Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Tesis de Licenciatura

Otro dominio principal que no es un dominio euclídeo

Nicolás Allo Gómez

Directora: Teresa Krick

Junio de 2024

Agradecimientos

Sin duda alguna no hubiese podido llegar hasta aquí sin el apoyo de toda la gente tan increíble que tuve y tengo en mi vida. Quisiera no olvidarme de nombrar a nadie en esta lista, pero pido disculpas anticipadamente porque probablemente eso ocurra.

A Alexis, por llegar a mi vida de forma tan inesperada y hacerme muy feliz desde ese momento. Por nuestras charlas, tus consejos, tu infinita paciencia y tu comprensión. Por confiar siempre en mí y en mi capacidad, incluso a veces más que yo mismo. Por compartir tantas alegrías conmigo, por festejar mis logros y emocionarte cada vez que te cuento algo lindo que me pasa. Por esa virtud que tenés de verle el lado positivo a todo. Sin tu apoyo me hubiese sido imposible darle un cierre a esto. Te amo.

A mi madrina Gaby, por estar siempre para mí y acompañarme. Por enseñarme tantas cosas, por tantos consejos a lo largo de mi vida y, por sobre todo, por siempre quererme incondicionalmente como soy. Desearía que todos tuvieran una madrina tan increíble, loca, divertida y buena como vos.

A mi abuela Marysol y a mi *abuelito* Héctor, por ser un ejemplo de amor y cariño desde que tengo memoria. Por ser los abuelos más comprensivos del mundo, y por ser siempre de mente tan abierta y de espíritu tan joven. Por enseñarme que la edad es solo un número anecdótico, y por todas las charlas que hemos tenido en la playa y en la casa de los abuelos. Voy a estar eternamente agradecido por haberme dado una familia del corazón tan linda.

A mi hermano Fede, por ser una de las personas más importantes en mi vida. Por escucharme, aconsejarme y hacerme entrar en razón muchas veces, y por tus esporádicos "te quiero bro".

A mi *aunt* Lily, por motivarme a estudiar desde chiquito y por fomentar la idea de que aprender es algo lindo y no solo una responsabilidad. Por interesarte junto al tío Jimmy cada vez que vienen a la Argentina por cómo voy con el estudio, y por tus mensajitos ante cada uno de mis logros. Por regalarme mi primera biblia del Álgebra (*Modern Computer Algebra*).

A mis primos Mati, Yani y Flo y a mis tíos Lili y Jorge, por todos los findes en lo del abuelo José y los recuerdos tan lindos de esos años.

A mis viejos, por apoyarme y estar siempre presentes. Por contribuir a mi formación incluso cuando la situación económica en casa fue difícil. Por respetarme y entenderme pese a pensar muy distinto en tantas cosas. Gracias especialmente por haberme enseñado a ser fiel a lo que siento y a defender lo que pienso.

A Caro Fort, por ser amigos desde tan chiquitos y estar siempre tan presente en todo en mi vida. Por ser como mi hermana y ser mi cable a tierra tantas veces. Por apoyarme en todo, por ponerte tan feliz cada vez que te cuento algo bueno que me pasa y también por emocionarte a la par mío tantas otras veces. Por retarme y hacerme ver las cosas desde otra perspectiva en muchas ocasiones. Por entenderme y comprenderme con solo mirarme, por tantas risas (sobre todo después de la una) y también por conocerme como casi nadie me conoce. Por haberme ido a buscar a una plaza un día que estaba harto de todo y me senté en el pasto a llorar. Por tantas charlas sobre nuestra vida, nuestros sueños y nuestro futuro. Sin tu apoyo no estaría hoy acá terminando esta tesis.

A Lari, por ser una amiga con la que siempre puedo debatir lo que sea (hasta casi matarnos si hace falta) pero decirnos al ratito un "te quiero" y seguir como si nada. Por tantas charlas que hemos tenido desde la época del colegio. Por estar siempre presente y disponible a cualquier hora para que te cuente lo que sea para luego darme algún consejo contundente y preciso. Por haber sido mi compañera de coro a la que le hice bullying tantas veces y que, como corresponde, me mandaste a cagar tantas otras. Por habernos entrenado a mí y a Jess para sobrevivir a lo que sea durante nuestro primer viaje juntos a la costa en 2011. Por haber compartido conmigo también el CBC de Económicas, y que al verme tan fascinado cursando análisis matemático me terminaste acompañando a cambiarme de carrera.

A Jess, por escucharme siempre cuando les cuento algo y darme tu opinión seguida de un "amii" que descontractura todo y me hace reír tanto. Por los viajecitos que compartimos y por las anécdotas tan graciosas que quedaron. Por ser mi compañera fiel que toma Fernet, por tu carrera icónica como imitadora de Patito Feo y por tu habilidad para adivinar el futuro usando las cartas del Uno. Te admiro muchísimo por cómo te la jugaste para irte a la otra punta del mundo porque sentiste que era lo que te haría feliz... pero obviamente por ello te extraño un montón.

A Xime, por estar tan loca como yo y ser una de las personas más lindas que me dio la Facultad. Por volverte prácticamente mi hermana, por llorar y reír conmigo tantas veces, por pelearnos y amigarnos como nenes chiquitos, por conocerme tanto y por estar siempre para mí (incluso a la distancia). Nunca nada va a superar las salidas a comprar un Blem y un Nesquik a la 4 a.m. Por haberme elegido de testigo para tu casamiento con Euge, y también por el mes hermoso que compartimos juntos en UK.

A Euge, por ser un amigo que dice poco pero siempre dice la posta. Por ser de las personas más inteligentes que tuve la suerte de conocer, y que siempre que necesité ayuda con algo lo pensaste a la par conmigo, pero siempre desde la más absoluta humildad. Por los debates de política, de Historia, de Economía, de la vida misma...

A Maga de Magalás, porque a pesar de ser la amistad más perjudicial que puede existir nos seguimos eligiendo. Por tantas películas de terror pésimas que vimos, por aguantar mis crisis Comaneci, por nuestras discusiones acaloradas pero que siempre terminan en "igual soy team MagaLás". Por hacer que ese cuatrimestre fatídico en que dábamos clase de 8 a 23 fuese tan divertido y lleno de recuerdos tan lindos. Sin tu apoyo, tus consejos y nuestras llamadas hasta las 5 a.m. no habría llegado hasta acá (*aunque biológicamente...*).

A Isa, por haberme hablado por primera vez de los polinomios en varias variables. Por haber sido una de las mejores docentes que tuve y de quien aprendí mucho. Por haber aceptado mi decisión de ser tu amigo cuando te tuve en Álgebra Lineal, y por haber sido una gran amiga desde ese momento. Me pone muy feliz haberte presentado a Juli y verte hoy disfrutando siendo mamá de Lu.

A Tere, como profesora, como directora y como amiga. Como profesora, por haberme reconectado con la Matemática en esa cursada tan maravillosa de Álgebra II (y luego de Álgebra III), por tu forma de ver y transmitir la Matemática y la dedicación que le ponés a tus clases, y también por tus fulminantes "pero a ver, tesoro..." cuando he dicho alguna burrada. Como directora, por tu infinita paciencia y correcciones, por la buena onda cada vez que nos reunimos y por pensar a la par conmigo cada detalle de este trabajo. Como amiga, por ser una de las mejores personas que conocí en Exactas. Por las charlas tan lindas de Matemática, de política y de skincare (entre muchos otros temas, algunos mucho más emotivos), por tus consejos y por ayudarme en proyectos muy importantes para mí como fue el de traer a Emilce Moler a la Facultad.

A Pablo Azcue, por haber sido un mentor para mí. Por enseñarme tanto de docencia, de Matemática y, sobre todo, de compañerismo y calidad humana. Por haberme dado tantas oportunidades y valorar siempre mi trabajo y mi esfuerzo. Por recomendarme en tantos lugares y permitirme trabajar tan cómodo en UTDT. Esta tesis va dedicada especialmente a vos.

A Romi, Anto y Vicky, por ser una parte fundamental de que disfrute tanto dar clase en UTDT. Por volverse amigas con las que puedo compartir risas, cansancio y hasta momentos tan duros como el que ocurrió este año. Gracias especialmente a Anto por haber valorado mi forma de trabajar desde el primer día, por compartir tantos alfajores de nuez y café conmigo, y por todas esas charlas "entre nosotros" y todos tus consejos.

A Ceci, por las cursadas que compartimos, las selfies juntos, el perreo en la Bresh, la Ceci Dory, las UMAs (con mi agua termal) y el ENA. Por las crisis de estudio, los llantos en el DM y preparar concursos juntos. Por tantas charlas y consejos mutuos, y por tus abrazos cuando los necesité.

A Juja, por haberte hecho mi amiga después de haber empezado tan mal nuestra relación. Por tantas tardes de estudio compartidas, tantas risas en esos momentos y tantos audios (y selfies) en crisis, y también por las fotos de Jaime siendo feliz mientras nosotros no dábamos más de la ansiedad. Por ese abrazo que nos dimos al rendir el último final juntos. Por los cafecitos que compartimos y los que vendrán. Por ser *el team*. Por abrirte a hablar de tantas cosas e intercambiar opiniones y consejos. Sin vos hubiese sido imposible terminar esta etapa.

A Marcos, siempre y cuando no divida por cero otra vez. Por tantas cursadas juntos, por tantos mates, y por esos momentos de hartazgo donde solo se podía decir "¿ya merito?". Por ser el creador oficial de mis memes. Por tantas charlas sobre lo difícil que fue estudiar y laburar tanto, y por aguantarme llorando antes de rendir los parciales.

A Juani Piombo, por ser tan insoportable como querible. Por bautizarme como *el coloradito*, por recordarme que separé mal la palabra "constante" en el parcial de Avanzado, y por descansarme por no saber la diferencia entre Lanús y Banfield. Por ser Helga y Arnold, querido Juani.

A todas las personas con las que cursé y que hicieron mucho más divertido no entender casi nada por momentos: Ceci, Marcos, Max, Cristian, Martín, Sol, Gabimon, Clari, Leila, Joaco L., Juja, Georgi, Emi y seguro me estoy olvidando de muchos otros (¡perdón!).

A todos los profes increíbles que tuve a lo largo de los años, especialmente a aquellos que no solo me enseñaron los contenidos correspondientes a su materia sino que lo hicieron con una pasión extraordinaria. Quiero destacar especialmente en esto a Tere, a Alicia Dickenstein, a Pablo Ámster, a Dano Perrucci y a Mariano Suárez-Álvarez. También quiero agradecer a los ayudantes y compañeros auxiliares que tuve y que luego muchos se volvieron amigos, entre ellos especialmente a Caro Mosquera, Dani Cuesta, Diana Carbajal, Isa Herrero, Ro Balderrama y Ale Nasif.

A mis teachers del colegio Ms. Liz y Ms. Regina. Fueron una parte indispensable en mi formación académica y humana, y siempre voy a estar agradecido por el espacio que me brindaron para expresarme. Gracias a ustedes descubrí lo fundamental que puede ser un docente en la vida de un estudiante.

A mi profesora del colegio Graciela Brizio, por incentivarme a siempre dar lo mejor de mí y por ser quien me permitió empezar con la docencia. Quiero agradecer también a mi profesora del colegio Rina Fernández, por transmitirme su pasión por la Matemática y por traerme un acertijo de Adrián Paenza (y Juan Sabia) que me permitió descubrir que la Matemática no es solo hacer cuentas.

A todos mis compañeros docentes en UTDT, por tantos almuerzos y asados de fin de año. Por los debates, charlas y muchísimas horas de corrección de exámenes. Quiero destacar especialmente a Andre Olivo, Pato, Romi, Vicky, Pau K., Isa, Mariano M., Román, Damián, Maxi y Martín VV. Quiero agradecer también a todo el equipo del MiM por permitirme ser uno más del equipo y por la buena onda con la que siempre trabajamos.

A Juan y Dano, por haber aceptado ser jurados de esta tesis. Por sus correcciones, sugerencias y sus comentarios tan positivos sobre este trabajo.

A todos los que estuvieron presentes el día de la defensa de esta tesis. Les agradezco mucho haber compartido ese momento tan especial conmigo.

A la educación pública y, en especial, a la Universidad de Buenos Aires, sobre todo en este difícil momento. Me hubiese sido imposible llegar hasta acá si hubiese tenido que pagar para poder estudiar.

Índice general

Introducción

Uno de los teoremas más famosos de la historia es el Último Teorema de Fermat (UTF). Desde que el abogado-matemático Pierre de Fermat lo enunció en el margen de una hoja en el año 1637 con la leyenda "he encontrado una demostración verdaderamente maravillosa de esta proposición, pero este margen es demasiado estrecho para contenerla", el mismo despertó una cantidad desmedida de emociones muy diversas en los matemáticos durante siglos.

La historia del UTF es alucinante por donde se la mire y gira alrededor de una supuesta demostración no exhibida. Sin embargo, el UTF representó un verdadero cisma en la Matemática. El poder de una demostración radica en que una vez probado el valor de verdad de una proposición a partir de una serie de axiomas y de un proceso lógico-deductivo, tal valor de verdad durará hasta el final de los tiempos. Fue por eso que numerosos matemáticos intentaron demostrar la entonces Conjetura de Fermat durante tantos años, convencidos de que la misma era cierta. Sin embargo, y pese a los muchos avances obtenidos en ello, los esfuerzos nunca eran suficientes para probar todos los casos.

En el afán de demostrar el teorema, diversos matemáticos dieron pruebas para casos particulares del mismo. Entre ellos se pueden mencionar a Leonhard Euler, Sophie Germain, Adrien-Marie Legendre, Gabriel Lamé, Ernst Kummer y Lejeune Dirichlet. No obstante, sería el matemático inglés Andrew Wiles quien pondría fin al misterio al presentar una demostración irrefutable del UTF en 1995.

A lo largo de los diversos intentos por demostrarlo, el matemático Gabriel Lamé creyó haberlo logrado hasta que Ernst Kummer notó un error fatal en la supuesta prueba de Lamé: el uso de la unicidad de factorización en irreducibles en anillos numéricos. El error de Lamé se debió al hecho de asumir que cualquier anillo numérico tiene propiedades análogas a las de los números enteros.

Actualmente, en cualquier curso donde se aborde el estudio de estructuras algebraicas, se estudian las nociones de factorización en irreducibles, máximo común divisor de dos elementos no nulos y la existencia de algoritmos que permitan su cálculo.

Siguiendo esta línea de estudio y previo a abordar la demostración de dos casos particulares del UTF, en una materia optativa me presentaron un ejemplo de un llamado *Dominio Principal que no es un Dominio Euclídeo*. El UTF y su impacto en el desarrollo moderno de la Teoría de Números me parecieron fascinantes desde un primer momento, pero las demostraciones vinculadas a ese ejemplo me resultaron poco naturales en comparación a los otros ejemplos y contraejemplos estudiados previamente en ese mis-

mo eje temático.

Luego de un tiempo encontré un ejemplo distinto en internet pero sin referencia alguna a una prueba, por lo que su veracidad era incluso incierta. Finalmente encontré una publicación en [mat14] con un esbozo de demostración que aún no me resultaba del todo satisfactoria, por lo que me propuse desarrollar una demostración por mi cuenta y abordarla conjuntamente con algunas de las ideas presentes en tal publicación y con ideas propias. Para ello recurrí a la teoría de resultantes y a los conocimientos adquiridos en materias como Álgebra II y Álgebra III.

Esta tesis busca organizar los conceptos conocidos pero imprescindibles para que todo sea autocontenido y también apunta a presentar algunos resultados necesarios menos conocidos para finalmente exhibir este ejemplo de *Otro Dominio Principal que no es un Dominio Euclídeo* y dar una prueba de ello.

Damos a continuación un breve detalle acerca de cómo está organizada esta tesis.

El enfoque con el que abordaremos los primeros cuatro capítulos de este trabajo corresponde en parte al que generalmente se sigue en cualquier curso de estructuras algebraicas (cf. [DF04], [Lan02], [Rot23], [SK90], [ST01], entre otros).

En el Capítulo 1 se podrán encontrar resultados preliminares acerca de la teoría de anillos conmutativos, dominios íntegros y elementos irreducibles y primos. La idea es que el lector tenga presentes todas las definiciones y resultados que figuran allí ya que serán utilizados a lo largo de todo este trabajo.

En el Capítulo 2 abordaremos como tema central la factorización de elementos en un dominio íntegro como producto de irreducibles y las propiedades que resultan análogas a las conocidas para los anillos $\mathbb{Z}$ y $\mathbb{K}[X]$ con $\mathbb{K}$ cuerpo. Aquí veremos ejemplos de dominios donde la factorización en irreducibles no es única, o incluso no es posible. A su vez, estudiaremos resultados que permitan garantizar la existencia de factorización y su unicidad. Además, analizaremos cuándo es posible asegurar la existencia de un máximo común divisor dados dos elementos no ambos nulos en un dominio íntegro y, en tal caso, qué propiedades tiene en contraste con las que se conocen en los dos anillos mencionados anteriormente.

En el Capítulo 3 daremos las definiciones de Dominio Principal y Dominio Euclídeo, las cuales resultan muy naturales cuando se busca generalizar dos propiedades fundamentales del máximo común divisor a anillos que no sean necesariamente el de los números enteros $\mathbb{Z}$: la escritura del máximo común divisor entre dos elementos no ambos nulos como combinación de los mismos (con coeficientes en el anillo) y la existencia de un algoritmo que permita calcularlo de forma similar al de Euclides conocido para $\mathbb{Z}$. Aquí introduciremos el problema que motiva esta tesis: la relación entre los conceptos de Dominio Euclídeo, Dominio Principal y la existencia y unicidad de factorización.

En el Capítulo 4 trabajaremos con anillos de polinomios, sus propiedades y la existencia y unicidad de factorización como producto de polinomios irreducibles. En este capítulo recordaremos definiciones y resultados básicos sin demostración, pero también enunciaremos y probaremos otros resultados menos clásicos que serán necesarios

en el último capítulo de esta tesis. Aquí exhibiremos también algunos ejemplos que ayudarán a responder algunas de las preguntas abordadas en los capítulos anteriores. Finalizaremos este capítulo introduciendo el concepto de Resultante de dos polinomios univariados y sus propiedades más relevantes.

Finalmente, en el Capítulo 5 exhibiremos el ejemplo que motiva este trabajo y procederemos a enunciar y probar los resultados necesarios con algunas demostraciones de autoría propia para concluir que efectivamente se trata de *Otro Dominio Principal que no es un Dominio Euclídeo*.

Capítulo 1

Preliminares

En esta sección fijaremos algunas nociones generales que usaremos en el trabajo.

