TREBALL DE FI DE GRAU

Grau en Matemàtiques

Títol: Anells commutatius i Teoria de la divisibilitat

Autor: Clara Tapia Pérez

Director: Francesc Planas Vilanova

Departament: Departament de matemàtiques

Convocatòria: 2019-2020

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Grau en Matemàtiques
Treball de fi de Grau

Anells commutatius i Teoria de la divisibilitat

Clara Tapia Pérez

Tutor del treball:
Francesc Planas Vilanova

25 de juny de 2020

Voldria agrair, en primer lloc i especialment, al director del treball, el Francesc Planas, qui em va introduir en el camp de l'àlgebra commutativa, per guiar-me, ajudar-me i encoratjar-me durant tot el procés. Finalment, als meus pares, la Lourdes i el Manuel, i a la meva germana, la Lucía, pel seu suport i confiança.

Índex

Introducció **7**

1 Preliminars **9**
1.1 Definició d'anell . . . 9
1.2 Ideals . . . 12
1.3 Anell quocient . . . 13
1.4 Simetrització . . . 15
1.5 Ideals maximals i primers . . . 17

2 Anells Noetherians i Artinians **21**
2.1 Anells Noetherians . . . 21
2.2 Anells Artinians . . . 23
2.3 Una altra caracterització dels Anells Artinians . . . 23

3 Famílies de dominis **31**
3.1 Divisibilitat . . . 31
3.2 Dominis GCD . . . 33
3.3 Dominis de Bézout . . . 35
3.4 Anells factorials . . . 37
3.5 Una altra caracterització dels DFU . . . 41
3.6 Dominis d'Ideals Principals . . . 43
3.7 Dominis Euclidians . . . 46
3.8 Algorisme d'Euclides . . . 47

4 Ordenant dominis **49**
4.1 Dominis no GCD . . . 49
4.2 Dominis no DFU . . . 49
4.3 GCD no DFU . . . 50
4.4 DFU no DIP . . . 52
4.4.1 Anells de polinomis sobre DFUs . . . 52
4.4.2 Exemples de DFUs no DIPs . . . 56
4.5 DIP no Euclidià . . . 57
4.5.1 Caracterització dels DIP usant la norma de Dedekind-Hasse . . . 58
4.5.2 $\mathbb{Z}[\theta]$ és DIP . . . 59

4.5.3 $\mathbb{Z}[\theta]$ no és un domini Euclidià 60
4.6 Dominis de Bézout 63

5 Conclusions i treball futur **65**

Bibliografia **67**

Introducció

El concepte abstracte d'anell va sorgir, en la segona meitat del segle XIX, de dues teories diferents; la teoria d'anells commutatius i la teoria d'anells no commutatius. Aquestes, al seu torn, van sorgir de l'estudi de problemes diferents.

D'una banda, la teoria d'anells no commutatius va sorgir de l'intent d'estendre els nombres complexos a diversos sistemes de nombres hipercomplexos.

En canvi, la teoria d'anells commutatius moderna, objecte d'estudi d'aquest treball, té origen en l'estudi de geometria algebraica i la teoria de nombres algebraics. En aquest context, la primera definició del concepte d'anell commutatiu, va ser introdïda en 1981 per Richard Dedekind, en connexió amb el problema de la factorització no única d'enters algebraics, tot i que no el va anomenar així. No obstant, actualment, s'acostuma a usar la definició donada per Emmy Noether l'any 1921, en el seu article *Idealtheorie in Ringbereichen*, en el qual va desenvolupar les bases de la teoria d'anells commutatius. Veure, per exempe [11], [12].

A grans trets, un anell és un sistema algebraic format per un conjunt no buit i dues operacions internes, la suma i el producte, que verifiquen certes propietats.

Aquest treball, motivat per l'interès personal en la matèria, es centra de forma exclusiva en l'estudi dels anells commutatius i, especialment, en l'estudi de la teoria de la divisibilitat en dominis íntegres. Més concretament, els objectius d'aquest treball es resumeixen en:

1. Analitzar les conseqüències i resultats que deriven d'imposar certes condicions en els anells commutatius; com per exemple, entre d'altres, les condicions de cadena ascendent i descendent, l'existència de màxims comuns divisors i mínims comuns múltiples, l'existència d'una factorització única o bé l'existència d'una norma Euclidiana.

2. Caracteritzar, en funció de les propietats anteriors, les famílies d'anells: Noetherians, Artinians, dominis GCD, dominis de Bézout, dominis de factorització única (DFUs), dominis d'ideals principals (DIPs) i dominis Euclidians.

3. Estudiar i entendre les relacions que existeixen entre les famílies anteriors. En paricular, comprovar que es verifiquen les implicacions següents:

$$A \text{ Artinià} \iff A \text{ Noetherià i } \dim(\mathrm{A}) = 0. \tag{1}$$

$$A \text{ Euclidià} \implies A \text{ DIP} \implies A \text{ DFU} \implies A \text{ domini GCD} \implies A \text{ domini}. \tag{2}$$

$$\begin{array}{ccc} A \text{ DIP} & \Longrightarrow & A \text{ domini de Bézout} \\ \Downarrow & & \Downarrow \\ A \text{ DFU} & \Longrightarrow & A \text{ domini GCD} \end{array} \tag{3}$$

4. Comprovar i entendre, per mitjà de contraexemples, que cap dels recíprocs de les implicacions en (2) i (3) és cert en general. Al seu torn, entendre per què els dominis de Bézout no es poden incloure en la cadena d'implicacions (2).

5. Presentar i demostrar els resultats i exemples comentats en els punts anteriors de forma clara i ordenada. Així com introduir els conceptes i resultats previs necessaris per a entendre'ls.

L'estructura d'aquest treball és la següent:

Capítol 1. Establim la base d'aquest treball, introduint els anells de forma general. Presentem la definició d'anell detalladament, així com les seves propietats més generals. Presentem també diversos conceptes i subsistemes bàsics: els morfismes d'anells, els ideals, els anells quocient i els anells de fraccions, juntament amb algunes propietats útils en demostracions posteriors. Finalment, estudiem dos tipus d'ideals de gran importància en la teoria d'anells i, en definitiva, en aquest treball: els ideals primers i els ideals maximals.

Capítol 2. Comencem a imposar certes condicions en els anells per tal d'obtenir resultats més forts. En particular, estudiem les condicions de cadena ascendent i descendent, i d'element maximal i minimal. En funció d'aquestes condicions, distingim dos tipus d'anells: els anells Noetherians i els anells Artinians. Provem que es verifica l'equivalència (1). Per tal de provar-ho, introduïm els conceptes de radical i mòdul, i analitzem diverses característiques dels anells Noetherians i Artinians.

Capítol 3. Amb l'objectiu de tractar la divisibilitat en els anells, centrem l'estudi del capítol en els dominis. Estudiem, entre d'altres, l'existència de màxims comuns divisors, mínims comuns múltiples i solucions per a l'equació de Bézout en dominis, el problema de la factorització única i l'algorisme d'Euclides, i les conseqüències que en deriven. En funció d'aquestes propietats, distingim i caracteritzem les famílies de dominis GCD, de Bézout, factorials, d'ideals principals i Euclidians. Provem que es satisfan les implicacions en (2) i (3).

Capítol 4. En aquest capítol estudiem els recíprocs de les implicacions en (2) i (3), i demostrem que no són certs en general. Estudiem també per què els dominis de Bézout no es poden incloure en la cadena d'implicacions (2). Més concretament, analitzem exemples de dominis no GCD, dominis no factorials, dominis factorials que no són d'ideals principals, un exemple de domini d'ideals principals que no és Euclidià, un exemple de domini DFU (i GCD) que no és de Bézout, i un exemple de domini de Bézout (i GCD) que no és DFU (ni DIP).

Capítol 5. Exposem breument les conclusions i comentem el possible camí a seguir en un treball futur.

Capítol 1

Preliminars

En aquest capítol introduïm una sèrie de definicions i resultats, alguns d'ells bàsics, que constitueixen part de la base matemàtica sobre la qual es desenvolupa aquest treball. Per a més detalls o demostracions es recomana la referència [2].

1.1 Definició d'anell

Comencem per recordar la definició d'anell i algunes de les seves propietats més bàsiques.

Definició 1.1.1. Un *anell* A és un conjunt, no buit, dotat de dues operacions algebraiques internes, que denotem $(+)$ i $(\cdot)$, i anomenem suma i producte, respectivament, tals que, per a tot $a, b, c \in A$, es satisfan els axiomes següents:

1. $(A, +)$ és un grup abelià, és a dir:
   - $(a + b) + c = a + (b + c)$ (associativitat de la suma);
   - $a + b = b + a$ (commutativitat de la suma);
   - existeix un element de A, que denotem 0, i anomenem *element neutre de la suma*, o *zero*, tal que $0 + a = a + 0 = a$ (existència de l'element neutre per a la suma);
   - existeix un element de A, que denotem $-a$, i anomenem *element oposat de* a, tal que $a + (-a) = (-a) + a = 0$ (existència de l'oposat per a la suma).
2. $(A, \cdot)$ verifica que:
   - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativiat del producte).
3. $(A, +, \cdot)$ verifica que:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ (propietat distributiva del producte respecte de la suma).

Nota 1.1.2. Sovint escriurem ab, enlloc de $a \cdot b$, per a referir-nos al producte de a per b.

Observació 1.1.3. Sigui A un anell. Aleshores l'element neutre de la suma és únic. Per a tot $a \in A$, el seu oposat $-a$ és únic.

Observació 1.1.4. Sigui A un anell, $a \in A$. Aleshores, $0 \cdot a = a \cdot 0 = 0$.

Un exemple trivial d'anell és l'anell format per un únic element, el zero. Aquest anell s'anomena *l'anell trivial* o *l'anell nul*. No obstant, l'estructura interna de l'anell nul no resulta interessant i, per aquest motiu, en aquest treball es consideraran anells de més d'un element.

Definició 1.1.5. Sigui A un anell. Diem que A és un *anell unitari* si:

4. A verifica que:

   - existeix un element de A, que denotem 1, tal que $1 \cdot a = a \cdot 1 = a$, per a tot a de A (l'anomenem *element unitat*).

Observació 1.1.6. L'element unitat d'un anell unitari és únic.

Observació 1.1.7. Sigui A un anell unitari. Aleshores, $1 = 0 \iff A = \{0\}$.

Observació 1.1.8. Sigui A un anell unitari. Aleshores, $(-1) \cdot a = a \cdot (-1) = -a$, per a tot a de A.

Definició 1.1.9. Sigui A un anell diferent de zero i unitari, $a \in A$. Diem que a és un element *invertible* si existeix un element de A, que denotem a^{-1}, tal que, $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (l'anomenem *element invers de* a). Denotem A^* al conjunt dels elements invertibles de l'anell A.

Nota 1.1.10. Fixem-nos que en general no té per què existir l'element invers per al producte. Per exemple en l'anell dels enters, $\mathbb{Z}$, el número 2 no té invers pel producte.

Definició 1.1.11. Sigui A un anell. Diem que A és un *anell commutatiu* si:

5. A verifica que:

   - $a \cdot b = b \cdot a$, per a tot a, b de A (commutativitat).

Observació 1.1.12. Sigui A un anell diferent de zero, commutatiu i unitari. Aleshores $(A^*, \cdot)$ és un grup commutatiu. L'anomenem el *grup multiplicatiu de* A.

Definició 1.1.13. Un *cos* $\mathbb{K}$ és un anell commutatiu i amb unitat, $1 \neq 0$, tal que $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Definició 1.1.14. Sigui A un anell diferent de zero, commutatiu i unitari, $B \subseteq A$. Diem que B és un *subanell* de A si amb la suma i el producte de A, B és un anell, i $1_A \in B$. La notació 1_A fa referència a l'element unitat de l'anell A.

Definició 1.1.15. Siguin A i B dos anells diferents de zero, commutatius i unitaris. Diem que una aplicació $f : A \longrightarrow B$ és un *morfisme d'anells* si f és invariant respecte de la suma, el producte i l'element unitari. És a dir, si, donats $x, y \in A$, es verifica:

(i) $f(x+y) = f(x) + f(y)$,

(ii) $f(xy) = f(x)f(y)$,

(iii) $f(1_A) = 1_B$.

Es comprova que la imatge de A per f és un subanell de B.

Definició 1.1.16. Sigui A un anell diferent de zero, commutatiu i unitari, $a \in A$. Diem que a és un *divisor de zero* si existeix $b \in A$, $b \neq 0$, tal que $ab = 0$. Denotem per $\mathrm{Z}(A)$ al conjunt dels divisors de zero de l'anell A. És a dir:

$$\mathrm{Z}(A) = \{a \in A \mid \exists\, b \in A, b \neq 0 \text{ i } ab = 0\}.$$

És trivial veure que el zero és un divisor de zero. Els anells on el zero és l'únic divisor de zero són prou importants com per a tenir nom propi.

Definició 1.1.17. Sigui A un anell diferent de zero, commutatiu i unitari. Diem que A és un *anell íntegre* o *domini (d'integritat)* si:

6. A verifica que:

   - $ab = 0 \Longrightarrow a = 0$ o $b = 0$, per a tot a, b de A.

En aquest treball, si no s'indica el contrari, es suposarà que tots els anells són commutatius i amb unitat 1, $1 \neq 0$.

Exemple 1.1.18. Vegem alguns exemples d'anells [12]:

1. l'anell commutatiu, unitari i íntegre, dels enters: $\mathbb{Z}$;
2. l'anell commutatiu, unitari i íntegre, dels enters de Gauss: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$;
3. l'anell commutatiu i unitari, però no íntegre en general: $\mathbb{Z}/n\mathbb{Z}$, on n és un enter;
4. els cossos: $\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$, i $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, on p és primer;
5. l'anell commutatiu, unitari i íntegre, dels polinomis amb coeficients en un cos $\mathbb{K}$: $\mathbb{K}[X]$, $\mathbb{K}[X_1, \ldots, X_n]$.

Els seus respectius grups multiplicatius són:

1. $(\mathbb{Z})^* = \{1, -1\}$;
2. $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$;
3. $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \left\{\bar{k} \mid n \text{ i } k \text{ són coprimers}\right\}$;
4. $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$;
5. $(\mathbb{K}[x])^* = \mathbb{K} \setminus \{0\}$ i $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K} \setminus \{0\}$.

1.2 Ideals

Recordem que, si no s'indica explícitament el contrari, tots els anells són diferents de zero, commutatius i unitaris.

Definició 1.2.1. Sigui A un anell. Un *ideal* de A és un subconjunt $I \subseteq A$ que verifica:

1. $0 \in I$,
2. $x, y \in I \Longrightarrow x + y \in I$,
3. $a \in A$, $x \in I \Longrightarrow ax \in I$.

Exemple 1.2.2. El subconjunt de l'anell dels enters format pels nombres parells és un ideal. Més generalment, donat un enter $n \in \mathbb{Z}$, el subconjunt format pels múltiples de n és un ideal de $\mathbb{Z}$. De fet, veurem que tot ideal de $\mathbb{Z}$ és d'aquesta forma.

Observació 1.2.3. Sigui A un anell. Aleshores es verifica:

1. A té, com a mínim, dos ideals trivials, $\{0\}$ i A. Són els anomenats *ideals impropis*. Qualsevol altre ideal de A és anomenat *ideal propi*.
2. Sigui I un ideal de A. Aleshores, $I = A \iff 1 \in I \iff I \cap A^* \neq \varnothing$.
3. A és un cos $\iff$ els únics ideals de A són els impropis.
4. Si I i J són ideals de A, aleshores la intersecció $I \cap J$, és un ideal de A. Més en general, si $\{I_\lambda\}_\lambda$ és una família d'ideals de A, aleshores la intersecció $\cap_\lambda I_\lambda$ és un ideal de A.
5. Si I i J són ideals de A, aleshores la suma $I + J := \{x + y \mid x \in I, y \in J\}$, és un ideal de A. Més en general, si $\{I_\lambda\}_\lambda$ és una família d'ideals de A, aleshores la suma $\sum_\lambda I_\lambda := \left\{\sum{}' x_\lambda \mid x_\lambda \in I_\lambda\right\}$, és un ideal de A. La notació $\sum'$ fa referència a suma finita.
6. Si I i J són ideals de A, aleshores el producte $I \cdot J := \{xy \mid x \in I, y \in J\}$, és també un ideal de A.
7. Si I i J són ideals de A, aleshores, $I \cdot J \subseteq I \cap J \subseteq I$, $J \subseteq I + J$.

Definició 1.2.4. Sigui A un anell, $x_1, \ldots, x_n \in A$.

- Anomenem *ideal finitament generat per* $x_1, \ldots, x_n$, a:

$$\langle x_1, x_2, \ldots, x_n \rangle = \{a_1x_1 + \ldots + a_nx_n \mid a_i \in A\}.$$

  En particular, si $n = 1$, diem que és un *ideal principal*, i el denotem per:

$$(x) = \langle x \rangle = \{ax \mid a \in A\}.$$

Aquesta definició s'estén fàcilment a un subconjunt no finit $N \subseteq A$ qualsevol:

- Sigui $N \subseteq A$. Anomenem *ideal generat per* N a:

$$\langle N \rangle = \left\{ \sum{}' ax \mid a \in A, x \in N \right\}.$$

Observació 1.2.5. Sigui A un anell, $N \subseteq A$. L'ideal generat per N és el menor ideal de A que conté N. De fet, es té:

$$\langle N \rangle = \bigcap_{I \text{ ideal de } A,\ N \subseteq I} I.$$

Exemple 1.2.6. Sigui $f : A \longrightarrow B$ un morfisme d'anells. Aleshores el nucli de f, $\mathrm{Ker}(f)$, és un ideal de A.

1.3 Anell quocient

De forma anàloga a la teoria de grups, s'introdueix el concepte d'anell quocient.

Definició 1.3.1. Sigui A un anell, I un ideal de A, $x, y \in I$. Definim la relació: $x \sim y \iff x - y \in I$.

Observació 1.3.2. La relació definida prèviament és una relació d'equivalència, *i.e.,* reflexiva, simètrica i transitiva.

Observació 1.3.3. Donat $x \in A$, la classe de x ve donada per:

$$\begin{aligned} \bar{x} &= \{y \in A \mid y \sim x\} = \{y \in A \mid y - x = z, z \in I\} \\ &= \{y \in A \mid y = x + z, z \in I\} =: x + I. \end{aligned}$$

Definició 1.3.4. Sigui A un anell, I un ideal de A. Definim *el conjunt quocient de A mòdul I* com:

$$A/I = \{\bar{x} \mid x \in A\} = \{x + I \mid x \in A\},$$

és a dir, el conjunt de les classes d'equivalència de A mòdul I.

L'interès d'aquest conjunt és que hereta l'estructura d'anell de A. La clau per a veure-ho resideix en l'observació següent.

Observació 1.3.5. Sigui A un anell, I un ideal de A, $\bar{x}, \bar{y} \in A/I$. Aleshores les operacions suma $(+)$ i producte $(\cdot)$ en A/I, definides per:

- $\bar{x} + \bar{y} := \overline{x + y}$,
- $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$,

no depenen de l'elecció del representant. És a dir, donats $x', y' \in A$, tals que $x' \sim x$, $y' \sim y$, es té:

- $x + y \sim x' + y'$, i per tant, $\bar{x} + \bar{y} = \overline{x + y} = \overline{x' + y'} = \bar{x'} + \bar{y'}$.

- $xy \sim x'y'$, i per tant, $\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \overline{x' \cdot y'} = \bar{x'} \cdot \bar{y'}$.

L'Observació 1.3.5 ens diu, en altres paraules, que tant la suma com el producte de A estan ben definits en A/I. Es comprova que amb aquestes operacions el conjunt quocient té efectivament estructura d'anell.

Proposició 1.3.6. *Sigui A un anell, I un ideal de A. Aleshores $(A/I, +, \cdot)$ és un anell. En particular, si A és unitari, respectivament, commutatiu, aleshores A/I és unitari, respectivament, commutatiu.*

Definició 1.3.7. L'anell $(A/I, +, \cdot)$ s'anomena *anell quocient de A mòdul I.*

El resultat següent estableix una identificació entre els ideals d'un anell A que contenen l'ideal I, i els ideals de A/I. Aquesta identificació s'usa sovint en demostracions en teoria d'anells.

Proposició 1.3.8. *Sigui A un anell, I un ideal de A. Aleshores, l'aplicació*

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ x &\longmapsto \overline{x}, \end{aligned}$$

és un morfisme d'anells. A més, existeix una correspondència bijectiva entre els ideals J de A que contenen I, i els ideals $\overline{J}$ de A/I, donada per $J = \pi^{-1}\left(\overline{J}\right)$.

Exemple 1.3.9. Sigui $A = \mathbb{Z}$, $I = (n) = n\mathbb{Z} \subseteq A$. Aleshores $A/I = \mathbb{Z}/n\mathbb{Z}$, és a dir, és l'anell de les classes d'enters mòdul n, que ve donat per:

$$A/I = \mathbb{Z}/n\mathbb{Z} = \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}.$$

Exemple 1.3.10. Sigui $A = \mathbb{K}[x]$, $I = (f(x))$, on $f(x) \in A$ és un polinomi de grau $n \geq 1$. Vegem quina forma tenen els elements de l'anell quocient $A/I = \mathbb{K}[x]/(f(x))$. Sigui $\overline{g(x)} \in A/I$. Podem expressar $g(x)$ com: $g(x) = f(x)q(x) + r(x)$, on o bé $r = 0$, o bé $\text{grau}(r(x)) < \text{grau}(f(x)) = n$ (més endavant tornarem a aquest punt i ho provarem amb més detall). Aleshores, tenim:

$$\bar{g} = \overline{fq + r} = \bar{f}\bar{q} + \bar{r} = \bar{r} = \overline{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}} = \overline{a_0} + \overline{a_1}\bar{x} + \ldots + \overline{a_{n-1}}\bar{x}^{n-1}.$$

A més, donats dos polinomis constants $\alpha, \beta \in A$, es té: $\alpha \sim \beta \iff \alpha - \beta \in \langle f(x) \rangle \iff \alpha - \beta = f(x)h(x)$, per a algun $h(x) \in A$. Com que $\alpha = \beta$, i $\text{grau}(f(x)) \geq 1$, necessàriament $h(x) = 0$. Per tant, $\alpha \sim \beta \iff \alpha = \beta$. És a dir, en la classe d'equivalència $\bar{\alpha} \in A/I$ d'una constant $\alpha \in A$, no hi ha cap altre constant que no sigui α. Això ens permet escriure $\bar{\alpha} = \alpha$, entenent que qualsevol altre representant de la classe $\bar{\alpha}$ és de la forma $\alpha + f(x)h(x)$, per a algun $h(x) \in A$. Així, tenim:

$$A/I = \mathbb{K}[x]/(f(x)) = \left\{a_0 + a_1\bar{x} + \ldots + a_{n-1}\bar{x}^{n-1} \mid a_i \in \mathbb{K}, \forall i = 0, 1, \ldots, n-1\right\}.$$

Un punt interessant de l'Exemple 1.3.10 és, que quan es fa el quocient d'un anell de polinomis mòdul un dels seus polinomis, automàticament s'obté una arrel d'aquest. És a dir, en el quocient $A[x]/(f(x))$, es té la igualtat $\overline{f(x)} = \bar{0}$ i, per tant, $f(\bar{x}) = 0$ i $\bar{x}$ és una arrel de f.

Exemple 1.3.11. Vegem un cas particular de l'Exemple 1.3.10. Sigui $A = \mathbb{R}[x]$, $I = (x^2+1)$. Aleshores $A/I = \mathbb{R}[x]/(x^2+1) = \{a + b\bar{x} \mid a, b \in \mathbb{R}\}$. Observem que l'equació $\bar{x}^2 + \bar{1} = \bar{0}$ té solució en A/I. De fet, es comprova que $A/I = \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, on la classe de x s'identifica amb el nombre complex i, veure [4].

Teorema 1.3.12 (Primer Teorema d'Isomorfisme)**.** *Sigui $f : A \longrightarrow B$ un morfisme d'anells. Aleshores, l'aplicació:*

$$\tilde{f} : A/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f),$$

amb $\tilde{f}(\bar{a}) = \overline{f(a)}$, és un isomorfisme d'anells.

Demostració. Siguin $\bar{a}, \bar{b} \in A/\mathrm{Ker}(f)$. Tenim:

1. $\tilde{f}(\overline{a+b}) = \overline{f(a+b)} = \overline{f(a)+f(b)} = \overline{f(a)} + \overline{f(b)} = \tilde{f}(a) + \tilde{f}(b)$.
2. $\tilde{f}(\overline{ab}) = \overline{f(ab)} = \overline{f(a)f(b)} = \overline{f(a)} \cdot \overline{f(b)} = \tilde{f}(a)\tilde{f}(b)$.
3. $\tilde{f}(\bar{1}) = \overline{f(1)} = 1$.

