D)** that will be useful in the sequel:

(D') If R is a Prüfer domain that is not a Bézout domain, then R does not satisfy property (ID_2).

4.2 A new relation between properties $(\mathbf{GE}_2)$ and $(\mathbf{ID}_2)$

In this section we prove that every integral domain satisfying property (ID_2) must also satisfy property (GE_2). This fact allows us to prove that some special classes of Prüfer domains R verify the conjecture **(D')** by proving that, if R is non-Bézout, then there exist invertible 2×2 matrices over R that are not products of elementary matrices. Actually, using this argument and conveniently applying some results by Cohn, we prove the conjecture **(D')** for the coordinate rings of a large class of non-singular curves and for the ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials.

Let us recall an important result due to Kaplansky [35]:

Lemma 4.2.1 (Lemma 1 of [35])**.** *Let R be an integral domain and let $I_1, \ldots, I_m, J_1, \ldots, J_m$ be (integral or fractional) ideals of R such that*

$$I_1 \oplus \cdots \oplus I_m \cong J_1 \oplus \cdots \oplus J_m$$

as R-modules. Then

$$I_1 \cdots I_m \cong J_1 \cdots J_m.$$

From this lemma, we immediately get the following corollary

Corollary 4.2.2. *Let R be an integral domain and J a fractional ideal of R. If $R \oplus R \cong J \oplus R$, then J is a free R-module*

Proof. By 4.2.1 $R \cdot R \cong J \cdot R$, hence $J \cong R$. □

We are now able to prove the next proposition.

Proposition 4.2.3. *Let A and B be free direct summands of rank one of the free R-module R^2 with $A \cap B = 0$. Then there exists an endomorphism β of R^2 with $Ker(\beta) = B$ and $Im(\beta) = A$.*

Proof. Let A and B be free direct summands of rank one of R^2, i.e. $R \oplus R = A \oplus A' = B \oplus B'$ with $A \cong R$ and $B \cong R$. Hence, by Corollary 4.2.2 A' and B' are free of rank one. Let $A = Ra$, $A' = Ra'$, $B = Rb$, $B' = Rb'$. Then there exists $r_{ij} \in R$ with $r_{11}r_{22} - r_{12}r_{21} \in R^*$ such that

$$\begin{pmatrix} b \\ b' \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \begin{pmatrix} a \\ a' \end{pmatrix}.$$

We may actually assume that $r_{11}r_{22} - r_{12}r_{21} = 1$.
Let's define on $A \oplus A'$ the endomorphism β by extending the following assignments:

$$\beta(a) = r_{12}a, \qquad \beta(a') = -r_{11}a.$$

The matrix associated to β with respect to the basis $\{a, a'\}$ is

$$T_\beta = \begin{pmatrix} r_{12} & -r_{11} \\ 0 & 0 \end{pmatrix}$$

and it is clear that $Im(\beta) \subseteq Ra = A$. Moreover

$$a = (r_{11}r_{22} - r_{12}r_{21})a = -r_{22}\beta(a') - r_{21}\beta(a) = \beta(-r_{22}a' - r_{21}a) \in Im(\beta),$$

hence $Im(\beta) = A$.

Now, from $b = r_{11}a + r_{12}a'$ we get

$$\beta(b) = r_{11}\beta(a) + r_{12}\beta(a') = r_{11}r_{12}a - r_{12}r_{11}a = 0.$$

It follows that $Rb = B \subseteq Ker(\beta)$. Let z be an arbitrary element of $Ker(\beta)$. We can write $z = sb + tb'$ for suitable $s, t \in R$. Then $0 = \beta(z) = s\beta(b) + t\beta(b') = t\beta(b')$. However $\beta(b') \neq 0$, otherwise $Ker(\beta) = B \oplus B' = A \oplus A'$ and $\beta = 0$, impossible. It follows that, necessarily, $t = 0$ so that $z \in B$. We conclude that $Ker(\beta) = B$, as required. □

Let us recall that in Theorem 3.4 of [53], it is proved that an integral domain R satisfies property (GE_n), with $n > 0$, if and only if it satisfies the following property:

(HF_n) For any free direct summand A, B of the free R-module R^n, of ranks r and $n - r$ respectively ($1 \leq r \leq n$), there exists an endomorphism β of R^n with $\mathrm{Ker}(\beta) = B$ and $\mathrm{Im}(\beta) = A$, that is a product of idempotent endomorphisms of rank r.