Siempre que utilicemos $\mathbb{K}$ nos referiremos a un cuerpo arbitrario y siempre que consideremos un anillo A será con elemento neutro para el producto $1 \neq 0$. Además, asumiremos como ejemplos conocidos el anillo de números enteros $\mathbb{Z}$ y al anillo de polinomios $\mathbb{K}[X]$.

En esta tesis se trabajará principalmente con el anillo de polinomios $\mathbb{R}[X, Y]$ y uno de sus cocientes.

1.1. Anillos

Definición 1.1.1. Sea A un anillo conmutativo. Un ideal I de A es un subconjunto $I \subseteq A$ que cumple simultáneamente:

- $0 \in I$,
- $x, y \in I \Longrightarrow x + y \in I$,
- $x \in I$ y $a \in A \Longrightarrow a \cdot x \in I$.

Si I es un ideal de A se denota $I \trianglelefteq A$.

Definición 1.1.2. Sean A un anillo conmutativo y un subconjunto $\mathcal{X} \subseteq A$. El ideal de A generado por $\mathcal{X}$ es el menor ideal (con respecto a la inclusión) que contiene a $\mathcal{X}$ y se denota $\langle \mathcal{X} \rangle$. Esto es: $\langle \mathcal{X} \rangle = \bigcap_{\mathcal{X} \subseteq I \trianglelefteq A} I = \left\{ \sum_{i=1}^{r} a_i \cdot x_i \ : \ r \in \mathbb{N}, a_i \in A, x_i \in \mathcal{X} \right\}$.

Definición 1.1.3. Sea A un anillo conmutativo. Decimos que el ideal $I \trianglelefteq A$ es finitamente generado si existe un conjunto finito $\mathcal{X} = \{x_1, \ldots, x_k\} \subseteq A$ tal que $I = \langle \mathcal{X} \rangle$ y se suele denotar $I = \langle x_1, \ldots, x_k \rangle$.

Si existe un elemento $x \in A$ tal que $I = \langle x \rangle$ decimos que el ideal I es principal.

Definición 1.1.4. Sea A un anillo conmutativo y sean $I, J \trianglelefteq A$. Se definen:

1. $I \cap J = \{x \in A : x \in I \ , \ x \in J\} \trianglelefteq A$,
2. $I + J = \{x + y : x \in I \ , \ y \in J\} \trianglelefteq A$,
3. $IJ = \langle x \cdot y : x \in I \ , \ y \in J \rangle \trianglelefteq A$,

y se tiene que $IJ \subseteq I \cap J \subseteq I, J \subseteq I + J$.

Definición 1.1.5. Sea A un anillo conmutativo y sea $I \subsetneq A$ un ideal propio de A.

1. El ideal I se dice primo si $\forall\, a, b \in A, a \cdot b \in I \Longrightarrow a \in I \quad$ ó $\quad b \in I$.
2. El ideal I se dice maximal si $\forall\, J \trianglelefteq A, I \subsetneq J \Longrightarrow J = A$.

Definición 1.1.6. Un anillo A se dice un dominio íntegro (o simplemente un dominio) si es conmutativo y dados $a, b \in A$, $a \cdot b = 0 \Longrightarrow a = 0 \quad$ ó $\quad b = 0$.

Definición 1.1.7. Sea A un dominio íntegro.

1. Un elemento $u \in A$ se dice una unidad si existe $s \in A$ tal que $u \cdot s = 1$. En tal caso, decimos que u es inversible y s, que es único, se denomina inverso multiplicativo de u, al cual denotamos $s = u^{-1}$.
   Al conjunto de todas las unidades de A lo denotamos $\mathcal{U}(A)$ (o también $A^{\times}$) y resulta que $\big(\mathcal{U}(A), \cdot\big)$ es un grupo abeliano.
2. Dados $a, b \in A$ decimos que a divide a b (o que b es divisible por a) si existe $c \in A$ tal que $b = a \cdot c$ y en tal caso se denota $a \mid b$.
3. Un elemento $\tilde{a} \in A$ se dice asociado a $a \in A$ si existe $u \in \mathcal{U}(A)$ tal que $\tilde{a} = u \cdot a$ y en tal caso se denota $\tilde{a} \sim a$.

   Notar que:

   - Si $a, b \in A$ tales que $a \mid b \ \text{ y } \ b \mid a$, entonces $a \sim b$,
   - Si $a, b, c \in A$ tales que $a \mid b \ \text{ y } \ b \sim c$, entonces $a \mid c$,
   - $\sim$ es una relación de equivalencia.

4. Si $u \in \mathcal{U}(A)$ y $a \in A$ satisfacen que $a \mid u$, entonces $a \in \mathcal{U}(A)$.
5. Un elemento $q \in A \setminus \{0\}$ se dice irreducible si satisface a la vez:

   - $q \notin \mathcal{U}(A)$,
   - $\forall\, a \in A, \ a \mid q \Longrightarrow a \in \mathcal{U}(A) \quad$ ó $\quad a \sim q$.

6. Un elemento $r \in A \setminus \mathcal{U}(A)$, $r \neq 0$, se dice reducible si no es irreducible, es decir, si existen $a, b \in A \setminus \mathcal{U}(A)$ tales que $r = a \cdot b$, y decimos que esta escritura es una factorización propia de r.

7. Un elemento $p \in A \setminus \{0\}$ se dice primo si satisface a la vez:
   - $p \notin \mathcal{U}(A)$,
   - $\forall\, a, b \in A,\ p \mid a \cdot b \Longrightarrow p \mid a$ ó $p \mid b$.

Definición 1.1.8. Sea A un dominio íntegro. Definimos en $A \times (A \setminus \{0\})$ la relación dada por: $(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$, que resulta una relación de equivalencia.

Definimos el cuerpo de fracciones $\mathrm{Frac}(A)$ como el conjunto de clases de equivalencia inducidas por la relación anterior:

$$\mathrm{Frac}(A) = A \times (A \setminus \{0\}) \Big/ \sim$$

Con las operaciones $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$ y $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$, $\mathrm{Frac}(A)$ resulta un cuerpo.

Denotamos a los elementos de $\mathrm{Frac}(A)$ por $\dfrac{a}{b} := \overline{(a,b)}$ y, en particular, $a := \overline{(a,1)}$ por lo que tenemos una inclusión natural $A \hookrightarrow \mathrm{Frac}(A)$.

Recordamos por último algunos resultados sobre morfismos de anillos, anillos cocientes y su relación con ideales maximales e ideales primos:

Definición 1.1.9. Sean A, B anillos conmutativos. Una función $f : A \longrightarrow B$ se dice un morfismo de anillos si satisface simultáneamente las siguientes condiciones para todos $x, y \in A$:

- $f(x +_A y) = f(x) +_B f(y)$,
- $f(x \cdot_A y) = f(x) \cdot_B f(y)$,
- $f(1_A) = 1_B$.

Para $f : A \longrightarrow B$ morfismo de anillos se definen:

1. $\mathrm{Ker}(f) = \{x \in A \ :\ f(x) = 0\} \subseteq A$ el núcleo de f, que resulta un ideal de A.
2. $\mathrm{Im}(f) = \{f(a) \ :\ a \in A\} \subseteq B$ la imagen de f, que resulta un subanillo de B.
3. Si $J \trianglelefteq B$, $f^{-1}(J) = \{x \in A \ :\ f(x) \in J\}$ es la preimagen por f de J, y resulta un ideal de A.
4. Si $I \trianglelefteq A$, $f(I) = \{f(x) :\ x \in I\}$ es la imagen por f de I, y resulta un ideal de $\mathrm{Im}(f)$.

Definición 1.1.10. Sean A, B anillos conmutativos y sea $f : A \longrightarrow B$ un morfismo de anillos. Entonces,

1. f se dice un monomorfismo si $\mathrm{Ker}(f) = 0$.
2. f se dice un epimorfismo si $\mathrm{Im}(f) = B$.
3. f se dice un isomorfismo si es monomorfismo y epimorfismo. En tal caso, los anillos A y B se dicen isomorfos y se denota $A \simeq B$.

Proposición 1.1.11. *Sean A, B anillos conmutativos y sea $f : A \longrightarrow B$ un morfismo de anillos. Entonces, se tiene la correspondencia:*

$$\begin{array}{rcl} \{I \trianglelefteq A : \mathrm{Ker}(f) \subseteq I\} & \longleftrightarrow & \{J \trianglelefteq \mathrm{Im}(f)\} \\ I & \longrightarrow & f(I) \\ f^{-1}(J) & \longleftarrow & J \end{array}$$

Definición 1.1.12. Sea A un anillo conmutativo y sea $I \trianglelefteq A$. Definimos en A la relación dada por: $a \sim b \iff a - b \in I$, que resulta una relación de equivalencia.

Definimos el anillo cociente A/I como el conjunto de clases de equivalencia inducidas por la relación anterior:

$$A/I = A/\sim$$

Con las operaciones $\overline{a} + \overline{b} = \overline{a+b}$ y $\overline{a} \cdot \overline{b} = \overline{ab}$, A/I resulta un anillo conmutativo con unidad $\overline{1}$. Se tiene además la proyección al cociente $\pi_I : A \longrightarrow A/I$ definida por $\pi_I(a) = \overline{a}$ que resulta un epimorfismo de anillos con $\mathrm{Ker}(\pi_I) = I$.

Teorema 1.1.13 (Primer teorema de isomorfismo de Noether)**.** *Sean A, B anillos conmutativos y sea $f : A \longrightarrow B$ un morfismo de anillos. Entonces, $A/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.*

Proposición 1.1.14. *Sean A un anillo conmutativo e $I \trianglelefteq A$ y consideremos la proyección al cociente $\pi_I : A \longrightarrow A/I$. En virtud de la proposición 1.1.11 y del primer teorema de isomorfismo 1.1.13 se tiene que la función*

$$\begin{array}{rcl} \phi : \{J \trianglelefteq A : I \subseteq J\} & \longrightarrow & \left\{\overline{J} \trianglelefteq A/I\right\} \\ J & \longrightarrow & \pi_I(J) =: J/I \end{array}$$

es biyectiva. En particular, todo ideal de A/I es de la forma J/I para algún $J \trianglelefteq A$ con $I \subseteq J$. Además, esta correspondencia preserva ideales primos y maximales (que contienen a I).

Teorema 1.1.15 (Segundo teorema de isomorfismo de Noether)**.** *Sea A un anillo conmutativo. Si $I, J \trianglelefteq A$ con $I \subseteq J$, entonces $\frac{A/I}{J/I} \simeq A/J$.*

Proposición 1.1.16. *Sea A un anillo conmutativo y sea $I \subsetneq A$ un ideal propio de A. Entonces,*

1. *I es primo $\iff A/I$ es un dominio íntegro.*
2. *I es maximal $\iff A/I$ es un cuerpo.*
3. *I maximal $\Rightarrow$ I primo.*

Definición 1.1.17. Sea $(\mathcal{X}, \preceq)$ un conjunto parcialmente ordenado.

1. Si $A \subseteq \mathcal{X}$, un elemento $t \in \mathcal{X}$ se dice una cota superior de A si $\forall\, a \in A,\ a \preceq t$.
2. Un elemento $x \in \mathcal{X}$ se dice maximal si $\forall\, y \in \mathcal{X}, x \preceq y \Rightarrow x = y$.
3. Un conjunto $\mathcal{C} \subseteq \mathcal{X}$ se dice una cadena si $\mathcal{C}$ resulta un conjunto totalmente ordenado con respecto al orden inducido de $(\mathcal{X}, \preceq)$.

Lema 1.1.18 (Lema de Zorn)**.** *Sea $(\mathcal{X}, \preceq)$ un conjunto no vacío parcialmente ordenado tal que toda cadena $\mathcal{C} \subseteq \mathcal{X}$ tiene una cota superior. Entonces, $\mathcal{X}$ posee un elemento maximal. (El Lema de Zorn es equivalente al Axioma de Elección, el cual asumiremos como válido).*

Teorema 1.1.19 (Krull)**.** *Sea A un anillo conmutativo. Si I es un ideal propio de A, entonces existe $\mathcal{M}$ ideal maximal de A tal que $I \subseteq \mathcal{M}$.*

1.2. Cuerpos

Recordamos a continuación algunos conceptos y resultados clásicos de la teoría de cuerpos.

Definición 1.2.1. Sean $\mathbb{K}$ y $\mathbb{F}$ cuerpos. Si $\mathbb{K}$ es un subcuerpo de $\mathbb{F}$ decimos que $\mathbb{F}$ es una extensión de $\mathbb{K}$ y lo notamos $\mathbb{F}/\mathbb{K}$.

Observación 1.2.2. Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos. Entonces $\mathbb{F}$ es un $\mathbb{K}$-espacio vectorial.

Definición 1.2.3. Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos.

1. Decimos que el elemento $\alpha \in \mathbb{F}$ es algebraico sobre $\mathbb{K}$ si existe un polinomio $f \in \mathbb{K}[X] \setminus \{0\}$ tal que $f(\alpha) = 0$.
2. La extensión $\mathbb{F}/\mathbb{K}$ se dice algebraica si todo elemento $\alpha \in \mathbb{F}$ es algebraico sobre $\mathbb{K}$.

Definición 1.2.4. Un cuerpo $\mathbb{K}$ se dice algebraicamente cerrado si todo polinomio $f \in \mathbb{K}[X]$ de grado positivo tiene alguna raíz en $\mathbb{K}$.

Definición 1.2.5. Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos. Decimos que $\mathbb{F}$ es una clausura algebraica de $\mathbb{K}$ si $\mathbb{F}$ es algebraicamente cerrado y la extensión $\mathbb{F}/\mathbb{K}$ es algebraica.

Teorema 1.2.6. *Sea $\mathbb{K}$ un cuerpo. Entonces,*

1. *Existe una clausura algebraica de $\mathbb{K}$.*
2. *Dos clausuras algebraicas de $\mathbb{K}$ son $\mathbb{K}$-isomorfas.*

En consecuencia, dado un cuerpo $\mathbb{K}$ denotaremos $\overline{\mathbb{K}}$ a alguna clausura algebraica del mismo. Por último, recordamos que $\overline{\mathbb{R}} \simeq \mathbb{C} = \mathbb{R}[i]$, por lo que su dimensión como $\mathbb{R}$-espacio vectorial es 2.

Capítulo 2

Factorización en Dominios

En este capítulo extenderemos la idea de *factorización en irreducibles* a dominios más generales que $\mathbb{Z}$ y $\mathbb{K}[X]$. Veremos cómo generalizar esto al igual que la noción de máximo común divisor, como así también estudiaremos ciertas condiciones que nos permitan asegurar la existencia de factorización y la unicidad de la misma (con ciertos cuidados). Procederemos a estudiar ciertas propiedades análogas a las conocidas para los dos anillos mencionados anteriormente, y además exhibiremos contraejemplos para ciertos resultados que no son válidos en anillos más generales.

2.1. Dominios de Factorización

Definición 2.1.1. Sea A un anillo. Decimos que A es un Dominio de Factorización (DF) si es un dominio íntegro que además satisface que para todo $a \in A$, $a \neq 0$, $a \notin \mathcal{U}(A)$, existen $r \in \mathbb{N}$ y $q_1, \ldots, q_r \in A$ irreducibles tales que $a = \prod_{j=1}^{r} q_j$. En tal caso, decimos que esa escritura es una factorización en irreducibles de a.

Ejemplo 2.1.2. $\mathbb{K}$, $\mathbb{Z}$ y $\mathbb{K}[X]$ con $\mathbb{K}$ un cuerpo son todos DF.

Observación 2.1.3. No todo dominio íntegro es un DF.

Ejemplo 2.1.4. El anillo $A = \bigcup_{n \in \mathbb{N}_0} \mathbb{C}\left[X^{\frac{1}{2^n}}\right]$ es un dominio íntegro que no es un DF.

Demostración.

Empecemos observando que

$$\mathbb{C}[X] \subseteq \mathbb{C}\left[X^{\frac{1}{2}}\right] \subseteq \mathbb{C}\left[X^{\frac{1}{4}}\right] \subseteq \cdots \subseteq \mathbb{C}\left[X^{\frac{1}{2^n}}\right] \subseteq \mathbb{C}\left[X^{\frac{1}{2^{n+1}}}\right] \subseteq \ldots$$

Luego dados $f, g \in A$ existe $m \in \mathbb{N}_0$ tal que $f, g \in \mathbb{C}\left[X^{\frac{1}{2^m}}\right]$ y allí tiene sentido calcular $f + g$ y $f \cdot g$ de la forma usual, y además se tiene que $f \cdot g = 0$ si y solo si $f = 0$ ó $g = 0$. Así, A resulta un dominio íntegro.

Por otro lado, veamos que $\mathcal{U}(A) = \mathbb{C} \setminus \{0\}$. Es claro que $\mathbb{C} \setminus \{0\} \subseteq \mathcal{U}(A)$ por lo que solo resta ver la otra inclusión.

Si $f \in \mathcal{U}(A)$, existe $g \in A$ tal que $f \cdot g = 1$. Sea $m \in \mathbb{N}_0$ tal que $f, g \in \mathbb{C}\left[X^{\frac{1}{2^m}}\right]$. Entonces, existen $d, e \in \mathbb{N}_0$ tales que $f = \sum_{k=0}^{d} a_k \left(X^{\frac{1}{2^m}}\right)^k$ y $g = \sum_{j=0}^{e} b_j \left(X^{\frac{1}{2^m}}\right)^j$.

Vía un cambio de variable $T = X^{\frac{1}{2^m}}$ y considerando $F(T) = f\left(T^{2^m}\right)$ y $G(T) = g\left(T^{2^m}\right)$ se sigue que $1 = F(T) \cdot G(T)$ igualdad en $\mathbb{C}[T]$, por lo que F y G deben ser constantes. Así, $a_k = 0$ y $b_j = 0$ para todos $j, k \geq 1$, por lo que f y g originalmente eran constantes.

Por último, probemos que A no es un DF. Para ello, vamos a mostrar que $X \in A$ no se puede escribir como producto de irreducibles en A.

Dado $f \in A \setminus \{0\}$, escribámoslo como $f = \sum_{k=0}^{d} a_k \left(X^{\frac{1}{2^m}}\right)^k = \sum_{k=0}^{d} a_k X^{\frac{k}{2^m}}$ para ciertos $m \in \mathbb{N}_0$ y $d \in \mathbb{N}_0$. Veamos que si $a_0 = 0$ entonces f es reducible (notar que si $a_0 = 0$, como $f \neq 0$, debe ser $d \geq 1$). En efecto:

- Si $d = 1$, $f = a_1 X^{\frac{1}{2^m}} = a_1 \underbrace{X^{\frac{1}{2^{m+1}}}}_{\notin \mathcal{U}(A)} \cdot \underbrace{X^{\frac{1}{2^{m+1}}}}_{\notin \mathcal{U}(A)}$.
- Si $d > 1$, $f = \underbrace{X^{\frac{1}{2^m}}}_{\notin \mathcal{U}(A)} \cdot \underbrace{\sum_{k=1}^{d} a_k X^{\frac{k-1}{2^m}}}_{\notin \mathcal{U}(A)}$.