I f és clarament injectiva i exhaustiva. □

1.4 Simetrització

Sabem que els únics elements invertibles en $\mathbb{Z}$ són 1 i -1. No obstant, tot element de $\mathbb{Z}$ és invertible en $\mathbb{Q}$, on els elements són de la forma a/b, on $a, b \in \mathbb{Z}, b \neq 0$. En teoria d'anells, diem que $\mathbb{Q}$ és el cos de fraccions de l'anell $\mathbb{Z}$.

En aquesta secció introduïm el cas general d'aquest concepte. Provarem que donat un anell A, es pot construir un anell Q, contenint A, en el qual tot element de $A \setminus \mathrm{Z}(A)$ és invertible. En particular, si A és un domini, aleshores l'anell Q és un cos, i tot element de Q és de la forma a/b, on $a, b \in A, b \neq 0$.

Definició 1.4.1. Sigui S un subconjunt no buit d'un anell A. Diem que S és un sistema multiplicatiu si

1. $1 \in S$.
2. $a, b \in S \Longrightarrow ab \in S$.

Observació 1.4.2. Sigui A un anell. Aleshores $S = A \setminus Z(A)$ és un sistema multiplicatiu. En particular, si A és un domini, $S = A \setminus \{0\}$ és un sistema multiplicatiu.

Definició 1.4.3. Sigui A un anell, S un sistema multiplicatiu de A i $A \times S$ el conjunt dels parells ordenats (a, b) tals que $a \in A$ i $b \in S$. Siguin (a, b), $(c, d) \in A \times S$. Definim la relació: $(a, b) \sim (c, d) \iff \exists\, t \in S$, tal que $t(ad - bc) = 0$.

Observació 1.4.4. La relació definida prèviament és una relació d'equivalència, *i.e.,* reflexiva, simètrica i transitiva.

Nota 1.4.5. Denotem per $\frac{a}{b}$, o bé $\overline{(a,b)}$, la classe d'equivalència de (a,b). El conjunt de totes les classes d'equivalència de A es denota per $S^{-1}A$. És a dir,

$$S^{-1}A = \left\{ \overline{(a,b)} \mid a \in A, b \in S \right\} = \left\{ \frac{a}{b} \mid a \in A, b \in S \right\}.$$

Observació 1.4.6. Sigui A un anell, S un sistema multiplicatiu de A, $a/b, c/d \in S^{-1}A$. Aleshores les operacions suma $(+)$ i producte $(\cdot)$ en $S^{-1}A$, definides per:

- $\frac{a}{b} + \frac{c}{d} := \frac{(ad+bc)}{bd}$,
- $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) := \frac{ac}{bd}$,

no depenen de l'elecció del representant. És a dir, estan ben definides.

Es comprova que, amb les operacions suma i producte definides prèviament, el conjunt quocient $S^{-1}A$ té estructura d'anell.

Teorema 1.4.7. *Sigui A un anell commutatiu i unitari, S un sistema multiplicatiu. Aleshores $(S^{-1}A, +, \cdot)$ és un anell commutatiu i unitari.*

Definició 1.4.8. Sigui A un anell, S un sistema multiplicatiu. L'anell $S^{-1}A$ s'anomena *anell de fraccions de A respecte de S.*

Observació 1.4.9. Sigui A un anell, S un sistema multiplicatiu. Considerem l'aplicació

$$\begin{aligned} \varphi : A &\longrightarrow S^{-1}A \\ a &\longmapsto \varphi(a) = \frac{a}{1}. \end{aligned}$$

Tenim que φ és un morfisme d'anells, amb $\mathrm{Ker}(\varphi) = \{a \in A \mid \exists\, s \in S \text{ tal que } sa = 0\}$. En particular, si $S \cap \mathrm{Z}(A) = \varnothing$, aleshores φ és injectiva. Per tant, en aquest cas, podem identificar tot element de a amb l'element $\varphi(a) = a/1 \in S^{-1}A$. D'aquesta forma, si $S = A \setminus \mathrm{Z}(A)$, podem considerar $A \subseteq S^{-1}A$.

Teorema 1.4.10. *Sigui A un anell, $S = A \setminus Z(A)$. Aleshores l'anell de fraccions de A respecte de S, $S^{-1}A$, verifica les propietats següents:*

(i) A és un subanell de $S^{-1}A$ (amb la identificació vista a l'Observació 1.4.9).

(ii) Tot element $a \in A \setminus Z(A)$ és invertible en $S^{-1}A$.

(iii) Tot element de $S^{-1}A$ és de la forma a/b, $a \in A, b \in S$.

El Teorema 1.4.10 és vàlid per a tot anell A. Observem que en el cas particular en què A és un domini, es té $Z(A) = \{0\}$, i per tant $S = A \setminus \{0\}$. En aquest cas, amb les propietats vistes al Teorema 1.4.10 és fàcil veure que $S^{-1}A$ és un cos.

Definició 1.4.11. Sigui A un domini, $S = A \setminus \{0\}$. Aleshores el cos $S^{-1}A$ s'anomena *cos de fraccions de* A. El denotem $K(A)$.

Trivialment, podem reescriure el Teorema 1.4.10 de la forma següent.

Teorema 1.4.12. *Sigui A un domini, $K(A)$ és cos de fraccions de A. Aleshores es verifiquen les propietats següents:*

(i) A és un subanell de $K(A)$ (amb la identificació vista a l'Observació 1.4.9).

(ii) Tot element $a \in A$, $a \neq 0$, és invertible en $K(A)$.

(iii) Tot element de $K(A)$ és de la forma a/b, $a, b \in A, b \neq 0$.

Exemple 1.4.13. Considerem l'anell dels enters, $\mathbb{Z}$. Per ser $\mathbb{Z}$ un domini, podem prendre el sistema multiplicatiu $S = \mathbb{Z} \setminus \{0\}$. Aleshores el cos de fraccions de $\mathbb{Z}$ ve donat per:

$$K(\mathbb{Z}) = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\} = \mathbb{Q}.$$

1.5 Ideals maximals i primers

Tot ideal propi d'un anell A està contingut com a mínim en un ideal més gran, A. Si un ideal propi és tan gran que només està estrictament contingut en A diem que és maximal. Més formalment:

Definició 1.5.1. Sigui A un anell, $\mathfrak{m}$ un ideal de A. Diem que $\mathfrak{m}$ és un *ideal maximal* si $\mathfrak{m} \subsetneq A$ i satisfà:

$$\mathfrak{m} \subseteq J \subseteq A \Longrightarrow \mathfrak{m} = J \text{ o bé } J = A,$$

per a qualsevol ideal J de A. És a dir, si $\mathfrak{m}$ és un element maximal del conjunt:

$$\{J \mid J \text{ ideal de } A, J \neq A\},$$

per la relació d'ordre inclusió.

Definició 1.5.2. Sigui A un anell. Definim *l'espectre maximal* de A com:

$$\mathrm{Max}(A) = \{\mathfrak{m} \mid \mathfrak{m} \text{ és un ideal maximal de } A\}.$$

Els ideals maximals són de gran importància en la teoria d'anells. Malaularadament, en general no es disposa de cap mètode constructiu per a obtenir ideals maximals d'un anell donat. No obstant, el Lema de Zorn ens assegura l'existència d'ideals maximals.

Definició 1.5.3. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Sigui $X \subseteq \Sigma$ un subconjunt de Σ.

- Diem que $y \in \Sigma$ és una *cota superior de* X si $x \leq y$, per a tot $x \in X$.

- Diem que $z \in \Sigma$ és un *element maximal* de Σ si, quan es compleix $z \leq s$, per algun $s \in \Sigma$, aleshores necessàriament $z = s$.

En general no tot conjunt parcialment ordenat té elements maximals.

Definició 1.5.4. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Donat un subconjunt $X \subseteq \Sigma$, diem que X és una *cadena* de Σ si és totalment ordenat, és a dir, si per a tot parell $x, y \in X$, o bé $x \leq y$, o bé $y \leq x$.

Ens trobem ara en condicions d'enunciar el Lema de Zorn. El Lema de Zorn dona unes condicions suficients per a l'existència d'ideals maximals.

Lema 1.5.5 (Lema de Zorn)**.** *Sigui $(\Sigma, \leq)$ un conjunt no buit i parcialment ordenat on tota cadena X de Σ té cota superior en Σ. Aleshores Σ té un element maximal.*

L'enunciat del Lema de Zorn 1.5.5 és suficientment complex com per no ser un resultat intuïtiu. No obstant, és possible provar que és equivalent a l'Axioma de l'elecció, el qual és força raonable. La prova d'aquesta equivalència queda fora de l'abast d'aquest treball.

Utilitzant el Lema de Zorn 1.5.5 es pot provar el resultat següent.

Teorema 1.5.6 (Teorema d'Artin)**.** *Sigui A un anell, $A \neq \{0\}$. Aleshores A té ideals maximals.*

Demostració. Sigui $\Sigma = \{I \mid I \text{ ideal de } A, I \neq A\}$. Aleshores $(0) \in \Sigma$, per tant $\Sigma \neq \varnothing$. A més, la inclusió indueix un ordre parcial sobre Σ. Sigui X una cadena de Σ, $X = \{I_\lambda \mid \lambda \in \Lambda\}$. Prenem $I = \cup_{\lambda \in \Lambda} I_\lambda$. Vegem primer que I és un ideal. Clarament $0 \in I$, i $ax \in I$, per qualssevol $a \in A$, $x \in I$. A més, per a tot parell $x, y \in I$, es té que $x \in I_\lambda$, $y \in I_\mu$, per a certs $\lambda, \mu \in \Lambda$, i donat l'ordre total de la cadena X, sense pèrdua de generalitat, podem suposar que $I_\lambda \subseteq I_\mu \implies x + y \in I_\mu \subseteq I$. En particular, $I \in \Sigma$, ja que altrament tindríem $1 \in A = I \implies 1 \in I_\lambda$, per a algun $\lambda \in \Lambda \implies I_\lambda = A$, fet que es contradiu amb $I_\lambda \in \Sigma$. Així, doncs, I és clarament una cota superior de la cadena X. Per tant ens trobem en condicions per a aplicar el Lema de Zorn 1.5.5, i podem afirmar que existeix un element $J \in \Sigma$ maximal de Σ. Clarament J és també un ideal maximal de A. □

Un tipus molt important d'ideals maximals en teoria d'anells són els ideals primers. La noció d'ideal primer és una generalització dels elements primers en aritmètica, i els punts en geometria.

Definició 1.5.7. Sigui A un anell, $\mathfrak{p}$ un ideal de A. Diem que $\mathfrak{p}$ és un *ideal primer* de A si $\mathfrak{p} \subsetneq A$ i satisfà:

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ o bé } y \in \mathfrak{p},$$

per a tot $x, y \in A$.

Definició 1.5.8. Sigui A un anell. Definim *l'espectre primer* de A com:

$$\operatorname{Spec}(A) = \{\mathfrak{p} \mid \mathfrak{p} \text{ és un ideal primer de } A\}.$$

Lema 1.5.9. *Sigui A un anell, si $\mathfrak{m}$ és un ideal maximal, aleshores $\mathfrak{m}$ és primer.*

Demostració. Siguin $x, y \in A$ tals que $xy \in \mathfrak{m}$. Si $x \in \mathfrak{m}$, ja ho tenim. Altrament $\mathfrak{m} \subsetneq \mathfrak{m} + (x)$. Per ser $\mathfrak{m}$ maximal, $\mathfrak{m} + (x) = A$. Aleshores, $1 \in \mathfrak{m} + (x)$, és a dir, $1 = z + ax$, per a alguns $z \in \mathfrak{m}$, $a \in A$. Per tant, $y = yz + axy \in \mathfrak{m}$. □

Observació 1.5.10. El recíproc del Lema 1.5.9 no és cert en general.

Exemple 1.5.11. Sigui $A = \mathbb{Z}$, i $\mathfrak{p} = (0)$. Clarament $\mathfrak{p}$ és un ideal primer de A, ja que $\mathbb{Z}$ és un domini. En canvi, $\mathfrak{p} \subsetneq (2) \subsetneq A$, i per tant $\mathfrak{p}$ no és un ideal maximal. Més generalment, donat un domini $A \neq 0$, on A no és un cos, aleshores l'ideal (0) és primer però no maximal.

Definició 1.5.12. Sigui A un anell, $\mathfrak{p}$ un ideal primer de A. Anomenem *alçada de* $\mathfrak{p}$, si és finita, a la longitud màxima h, d'una cadena d'ideals primers $P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_h = \mathfrak{p}$ en A.

Definició 1.5.13. Sigui A un anell. Anomenem *dimensió de Krull* de A, si és finita, a l'alçada màxima d'un ideal primer de A. La dimensió de A es denota per $\dim(A)$.

La proposició següent dona una definició alternativa d'ideal primer i maximal, d'ús recurrent en demostracions.

Proposició 1.5.14. *Sigui A un anell, $\mathfrak{m}, \mathfrak{p}$ ideals de A. Aleshores:*

(i) $\mathfrak{m}$ *és maximal* $\iff {}^{A}\!/_{\mathfrak{m}}$ *és un cos.*

(ii) $\mathfrak{p}$ *és primer* $\iff {}^{A}\!/_{\mathfrak{p}}$ *és íntegre.*

Capítol 2

Anells Noetherians i Artinians

Els resultats vists en el Capítol 1 són vàlids per a qualsevol anell, recordant que en aquest treball tot anell és diferent de zero, commutatiu i unitari. Per tal d'obtenir teoremes i resultats més forts és necessari imposar certes condicions de finitud. En particular, les condicions de cadena ascendent i descendent, i d'element maximal i minimal, juguen un paper important. En aquest capítol estudiem les condicions anteriors, i distingim, en funció d'aquestes, dues classes d'anells: els anells Noetherians i els anells Artinians. La referència principal és [2].

Novament suposem, si no es diu el contrari, que tots els anells són commutatius, amb unitat 1 i $1 \neq 0$.

2.1 Anells Noetherians

Comencem per definir formalment les condicions de cadena descendent i element maximal. Veurem, en la Proposició 2.1.3, que de fet aquestes dues condicions són equivalents en un conjunt no buit parcialment ordenat.

Definició 2.1.1. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Diem que Σ verifica la *condició de cadena ascendent* (CCA), si tota cadena ascendent, és a dir, conjunt numerable totalment ordenat, estabilitza. És a dir;

$$x_1 \leq x_2 \leq \ldots \Longrightarrow \exists\, N \in \mathbb{N}, \text{ tal que } x_N = x_{N+1} = \ldots$$

Definició 2.1.2. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Diem que Σ verifica la *condició de l'element maximal* (CMax), si tot subconjunt no buit de Σ té un element maximal.

Proposició 2.1.3. *Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Aleshores són equivalents:*

(i) Σ verifica la CCA;

(ii) Σ verifica la CMax.

Demostració. (i) $\Longrightarrow$ (ii). Sigui X un subconjunt de Σ, X no buit. Suposem que X no té element maximal. Prenem $x_0 \in X$. Com que x_0 no és maximal, podem prendre $x_1 \in X \setminus \{x_0\}$, amb $x_1 > x_0$. Com que x_1 no és maximal, podem prendre $x_2 \in X \setminus \{x_0, x_1\}$, amb $x_2 > x_1$. Recursivament, construïm una successió $(x_i)_i$, amb $x_i \in X \setminus \{x_0, \ldots, x_{i-1}\}$, i $x_i > x_{i-1}$, per a tot i. Aleshores, la cadena ascendent:

$$x_0 < x_1 < x_2 < \ldots,$$

no estabilitza, fet que es contradiu amb la hipòtesi.
(i) $\Longleftarrow$ (ii). Sigui

$$x_0 \leq x_1 \leq x_2 \leq \ldots,$$

una cadena ascendent de Σ. Considerem el conjunt $X = \{x_0, x_1, \ldots\}$. Per hipòtesi, X té un element maximal. Sigui x_N l'element maximal de X, aleshores és clar que la cadena estabilitza a partir de N. □

Les definicions i proposició prèvies són vàlides per a tot conjunt no buit parcialment ordenat. Observem que en un anell, A, la inclusió, $\subseteq$, indueix un ordre parcial en el conjunt format pels ideals de A. Amb aquestes nocions podem introduir els anells Noetherians, una classe d'anells de gran importància en geometria i en algebra commutativa.

Teorema 2.1.4. *Sigui A un anell. Aleshores són equivalents:*

(i) el conjunt dels ideals de A verifica la CCA;

(ii) el conjunt dels ideals de A verifica la CMax;

(iii) tot ideal I de A és finitament generat.

Demostració. (i) $\Longleftrightarrow$ (ii). Vist a la Proposició 2.1.3.
(i) $\Longrightarrow$ (iii). Sigui I un ideal de A. Suposem que I no és finitament generat. Prenem $a_0 \in I$. Com que I no és finitament generat, podem prendre $a_1 \in I \setminus (a_0)$. De nou, com que I no és finitament generat, prenem $a_2 \in I \setminus \langle a_0, a_1 \rangle$. Recursivament, construïm una successió $(a_i)_i$, tal que, $a_i \in I \setminus \langle a_0, a_1, \ldots, a_{i-1} \rangle$, per a tot i. Aleshores:

$$(a_0) \subsetneq \langle a_0, a_1 \rangle \subsetneq \langle a_0, a_1, a_2 \rangle \subsetneq \ldots,$$

és una cadena ascendent d'ideals que no estabilitza, la qual cosa suposa una contradicció amb la hipòtesi.
(i) $\Longleftarrow$ (iii). Sigui

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots,$$

una cadena ascendent d'ideals de A. Considerem $I = \bigcup_{i \geq 0} I_i$. Es comprova fàcilment que I és un ideal. Per hipòtesi $I = \langle a_1, \ldots, a_m \rangle$, per tant, existeix N tal que $a_1, \ldots, a_m \in I_N$. Així doncs, la cadena estabilitza a partir de I_N. □

Definició 2.1.5. Sigui A un anell. Diem que A és *Noetherià* si A satisfà les condicions equivalents del Teorema 2.1.4.

Proposició 2.1.6. *Sigui A un anell Noetherià, I un ideal de A. Aleshores A/I és Noetherià.*

Demostració. Vegem que tot ideal de A/I és finitament generat. Sigui $\overline{J}$ un ideal de A/I. Per la Proposició 1.3.8, sabem que J és un ideal de A que conté I. Com que A és Noetherià, $A = \langle x_0, \ldots, x_n \rangle$, per a alguns $x_0, \ldots, x_n \in A$. Aleshores, $\overline{J} = \langle \overline{x_0}, \ldots, \overline{x_n} \rangle$ en A/I. □

2.2 Anells Artinians

Anàlogament, de forma dual, es pot definir la condició de cadena descendent i la condició d'element minimal en un conjunt no buit parcialment ordenat. És fàcil veure que aquestes dues condicions són equivalents.

Definició 2.2.1. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Diem que Σ verifica la *condició de cadena descendent* (CCD), si tota cadena descendent estabilitza, és a dir;

$$x_1 \geq x_2 \geq \ldots \Longrightarrow \exists\, N \in \mathbb{N}, \text{ tal que } x_N = x_{N+1} = \ldots$$

Definició 2.2.2. Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Diem que Σ verifica la *condició de l'element minimal* (CMin), si tot subconjunt no buit de Σ té un element minimal.

Proposició 2.2.3. *Sigui $(\Sigma, \leq)$ un conjunt no buit parcialment ordenat. Aleshores són equivalents:*

(i) Σ verifica la CCD;

(ii) Σ verifica la CMin.

Definició 2.2.4. Sigui A un anell. Diem que A és *Artinià* si el conjunt dels ideals de A satisfà les condicions equivalents de la Proposició 2.2.3.

Proposició 2.2.5. *Sigui A un anell Artinià, I un ideal de A. Aleshores A/I és Artinià.*

Demostració. Donada una cadena descendent d'ideals de A/I, per la Proposició 1.3.8, sabem que és de la forma:

$$\overline{J}_0 \supseteq \overline{J}_1 \supseteq \overline{J}_2 \supseteq \ldots,$$

on els J_i són ideals de A que contenen I. Aleshores, $J_0 \supseteq J_1 \supseteq J_2 \supseteq \ldots$ és una cadena descendent d'ideals de A que contenen I. Com que A és Artinià, $J_N = J_{N+1} = \ldots$, per a algun $N \geq 0$. Aleshores, $\overline{J}_N = \overline{J}_{N+1} = \ldots$, i per tant, la cadena estabilitza. □

2.3 Una altra caracterització dels Anells Artinians

Tot i l'aparent similitud en les definicions d'anell Artinià i anell Noetherià, la condició Artiniana és molt més restrictiva. De fet, es comprova el següent:

Teorema 2.3.1. *Sigui A un anell. Aleshores:*

$$A \text{ és un anell Artinià} \iff A \text{ és un anell Noetherià i } \dim(A) = 0.$$

Per tal de provar les implicacions anteriors, és necessari introduir els conceptes de radical i mòdul, i fer algunes deduccions que deriven de les condicions Noetheriana i Artiniana.

Definició 2.3.2. Sigui A un anell, I un ideal de A. El *radical* de I, denotat per $\mathrm{rad}(I)$, és

$$\mathrm{rad}(I) = \{x \in A \mid x^n \in I, \text{ per a algun } n > 0\}.$$

Observació 2.3.3. Sigui A un anell, I un ideal de A. Aleshores $\mathrm{rad}(I)$ és un ideal de A.

Demostració. Clarament $0 \in \mathrm{rad}(I)$. Sigui $x \in \mathrm{rad}(I)$, $a \in A$. Com que $x \in \mathrm{rad}(I)$, $x^n \in I$, per a algun $n > 0$. Aleshores $(ax)^n = a^n x^n \in I$, i per tant $ax \in \mathrm{rad}(I)$. Prenem ara $y \in \mathrm{rad}(I)$, amb $y^m \in I$, per a algun $m > 0$. Sigui $l := n + m - 1$. Aleshores, tenim:

$$(x+y)^l = \sum_{k=0}^{l} \binom{n}{k} x^{l-k} y^k.$$

Cadascun dels termes de l'expressió anterior és de la forma $x^{l-k}y^k$. Si $k \geq m$, aleshores $y^k \in I \implies x^{l-k}y^k \in I$. Altrament, $x^{l-k} \in I \implies x^{l-k}y^k \in I$. Per tant, $(x+y)^l \in I$ i $(x+y) \in \mathrm{r}(I)$. □

Definició 2.3.4. Sigui A un anell. Anomenem *nilradical* de A al conjunt dels elements nilpotents de A. El denotem $\mathfrak{n}(A)$. És a dir:

$$\mathfrak{n}(A) = \mathrm{rad}(0) = \{x \in A \mid x^n = 0, \text{ per a algun } n > 0\}.$$

Proposició 2.3.5. *Sigui A un anell. Aleshores el nilradical de A és la intersecció de tots els ideals primers de A.*

Demostració. Sigui $\mathfrak{n}'$ la intersecció de tots els ideals primers de A. Hem de veure que $\mathfrak{n}' = \mathfrak{n}(A)$. Comencem per veure que $\mathfrak{n}(A) \subseteq \mathfrak{n}'$. Sigui $x \in \mathfrak{n}(A)$. Aleshores $x^n = 0$, per a algun $n > 0$. Sigui $\mathfrak{p}$ un ideal primer de A qualsevol. Tenim que $x^n = 0 \in \mathfrak{p}$ i, com que $\mathfrak{p}$ primer, necessàriament $x \in \mathfrak{p}$. És a dir, x pertany a tots els ideals primers de A i, conseqüentment, $x \in \mathfrak{n}'$. Recíprocament, suposem que $x \in A$ no és nilpotent. Sigui

$$\Sigma = \{I \subseteq A \mid I \text{ ideal de } A,\ x^n \notin I, \forall n > 0\}.$$

Clarament $(0) \in \Sigma$ i, amb la inclusió, Σ és un conjunt no buit, parcialment ordenat, on tota cadena té cota superior. Pel Lema de Zorn 1.5.5, Σ té un element maximal. Sigui J l'element maximal de Σ. Vegem que J és primer. Siguin $a, b \notin J$. Aleshores els ideals $J + (a)$ i $J + (b)$ contenen estrictament a $\mathfrak{p}$ i, per tant, no pertanyen a Σ (ja que $\mathfrak{p}$ és maximal en Σ). Així, $x^n \in J + (a)$, i $x^m \in J + (b)$, per a alguns $n, m > 0$. Per tant, $x^{n+m} \in J + (ab)$ i, conseqüentment, $J + (ab) \notin \Sigma$. Aleshores, necessàriament $ab \notin J$, la qual cosa implica que J és primer. Així, docns, hem trobat un ideal primer de A que no conté a x, és a dir, $x \notin \mathfrak{n}'$. □

Vegem primerament algunes propietats que deriven de la condició Noetheriana. Començant per provar que el nilradical d'un anell Noetherià és nilpotent. De fet, provarem el resultat següent, més general.