From this result and from the preceding proposition we get an important corollary.

Corollary 4.2.4. *If R satisfies (ID_2), then it also satisfies (GE_2).*

Proof. Since (ID_2) holds by hypothesis, then every endomorphism of R^2 with rank 1, is a product of idempotent endomorphisms of rank 1. Therefore, by 4.2.3 the property (HF_2) in Theorem 3.4 of [53] is verified and then so is (GE_2). □

Remark 7. From the preceding discussion we get that if an integral domain R does not satisfy (GE_2), then it does not satisfy (ID_2). As a consequence, any non-Bézout Prüfer domain that does not satisfy (GE_2) verifies the conjecture **(D')**.

In the rest of the chapter we prove that the coordinate rings of a large class of curves and the ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z})$ satisfy **(D')**.

4.2.1 Some coordinate rings satisfying (D')

The notation will be the same as that in Sections 1.3 and 2.1.

Let k be a perfect field, $\bar{k}$ its algebraic closure, $\mathcal{C}$ a smooth projective curve over k, $\mathcal{C}_0$ an affine part of $\mathcal{C}$ and $\mathcal{C}_\infty$ the corresponding set of points at infinity. Let us consider the affine coordinate ring $R = k[\mathcal{C}_0]$ and define, for any $z \in R$

$$d(z) = -\sum_{P \in C_\infty} \mathrm{ord}_P(z). \tag{4.6}$$

We will need some lemmas.

Lemma 4.2.5. *Let $R = k[\mathcal{C}_0]$ be the affine coordinate ring of the smooth curve $\mathcal{C}$ over the field k. If all the points at infinity of $\mathcal{C}$ are conjugate by elements of the Galois group $G_{\bar{k}/k}$, then R is a k-ring, i.e. $R^* = k^*$.*

Proof. Let us assume that all the elements of $\mathcal{C}_\infty$ are conjugate by elements of $G_{\bar{k}/k}$. It follows that any nonzero rational divisor at infinity has the form $m\sum_{P\in\mathcal{C}_\infty} P$, for some nonzero integer m. Let u be a unit of R. Then u has no zeroes in $\mathcal{C}_0$, hence $\mathrm{div}(u)$ is a divisor at infinity. Then $\deg(\mathrm{div}(u)) = 0$ implies $\mathrm{div}(u) = 0$, hence $u \in k^*$ by Proposition 1.3.11 (i). □

It is worth noting that this lemma is nothing but one of the two implications in Lemma 2.3.4; here we do not need to assume that the curve has genus 0.

From Lemma 4.2.5 and Lemma 2.3.3 in chapter 2, we immediately get the following result.

Lemma 4.2.6. *In the above notation, if all the points at infinity of $\mathcal{C}$ are conjugate by elements of the Galois group $G_{\bar{k}/k}$, then the map $d : R \to \mathbb{N} \cup \{-\infty\}$ defined by 4.6 satisfies the following properties:*

(d1) $d(z) = -\infty$ *if and only if* $z = 0$,

(d2) $d(z) = 0$ *if and only if* $z \in k^*$,

(d3) $d(z+t) \leq \max\{d(z), d(t)\}$,

(d3') $d(z+t) = \max\{d(z), d(t)\}$ *whenever* $d(z) \neq d(t)$

(d4) $d(zt) = d(z) + d(t)$,

for any $zt \in R$

These two lemmas permit the use of Cohn's result on k-rings (cf. Proposition 2.3.2) to prove the next theorem.

Theorem 4.2.7. *Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane smooth curve over the field k, having degree ≥ 2, such that all the points at infinity are conjugate by elements of the Galois group $G_{\bar{k}/k}$. Then $R = k[\mathcal{C}_0] = k[\mathcal{C} \setminus \mathcal{C}_\infty]$ does not satisfy property (GE_2).*

Proof. Since all the elements of $\mathcal{C}_\infty$ are conjugate, then from Lemma 4.2.5, R is a k-ring. Moreover since the number of the points at infinity is ≥ 2, no one of them is rational.