Supongamos entonces que X se factoriza en irreducibles en A:

$$X = \prod_{i=1}^{r} q_i \text{ con } q_i \text{ irreducible en } A.$$

Para cada $i \in \{1, \ldots, r\}$, escribamos $q_i = \sum_{k=0}^{d_i} a_k^{(i)} \left(X^{\frac{1}{2^{m_i}}}\right)^k$. Luego como q_i es irreducible, a partir de lo hecho anteriormente, debe ser $a_0^{(i)} \neq 0$. Pero así, el término independiente del producto $\prod_{i=1}^{r} q_i$ es $\prod_{i=1}^{r} a_0^{(i)} \neq 0$, lo cual es absurdo ya que el mismo debe ser 0 por ser el término independiente de $X = \prod_{i=1}^{r} q_i$.

Luego X no se factoriza en irreducibles en A. □

Daremos a la brevedad una condición suficiente (que veremos en el Capítulo 4 que no es necesaria) para que un dominio íntegro sea un DF.

Previo a ello, vamos a recordar la condición de noetherianidad en un anillo conmutativo y algunos resultados elementales sobre anillos noetherianos.

Definición 2.1.5. Sea A un anillo conmutativo. Decimos que A es noetheriano si todo ideal de A es finitamente generado.

Teorema 2.1.6. *Sea A un anillo conmutativo. Son equivalentes:*

(1) A es noetheriano.

(2) Toda sucesión ascendente de ideales de A se estaciona, es decir, si $(I_n)_{n\in\mathbb{N}}$ es una sucesión de ideales de A tal que $I_n \subseteq I_{n+1}$ para todo $n \in \mathbb{N}$, entonces existe $N \in \mathbb{N}$ tal que $I_n = I_N$ para todo $n \geq N$.

(3) Todo conjunto no vacío de ideales propios de A tiene un elemento maximal con respecto a la inclusión, es decir, hay algún ideal del conjunto que no está incluido estrictamente en ningún otro del mismo.

Demostración.

$\underline{(1) \Rightarrow (2)}$: sea $(I_n)_{n\in\mathbb{N}}$ una sucesión ascendente de ideales de A. Definimos $I = \bigcup_{n\in\mathbb{N}} I_n$, que resulta un ideal de A debido a que la sucesión de ideales considerada es ascendente.

Por hipótesis, como A es noetheriano, el ideal I es finitamente generado, o sea, existen $a_1, \ldots, a_r \in A$ tales que $I = \langle a_1, \ldots, a_r \rangle$.

Para cada $i \in \{1, \ldots, r\}$ existe $n_i \in \mathbb{N}$ tal que $a_i \in I_{n_i}$. Sea $N = \max\{n_i : 1 \leq i \leq r\}$. Luego $a_i \in I_N, \forall\, 1 \leq i \leq r$ y entonces $I = \langle a_1, \ldots, a_r \rangle \subseteq I_N \subseteq I$, por lo que $I = I_N$. Así, se tiene que $I_n = I_N$ para todo $n \geq N$.

$\underline{(2) \Rightarrow (3)}$: sea $\mathcal{F} \neq \varnothing$ un conjunto no vacío de ideales propios de A y supongamos que $\mathcal{F}$ no tiene un elemento maximal.

Sea $I_1 \in \mathcal{F}$. Como I_1 no es maximal, existe $I_2 \in \mathcal{F}$ tal que $I_1 \subsetneq I_2$. A su vez, como I_2 no es maximal, existe $I_3 \in \mathcal{F}$ tal que $I_2 \subsetneq I_3$. Inductivamente, dado $n \in \mathbb{N}$ y teniendo $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$, como I_n no es maximal, existe $I_{n+1} \in \mathcal{F}$ tal que $I_n \subsetneq I_{n+1}$, y conseguimos así una cadena ascendente de ideales de A que no se estaciona, lo cual contradice nuestra hipótesis.

$\underline{(3) \Rightarrow (1)}$: sea I un ideal de A y consideremos el conjunto de ideales $\mathcal{F} = \big\{J \subseteq A \ : \ J$ es un ideal de A finitamente generado, $J \subseteq I\big\}$.

Claramente $\mathcal{F} \neq \varnothing$ ya que $J = \langle 0 \rangle \in \mathcal{F}$. Luego por hipótesis, existe $J \in \mathcal{F}$ que es maximal con respecto a la inclusión, $J = \langle a_1, \ldots, a_r \rangle \subseteq I$.

Si fuese $J \subsetneq I$, entonces existiría $a_0 \in I \setminus J$, y en consecuencia se tendría que $J \subsetneq \langle a_0, a_1, \ldots, a_r \rangle \subseteq I$, lo cual contradice la maximalidad de J. Debe ser entonces $I = J = \langle a_1, \ldots, a_r \rangle$, por lo que I es finitamente generado. $\square$

Veamos ahora un resultado importante sobre factorización en dominios noetherianos.

Teorema 2.1.7. *Sea A un dominio íntegro que es noetheriano. Entonces, A es un DF.*

Demostración.

Supongamos que A no es un DF y sea entonces $a_0 \in A \setminus \{0\}$, $a_0 \notin \mathcal{U}(A)$, tal que a_0 no se puede escribir como producto de irreducibles en A.

Consideremos el conjunto de ideales $\mathcal{F} = \Big\{\langle a\rangle \,:\, a \neq 0, a \notin \mathcal{U}(A), a \text{ no se puede escribir como producto de irreducibles en } A\Big\}$. Se tiene que $\mathcal{F} \neq \varnothing$ ya que $\langle a_0\rangle \in \mathcal{F}$, y entonces, como A es noetheriano, por el teorema 2.1.6, $\mathcal{F}$ tiene un elemento maximal $\langle a\rangle$.

Como a no se puede escribir como producto de irreducibles en A, en particular a no es irreducible. Luego existen $b, c \in A \setminus \{0\}$ y $b, c \notin \mathcal{U}(A)$ tales que $a = b \cdot c$. Se tiene entonces que $\langle a\rangle \subsetneq \langle b\rangle$ ya que a y b no son asociados y $b \mid a$. Análogamente, $\langle a\rangle \subsetneq \langle c\rangle$.

Pero así, por la maximalidad de $\langle a\rangle$, como $b, c \in A \setminus \{0\}$ y $b, c \notin \mathcal{U}(A)$, debe ser $\langle b\rangle, \langle c\rangle \notin \mathcal{F}$, y entonces b y c se pueden escribir como producto de irreducibles en A:

$$b = \prod_{i=1}^{n} q_i \quad y \quad c = \prod_{j=1}^{m} q'_j \quad \text{con } q_i \text{ , } q'_j \text{ irreducibles en } A,$$

y entonces $a = b \cdot c = \prod_{i=1}^{n} q_i \cdot \prod_{j=1}^{m} q'_j$ se escribe como producto de irreducibles en A, lo cual es absurdo.

□

Por último, exhibimos a continuación la relación entre el concepto de elemento primo y elemento irreducible en un dominio íntegro.

Teorema 2.1.8. *Sea A un dominio íntegro. Si $p \in A$ es primo, entonces p es irreducible en A.*

Demostración.

Sean $p \in A$ primo y $a \in A$ tal que $a \mid p$. Debemos ver que $a \in \mathcal{U}(A)$ o bien $a \sim p$.

Como $a \mid p$, existe $b \in A$ tal que $p = a \cdot b$, y entonces $p \mid a \cdot b$. Luego dado que p es primo, debe ser $p \mid a$ o bien $p \mid b$.

Si $p \mid a$, como también $a \mid p$, resulta que $a \sim p$.

Análogamente, si $p \mid b$, se sigue que $b \sim p$ y entonces existe $u \in \mathcal{U}(A)$ tal que $p = u \cdot b$. Se tiene así que $a \cdot b = p = u \cdot b$, y entonces $b \cdot (a - u) = 0$. Como A es un dominio íntegro y $b \neq 0$ ya que $p \neq 0$, se concluye que $a = u \in \mathcal{U}(A)$. □

Observación 2.1.9. El enunciado recíproco al teorema 2.1.8 no es cierto en un dominio íntegro arbitrario, es decir, si A es un dominio íntegro y $q \in A$ es irreducible en A, no necesariamente q es primo.

Proposición 2.1.10. *En el dominio íntegro $A = \mathbb{Z}[i\sqrt{5}] = \big\{a + b\sqrt{5}\, i \;/\; a, b \in \mathbb{Z}\big\}$, el elemento $q = 2$ es irreducible en A pero no es primo.*

Demostración.

- 2 es irreducible en A:

  Sea $z = a + b\sqrt{5}\ i \in A$ tal que $z \mid 2$. Luego existe $w = c + d\sqrt{5}\ i$ en A tal que $2 = z \cdot w$, y entonces al tomar módulo complejo en ambos miembros y elevar al cuadrado tenemos la igualdad en $\mathbb{N}_0$

  $$|2|^2 = |a + b\sqrt{5}\ i|^2 \cdot |c + d\sqrt{5}\ i|^2 \iff 4 = (a^2 + 5b^2) \cdot (c^2 + 5d^2),$$

  de donde se concluye que $a^2 + 5b^2 = 2$ y $c^2 + 5d^2 = 2$, o bien $a^2 + 5b^2 = 1$ y $c^2 + 5d^2 = 4$ (o al revés).

  Sin embargo, como $a, b, c, d \in \mathbb{Z}$, la ecuación $a^2 + 5b^2 = 2$ no tiene soluciones enteras. En efecto, si $b = 0$ debería ser que $a^2 = 2$ en $\mathbb{Z}$, mientras que si $b \neq 0$, se tendría que $a^2 + 5b^2 \geq 5$.

  Luego debe ser $a^2 + 5b^2 = 1$ y $c^2 + 5d^2 = 4$ (o al revés).

  Si $a^2 + 5b^2 = 1$, nuevamente si fuese $b \neq 0$ tendríamos que $a^2 + 5b^2 \geq 5$, por lo cual debe ser $b = 0$ y entonces $a = \pm 1$. Concluimos así que $z = \pm 1 \in \mathcal{U}(A)$.

  Del mismo modo, si $c^2 + 5d^2 = 1$ se concluye que $w = \pm 1$ y entonces $2 \sim z$.

- 2 no es primo en A:

  En A podemos escribir $6 = (1 + \sqrt{5}\ i) \cdot (1 - \sqrt{5}\ i)$ y entonces, como $2 \mid 6$, resulta que $2 \mid (1 + \sqrt{5}\ i) \cdot (1 - \sqrt{5}\ i)$. Sin embargo, veamos que $2 \nmid 1 \pm \sqrt{5}\ i$.

  Si suponemos que existe $a + b\sqrt{5}\ i \in A$ tal que $1 + \sqrt{5}\ i = 2 \cdot (a + b\sqrt{5}\ i)$, entonces al igualar parte real en ambos miembros tendríamos que $2a = 1$ con $a \in \mathbb{Z}$, lo cual es absurdo. Análogamente, suponer que $2 \mid 1 - \sqrt{5}\ i$ nos lleva a la misma contradicción.

□

2.2. Dominios de Factorización Única

Definición 2.2.1. Sea A un anillo. Decimos que A es un Dominio de Factorización Única (DFU) si A es un DF y además cada vez que $\prod_{i=1}^{n} q_i = \prod_{j=1}^{m} q'_j$, con q_i, q'_j irreducibles en A se cumple simultáneamente:

- $n = m$,
- Existe una permutación $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tal que para todo $i \in \{1, \ldots, n\}$, $q_i \sim q'_{f(i)}$.

Observación 2.2.2. La definición de DFU esencialmente nos dice que debemos poder factorizar en irreducibles (así tenemos un DF) y que si se consideran dos escrituras como producto de irreducibles de un mismo elemento, entonces ocurra que los irreducibles en ambas factorizaciones sean "los mismos" salvo asociados y el orden en que aparecen.

Luego dos factorizaciones en irreducibles de un mismo elemento no nulo ni unidad en un DFU difieren solo en un factor inversible.

En un DFU, los elementos irreducibles siempre son primos. Más aún, esta condición es la que proporciona en algún sentido la unicidad de factorización.

Teorema 2.2.3. *Sea A un DF. Entonces, A es un DFU si y solo si todo elemento $q \in A$ irreducible también es primo.*

Demostración.

($\Rightarrow$) Sea $q \in A$ irreducible y sean $a, b \in A$ tales que $q \mid a \cdot b$. Debemos probar que $q \mid a$ ó $q \mid b$.

Si $a = 0$ ó $b = 0$ es inmediato. Supongamos entonces que $a, b \neq 0$, y así, como $q \mid a \cdot b$, existe $c \in A \setminus \{0\}$ tal que $a \cdot b = q \cdot c$.

Como A es DFU, existen $r, s, t \in \mathbb{N}_0$ y $q_1, \ldots, q_r, p_1, \ldots, p_s, g_1, \ldots, g_t$ irreducibles en A tales que

$$a = \prod_{i=1}^{r} q_i \ , \quad b = \prod_{j=1}^{s} p_j \quad \text{y} \quad c = \prod_{k=1}^{t} g_k \ ,$$

y entonces

$$a \cdot b = q \cdot c \quad \Longleftrightarrow \quad \prod_{i=1}^{r} q_i \cdot \prod_{j=1}^{s} p_j = q \cdot \prod_{k=1}^{t} g_k \ .$$

Por unicidad de factorización, como q es irreducible en A, debe ser $q \sim q_i$ para algún $i \in \{1, \ldots, r\}$ o bien $q \sim p_j$ para algún $j \in \{1, \ldots, s\}$, de donde se sigue que $q \mid a$ o bien $q \mid b$ respectivamente.

($\Leftarrow$) Lo probamos por inducción en el número n de factores irreducibles que aparecen en alguna descomposición como producto de irreducibles en A de un elemento $a \in A \setminus \{0\}$, $a \notin \mathcal{U}(A)$.

Si $n = 1$, a admite una factorización con un irreducible y supongamos que admite otra factorización con m factores irreducibles:

$$a = p = \prod_{i=1}^{m} q_i, \ \text{ con } \ p, q_1, \ldots, q_m \text{ irreducibles en } A.$$

Supongamos $m \geq 2$. Como $p \mid a = \prod_{i=1}^{m} q_i$ con p irreducible en A y luego primo por hipótesis, entonces existe $i \in \{1, \ldots, m\}$ tal que $p \mid q_i$. Sin pérdida de generalidad podemos suponer $i = m$ (si no, basta reordenar el producto), y entonces tenemos que $p \mid q_m$ con $p, \ q_m$ irreducibles en A, por lo cual deben ser asociados: $q_m = u \cdot p$ con $u \in \mathcal{U}(A)$.

Así, a partir de las escrituras de a como producto de irreducibles tenemos:

$$p = u \cdot p \cdot \prod_{i=1}^{m-1} q_i,$$

y como A es un dominio íntegro y $p \neq 0$, resulta que

$$1 = u \cdot \prod_{i=1}^{m-1} q_i.$$

Pero entonces no puede haber factores irreducibles en el miembro derecho (ya que si no tendríamos que un irreducible divide a 1 y luego debería ser una unidad), lo cual es un absurdo ya que asumimos $m \geq 2$. Así, si $n = 1$, y consideramos otra factorización de m factores irreducibles, resulta $m = 1$ y entonces $q_m = a = u \cdot p$ con $u \in \mathcal{U}(A)$, de donde $q_m \sim p$.

Supongamos ahora que el enunciado es cierto para todo elemento $a \in A \setminus \{0\}$, $a \notin \mathcal{U}(A)$ que admite alguna descomposición como producto de n irreducibles en A y veamos que vale para aquellos elementos no nulos ni unidades que admiten alguna factorización con $n+1$ irreducibles en A.

Sea $a \in A \setminus \{0\}$, $a \notin \mathcal{U}(A)$ tal que a se factoriza como producto de $n+1$ irreducibles en A y supongamos que a admite otra factorización con m factores irreducibles en A:

$$a = \prod_{i=1}^{n+1} q_i = \prod_{j=1}^{m} p_j, \quad \text{con } q_1, \ldots, q_{n+1}, p_1, \ldots, p_m \text{ irreducibles en } A.$$

Notar que debe ser $m \geq 2$ ya que si no tendríamos un solo factor irreducible en el miembro derecho, y por el caso base ya probado, debería ser $n + 1 = 1$ con $n \in \mathbb{N}$. Análogo a lo hecho anteriormente, como $q_{n+1} \mid a = \prod_{j=1}^{m} p_j$ con q_{n+1} irreducible en A y luego primo por hipótesis, entonces existe $j \in \{1, \ldots, m\}$ tal que $q_{n+1} \mid p_j$. Sin pérdida de generalidad podemos suponer $j = m$ (si no, basta reordenar el producto), y entonces tenemos que $q_{n+1} \mid p_m$ con $q_{n+1},\ p_m$ irreducibles en A, por lo cual deben ser asociados: $p_m = u \cdot q_{n+1}$ con $u \in \mathcal{U}(A)$.

A partir de las escrituras de a como producto de irreducibles en A que es dominio íntegro concluimos que:

$$q_{n+1} \cdot \prod_{i=1}^{n} q_i = u \cdot q_{n+1} \cdot \prod_{j=1}^{m-1} p_j \quad \underset{q_{n+1} \neq 0}{\iff} \quad \prod_{i=1}^{n} q_i = u \cdot \prod_{j=1}^{m-1} p_j$$

Por hipótesis inductiva, resulta que $n = m - 1$ (y por ende $n + 1 = m$) y que cada irreducible en el miembro izquierdo es asociado a un único irreducible del miembro derecho. Reordenando los factores de ser necesario, podemos asumir sin pérdida de

generalidad que $q_i \sim p_i$, para todo $i \in \{1, \dots, n\}$. Así, volviendo a la factorización original, teníamos:

$$a = \prod_{i=1}^{n+1} q_i = \prod_{j=1}^{m} p_j,$$

y probamos que $n+1 = m$ y que, reordenando los factores de ser necesario, $q_1 \sim p_1$, $\dots$, $q_n \sim p_n$ y $q_{n+1} \sim p_{n+1}$. □

Surge aquí una pregunta natural: ¿es necesario verificar la condición "primo = irreducible" en un DF? Esto es: ¿puede efectivamente un DF no ser un DFU?

Daremos respuesta a esta pregunta en el Capítulo 4 al probar que el dominio $\mathbb{Z}[i\sqrt{5}]$ es efectivamente un DF.

2.3. Máximo Común Divisor y Mínimo Común Múltiplo

Veremos a continuación que en un DFU arbitrario siempre existe el máximo común divisor (mcd), y que la definición es análoga a la conocida para $\mathbb{Z}$.