Proposició 2.3.6. *Sigui A un anell Noetherià. Aleshores tot ideal de A conté una potència del seu radical.*

Demostració. Sigui I un ideal de A, $\mathrm{rad}(I)$ el seu radical. En particular, per l'Observació 2.3.3, $\mathrm{rad}(I)$ és també un ideal de A. Per ser A Noetherià, $\mathrm{rad}(I)$ és finitament generat. Siguin $x_1, \ldots, x_n \in A$, tals que $\mathrm{rad}(I) = \langle x_1, \ldots, x_n \rangle$. Aleshores, per a tot $i = 1, \ldots, n$, tenim $x_i^{n_i} \in I$, per a algun $n_i > 0$. Sigui $m = (\sum_{i=1}^n n_i - 1) + 1$. Aplicant la fòrmula del Binomi de Newton, obtenim que tot element de $\mathrm{rad}(I)^m$ està generat pels productes $x_1^{k_1} \cdots x_n^{k_n}$, amb $\sum_{i=1}^n k_i = m$. Per la definició de m, necessàriament $k_i \geq n_i$, per a algun i. És a dir, tots els productes $x_1^{k_1} \cdots x_n^{k_n}$, amb $\sum_{i=1}^n k_i = m$, pertanyen a $\mathrm{rad}(I)$ i, per tant, $\mathrm{rad}(I)^m \subseteq \mathrm{r}(I)$. □

Corol·lari 2.3.7. *Sigui A un anell Noetherià. Aleshores el nilradical de A és nilpotent.*

Amb l'ajuda dels propers resultats, es comprova que, en els anells Noetherians, el nilradical es pot expressar com una intersecció finita d'ideals primers.

Observació 2.3.8. Sigui A un anell reduït, és a dir, $\mathfrak{n}(A) = 0$. Si $a, b \in A$, i $ab = 0$, aleshores $\mathrm{rad}(a) \cap \mathrm{rad}(b) = 0$.

Demostració. En efecte, és fàcil veure que $\mathrm{rad}(a) \cap \mathrm{rad}(b) = \mathrm{rad}(ab)$. Per tant, $\mathrm{rad}(a) \cap \mathrm{rad}(b) = \mathrm{rad}(ab) = \mathrm{rad}(0) = \mathfrak{n}(A) = 0$. □

Proposició 2.3.9. *Sigui A un anell, I un ideal radical de A, és a dir, rad$(I) = I$. Si $a, b \in A$ són tals que $ab \in I$, aleshores $I = \mathrm{rad}(I + (a)) \cap \mathrm{rad}(I + (b))$.*

Demostració. Prenem $B = A/I$. Com que I és un ideal radical, aleshores B és un anell reduït. En efecte, si $\bar{x} \in B$ és tal que $\bar{x}^n = 0$, per a algun $n > 0$, aleshores $x^n \in I \Longrightarrow x \in \mathrm{rad}(I) = I \Longrightarrow \bar{x} = 0$. Com que $ab \in I$, aleshores $\overline{ab} = \bar{0}$ en B. Aplicant l'Observació 2.3.8, tenim $\mathrm{rad}(\bar{a}) \cap \mathrm{rad}(\bar{b}) = (\bar{0})$. És a dir,

$$\mathrm{rad}\left((I + (a))/I\right) \cap \mathrm{rad}\left((I + (b))/I\right) = (\bar{0}) \text{ en } B.$$

Així, doncs,

$$(\bar{0}) = (\mathrm{rad}(I + (a))/I) \cap (\mathrm{rad}(I + (b))/I).$$

És a dir, $I = \mathrm{rad}(I + (a)) \cap \mathrm{rad}(I + (b))$, per la Proposició 1.3.8. □

Proposició 2.3.10. *Sigui A un anell Noetherià. Aleshores tot ideal radical de A és intersecció finita d'ideals primers.*

Demostració. Sigui

$$\Sigma = \{I \mid I \text{ ideal radical de } A,\ I \text{ no és intersecció finita d'ideals primers de } A\}.$$

Volem veure que $\Sigma = \varnothing$. Suposem que $\Sigma \neq \varnothing$. Com que A és Noetherià, existeix $I \in \Sigma$ element maximal de Σ. En particular, I no és primer. Per tant, existeixen $a, b \in A$, tals que $ab \in I$, i $a, b \notin I$. Per la Proposició 2.3.9, $I = \mathrm{rad}(I + (a)) \cap \mathrm{rad}(I + (b))$. Observem que $I \subsetneq I + (a) \subseteq \mathrm{rad}(I + (a))$ i, anàlogament, $I \subsetneq \mathrm{rad}(I + (b))$. Com que I és element maximal de Σ, aleshores $\mathrm{rad}(I + (a))$ i $\mathrm{rad}(I + (b))$ no són de Σ. Per tant, $\mathrm{rad}(I + (a))$ i $\mathrm{rad}(I + (b))$ són intersecció finita d'ideals primers i, en particular, $I = \mathrm{rad}(I + (a)) \cap \mathrm{rad}(I + (b))$ és intersecció finita de primers, la qual cosa suposa una contradicció. □

Corol·lari 2.3.11. *Sigui A un anell Noetherià. Aleshores el nilradical de A és intersecció finita d'ideals primers de A.*

Demostració. Tenim $\mathfrak{n}(A) = \text{rad}(0)$ és un ideal radical. Aplicant la Proposició 2.3.10, ja ho tenim. □

Estudiem ara algunes de les propietats dels anells Artinians. Començant per provar que els anells Artinians tenen, efectivament, dimensió zero.

Proposició 2.3.12. *Sigui A un anell Artinià. Aleshores tot ideal primer de A és maximal.*

Demostració. Sigui $\mathfrak{p}$ un ideal primer de A. Aleshores, per les Proposicions 1.3.8 i 2.2.5, tenim que $B = A/\mathfrak{p}$ és un domini Artinià. Sigui $x \in B$, $x \neq 0$. Aleshores, per la CCD, $(x^N) = (x^{N+1})$, per a cert $N \in \mathbb{N}$. Per tant, $x^N = x^{N+1}y = x^N xy$, per a algun $y \in B$. Com B és un domini i $x \neq 0$, necessàriament $xy = 1$. És a dir, x és invertible en B, la qual cosa implica que B és un cos. Concloem, de nou per la Proposició 1.3.8, que $\mathfrak{p}$ és maximal. □

Corol·lari 2.3.13. *Sigui A un anell Artinià. Aleshores* $\dim(A) = 0$.

El Corol·lari 2.3.7, ens assegura que en un anell Noetherià, el nilradical és nilpotent. Vegem que aquesta propietat també es verifica en els anells Artinians.

Proposició 2.3.14. *Sigui A un anell Artinià. Aleshores el nilradical de A és nilpotent.*

Demostració. Com que A verifica la CCD, $\mathfrak{n}(A)^k = \mathfrak{n}(A)^{k+1} = \ldots =: I$, per a algun $k > 0$. Suposem que $I \neq (0)$. Sigui

$$\Sigma = \{J \mid J \text{ ideal de A, } IJ \neq (0)\}.$$

Aleshores $I \in \Sigma \neq \varnothing$. Com que A és Artinià i Σ no buit, sabem que existeix K un element minimal de Σ. Com que $JK \neq (0)$, aleshores existeix $x \in K$, tal que $xI \neq (0)$. Tenim $(x) \subseteq K$ i $(x) \in \Sigma$. Per la minimalitat de K en Σ, necessàriament $(x) = K$. Però $(xI)I = xI^2 = xI \neq (0)$ i $xI \subseteq (x)$. De nou, per la minimalitat de $(x) = K$, tenim $(x) = xI$. Així, $x = xy$, per a algun $y \in I$. Per tant, $x = xy = xy^2 = \ldots = xy^n = \ldots$. Però $y \in I = \mathfrak{n}(A)^k \subseteq \mathfrak{n}(A)$. Per tant, y és nilpotent i $x = 0$, la qual cosa suposa una contradicció. □

A partir del lema següent, es demostra que els anells Artinians tenen un nombre finit d'ideals maximals.

Lema 2.3.15. *Sigui A un anell, $I_1, \ldots, I_n$ ideals de A, $\mathfrak{p}$ un ideal primer de A. Suposem que $\cap_{i=1}^n I_i \subseteq \mathfrak{p}$. Aleshores $I_i \subseteq \mathfrak{p}$, per a algun i.*

Demostració. Suposem que $I_i \nsubseteq \mathfrak{p}$, per a tot i. Aleshores, per a cada i, existeix x_i, tal que $x_i \in I_i$, $x_i \notin \mathfrak{p}$. Per tant, $\prod_i x_i \in \prod_i I_i \subseteq \cap_i I_i$. Però, $\prod_i x_i \notin \mathfrak{p}$, ja que $\mathfrak{p}$ és primer. Per tant, $\cap_{i=1}^n I_i \nsubseteq \mathfrak{p}$. □

Proposició 2.3.16. *Sigui A un anell Artinià. Aleshores A té un nombre finit d'ideals maximals.*

Demostració. Considerem el conjunt format per totes les interseccions finites $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r$, on els m_i són ideals maximals. Aquest conjunt té un element minimal. Sigui $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ l'element minimal. Aleshores, per a tot ideal maximal $\mathfrak{m}$, es té $\mathfrak{m} \cap \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. Pel Lema 2.3.15, tenim que $\mathfrak{m}_i \subseteq \mathfrak{m}$, per a algun i, i per ser m_i maximal, es té $\mathfrak{m} = \mathfrak{m}_i$. □

Un punt clau de la demostració del Teorema 2.3.1, es basa en el fet que, en un anell en el qual l'ideal (0) es pot expressar com a producte finit d'ideals maximals, les condicions Noetheriana i Artiniana són equivalents. Per tal de demostrar aquest resultat, és necessari introduir el concepte de mòduls.

Definició 2.3.17. Sigui $(M, +)$ un grup abelià i A un anell commutatiu i unitari. Una *estructura de A-mòdul en M* és una aplicació:

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, x) &\longmapsto ax, \end{aligned}$$

que anomenem producte per elements de A, tal que, per a tot $a, b \in A$, $x, y \in M$, verifica:

1. $a(x + y) = ax + ay$.
2. $(a + b)x = ax + bx$.
3. $(ab)x = a(bx)$.
4. $1 \cdot x = x$.

Observació 2.3.18. Si A és un cos, un A-mòdul és el mateix que un espai vectorial sobre A.

Observació 2.3.19. Si $A = \mathbb{Z}$, els $\mathbb{Z}$-mòduls són els grups abelians.

Observació 2.3.20. Totes les definicions vàlides en teoria d'espais vectorials es poden estendre a la teoria de mòduls excepte aquelles en que s'hagi de dividir per escalars.

Definició 2.3.21. Un A-mòdul M es diu *Noetherià* si la família de submòduls de M verifica la CCA. Anàlogament, un A-mòdul M es diu *Artinià* si la família de submòduls de M verifica la CCD.

Proposició 2.3.22. *Sigui $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ una successió exacta de A-mòduls. És a dir, f injectiva, $\mathrm{Im}(f) = \mathrm{Ker}(g)$ i g exhaustiva. Aleshores, M_2 és Noetherià (respectivament, Artinià) $\iff$ M_1 i M_3 són Noetherians (respectivament, Artinians).*

Demostració. Veurem la demostració per al cas Noetherià. Per al cas Artinià la prova es realitza de forma similar.
($\Longrightarrow$). Una cadena ascendent de submòduls de M_1 (o M_3') dona una cadena ascendent de submòduls de M_2 i, per tant, estabilitza.
($\Longleftarrow$). Sigui $(L_n)_{n\geq 0}$ una cadena ascendent de submòduls de M_1. Aleshores $(g(L_n))_{n\geq 0}$ és una cadena en M_3, i $(f^{-1}(L_n))_{n\geq 0}$ és una cadena en M_1. Per a n prou gran, ambdues cadenes estabilitzen i per tant, $(L_n)_{n\geq 0}$ estabilitza. □

Proposició 2.3.23. *Sigui E un $\mathbb{K}$-espai vectorial. Aleshores són equivalents:*

(i) E és de dimensió finita;

(ii) tota cadena de subespais vectorials de E té un nombre finit d'inclusions estrictes;

(iii) el conjunt dels subespais vectorials de E verifica la CCA;

(iv) el conjunt dels subespais vectorials de E verifica la CCD.

Demostració. (i) $\Longrightarrow$ (ii). Trivial.
(ii) $\Longrightarrow$ (iii) i (iv). És clar per la pròpia definició.
(iii) i (iv) $\Longrightarrow$ (i). Suposem que E és de dimensió infinita. Sigui $(x_n)_{n\geq 0}$ un conjunt infinit numerable de vectors linealment independents de E. Sigui U_n, respectivament V_n, el subespai vectorial generat per $x_1, \ldots, x_n$, respectivament, $x_{n+1}, x_{n+2}, \ldots$. Aleshores, la cadena $(U_n)_{n\geq 0}$, respectivament, $(V_n)_{n\geq 0}$, és infinita i estrictament ascendent, respectivament, descendent. □

Proposició 2.3.24. *Sigui A un anell en el qual el producte $\mathfrak{m}_1 \cdots \mathfrak{m}_n$, on els $\mathfrak{m}_i$ són ideals maximals de A no necessàriament diferents, és igual a l'ideal (0). Aleshores A és Noetherià si i només si A és Artinià.*

Demostració. Tenim les successions exactes

$$\begin{aligned}
&0 \longrightarrow \mathfrak{m}_1 \longrightarrow A \longrightarrow A/\mathfrak{m}_1 \longrightarrow 0,\\
&0 \longrightarrow \mathfrak{m}_1\mathfrak{m}_2 \longrightarrow \mathfrak{m}_1 \longrightarrow \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2 \longrightarrow 0,\\
&\ldots\\
&0 \longrightarrow (\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}) \longrightarrow (\mathfrak{m}_1 \cdots \mathfrak{m}_{n-2}) \longrightarrow (\mathfrak{m}_1 \cdots \mathfrak{m}_{n-2})/(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}) \longrightarrow 0.
\end{aligned}$$

De les successions exactes i de la Proposició 2.3.22, es dedueix que A és Noetherià $\Longleftrightarrow$ $A/\mathfrak{m}_1$, $\mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2$, …, $(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-2})/(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1})$ són Noetherians. Com els $\mathfrak{m}_i$ són maximals, $A/\mathfrak{m}_i$ és un cos. Observem que els factors $(\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1})/(\mathfrak{m}_1 \cdots \mathfrak{m}_i)$, són espais vectorials sobre el cos $A/\mathfrak{m}_i$. Per tant, per la Proposició 2.3.23, $A/\mathfrak{m}_1$, $\mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2$, …, $(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-2})/(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1})$ són Noetherians si i només si són Artinians. Així, de nou per la Proposició 2.3.22, $A/\mathfrak{m}_1$, $\mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2$,…, $(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-2})/(\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1})$ són Artinians si i només si A és Artinià. □

Ens trobem ara en condicions d'abordar la demostració del Teorema 2.3.1.

Demostració del Teorema 2.3.1. ($\Longrightarrow$). Pel Corol·lari 2.3.13, tenim que $\dim(A) = 0$. Per tant, $\mathrm{Spec}(A) = \mathrm{Max}(A)$. A més, la Proposició 2.3.16 ens assegura que A té un nombre finit d'ideals maximals. Siguin $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, els ideals maximals de A. Aleshores, $\mathfrak{n}(A) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. Per la Proposició 2.3.14, existeix $k > 0$, tal que $\mathfrak{n}(A)^k = (0)$. Així, com que $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$, aleshores:

$$\mathfrak{m}_1^k \cdots \mathfrak{m}_n^k \subseteq (\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n)^k = \mathfrak{n}(A)^k = 0.$$

Per tant, com A és Artinià, per la Proposició 2.3.24, A és Noetherià.
($\Longleftarrow$). Per hipòtesi, $\dim(A) = 0$. Per tant, $\mathrm{Spec}(A) = \mathrm{Max}(A)$. Pel Corol·lari 2.3.11, tenim

$\mathfrak{n}(A) = \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_n$, amb $\mathfrak{m}_i \in \text{Max}(A)$. Pel Corol·lari 2.3.7, $\exists\, k \geq 1$, tal que $\mathfrak{n}(A)^k = 0$. Com en la implicació anterior, tenim que $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap ... \cap \mathfrak{m}_n$, aleshores:

$$\mathfrak{m}_1^k \cdots \mathfrak{m}_n^k \subseteq (\mathfrak{m}_1 \cap ... \cap \mathfrak{m}_n)^k = \mathfrak{n}(A)^k = 0.$$

Com A és Noetherià, per la Proposició 2.3.24, deduïm que A és Artinià. □

Capítol 3

Famílies de dominis

En aquest capítol estudiem la teoria de la divisibilitat en dominis. Així, suposem que tots els anells són diferents de zero, commutatius, unitaris i íntegres. Les referències principals són [2], [1] i [9].

3.1 Divisibilitat

Recordem que, si no s'indica explícitament el contrari, a partir d'ara tots els anells són diferents de zero, commutatius, unitaris i íntegres.

Definició 3.1.1. Sigui A un domini, $x, y \in A$. Diem que x *divideix* y (o y és *múltiple* de x) si existeix $z \in A$, tal que $y = xz$. Escrivim $x|y$, o bé $y = \dot{x}$. L'element z s'anomena *quocient* de y per x.

Observació 3.1.2. És trivial veure que $x|y \iff (y) \subseteq (x)$. És a dir, l'estudi de la divisibilitat és equivalent a l'estudi de les relacions d'inclusió entre els ideals principals.

Observació 3.1.3. Sigui A un domini, $x, y \in A$. Són equivalents:

(i) existeix un element $u \in A^*$, tal que $y = ux$;

(ii) $x|y$ i $y|x$;

(iii) $(x) = (y)$.

Demostració. (i) $\implies$ (ii). De l'expressió $y = ux$, deduïm que $x|y$. A més, com que $u \in A^*$, multiplicant ambdós costats de $y = ux$, per u^{-1}, obtenim $u^{-1}y = x$, provant que $y|x$.
(ii) $\implies$ (iii). En aquest cas tenim $(y) \subseteq (x)$ i $(x) \subseteq (y)$, és a dir, $(y) = (x)$.
(iii) $\implies$ (i). En particular $y \in (x)$, i per tant $\exists\, u \in A$ tal que $y = ux$. Vegem ara que $u \in A^*$. Per hipòtesi tenim que $x \in (y)$, és a dir, $\exists\, w \in A$ tal que $x = wy$. Substituint $x = wy$, en l'expressió $y = ux$, obtenim: $y = uwy \implies y - uwy = 0 \implies y(1 - uw) = 0$. Per ser A domini, la darrera expressió implica que o bé $y = 0$ o bé $1 - uw = 0$. Si $y = 0$, aleshores $x = 0$ i podem prendre $u = 1 \in A^*$. Altrament $uw = 1$, i per tant $u \in A^*$. □

Definició 3.1.4. Sigui A un domini, $x, y \in A$. Diem que x i y són *associats*, i denotem $x \sim y$, si es compleix la condició (i) (equivalentment (ii) o bé (iii)) de l'Observació 3.1.3.

Observació 3.1.5. La relació $x \sim y$,"ser associats", és una relació d'equivalència, *i.e.*, verifica les propietats reflexiva, simètrica i transitiva.

En l'estudi de la divisibilitat, els elements els distingirem llevat classe d'equivalència per la relació ser associat.

Definició 3.1.6. Sigui A un domini, $a, b \in A$:

- Diem que $d \in A$ és un *màxim comú divisor* de a i b, i el denotem $d = \text{mcd}(a, b)$, si

$$d|a, d|b, \text{ i, si } c|a, c|b \Longrightarrow c|d,$$

  per a qualsevol $c \in A$. Dit amb altres paraules, $d = \text{mcd}(a, b)$ si, $\langle a, b\rangle \subseteq (d)$, i (d) és el menor ideal principal de A que compleix aquesta propietat, *i.e.*, $\langle a, b\rangle \subseteq (c) \Longrightarrow (d) \subseteq (c)$, per a qualsevol $c \in A$.

- Diem que $m \in A$ és un *mínim comú múltiple* de a i b, i el denotem $m = \text{mcm}(a, b)$, si

$$m = \dot{a}, m = \dot{b}, \text{ i, si } c = \dot{a}, c = \dot{b} \Longrightarrow c = \dot{m},$$

  per a qualsevol $c \in A$. Dit amb altres paraules, $m =$mcm(a, b) si, $(m) \subseteq (a) \cap (b)$, i (m) és el major ideal principal de A que compleix aquesta propietat, *i.e.*, $(c) \subseteq (a) \cap (b) \Longrightarrow (c) \subseteq (m)$, per a qualsevol $c \in A$.

Aquestes definicions s'estenen de forma immediata per a tot nombre finit d'elements.

Observació 3.1.7. Sigui A un domini, $a, b \in A$. Siguin $d, d', m, m' \in A$. Suposem que $d =$mcd(a, b), $m =$mcm(a, b). Aleshores:

$$d \sim d' \Longleftrightarrow d' \text{ és un màxim comú divisor de } a \text{ i } b;$$
$$m \sim m' \Longleftrightarrow m' \text{ és un mínim comú múltiple de } a \text{ i } b.$$

Demostració. ($\Longrightarrow$). Comencem pel primer cas. Sigui $d' \in A$, tal que $d \sim d'$. Vegem que d' és un màxim comú divisor de a i b. Sabem que $d' = du$, per a algun $u \in A^*$. Al seu torn, per hipòtesi, d és un màxim comú divisor de a i b, i en particular, $d \mid a$ i $d \mid b$, és a dir, $a = \alpha d$, $b = \beta d$, per a certs $\alpha, \beta \in A$. Com que $d = u^{-1}d'$, obtenim $a = \alpha u^{-1}d'$, $b = \beta u^{-1}d' \Longrightarrow d' \mid a, d' \mid b$. Suposem ara que existeix $c \in A$, tal que $c \mid a$, $c \mid b$. Per hipòtesi, $c \mid d$, és a dir, existeix $\delta \in A$, tal que $d = \delta c \Longrightarrow u^{-1}d' = \delta c \Longrightarrow d' = u\delta c \Longrightarrow c \mid d'$. Per tant, d' és un màxim comú divisor de a i b.

Provem ara el segon cas. Sigui $m' \in A$, tal que $m \sim m'$. Vegem que m' és un mínim comú múltiple de a i b. Sabem que $m' = um$, per a algun $u \in A^*$. Al seu torn, per hipòtesi, m és un mínim comú múltiple de a i b, i en particular, $m = \dot{a}$ i $m = \dot{b}$, és a dir, $m = \alpha a$, $m = \beta b$, per a certs $\alpha, \beta \in A$. Prenent $m = u^{-1}m'$, obtenim $u^{-1}m' = \alpha a \Longrightarrow m' = u\alpha a \Longrightarrow m' = \dot{a}$, i $u^{-1}m' = \beta b \Longrightarrow m' = u\beta b \Longrightarrow m' = \dot{b}$. Suposem ara que existeix $c \in A$, tal que $c = \dot{a}, c = \dot{b}$.

Per hipòtesi, $c = \dot{m}$, és a dir, existeix $\delta \in A$, tal que $c = \delta m \Longrightarrow c = \delta u^{-1} m' \Longrightarrow c = \dot{m'}$. Per tant, m' és un mínim comú múltiple de a i b.

($\Longleftarrow$). En el primer cas, per hipòtesi tenim que d i d' són màxims comuns divisors de a i b, i en particular, d' i d són divisors de a i b. Per ser d màxim comú divisor de a i b, i d' divisor de a i b, es té que $d' \mid d$. Anàlogament, obtenim que $d \mid d'$. És a dir, $d \sim d'$.

Finalment, tenim que m i m' són mínims comuns múltiples de a i b, i en particular, m i m' són múltiples de a i b. Per ser m mínim comú múltiple de a i b, i m' i múltiple de a i b, es té que $m' = \dot{m}$. Anàlogament, obtenim que $m = \dot{m'}$. És a dir, $m \sim m'$ □

Així doncs, les notacions 'mcd(a, b)', respectivament, 'mcm(a, b)', fan referència a la classe d'associats formada per tots els màxims comuns divisors de a i b, respectivament, tots els mínims comuns múltiples de a i b. És clar, en certes ocasions cometem un abús del llenguatge. Per exemple, en dominis com $\mathbb{Z}$, i $\mathbb{K}[x]$, parlem de *el* màxim comú divisor de dos elements ja que existeix un representant destacat d'entre tots els elements de la classe d'associats: l'enter positiu a $\mathbb{Z}$ i el polinomi mònic a $\mathbb{K}[x]$.

3.2 Dominis GCD

Definició 3.2.1. Sigui A un domini. Diem que A és un *domini GCD* (de l'anglès, 'greatest common divisor') si tot parell d'elements de A té un màxim comú divisor.