Let $F(x, y) = 0$ be the defining equation of $\mathcal{C}_0$, where $F \in k[x, y]$ is a polynomial of degree $n \geq 2$; we assume, without loss of generality, that $F(0, 0) \neq 0$. Let $F_n(X, Y)$ be the homogeneous component of F of degree n. Since the points at infinity are conjugate and not rational, it follows that $F_n(X, Y) = c \prod_{i=1}^{n} (Y - \alpha_i X)$, where $c \in k$, $\alpha_i \in \bar{k} \setminus k$, and $P_i = (1, \alpha_i, 0)$ are the points at infinity, $1 \leq i \leq n$. Since the P_i's are conjugate, from Lemma 4.2.6 we get that the map $d = -\sum_{i=1}^{n} \mathrm{ord}_{P_i}$ satisfies properties (d1)-(d4).

Now we consider the elements x, y of R. Since $F(0, 0) \neq 0$, it is clear that x, y form a regular row. Taking homogeneous coordinates, it is straightforward to verify that $d(x) = d(y)$. Let us verify that x, y are R-independent. Take any nonzero $c \in R$. If $c \notin k^*$, than $d(c) > 0$ and so $d(x + yc) > d(x), d(y + xc) > d(y)$ by the properties of d. If $c \in k^*$, it is easily seen that $d(x + yc) = d(x) = d(y) = d(y + xc)$. Now we can apply Proposition 2.3.2, and conclude that R does not satisfy property (GE_2). □

Corollary 4.2.8. *Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane smooth curve over the field k, having degree ≥ 2, such that all the points at infinity are conjugate by elements of the Galois group $G_{\bar{k}/k}$. Then $R = k[\mathcal{C}_0] = k[\mathcal{C} \setminus \mathcal{C}_\infty]$ does not satisfy property (ID_2).*

Proof. Straightforward from Theorem 4.2.7 and Corollary 4.2.4. □

Therefore, given a plane smooth curve $\mathcal{C}$ of degree ≥ 2 having conjugate points at infinity, whenever its coordinate ring R is a PID, (as in the cases described by Corollary 2.3.6), then R is a non-Euclidean PID satisfying the

conjecture **(C)**; whenever its coordinate ring R is not a principal ideal domain, then R is a Dedekind domain (so also a Prüfer domain) that satisfies the conjecture **(D')**.

Example 4.2.9. Let us consider the coordinate ring $R = \mathbb{R}[\mathcal{C}_0]$ of the affine smooth curve $\mathcal{C}_0$ over $\mathbb{R}$ having defining equation $x^4 + y^4 + 1 = 0$. Then R is a non-UFD Dedekind domain. This can be seen observing that

$$(x^2 + y^2 - 1)(x^2 + y^2 + 1) = 2(xy - 1)(xy + 1)$$

is a non-unique factorization into indecomposable factors. Moreover R does not satisfy property (ID_2) by Corollary 4.2.8.

4.2.2 $\mathbf{Int}(\mathbb{Z})$ and the property $(\mathbf{ID}_2)$

A natural example of Prüfer domain that fails to be a Bézout domain is the celebrated ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z})$. In this section we prove that this ring satisfies the conjecture **(D)** in its equivalent formulation **(D')**, i.e. that it does not satisfy property (ID_2).

The ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials is defined as the set of rational polynomials taking integral values on integers:

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

It is clear that $\mathrm{Int}(\mathbb{Z})$ is a $\mathbb{Z}$-module such that

$$\mathbb{Z}[X] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[X].$$

Integer-valued polynomials and their various generalizations have been deeply studied in the last century, and they revealed many interesting properties. We refer to [9] for an overview of the main results on this topic, and to [8] for more details and proofs. For our purposes it is enough to consider the following two propositions.

Proposition 4.2.10. *The polynomials*

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!},$$

with the convention $\binom{X}{n} = 0$ *and* $\binom{X}{1} = X$*, form a basis for the* $\mathbb{Z}$*-module* $\mathrm{Int}(\mathbb{Z})$*. Any element* $f \in \mathrm{Int}(\mathbb{Z})$ *can be uniquely written as*

$$f = a_0 + a_1 X + \cdots + a_n \binom{X}{n},$$

with $a_0, \ldots, a_n \in \mathbb{Z}$*, for some* $n \in \mathbb{N}$*.*

Proof. See [8, Prop. I.1.1.]. □

Proposition 4.2.11. *The ring Int($\mathbb{Z}$) of integer-valued polynomials is a Prüfer domain. Moreover, it is not a Bézout domain*

Proof. The thesis is an immediate consequence of [11, Prop.6.3], or equivalently of [8, Th.VI.1.7]. □

In accordance with Cohn [15, Sect.8], we say that a ring R is *discretely ordered* if it is totally ordered and, for any $r \in R$, if $r > 0$, then $r \geq 1$. The ring of integers $\mathbb{Z}$ is the most obvious example of a discretely ordered ring.