Definición 2.3.1. Sea A un dominio íntegro y sean $a, b \in A$ no ambos nulos. Decimos que un elemento $d \in A$ es un máximo común divisor (mcd) de a y b si satisface a la vez las siguientes condiciones:

- $d \mid a$ y $d \mid b$,
- Si $c \in A$ tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Observación 2.3.2. Sea A un dominio íntegro y sean $a, b \in A$ no ambos nulos. Si existe un mcd de a y b entonces es único salvo asociados y se nota $\mathrm{mcd}(a, b)$ (que está bien definido salvo asociados).

Veremos ahora que si A es un DFU entonces el mcd de dos elementos no ambos nulos siempre existe. Más aún, es posible hallarlo a partir de las factorizaciones en irreducibles de los dos elementos en cuestión.

Para ello, en virtud de la observación 2.2.2, si A es un DFU podemos fijar un sistema de representantes $\mathcal{P}$ de irreducibles (= primos) en A, es decir, un irreducible por cada clase de asociados (dado $p \in A$ irreducible, existe un único $p_0 \in \mathcal{P}$ tal que $p \sim p_0$).

Bajo esta misma idea, fijamos al $1 \in A$ como representante de $\mathcal{U}(A)$.

Observación 2.3.3. Sea A un DFU y sean $a, b \in A$ no ambos nulos. Fijemos $\mathcal{P}$ un sistema de representantes por clase de asociados de los irreducibles en A y al $1 \in A$ como representante de $\mathcal{U}(A)$.

(1) Si $a \in \mathcal{U}(A)$ o $b \in \mathcal{U}(A)$, entonces $\mathrm{mcd}(a, b) = 1$.

(2) Si $a, b \notin \mathcal{U}(A)$ y $b = 0$, entonces $a \neq 0$ y podemos considerar su factorización en irreducibles en A a partir del sistema de representantes de irreducibles $\mathcal{P}$.

Luego podemos escribir $a = u \cdot \prod_{i=1}^{r} p_i^{m_i}$ con $u \in \mathcal{U}(A)$ y $m_i \in \mathbb{N}$ para todo $1 \leq i \leq r$, y en consecuencia $\mathrm{mcd}(a, 0) = \prod_{i=1}^{r} p_i^{m_i}$.

Si $a = 0$ pero $b \neq 0$ es análogo.

(3) Si $a, b \notin \mathcal{U}(A)$ son ambos no nulos, consideramos sus factorizaciones en irreducibles en A a partir del sistema de representantes de irreducibles $\mathcal{P}$ y tomamos $p_1, \ldots, p_r \in \mathcal{P}$ todos los irreducibles que aparecen en alguna de las factorizaciones.

Luego podemos escribir $a = u_a \cdot \prod_{i=1}^{r} p_i^{m_i}$ y $b = u_b \cdot \prod_{j=1}^{r} p_j^{n_j}$, con $u_a, u_b \in \mathcal{U}(A)$ y $m_i, n_j \in \mathbb{N}_0$ para todos $1 \leq i, j \leq r$, y entonces:

$$\mathrm{mcd}(a, b) = \prod_{k=1}^{r} p_k^{\mín\{m_k \,;\, n_k\}}$$

Por lo tanto, si A es un DFU y $a, b \in A$ no son ambos nulos entonces siempre existe $\mathrm{mcd}(a, b)$, y eligiendo un sistema de representantes de irreducibles $\mathrm{mcd}(a, b)$ se puede definir de forma unívoca. En particular, en tal caso resulta inmediato que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a)$.

Definición 2.3.4. Sea A un DFU y fijemos un sistema de representantes $\mathcal{P}$ de irreducibles en A y al $1 \in A$ como representante de $\mathcal{U}(A)$. Dados $a, b \in A$ no ambos nulos, decimos que a y b son coprimos si $\mathrm{mcd}(a, b) = 1$.

Observación 2.3.5. Si A es un DFU, la coprimalidad induce las siguientes propiedades (que son análogas a las conocidas para $\mathbb{Z}$): si $a, b, c \in A$ con a y b no ambos nulos, entonces

(1) Los elementos $\dfrac{a}{\mathrm{mcd}(a, b)}, \dfrac{b}{\mathrm{mcd}(a, b)} \in A$ son coprimos.

(2) Si $a \mid b \cdot c$ y $\mathrm{mcd}(a, b) = 1$, entonces $a \mid c$.

(3) Si $a \mid c$, $b \mid c$ y $\mathrm{mcd}(a, b) = 1$, entonces $a \cdot b \mid c$.

Por último, si bien no será objeto de estudio en este trabajo, damos a continuación la definición de mínimo común múltiplo de dos elementos no nulos en A un DFU.

Definición 2.3.6. Sea A un dominio íntegro y sean $a, b \in A$ no nulos. Decimos que un elemento $m \in A$ es un mínimo común múltiplo (mcm) de a y b si satisface a la vez las siguientes condiciones:

- $a \mid m$ y $b \mid m$,
- Si $c \in A$ tal que $a \mid c$ y $b \mid c$, entonces $m \mid c$.

Observación 2.3.7. Sea A un dominio íntegro y sean $a, b \in A$ no nulos. Si existe un mcm de a y b entonces es único salvo asociados y se nota $\mathrm{mcm}(a, b)$ (que está bien definido salvo asociados).

Damos a continuación una caracterización (análoga a la vista para mcd) para el mcm de dos elementos no nulos en un DFU a partir de las factorizaciones en irreducibles de los dos elementos en cuestión.

Observación 2.3.8. Sea A un DFU y sean $a, b \in A$ no nulos. Fijemos $\mathcal{P}$ un sistema de representantes por clase de asociados de los irreducibles en A y al $1 \in A$ como representante de $\mathcal{U}(A)$.

(1) Si $a, b \in \mathcal{U}(A)$, entonces $\mathrm{mcm}(a, b) = 1$.

(2) Si $a \notin \mathcal{U}(A)$ o $b \notin \mathcal{U}(A)$, consideramos sus factorizaciones en irreducibles en A a partir del sistema de representantes de irreducibles $\mathcal{P}$ y tomamos $p_1, \ldots, p_r \in \mathcal{P}$ todos los irreducibles que aparecen en alguna de las factorizaciones.

Luego podemos escribir $a = u_a \cdot \prod_{i=1}^{r} p_i^{m_i}$ y $b = u_b \cdot \prod_{j=1}^{r} p_j^{n_j}$, con $u_a, u_b \in \mathcal{U}(A)$ y $m_i, n_j \in \mathbb{N}_0$ para todos $1 \leq i, j \leq r$, y entonces:

$$\mathrm{mcm}(a, b) = \prod_{k=1}^{r} p_k^{\mathrm{máx}\{m_k \,;\, n_k\}}$$

Por lo tanto, si A es un DFU y $a, b \in A$ son ambos no nulos entonces siempre existe $\mathrm{mcm}(a, b)$, y eligiendo un sistema de representantes de irreducibles $\mathrm{mcm}(a, b)$ se puede definir de forma unívoca. En particular, en tal caso resulta inmediato que $\mathrm{mcm}(a, b) = \mathrm{mcm}(b, a)$, y también que $\mathrm{mcd}(a, b) \cdot \mathrm{mcm}(a, b) \sim a \cdot b$ en A.

Es importante tener presente que dado un dominio íntegro arbitrario (incluso si es un DF) el mcd de dos elementos no ambos nulos podría no existir.

Ejemplo 2.3.9. Sea el dominio íntegro $A = \mathbb{Z}[i\sqrt{5}]$. Si consideramos los elementos $z = 6$ y $w = 2 \cdot (1 + \sqrt{5}\, i)$ de A, entonces no existe un máximo común divisor de z y w.

Demostración.

Tengamos presente que en virtud de lo que probamos en 2.1.10 concluimos que A no es un DFU.

Supongamos que $d = a + b\sqrt{5}\, i \in A$ satisface la definición de mcd de z y w y observemos que $z = 6 = 2 \cdot 3 = (1 + \sqrt{5}\, i) \cdot (1 - \sqrt{5}\, i)$ y $w = 2 \cdot (1 + \sqrt{5}\, i)$.

Por un lado, como $d \mid z$ y $d \mid w$ en A se sigue que $|d|^2 \mid |z|^2$ y $|d|^2 \mid |w|^2$ en $\mathbb{Z}$, es decir, $a^2 + 5b^2 \mid 36$ y $a^2 + 5b^2 \mid 24$ en $\mathbb{Z}$. Concluimos entonces que $a^2 + 5b^2 \mid \mathrm{mcd}_{\mathbb{Z}}(24, 36) = 12$.

Por otro lado, tenemos que:

- $1+\sqrt{5}\,i \mid z$ y $1+\sqrt{5}\,i \mid w$ en $A \Longrightarrow 1+\sqrt{5}\,i \mid d$ en $A \Longrightarrow |1+\sqrt{5}\,i|^2 \mid |d|^2$ en $\mathbb{Z}$.
  Luego $6 \mid a^2+5b^2$.
- $2 \mid z$ y $2 \mid w$ en $A \Longrightarrow 2 \mid d$ en $A \Longrightarrow |2|^2 \mid |d|^2$ en $\mathbb{Z}$.
  Así $4 \mid a^2+5b^2$.

Se tiene entonces que $\mathrm{mcm}_{\mathbb{Z}}(6,4) = 12 \mid a^2+5b^2$. En consecuencia, resulta que $a^2+5b^2 = 12$, pero

- $|b| \geq 2 \Longrightarrow 5b^2 \geq 20 \Longrightarrow 12 = a^2+5b^2 \geq 20$,
- $|b| = 1 \Longrightarrow a^2 = 7$ con $a \in \mathbb{Z}$,
- $|b| = 0 \Longrightarrow a^2 = 12$ con $a \in \mathbb{Z}$,

por lo que llegamos a un absurdo en cualquier caso. □

Terminamos este capítulo dos observaciones que abordaremos en capítulos posteriores de este trabajo.

Observación 2.3.10.

(1) Queda pendiente justificar que el dominio íntegro $A = \mathbb{Z}[i\sqrt{5}]$ es un DF.

(2) Dado A un DFU intentamos generalizar la noción de mcd a partir de la de $\mathbb{Z}$. ¿Qué podemos decir de las propiedades del mcd conocidas en $\mathbb{Z}$ para A un DFU arbitrario? En especial, ¿qué ocurre con el algoritmo de Euclides y con la escritura del $\mathrm{mcd}(a,b)$ como combinación de a y b?

Capítulo 3

Dominios Principales y Dominios Euclídeos

En este capítulo estudiaremos las dos propiedades que quedaron pendientes del mcd: la escritura del mcd entre dos elementos no ambos nulos como combinación de los mismos (con coeficientes en el anillo) y la existencia de un algoritmo que permita calcularlo de forma similar al de Euclides conocido para $\mathbb{Z}$. Veremos además que pese a tener existencia de factorización y unicidad de la misma (salvo asociados) tales propiedades no siempre pueden asegurarse, pero que en algún sentido contar con esas dos propiedades permite garantizar ambas condiciones con respecto a la factorización en irreducibles.

3.1. Dominios Principales

Definición 3.1.1. Sea A un anillo. Decimos que A es un Dominio Principal (DP) si A es un dominio íntegro y además todo ideal I de A es principal.

Ejemplo 3.1.2.

(1) Todo cuerpo $\mathbb{K}$ es un DP ya que sus únicos ideales son $\{0\} = \langle 0\rangle$ y $\mathbb{K} = \langle 1\rangle$ que son ambos principales.

(2) $\mathbb{Z}$ es un DP ya que sus ideales son todos de la forma $n\mathbb{Z} = \langle n\rangle$ con $n \in \mathbb{N}_0$.

(3) Si $\mathbb{K}$ es un cuerpo, $\mathbb{K}[X]$ es un DP.

Proposición 3.1.3. *Sea A un dominio íntegro y sean $a, b \in A$ no ambos nulos tales que existe $d \in A$ con $\langle a, b\rangle = \langle d\rangle$. Entonces, d es un mcd entre a y b que, además, satisface la identidad de Bézout: existen $s, t \in A$ tales que $d = s \cdot a + t \cdot b$. En particular, si A es un DP entonces para todos $a, b \in A$ no ambos nulos existe $d = \mathrm{mcd}(a, b)$ y es combinación lineal con coeficientes en A de a y b.*

Demostración.

Debemos probar que el elemento d satisface las dos condiciones de la definición 2.3.1 de mcd y la identidad de Bézout sabiendo que $\langle a, b\rangle = \langle d\rangle$.

Por un lado resulta que $a, b \in \langle d\rangle$ y entonces $d \mid a$ y $d \mid b$. A su vez, $d \in \langle a, b\rangle$ y entonces existen $s, t \in A$ tales que $d = s \cdot a + t \cdot b$. Así, si $c \in A$ cumple que $c \mid a$ y $c \mid b$ entonces $c \mid s \cdot a + t \cdot b = d$. □

Daremos a continuación un resultado que es una consecuencia del Lema de Zorn y que permite reducir la definición de DP solo a sus ideales primos.

Teorema 3.1.4. *Sea A un dominio íntegro. Entonces, A es un DP si y solo si todo ideal primo de A es principal.*

Demostración.

($\Rightarrow$) Es evidente ya que A es un DP.

($\Leftarrow$) Supongamos que A no es un DP. Luego el conjunto $\mathcal{X} = \{I \trianglelefteq A : I \text{ no es principal}\}$ es no vacío.

- En $\mathcal{X}$ definimos la relación $\preceq$ dada por la inclusión: $I_1 \preceq I_2 \Leftrightarrow I_1 \subseteq I_2$.

  Así $(\mathcal{X}, \preceq)$ resulta un conjunto parcialmente ordenado.

- Sea $\mathcal{C} = (I_j)_{j\in\Lambda} \subseteq \mathcal{X}$ una cadena, es decir, un conjunto que es totalmente ordenado con respecto a $\preceq$ y sea $J = \bigcup_{j\in\Lambda} I_j$.

  J resulta un ideal de A pues $\mathcal{C}$ es totalmente ordenado y es claro que es una cota superior de $\mathcal{C}$ con respecto a $\preceq$. Veamos que $J \in \mathcal{X}$.

  Supongamos que no. Luego $J \trianglelefteq A$ es principal y existe $\alpha \in A$ tal que $J = \langle\alpha\rangle$.

  Así, $\alpha \in J = \bigcup_{j\in\Lambda} I_j$ por lo que existe $j_0 \in \Lambda$ tal que $\alpha \in I_{j_0}$, y entonces:

  $$\langle\alpha\rangle \subseteq I_{j_0} \subseteq J = \langle\alpha\rangle \Longrightarrow I_{j_0} = \langle\alpha\rangle \text{ con } I_{j_0} \in \mathcal{X},$$

  lo cual es absurdo. Luego debe ser $J \in \mathcal{X}$.

Concluimos de este modo que toda cadena en $\mathcal{X}$ tiene una cota superior en $\mathcal{X}$ y entonces, por el Lema de Zorn 1.1.18, existe $\mathcal{M} \in \mathcal{X}$ elemento maximal. Notar que $\mathcal{M} \neq \{0\}$ ya que no es principal.

Veamos que $\mathcal{M} \trianglelefteq A$ debe ser primo. Supongamos que no lo es y entonces deben existir $a, b \in A$ tales que $a \cdot b \in \mathcal{M}$ pero $a \notin \mathcal{M}$ y $b \notin \mathcal{M}$. Así, $K = \mathcal{M} + \langle a\rangle$ es un ideal de A que cumple $\mathcal{M} \subsetneq K$, por lo que $K \notin \mathcal{X}$ y entonces debe ser principal: existe $c \in A$ tal que $K = \langle c\rangle$. Consideremos el transportador de a en $\mathcal{M}$:

$$(\mathcal{M} : a) = \{t \in A \ : \ t \cdot a \in \mathcal{M}\} \trianglelefteq A.$$

Se tiene entonces que $\mathcal{M} \subseteq (\mathcal{M} : a)$, y como $b \in (\mathcal{M} : a)$ pero $b \notin \mathcal{M}$, resulta $\mathcal{M} \subsetneq (\mathcal{M} : a)$. Debe ser entonces $(\mathcal{M} : a) \notin \mathcal{X}$ y por ende $(\mathcal{M} : a)$ debe ser principal: $(\mathcal{M} : a) = \langle d \rangle$ para cierto $d \in A$.

Veamos que en estas condiciones se tiene entonces que $\mathcal{M} = \langle c \cdot d \rangle$.

($\supseteq$) Basta ver que $c \cdot d \in \mathcal{M}$. Como $d \in \langle d \rangle = (\mathcal{M} : a)$, entonces $d \cdot a \in \mathcal{M}$.

A su vez, $c \in \langle c \rangle = \mathcal{M} + \langle a \rangle$, por lo que existen $m \in \mathcal{M}$ y $r \in A$ tales que $c = m + r \cdot a$.

Luego $c \cdot d = \underbrace{m}_{\in \mathcal{M}} \cdot d + r \cdot (\underbrace{d \cdot a}_{\in \mathcal{M}}) \in \mathcal{M}$.

($\subseteq$) Sea $m \in \mathcal{M}$. Como $\langle c \rangle = \mathcal{M} + \langle a \rangle$ existen entonces $s, t \in A$ tales que $m = s \cdot c$ y $a = t \cdot c$. Luego $s \cdot a = t \cdot m \in \mathcal{M}$ y entonces $s \in (\mathcal{M} : a) = \langle d \rangle$, por lo que $s = h \cdot d$ para algún $h \in A$. Así, $m = s \cdot c = (h \cdot d) \cdot c = h \cdot (c \cdot d) \in \langle c \cdot d \rangle$.

Concluimos entonces que efectivamente $\mathcal{M} = \langle c \cdot d \rangle$, lo cual contradice el hecho de que $\mathcal{M} \in \mathcal{X}$ por lo que no puede ser principal. El absurdo provino de suponer que $\mathcal{M}$ no es un ideal primo, y en consecuencia sí debe serlo. Sin embargo, esto también nos lleva a una contradicción ya que por hipótesis todo ideal primo de A es principal.

Luego $\mathcal{X}$ debe ser vacío.

□

3.2. Dominios Euclídeos

Definición 3.2.1. Sea A un anillo. Decimos que A es un Dominio Euclídeo (DE) si A es un dominio íntegro y además existe una función $f : A \setminus \{0\} \longrightarrow \mathbb{N}_0$ que satisface simultáneamente:

(I) Para todos $a, b \in A \setminus \{0\}$ se tiene $f(a \cdot b) \geq f(a)$,

(II) Si $a, b \in A$, $b \neq 0$, existen $q, r \in A$ tales que $a = b \cdot q + r$ con $r = 0$ ó $f(r) < f(b)$.

En tal caso, la función f de la definición anterior se dice una función euclídea en A.

Ejemplo 3.2.2.