Veurem que els dominis GCD es poden definir de forma equivalent com dominis on tot parell d'elements té un mínim comú múltiple.

Proposició 3.2.2. *Sigui A un domini, $a, b \in A$. Aleshores es verifica:*

(i) existeix el mínim comú múltiple de a i $b \Longleftrightarrow (a) \cap (b)$ és un ideal principal. En particular, en aquest cas el mínim comú múltiple de a i b és un generador de l'ideal $(a) \cap (b)$;

(ii) existeix el mínim comú múltiple de a i $b \Longrightarrow$ existeix el màxim comú divisor de a i b.

Demostració. (i) ($\Longrightarrow$). Suposem que m = mcm(a,b). Vegem que $(a) \cap (b) = (m)$. En efecte, si $x \in (a) \cap (b) \Longrightarrow x = au$ i $x = bv$, per a certs $u, v \in A$. És a dir, x és múltiple comú de a i b. Per definició de mcm, x és múltiple de m, o sigui $x \in (m)$. Recíprocament, sigui $x \in (m)$. Com que m = mcm(a,b), aleshores $m = au$ i $m = bv$, per a certs $u, v \in A$. Per tant $x = my = auy = bvy$ i $x \in (a) \cap (b)$.
($\Longleftarrow$). Suposem que $(a) \cap (b) = (m)$. Vegem que m = mcm(a,b). En efecte, com que $m \in (m) = (a) \cap (b) \Longrightarrow m = ax = by$, per a certs $x, y \in A$. Per tant, m és un múltiple comú de a i b. D'altra banda, si m' és un altre múltiple comú de a i b, aleshores $m' \in (a) \cap (b)$. Per tant, $m' \in (m)$ i $m' = \dot{m}$. Així m és mcm(a, b).
(ii). Suposem que existeix m = mcm(a,b). Per la propietat (i), $(a) \cap (b) = (m)$ és un ideal principal generat pel mínim comú múltiple. Com que $ab \in (a) \cap (b) = (m)$, aleshores $ab = md$,

amb $d \in A$. Vegem que d és un $\mathrm{mcd}(a,b)$, on $d = ab/m$. En efecte, tenim $m = ax = by$, per a certs $x, y \in A$. A més, $ab = md = axd = byd$. Simplificant, $a = yd$ i $b = xd$. Per tant, d és un divisor comú de a i b. Suposem que $d' \mid a$ i $d' \mid b$. Aleshores $a = d'u$ i $b = d'v$, per a certs $u, v \in A$. Multiplicant $a = d'u$ per v obtenim $av = d'uv = bu$. O sigui, $av = bu \in (a) \cap (b) = (m)$. Així, $bu = mz$, per a algun $z \in A$. Multiplicant $a = d'u$ per b obtenim $ab = bd'u = md'z$ i, com que $ab = md$, aleshores $md = ab = md'z$ i, simplificant, $d = d'z$. Així $d' \mid d$ i d és el màxim comú divisor de a i b.

□

Teorema 3.2.3. *Sigui A un domini, $a, b \in A$. Aleshores són equivalents:*

(i) existeix $m \in A$, tal que $m = \mathrm{mcm}(a,b)$;

(ii) per a tot $r \in A \setminus \{0\}$, existeix $d \in A$, tal que $d = \mathrm{mcd}(ra,rb)$.

Demostració. (i) $\Longrightarrow$ (ii). Sigui $m = \mathrm{mcm}$(a,b). De la prova de la Proposició 3.2.2, deduïm que $d := ab/m$ és el màxim comú divisor de a i b. Sigui $r \in A, r \neq 0$. Vegem que $rd = \mathrm{mcd}$(ra,rb). En efecte, $d \mid a$ i $d \mid b$, implica que $rd \mid ra$ i $rd \mid rb$. Sigui $e \in A$, tal que $e \mid ra$ i $e \mid rb$. Aleshores $e \mid rab$. A més, l'element rab/e satisfà $a \mid (rab/e)$, respectivament, $b \mid (rab/e)$, ja que $e \mid rb$, respectivament $e \mid ra$. Per tant, $m \mid (rab/e) \Longrightarrow em \mid rab \Longrightarrow e \mid rab/m = rd$.
(ii) $\Longrightarrow$ (i). Vegem que

$$\mathrm{mcm}(a,b) = \frac{ab}{\mathrm{mcd}(a,b)}.$$

En efecte, sigui $d := \mathrm{mcd}$(a,b), $m := ab/d$. Tenim,

$$m = a\frac{b}{d} \text{ i } m = b\frac{a}{d}.$$

És a dir, $m = \dot{a}$ i $m = \dot{b}$. Sigui $n \in A$, tal que $n = \dot{a}$ i $n = \dot{b}$. Aleshores $ab \mid nb$ i $ab \mid na$. Per tant, $ab \mid \mathrm{mcd}(na, nb)$. Per hipòtesi sabem que $\mathrm{mcd}(na, nb)$ existeix, i de la prova de la implicació anterior deduïm que $\mathrm{mcd}(na, nb) = n \cdot \mathrm{mcd}$(a,b) $= nd$. Per tant, $ab \mid nd \Longrightarrow (ab/d) \mid n \Longrightarrow m \mid n$. □

Corol·lari 3.2.4. *Sigui A un domini. Aleshores són equivalents:*

(i) existeix el mínim comú múltiple per a tot parell d'elements de A;

(ii) existeix el màxim comú divisor por a tot parell d'elements de A.

Observació 3.2.5. És important remarcar que hi ha dominis en què tant el màxim comú divisor com el mínim comú múltiple no tenen per què existir.

Exercici 3.2.6. Sigui A el subanell de $\mathbb{Z}[t]$ format pels polinomis sense terme de grau 1.

1. Proveu que efectivament A és un subanell de $\mathbb{Z}[t]$, i deduïu que A és íntegre.
2. Llisteu els divisors comuns de t^5, t^6, en A.

3. Proveu que t^5, t^6, no tenen màxim comú divisor en A.

4. Proveu que t^2, t^3, no tenen mínim comú múltiple en A.

Resolució. Clarament, $A = \{a_0 + a_1 t + a_2 t^2 + ... + a_r t^r \mid r \geq 1,\ a_i \in \mathbb{Z},\ a_1 = 0\} \subseteq \mathbb{Z}[t]$.

1. És trivial veure que $1 \in A$. Per tant, per provar que A és un subanell de $\mathbb{Z}[t]$, resta veure que A és tancat per a la suma i el producte de $\mathbb{Z}[t]$, i conté els elements oposats. Donats $f = \alpha_0 + \alpha_2 t^2 + ...\alpha_n t^n \in A$, $g = \beta_0 + \beta_2 t^2 + ...\beta_m t^m \in A$, es té:

$$f + g = \alpha_0 + \beta_0 + (\alpha_2 + \beta_2)t^2 + ... + (\alpha_n + \beta_m)t^{n+m} \in A,$$

$$f \cdot g = \alpha_0\beta_0 + \alpha_0\beta_2 t^2 + \alpha_2\beta_0 t^2 + ... + \alpha_n\beta_m t^{n+m} \in A,$$

$$-f = -\alpha_0 + (-\alpha_2)t^2 + ... + (-\alpha_n)t^n \in A.$$

Concloem, doncs, que A és un subanell de $\mathbb{Z}[t]$. Per ser $\mathbb{Z}[t]$ íntegre, i A un subanell de $\mathbb{Z}[t]$, A és integre.

2. Els divisors de t^5 són, llevat d'associats, $1, t^2, t^3, t^5$, i els divisors de t^6 són, llevat d'associats, $1, t^2, t^3, t^4, t^6$. És a dir, els divisors comuns són, llevat d'associats, $1, t^2, t^3$.

3. Observem que $t^2 \nmid 1, t^3 \nmid t^2, t^2 \nmid t^3$, i per tant cap d'ells pot ser el màxim comú divisor.

4. Observem que t^5 és un múltiple comú de t^2 i t^3, ja que $t^5 = t^2 \cdot t^3$. Així doncs, en cas d'existir el mínim comú múltiple de t^2, t^3, aquest hauria de dividir t^5. A més, no pot tenir un grau inferior a 5, ja que aleshores o bé t^2 o bé t^3 no el dividirien. Per tant, l'únic possible candidat, tret d'associats, és t^5. Però $t^6 = t^2 \cdot t^4 = t^3 \cdot t^3$ també és un múltiple comú, i $t^5 \nmid t^6$. Per tant, no exiteix el mínim comú múltiple de t^2, t^3.

□

3.3 Dominis de Bézout

Observació 3.3.1. Sigui A un domini, $a, b \in A$. Aleshores:

$$(d) = \langle a, b\rangle \iff d = \text{mcd}(a, b) \text{ i l'equació } aX + bY = d, \text{ té solució en } A.$$

Demostració. ($\Longrightarrow$). Si $\langle a, b\rangle = (d)$, clarament (d) és el menor ideal principal de A que compleix $\langle a, b\rangle \subseteq (d)$, i per tant $d =$mcd(a, b). A més, en particular, $d \in \langle a, b\rangle$, és a dir, existeixen $x, y \in A$, tals que $ax + by = d$.
($\Longleftarrow$). Per ser d el màxim comú divisor de a i b, es té $\langle a, b\rangle \subseteq (d)$. A més, per hipòtesi existeixen $x, y \in A$, tals que $ax + by = d$, d'on deduïm que $(d) \subseteq \langle a, b\rangle$. Conseqüentment, $(d) = \langle a, b\rangle$. □

Definició 3.3.2. Sigui A un domini, $a, b \in A$, i $d =$mcd(a, b). Anomenem *equació de Bézout* a l'equació $aX + bY = d$, i *identitat de Bézout* a l'expressió $d = au + bv$, on $(u, v) \in A \times A$, *i.e.*, a una solució de l'equació de Bézout.

Definició 3.3.3. Sigui A un domini. Diem que A és un *domini de Bézout* si per a tot parell d'elements $a, b \in A$, existeix un màxim comú divisor de a i b, i l'equació de Bézout té solució en A.

Observació 3.3.4. Sigui A un domini de Bézout. Aleshores A és un domini GCD.

Sovint també es defineix un domini de Bézout com un domini on la suma de dos ideals principals és també un ideal principal, o bé un domini on tot ideal finitament generat és principal.

Proposició 3.3.5. *Sigui A un domini. Aleshores són equivalents:*

(i) A és un domini de Bézout;

(ii) la suma de dos ideals principals de A és un ideal principal de A;

(iii) tot ideal finitament generat de A és principal.

Demostració. (i) $\Longrightarrow$ (ii). Sigui A un domini de Bézout, $a, b \in A$. Volem veure que la suma d'ideals principals $(a) + (b) = \langle a, b\rangle$, és també un ideal principal. Per ser A un domini de Bézout, existeix un màxim comú divisor, $d \in A$, de a i b. Per tant, $\langle a, b\rangle \subseteq (d)$. A més, de nou per hipòtesi, l'equació de Bézout té solució, és a dir, $d = ax + by \in \langle a, b\rangle$, per a certs $x, y \in A$. Concloem que $(d) = \langle a, b\rangle$.
(ii) $\Longrightarrow$ (iii). Veure que tot ideal finitament generat és principal és equivalent a veure que tot ideal generat per dos elements pot ser generat per un de sol. Sigui $I = \langle a, b\rangle = (a) + (b)$, per a certs $a, b \in A$. Aleshores, per hipòtesi, existeix $d \in A$, tal que $(a) + (b) = (d)$.
(iii) $\Longrightarrow$ (i). Siguin $a, b \in A$. Volem veure que existeix un màxim comú divisor de a i b, i que l'equació de Bézout té solució en A. Per hipòtesi, existeix $d \in A$, tal que $(a)+(b) = \langle a, b\rangle = (d)$. Aleshores clarament d és un màxim comú divisor de a i b. A més, $d \in \langle a, b\rangle$, per tant l'equació de Bézout té solució en A. □

Observació 3.3.6. Notem que hi ha dominis on pot existir el màxim comú divisor de dos elements i en canvi pot no existir una solució per a l'equació de Bézout.

Exercici 3.3.7 (Exercici 2.4 de [1])**.** Considereu els elements x, y, de $\mathbb{Z}[x, y]$. Proveu que 1 és el màxim comú divisor de x i y, però 1 no és combinació lineal de x i y (*i.e.,* l'equació de Bézout no té solució).

Resolució. Els divisors de x a $\mathbb{Z}[x, y]$ són, llevat d'associats, 1 i x. Els divisors de y a $\mathbb{Z}[x, y]$ són llevat d'associats, 1 i y. És a dir, l'únic divisor comú de x i y a $\mathbb{Z}[x, y]$ és, llevat d'associats, 1. Per tant, en particular, 1 és el màxim comú divisor de x i de y. Considerem ara una combinació lineal qualsevol de x i y:

$$ax + by,$$

on $a, b \in \mathbb{Z}[x, y]$. Observem que ax, respectivament, bx, no pot tenir terme independent, ja que tots els termes estan multiplicats per x, respectivament, per y. És a dir, les combinacions lineals de x i y a $\mathbb{Z}[x, y]$ no tenen terme independent, i cap d'elles pot ser igual a 1. □

3.4 Anells factorials

És ben sabut que tot element de $\mathbb{Z}$ diferent de zero té una factorització en producte d'enters irreductibles, i que aquesta factorització és única llevat d'ordre i associats. L'anell de polinomis $\mathbb{K}[x]$ sobre un cos $\mathbb{K}$ gaudeix de la mateixa propietat. En aquesta secció analitzem la classe d'anells que satisfan aquesta propietat: els anells factorials.

Definició 3.4.1. Sigui A un domini, $p \in A \setminus (A^* \cup \{0\})$. Diem que p és un element *irreductible* si $p = ab \Longrightarrow a \in A^*$ o $b \in A^*$, per a tot $a, b \in A$.

Definició 3.4.2. Sigui A un domini, $p \in A \setminus (A^* \cup \{0\})$. Diem que p és un element *primer* si $ab \in (p) \Longrightarrow a \in (p)$ o $b \in (p)$. És a dir, si (p) és un ideal primer.

Lema 3.4.3. *Sigui A un domini, $p \in A \setminus (A^* \cup \{0\})$. Si p és primer, aleshores p és irreductible.*

Demostració. Suposem que $p = ab$. Aleshores $ab \in (p)$. Com a conseqüència de la primalitat de p, podem afirmar, sense pèrdua de generalitat, que $a \in (p)$. És a dir, existeix $\alpha \in A$ tal que $a = p\alpha$. Per tant, $a = ab\alpha$. Per ser A íntegre i $a \neq 0$, aleshores necessàriament $1 = b\alpha$ i $b \in A^*$. □

Observació 3.4.4. En general, com es veurà a l'exemple següent, irreductibilitat no implica primalitat.

Exemple 3.4.5. Sigui $A = \{a_0 + a_1 t + a_2 t^2 + ... + a_r t^r \mid r \geq 1,\ a_i \in \mathbb{Z}[t],\ a_1 = 0\} \subseteq \mathbb{Z}$. A l'exercici 3.2.6 s'ha vist que $A \subseteq \mathbb{Z}[t]$ és un subanell de $\mathbb{Z}[t]$, i en particular, un domini. Vegem que $t^2 \in A$ és irreductible però no primer. Que t^2 és irreductible és trivial, ja que els seus únics divors són, llevat d'associats, 1 i t^2. No obstant, $t^3 \cdot t^3 = t^2 \cdot t^4 \in (t^2)$, però $t^3 \notin (t^2)$, per tant t^2 no és primer.

Definició 3.4.6. Sigui A un domini. Diem que A verifica la *condició de l'element primer* (CEP) si tot element irreductible de A és primer.

En els propers Lemes, el 3.4.7 i el 3.4.8, es veuran condicions suficients per a que es verifiqui la CEP.

Lema 3.4.7. *Sigui A un domini. Si per a tot $a \in A \setminus (A^* \cup \{0\})$, existeix una única descomposició de a en producte d'elements irreductibles (llevat d'ordre i associats), aleshores A verifica la CEP.*

Demostració. Sigui $p \in A \setminus (A^* \cup \{0\})$ un element irreductible; vegem que p és primer. Suposem que $ab \in (p)$, aleshores existeix $\alpha \in A$ tal que $ab = p\alpha$. Si $ab = 0$, per ser A íntegre, o bé $a = 0 \in (p)$, o bé $b = 0 \in (p)$. Si $a \in A^*$, aleshores $b = a^{-1}ab \in (p)$, i viceversa. Prenem, doncs, $a, b \in A \setminus (A^* \cup \{0\})$. Observem que en aquest cas $\alpha \in A \setminus (A^* \cup \{0\})$; sinó tornariem a un dels casos anteriors. Per hipòtesi, $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $b = q_1^{\beta_1} \cdots q_m^{\beta_m}$, $\alpha = r_1^{\gamma_1} \cdots r_s^{\gamma_s}$, on els p_i, q_j, r_k, són elements irreductibles de A, i els $\alpha_i, \beta_i, \gamma_i$ són enters no negatius. Aleshores:

$$ab = p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\beta_1} \cdots q_m^{\beta_m} = p\alpha = p r_1^{\gamma_1} \cdots r_s^{\gamma_s}.$$

De la unicitat en la descomposició en factors irreductibles deduïm que p ha de ser igual a algun dels p_i, q_j. En el primer cas $a \in (p)$, i en el segon $b \in (p)$. □

Lema 3.4.8. *Sigui A un domini. Si per a tot $a \in A \setminus (A^* \cup \{0\})$, existeix una descomposició de a en producte d'elements primers, aleshores A verifica la CEP.*

Demostració. Sigui $p \in A \setminus (A^* \cup \{0\})$ un element irreductible; vegem que p és primer. Per hipòtesi, $p = p_1 \cdots p_r$, on $r \geq 1$ i els p_i són primers. Vegem que $r = 1$, i per tant $p = p_1$ és primer. Per hipòtesi $p \notin (A^* \cup \{0\})$, per tant $r > 0$. Suposem que $r \geq 2$. Sabem que $p_i \notin (A^* \cup \{0\})$, per a tot $i \leq r$. En particular, $p_1 \notin (A^* \cup \{0\})$, i per ser p irreductible, necessàriament $(p_2 \cdots p_r) \in A^*$. Aleshores, $p_2 \cdot (p_3 \cdots p_r) \cdot (p_2 \cdot p_3 \cdots p_r)^{-1} = 1$, la qual cosa suposa una contradicció amb $p_2 \notin A^*$. □

En el darrer Lema, 3.4.8, no s'ha imposat que la descomposició en primers sigui única. No obstant, en el cas d'existir, ho és:

Lema 3.4.9. *Sigui A un domini i siguin $p_1, \ldots, p_m$, $q_1, \ldots, q_n$, elements primers de A tals que:*

$$p_1 \cdots p_m = q_1 \cdots q_n.$$

Aleshores es té que $m = n$, i que $p_i = q_i$, llevat d'ordre i associats.

Demostració. Siguin $p_1, \ldots, p_m$, i $q_1, \ldots, q_n$ elements primers de A, i suposem

$$p_1 \cdots p_m = q_1 \cdots q_n.$$

Procedirem per inducció sobre m. Si $m = 0$, tenim $q_1 \cdots q_n \in A^*$, de forma que $n = 0$ (ja que els q_i no són invertibles). Per $m > 0$, $p_1 \cdots p_m = q_1 \cdots q_n \implies q_1 \cdots q_n \in (p_1)$. Com que p_1 és primer, podem suposar que $q_1 \in (p_1)$. Així $q_1 = p_1\alpha$. Com que $p_1 \notin A^*$ i q_1 és irreductible, aleshores $\alpha \in A^*$. Així doncs, simplificant ambdós costats i canviant q_2 per αq_2 tenim

$$p_1 \cdots p_m = q_1 \cdots q_n \implies p_2 \cdots p_m = q_2 \cdot .... \cdot q_n.$$

Per hipòtesi d'inducció concloem que $m = n$ i p_i i q_i són associats. □

Teorema 3.4.10. *Sigui A un domini. Aleshores són equivalents:*

(i) Per a tot $a \in A \setminus (A^* \cup \{0\})$, existeix una única descomposició de a en producte d'elements irreductibles (llevat d'ordre i associats).

(ii) Per a tot $a \in A \setminus (A^* \cup \{0\})$, existeix una única descomposició de a en producte d'elements primers (llevat d'ordre i associats).

(iii) per a tot $a \in A \setminus (A^* \cup \{0\})$, existeix una descomposició de a en producte d'elements primers (llevat d'ordre i associats).

Demostració. (i) $\implies$ (ii). Sigui $a \in A \setminus (A^* \cup \{0\})$. L'existència de la descomposició de a en producte d'elements primers és conseqüència directa del Lema 3.4.7. Al seu torn, del Lema 3.4.9, deduïm la unicitat d'aquesta descomposició (llevat d'ordre i associats).
(ii) $\implies$ (iii). És obvi.
(iii) $\implies$ (i). Sigui $a \in A \setminus (A^* \cup \{0\})$. Per hipòtesi, a descomposa en producte d'elements

primers. Pel Lema 3.4.3, sabem que els elements primers són irreductibles, i per tant, en particular, existeix una descomposició de a en producte d'elements irreductibles. D'altra banda, de la hipòtesi (iii) i del Lema 3.4.8, en deduïm que A verifica la CEP. És a dir, en aquest cas, la primalitat és equivalent a la irreductibilitat. Finalment, pel Lema 3.4.9, sabem que la descomposició de a en producte d'elements primers és única (llevat d'ordre i associats). Concloem, doncs, que la descomposició de a en producte d'elements irreductibles també és única (llevat d'ordre i associats). □

Definició 3.4.11. Sigui A un domini. Diem que A és un *domini de factorització única* (DFU) o *anell factorial* si satisfà (i) (o (ii) o (iii)).

Observació 3.4.12. Sigui A un DFU. Aleshores tot element $a \in (A \setminus \{0\})$, es pot expressar de la forma:

$$a = uq_1^{\alpha_1} \cdots q_r^{\alpha_r},$$

on u és invertible, els elements q_i són irreductibles, q_i i q_j no són associats per $i \neq j$, i $\alpha_i \geq 0$. Si $a \in A^*$, aleshores per a tot i, $\alpha_i = 0$, i $a = u$. Altrament, els q_i tals que $\alpha_i > 0$, juntament amb les seves multiplicitats, α_i, són els factors irreductibles en què descomposa a.

El resultat següent és la base de moltes de les propietats elementals dels DFUs, com per exemple el Teorema de caracterització 3.5.3, que es veurà més endavant.

Lema 3.4.13. *Sigui A un DFU, i siguin a, b elements de A diferents de zero. Per l'Observació 3.4.12 sabem que són de la forma:*

$$a = uq_1^{\alpha_1} \cdots q_r^{\alpha_r},$$
$$b = vq_1^{\beta_1} \cdots q_r^{\beta_r},$$

on u i v són invertibles, els elements q_i són irreductibles, q_i i q_j no són associats per a $i \neq j$, i $\alpha_i \geq 0$, $\beta_i \geq 0$ (de manera que els factors irreductibles de a, respectivament, b, són aquells q_i tals que $\alpha_i > 0$, amb multiplicitat α_i, respectivament, $\beta_i > 0$, amb multiplicitat β_i). Aleshores es compleix:

(i) $(a) \subseteq (b) \iff \alpha_i \geq \beta_i$, per a tot $i = 1, \ldots, r$.

(ii) a i b són associats (és a dir, $(a) = (b)$) $\iff \alpha_i = \beta_i$, per a tot $i = 1, \ldots, r$.

(iii) Els factors irreductibles del producte ab son la col.lecció de tots els factors irreductibles de a i de b.

Demostració. Començarem per veure (iii). Tenim que:

$$ab = uq_1^{\alpha_1} \cdots q_r^{\alpha_r} \cdot vq_1^{\beta_1} \cdots q_r^{\beta_r} = uvq_1^{\alpha_1+\beta_1} \cdot \ldots \cdot q_r^{\alpha_r+\beta_r},$$

on uv és invertible, per ser u, v invertibles i clarament, per l'Observació 3.4.12, els factors irreductibles del producte ab son la col.lecció de tots els factors irreductibles de a i de b. Provem ara (i). Comencem per la implicació directa. Suposem que $(a) \subseteq (b)$, en particular

$a \in (b)$ i per tant $\exists\, x \in A$ tal que $a = bx$. Per (iii) sabem que els factors irreductibles de a són la col·lecció dels factors irreductibles de b i de x i per tant, en concret, $\alpha_i \geq \beta_i$, per a tot $i = 1, \ldots, r$. Recíprocament, suposem $\alpha_i \geq \beta_i$, per a tot $i = 1, \ldots, r$. Aleshores $\exists\, y \in A$ tal que $a = by$, per tant $a \in (b)$ i conseqüentment $(a) \subseteq (b)$. Finalment vegem (ii): a i b són associats (és a dir, $(a) = (b)) \iff (a) \subseteq (b)$ i $(b) \subseteq (a)$. Per (i) sabem que això es compleix si i només si $\alpha_i \geq \beta_i$ i $\alpha_i \leq \beta_i$, per a tot $i = 1, \ldots, r$. És a dir, si i només si $\alpha_i = \beta_i$, per a tot $i = 1, \ldots, r$. □

Aquest resultat és molt útil ja que permet transformar problemes de teoria d'anells en problemes d'aritmètica. Una de les aplicacions d'aquest mecanisme es troba en la prova d'existència de mínims comuns múltiples i màxims comuns divisors en els DFUs. S'ha vist prèviament, a l'Exercici 3.2.6, que aquests no tenen per què existir en un domini qualsevol. Aplicant el resultat anterior, es comprova que sí que existeixen en els DFUs.