Proposition 4.2.12. *The ring of integer-valued polynomials Int(Z) is a discretely ordered ring.*

Proof. Let $f = a_0 + a_1 X + \cdots + a_n \binom{X}{n}$ be an element of $\mathrm{Int}(\mathbb{Z})$. We will say that $f > 0$ if and only if $a_n > 0$. Then, given any $f, g \in \mathrm{Int}(\mathbb{Z})$, we have $f > g$ if and only if $f - g > 0$. Moreover, if $f > 0$, then it is clear from the definition of the order relation that it must be $f \geq 1$. □

We now summarize some results on discretely ordered ring contained in Section 8 of Cohn's fundamental paper [15].

Let us recall that a ring R satisfies property (GE_2) if the group $GL_2(R)$ of invertible matrices over R coincides with the subgroup $GE_2(R)$ generated by elementary matrices.

Theorem 4.2.13 (cf. Theorem 8.2 of [15])**.** *Let R be a discretely ordered ring. Then any $\mathbf{M} \in GL_2(R)$ can be uniquely written in the form*

$$\mathbf{M} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mathbf{T}(r_1) \cdots \mathbf{T}(r_k), \tag{4.7}$$

where $\alpha, \beta \in R^*$,

$$\mathbf{T}(r_i) = \begin{pmatrix} r_i & 1 \\ 1 & 0 \end{pmatrix},$$

and the $r_i \in R$ satisfy

$$r_1 \geq 0, \quad r_i > 0 \quad \textit{for } 1 < i < k,$$

and when $k = 2$, r_1, r_2 are not both zero.

Let $t_1, t_2, \ldots$ be a sequence of non-commuting indeterminates and define recursively by the following equations a sequence of polynomials in the t_i's with integer coefficients:

$$\begin{aligned} &p_{-1} = 0, \\ &p_0 = 1, \\ &p_k(t_1, \ldots, t_k) = p_{k-1}(t_1, \ldots, t_{k-1})t_k + p_{k-2}(t_1, \ldots, t_{k-2}). \end{aligned} \tag{4.8}$$

We observe that for $k \geq 0$, the suffix of p_k just indicates the number of arguments, so it can be omitted when the arguments are given explicitly.

Then

$$\mathbf{T}(r_1) \cdots \mathbf{T}(r_k) = \begin{pmatrix} p(r_1, \ldots, r_k) & p(r_1, \ldots, r_{k-1}) \\ p(r_2, \ldots, r_k) & p(r_2, \ldots, r_{k-1}) \end{pmatrix}. \tag{4.9}$$

This can be easily seen by induction. It is clear for $k = 1$ and, if we set $p_i = p(r_1, \ldots, r_i)$ and $p'_i = p(r_2, \ldots, r_{i+1})$, so that $\mathbf{T}(r_1) \cdots \mathbf{T}(r_k) = \begin{pmatrix} p_k & p_{k-1} \\ p'_{k-1} & p'_{k-2} \end{pmatrix}$, we have

$$\begin{pmatrix} p_{k-1} & p_{k-2} \\ p'_{k-2} & p'_{k-3} \end{pmatrix} \begin{pmatrix} r_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ p'_{k-1} & p'_{k-2} \end{pmatrix}.$$

Lemma 4.2.14 (cf. 8.3 in [15])**.** *Let R be a discretely ordered ring and $r_1, \ldots, r_k \in R$. If $r_1 \geq 0$, $r_i > 0$, $1 < i < k$ with $k \geq 2$, then*

$$p(r_1, \ldots, r_k) > p(r_1, \ldots, r_{k-1}).$$

Let $\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $GE_2(R)$, with R a discretely ordered ring. Then, from Theorem 4.2.13 and equation 4.9 we get