(1) $\mathbb{Z}$ es un DE con función euclídea $f : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0$, $f(m) = |m|$.

(2) Todo cuerpo $\mathbb{K}$ es un DE con función euclídea $f : \mathbb{K} \setminus \{0\} \longrightarrow \mathbb{N}_0$, $f(x) = 1$.

(3) Si $\mathbb{K}$ es un cuerpo, $\mathbb{K}[X]$ es un DE con función euclídea $f : \mathbb{K}[X] \setminus \{0\} \longrightarrow \mathbb{N}_0$, $f(p) = \deg(p)$.

Observación 3.2.3. En un DE arbitrario A, los elementos $q, r \in A$ del inciso (II) de la definición de función euclídea no son necesariamente únicos.

Proposición 3.2.4. *Sea A un DE. La condición (II) de la definición de función euclídea da lugar a un algoritmo (análogo al de Euclides en $\mathbb{Z}$) para el cálculo del* mcd *entre dos elementos $a, b \in A \setminus \{0\}$ por medio de divisiones sucesivas.*

En particular, si A es un DE entonces para todos $a, b \in A$ no nulos existe el $\mathrm{mcd}(a, b)$ *y es combinación lineal con coeficientes en A de a y b. Además, una escritura así del* $\mathrm{mcd}(a, b)$ *puede obtenerse del algoritmo de Euclides inducido por la función euclídea en A.*

Demostración.

Sean $a, b \in A \setminus \{0\}$.

$$a = b \cdot q_0 + r_0 \quad \text{con} \quad \big(r_0 = 0 \ \text{ó} \ f(r_0) < f(b)\big) \tag{0}$$

Si $r_0 \neq 0$:

$$b = r_0 \cdot q_1 + r_1 \quad \text{con} \quad \big(r_1 = 0 \ \text{ó} \ f(r_1) < f(r_0)\big) \tag{1}$$

Si $r_1 \neq 0$:

$$r_0 = r_1 \cdot q_2 + r_2 \quad \text{con} \quad \big(r_2 = 0 \ \text{ó} \ f(r_2) < f(r_1)\big) \tag{2}$$

$$\vdots$$

Si $r_k \neq 0$:

$$r_{k-1} = r_k \cdot q_{k+1} + r_{k+1} \quad \text{con} \quad \big(r_{k+1} = 0 \ \text{ó} \ f(r_{k+1}) < f(r_k)\big) \tag{k+1}$$

$$\vdots$$

Si $r_{n-1} \neq 0$:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \quad \text{con} \quad \big(r_n = 0 \ \text{ó} \ f(r_n) < f(r_{n-1})\big) \tag{n}$$

Si $r_n \neq 0$:

$$r_{n-1} = r_n \cdot q_{n+1} \tag{n+1}$$

Aquí r_n es el último resto no nulo, el cual existe ya que para todo $a \in A \setminus \{0\}$ se tiene $f(a) \in \mathbb{N}_0$, y a partir de las divisiones anteriores

$$f(b) > f(r_0) > f(r_1) > \ldots > f(r_k) > \cdots \geq 0,$$

por lo que en a lo sumo $f(b)$ pasos termina.

Veamos que r_n satisface la definición 2.3.1 de $\operatorname{mcd}(a, b)$. De la última igualdad (n+1) resulta que $r_n \mid r_{n-1}$. Luego de la igualdad (n):

$r_{n-1} = \underbrace{r_{n-1}}_{r_n \mid} \cdot q_n + \underbrace{r_n}_{r_n \mid} \implies r_n \mid r_{n-2}$.

Inductivamente, si $r_n \mid r_{k+1}$ y $r_n \mid r_k$, como $r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$ resulta $r_n \mid r_{k-1}$. Luego se tiene que $r_n \mid r_i$ para todo $i \in \{0, \ldots, n\}$. Así,

- A partir de la igualdad (1): $b = \underbrace{r_0}_{r_n \mid} \cdot q_1 + \underbrace{r_1}_{r_n \mid} \implies r_n \mid b$.
- Luego a partir de la igualdad (0): $a = \underbrace{b}_{r_n \mid} \cdot q_0 + \underbrace{r_0}_{r_n \mid} \implies r_n \mid a$.
- Si $c \in A$ satisface que $c \mid a$ y $c \mid b$, entonces $c \mid r_0 = a - b \cdot q_0$.

  Luego $c \mid r_1 = b - r_0 \cdot q_1$, y entonces también $c \mid r_2 = r_0 - r_1 \cdot q_2$.

  Inductivamente, sabiendo que $c \mid r_{k-1}$ y $c \mid r_k$ resulta $c \mid r_{k+1} = r_{k-1} - r_k \cdot q_{k+1}$.

  Repitiendo este proceso obtenemos de la igualdad (n) que $c \mid r_n = r_{n-2} - r_{n-1} \cdot q_n$.

□

Daremos a continuación un resultado para DE no triviales que será muy útil en el último capítulo de este trabajo.

Proposición 3.2.5. *Sea A un DE que no es un cuerpo con función euclídea $f : A\setminus\{0\} \longrightarrow \mathbb{N}_0$. Entonces, existe $p \in A$ primo tal que al considerar la proyección al cociente $\pi : A \longrightarrow {}^{A}\!\Big/\!_{\langle p\rangle}$ se tiene que $\pi\big(\mathcal{U}(A)\big) = \mathcal{U}\Big({}^{A}\!\Big/\!_{\langle p\rangle}\Big)$.*

Demostración.

Sea $S = \big\{f(a) : a \in A \setminus \{0\}, a \notin \mathcal{U}(A)\big\} \subseteq \mathbb{N}_0$. Entonces, $S \neq \varnothing$ ya que A no es un cuerpo, y entonces tiene mínimo. Sea $p \in A \setminus \{0\}, p \notin \mathcal{U}(A)$ tal que $f(p)$ es mínimo. Veamos que p es primo en A. Supongamos que no lo es, por lo que existen $a, b \in A$ tales que $p \mid a \cdot b$ pero $p \nmid a$ y $p \nmid b$.

Como A es un DE y $p \neq 0$, existen $q_a, r_a \in A$ tales que $a = q_a \cdot p + r_a$ con $r_a = 0$ ó $f(r_a) < f(p)$. Como $p \nmid a$, debe ser $r_a \neq 0$ y entonces $f(r_a) < f(p)$, por lo que $r_a \in \mathcal{U}(A)$ debido a la minimalidad de $f(p)$. Análogamente existen $q_b, r_b \in A$ tales que $b = q_b \cdot p + r_b$ con $r_b \in \mathcal{U}(A)$.

Luego:

$$\underbrace{a \cdot b}_{p\mid} = (q_a \cdot p + r_a) \cdot (q_b \cdot p + r_b) = \underbrace{\Big[q_a \cdot (q_b \cdot p + r_b) + r_a \cdot q_b\Big] \cdot p}_{p\mid} + r_a \cdot r_b\,,$$

y entonces $p \mid r_a \cdot r_b$. Pero $r_a, r_b \in \mathcal{U}(A)$, por lo que $r_a \cdot r_b \in \mathcal{U}(A)$ y resulta así $p \in \mathcal{U}(A)$, lo cual contradice la elección de p. Concluimos así que p es primo.

Sea $\pi : A \longrightarrow {}^{A}\!\Big/\!_{\langle p\rangle}$ la proyección al cociente y veamos que $\pi\big(\mathcal{U}(A)\big) = \mathcal{U}\Big({}^{A}\!\Big/\!_{\langle p\rangle}\Big)$.

($\subseteq$) Sean $\bar{y} \in \pi\big(\mathcal{U}(A)\big)$ y $u \in \mathcal{U}(A)$ tal que $\bar{y} = \pi(u)$.

Como π es morfismo de anillos, se tiene: $\bar{1} = \pi(1) = \pi(u \cdot u^{-1}) = \pi(u) \cdot \pi(u)^{-1}$, y resulta entonces que $\bar{y} = \pi(u) \in \mathcal{U}\Big({}^{A}\!\Big/\!_{\langle p\rangle}\Big)$.

($\supseteq$) Sean $\bar{x} \in \mathcal{U}\Big({}^{A}\!\Big/\!_{\langle p\rangle}\Big)$ y $x \in A$ tal que $\bar{x} = \pi(x)$. Notar que $\bar{x} \neq 0$ en ${}^{A}\!\Big/\!_{\langle p\rangle}$ ya que es una unidad. Como A es un DE y $p \in A \setminus \{0\}$, existen $q, r \in A$ tales que $x = q \cdot p + r$ con $r = 0$ ó $f(r) < f(p)$. Sin embargo, si fuese $r = 0$ se tendría que $x = q \cdot p \in \langle p\rangle$, y en consecuencia $\bar{x} = 0$ en ${}^{A}\!\Big/\!_{\langle p\rangle}$. Luego debe ser $r \neq 0$ con $f(r) < f(p)$, por lo que $r \in \mathcal{U}(A)$ por la minimalidad de $f(p)$, y entonces $\pi(r) \in \pi\big(\mathcal{U}(A)\big)$.

Finalmente, $\bar{x} = \pi(x) = \pi(q \cdot p + r) = \pi(r) \in \pi\big(\mathcal{U}(A)\big)$.

□

3.3. DE ⇒ DP ⇒ DFU ⇒ DF

Terminamos este capítulo con un teorema que será el que motiva el objeto de estudio de esta tesis: la relación entre los dominios considerados (DF, DFU, DP y DE).

Teorema 3.3.1. *Sea A un dominio íntegro. Entonces,*

$$A \text{ es } DE \underset{(1)}{\Longrightarrow} A \text{ es } DP \underset{(2)}{\Longrightarrow} A \text{ es } DFU \underset{(3)}{\Longrightarrow} A \text{ es } DF.$$

Demostración.

Veamos cada implicación.

(1) Sea A un DE con función euclídea $f : A \setminus \{0\} \longrightarrow \mathbb{N}_0$ y sea $I \trianglelefteq A$.

Si $I = \{0\} = \langle 0 \rangle$ es claramente principal. Supongamos entonces $I \neq \{0\}$, por lo que existe $a \in I \setminus \{0\}$. Luego el conjunto $M = \Big\{ f(a) : a \in I \setminus \{0\} \Big\} \subseteq \mathbb{N}_0$ es no vacío y entonces tiene mínimo.

Sea $x \in I \setminus \{0\}$ tal que $f(x)$ es mínimo. Veamos que $I = \langle x \rangle$.

($\supseteq$) Es inmediato ya que $x \in I \setminus \{0\}$.

($\subseteq$) Sea $y \in I$ y veamos que $y \in \langle x \rangle$. Como $x \neq 0$, por la definición de función euclídea existen $q, r \in A$ tales que $y = x \cdot q + r$ con $\big(r = 0 \text{ ó } f(r) < f(x)\big)$.

Luego como $x, y \in I$ resulta entonces que $r = y - x \cdot q \in I$, y por ende si fuese $r \neq 0$ tendríamos que $r \in I \setminus \{0\}$ con $f(r) < f(x)$, lo cual contradice la minimalidad de $f(x)$.

Concluimos así que debe ser $r = 0$, y entonces $y = x \cdot q \in \langle x \rangle$.

Así, $I = \langle x \rangle$ es principal.

(2) Si A es un DP, en particular todo ideal de A es finitamente generado, por lo que A es un dominio íntegro noetheriano. Luego por el teorema 2.1.7, A es un DF.

Así, para ver que A es un DFU, en virtud del teorema 2.2.3, basta ver que todo elemento irreducible en A es también primo.

Sea $q \in A$ irreducible y sean $a, b \in A$ tales que $q \mid a \cdot b$.

Si $q \mid a$ no hay nada que probar, así que supongamos $q \nmid a$. En consecuencia, $a \notin \langle q \rangle$ y por consiguiente $\langle q \rangle \subsetneq \langle q, a \rangle$. Como A es un DP, existe $c \in A$ tal que $\langle q, a \rangle = \langle c \rangle$, y por ende $\langle q \rangle \subsetneq \langle c \rangle$. De esto último resulta que $c \mid q$ pero $q \nmid c$ con q irreducible en A, por lo que $c \in \mathcal{U}(A)$ y entonces $\langle q, a \rangle = \langle c \rangle = A$.

Luego como $1 \in A = \langle q, a \rangle$, existen $s, t \in A$ tales que $1 = s \cdot q + t \cdot a$, y entonces $b = s \cdot \underbrace{(q \cdot b)}_{q \mid} + t \cdot \underbrace{(a \cdot b)}_{q \mid}$, por lo que $q \mid b$.

(3) Es inmediata de las definiciones de DFU y DF respectivamente.

□

Observación 3.3.2. Como consecuencia de las implicaciones probadas se tiene que tanto $\mathbb{Z}$ como $\mathbb{K}[X]$ son efectivamente DF, DFU y DP porque son DE.

A su vez, hemos probado en el teorema anterior que en todo DE y en todo DP es posible factorizar en irreducibles y de forma única salvo asociados y el orden de los factores. Más aún, las construcciones de DE y DP surgieron naturalmente al querer "recuperar" en algún sentido las propiedades más relevantes del mcd conocidas para $\mathbb{Z}$: la identidad de Bézout y el algoritmo de Euclides.

Eso nos conduce a una pregunta que responderemos a lo largo de los capítulos restantes de este trabajo: ¿qué ocurre con las implicaciones recíprocas del teorema 3.3.1?

Capítulo 4

Polinomios en $A[X]$ con A un DFU

El objetivo del presente capítulo es obtener una condición necesaria y suficiente para que la factorización en irreducibles en $A[X]$ sea posible y única, donde A será en principio un dominio íntegro. Más precisamente, probaremos que el anillo $A[X]$ es un DFU si y solo si A es un DFU. Procederemos luego a enunciar criterios clásicos para estudiar irreducibilidad en $A[X]$, y daremos también contraejemplos para las implicaciones recíprocas del teorema 3.3.1. Finalmente, introduciremos el concepto de resultante de dos polinomios en $A[X]$ junto a algunas de sus propiedades que serán fundamentales en el último capítulo de esta tesis.

4.1. Generalidades en $A[X]$, con A un anillo conmutativo y un dominio íntegro

Fijamos a continuación la notación que usaremos a lo largo de este capítulo.

Notación 4.1.1. Sea A un anillo conmutativo. Dada X una indeterminada sobre A, denotamos $A[X]$ al anillo de polinomios en la variable X con coeficientes en A.

Escribiremos $\mathrm{cp}(f)$ para indicar el coeficiente principal y $\deg(f)$ el grado de un polinomio $f \in A[X] \setminus \{0\}$.

Notación 4.1.2. Sea $m \in \mathbb{N}$. Notaremos $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ al vector formado por $\alpha_1, \ldots, \alpha_m$, y su longitud es $|\alpha| = \sum_{i=1}^{m} \alpha_i$.

Notación 4.1.3. Sea A un anillo conmutativo. Dadas $X_1, \ldots, X_n$ indeterminadas sobre A, el monomio de multiíndice $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ es $\underline{X}^{\alpha} := X_1^{\alpha_1} \ldots X_n^{\alpha_n}$.

Notación 4.1.4. Sea A un anillo conmutativo. Dadas $X_1, \ldots, X_n$ indeterminadas sobre A, denotamos $A[\underline{X}] = A[X_1, \ldots, X_n]$ al anillo de polinomios en n variables con coeficientes en A:

$$A[X_1, \ldots, X_n] = \left\{ \sum_{|\alpha| \leq d} c_\alpha \, \underline{X}^{\alpha} \;\; : \;\; d \in \mathbb{N}_0 \, , \; \alpha \in \mathbb{N}_0^n \, , \; c_\alpha \in A \right\}$$

Escribiremos $\deg(f)$ para referirnos al grado total de un polinomio $f \in A[\underline{X}] \setminus \{0\}$, es decir, $\deg(f) = \max\{|\alpha| : c_\alpha \neq 0 \text{ coeficiente de } f\}$, y para $i \in \{1, \dots, n\}$ usaremos $\deg_{X_i}(f)$ para indicar su grado como polinomio en la variable X_i, es decir, pensando $f \in (A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n])[X_i]$.

Procedemos ahora a recordar resultados preliminares sobre anillos de polinomios con coeficientes en un dominio íntegro.

Proposición 4.1.5. *Sea A un dominio íntegro y sean $f, g \in A[X]$. Entonces,*

(1) si $f + g \neq 0$, $\deg(f + g) \leq max\{\deg(f); \deg(g)\}$,

(2) si $f, g \neq 0$, entonces $f \cdot g \neq 0$, $\deg(f \cdot g) = \deg(f) + \deg(g)$ y $\operatorname{cp}(f \cdot g) = \operatorname{cp}(f) \operatorname{cp}(g)$,

(3) $\mathcal{U}(A[X]) = \mathcal{U}(A)$,

(4) $A[X]$ es un dominio íntegro.

Observación 4.1.6. Dado A un dominio íntegro, consideremos $\mathbb{K} = \operatorname{Frac}(A)$ y entonces $A[X] \subseteq \mathbb{K}[X]$. Luego dado $f \in A[X] \subseteq \mathbb{K}[X]$, existen $q_1, \dots, q_r \in \mathbb{K}[X]$ irreducibles tales que $f = \prod_{i=1}^{r} q_i$, y esta escritura es única salvo asociados ya que $\mathbb{K}[X]$ es un DFU.

¿Bajo qué condiciones podemos "recuperar" una factorización de f en $A[X]$ a partir de la obtenida en $\mathbb{K}[X]$ y que sea única salvo asociados?

Empecemos por observar que si $A[X]$ es un DFU y consideramos $f \in A[X]$ no nulo con $\deg(f) = 0$, $f \notin \mathcal{U}(A)$, entonces deben existir $q_1, \dots, q_r \in A[X]$ irreducibles tales que $f = \prod_{i=1}^{r} q_i$, y como $\deg(f) = 0$ debe ser $\deg(q_i) = 0$, o sea, $q_i \in A$ para todo $i \in \{1, \dots, r\}$.

Esto muestra que para que $A[X]$ pueda ser un DFU es condición necesaria que A sea un DFU.

4.2. Contenido de un polinomio y polinomio primitivo

Observación 4.2.1. Sean A un dominio íntegro, $a \in A \setminus \{0\}$ y $f = \sum_{i=0}^{d} a_i X^i \in A[X]$. Entonces, $a \mid f$ en $A[X]$ si y solo si $a \mid a_i$ en A para todo $i \in \{0, \dots, d\}$.

Dado A un DFU fijamos un sistema de representantes $\mathcal{P}$ de irreducibles (= primos) en A por cada clase de asociados y fijamos al $1 \in A$ como representante de $\mathcal{U}(A)$. Así, podemos calcular de forma unívoca el mcd de dos elementos en A no ambos nulos como vimos en la observación 2.3.3.