Proposició 3.4.14. *Sigui A un anell factorial i siguin a, b, elements de A diferents de zero. Aleshores existeixen tant el màxim comú divisor com el mínim comú múltiple de a, b.*

Demostració. Per ser A un DFU, tenint en compte l'Observació 3.4.12 podem escriure:

$$a = uq_1^{\alpha_1} \cdots q_r^{\alpha_r}, \quad b = vq_1^{\beta_1} \cdots q_r^{\beta_r},$$

on u i v són invertibles, els elements q_i són irreductibles, q_i i q_j no són associats per $i \neq j$, i $\alpha_i \geq 0$, $\beta_i \geq 0$. Vegem que

$$d = q_1^{\gamma_1} \cdots q_r^{\gamma_r},$$
$$m = q_1^{\sigma_1} \cdots q_r^{\sigma_r},$$

on $\gamma_i = \min(\alpha_i, \beta_i)$ i $\sigma_i = \max(\alpha_i, \beta i)$, són, respectivament, el màxim comú divisor i el mínim comú múltiple de a, b. Comencem per veure que $d = \operatorname{mcd}(a, b)$. Clarament $d|a, d|b$. Sigui c, tal que $c|a, c|b$. Aleshores, pel Lema 3.4.13, necessàriament $c = wq_1^{\tilde{\gamma_1}} \cdots q_r^{\tilde{\gamma_r}}$, on $w \in A^*$, i $\tilde{\gamma_i} \leq \min(\alpha_i, \beta i)$. Per tant, de nou pel Lema 3.4.13, $c|d$. Vegem ara que $m = \operatorname{mcm}(a, b)$. Clarament $m = \dot{a}, m = \dot{b}$. Sigui e, tal que $e = \dot{a}, e = \dot{b}$. Aleshores, pel Lema 3.4.13, necessàriament $e = zq_1^{\tilde{\sigma_1}} \cdots q_r^{\tilde{\sigma_r}}$, on $z \in A^*$ i $\tilde{\sigma_i} \geq \max(\alpha_i, \beta_i)$. Per tant, de nou pel Lema 3.4.13, $e = \dot{m}$. □

Observem que l'argument seguit en la demostració anterior ens dona una forma de calcular màxims comuns divisors i mínims comuns múltiples en un DFU. Aquest procediment és una de les formes estàndard de calcular el mcd a $\mathbb{Z}$: *factors comuns elevats al mínim exponent*. No obstant, aquesta no és l'única forma de calcular el mcd a $\mathbb{Z}$. Més endavant tornarem a aquest punt. De fet, els mcds a $\mathbb{Z}$ gaudeixen de propietats que no hauríem d'esperar en un domini qualsevol, ni tan sols en un DFU.

Corol·lari 3.4.15. *Sigui A un DFU. Aleshores A és un domini GCD.*

Exercici 3.4.16 (Exercici 2.2 de [1])**.** Sigui A un DFU, siguin $a, b, c \in A$, tals que $a \mid bc$ i $\operatorname{mcd}(a, b) = 1$. Proveu que a divideix c. Aquest resultat es coneix com el Teorema d'Euclides.

Resolució. Com $a \mid bc$, tenim que $(bc) \subseteq (a)$, i per tant, pel Lema 3.4.13, els factors irreductibles de a, formen part dels factors irreducitbles de bc, que, de nou pel Lema 3.4.13, sabem que són la col·lecció de tots els factors irreductibles de b i de c. Però $\text{mcd}(a, b) = 1$, i tenint en compte la demostració de la Proposició 3.4.14, deduïm que cap dels factors irreductibles de a, ho és també de b. Per tant, necessàriament, tots els factors irreductibles de a, comptant multiplicitats, han de formar part dels de c. De nou pel Lema 3.4.13, obtenim que $a \mid c$. □

3.5 Una altra caracterització dels DFU

En el proper capítol s'analitzaran alguns dominis on la factorització única falla, és a dir, que no tots els dominis són DFU, com ja es podia intuir. Per a provar-ho, vegem a continuació que el problema de la factorització única en un domini està lligat amb la relació entre primalitat i irreductibilitat. Primer, notem:

Observació 3.5.1. Sigui A un DFU, aleshores A satisfà la CEP.

Demostració. Conseqüència directa del Teorema 3.4.10 i del Lema 3.4.7 (o bé el Lema 3.4.8). □

A continuació, veurem que suposant que es verifica la CCA, els DFU queden totalment caracteritzats per l'equivalència entre primalitat i irreductibilitat.

Observació 3.5.2. Sigui A un DFU i sigui $\Sigma = \{(a) \mid a \in A\}$, *i.e.*, el conjunt dels ideals principals de A. Aleshores el conjunt parcialment ordenat $(\Sigma, \subseteq)$ verifica la CCA.

Demostració. Considerem una cadena ascendent d'ideals principals:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \dots$$

Veurem que només pot haver-hi un nombre finit d'inclusions estrictes, i per tant la cadena estabilitza. Siguin $(0) \subsetneq (a_i) \subseteq (a_j)$ on $i < j$. Si a_j o bé a_i és invertible, aleshores necessàriament $(a_j) = A$, i la cadena estabilitza. Prenem doncs, $a_i, a_j \in A \setminus (A^* \cup \{0\})$. Suposem que $(a_i) \subsetneq (a_j)$. En particular, $a_i \in (a_j)$, és a dir, $a_j \mid a_i$. Aleshores, pel Lema 3.4.13, el nombre de factors irreductibles de a_j (comptant multiplicitats), ha de ser estrictament menor al de a_i, (no poden ser iguals ja que aleshores, de nou pel Lema 3.4.13, tindríem $(a_i) = (a_j)$). Com que aquest nombre ha de ser finit, enter i no negatiu, no pot decréixer de forma infinita. És a dir, només pot haver-hi un nombre finit d'inclusions estrictes, i passat aquest nombre la cadena estabilitza. □

Teorema 3.5.3. *Sigui A un domini. Aleshores A és un anell factorial si i només si*

- *es compleix la condició de cadena ascendent per a ideals principals de A i*
- *tot element irreductible és primer.*

Demostració. ($\Longrightarrow$) Vist al Corol.lari 3.5.1 i a l'Observació 3.5.2.
($\Longleftarrow$) Suposem ara que es compleix la condició de cadena ascendent per a ideals principals i que tot element irreductible és primer en A. Vegem que A és DFU. Prenem $a \in A \setminus (A^* \cup \{0\})$ i suposem que no existeix una descomposició de a en factors irreductibles. En particular a no és irreductible: $\exists a_1, b_1 \in A \setminus (A^* \cup \{0\})$ tals que $a = a_1 b_1$ i, o bé a_1 o bé b_1 no descomposa en producte d'irreductibles. Sense pèrdua de generalitat, podem suposar que a_1 no descomposa en producte de factors irreductibles. En particular a_1 no és irreductible i podem escriure $a_1 = a_2 b_2$, on $a_2, b_2 \in A \setminus (A^* \cup \{0\})$ i, o bé a_2 o bé b_2 no descomposa en producte de factors irreductibles. Podem seguir amb aquest procediment indefinidament i obtenim

$$a = a_1 b_1 = a_2 b_2 b_1 = a_3 b_3 b_2 b_1 = \cdots.$$

Donat que els b_i no són invertibles,

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

és una cadena ascendent d'ideals principals que no estabilitza, cosa que suposa una contradicció amb la hipòtesi. Així, doncs, tot $a \in A \setminus (A^* \cup \{0\})$ admet una descomposició única en factors irreductibles. En particular, com que, per hipòtesi, A verifica la CEP, per a tot $a \in A \setminus (A^* \cup \{0\})$ existeix una descomposició de a en producte d'elements primers. Aplicant el Teorema 3.4.10 concloem que A és DFU. □

Exercici 3.5.4 (Exercici 2.8 de [1])**.** Sigui A un DFU i sigui $I \neq (0)$ un ideal de A. Proveu que tota cadena descendent d'ideals principals de A contenint I estabilitza.

Resolució. Considerem

$$(a_1) \supseteq (a_2) \supseteq (a_3) \supseteq \ldots \subseteq I,$$

on $a_i \in A$, $I \subseteq (a_i)$, per a tot i. Per a cada i, denotem per m_i, la quantitat de factors irreductibles, comptant multiplicitats, en què descomposa a_i. Pel Lema 3.4.13, sabem que la successió de naturals $(m_i)_{i>0}$ és creixent. Prenem $x \in I$, és clar que $(a_i) \supseteq (x)$, per a tot i. Sigui n la quantitat de factors irreductibles, comptant multiplicitats, en què descomposa x. Pel Lema 3.4.13, sabem que $m_i \leq n$, per a tot i. Aleshores, la successió de naturals $(m_i)_{i>0}$, per ser creixent i fitada, estabilitza. Conseqüentment, de nou pel Lema 3.4.13, la respectiva cadena descendent també estabilitza. □

Exercici 3.5.5 (Exercici 2.9 de [1])**.** Proveu que si A és un DFU, aleshores tot ideal primer de A d'alçada 1 és principal.

Resolució. Sigui $\mathfrak{p}$ un ideal primer de A d'alçada 1. Per ser $\mathfrak{p}$ d'alçada 1, sabem que $\mathfrak{p} \neq (0)$. Prenem $a \in \mathfrak{p}$, $a \neq 0$, sabem que $a \notin A^*$, ja que $\mathfrak{p} \neq A$. Sigui $a = p_1 \cdots p_r$, la descomposició de a en elements primers. Aleshores $p_1 \cdots p_r \in \mathfrak{p}$. Com a conseqüència de la primalitat de $\mathfrak{p}$, podem assumir, sense pèrdua de generalitat, que $p_1 \in \mathfrak{p}$, *i.e.*, $(p_1) \subseteq \mathfrak{p}$. Si $(p_1) = \mathfrak{p}$, ja ho tenim. Altrament, $(0) \subsetneq (p_1) \subsetneq \mathfrak{p}$ és una cadena d'alçada 2 de $\mathfrak{p}$, cosa que contradiu la hipòtesi. □

Exercici 3.5.6 (Exercici 2.6 de [1])**.** Sigui A un domini que verifica la propietat següent: la intersecció d'una família qualsevol d'ideals principals de A és un ideal principal de A.

- Proveu que existeixen els màxims comuns divisors en A.
- Proveu que els DFU verifiquen aquesta propietat.

Resolució. Donat un subconjunt $N \subset A$ qualsevol, prenem $d \in A$, tal que $(d) = \bigcap_{x \in A, \langle N \rangle \subseteq (x)} (x)$. Per hipòtesi sabem que existeix. Comprovem que d és el màxim comú divisor de N. Per a tot $a \in N$, és té que $a \in (d)$, i per tant $d \mid a$. A més, si existeix $c \in A$, tal que $a \in (c)$ per a tot $a \in N$, aleshores $\langle N \rangle \subseteq (c)$. Per tant $(d) \subseteq (c)$, i $c \mid d$. Vegem ara que els DFU verifiquen aquesta propietat. Sigui A un DFU, $\{(a_\lambda)\}_{\lambda \in \Lambda}$ una família d'ideals principals de A. Prenem $I = \cap_{\lambda \in \Lambda}(a_\lambda)$. Sabem que I és un ideal de A. Hem de veure que és principal. Per la Proposició 3.4.14, podem assegurar que existeix $m \in A$, tal que m és el mínim comú múltiple del conjunt $\{a_\lambda\}_{\lambda \in \Lambda}$. Aleshores clarament $(m) = \cap_\lambda (a_\lambda)$. □

3.6 Dominis d'Ideals Principals

Definició 3.6.1. Sigui A un domini. Diem que A és un *domini d'ideals principals* (DIP) si tot ideal I de A és principal.

Corol·lari 3.6.2. *Sigui A un DIP. Aleshores A és Noetherià.*

Demostració. Per ser A DIP, tot ideal de A és principal, i en particular, finitament generat. □

Proposició 3.6.3. *Sigui A un DIP. Sigui $N \subseteq A \setminus (A^* \cup \{0\})$, un subconjunt de A. Aleshores existeixen* $\mathrm{mcd}(N)$ *i* $\mathrm{mcm}(N)$*, i l'equació de Bézout té solució en A.*

Demostració. Considerem $I = \langle N \rangle$, l'ideal generat per tots els elements de N. Per ser A DIP, existeix $d \in A$, tal que $\langle N \rangle = (d)$. Per definició és clar que d és un màxim comú divisor de N. Com que $d \in \langle N \rangle$, l'equació de Bézout té solució en A. Prenem ara m, tal que $(m) = \bigcap_{a \in N}(a)$. Clarament m és un mínim comú múltiple de N. □

Corol·lari 3.6.4. *Sigui A un DIP. Aleshores A és un domini de Bézout i, en particular, un domini GCD.*

Proposició 3.6.5. *Sigui A DIP, i sigui $p \in A$ irreductible. Aleshores (p) és maximal.*

Demostració. Donat que p és irreductible, $p \notin (A^* \cup \{0\})$ i es té $(0) \subsetneq (p) \subsetneq A$. Vegem que (p) és maximal. Sigui I un ideal propi tal que $(p) \subseteq I$. Per ser A DIP, $I = (x)$ per a algun $x \in A \setminus (A^* \cup \{0\})$. Tenim que $p = ax$, per a algun $a \in A$. Per ser p irreductible, necessàriament $a \in A^*$ i concloem que $(p) = I$. □

Corol·lari 3.6.6. *Sigui A un DIP. Aleshores A verifica la CEP.*

Demostració. Sigui $p \in A$ un element irreductible. Aleshores, per la Proposició 3.6.5, (p) és un ideal maximal, per tant, pel Lema 1.5.9, (p) és un ideal primer i en particular p és primer. □

Proposició 3.6.7. *Sigui A un DIP. Aleshores* $\mathrm{Spec}(A) = \mathrm{Max}(A) \cup \{0\}$.

Demostració. ($\supseteq$). Aplicació directa del Lema 1.5.9.
($\subseteq$). Sigui $\mathfrak{p}$ un ideal primer de A. Per ser A DIP, $\mathfrak{p} = (p)$, per a algun $p \in A$. Si $p = 0$, aleshores $\mathfrak{p} = (0)$ i ja ho tenim. Altrament p és primer i, en particular, pel Lema 3.4.3, p és irreductible. Aleshores, aplicant la Proposició 3.6.5, tenim que (p) és maximal. □

Corol·lari 3.6.8. *Sigui A un DIP. Aleshores* $\dim(A) \leq 1$.

Demostració. Per la Proposició 3.6.7, sabem que tot ideal primer (diferent de zero) és maximal. És a dir, per a tot parell d'ideals primers $\mathfrak{p}_1 \neq (0), \mathfrak{p}_2 \neq (0)$, tals que $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$, es té $\mathfrak{p}_1 = \mathfrak{p}_2$. En particular, donada una cadena d'ideals primers de A, $(0) \subsetneq \mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq ... \subseteq \mathfrak{p}_n$, necessàriament, $\mathfrak{p}_0 = \mathfrak{p}_1 = ... = \mathfrak{p}_n$. És a dir, tota cadena d'ideals primers de A té com a molt longitud 1. □

Teorema 3.6.9. *Sigui A un DIP, aleshores A és DFU.*

Demostració. Per ser A un DIP, A verifica la CEP (Corol·lari 3.6.6). A més, per l'Observació 3.6.2, sabem que A és Noetherià, i per tant, tots els ideals de A, i en particular els principals, verifiquen la CCA. Conseqüentment, pel Teorema 3.5.3, A és DFU. □

S'ha vist doncs, que el conjunt format pels DIPs està inclòs en el conjunt format pels DFUs. Més endavant es veurà que aquesta inclusió és estricta; és a dir, el recíproc del Teorema 3.6.9 no és cert en general. Hom podria començar a intuir aquest fet observant que, tal i com s'ha vist a la Proposició 3.6.3, en els DIPs, els màxims comuns divisors de a i b, són combinacions lineals de a i b. Aquesta és una condició forta que de fet caracteritza els DIPs dins del conjunt dels anells Noetherians, tal i com es comprovarà en l'Exercici següent. Aquesta condició no es compleix en general en els DFU.

Exercici 3.6.10 (Exercici 2.7 [1])**.** Sigui A un domini Noetherià. Suposeu que per a tot $a, b \in A$, a, b diferents de zero, el màxim comú divisor de a i b és combinació lineal de a i b. Proveu que A és DIP.

Resolució. Per ser A Noetherià, sabem que tot ideal de A és finitament generat. Per tant, és suficient veure que tot ideal de A generat per dos elements pot ser generat per un de sol. Sigui $I = \langle a, b \rangle$ un ideal de A. Prenem $d = \text{mcd}(a, b)$, i vegem que $\langle a, b \rangle = (d)$. La inclusió $\langle a, b \rangle \subseteq (d)$ és trivial, ja que, per ser $d = \text{mcd}(a, b)$, és té que $d \mid a$, i $d \mid b$. A més, per hipòtesi d és combinació lineal de a i b, és a dir, $d \in \langle a, b \rangle$, i per tant $(d) \subseteq \langle a, b \rangle$. □

Es podrien resumir els darrers resultats com:

$$A \text{ DIP} \implies A \text{ DFU, Noetherià i } \dim(A) \leq 1.$$

Seria raonable preguntar-se si la implicació contrària de la darrera expressió és certa. A continuació veurem que sí. És més, veurem que les condicions A Noetherià i $\dim(A) \leq 1$, ja caracteritzen els DIPs.

Lema 3.6.11. *Sigui A un domini. Aleshores, A és un DIP $\iff$ tot ideal primer de A és principal.*

Demostració. ($\Longrightarrow$). Per ser A DIP, tot ideal de A és principal. En particular, tot ideal primer de A és principal.
($\Longleftarrow$). Sigui $\Sigma = \{I \mid I \text{ ideal de } A, I \text{ no principal}\}$, *i.e.,* Σ és el conjunt dels ideals de A que no són principals. Si $\Sigma = \varnothing$, ja hem acabat. Volem veure que si $\Sigma \neq \varnothing$, aleshores existeixen ideals primers no principals de A. En efecte, suposem que $\Sigma \neq \varnothing$. Primerament observem que el conjunt $(\Sigma, \subseteq)$, és un conjunt no buit, parcialment ordenat, on tota cadena ascendent té una cota superior. Efectivament, sigui $I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$, una cadena ascendent de Σ. Prenem $I = \cup_{i\in\mathbb{N}} I_i$. Aleshores I és un ideal de A inclòs a Σ, i és una cota superior de la cadena. En primer lloc, $0 \in I_i$, per a tot i, i per tant $0 \in I$. Siguin $x, y \in I$, aleshores existeixen i, j, tals que $x \in I_i$, $y \in I_j$, sense pèrdua de generalitat $I_i \subseteq I_j$, i per tant $x + y \in I_j \subseteq I$. Sigui $x \in I$, $a \in A$, aleshores $x \in I_i$ per a algun i, i conseqüentment $ax \in I_i \subseteq I$. Per tant hem vist que I és un ideal de A. A més, aquest ideal no és principal, ja que si $I = (x)$, per a algun $x \in A$, aleshores $x \in I_i$ per a algun i, i es té $I = (x) \subseteq I_i \subseteq I \Longrightarrow I_i = I = (x)$, fet que suposa una contradicció amb $I_i \in \Sigma$. És a dir, $I \in \Sigma$, i clarament I és una cota superior de la cadena $(I_i)_i$. Per tant, pel Lema de Zorn 1.5.5, podem assegurar que el conjunt $(\Sigma, \subseteq)$ té un element maximal. Sigui $J \in \Sigma$, l'element maximal de Σ. Vegem que J és primer. En primer lloc, $J \neq A$, ja que $J = A = (1)$, suposa una contradicció amb $J \in \Sigma$. Suposem que $\exists\, a, b \in A$, tals que $ab \in J$, $a \notin J, b \notin J$. Aleshores $J \subsetneq \langle J, a\rangle$, i per ser J maximal a Σ, necessàriament $\langle J, a\rangle \notin \Sigma$, i per tant $\langle J, a\rangle$ és un ideal principal de A, *i.e.,* $\langle J, a\rangle = (c)$, per a algun $c \in A$. Observem que $J \subsetneq (J : c) := \{x \in A \mid xc \in J\}$. En efecte, clarament $J \subseteq (J : c)$. A més, podem expressar c de la forma $c = u + va$, on $u \in J, v \in A$. Així, $bc = bu + bva$, amb $u \in J, ab \in J$. Tenim $bc \in J$, i per tant $b \in (J : c)$, però en canvi $b \notin J$. Per tant $J \subsetneq (J : c)$. De la maximalitat de J a Σ deduïm que $(J : c)$ és principal, és a dir, $(J : c) = (d)$, per a algun $d \in A$. A més, tenim $J \subseteq (J : c) \cdot c$, ja que si $x \in J$, aleshores $x \in (J, a) = (c) \Longrightarrow x = \alpha c$, on $\alpha \in (J : c)$. Per tant, $x = \alpha c \in (J : c) \cdot c$. Així:

$$\left.\begin{array}{l} J \subseteq (J : c) \cdot c = (d) \cdot c = (cd) \\ d \in (d) = (J : c) \Longrightarrow cd \in J \end{array}\right\} \Longrightarrow (cd) \subseteq J \subseteq (cd) \Longrightarrow J = (cd),$$

fet que suposa una contradicció amb $J \in \Sigma$. Per tant, tal i com volíem veure, J és un ideal primer no principal. □

Teorema 3.6.12. *Sigui A un domini. Aleshores les tres condicions següents són equivalents:*

(i) A és DIP;

(ii) A és DFU, Noetherià i $\dim(A) \leq 1$;

(iii) A és DFU i $\dim(A) \leq 1$.

Demostració. (i) $\Longrightarrow$ (ii). Vist al Teorema 3.6.9 i als Corol·laris 3.6.8 i 3.6.2.
(ii) $\Longrightarrow$ (iii). És obvi.
(iii) $\Longrightarrow$ (i). Primerament veurem que tot ideal primer de A és principal. En efecte, sigui $\mathfrak{p}$ un ideal pimer de A. Si $\mathfrak{p} = \{0\}$ ja ho tenim. Altrament, existeix algun $x \in \mathfrak{p}, x \neq 0$. Per ser $\mathfrak{p}$ primer, $x \notin A^*$. Aleshores, per hipòtesi, $x = p_1 \cdots p_r \in \mathfrak{p}$, on els p_i són primers. Sense pèrdua de generalitat, podem suposar que $p_1 \in \mathfrak{p}$ i $(p_1) \subseteq \mathfrak{p}$. Per ser $\dim(A) \leq 1$, necessàriament $(p_1) = \mathfrak{p}$, i per tant $\mathfrak{p}$ és principal. Aleshores, pel Lema 3.6.11, deduïm que A és DIP.

□

3.7 Dominis Euclidians

Els dominis Euclidians són anells en els quals es pot efectuar una 'divisió amb residu'. És per exemple el cas de $\mathbb{Z}$ i $\mathbb{K}[x]$, on $\mathbb{K}$ és un cos. El punt clau resideix en que tant a $\mathbb{Z}$, com a $\mathbb{K}[x]$, es té una noció de la 'mida' dels elements; el valor absolut d'un enter a $\mathbb{Z}$ i el grau d'un polinomi a $\mathbb{K}[x]$. En ambdós casos, s'obté un control sobre la 'mida' del residu quan s'efectua la divisió. La definició de domini Euclidià és simplement una abstracció d'aquest fet.

Definició 3.7.1. Sigui A un domini. Anomenem *norma Euclidiana* a una aplicació,

$$\begin{aligned} N : A \setminus \{0\} &\longrightarrow \mathbb{N} \\ a &\longmapsto N(a), \end{aligned}$$

tal que oer a tot $a, b \in A$, amb $b \neq 0$, existeixen $q, r \in A$, amb $r = 0$ o bé $N(r) < N(b)$, tals que

$$a = bq + r.$$

La darrera expressió, s'anomena *divisió Euclidiana* de a per b, i els elements q i r són, respectivament, el *quocient* i el *residu (o reste)*.