$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha\, p(r_1, \ldots, r_k) & \alpha\, p(r_1, \ldots, r_{k-1}) \\ \beta\, p(r_2, \ldots, r_k) & \beta\, p(r_2, \ldots, r_{k-1}) \end{pmatrix}, \tag{4.10}$$

with $\alpha, \beta \in R^*$ and $r_1, \ldots, r_k \in R$ such that $r_1 \geq 0$ and $r_i > 0$, $1 < i < k$. Moreover, from 4.10 and 4.8, we also get

$$\begin{aligned} \mathbf{M}(\mathbf{T}(r_k))^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -r_k \end{pmatrix} = \begin{pmatrix} b & a - br_k \\ d & c - dr_k \end{pmatrix} \\ &= \begin{pmatrix} \alpha\, p(r_1, \ldots, r_{k-1}) & \alpha\, p(r_1, \ldots, r_{k-2}) \\ \beta\, p(r_2, \ldots, r_{k-1}) & \beta\, p(r_2, \ldots, r_{k-2}) \end{pmatrix} \end{aligned} \tag{4.11}$$

Therefore, when $k \geq 2$, Lemma 4.2.14 implies that $b = \alpha\, p(r_1, \ldots, r_{k-1})$ and $a - br_k = \alpha\, p(r_1, \ldots, r_{k-2})$ must have the same sign, depending on α. Say $b, a - br_k > 0$ (if they are not it suffices to replace $\mathbf{M}$ with $-\mathbf{M}$). Thus, from Lemma 4.2.14,

$$b > a - br_k > 0. \tag{4.12}$$

Lemma 4.2.15 (cf. Lemma 8.4 of [15])**.** *Let R be a discretely ordered ring and $\boldsymbol{M}$ any matrix in $GE_2(R)$ with first row (a, b) and $b > 0$. Assume that*

$$\mathbf{M} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mathbf{T}(r_1) \cdots \mathbf{T}(r_k)$$

with $\alpha, \beta \in R^*$, $r_1, \ldots, r_k \in R$ such that $r_1 \geq 0$ and $r_i > 0$ for $1 < i < k$, and $k \geq 2$. Then

(i) if $r_k > 0$, then $a > b > 0$;

(ii) if $r_k = 0$, then $b > a > 0$;

(iii) if $r_k = -c < 0$, then $b > a > -bc$.

Let us remark that all the above results are true for the discretely ordered ring $\mathrm{Int}(\mathbb{Z})$.

We are finally able to prove the following

Theorem 4.2.16. *The ring of integer-valued polynomials Int($\mathbb{Z}$) does not satisfy property (GE_2).*

Proof. Assume by contradiction that every invertible matrix over $\mathrm{Int}(\mathbb{Z})$ is an element of $GE_2(\mathrm{Int}(\mathbb{Z}))$, and consider the invertible matrix

$$\mathbf{M} = \begin{pmatrix} 1 + 2X & 4 \\ 1 + 4X + 2\binom{X}{2} & 5 + 2X \end{pmatrix}.$$

By Theorem 4.2.13, $\mathbf{M} = [\alpha, \beta]\mathbf{T}(r_1) \cdots \mathbf{T}(r_k)$ with $\alpha, \beta \in R^*$, $r_i \in R$, such that $r_1 \geq 0$, $r_i > 0$ for $1 < i < k$. Note that $k \geq 2$; in fact for $k = 0$, $\mathbf{M} = [\alpha, \beta]$ while, for $k = 1$, $\mathbf{M} = \begin{pmatrix} \alpha r_1 & \alpha \\ \beta & 0 \end{pmatrix}$. Moreover, if we set $(a, b) = (1 + 2X, 4)$, then $b > 0$ and $a > b > 0$. Therefore, we are in case (i) of Lemma 4.2.15, and it must be $r_k > 0$. But from 4.12 we also have $b > a - br_k > 0$, in particular

$$a > br_k.$$

Let $r_k = a_{0k} + a_{1k}X + \cdots + a_{mk}\binom{X}{m}$. Thus, since $r_k > 0$, then $a_{mk} > 0$, hence $a_{mk} \geq 1$ and $4a_{mk} > 2$. This shows that r_k must be an element of $\mathbb{Z}$ otherwise we would get $a - br_k < 0$. But for such r_k we have $a - br_k = (1 - 4a_{0k}) + 2X > 4 = b$, thus contradicting 4.12. It follows that $\mathbf{M}$ cannot be written as a product of elementary matrices and we finally conclude that $\mathrm{Int}(\mathbb{Z})$ does not satisfy property (GE_2). □

In view of Corollary 4.2.4 we get as an immediate consequence that

Corollary 4.2.17. *The ring Int($\mathbb{Z}$) of integer-valued polynomials does not satisfy property (ID_2). In particular Int($\mathbb{Z}$) verifies the conjecture **(D')**.*

BIBLIOGRAPHY

[1] D. D. Anderson. An existence theorem for non-Euclidean PIDs. *Comm. Algebra*, 16(6):1221–1229, 1988.