Definición 4.2.2. Sea A un DFU y sea $f = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$. Entonces,

1. El contenido de f es $\mathrm{cont}(f) = \mathrm{mcd}(a_d, \ldots, a_0) \in A$.
2. f se dice primitivo si $\mathrm{cont}(f) = 1$.

Observación 4.2.3. Sea A un DFU y sean $a \in A \setminus \{0\}$ y $f \in A[X] \setminus \{0\}$. Entonces,

(1) $\mathrm{cont}(a) \sim a$,

(2) $\mathrm{cont}(af) \sim a \cdot \mathrm{cont}(f)$,

(3) $\dfrac{f}{\mathrm{cont}(f)} \in A[X]$ es primitivo y por ende $f = \mathrm{cont}(f) \cdot \tilde{f}$ con $\tilde{f} \in A[X]$ primitivo,

(4) $a \mid f$ en $A[X] \Leftrightarrow a \mid \mathrm{cont}(f)$ en A.

Teorema 4.2.4 (Lema de Gauss)**.** *Sea A un DFU y sean $f, g \in A[X] \setminus \{0\}$. Entonces,*

(1) Si f, g son primitivos, $f \cdot g$ es primitivo.

(2) $\mathrm{cont}(f \cdot g) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.

Demostración.

(1) Sean $f = \sum_{i=0}^{d} a_i X^i, g = \sum_{j=0}^{e} b_j X^j$ en $A[X]$ ambos primitivos.

Consideremos $f \cdot g = \sum_{k=0}^{d+e} c_k X^k$, donde $c_k = \sum_{i+j=k} a_i \cdot b_j$, y veamos que es primitivo.

Sea $q \in A$ irreducible. Como f y g son ambos primitivos, sean $i_0 = \mín\{i \,/\, q \nmid a_i\}$ y $j_0 = \mín\{j \,/\, q \nmid b_j\}$ y definamos $k_0 = i_0 + j_0$. Veamos que $q \nmid c_{k_0}$.

Escribamos $c_{k_0} = \sum_{i+j=k_0} a_i \cdot b_j = a_{i_0} \cdot b_{j_0} + \sum_{\substack{i+j=k_0,\\ i \neq i_0,\ j \neq j_0}} a_i \cdot b_j$.

Como q es irreducible en A DFU, entonces q es primo, y por lo tanto como $q \nmid a_{i_0}$ y $q \nmid b_{j_0}$ resulta que $q \nmid a_{i_0} \cdot b_{j_0}$.

A su vez, dados i, j tales que $i \neq i_0$, $j \neq j_0$ y $i + j = k_0$, como $i_0 + j_0 = k_0$, debe ser $i < i_0$ o $j < j_0$. Por otro lado, por la minimalidad en la definición de i_0 y j_0 se tiene que si $i < i_0$ entonces $q \mid a_i$, y si $j < j_0$ entonces $q \mid b_j$.

Luego si $i + j = k_0$ con $i \neq i_0$ y $j \neq j_0$ entonces $q \mid a_i \cdot b_j$, y así:

$$c_{k_0} = \underbrace{a_{i_0} \cdot b_{j_0}}_{q \nmid} + \underbrace{\sum_{\substack{i+j=k_0,\\ i \neq i_0,\ j \neq j_0}} \underbrace{a_i \cdot b_j}_{q \mid}}_{q \mid} \Longrightarrow q \nmid c_{k_0}$$

Probamos entonces que dado cualquier elemento irreducible en A siempre hay algún coeficiente de $f \cdot g$ al que no divide, y por consiguiente $\mathrm{cont}(f \cdot g) \in A \setminus \{0\}$ no es divisible por ningún irreducible.

Así, $\mathrm{cont}(f \cdot g)$ debe ser una unidad de A y, por cómo fijamos los representantes por clases de asociados para el mcd, resulta entonces $\mathrm{cont}(f \cdot g) = 1$.

(2) Escribamos $f = \mathrm{cont}(f) \cdot \tilde{f}$ y $g = \mathrm{cont}(g) \cdot \tilde{g}$ con $\tilde{f}, \tilde{g} \in A[X]$ ambos primitivos. Luego:

$$\begin{aligned} \mathrm{cont}(f \cdot g) &= \mathrm{cont}\left(\underbrace{\mathrm{cont}(f) \cdot \mathrm{cont}(g)}_{\in A} \cdot \tilde{f} \cdot \tilde{g}\right) \\ &= \mathrm{cont}(f) \cdot \mathrm{cont}(g) \cdot \underbrace{\mathrm{cont}(\tilde{f} \cdot \tilde{g})}_{=1} \\ &= \mathrm{cont}(f) \cdot \mathrm{cont}(g). \end{aligned}$$

□

Corolario 4.2.5. *Sean A un DFU y $q \in A$. Entonces, q es irreducible (= primo) en A si y solo si q es primo en $A[X]$. En particular, todo q irreducible (= primo) en A es también irreducible en $A[X]$.*

Demostración.

($\Rightarrow$) Sean $f, g \in A[X]$ tales que $q \mid f \cdot g$ en $A[X]$. Luego, $q \mid \mathrm{cont}(f \cdot g) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ en A y en consecuencia como q es primo en A resulta $q \mid \mathrm{cont}(f)$ o bien $q \mid \mathrm{cont}(g)$ en A, de donde $q \mid f$ ó $q \mid g$ en $A[X]$ respectivamente.

($\Leftarrow$) Sean $a, b \in A$ tales que $q \mid ab$ en A. Luego $q \mid ab$ en $A[X]$, y como q es primo allí se sigue que $q \mid a$ o bien $q \mid b$ en $A[X]$, y por ende $q \mid a$ ó $q \mid b$ en A respectivamente.

□

Teorema 4.2.6 (Lema de Gauss II)**.** *Sean A un DFU y $\mathbb{K} = \mathrm{Frac}(A)$ y sea $f \in A[X]$ tal que existen $g, h \in \mathbb{K}[X]$ no constantes de manera que $f = g \cdot h$ en $\mathbb{K}[X]$. Entonces, existen $G, H \in A[X]$ tales que $f = G \cdot H$ en $A[X]$ con G asociado a g y H asociado a h en $\mathbb{K}[X]$. En particular, $\deg(G) = \deg(g)$ y $\deg(H) = \deg(h)$.*

Demostración.

Tenemos $f = g \cdot h$ en $\mathbb{K}[X]$ con $\deg(g), \deg(h) > 0$, $g, h \in \mathbb{K}[X]$.

Multiplicando por denominadores comunes $a, b \in A \setminus \{0\}$ de los coeficientes de g y h respectivamente obtenemos que $ag \in A[X]$ y $bh \in A[X]$.

Luego $abf = (ag) \cdot (bh)$ en $A[X]$, y entonces $\mathrm{cont}(abf) = \mathrm{cont}\big((ag) \cdot (bh)\big)$. Así,

$$\begin{aligned} ab\,\mathrm{cont}(f) \sim \mathrm{cont}(ag) \cdot \mathrm{cont}(bh) &\text{ en } A \\ \Rightarrow\ ab \mid \mathrm{cont}(ag) \cdot \mathrm{cont}(bh) &\text{ en } A \\ \Rightarrow\ \frac{\mathrm{cont}(ag) \cdot \mathrm{cont}(bh)}{ab} &\in A. \end{aligned}$$

En consecuencia, si escribimos $ag = \operatorname{cont}(ag) \cdot \widetilde{ag}$ y $bh = \operatorname{cont}(bh) \cdot \widetilde{bh}$, donde $\widetilde{ag}, \widetilde{bh} \in A[X]$ son ambos primitivos, se tiene que:

$$f = \frac{(ag)\cdot(bh)}{ab} = \underbrace{\frac{\operatorname{cont}(ag)\cdot\operatorname{cont}(bh)}{ab}}_{\in A} \cdot \underbrace{\widetilde{ag}}_{\in A[X]} \cdot \underbrace{\widetilde{bh}}_{\in A[X]} \quad \text{en } A[X].$$

Así, si definimos $G = \dfrac{\operatorname{cont}(ag)\cdot\operatorname{cont}(bh)}{ab} \cdot \widetilde{ag}$ y $H = \widetilde{bh}$, entonces

- $G, H \in A[X]$,
- $f = G \cdot H$,
- $H \sim h$ en $\mathbb{K}[X]$ ya que $H = \widetilde{bh} = \underbrace{\dfrac{b}{\operatorname{cont}(bh)}}_{\in \mathbb{K}} \cdot h$,
- $G \sim g$ en $\mathbb{K}[X]$ ya que $G = \dfrac{\operatorname{cont}(ag)\cdot\operatorname{cont}(bh)}{ab} \cdot \widetilde{ag} = \underbrace{\dfrac{\operatorname{cont}(bh)}{b}}_{\in \mathbb{K}} \cdot g$,

y por lo tanto $\deg(H) = \deg(h)$ y $\deg(G) = \deg(g)$. □

Corolario 4.2.7. *Si A es un DFU, $\mathbb{K} = \operatorname{Frac}(A)$ y $f \in A[X]$ con $\deg(f) > 0$ es reducible en $\mathbb{K}[X]$, entonces f también es reducible en $A[X]$.*

Observación 4.2.8. La implicación recíproca del corolario 4.2.7 no es cierta. Por ejemplo, el polinomio $f = 2X + 2 = 2 \cdot (X + 1)$ es reducible en $\mathbb{Z}[X]$ ya que $2 \notin \mathcal{U}(\mathbb{Z}) = \{\pm 1\}$ pero es irreducible en $\mathbb{Q}[X]$ por ser un polinomio de grado 1.

Sin embargo, si el polinomio es primitivo sí es cierto.

Teorema 4.2.9. *Sean A un DFU, $\mathbb{K} = \operatorname{Frac}(A)$ y $f \in A[X]$ primitivo con $\deg(f) > 0$. Entonces, f es irreducible en $A[X]$ si y solo si f es irreducible en $\mathbb{K}[X]$.*

Demostración.

($\Rightarrow$) Si f es irreducible en $A[X]$, como $\deg(f) > 0$, por el corolario 4.2.7 f resulta irreducible en $\mathbb{K}[X]$.

($\Leftarrow$) Supongamos que f es reducible en $A[X]$. Luego existen $g, h \in A[X] \setminus \mathcal{U}(A)$ tales que $f = g \cdot h$, y como f es primitivo debe ser $\deg(g), \deg(h) > 0$.

Así $f = g \cdot h$ es también una factorización propia de f en $\mathbb{K}[X]$ y f resulta reducible en $\mathbb{K}[X]$.

□

Proposición 4.2.10. *Si A es un DFU, $\mathbb{K} = \operatorname{Frac}(A)$, $f, g \in A[X]$ con g primitivo y $g \mid f$ en $\mathbb{K}[X]$, entonces $g \mid f$ en $A[X]$.*

Demostración.

Como $g \mid f$ en $\mathbb{K}[X]$, existe $h \in \mathbb{K}[X]$ tal que $f = g \cdot h$, siendo g primitivo en $A[X]$. Veamos que en realidad $h \in A[X]$.

Dado que $f \in A[X]$, por el Lema de Gauss II 4.2.6 existen $G, H \in A[X]$ tales que $f = G \cdot H$ y $G \sim g$ en $\mathbb{K}[X]$.

Escribamos $G = \frac{a}{b} \cdot g$ con $a, b \in A$ y, como A es un DFU, podemos tomar a y b con $\mathrm{mcd}(a, b) = 1$. Luego tenemos $bG = ag$ en $A[X]$, y como g es primitivo y $\mathrm{mcd}(a, b) = 1$ resulta entonces que $a \mid \mathrm{cont}(G)$ y que $b \in \mathcal{U}(A)$ pues $b \mid \mathrm{cont}(g) = 1$. Sin pérdida de generalidad podemos asumir $b = 1$, y así $G = ag$.

Luego, $f = G \cdot H = (aH) \cdot g$ en $A[X]$, y como también $f = g \cdot h$ se concluye que $h = aH \in A[X]$. □

4.3. Factorización en $A[X]$

Comenzaremos esta sección dando una caracterización de los irreducibles en $A[X]$ con A un DFU.

Teorema 4.3.1. *Sea A un DFU con $\mathbb{K} = \mathrm{Frac}(A)$ y sea $f \in A[X]$. Entonces, f es irreducible en $A[X]$ si y solo si f satisface alguna de las siguientes condiciones:*

(I) *$f \in A \setminus \{0\}$ (o sea, $\deg(f) = 0$) y f es irreducible en A.*

(II) *$\deg(f) > 0$, f es primitivo y f es irreducible como polinomio en $\mathbb{K}[X]$.*

Demostración.

($\Leftarrow$) Los polinomios que satisfacen (I) son irreducibles en $A[X]$ por el corolario 4.2.5, mientras que aquellos que satisfacen (II) son irreducibles en $A[X]$ por el teorema 4.2.9.

($\Rightarrow$) Sea $f \in A[X]$ irreducible. Veamos que f satisface (I) ó (II).

Como f es irreducible en $A[X]$ entonces $f \notin \mathcal{U}(A)$, $f \neq 0$.

Si $\deg(f) = 0$ tenemos que $f \in A$. Supongamos que f es reducible en A.

Como A es un DFU, sea $q \in A$ irreducible tal que $q \not\sim f$ y $q \mid f$ en A. En particular, tendríamos que $q \mid f$ en $A[X]$ con $q \not\sim f$ y, además, por el corolario 4.2.5 q sería irreducible en $A[X]$, lo cual es absurdo. Luego f debe ser irreducible en A y entonces satisface (I).

Si $\deg(f) > 0$, como f es irreducible en $A[X]$ debe ser entonces f primitivo (ya que si no tendríamos una factorización propia $f = \mathrm{cont}(f) \cdot \tilde{f}$ con $\tilde{f} \in A[X]$ primitivo) y Luego por el teorema 4.2.9, f resulta irreducible en $\mathbb{K}[X]$. Así, f satisface (II).

□

Teorema 4.3.2. *Sean A un DFU y $f \in A[X]$. Si f es irreducible en $A[X]$, entonces f es primo en $A[X]$.*

Demostración.

Si f es irreducible en $A[X]$, por el teorema 4.3.1, hay dos casos posibles:

- Si $f \in A \setminus \{0\}$ (o sea, $\deg(f) = 0$) y f es irreducible en A:

  Por el corolario 4.2.5, f es primo en $A[X]$.

- Si $\deg(f) > 0$, f es primitivo y f es irreducible como polinomio en $\mathbb{K}[X]$:

  Sean $g, h \in A[X]$ tales que $f \mid g \cdot h$ en $A[X]$. En particular, $f \mid g \cdot h$ en $\mathbb{K}[X]$, y como f es irreducible en $\mathbb{K}[X]$ DFU, f es primo allí.

  Así, $f \mid g \cdot h \underset{\substack{f \text{ primo} \\ \text{en } \mathbb{K}[X]}}{\Longrightarrow} f \mid g$ ó $f \mid h$ en $\mathbb{K}[X]$.

  Si $f \mid g$ en $\mathbb{K}[X]$, como $f, g \in A[X]$ y f es primitivo, entonces por la proposición 4.2.10, $f \mid g$ en $A[X]$. Análogamente, si $f \mid h$ en $\mathbb{K}[X]$ resulta $f \mid h$ en $A[X]$.

  Luego f es primo en $A[X]$.

□

Procedemos ahora a enunciar el teorema principal de esta sección.

Teorema 4.3.3. *Sea A un dominio íntegro. Entonces, $A[X]$ es un DFU si y solo si A es un DFU.*

Demostración.
($\Rightarrow$) Sea $a \in A \setminus \{0\}$, $a \notin \mathcal{U}(A)$. Pensemos $a \in A[X]$ como un polinomio de grado 0, donde se factoriza:

$$a = \prod_{i=1}^{r} q_i \quad \textit{con } q_i \textit{ irreducible en } A[X] \textit{ para todo } i \in \{1, \dots, r\}.$$

Como $\deg(a) = 0$, debe ser $\deg(q_i) = 0$ para todo $i \in \{1, \dots, r\}$. En virtud del teorema 4.3.1, todos los q_i son irreducibles en A y obtenemos una factorización de a como producto de irreducibles en A. Esto prueba que A es un DF.

Para la unicidad, si en A tuviésemos dos factorizaciones como producto de irreducibles del elemento a, entonces también tendríamos dos factorizaciones en $A[X]$, lo cual contradice que $A[X]$ sea un DFU.

($\Leftarrow$) Por el teorema 4.3.2 ya sabemos que como A es un DFU entonces en $A[X]$ se cumple que todo elemento irreducible es también primo. Luego por el teorema 2.2.3, basta ver que $A[X]$ es un DF.

Sea $f \in A[X] \setminus \{0\}, f \notin \mathcal{U}(A[X]) = \mathcal{U}(A)$. Veamos que f se puede escribir como producto de irreducibles en $A[X]$, los cuales sabemos cómo son en virtud de la caracterización dada en el teorema 4.3.1.

Escribamos $f = \operatorname{cont}(f) \cdot \tilde{f}$ con $\tilde{f} \in A[X]$ primitivo.

Como $\operatorname{cont}(f) \in A$ que es un DFU, factorizamos como producto de irreducibles: $\operatorname{cont}(f) = \prod_{i=1}^{r} q_i$ con q_i irreducible en A y por ende en $A[X]$ para todo $i \in \{1, \dots, r\}$.

A su vez, consideremos $\mathbb{K} = \mathrm{Frac}(A)$ y pensemos $\tilde{f} \in \mathbb{K}[X]$. Como $\mathbb{K}[X]$ es un DFU, factorizamos $\tilde{f}$ allí como producto de irreducibles:

$$\tilde{f} = \prod_{j=1}^{s} p_j \quad \text{con } p_j \text{ irreducible en } \mathbb{K}[X] \text{ para todo } j \in \{1, \dots, s\}.$$

Por el Lema de Gauss II 4.2.6, para cada $j \in \{1, \dots, s\}$ existe $P_j \in A[X]$ tal que $p_j \sim P_j$ en $\mathbb{K}[X]$, por lo que P_j es irreducible en $\mathbb{K}[X]$, y además $\tilde{f} = \prod_{j=1}^{s} P_j$. Así, dado $j \in \{1, \dots, s\}$, como $P_j \mid \tilde{f}$ en $A[X]$ y $\tilde{f}$ es primitivo, P_j resulta primitivo. Luego P_j es irreducible en $A[X]$ y se tiene entonces una escritura

$$f = \mathrm{cont}(f) \cdot \tilde{f} = \prod_{i=1}^{r} q_i \cdot \prod_{j=1}^{s} P_j$$

como producto de irreducibles en $A[X]$.

□

Corolario 4.3.4.

(1) Sabemos por el Teorema Fundamental de la Aritmética que $\mathbb{Z}$ es un DFU, con lo cual $\mathbb{Z}[X]$ resulta un DFU.