Definició 3.7.2. Sigui A un domini. Diem que A és un *domini Euclidià* si A té una norma Euclidiana.

Nota 3.7.3. La norma Euclidiana no té per què ser única.

Exercici 3.7.4. Proveu que $\mathbb{Z}$ és un domini Euclidià.

Resolució. Es comprova que l'aplicació

$$\begin{aligned} |\cdot| : \mathbb{Z} \setminus \{0\} &\longrightarrow \mathbb{N} \\ x &\longmapsto |x|, \end{aligned}$$

és una norma Euclidiana a $\mathbb{Z}$. Donats $a, b \in \mathbb{Z}$, amb $b \neq 0$. Usant l'algorisme de divisó usual a $\mathbb{Z}$, (veure [13]), obtenim q, r, amb $r \geq 0$ tals que $a = bq + r$, i o bé $r = 0$, o bé $0 < r < |b|$. □

Exercici 3.7.5. Proveu que si $\mathbb{K}$ és un cos, aleshores $\mathbb{K}[x]$ és un domini Euclidià.

Resolució. Es comprova que l'aplicació

$$\begin{aligned} \text{grau} : \mathbb{K}[x] \setminus \{0\} &\longrightarrow \mathbb{N} \\ f &\longmapsto \text{grau}(f), \end{aligned}$$

és una norma Euclidiana a $\mathbb{K}[x]$. Donats $f, g \in \mathbb{K}[x]$, $g \neq 0$, usant l'algorisme de divisió usual a $\mathbb{K}[x]$ (veure [8]), obtenim q, r, tals que $f = gq + r$, i o bé $r = 0$, o bé $\text{grau}(r) < \text{grau}(g)$. □

Proposició 3.7.6. *Sigui A un domini Euclidià. Aleshores A és un DIP.*

Demostració. Sigui I un ideal de A, hem de veure que I és un ideal principal. Si $I = \{0\} \Longrightarrow I = (0)$ i ja ho tenim. Altrament, prenem $b \in I, b \neq 0$, un element tal que $N(b) \leq N(x)$, per a tot $x \in I \setminus \{0\}$. Vegem que $I = (b)$. Clarament $(b) \subseteq (I)$, donat que $b \in I$. Hem de veure que $I \subseteq (b)$. Sigui $a \in I$, considerem la divisió Euclidiana de a per b :

$$a = bq + r,$$

per a alguns $q, r \in A$, amb $r = 0$ o bé $N(r) < N(b)$. Observem que

$$r = a - bq \quad \in I.$$

Per ser $N(b)$ la norma mínima dels elements de I diferents de zero no es pot complir $N(r) < N(b)$. Per tant, necessàriament, $r = 0$ i $a = bq \in (b)$, tal i com volíem veure. □

3.8 Algorisme d'Euclides

Una de les característiques més importants dels dominis Euclidians és l'existència d'un algorisme eficient per al càlcul de màxims comuns divisors: *l'algorisme d'Euclides*. Tal i com s'ha comprovat a la Proposició 3.7.6, els dominis Euclidians són DIPs, i en conseqüència, pel Teorema 3.6.9, són DFUs. La Proposició 3.4.14 ens assegura l'existència de màxims comuns divisors en els DFUs, i en la seva demostració s'indica un procediment per a trobar-los. No obstant, 'l'algorisme' vist a la prova de la Proposició 3.4.14 no resulta pràctic; per exemple, si es volgués trobar el màxim comú divisor de dos enters a, b, caldria factoritzar a i b, cosa que, amb els algorismes i tecnologies actuals, resulta infactible per a números d'uns pocs centenars de dígits. El gran avantatge de l'algorisme d'Euclides resideix precisament en que esquiva la necessitat de factorització.

El lema clau en què es basa l'algorisme d'Euclides és el resultat següent:

Lema 3.8.1. *Sigui $a = bq + r$, en un domini A. Aleshores $\langle a, b\rangle = \langle b, r\rangle$.*

Demostració. De la hipòtesi deduim que $r = a - bq$, provant que $\langle b, r\rangle \subseteq \langle a, b\rangle$. De $a = bq + r$, es dedueix que $\langle a, b\rangle \subseteq \langle b, r\rangle$. □

Observació 3.8.2. En particular, si $a = bq + r$, i $c \in A$, aleshores:

$$\langle a, b\rangle \subseteq (c) \Longleftrightarrow \langle b, r\rangle \subseteq (c).$$

És a dir, els divisors comuns de a i b són els mateixos que els de b i r.

Corol·lari 3.8.3. *Suposem que $a = bq + r$, en un domini A. Aleshores a, b tenen màxim comú divisor si i només si b, r tenen màxim comú divisor, i en aquest cas* $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$.

Demostració. Sabem que d és el màxim comú divisor de $a, b \Longleftrightarrow \langle a, b\rangle \subseteq (d)$ i (d) és el menor ideal principal de A que compleix aquesta propietat $\Longleftrightarrow \langle b, r\rangle \subseteq (d)$ i (d) és el menor ideal principal de A que compleix aquesta propietat $\Longleftrightarrow d$ és el màxim comú divisor de b, r. □

Els resultats previs: Lema 3.8.1, Observació 3.8.2 i Corol·lari 3.8.3, es compleixen en qualsevol domini; suposem ara que A és un domini Euclidià. En aquest cas es pot utilitzar la divisió Euclidiana per a guanyar cert control sobre els residus r. Donats $a, b \in A$, amb $b \neq 0$, es pot aplicar la divisió Euclidiana repetidament de la forma següent:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\dots \end{aligned}$$

mentre el residu r_i sigui diferent de zero.

Lema 3.8.4. *Aquest procés finalitza; és a dir, $r_N = 0$ per a N suficientment gran.*

Demostració. Cada línia del procès anterior és una divisió Euclidiana, per definició de norma Euclidiana, mentre r_i sigui diferent de zero es compleix:

$$N(r_1) > N(r_2) > N(r_3) > \dots$$

Si no existís N amb $r_N = 0$, tindríem una successió infinita i estrictament decreixent d'enters no negatius, cosa que no és possible. □

Per tant, la taula de divisions, amb $r_0 = b$, ha de ser de la forma següent:

$$\begin{aligned} a &= r_0q_1 + r_1, \\ r_0 &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\dots \\ r_{N-3} &= r_{N-2}q_{N-1} + r_{N-1}, \\ r_{N-2} &= r_{N-1}q_{N+1}, \end{aligned}$$

amb $r_{N-1} \neq 0$, l'últim reste no nul.

Proposició 3.8.5. *Amb la notació prèvia, r_{N-1} és el màxim comú divisor de a, b.*

Dempstració. Pel Corol·lari 3.8.3 tenim:

$$\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r_1) = \operatorname{mcd}(r_1, r_2) = \dots = \operatorname{mcd}(r_{N-1}, r_{N-2}).$$

Com que $r_{N-2} = r_{N-1}q_{N-1}$ es té $r_{N-2} \in (r_{N-1})$; per tant $\langle r_{N-1}, r_{N-2} \rangle = (r_{N-1})$ i clarament r_{N-1} és el màxim comú divisor de r_{N-1}, r_{N-2} i, en conseqüència, de a i b. □

Capítol 4

Ordenant dominis

En el Capítol 3 s'han introduït i caracteritzat les famílies de dominis GCD, de Bézout, factorials, d'ideals principals i Euclidians. De les Proposicions 3.7.6 i 3.4.14, i el Teorema 3.6.9, es dedueix la cadena d'inclusions següent:

$$\{\text{Dominis Euclidians}\} \subseteq \{\text{DIPs}\} \subseteq \{\text{DFUs}\} \subseteq \{\text{Dominis GCD}\} \subseteq \{\text{Dominis}\}.$$

En aquest capítol provem, analitzant alguns contraexemples, que totes les inclusions anteriors són estrictes.

4.1 Dominis no GCD

Primer cal remarcar, tal i com s'ha vist en el Capítol 3, que l'existència de màxims comuns divisors per a tot parell d'elements no és una característica pròpia de tots els dominis íntegres. En efecte, a l'Exercici 3.2.6, s'ha vist que en el domini:

$$A = \left\{a_0 + a_1 t + a_2 t^2 + ... + a_n t^n \mid a_i \in \mathbb{Z},\ a_1 = 0\right\} \subset \mathbb{Z}[t],$$

no existeixen ni el màxim comú divisor de t^5 i t^6, ni el mínim comú múltiple de t^2 i t^3.

4.2 Dominis no DFU

Clarament, els exemples de dominis no GCD són també exemples de dominis no DFU. No obstant, en aquesta secció abordem alguns exemples clàssics, des del punt de vista de la factorització única, de dominis no DFU. Per exemple, sigui A l'anell vist en la secció anterior,

$$A = \left\{a_0 + a_1 t + a_2 t^2 + ... + a_n t^n \mid a_i \in \mathbb{Z},\ a_1 = 0\right\} \subset \mathbb{Z}[t].$$

Ja hem comentat que és un domini no GCD i, per tant, ja podem deduir que no és factorial. En efecte, és fàcil veure que, $t^3 \cdot t^3$ i $t^2 \cdot t^2 \cdot t^2$, són dues factoritzacions diferents de t^6 en producte d'elements irreductibles de A.

Vegem ara, des del punt de vista de la factorització única, alguns exemples clàssics, extrets de [9], de dominis no DFU.

Exemple 4.2.1. Sigui $A = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5}, a, b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$. A és clarament un subanell dels complexos i, en particular, un domini. No obstant, no és un DFU. En efecte, observem que $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Provarem que aquestes són dues factoritzacions diferents de 6 en producte d'elements irreductibles de l'anell A. Per a tractar el problema de la factorització en A considerem l'aplicació:

$$\begin{aligned} N : A &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto N(\alpha), \end{aligned}$$

on, donat $\alpha = a + b\sqrt{-5} \in A$, es defineix $\alpha' = a - \sqrt{-5}$, i $N(\alpha) = \alpha\alpha' = a^2 + 5b^2$. És fàcil veure que l'aplicació N satisfà:

1. $N(\alpha) \in \mathbb{N}$, per a tot $\alpha \in A$; i $N(\alpha) = 0$ si i només si $\alpha = 0$,
2. $N(\alpha\beta) = N(\alpha)N(\beta)$, per a tot $\alpha, \beta \in A$,
3. $N(\alpha) = 1$ si i només si $\alpha \in A$ és invertible.

De la darrera propietat deduïm que els únics elements invertibles de A són ± 1. Per tant, els elements $2, 3, 1+\sqrt{-5}$ i $1-\sqrt{-5}$ no són invertibles en A. Vegem que són irreductibles. Suposem que $2 = \alpha\beta$, per a certs $\alpha, \beta \in A$. Aleshores $4 = N(\alpha)N(\beta)$, i de les propietats de N deduïm que $N(\alpha) \in \{1, 2, 4\}$. Si $N(\alpha) = 1$, aleshores α és invertible, i ja ho tenim. Si $N(\alpha) = 4$, aleshores β és invertible i ja ho tenim. Altrament, $N(\alpha) = 2$ i $2 = a^2 + 5b^2$, on $a, b \in \mathbb{Z}$ i $\alpha = a + b\sqrt{-5}$. Però l'equació $2 = a^2 + 5b^2$ no té solucions en els enters i per tant suposa una contradicció. De forma similar es comprova que $3, 1+\sqrt{-5}$ i $1-\sqrt{-5}$ són també irreductibles. Per tant, $2 \cdot 3$, i $(1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, són dues factoritzacions de 6 en producte d'elements irreductibles de A. A més, donat que els únics elements invertibles de A són ± 1, clarament $2, 3$ no són associats de $(1+\sqrt{-5}), (1-\sqrt{-5})$. Per tant, hem trobat dues factoritzacions diferents de 6 en producte d'elements irreductibles en A.

Seguint el mateix raonament que a l'Exemple 4.2.1, és fàcil provar que els següents casos són també exemples de dominis que no són DFU.

Exemple 4.2.2. Sigui $A = \mathbb{Z}[\sqrt{-6}]$. A és un domini on la factorització en producte d'elements irreductibles no és necessàriament única. En particular, tenim $6 = 2 \cdot 3 = \sqrt{-6}\sqrt{-6}$.

Exemple 4.2.3. Sigui $A = \mathbb{Z}[\sqrt{10}]$. Aleshores $2 \cdot 5$ i $\sqrt{10} \cdot \sqrt{10}$, són dues factoritzacions diferents de 10 en producte d'elements irreductibles de A.

4.3 GCD no DFU

Trobar exemples assequibles de dominis GCD que no són DFU resulta complicat. A continuació, n'estudiem un. L'exemple següent es troba en [5] en forma d'exercici, com a exemple de domini de Bézout no DIP. Veurem que de fet, es tracta d'un domini de Bézout (i, en particular, GCD), que no és DFU.

Exemple 4.3.1. Sigui $\mathbb{K}$ un cos, $X_0, X_1, \ldots, X_n, \ldots$ un conjunt infinit numerable de variables. Sigui $A = \mathbb{K}[X_0, X_1, \ldots, X_n, \ldots]$ l'anell de polinomis en el conjunt infinit numerable de variables $X_0, X_1, \ldots, X_n, \ldots$ sobre el cos $\mathbb{K}$. Sigui $I = \langle X_0 - X_1^2, X_1 - X_2^2, \ldots, X_n - X_{n+1}^2, \ldots \rangle \subseteq A$ ideal de A. Considerem l'anell quocient

$$R = A/I = \mathbb{K}[x_0, x_1, \ldots, x_n, \ldots],$$

on denotem $x_i = \overline{X_i} = X_i + I$. Veurem que R és un domini de Bézout que no és DFU.

Comencem per veure que R és un domini de Bézout. Per a cada $i \geq 0$, considerem el morfisme d'anells $\varphi_i : \mathbb{K}[X_i] \longrightarrow R$, que envia X_i a x_i. Prenem $R_i := \mathrm{Im}(\varphi_i)$. Com R_i és la imatge del subanell $\mathbb{K}[X_i] \subseteq A$ pel morfisme d'anells φ_i, tenim que R_i és un subanell de R. Resumint, pel Primer Teorema d'isomofisme 1.3.12, $\varphi_i : \mathbb{K}[X_i] \longrightarrow R_i$ és un isomorfisme d'anells. Es comprova que $R_i \subseteq R_{i+1}$, per a tot $i \geq 0$. En efecte, sigui $\alpha \in R_i$, aleshores $\alpha = ax_i$, per a algun $a \in \mathbb{K}$. Per tant, $\alpha = ax_i = ax_{i+1}^2 = \varphi_{i+1}(aX_{i+1}^2) \in R_{i+1}$. Així, és fàcil veure que $R = \cup_{i \geq 0} R_i$. Concloem, doncs, que R és un domini de Bézout. En efecte, sigui I un ideal finitament generat de R. Aleshores, exiteix un $N \in \mathbb{N}$, tal que els generadors de I pertanyen a R_N i, per tant, $I \subseteq R_N$. Com que $\mathbb{K}[X_N]$ és Euclidià i, en particular és DIP, i R_N és isomorf a $\mathbb{K}[X_N]$, es comprova que R_N és DIP. Per tant, I és principal.

Vegem ara que R no és DFU. Més concretament, veurem que existeix una cadena d'ideals principals en R que no estabilitza. Sigui $P_n = \langle X_0, \ldots, X_n \rangle$ ideal de A. Observem que $A/P_n = \mathbb{K}[X_{n+1}, X_{n+2}, \ldots]$ és un domini. Per tant, per la Proposició 1.5.14, P_n és un ideal primer. Sigui

$$J_n = P_n + I = \langle X_0, \ldots, X_n \rangle + \langle X_0 - X_1^2, \ldots, X_n - X_{n+1}^2, \ldots \rangle.$$

Sigui $\mathfrak{a}_n = J_n/I = (P_n + I)/I = \langle x_0, x_1, \ldots, x_n \rangle$, ja que, en R, $x_i = x_{i+1}^2$. Aleshores, clarament,

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$

és una cadena ascendent. Com que, en R, $x_0 = x_1^2$, $x_1 = x_2^2, \ldots$, $x_{n-1} = x_n^2$, aleshores, tenim que $x_0 = x_n^{2^n}, x_1 = x_n^{2^{n-1}}, \ldots, x_{n-1} = x_n^2$. Així, doncs,

$$\mathfrak{a}_n = \langle x_0, x_1, \ldots, x_n \rangle = \langle x_n^{2^n}, x_n^{2^{n-1}}, \ldots, x_n^2, x_n \rangle = (x_n).$$

Per tant,

$$\mathfrak{a}_0 = (x_0) \subseteq \mathfrak{a}_1 = (x_1) \subseteq \ldots \subseteq \mathfrak{a}_n = (x_n) \subseteq \ldots$$

és una cadena ascendent d'ideals principals de R. Volem veure que no estabilitza. És suficient veure que $\mathfrak{a}_{n-1} \subsetneq \mathfrak{a}_n$, per a tot $n \geq 1$. Suposem que $\mathfrak{a}_{n-1} = \mathfrak{a}_n$. Aleshores, per la Proposició 1.3.8, $P_{n-1} + I = P_n + I$. Però,

$$\begin{aligned} P_{n-1} + I = \langle X_0, \ldots, X_{n-1} \rangle + \langle X_0 - X_1^2, \ldots, X_n - X_{n+1}^2, \ldots \rangle \Longrightarrow \\ \Longrightarrow P_{n-1} + I = \langle X_0, \ldots, X_{n-1}, X_0 - X_1^2, \ldots, X_n - X_{n+1}^2, \ldots \rangle. \end{aligned}$$

Anàlogament,

$$P_n + I = \langle X_0, \ldots, X_n, X_0 - X_1^2, \ldots, X_n - X_{n+1}^2, \ldots \rangle$$

Com que $X_n \in P_n + I$, si $P_{n-1} + I = P_n + I$, tenim:

$$X_n \in P_{n-1} + I = \langle X_0, \dots, X_{n-1}, X_0 - X_1^2, \dots, X_n - X_{n+1}^2, \dots \rangle \Longrightarrow$$
$$\Longrightarrow X_n = \sum_{i=0}^{n-1} X_i f_i + X_n^2 f_n + (X_n - X_{n+1}^2) f_{n+1} + \dots + (X_{m-1} + X_m^2) f_m, \tag{4.1}$$

per a alguns $f_0, \dots, f_m \in \mathbb{K}$. I l'expressió anterior és vàlida en tot $\mathbb{K}[X_0, \dots, X_N]$ on $N \geq m$. Vegem que l'equació anterior no té solucions en $\mathbb{K}[X_0, \dots, X_N]$, $N \geq m$. En efecte, sigui $N \geq m$,

$$\varphi : \mathbb{K}[X_0, \dots, X_N] \longrightarrow \mathbb{K}[X_0, \dots, X_N],$$

tal que

$$\varphi(X_i) = \begin{cases} 0, \text{ per a tot } i = 0, \dots, n-1. \\ X_N^{2^{N-i}}, \text{ per a tot } i = n, \dots, N. \end{cases}$$

Aplicant φ en la igualtat (4.1), obtenim $X_N^{2^{N-n}} = X_N^{2^{N-n+1}} f_n$, la qual cosa suposa una contradicció. Així, hem trobat una cadena ascendent d'ideals principals de R que no estabilitza. Per tant, pel Teorema 3.5.3, concloem que R no és DFU.

4.4 DFU no DIP

Un dels exemples clàssics de DFU que no és DIP és l'anell de polinomis en dues variables x, y, sobre un cos $\mathbb{K}$, és a dir, $\mathbb{K}[x, y]$. Resulta relativament fàcil veure que $\mathbb{K}[x, y]$ no és un DIP. No obstant, veure que és un DFU és més complicat. Per tal de provar que $\mathbb{K}[x, y]$ és efectivament un DFU, són necessaris diversos resultats dels anells de polinomis sobre DFUs, que introduïm en la Secció 4.4.1.

4.4.1 Anells de polinomis sobre DFUs

És ben sabut que l'anell de polinomis en una variable x sobre un cos $\mathbb{K}$, *i.e.,* $\mathbb{K}[x]$, és un DFU. És més, a l'Exercici 3.7.5, s'ha comprovat que és Euclidià. En aquesta secció provem que l'anell de polinomis en n variables $x_1, \dots, x_n$ sobre un cos $\mathbb{K}$, *i.e.,* $\mathbb{K}[x_1, \dots, x_n]$, és també un DFU. De fet, provem el resultat següent, més general:

Teorema 4.4.1 (C.F.Gauss)**.** *Sigui A un DFU. Aleshores $A[x]$ és un DFU.*

Abans de veure la prova del Teorema 4.4.1 és convenient estudiar les propietats de l'anell de polinomis $A[x]$, on A és un DFU. Per a més detall, es recomanen les referències [9] i [2].

Observació 4.4.2. Sigui A un domini. Aleshores $A[x]$ és un domini.

Observació 4.4.3. Sigui A un domini. Aleshores $(A[x])^* = A^*$.

Demostració. Si $f(x) \in (A[x])^*$, aleshores $1 = f(x)g(x)$ per a algun $g(x) \in A[x]$. Com grau$(1) = 0$, necessàriament $f, g \in A^*$. □

Observació 4.4.4. Sigui A un domini. Aleshores, si p és irreductible en A, p és irreductible en $A[x]$.

Demostració. Sigui $p \in A$ irreductible. Suposem que $p = f(x)g(x)$, per a alguns $f(x), g(x) \in A[x]$. Com grau$(p) = 0$, necessàriament $f, g \in A$. Per tant, o bé $f \in A^* = (A[x])^*$, o bé $g \in A^* = (A[x])^*$. □

Definició 4.4.5. Sigui A un DFU, $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$. Anomenem *contingut de* $f(x)$ a:

$$c(f(x)) = \text{mcd}(a_0, a_1, \ldots, a_n),$$

i el denotem per c$(f(x))$. Diem que $f(x)$ és *primitiu* si c$(f(x)) = 1$.

Observació 4.4.6. Sigui $\mathbb{K}$ un cos, $f(x) \in \mathbb{K}[x]$ un polinomi no constant i no irreductible. Aleshores, $f(x) = g(x)h(x)$ per alguns $g(x), h(x) \in \mathbb{K}[x]$, amb grau$(g(x))$, grau$(h(x)) \geq 1$. En particular, grau$(f(x)) \geq 2$.

Demostració. Si grau$(g(x)) = 0$, respectivament, grau$(h(x)) = 0$, aleshores $g(x) = g \in \mathbb{K} \setminus \{0\} = \mathbb{K}^*$, respectivament $h(x) = h \in \mathbb{K} \setminus \{0\} = \mathbb{K}^*$. □

Observació 4.4.7. Sigui A un domini, $f(x) \in A[x]$ un polinomi no constant, no irreductible i primitiu. Aleshores, $f(x) = g(x)h(x)$, per a alguns $g(x), h(x) \in A[x]$, amb grau$(g(x))$, grau$(h(x)) \geq 1$. En particular, grau$(f(x)) \geq 2$.

Demostració. Com $f(x)$ no és irreductible, $f(x) = g(x)h(x)$, per a alguns $g(x), h(x) \in A[x]$ no invertibles. Suposem que grau$(g(x)) = 0$. Aleshores $g \in A \setminus (A^* \cup \{0\})$ i g divideix tots els coeficients de $f(x)$. Per tant, c$(f(x)) \neq 0$ i $f(x)$ no és primitiu, la qual cosa suposa una contradicció amb la hipòtesi. □

Proposició 4.4.8. *Sigui A un DFU, $p \in A$. Aleshores, si p és primer en A, p és primer en $A[x].$*

Demostració. Clarament $p \neq 0$ i p no és invertible en A. Per tant, p no és invertible en $A[x]$. Siguin

$$d(x) = d_0 + d_1x + ... + d_nx^n \in A[x],$$

$$e(x) = e_0 + e_1x + ... + e_mx^m \in A[x],$$

tals que $p \nmid d(x)$ i $p \nmid e(x)$ en $A[x]$. Vegem que $p \nmid d(x)e(x)$ en $A[x]$. Prenem $d_r, e_s \in A$ els coeficients d'índex mínim tals que $p \nmid d_r$ i $p \nmid e_s$. En particular, com que p és primer en A, $p \nmid d_re_s$. Tenim,

$$d(x)e(x) = d_0e_0 + ... + \left(\sum_{i=-r}^{r+s} d_{r+i}e_{s-i}\right) x^{r+s} + ... + d_ne_mx^{n+m}.$$

Observem que p divideix tots els sumands del coeficient de x^{r+s} llevat de d_re_s. Així, doncs, $p \nmid d(x)e(x)$ i concloem que p és primer en $A[x]$. □

Proposició 4.4.9. *Sigui A un DFU i $K = K(A)$ el seu cos de fraccions. Sigui $f(x) \in A[x]$, un polinomi no constant. Suposem que $f(x)$ descomposa en $f(x) = u(x)v(x)$, on $u(x), v(x) \in K(x)$ son de grau ≥ 1. Aleshores, existeix $\lambda \in K$, tal que $\lambda u(x) \in A[x]$, $\lambda^{-1}v(x) \in A[x]$ i $f(x) = (\lambda u(x))(\lambda^{-1}v(x))$ és una descomposició de f en producte de polinomis de $A[x]$ de graus ≥ 1. En particular, si f és irreductible en $A[x]$, aleshores f és irreductible en $K[x]$.*

Demostració. Sigui $a \in A$, respectivament, $b \in A$, el mínim comú múltiple dels denominadors dels coeficients de $u(x)$, respectivament, $v(x)$. Aleshores, $f(x) = u(x)v(x) = (1/a)g(x)(1/b)h(x)$, amb $g(x), h(x) \in A[x]$. Multiplicant per ab, tenim $abf(x) = g(x)h(x)$.