[2] E. Artin. *Algebraic numbers and algebraic functions*. Gordon and Breach Science Publishers, New York-London-Paris, 1967.

[3] M. Auslander and D. A. Buchsbaum. *Groups, rings, modules*. Harper & Row, Publishers, New York-London, 1974. Harper's Series in Modern Mathematics.

[4] H. Bass. *Introduction to some methods of algebraic K-theory*. American Mathematical Society, Providence, R.I., 1974. Expository Lectures from the CBMS Regional Conference held at Colorado State University, Ft. Collins, Colo., August 24-28, 1973, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 20.

[5] K. P. S. Bhaskara Rao. Products of idempotent matrices over integral domains. *Linear Algebra Appl.*, 430(10):2690–2695, 2009.

[6] M. L. Brown. A note on Euclidean rings of affine curves. *J. London Math. Soc. (2)*, 29(2):229–236, 1984.

[7] M. L. Brown. Euclidean rings of affine curves. *Math. Z.*, 208(3):467–488, 1991.

[8] P.-J. Cahen and J.-L. Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[9] P.-J. Cahen and J.-L. Chabert. What you should know about integer-valued polynomials. *Amer. Math. Monthly*, 123(4):311–337, 2016.

[10] J. W. S. Cassels. *LMSST: 24 Lectures on Elliptic Curves*. Cambridge University Press, 1991. Cambridge Books Online.

[11] J.-L. Chabert. Un anneau de Prüfer. *J. Algebra*, 107(1):1–16, 1987.

[12] C.-A. Chen and M.-G. Leu. The 2-stage Euclidean algorithm and the restricted Nagata's pairwise algorithm. *J. Algebra*, 348:1–13, 2011.

[13] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.

[14] P. M. Cohn. Rings with a weak algorithm. *Trans. Amer. Math. Soc.*, 109:332–356, 1963.

[15] P. M. Cohn. On the structure of the GL_2 of a ring. *Inst. Hautes Études Sci. Publ. Math.*, (30):5–53, 1966.

[16] G. E. Cooke. A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I. *J. Reine Angew. Math.*, 282:133–156, 1976.

[17] G. E. Cooke. A weakening of the Euclidean property for integral domains and applications to algebraic number theory. II. *J. Reine Angew. Math.*, 283/284:71–85, 1976.

[18] L. Cossu, P. Zanardo, and U. Zannier. Products of elementary matrices and non-Euclidean principal ideal domains. *submitted*, 2017.

[19] R. J. H. Dawlings. Products of idempotents in the semigroup of singular endomorphisms of a finite-dimensional vector space. *Proc. Roy. Soc. Edinburgh Sect. A*, 91(1-2):123–133, 1981/82.

[20] J. A. Erdos. On products of idempotent matrices. *Glasgow Math. J.*, 8:118–122, 1967.

[21] M. Fontana, J. A. Huckaba, and I. J. Papick. *Prüfer domains*, volume 203 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1997.

[22] J. Fountain. Products of idempotent integer matrices. *Math. Proc. Cambridge Philos. Soc.*, 110(3):431–441, 1991.

[23] L. Fuchs and L. Salce. *Modules over non-Noetherian domains*, volume 84 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2001.

[24] W. Fulton. *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[25] R. Gilmer. *Multiplicative ideal theory*, volume 90 of *Queen's Papers in Pure and Applied Mathematics*. Queen's University, Kingston, ON, 1992. Corrected reprint of the 1972 edition.

[26] R. Gilmer and W. Heinzer. On the number of generators of an invertible ideal. *J. Algebra*, 14:139–151, 1970.

[27] P. Glivický and J. Šaroch. Quasi-Euclidean subrings of $\mathbb{Q}[X]$. *Comm. Algebra*, 41(11):4267–4277, 2013.