(2) Si A es un DFU, inductivamente $A[X_1, \dots, X_n]$ resulta un DFU. En particular, para cualquier cuerpo $\mathbb{K}$ se tiene que $\mathbb{K}[X_1, \dots, X_n]$ es un DFU.

Observación 4.3.5. En virtud del teorema anterior y del corolario 2.3.3 se tiene que si A es un DFU entonces dados dos polinomios $f, g \in A[X]$ no ambos nulos siempre existe $\mathrm{mcd}(f, g) \in A[X]$.

Damos por último un resultado importante sobre la existencia de factorización en $A[X]$ cuando A no es necesariamente un DFU.

Teorema 4.3.6 (Teorema de la Base de Hilbert)**.** *Sea A un anillo conmutativo. Entonces, A es noetheriano si y solo si $A[X]$ es noetheriano.*

Demostración.

($\Rightarrow$) Sea $I \trianglelefteq A[X]$ y veamos que es finitamente generado.

Si $I = \{0\}$ no hay nada que probar. Consideremos entonces $I \neq \{0\}$ y supongamos que no es finitamente generado. Sea $f_1 \in I$ de grado mínimo y sea $a_1 = \mathrm{cp}(f_1) \in A$. Como I no es finitamente generado, consideremos $f_2 \in I \setminus \langle f_1 \rangle$ de grado mínimo y sea $a_2 = \mathrm{cp}(f_2) \in A$. Notar que por las definiciones de f_1 y f_2 resulta $\deg(f_1) \leq \deg(f_2)$. A su vez, como I no es finitamente generado, podemos tomar $f_3 \in I \setminus \langle f_1, f_2 \rangle$ de grado mínimo y considerar $a_3 = \mathrm{cp}(f_3) \in A$, y resulta entonces $\deg(f_1) \leq \deg(f_2) \leq \deg(f_3)$.

Inductivamente obtenemos:

- Una sucesión $(I_n)_{n\in\mathbb{N}}$ de ideales de $A[X]$ que es ascendente, donde $I_n = \langle f_1, \ldots, f_n\rangle \subseteq I$ y $f_{n+1} \in I \setminus I_n$ es de grado mínimo para todo $n \in \mathbb{N}$.

  Además, si llamamos $d_n = \deg(f_n)$ resulta que $d_n \leq d_{n+1}$ para todo $n \in \mathbb{N}$.

- Una sucesión $(J_n)_{n\in\mathbb{N}}$ de ideales de A que es ascendente, donde $J_n = \langle a_1, \ldots, a_n\rangle$, siendo $a_n = \mathrm{cp}(f_n)$.

Como A es noetheriano, por el teorema 2.1.6, la sucesión ascendente $(J_n)_{n\in\mathbb{N}}$ se estaciona: existe $N \in \mathbb{N}$ tal que $J_n = J_N = \langle a_1, \ldots, a_N\rangle$ para todo $n \geq N$.

Luego como $J_{N+1} = J_N$, existen $b_1, \ldots, b_N \in A$ tales que $a_{N+1} = \sum_{j=1}^{N} b_j \cdot a_j$.

Por otro lado, escribamos $f_{N+1} = a_{N+1}X^{d_{N+1}} + \text{“}\textit{términos de menor grado}\text{”}$, y definamos para cada $j \leq N$ el polinomio $g_j = b_j X^{d_{N+1}-d_j} \cdot f_j$.

Así, $\deg(g_j) = d_{N+1} = \deg(f_{N+1})$ y $\mathrm{cp}(g_j) = b_j \cdot a_j$ para todo $j \leq N$, por lo cual

$$\begin{aligned}\sum_{j=1}^{N} g_j &= \sum_{j=1}^{N}(a_j \cdot b_j)X^{d_{N+1}} + \text{términos de menor grado}\\ &= a_{N+1}X^{d_{N+1}} + \text{términos de menor grado}\end{aligned}$$

Como $\sum_{j=1}^{N} g_j = \sum_{j=1}^{N}(b_j X^{d_{N+1}-d_j}) \cdot f_j \in I_N \subseteq I$ pero $f_{N+1} \in I \setminus I_N$, resulta entonces que $f_{N+1} - \sum_{j=1}^{N} g_j \in I \setminus I_N$ y tiene grado menor estricto al de f_{N+1} (ya que se cancelan los monomios de grado d_{N+1}). Esto es absurdo ya que el polinomio f_{N+1} era un polinomio de grado mínimo en $I \setminus I_N$. Luego I debe ser finitamente generado.

($\Leftarrow$) Sea $J \trianglelefteq A$. Veamos que J es finitamente generado.

Consideremos $I = \left\{ \sum_{i=0}^{d} a_i X^i \ : \ d \in \mathbb{N}_0 \ , \ a_i \in J \ , \ 0 \leq i \leq d \right\}$, que resulta un ideal de $A[X]$.

Como $A[X]$ es noetheriano, existen $f_1, \ldots, f_s \in I$ tales que $I = \langle f_1, \ldots, f_s\rangle$.

Veamos que $J = \langle f_1(0), \ldots, f_s(0)\rangle$.

($\supseteq$) Como $f_1, \ldots, f_s \in I$, es claro que $f_1(0), \ldots, f_s(0) \in J$ pues son sus términos independientes.

($\subseteq$) Sea $a \in J$ y pensémoslo como un polinomio constante en $A[X]$. Luego $a \in I$ y entonces existen polinomios $g_1, \ldots, g_s \in A[X]$ tales que $a = \sum_{j=1}^{s} g_j \cdot f_j$

$$\Rightarrow a = \sum_{j=1}^{s} g_j(0) \cdot f_j(0) \in \langle f_1(0), \ldots, f_s(0)\rangle. \qquad \square$$

Corolario 4.3.7.

1 *Si A es un DP entonces es un dominio íntegro noetheriano, y por lo tanto $A[X]$ también es un dominio íntegro noetheriano. En particular, $\mathbb{Z}[X]$ es un dominio íntegro noetheriano.*

2 *Si A es un dominio íntegro noetheriano, inductivamente $A[X_1, \ldots, X_n]$ es también un dominio íntegro noetheriano y entonces, por el teorema 2.1.7, es un DF. En particular, dado $\mathbb{K}$ un cuerpo arbitrario, como $\mathbb{K}$ es un DP, $\mathbb{K}[X_1, \ldots, X_n]$ resulta un dominio íntegro noetheriano.*

4.4. Criterios de irreducibilidad en $A[X]$

Daremos a continuación algunas propiedades y resultados sobre irreducibilidad en $A[X]$ con A un DFU.

Teorema 4.4.1 (Gauss). *Sean A un DFU con $\mathbb{K} = \mathrm{Frac}(A)$ y $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ de grado positivo con $a_0 \neq 0$. Si $\frac{\alpha}{\beta} \in \mathbb{K}$ con $\alpha, \beta \in A, \mathrm{mcd}(\alpha, \beta) = 1$ es una raíz de f, entonces $\alpha \mid a_0$ y $\beta \mid a_d$. En particular, si $a_d = \mathrm{cp}(f) \in \mathcal{U}(A)$, entonces las raíces de f en $\mathbb{K}$ pertenecen a A.*

Demostración.

Como $0 = f\left(\frac{\alpha}{\beta}\right) = \sum_{i=0}^{d} a_i \cdot \frac{\alpha^i}{\beta^i}$ en $\mathbb{K}$, multiplicando por β^d obtenemos la igualdad $\sum_{i=0}^{d} a_i \alpha^i \beta^{d-i} = 0$ en A. Así, como $\beta \mid a_i \alpha^i \beta^{d-i}$ para todo $0 \leq i < d$ y $\beta \mid 0 = \sum_{i=0}^{d} a_i \alpha^i \beta^{d-i}$ resulta entonces que $\beta \mid a_d \alpha^d$, y por lo tanto $\beta \mid a_d$ ya que $\mathrm{mcd}(\alpha, \beta) = 1$.

Análogamente, como $\alpha \mid a_i \alpha^i \beta^{d-i}$ para todo $0 < i \leq d$ y $\alpha \mid 0 = \sum_{i=0}^{d} a_i \alpha^i \beta^{d-i}$ con $\mathrm{mcd}(\alpha, \beta) = 1$, se concluye que $\alpha \mid a_0$.

□

Observación 4.4.2. Si A es un DFU con $\mathbb{K} = \mathrm{Frac}(A)$ y $f \in A[X] \setminus \{0\}$ es primitivo y de grado positivo, por el teorema 4.2.9, sabemos que f es irreducible en $A[X]$ si y solo si f es irreducible en $\mathbb{K}[X]$.

Por otro lado, sabemos que $f \in \mathbb{K}[X]$ admite un factor de grado 1 en su factorización en irreducibles si y solo si f tiene alguna raíz en $\mathbb{K}$.

Así, la propiedad anterior junto al Lema de Gauss II 4.2.6 nos muestra cómo saber si $f \in A[X] \setminus \{0\}$ primitivo y de grado positivo admite un factor de grado 1 o no en $A[X]$.

Teorema 4.4.3 (Eisenstein). *Sea A un DFU y sea $f = \sum_{k=0}^{d} a_k X^k \in A[X]$ primitivo y de grado positivo. Si existe $p \in A$ irreducible (= primo) que satisface simultáneamente que*

- $p \mid a_i\ ,\ \ \forall\, 0 \leq k \leq d-1$
- $p \nmid a_d$
- $p^2 \nmid a_0$

entonces f es irreducible en $A[X]$.

Demostración.

Supongamos que f es reducible en $A[X]$ teniendo presente que f no puede tener factores constantes ya que es primitivo. Escribamos entonces $f = g \cdot h$ con $g, h \in A[X]$, con $0 < \deg(g), \deg(h) < \deg(f)$.

Así, si $g = \sum_{i=0}^{r} b_i X^i$ y $h = \sum_{j=0}^{s} c_j X^j$ donde $r = \deg(g)$ y $s = \deg(h)$, entonces para todo $k \in \{0, \ldots, d\}$ se tiene que $a_k = \sum_{i+j=k} b_i c_j$.

Como $p \mid a_0 = b_0 \cdot c_0$ y p es primo, debe ser $p \mid b_0$ ó $p \mid c_0$ pero no a ambos ya que $p^2 \nmid a_0$. Sin pérdida de generalidad, supongamos que $p \mid b_0$ y $p \nmid c_0$.

Si fuese que $p \mid b_i$ para todo $0 \leq i \leq r$, por la observación 4.2.1 tendríamos que $p \mid g$ en $A[X]$ y entonces $p \mid f$ siendo $p \in A$ irreducible y f primitivo, lo cual es absurdo. Luego algún coeficiente de g no debe ser divisible por p.

Sea $\ell = \min\{i : p \nmid b_i\}$. Como $p \mid b_0$ debe ser $\ell > 0$, y entonces:

$$a_\ell = \sum_{i+j=\,\ell} b_i c_j = \sum_{i=0}^{\ell} b_i c_{\ell-i} = \underbrace{\underbrace{b_\ell}_{p\nmid} \cdot \underbrace{c_0}_{p\nmid}}_{p\nmid} + \underbrace{\sum_{i=0}^{\ell-1} \underbrace{b_i}_{p\mid} \cdot c_{\ell-i}}_{p\mid} \implies p \nmid a_\ell$$

Esto es absurdo pues $\ell \leq \deg(g) < \deg(f) = d$ y por hipótesis entonces $p \mid a_\ell$.

□

Observación 4.4.4. Si f no es primitivo pero satisface las demás hipótesis del criterio de Eisenstein, el teorema permite concluir que f es irreducible en $\mathbb{K}[X]$ (ya que podemos escribir $f = \mathrm{cont}(f) \cdot \tilde{f}$ con $\tilde{f} \in A[X]$ primitivo y usar Eisenstein con $\tilde{f}$).

Proposición 4.4.5. *Sean A un DFU y $p \in A[X]$ de grado positivo. Sea $f \in A[X]$ y definamos $F \in A[X]$ como $F(X) = f\big(p(X)\big)$. Si F es irreducible en $A[X]$, entonces f también es irreducible en $A[X]$.*

Demostración.

Supongamos que f es reducible en $A[X]$ y escribamos $f = g \cdot h$ con $g, h \in A[X] \setminus \mathcal{U}(A)$. Luego especializando en $p(X)$ obtenemos que

$$F(X) = f\big(p(X)\big) = \underbrace{g\big(p(X)\big)}_{\in A[X]\setminus\mathcal{U}(A)} \cdot \underbrace{h\big(p(X)\big)}_{\in A[X]\setminus\mathcal{U}(A)},$$

de donde concluimos que F es reducible en $A[X]$.

□

Damos a continuación un criterio que involucra el uso de ideales y la proyección al cociente.

Proposición 4.4.6. *Sean A un DFU, I un ideal primo de A y $\pi_I : A \longrightarrow {}^{A}\!/_{I}$, $a \mapsto \overline{a} = \pi_I(a)$, la proyección al cociente. Sea $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ primitivo y de grado positivo con $\mathrm{cp}(f) = a_d \notin I$ y consideremos $\bar{f} = \sum_{i=0}^{d} \overline{a_i} X^i \in \left({}^{A}\!/_{I}\right)[X]$. Si $\bar{f}$ es irreducible en $\left({}^{A}\!/_{I}\right)[X]$, entonces f es irreducible en $A[X]$.*

Demostración.

Como $I \trianglelefteq A$ es primo, entonces ${}^{A}\!/_{I}$ es un dominio íntegro. Supongamos que f es reducible en $A[X]$, teniendo presente que f no tiene factores constantes por ser primitivo:

$$f = g \cdot h \text{ con } g, h \in A[X],\ 0 < \deg(g), \deg(h) < \deg(f).$$

Así, si $g = \sum_{i=0}^{r} b_i X^i$ y $h = \sum_{j=0}^{s} c_j X^j$ donde $r = \deg(g)$ y $s = \deg(h)$, se tiene:

$$b_r \cdot c_s = \mathrm{cp}(g) \cdot \mathrm{cp}(h) = \mathrm{cp}(f) = a_d \notin I,$$

por lo que $\overline{b_r} \cdot \overline{c_s} = \overline{a_d} \neq 0$ en ${}^{A}\!/_{I}$, y entonces $\overline{b_r} \neq 0$ y $\overline{c_s} \neq 0$. En consecuencia, si definimos $\bar{g} = \sum_{i=0}^{r} \overline{b_i} X^i$ y $\bar{h} = \sum_{j=0}^{s} \overline{c_j} X^j$ entonces $\deg(\bar{g}) = \deg g$ y $\deg(\bar{h}) = \deg(h)$, y luego $\bar{f} = \bar{g} \cdot \bar{h}$ es una factorización propia de $\bar{f}$ en $\left({}^{A}\!/_{I}\right)[X]$.

□

Recordamos por último un resultado sobre cocientes de un anillo noetheriano que usaremos a continuación.

Proposición 4.4.7. *Sean A un anillo conmutativo e I un ideal de A. Si A es noetheriano, entonces ${}^{A}\!/_{I}$ es noetheriano.*

Demostración.

Sea $\pi_I : A \longrightarrow {}^{A}\!/_{I}$ la proyección al cociente, $a \mapsto \overline{a} = \pi_I(a)$. A partir de la proposición 1.1.14, se tiene la correspondencia:

$$\begin{aligned} \left\{J \trianglelefteq A : I \subseteq J\right\} &\longleftrightarrow \left\{\overline{J} \trianglelefteq {}^{A}\!/_{I}\right\} \\ J &\longrightarrow \pi_I(J) =: {}^{J}\!/_{I} \\ \pi_I^{-1}\left(\overline{J}\right) &\longleftarrow \overline{J} \end{aligned}$$

Sea $\overline{J} \trianglelefteq {}^{A}\!/_{I}$ y tomemos $J \trianglelefteq A$ con $I \subseteq J$ tal que $\overline{J} = {}^{J}\!/_{I}$. Como A es noetheriano, el ideal es finitamente generado: existen $a_1, \ldots, a_n \in A$ tales que $J = \langle a_1, \ldots, a_n \rangle$. Veamos que $\overline{J} = \langle \overline{a_1}, \ldots, \overline{a_n} \rangle$.

($\supseteq$) Vale ya que $\overline{a_i} \in \overline{J}$ pues $a_i \in J$ para todo $i \in \{1, \ldots, n\}$.

($\subseteq$) Sea $\overline{x} \in \overline{J}$ y tomemos $x \in J$ representante de clase. Como $J = \langle a_1, \ldots, a_n \rangle$, existen $r_1, \ldots, r_n \in A$ tales que $x = \sum_{i=1}^{n} r_i a_i$, y entonces $\overline{x} = \sum_{i=1}^{n} \underbrace{\overline{r_i}}_{\in {}^{A}\!/_{I}} \cdot \overline{a_i} \in \langle \overline{a_1}, \ldots, \overline{a_n} \rangle$.

Luego $\overline{J} = \langle \overline{a_1}, \ldots, \overline{a_n} \rangle$ es finitamente generado.

□

4.5. Contraejemplos: DF $\not\Rightarrow$ DFU $\not\Rightarrow$ DP $\not\Rightarrow$ DE

Nos proponemos ahora exhibir contraejemplos de las implicaciones recíprocas del teorema 3.3.1.

Ejemplo 4.5.1. El dominio íntegro $\mathbb{Z}[i\sqrt{5}]$ es un DF que no es DFU.

Demostración.

En virtud de lo probado en proposición 2.1.10, como exhibimos un elemento irreducible que no es primo, por el teorema 2.2.3, $\mathbb{Z}[i\sqrt{5}]$ no puede ser un DFU.

Para ver que sí es un DF, por el teorema 2.1.7 basta probar que $\mathbb{Z}[i\sqrt{5}]$ es noetheriano.

Sea $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i\sqrt{5}]$ el morfismo de anillos $\varphi(g) = g(i\sqrt{5})$, que es claramente un epimorfismo. Veamos que $\mathrm{Ker}(\varphi) = \langle X^2 + 5 \rangle$. En efecto, $\varphi(X^2 + 5) = 0$ y si $g \in \mathbb{Z}[X]$ con $\varphi(g) = 0$ resulta entonces que $i\sqrt{5}$ es una raíz de g, por lo que $X^2 + 5 \mid g$ en $\mathbb{Z}[X]$.

Por el primer teorema de isomorfismo de Noether 1.1.13 se tiene que $\mathbb{Z}[i\sqrt{5}] \simeq {}^{\mathbb{Z}[X]}\!/_{\langle X^2+5 \rangle}$, que resulta noetheriano por la proposición 4.4.7 ya que $\mathbb{Z}[X]$ lo es por lo visto en el corolario 4.3.7.

□

Ejemplo 4.5.2. El dominio íntegro $\mathbb{Z}[X]$ es un DFU que no es DP.

Demostración.

Ya vimos en el corolario 4.3.4 que $\mathbb{Z}[X]$ es un DFU.