Sigui $p_1 \in A$ primer que divideix ab (recordem que A és DFU). És a dir, $ab = p_1c_1$, per a algun $c_1 \in A$. Per la Proposició 4.4.8, p_1 també és un element primer de $A[x]$. Com que $p_1|abf(x) = g(x)h(x)$, aleshores o bé $p_1 \mid g(x)$ o bé $p_1 \mid h(x)$ en $A[x]$. Suposem que $p_1 \mid g(x)$. És a dir, $g(x) = p_1g_1(x)$, per a algun $g_1(x) \in A[x]$. Aleshores, $p_1c_1f(x) = abf(x) = g(x)h(x) = p_1g_1(x)h(x)$. Simplificant p_1, tenim $c_1f(x) = g_1(x)h(x)$ en $A[x]$, on $c_1 \in A$.

Repetim el procés: sigui $p_2 \in A$ primer que divideix a c_1. És a dir, $c_1 = p_2c_2$, per a algun $c_2 \in A$. Per la Proposició 4.4.8, p_2 també és un element primer de $A[x]$. Com que $p_2 \mid c_1f(x) = g_1(x)h(x)$, aleshores, o bé $p_2 \mid g_1(x)$ o bé $p_2 \mid h(x)$ en $A[x]$. Suposem que $p_2 \mid h(x)$ (altrament és anàleg). És a dir, $h(x) = p_2h_1(x)$, amb $h_1(x) \in A[x]$. Aleshores, $p_2c_2f(x) = c_1f(x) = g_1(x)h(x) = p_2g_1(x)h_1(x)$. Simplificant p_2, tenim $c_2f(x) = g_1(x)h(x)$ en $A[x]$, on $c_2 \in A$.

Sigui $ab = p_1 \cdots p_n$, la descomposició de ab en factors primers en A. Hem vist que cada factor p_i, o bé divideix $g(x)$ o bé divideix $h(x)$ (o bér ambdós). Podem anomenar $\alpha_1, \ldots, \alpha_r$ als factors primers de ab que divideixen $g(x)$ i $\alpha := \alpha_1 \cdots \alpha_r \in A$. Igualment, podem anomenar $\beta_1, \ldots, \beta_s$ als factors primers de ab que divideixen $h(x)$ i $\beta := \beta_1 \cdots \beta_s \in A$. De manera que $ab = \alpha\beta$. Aleshores, el que hem vist de manera recurrent és que: $\alpha_1 \mid g(x)$, $\alpha_2 \mid g(x)/\alpha_1$ i, successivament, $\alpha_r \mid g(x)/(\alpha \cdots \alpha_{r-1})$. Anàlogament, $\beta_1 \mid h(x)$, $\beta_2 \mid h(x)/\beta_1$ i, successivament, $\beta_s \mid h(x)/(\beta_1 \cdots \beta_{s-1})$.

Així, $ab = \alpha\beta$, amb $\alpha, \beta \in A$ i $g(x) = \alpha d(x)$, $h(x) = \beta e(x)$, amb $d(x), e(x) \in A[x]$. Finalment, $(ab)f(x) = g(x)f(x) = \alpha d(x)\beta e(x) = (\alpha\beta)d(x)e(x) = (ab)d(x)e(x)$. Simplificant, $f(x) = d(x)e(x)$. D'altra banda, $f(x) = u(x)v(x)$, amb $u(x) = (1/a)g(x)$, $g(x) = \alpha d(x)$, $v(x) = (1/b)h(x)$ i $h(x) = \beta e(x)$. Substituïnt, $f(x) = (\alpha/a)(\beta/b)d(x)e(x)$. De $f(x) = d(x)e(x)$ i de $f(x) = (\alpha/a)(\beta/b)d(x)e(x)$, deduïm que $(\alpha/a)(\beta/b) = 1$. Anomenant $\lambda = \beta/b \in K$, tenim $\alpha/a = \lambda^{-1}$ i $u(x) = (\alpha/a)d(x) = \lambda^{-1}d(x)$ i, per tant, $\lambda u(x) = d(x) \in A[x]$. Anàlogament, $v(x) = (\beta/b)e(x) = \lambda e(x)$ i, per tant, $\lambda^{-1}v(x) = e(x) \in A[x]$. □

Proposició 4.4.10. *Sigui A un DFU, $K = K(A)$ el cos de fraccions de A, $f(x) \in A[x]$ un polinomi no constant. Aleshores $f(x)$ és irreductible en $A[x]$ si i només si $f(x)$ és primitiu i $f(x)$ és irreductible en $K[x]$.*

Demostració. ($\Longrightarrow$). Suposem que $f(x)$ és irreductible en $A[x]$. Aleshores $f(x)$ és primitiu. En efecte, altrament, $f(x) = \mathrm{c}(f(x))f^*(x)$ seria una descomposició de $f(x)$ en dos elements no invertibles de $A[x]$, ja que $\mathrm{c}(f(x)) \notin A^*$ i $\mathrm{grau}(f^*(x)) \geq 1$. Com que, per hipòtesi, $f(x)$ no és constant, tenim que $f(x) \notin (K[x])^* = K \setminus \{0\}$. Suposem que $f(x) = u(x)v(x)$, amb $u(x), v(x) \in K[x]$ de grau major o igual a 1. Aleshores, per la Proposició 4.4.9, $f(x) = (\lambda u(x))(\lambda^{-1}v(x))$, amb $(\lambda u(x)), (\lambda^{-1}v(x)) \in A[x]$ no irreductibles.

($\Longleftarrow$). Com que $f(x)$ és no constant, tenim que $f(x) \notin A^*$, $f(x) \neq 0$. A més, per hipòtesi, $f(x)$ és primitiu. Si $f(x)$ no és irreductible en $A[x]$, per l'Observació 4.4.7, $f(x) = g(x)h(x)$, amb $g(x), h(x) \in A[x] \subseteq K[x]$ de grau ≥ 1. Per tant, $f(x)$ no és irreductible en $K[x]$. □

Proposició 4.4.11. *Sigui A un DFU, $f(x) \in A[x]$ un polinomi no constant. Si $f(x) = ag(x)$ amb $a \in A$ i $g(x)$ primitiu, aleshores $a = c(f(x))$.*

Demostració. És clar que $a \mid ag(x) = f(x) \Longrightarrow a \mid \mathrm{c}(f(x))$. Sigui $\mathrm{c}(f(x)) = p_1 \cdots p_r$ la descomposició en primers en A. Tenim $f(x) = \mathrm{c}(f(x))f^*(x)$, on $f^*(x)$ és primitiu. O sigui, $p_1 \cdots p_r f^*(x) = ag(x)$. Per tant, $p_1 \mid ag(x)$ i $p_1 \nmid g(x)$ (per ser $g(x)$ primitiu). Aleshores, per la Proposició 4.4.8, $p_1 \mid a$. És a dir, $a = p_1 a_2$, per a algun $a_2 \in A$. Així, $p_1 \cdots p_r f^*(x) = ag(x) = p_1 a_2 g(x)$. Simplificant, $p_2 \cdots p_r f^*(x) = a_2 g(x) \Longrightarrow p_2 \mid a_2 g(x)$ i $p_2 \nmid g(x)$. De nou, per la Proposició 4.4.8, tenim que $p_2 \mid a_2$ i $a_2 = p_2 a_3$. Així, $p_2 \cdots p_r f^*(x) = a_2 g(x) = p_2 a_3 g(x) \Longrightarrow p_3 \cdots p_r f^*(x) = a_3 g(x)$. Recursivament, $p_r f^*(x) = a_r g(x)$, $p_r \mid a_r g(x)$, $p_r \nmid g(x) \Longrightarrow p_r \mid a_r$ i $a_r = p_r a_{r+1}$. Per tant, $a = p_1 a_2 = p_1 p_2 a_3 = \ldots = p_1 \cdots p_{r-1} a_r = p_1 \cdots p_{r-1} p_r a_{r+1} = \mathrm{c}(f(x)) a_{r+1}$. O sigui, $\mathrm{c}(f(x)) \mid a$ i $a \mid \mathrm{c}(f(x))$. Per tant, $a = \mathrm{c}(f(x))$, llevat d'associats. □

Lema 4.4.12 (Lema de Gauss)**.** *Sigui A un DFU, $f(x), g(x) \in A[x]$ polinomis no constants. Aleshores $c(f(x)g(x)) = c(f(x))c(g(x))$. En particular: f, g primitius $\Longleftrightarrow fg$ primitiu.*

Demostració. Siguin $u(x), v(x) \in A[x]$. Suposem que $u(x)$ és primitiu i $u(x)v(x)$ no és primitiu. Aleshores existeix $p \in A$ primer, tal que $p \mid u(x)v(x)$. A més, $p \nmid u(x)$. Per tant, per la Proposició 4.4.8, $p \mid v(x)$ i $v(x)$ no és primitiu. És a dir, si $v(x)$ i $u(x)$ són primitius, aleshores $v(x)u(x)$ és primitiu. Ara escrivim $f(x) = \mathrm{c}(f(x))f^*(x)$ i $g(x) = \mathrm{c}(g(x))g^*(x)$ amb $f^*(x), g^*(x) \in A[x]$ primitius. Per tant, $f^*(x)g^*(x)$ és primitiu. Així, tenim $fg = (\mathrm{c}(f(x))\mathrm{c}(g(x)))f^*(x)g^*(x)$. Aleshores, per la Proposició 4.4.11, $\mathrm{c}(fg) = \mathrm{c}(f(x))\mathrm{c}(g(x))$. □

Demostració del Teorema 4.4.1. Hem de veure que per a tot $f(x) \in A[x] \setminus ((A[x])^* \cup \{0\})$, existeix una única descomposició de $f(x)$ en producte d'elements irreductibles de $A[x]$.

Veurem primerament l'existència de la descomposició. Si $\mathrm{grau}(f(x)) = 0$, aleshores $f \in A$. Com A és factorial, f descomposa de forma única en producte d'elements irreductibles de A. Per l'Observació 4.4.4, sabem que són també irreductibles en $A[x]$, i ja ho tenim. Si $\mathrm{grau}(f(x)) \geq 1$, aleshores, $f(x) \in A[x] \subseteq K[x]$, on $K = K(A)$, el cos de fraccions de A. Com K és un cos, $K[x]$ és Euclidià (vist a l'Exercici 3.7.5) i, en particular, un DFU. Per tant, existeix una única descomposició, $f(x) = f_1(x) \cdot \cdots \cdot f_r(x)$, on els $f_i(x)$ són elements irreductibles de $K[x]$ i, conseqüentment, $\mathrm{grau}(f_i(x)) \geq 1$. Per tant, aplicant la Proposició 4.4.9 de forma recursiva obtenim:

$$\begin{aligned}
&f(x) = f_1(x) \cdots f_r(x) \Longrightarrow f(x) = (\lambda_1 f_1(x)) \cdot (\lambda_1^{-1} f_2(x) \cdot \cdots \cdot f_r(x)),\\
&\ldots\\
&f(x) = (\lambda_1 f_1(x)) \cdots (\lambda_{r-1} f_{r-1}(x))(\lambda_1^{-1} \cdots \lambda_{r-1}^{-1} f_r(x)) \Longrightarrow\\
&\Longrightarrow f(x) = (\lambda_1 f_1(x)) \cdots (\lambda_{r-1} f_{r-1}(x))(\lambda_r f_r(x)),
\end{aligned}$$

on $\lambda_r = \lambda_1^{-1} \cdots \lambda_{r-1}^{-1}$ i, per a tot $i = 1, \ldots, r$, $\lambda_i \in K$, $\lambda_i f_i(x) \in A[x]$. Així doncs, tenim:

$$\begin{aligned}
f(x) &= (\lambda_1 f_1(x)) \cdots (\lambda_r f_r(x)) = c(\lambda_1 f_1(x))\hat{f}_1(x) \cdots c(\lambda_r f_r(x))\hat{f}_r(x) =\\
&= c(\lambda_1 f_1(x)) \cdots c(\lambda_r f_r(x))\hat{f}_1(x) \cdots \hat{f}_r(x),
\end{aligned}$$

on els $\hat{f}_i(x)$ són irreductibles en $A[x]$, per ser irreductibles en $K[x]$ i primitius (Proposició 4.4.10). A més, ja hem vist que $c(\lambda_1 f_1(x)) \cdots c(\lambda_r f_r(x)) \in A$ descomposa en producte d'elements irreductibles en $A[x]$. Per tant, hem provat que existeix una descomposició de $f(x)$ en elements irreductibles de $A[x]$.

Hem de veure ara que la descomposició és única. Suposem que

$$f(x) = g_1(x) \cdots g_n(x) = h_1(x) \cdots h_m(x),$$

on els $g_i(x), h_j(x)$ són elements irreductibles de $A[x]$. Suposem, sense pèrdua de generalitat, que $g_1(x), \ldots, g_r(x)$,$h_1(x), \ldots, h_s(x)$, són de grau zero, i $g_{r+1}(x), \ldots, g_n(x), h_{s+1}(x), \ldots, h_m(x)$, són de grau major o igual a 1. Prenem el contingut de $f(x)$, que pel Lema 4.4.12, i la Proposició 4.4.11, sabem que ve donat per:

$$c(f(x)) = g_1 \cdots g_r = h_1 \cdots h_s.$$

Per tant, per ser $g_1, \ldots, g_r, h_1, \ldots, h_s \in A$ irreductibles, i A un DFU, deduïm que $r = s$ i $g_i = h_i$, $\forall i \leq r$, llevat d'ordre i associats. Al seu torn,

$$g_{r+1}(x) \cdots g_n(x) = h_{s+1}(x) \cdots h_m(x),$$

en $K[x]$. En particular, per ser $g_{r+1}(x), \ldots, g_n(x), h_{s+1}(x), \ldots, h_m(x)$ irreductibles en $A[x]$ i de grau major o igual a 1, per la Proposició 4.4.10, sabem que són irreductibles i primitius en $K[x]$. Com $K[x]$ és un DFU, $n = m$, i $g_i(x) = h_i(x)$ en $K[x]$, llevat d'ordre d'associats. Per tant, $g_i(x) = c_i h_i(x)$, on $c_i = \frac{a_i}{b_i}, a_i, b_i \in A \Longrightarrow b_i g_i = a_i h_i$. Finalment, $b_i = c(b_i g_i(x)) = c(a_i h_i(x)) = a_i$, així doncs, $c_i = 1$, i $a_i = b_i$, llevat d'associats. Per tant, tal i com volíem veure, $h_i(x) = g_i(x)$, llevat d'associats. □

Teorema 4.4.13. *Sigui A un DFU. Aleshores $A[x_1, \ldots, x_n]$ és també un DFU.*

Demostració. Aquest resultat és conseqüència del Teorema 4.4.1 per inducció en el nombre de variables. □

Corol·lari 4.4.14. *Sigui $\mathbb{K}$ un cos. Aleshores $\mathbb{K}[x_1, \ldots, x_n]$ és DFU.*

4.4.2 Exemples de DFUs no DIPs

Ens trobem ara en condicions d'analitzar alguns exemples de DFUs que no són DIPs.

Exemple 4.4.15. Sigui $A = \mathbb{Z}[x]$, l'anell de polinomis en una variable x amb coeficients a l'anell dels enters $\mathbb{Z}$. Vegem que A és un DFU que no és DIP. Com $\mathbb{Z}$ és un DFU, pel Teorema 4.4.1, A és un DFU. Per tal de veure que A no és un DIP considerem, per exemple, l'ideal $I = \langle 2, x \rangle \subset A$. Veurem que I no és principal. Suposem que existeix $f(x) \in A$, tal que $I = (f(x))$, aleshores $2 = h(x)f(x)$ i $x = g(x)f(x)$, per a certs $h(x), g(x) \in A$. Com grau$(2) = 0$, necessàrimaent grau$(f(x)) = 0$, és a dir, $f(x) = \alpha \in \mathbb{Z}$. A més, α divideix 2 a $\mathbb{Z}$, per tant o bé $\alpha = \pm 1$, o bé $\alpha = \pm 2$. En el primer cas tindríem $1 \in \langle 2, x \rangle = A$, la qual cosa suposa una contradicció. Suposem doncs que $\alpha \in \{-2, 2\}$. En aquest cas, $x = g(x)\alpha$, on $g(x) = bx$, per a cert $b \in \mathbb{Z}$, és a dir, $x = \alpha bx$. De la darrera expressió obtenim $\alpha b = 1 \Longrightarrow \alpha \in (\mathbb{Z})^* = \{1, -1\}$, i per tant arribem a una contradicció.

Sabem que l'Exemple 4.4.15 no funciona en el cas d'un anell de polinomis en una variable x amb coeficients en un cos $\mathbb{K}$, ja que, tal i com s'ha vist, en aquest cas $\mathbb{K}[x]$ és DIP. No obstant, es comprova que la condició DIP desapareix quan afegim més d'una variable.

Exemple 4.4.16. Sigui $A = \mathbb{K}[x, y]$, l'anell de polinomis en dues variables x i y amb coeficients a un cos $\mathbb{K}$. Pel Teorema 4.4.13, sabem que A és un DFU. No obstant, A no és un DIP. Per tal de veure que A no és un DIP provarem que l'ideal $I = \langle x, y\rangle \subset A$ no és principal. En efecte, suposem que existeix $f(x, y) \in A$, tal que $I = (f(x, y))$, aleshores $x = bf(x, y)$ i $y = cf(x, y)$, per a certs $c, b \in A$. Igualant els graus en x i en y de les dues expressions anteriors és immediat veure que $f(x, y)$ és de la forma $f(x, y) = a_0+a_1x+a_2y+a_3xy$. Mirant ara el grau total obtenim $a_3 = 0$. Al seu torn, no pot ser $a_1 = a_2 = 0$, ja que aleshores tindríem o bé $(f(x, y)) = (0)$, o bé $(f(x, y)) = A$. Per tant necessàriament $f(x, y) = a_0 + a_1x + a_2y$, on o bé $a_1 \neq 0$, o bé $a_2 \neq 0$. Resulta fàcil veure que sota aquestes condicions el sistema d'equacions $x = bf(x, y)$ i $y = cf(x, y)$, on $c, b \in A$ no té solució.

De fet, utilitzant el mateix raonament que a l'Exemple 4.4.17, és trivial veure un cas més general:

Exemple 4.4.17. Sigui $A = \mathbb{K}[x_1, \ldots, x_n]$, l'anell de polinomis en n variables $x_1, \ldots, x_n$, on $n \geq 2$, amb coeficients en un cos $\mathbb{K}$. Aleshores A és un DFU però no és un DIP.

4.5 DIP no Euclidià

Generalment, en els texts d'àlgebra abstracta per a estudiants i graduats, es demostra amb un argument prou simple, tal i com s'ha vist a la Proposició 3.7.6, que tot domini Euclidià és DIP. Aleshores es menciona que el recíproc no és cert en general, i sovint es cita a [10], on es presenta el contraexemple:

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-19}}{2}\right) \mid a, b \in \mathbb{Z}\right\} \subseteq \mathbb{C}.$$

No obstant, els detalls d'aquest exemple acostumen a ser omesos o deixats en forma d'una sèrie d'exercicis.

Per tal de simplificar la notació, sigui

$$\theta := \frac{1+\sqrt{-19}}{2},$$

durant tot el punt 4. La prova de que $\mathbb{Z}[\theta]$ no és un domini Euclidià és relativament senzilla. En aquest treball, incloem una prova similar a la de [14]. En canvi, provar que A és un DIP resulta més complicat. En aquest treball fem una prova similar a la de [3], basada en la caracterització dels DIP amb la norma de Dedekind-Hasse.

4.5.1 Caracterització dels DIP usant la norma de Dedekind-Hasse

Sabem, per la Proposició 3.7.6, que el conjunt dels anells Euclidians es troba inclòs en el conjunt dels DIPs. No obstant, com ja hem comentant, aquesta inclusió és estricta. És a dir, no tots els DIPs tenen una norma Euclidiana. De fet, el que es veurà seguidament, és que els DIPs compleixen unes condicions similars però més febles que les de l'existència d'una norma Euclidiana.

Observació 4.5.1. Sigui A un domini, N una norma Euclidiana sobre A, $a, b \in A$, $b \neq 0$. Aleshores, per definició existeixen q, r, tals que $a = bq + r$, i o bé $r = 0$, o bé $N(r) < N(b)$. Observem que si $r = 0$, aleshores $b \mid a$. Altrament, $r = a - bq \in \langle a, b\rangle$, i $N(r) < N(b)$.

La darrera observació permet debilitar la definició de norma Euclidiana.

Definició 4.5.2. Sigui A un domini. Anomenem *norma de Dedekind-Hasse* a una aplicació,

$$\begin{aligned} N : A \setminus \{0\} &\longrightarrow \mathbb{N} \\ x &\longmapsto N(x), \end{aligned}$$

tal que, per a tot $a, b \in A$, amb $b \neq 0$, o bé $b|a$, o bé existeix algun $r \in \langle a, b\rangle$ no nul, tal que $N(r) < N(b)$.

Observació 4.5.3. Una norma Euclidiana és una norma de Dedekind-Hasse.

Demostració. Trivial a partir de l'Observació 4.5.1. □

L'interès d'aquesta nova definició resideix en que aquest tipus de norma no només es troba necessàriament als dominis Euclidians sinó en tot DIP. És més, l'existència d'una norma de Dedekind-Hasse caracteritza els DIPs.

Teorema 4.5.4. *Sigui A un domini. Aleshores A és un DIP si i només si A admet una norma de Dedekind-Hasse.*

Demostració. ($\Longrightarrow$). Donat que A és un DIP, A és un DFU. Considerem l'aplicació següent:

$$\begin{aligned} N : A \setminus \{0\} &\longrightarrow \mathbb{N} \\ a = p_1 \cdots p_n &\longmapsto N(a) = n, \end{aligned}$$

on $p_1 \cdots p_n$, és la descomposició de a en producte d'elements primers. En primer lloc observem, que per ser una descomposició única (llevat d'ordre i associats) l'aplicació està ben definida. Vegem que N és una norma de Dedekind-Hasse en A. Siguin $a, b \in A$, on $b \neq 0$. Si $b \mid a$, ja ho tenim. Altrament $\langle a, b\rangle = (d) \neq (0)$, on $d = \text{mcd}(a, b)$. Prenem $r := d$, i vegem que $N(r) = N(d) < N(b)$. En efecte, per ser $d = \text{mcd}(a, b)$, en particular $b = \alpha d$, per a algun $\alpha \in A$. Aleshores, pel Lema 3.4.13, necessàriament $N(r) = N(d) \leq N(b)$, i a més, la desigualtat anterior ha de ser estricta, ja que altrament tindríem $\alpha \in A^*$, la qual cosa es contradiu amb $b \nmid a$.
($\Longleftarrow$). Sigui I un ideal qualsevol de A. Si $I = \{0\} = (0)$, ja ho tenim. Altrament, prenem

$b \in I, b \neq 0$, un element tal que $N(b) \leq N(x)$, per a tot $x \in I \setminus \{0\}$. Vegem que $I = (b)$. Clarament $(b) \subseteq I$. Hem de veure, doncs, $I \subseteq (b)$. Sigui $x \in I$, si $x = 0$ o bé $b \mid x$, ja ho tenim. Altrament, per hipòtesi, existeix $r \in \langle x, b \rangle$, $r \neq 0$, amb $N(r) < N(b)$. Però $r \in \langle x, b \rangle \subseteq I$, i per tant $N(b) \leq N(x)$, la qual cosa suposa una contradicció amb el fet que $N(b) \leq N(x)$, per a tot $x \in I \setminus \{0\}$. □

4.5.2 $\mathbb{Z}[\theta]$ és DIP

Prenem $A := \mathbb{Z}[\theta]$ en tot el punt. Observem primer que $\theta^2 = \theta - 5$ i, per tant, $\theta^2 \in A$. És a dir, A és tancant respecte al producte dels complexos; condició necessària per a ser A un subanell de $\mathbb{C}$, però no trivial a partir de la definició. En particular, es comprova que, en efecte:

$$A = \mathbb{Z}[\theta] = \{(a + b\theta) \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C},$$

i A és un subanell de $\mathbb{C}$. En particular, A és un domini. Per a veure que A és un domini d'ideals principals, utilitzarem la caracterització dels DIP amb la norma de Dedeking-Hasse vista al Teorema 4.5.4. És a dir, provarem que podem definir una norma de Dedekind-Hasse en A.