[28] X. Guitart and M. Masdeu. Continued fractions in 2-stage Euclidean quadratic fields. *Math. Comp.*, 82(282):1223–1233, 2013.

[29] J. Hannah and K. C. O'Meara. Products of idempotents in regular rings. II. *J. Algebra*, 123(1):223–239, 1989.

[30] M. Harper and M. R. Murty. Euclidean rings of algebraic integers. *Canad. J. Math.*, 56(1):71–76, 2004.

[31] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[32] J. M. Howie. The subsemigroup generated by the idempotents of a full transformation semigroup. *J. London Math. Soc.*, 41:707–716, 1966.

[33] J. M. Howie. Some subsemigroups of infinite full transformation semigroups. *Proc. Roy. Soc. Edinburgh Sect. A*, 88(1-2):159–167, 1981.

[34] I. Kaplansky. Elementary divisors and modules. *Trans. Amer. Math. Soc.*, 66:464–491, 1949.

[35] I. Kaplansky. Modules over Dedekind rings and valuation rings. *Trans. Amer. Math. Soc.*, 72:327–340, 1952.

[36] I. Kaplansky. *Commutative rings*. The University of Chicago Press, Chicago, Ill.-London, revised edition, 1974.

[37] M. Kong. Euler classes of inner product modules. *Journal of Algebra*, 49(1):276 – 303, 1977.

[38] T. J. Laffey. Products of idempotent matrices. *Linear and Multilinear Algebra*, 14(4):309–314, 1983.

[39] T. Y. Lam. *Modules with isomorphic multiples, and rings with isomorphic matrix rings, a survey.* Monographie No. 35, L'Enseignement Math., 1999.

[40] S. Lang. *Introduction to algebraic and abelian functions*, volume 89 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1982.

[41] M.-G. Leu. The restricted Nagata's pairwise algorithm and the Euclidean algorithm. *Osaka J. Math.*, 45(3):807–818, 2008.

[42] D. Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[43] R. E. MacRae. On unique factorization in certain rings of algebraic functions. *J. Algebra*, 17:243–261, 1971.

[44] R. Markanda. Euclidean rings of algebraic numbers and functions. *J. Algebra*, 37(3):425–446, 1975.

[45] S. McAdam and R. G. Swan. Unique comaximal factorization. *J. Algebra*, 276(1):180–192, 2004.

[46] B. R. McDonald. *Linear algebra over commutative rings*, volume 87 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1984.

[47] K. C. O'Meara. Products of idempotents in regular rings. *Glasgow Math. J.*, 28(2):143–152, 1986.

[48] O.T. O'Meara. On the finite generation of linear groups over hasse domains. *Journal für die reine und angewandte Mathematik*, 217:79–108, 1965.

[49] G. Peruginelli, L. Salce, and P. Zanardo. *Idempotent Pairs and PRINC Domains*, pages 309–322. Springer International Publishing, Cham, 2016.

[50] M. A. Reynolds and R. P. Sullivan. Products of idempotent linear transformations. *Proc. Roy. Soc. Edinburgh Sect. A*, 100(1-2):123–138, 1985.

[51] J. J. Rotman. *Advanced modern algebra. Part 1*, volume 165 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.

[52] W. Ruitenburg. Products of idempotent matrices over Hermite domains. *Semigroup Forum*, 46(3):371–378, 1993.

[53] L. Salce and P. Zanardo. Products of elementary and idempotent matrices over integral domains. *Linear Algebra Appl.*, 452:130–152, 2014.

[54] J. D. Sally and W. V. Vasconcelos. Stable rings. *J. Pure Appl. Algebra*, 4:319–336, 1974.

[55] P. Samuel. *Lectures on unique factorization domains*. Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30. Tata Institute of Fundamental Research, Bombay, 1964.

[56] P. Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.

[57] H.-W. Schülting. Über die Erzeugendenanzahl invertierbarer Ideale in Prüferringen. *Comm. Algebra*, 7(13):1331–1349, 1979.

[58] J. H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[59] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[60] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[61] R. G. Swan. Algebraic vector bundles on the 2-sphere. *Rocky Mountain J. Math.*, 23(4):1443–1469, 12 1993.

[62] G. D. Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[63] P. J. Weinberger. On Euclidean rings of algebraic integers. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 321–332. Amer. Math. Soc., Providence, R. I., 1973.