Teorema 4.5.5. *$A = \mathbb{Z}[\theta]$ és un DIP.*

Demostració. Volem veure que podem definir una norma de Dedekind-Hasse, N, sobre A. És a dir, siguin $\alpha, \beta \in A$, $\beta \neq 0$. Volem provar que o bé $\beta \mid \alpha$, o bé existeix algun $r \in \langle \alpha, \beta \rangle$, no tul, tal que $N(r) < N(\beta)$. Dit amb altres paraules, si $\beta \nmid \alpha$, i $N(\alpha) \geq N(\beta)$, aleshores existeixen $\gamma, \delta \in A$, tals que $r := \gamma\alpha - \delta\beta \neq 0$, i $N(\gamma\alpha - \delta\beta) < N(\beta)$. Considerem l'aplicació:

$$\begin{aligned} N : A &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto N(\alpha) = \alpha\bar{\alpha}, \end{aligned}$$

és a dir, la norma usual als nombres complexos. Aleshores, és fàcil veure que es verifiquen les identitats següents:

(i) $N(a + b\theta) = a^2 + ab + 5b^2 \in \mathbb{Z}^{\geq 0}$.

(ii) $N(xy) = N(x)N(y)$, per a tot $x, y \in A$,

(iii) $N(x) \geq 0$ per a tot $x \in A$; i $N(x) = 0$ si i només si $x = 0$.

Vegem que N és una norma de Dedekind-Hasse en A. Siguin $\alpha, \beta \in A$, $\beta \neq 0$. Si $\beta \mid \alpha$, ja ho tenim. Si $\beta \nmid \alpha$ i $N(\alpha) < N(\beta)$, prenem $r = \alpha \in \langle \alpha, \beta \rangle$, i ja ho tenim. Altrament, escrivim:

$$\frac{\alpha}{\beta} = a + b\theta,$$

on $a, b \in \mathbb{Q}$, i almenys un dels dos no és un enter (ja que altrament tindríem $\beta \mid \alpha$). Això és possible degut a que l'invers de β com a complex pertany a $\mathbb{Q}[\theta] \subsetneq \mathbb{C}$ i, per tant, $\alpha\beta^{-1} \in \mathbb{Q}[\theta]$.

Veurem que, considerant tots els possibles valors de a i b, obtenim, per a cada cas, els elements $\gamma, \delta \in A$, tals que,

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) < 1 \text{ i per tant, } N(\alpha\gamma - \delta\beta) < N(\beta).$$

Podem agrupar tots els possibles valors de a i b en set casos diferents. Notem per $\{n\}$ l'enter més proper a n, amb $\{n + 1/2\} = n$. Tenim:

1. **Cas:** $a \notin \mathbb{Z}$**,** $b \in \mathbb{Z}$. Aleshores, prenem $\gamma = 1$, $\delta = \{a\} + b\theta$ i tenim:

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) \leq \frac{1}{4} < 1.$$

2. **Cas:** $a \in \mathbb{Z}$.

   (a) **Cas:** $5b \notin \mathbb{Z}$. Aleshores, $(\alpha/\beta)\bar{\theta} = a + 5b - a\theta$. Per tant, podem prendre $\gamma = \bar{\theta}$, $\delta = \{a + 5b\} - a\theta$.

   (b) **Cas:** $5b \in \mathbb{Z}$. En aquest cas, prenem $\gamma = 1$, $\delta = a + \{b\}\,\theta$.

3. **Cas:** $a, b \notin \mathbb{Z}$.

   (a) **Cas:** $2a$, $2b \in \mathbb{Z}$. En aquest cas, $(\theta\alpha)/\beta = -5b + (a + b)\theta$ i $a + b \in \mathbb{Z}$. Per tant, podem prendre $\gamma = \theta$, $\delta = \{-5b\} + \{a + b\}\,\theta$.

   (b) **Cas:** $2a$, $2b \notin \mathbb{Z}$. Aleshores, o bé $|b - \{b\}\,| \leq 1/3$, o bé $|2b - \{2b\}\,| \leq 1/3$. En el primer cas, prenem $\gamma = 1$ i $\delta = \{a\} + \{b\}\,\theta$ i tenim:

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) \leq \frac{35}{36} < 1.$$

   Per al segon cas, podem prendre $\gamma = 2$ i $\delta = \{2a\} + \{2b\}\,\theta$, amb la mateixa aproximació d'abans.

   (c) **Cas:** $2a \in \mathbb{Z}$ i $2b \notin \mathbb{Z}$. Si $5b \in \mathbb{Z}$, prenem $\gamma = 5$ i $\delta = \{5a\} + 5b\theta$. Quan $5b \notin \mathbb{Z}$, prenem $\gamma = 2\bar{\theta}$ i $\delta = \{2a + 10b\} - 2a\theta$.

   (d) **Cas:** $2a \notin \mathbb{Z}$ i $2b \in \mathbb{Z}$. Prenem $\gamma = 2$, $\delta = \{2a\} + 2b\theta$.

□

4.5.3 $\mathbb{Z}[\theta]$ no és un domini Euclidià

En la nostra prova de que $\mathbb{Z}[\theta]$ no és un DIP els elements $\pm 1, \pm 2$ i ± 3 juguen un paper molt important. Començarem per veure que ± 1 són els únics elements invertibles de $\mathbb{Z}[\theta]$. Seguidament, es veurà que els elements ± 2 i ± 3 són irreductibles en $\mathbb{Z}[\theta]$. Sigui $A := \mathbb{Z}[\theta]$ en tot el punt i,

$$\begin{aligned} N : A &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto N(\alpha) = \alpha\bar{\alpha}, \end{aligned}$$

és a dir, la norma usual als nombres complexos, vista en el punt anterior. Farem primer una sèrie d'observacions, que són conseqüència directa de la definició de θ.

Observació 4.5.6. Es verifiquen les identitats següents:

(i) $\bar{\theta} = 1 - \theta$,

(ii) $\theta\bar{\theta} = 5$,

(iii) per a tot $x = a + b\theta \in A$, $\theta x = -5b + (a + b)\theta$.

De (i) segueix que A és tancat per conjugació complexa. Més endavant es veurà que θ i $\bar{\theta}$ no són invertibles en A i, per tant, la identitat (ii) implica que 5 no és irreductible. Veurem ara, a partir de les observacions prèvies i les propietats de N vistes en el punt anterior, que efectivament ± 1 són els únics elements invertibles de A.

Lema 4.5.7. *Donat $\alpha \in A$, les afirmacions següents són equivalents:*

(i) $\alpha = 1$ o $\alpha = -1$;

(ii) α és invertible a A;

(iii) $|\alpha| = 1$.

Demostració. (i) $\Longrightarrow$ (ii). És clar.
(ii) $\Longrightarrow$ (iii). Si α és invertible en A, aleshores existeix $\beta \in A$, tal que $1 = \alpha\beta$. Per tant, $1 = |\alpha\beta| = |\alpha||\beta|$. Com $|\alpha|$ i $|\beta|$ són enters positius, deduïm que $|\alpha| = |\beta| = 1$.
(iii) $\Longrightarrow$ (i). Podem escriure $\alpha = a + b\theta$, per a certs $a, b \in \mathbb{Z}$. Aleshores, per les propietats de N, tenim $1 = |\alpha| = a^2 + ab + 5b^2 = (a + b/2)^2 + (19/4)b^2$. Com $a, b \in \mathbb{Z}$, necessàriament $b = 0$, que al seu torn implica que $a^2 = 1$. □

Lema 4.5.8. *Els elements ± 2 i ± 3 són irreductibles en A.*

Demostració. Com ± 1 són invertibles, només cal provar que 2 i 3 són irreductibles. Comencem per veure que 2 és irreductible. Clarament $2 \in A \setminus (A^* \cup \{0\})$. Suposem que tenim $2 = \alpha\beta$, per a certs $\alpha, \beta \in A$. Aleshores $4 = |2| = |\alpha\beta| = |\alpha||\beta|$. Com $|\alpha|$ i $|\beta|$ són enters positius, $(|\alpha|, |\beta|) = (1, 4), (2, 2)$ o $(4, 1)$. Aplicant el Lema 4.5.7, obtenim que $\alpha \in A^*$ en el primer cas, i $\beta \in A^*$ en el darrer. Suposem que $(|\alpha|, |\beta|) = (2, 2)$. Aleshores, podem escriure $\alpha = a + b\beta$, per a certs $a, b \in A$. Per tant, $2 = |\alpha| = a^2 + ab + 5b^2 = (a + b/2)^2 + (19/4)b^2$. Com $a, b \in \mathbb{Z}$, necessàriament $b = 0$, cosa que implica que $a^2 = 2$ i suposa una contradicció. La prova de que 3 és irreductible és similar. Clarament $3 \in A \setminus (A^* \cup \{0\})$. Suposem que tenim $3 = \alpha\beta$, per a certs $\alpha, \beta \in A$. Aleshores, $9 = |3| = |\alpha\beta| = |\alpha||\beta|$. De nou, com $|\alpha|$ i $|\beta|$ són enters positius, $(|\alpha|, |\beta|) = (1, 9), (3, 3)$ o $(9, 1)$. Aplicant el Lema 4.5.7, obtenim que $\alpha \in A^*$ en el primer cas, i $\beta \in A^*$ en el darrer. Suposem que $(|\alpha|, |\beta|) = (3, 3)$. Aleshores, podem escriure $\alpha = a + b\beta$, per a certs $a, b \in A$. Per tant, $3 = |\alpha| = a^2 + ab + 5b^2 = (a + b/2)^2 + (19/4)b^2$. Com $a, b \in \mathbb{Z}$, necessàriament $b = 0$, cosa que implica que $a^2 = 3$, la qual cosa suposa una contradicció. □

Teorema 4.5.9. *$A = \mathbb{Z}[\theta]$ no és un domini Euclidià.*

Demostració. Suposem que A és un domini Euclidià. Aleshores, per definició, existeix una norma Euclidiana, $D : A \setminus \{0\} \longrightarrow \mathbb{N}$, satisfent:

$$\forall\ \alpha, \beta \in A, \text{ on } \beta \neq 0, \exists\ q, r \in A, \text{ tals que } \alpha = \beta q + r, \text{ i o bé } r = 0, \text{ o bé } D(r) < D(\beta).$$

Com que la imatge de D viu a $\mathbb{N}$, podem triar $m \in A$, tal que $D(m)$ prengui el mínim valor possible subjecte a $m \neq 0, m \notin A^*$. Aleshores, siguin $q, r \in A$, el quocient i el residu, respectivament, obtinguts en dividir m entre 2 en A. Tenim:

$$2 = mq + r, \text{ on o bé } r = 0 \text{ o bé } D(r) < D(m).$$

Tenim que $D(m)$ és mínim subjecte a ser m diferent de zero i no invertible. Per tant, o bé $r = 0$, o bé $D(r) < D(m)$ i r és invertible en A, és a dir, $r = -1$ o $r = 1$ (Lema 4.5.7). Així:

- Si $r = 0$, aleshores m divideix 2. Com m no és invertible i 2 és irreductible en A, necessàriament q és invertible en A, és a dir, $q = \pm 1$. Per tant, o bé $q = 1$ i $m = 2$, o bé $q = -1$ i $m = -2$.

- Si $r = -1$, aleshores m divideix 3. De forma anàloga es dedueix que o bé $q = 1$ i $m = -3$ o bé $q = -1$ i $m = 3$.

- Si $r = 1$, aleshores m divideix 1, fet que suposa una contradicció donat que m no és invertible per hipòtesi.

Per tant hem vist que els únics possibles valors de m són ± 2 i ± 3. Dividim ara θ per m en A, obtenint:

$$\theta = mq' + r', \text{ per a certs } q', r' \in A, \text{ tals que o bé } r' = 0, \text{ o bé } D(r') < D(m).$$

De nou, donat que $D(m)$ és mínim subjecte a ser m diferent de zero i no invertible, obtenim que si $r \neq 0$, o bé $r' = -1$ o bé 1. Així:

- Si $r' = 0$, aleshores m divideix θ en A. Però $m \in \{\pm 2, \pm 3\}$. Per tant, $(1/m)\theta \notin A$, la qual cosa suposa una contradicció.

- Si $r' = -1$, aleshores m divideix $1+\theta$ en A. Però $m \in \{\pm 2, \pm 3\}$. Per tant, $(1/m)(1+\theta) \notin A$, la qual cosa suposa una contradicció.

- Si $r' = 1$, aleshores m divideix $-1+\theta$ en A. Però $m \in \{\pm 2, \pm 3\}$. Per tant, $(1/m)(-1+\theta) \notin A$, la qual cosa suposa una contradicció.

□

4.6 Dominis de Bézout

Fins ara hem comprovat que les famílies de dominis Euclidians, DIPs, DFUs, i GCD, compleixen les inclusions estrictes següents:

$$\{\text{Dominis Euclidians}\} \subsetneq \{\text{DIPs}\} \subsetneq \{\text{DFUs \$} \subsetneq \{\text{Dominis GCD}\} \subsetneq \{\text{Dominis}\}\,. \tag{4.2}$$

Seria raonable preguntar-se on queden els dominis de Bézout respecte de la cadena anterior. En aquesta secció, veurem que es verifiquen les inclusions estrictes:

$$\{\text{DIPs}\} \subsetneq \{\text{dominis de Bézout}\} \subsetneq \{\text{dominis GCD}\}\,. \tag{4.3}$$

Però, no obstant:

$$\{\text{dominis de Bézout}\} \nsubseteq \{\text{DFUs}\}\, i\, \{\text{DFUs}\} \nsubseteq \{\text{dominis de Bézout}\}\,.$$

Per tant, els dominis de Bézout no es poden incloure en la cadena (4.2).

Que els DIPs són dominis de Bézout és conseqüència directa de la Proposició 3.3.5. A més, per definició, els dominis de Bézout són dominis GCD. Per tant, de la cadena (4.3), només resta veure que les inclusions són estrictes.

Vegem primer un exemple de domini GCD que no és domini de Bézout, que també prova que $\{\text{DFUs}\} \nsubseteq \{\text{dominis de Bézout}\}$.

Exemple 4.6.1. Considerem l'anell de polinomis en dues variables x, y, sobre l'anell dels enters, $\mathbb{Z}[x, y]$. Com $\mathbb{Z}$ és factorial, pel Teorema 4.4.1, sabem que $\mathbb{Z}[x, y]$ és també factorial. Per tant, en particular, pel Corol·lari 3.4.15, és també un domini GCD. No obstant, no és un domini de Bézout. En efecte, a l'Exercici 3.3.7, s'ha comprovat que 1 és el màxim comú divisor de x i y en $\mathbb{Z}[x, y]$ i, l'equació de Bézout:

$$1 = ax + by,$$

no té solució en $\mathbb{Z}[x, y]$. És a dir, $\mathbb{Z}[x, y]$ és un domini GCD i DFU que no és domini de Bézout.

Així, tan sols resta veure que el recíproc de la implicació DIP $\Longrightarrow$ domini de Bézout, no és cert en general, i que $\{\text{dominis de Bézout}\} \nsubseteq \{\text{DFUs}\}$. Però, de fet, això ja ho hem vist. En efecte, a l'Exemple 4.3.1 hem estudiat un domini domini de Bézout (i, en particular, GCD) que no és DFU (ni, en particular, DIP).

L'Exemple 4.3.1 resulta molt útil per als objectius d'aquest treball. No obtant, es tracta d'un anell un pèl artificial. Un exemple més natural de domini de Bézout que no és DFU és l'anell de les funcions enteres. Recordem:

Definició 4.6.2. Una funció $f : D \subseteq \mathbb{C} \longrightarrow \mathbb{C}$ és anomenada *holomorfa en el domini* D si f és diferenciable (en el sentit complex) en tot punt de D. El conjunt format per les funcions holomorfes en D es denota per $\mathcal{O}(D)$.

Definició 4.6.3. Diem que una aplicació $f : \mathbb{C} \longrightarrow \mathbb{C}$ és *entera* si f és holomorfa en tot $\mathbb{C}$, és a dir, si $f \in \mathcal{O}(\mathbb{C})$.

Observació 4.6.4. Es comprova que, amb el producte i la suma puntuals, $\mathcal{O}(\mathbb{C})$ és un anell commutatiu i unitari. Els elements invertibles en $\mathcal{O}(\mathbb{C})$ són les funcions $f \in \mathcal{O}(\mathbb{C})$ que no s'anul·len en cap punt.

Així, l'anell de les funcions enteres és precisament $\mathcal{O}(\mathbb{C})$. Aquest anell va ser àmpliament estudiat per O.Helmer en [6]. En 1940, O.Helmer va provar en [6] que tot ideal finitament generat en $\mathcal{O}(\mathbb{C})$ és principal. Per tant, per la Proposició 3.3.5, $\mathcal{O}(\mathbb{C})$ és un domini de Bézout i, en particular, un domini GCD. No obstant, no és un DFU. En efecte, en un DFU tot element diferent de zero té necessàriament un nombre finit de divisors primers, i $\mathcal{O}(\mathbb{C})$ no verifica aquesta condició. D'una banda, es comprova que els elements primers de A són exactament les funcions afins, $f(z) = z - a$. D'altra banda, la funció $f(z) = \sin z$ té infinits divisors primers: $z - k\pi$, $k \in \mathbb{Z}$. No obstant, els detalls i demostracions d'aquest exemple queden fora de l'abast d'aquest treball. Si el lector està interessat es recomanen les referències [6] i [7].

Vegem, finalment, que els dominis de Bézout, tot i no ser DIPs en general, si verifiquen alguna de les condicions: factorització única, Noetheriana o bé la CCA en el conjunt dels ideals principals, aleshores necessàriament són DIPs. És més:

Proposició 4.6.5. *Sigui A un domini de Bézout. Aleshores són equivalents:*

(i) A és Noetherià;

(ii) A és un DIP;

(iii) A és un DFU;

(iv) A verifica la CCA en el conjunt dels ideals principals.

Demostració. (i) $\Longrightarrow$ (ii). Per ser A Noetherià tot ideal de A és finitament generat. Aleshores, com A és un domini de Bézout, per la Proposició 3.3.5, tot ideal de A és principal.
(ii) $\Longrightarrow$ (iii). Vist al Teorema 3.6.9.
(iii) $\Longrightarrow$ (iv). Vist al Teorema 3.5.3.
(iv) $\Longrightarrow$ (i). Volem veure que tot ideal de A és finitament generat. Suposem que existeix un ideal $I \in A$ que no pot ser finitament generat. Prenem $x_0 \in I$, tal que $I \setminus (x_0) \neq \varnothing$, que sabem que existeix ja que I no és finitament generat. Prenem ara, $x_1 \in I \setminus (x_0)$, tal que $I \setminus (x_0) \neq \varnothing$. Per ser A un domini de Bézout, tenim que $\langle x_0, x_1 \rangle$ és un ideal principal. Sigui $a_1 \in A$ tal que $\langle x_0, x_1 \rangle = (a_1)$. És clar que $(x_0) \subsetneq \langle x_0, x_1 \rangle = (a_1)$. Recursivament, obtenim $(x_i)_{i \geq 0}$, amb $x_i \in I \setminus \langle x_0, \ldots, x_{i-1} \rangle \neq \varnothing$, i $(a_i)_{i \geq 1}$ amb $(a_i) = \langle x_0, \ldots, x_i \rangle$. De forma que la cadena d'ideals principals

$$(x_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$$

no estabilitza, fet que suposa una contradicció amb la hipòtesis. □

Capítol 5

Conclusions i treball futur

L'objectiu general d'aquest treball és l'estudi dels anells commutatius i, especialment, els domínis íntegres. Resumint, els punts que hem tractat són:

1. *L'estudi de condicions de finitud en anells commutatius.* En particular, l'estudi de les condicions de cadena ascendent i descendent, i d'element maximal i minimal, així com de diverses propietats que s'en deriven.

2. *L'estudi de la teoria de la divisibilitat en dominis.* En particular, de les condicions: existència de màxims comuns divisors i/o mínims comuns múltiples, existència de solucions per a l'equació de Bézout, existència de factorització única, condició d'element primer, existència de norma de Dedekind-Hasse, condició que tot ideal sigui principal, i existència de norma Euclidiana.

3. *L'anàlisi de les relacions existents entre les condicions esmentades en els punts anteriors.* Hem definit els anells Noetherians, Artinians, dominis, dominis GCD, dominis de Bézout, DFUs, DIPs i dominis Euclidians. Demostrant, tal i com es volia, que:

$$A \text{ Artinià} \iff A \text{ Noetherià i } \dim(\mathrm{A}) = 0. \tag{5.1}$$

$$A \text{ Euclidià} \implies A \text{ DIP} \implies A \text{ DFU} \implies A \text{ domini GCD} \implies A \text{ domini.} \tag{5.2}$$

$$\begin{array}{ccc} A \text{ DIP} & \implies & A \text{ domini de Bézout} \\ \Downarrow & & \Downarrow \\ A \text{ DFU} & \implies & A \text{ domini GCD} \end{array} \tag{5.3}$$

així com altres caracteritzacions interessants, d'entre les quals destaquem:

$$\text{A DFU} \iff A \text{ verifica la CEP i la CCA en els ideals principals.} \tag{5.4}$$

$$A \text{ té norma de Dedekind-Hasse} \iff A \text{ DIP} \iff A \text{ DFU i } \dim(A) \leq 1. \tag{5.5}$$

$$A \text{ DIP} \iff A \text{ domini de Bézout i Noetherià} \iff A \text{ domini de Bézout i DFU} \iff \iff A \text{ Bézout i CCA en els ideals principals} \tag{5.6}$$

4. *La presentació i anàlisi de contraexemples de totes les implicacions en* (5.2) i (5.3). Donem, també, un exemple de domini de Bézout que no és DFU, i d'un domini DFU que no és de Bézout. Provant, així, que els dominis de Bézout no es poden incloure en la cadena d'implicacions (5.2).

Alguns punts que no s'han pogut abordar en aquest treball i que romanen com a possible treball futur són:

- L'estudi de l'anell de les funcions enteres, i l'anell dels nombres enters algebraics, com a exemples més naturals de dominis de Bézout no DFU.
- Aprofundir en la qüestió de la factoriabilitat.

Bibliografia

[1] P. Aluffi. *Algebra : chapter 0*. Graduate studies in mathematics. Providence, R.I. : American Mathematical Society, 2005.

[2] M.F. Atiyah i I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley series in mathematics. Publisher, 1969.

[3] O. A. Cámpoli. "A Principal Ideal Domain that is not a Euclidean Domain". A: *The American Mathematical Monthly,* 95.9 (1988), pàg. 868 - 871.

[4] A. Dorn. *The Elegant Way To Generate The Complex Number Field*. URL: `http://adriandorn.com/math/complex.htm`. (accedit: 15.3.2020).

[5] D. S. Dummit i R. M. Foote. *Abstract algebra*. Englewood Cliffs, N.J.: Prentice Hall, 1991.

[6] O. Helmer. "Divisibility properties of integral functions". A: *Duke Math. J.* 6.2 (1940), pàg. 345 - 356.

[7] M. Henrikssen. "On the ideal structure of the ring of entire functions". A: *Pacific J. Math.* 2.2 (1952), pàg. 179 - 184.

[8] B. Ikenaga. *Polinomial Rings*. URL: `http://sites.millersville.edu/bikenaga/abstract-algebra-1/polynomial-rings/polynomial-rings.html`. (accedit: 10.06.2020).

[9] N. Gubareni M. Hazewinkel i V.K. Kirichenco. *Algebras, Rings and Modules, volume 1*. Mathematics and Its Applications. Kluwer Academic Publishers, 2009.

[10] T. Motzkin. "The Euclidean Algorithm". A: *Bull. Amer. Math. Soc.* 55.1 (1949), pàg. 1142 - 1146.

[11] K. Pollock. *A Brief History of Ring Theory*. URL: `https://pdfs.semanticscholar.org/98f7/ba2cdd6987ffb441cc2eaed4e9619946ac07.pdf`. (accedit: 10.6.2020).

[12] *Ring (mathematics)*. URL: `https://en.wikipedia.org/wiki/Ring_(mathematics)#Basic_examples`. (accedit: 25.2.2020).

[13] *The division algorithm for N and Z*. URL: `https://www.math.wustl.edu/~freiwald/310divalgorithm.pdf`. (accedit: 10.06.2020).

[14] C. Wong. "On a Principal Ideal Domain that is not a Euclidean Domain". A: *International Mathematical Forum* 8.29 (2003), pàg. 1405 - 1412.