Para ver que no es un DP basta ver que el ideal $I = \langle 2, X\rangle$ no es principal. Notar que $\mathrm{mcd}(2, X) = 1$ ya que ambos son irreducibles no asociados en $\mathbb{Z}[X]$.

Supongamos que I sí es principal. Luego existe $f \in \mathbb{Z}[X]$ tal que $\langle 2, X\rangle = \langle f\rangle$. Por un lado, existen entonces $g, h \in \mathbb{Z}[X]$ tales que $f = g \cdot 2 + h \cdot X$. Por otro lado, debe ocurrir que $f \mid 2$ y $f \mid X$ en $\mathbb{Z}[X]$, con lo cual $f \mid \mathrm{mcd}(2, X) = 1$ y por ende $f = \pm 1$.

Así, $\pm 1 = g \cdot 2 + h \cdot X$ y entonces se tiene que

$$\pm 1 = g(0) \cdot 2 + h(0) \cdot 0 \quad \Longleftrightarrow \quad \pm 1 = \underbrace{g(0)}_{\in \mathbb{Z}} \cdot 2\,,$$

lo cual es absurdo. □

Observación 4.5.3. El ejemplo anterior nos muestra que un DFU arbitrario el mcd de dos elementos no ambos nulos no siempre se puede escribir como combinación de tales elementos con coeficientes en el DFU considerado.

Concluimos entonces que en un DFU el mcd siempre existe pero no siempre satisface la identidad de Bézout.

Con respecto a la última de las implicaciones mencionadas al comienzo de este capítulo, es sabido que un DP no siempre es un DE. Presentamos a continuación el conocido ejemplo de este hecho.

Ejemplo 4.5.4. El dominio íntegro $\mathbb{Z}\left[\dfrac{1 + i\sqrt{19}}{2}\right]$ es un DP que no es DE.

Luego de trabajos precursores de Richard Dedekind y Helmut Hasse, el matemático Theodore Motzkin da una prueba en [Motz49] de la afirmación anterior sin mayores detalles y de manera no elemental. Demostraciones meticulosas pueden verse en [Wil73] y [Cam88]. Aquí no trataremos ese ejemplo. En su lugar exhibiremos en el Capítulo 5, como resultado principal de esta tesis, otro ejemplo de DP que no es un DE .

Finalizamos esta sección con un ejemplo que muestra que la condición de noetherianidad no es necesaria para que haya factorización en irreducibles.

Ejemplo 4.5.5. El dominio íntegro $A = \mathbb{C}[X_n : n \in \mathbb{N}] = \bigcup_{n\in\mathbb{N}} \mathbb{C}[X_1, \ldots, X_n]$ es un DF que no es noetheriano.

Demostración.

- A no es noetheriano:

  Supongamos que sí lo es y consideremos la sucesión ascendente $(I_n)_{n\in\mathbb{N}}$ de ideales de A definida por $I_n = \langle X_1, \ldots, X_n\rangle$. Luego como supusimos que A es noetheriano, por el teorema 2.1.6, la sucesión se estaciona: existe $N \in \mathbb{N}$ tal que $I_n = I_N$ para todo $n \geq N$. En particular, $I_{N+1} = I_N$ y entonces $X_{N+1} \in I_N = \langle X_1, \ldots, X_N\rangle$.

Así, existen $g_1, \ldots, g_N \in A$ tales que $X_{N+1} = \sum_{i=1}^{N} g_i \cdot X_i$.

Como cada g_i tiene finitas variables, si listamos todas las que aparecen en la igualdad anterior $\{X_1, \ldots, X_N, X_{N+1}, \ldots, X_d\}$ obtenemos una igualdad en $\mathbb{C}[X_1, \ldots, X_d]$.

Luego si evaluamos en $e_{N+1} = (0, \ldots, 0, \underbrace{1}_{N+1}, 0, \ldots, 0) \in \mathbb{C}^d$ obtenemos que:

$$1 = \sum_{i=1}^{N} g_i(e_{N+1}) \cdot 0 = 0,$$

que es claramente absurdo.

- A es un DF:

  Es inmediato que $\mathcal{U}(A) = \mathbb{C} \setminus \{0\}$.

  Sea $f \in A \setminus \mathbb{C}$. Luego existe $k \in \mathbb{N}$ tal que $f \in \mathbb{C}[X_1, \ldots, X_k]$ que es un DFU, y como $f \notin \mathbb{C}$, f se factoriza en irreducibles allí. Basta ver entonces que si $g \in \mathbb{C}[X_1, \ldots, X_k]$ es irreducible, entonces g es también irreducible en A.

  Sea $g \in \mathbb{C}[X_1, \ldots, X_k]$ irreducible y supongamos que $h \in A$ satisface $h \mid g$. Luego podemos escribir $g = h \cdot p$ con $p \in A$.

  Consideremos cualquier variable $Y \in \{X_n : n > k\}$, y entonces $0 = \deg_Y(g) = \deg_Y(h) + \deg_Y(p)$ igualdad en $\mathbb{N}_0$, de donde concluimos que $0 = \deg_Y(h) = \deg_Y(p)$. Así, debe ser $h \mid g$ en $\mathbb{C}[X_1, \ldots, X_k]$, y como g es irreducible allí resulta que $h \sim g$ ó $h \in \mathbb{C} \setminus \{0\}$.

□

4.6. La Resultante

El objetivo de esta sección es introducir el concepto de resultante de dos polinomios univariados con coeficientes en un DFU y algunas de sus propiedades fundamentales, las cuales serán usadas en capítulos posteriores. La resultante se remonta a trabajos de G.W. Leibniz, L. Euler, E. Bézout y C.G.J. Jacobi, pero su formulación moderna se debe a J.J. Sylvester en [Syl53].

La resultante es una herramienta esencial que surge muy naturalmente en muchas áreas de la Matemática, además de tener una importancia algorítmica muy reconocida en la actualidad. Es un elemento clave de la Teoría de Eliminación que estuvo muy presente hasta mediados del siglo XX dada su utilidad para producir ejemplos y enunciados en el período pre-"haces y esquemas"de la Geometría Algebraica, y renació a partir del desarrollo masivo de la computación a fines de los años 60, cuando se pudo empezar a calcular cosas inimaginables previamente.

La noción de resultante se extiende dando lugar a las subresultantes, las cuales permitieron hacia fines de los 60 dar un algoritmo eficiente para el cálculo del máximo

común divisor de dos polinomios ([Col67], [BT71]), y más recientemente son también utilizadas en computación simbólica-numérica.

Observación 4.6.1. Si $\mathbb{K}$ es un cuerpo y fijamos $\overline{\mathbb{K}}$ alguna clausura algebraica de $\mathbb{K}$, al considerar $f, g \in \mathbb{K}[X]$ no nulos es un hecho conocido que f y g tienen alguna raíz en común en $\overline{\mathbb{K}}$ si y solo si su máximo común divisor $\mathrm{mcd}(f, g) \in \mathbb{K}[X]$ tiene grado positivo, el cual es a su vez un factor común de f y g.

¿Qué ocurre si f y g son polinomios en $A[X]$ con A un DFU?

Una estrategia posible es considerar $\mathbb{K} = \mathrm{Frac}(A)$ y recurrir al hecho mencionado anteriormente pensando a f y g como polinomios en $\mathbb{K}[X]$. Sin embargo, en diversos contextos, esta idea podría resultar problemática ya que no tiene en cuenta el llamado *coefficient growth* de los polinomios (cf. [vzGJ13]).

Queremos abordar el problema de saber si $f, g \in A[X]$ tienen un factor común de grado positivo en $A[X]$ sin pasar al cuerpo de fracciones de A.

Proposición 4.6.2. *Sean A un DFU y $f, g \in A[X] \setminus \{0\}$ de grados positivos. Entonces, f y g tienen un factor común de grado positivo en $A[X]$ si y solo si existen $s, t \in A[X] \setminus \{0\}$ tales que $\deg(s) < \deg(g)$, $\deg(t) < \deg(f)$ y $s \cdot f = t \cdot g$.*

Demostración.

($\Rightarrow$) Sea $h \in A[X]$ factor común entre f y g de grado positivo. Entonces, existen $s, t \in A[X] \setminus \{0\}$ tales que $f = t \cdot h$ y $g = s \cdot h$ con $\deg(s) < \deg(g)$ y $\deg(t) < \deg(f)$, y se cumple $s \cdot f = s \cdot (t \cdot h) = t \cdot (s \cdot h) = t \cdot g$.

($\Leftarrow$) Supongamos que $s \cdot f = t \cdot g$ con $\deg(s) < \deg(g)$ y $\deg(t) < \deg(f)$ pero que f y g no tienen un factor común de grado positivo en $A[X]$. Luego $\mathrm{mcd}(f, g) = 1$ y como $f \mid t \cdot g$ y $g \mid s \cdot f$ resulta entonces que $f \mid t$ y $g \mid s$, lo cual contradice la hipótesis sobre los grados de s y t.

□

Corolario 4.6.3. *Si A es un DFU y $f, g \in A[X] \setminus \{0\}$ con grados $n, m \geq 1$ respectivamente, entonces el problema de decidir si f y g tienen un factor común de grado positivo es equivalente al de decidir si existen $s, t \in A[X] \setminus \{0\}$ tales que $s \cdot f + t \cdot g = 0$ con $\deg(s) \leq m - 1$ y $\deg(t) \leq n - 1$.*

Introducimos a continuación el concepto de resultante de dos polinomios univariados, que dará una condición necesaria y suficiente para decidir lo anterior.

Definición 4.6.4. Sea A un DFU y sean $f, g \in A[X]$ de grados $n, m \geq 1$ respectivamente, es decir, $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$ con $a_n, b_m \neq 0$. Se definen:

(1) $\mathrm{Syl}(f, g) \in A^{(n+m)\times(n+m)}$ la matriz de Sylvester de f y g:

$$\mathrm{Syl}(f,g) = \underbrace{\left[\begin{array}{ccccccccccc}
a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & \cdots & 0 \\
0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\
0 & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\
\vdots & & \ddots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & & \ddots & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 \\
b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\
0 & b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & \ddots & & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0
\end{array}\right]}_{n+m} \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\end{array}}\right\} n \end{array}$$

(2) $\mathrm{Res}(f,g) = \det\Big(\mathrm{Syl}(f,g)\Big) \in A$ la resultante de f y g.

Notación 4.6.5. En el caso de polinomios $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ con $n \geq 2$, para $i \in \{1, \ldots, n\}$ sabemos por el corolario 4.3.4 que $A = \mathbb{K}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ es un DFU, por lo que podemos considerar la resultante de f y g como polinomios en $A[X_i]$, a la cual denotaremos como $R(f, g, X_i) \in \mathbb{K}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

Teorema 4.6.6. *Sea A un DFU con cuerpo de fracciones $\mathbb{K}$ y fijemos $\overline{\mathbb{K}}$ alguna clausura algebraica de $\mathbb{K}$. Sean $f, g \in A[X]$ de grados $n, m \geq 1$ respectivamente. Son equivalentes:*

(1) $\mathrm{Res}(f,g) = 0$,

(2) Existe $h \in A[X] \setminus \{0\}$ de grado positivo factor común de f y g,

(3) Existe $\alpha \in \overline{\mathbb{K}}$ tal que $f(\alpha) = g(\alpha) = 0$.

Demostración.

La equivalencia *(2)* $\Leftrightarrow$ *(3)* es conocida, por lo que nos dedicaremos a probar la equivalencia *(1)* $\Leftrightarrow$ *(2)*.

Sean $s, t \in A[X]$ tales que $s \cdot f + t \cdot g = 0$ con $\big(s = 0 \text{ ó } \deg(s) \leq m-1\big)$ y $\big(t = 0 \text{ ó } \deg(t) \leq n-1\big)$. Claramente esto es posible tomando $s = t = 0$, pero queremos ver cuándo podemos elegirlos a ambos no nulos. Notar que si alguno de los dos entre s y t es no nulo, como $f, g \neq 0$, el otro resulta también no nulo.

Por las condiciones en los grados, escribamos

$$s = \sum_{k=0}^{m-1} c_k X^k \text{ y } t = \sum_{\ell=0}^{n-1} d_\ell X^\ell,$$

pensando a los coeficientes $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{n-1} \in A$ como incógnitas. Luego $s \cdot f + t \cdot g$ es el polinomio nulo o bien un polinomio de grado $\leq n+m-1$ para cada posible elección de los coeficientes de s y de t, y entonces queremos:

$$\begin{aligned} 0 &= s \cdot f + t \cdot g \\ &= (a_n c_{m-1} + b_m d_{n-1}) X^{n+m-1} + (a_{n-1} c_{m-1} + a_n c_{m-2} + b_m d_{n-2} + b_{m-1} d_{n-1}) X^{n+m-2} + \ldots \\ &\cdots + (a_0 c_0 + b_0 d_0) \end{aligned}$$

igualdad en $A[X]$. Así, al igualar entonces cada coeficiente a cero obtenemos el sistema lineal homogéneo de $n+m$ ecuaciones y $n+m$ incógnitas

$$\begin{bmatrix} a_n & 0 & \cdots & \cdots & \cdots & 0 & b_m & 0 & \cdots & \cdots & 0 \\ a_{n-1} & a_n & 0 & \cdots & \cdots & 0 & b_{m-1} & b_m & \ddots & & \vdots \\ \vdots & a_{n-1} & a_n & \ddots & & \vdots & \vdots & b_{m-1} & \ddots & \ddots & \vdots \\ \vdots & \vdots & a_{n-1} & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & & \ddots & b_m \\ a_0 & \vdots & \vdots & & \ddots & a_n & \vdots & \vdots & & & b_{m-1} \\ 0 & a_0 & \vdots & & & a_{n-1} & b_0 & \vdots & & & \vdots \\ \vdots & 0 & a_0 & & & \vdots & 0 & b_0 & & & \vdots \\ \vdots & \vdots & 0 & \ddots & & \vdots & \vdots & 0 & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_0 & 0 & 0 & \cdots & 0 & b_0 \end{bmatrix} \cdot \begin{bmatrix} c_{m-1} \\ c_{m-2} \\ \vdots \\ \vdots \\ \vdots \\ c_0 \\ d_{n-1} \\ d_{n-2} \\ \vdots \\ \vdots \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

cuya matriz de coeficientes es $[\mathrm{Syl}(f,g)]^t$.

Sabemos que el hecho de que el sistema anterior tenga alguna solución no trivial en $\mathbb{K}^{n+m}$ es equivalente a $\det\left([\mathrm{Syl}(f,g)]^t\right) = 0$, y que dada una solución no trivial en $\mathbb{K}^{n+m}$ del sistema, al multiplicar por un denominador común de las coordenadas obtenemos una solución no trivial en A^{n+m}.

Así, por el corolario 4.6.3, concluimos que f y g tienen un factor común de grado positivo en $A[X]$ si y solo si el sistema homogéneo $[\mathrm{Syl}(f,g)]^t \cdot \vec{x} = \vec{0}$ tiene solución no trivial, y esto último es equivalente a que $\mathrm{Res}(f,g) = \det\left([\mathrm{Syl}(f,g)]^t\right) = 0$.

□

Damos a continuación una propiedad fundamental de la resultante que usaremos en el último capítulo de este trabajo: dados $f, g \in A[X]$, la resultante $\mathrm{Res}(f,g)$ satisface la identidad de Bézout ya que es una combinación polinomial de f y g.

Teorema 4.6.7. *Sean A un DFU y $f, g \in A[X]$ de grados $n, m \geq 1$ respectivamente. Entonces, existen $s, t \in A[X]$ no ambos nulos con $\deg(s) \leq m-1$ y $\deg(t) \leq n-1$ tales que $\mathrm{Res}(f,g) = s \cdot f + t \cdot g$.*

Demostración.

Si $\mathrm{Res}(f,g) = 0$ es inmediato en virtud del teorema 4.6.6 y del corolario 4.6.3.

Supongamos entonces que $\mathrm{Res}(f,g) \neq 0$ y escribamos $f = \sum_{i=0}^{n} a_i X^i$ y $g = \sum_{j=0}^{m} b_j X^j$, con $a_n, b_m \neq 0$. Para $0 \leq k \leq m-1$ y $0 \leq \ell \leq n-1$ tenemos que

$$\begin{aligned} X^k \cdot f &= a_n X^{n+k} + a_{n-1} X^{n+k-1} + \cdots + a_1 X^{k+1} + a_0 X^k \\ X^\ell \cdot g &= b_m X^{m+\ell} + b_{m-1} X^{m+\ell-1} + \cdots + b_1 X^{\ell+1} + a_0 X^\ell \end{aligned}$$

y podemos escribir entonces de forma matricial:

$$\begin{bmatrix} X^{m-1} \cdot f \\ X^{m-2} \cdot f \\ \vdots \\ \vdots \\ X \cdot f \\ f \\ X^{n-1} \cdot g \\ X^{n-2} \cdot g \\ \vdots \\ X \cdot g \\ g \end{bmatrix} = \underbrace{\begin{bmatrix} a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & \cdots & \cdots & b_0 \end{bmatrix}}_{\mathrm{Syl}(f,g)} \cdot \begin{bmatrix} X^{n+m-1} \\ X^{n+m-2} \\ \vdots \\ \vdots \\ \vdots \\ X^{m-1} \\ \vdots \\ \vdots \\ \vdots \\ X \\ 1 \end{bmatrix}$$

En consecuencia, al multiplicar ambos miembros por la matriz adjunta de $\mathrm{Syl}(f,g)$ obtenemos:

$$\operatorname{Adj}\big(\operatorname{Syl}(f,g)\big)\cdot\begin{bmatrix} X^{m-1}\cdot f\\ \vdots\\ X\cdot f\\ f\\ X^{n-1}\cdot g\\ \vdots\\ X\cdot g\\ g\end{bmatrix}=\operatorname{Res}(f,g)\ I_{n+m}\cdot\begin{bmatrix} X^{n+m-1}\\ X^{n+m-2}\\ \vdots\\ \vdots\\ \vdots\\ \vdots\\ X\\ 1\end{bmatrix}\qquad (*)$$

Como $\operatorname{Res}(f,g)=\det\big(\operatorname{Syl}(f,g)\big)\neq 0$, la matriz $\operatorname{Adj}\big(\operatorname{Syl}(f,g)\big)$ es inversible y por consiguiente su última fila $(c_{m-1},\dots,c_1,c_0,d_{n-1},\dots,d_1,d_0)\in A^{n+m}$ no es el vector nulo. Así, al considerar la última fila de cada miembro en la igualdad (*) obtenemos:

$$\begin{bmatrix} c_{m-1} & \dots & c_1 & c_0 & d_{n-1} & \dots & d_1 & d_0\end{bmatrix}\cdot\begin{bmatrix} X^{m-1}\cdot f\\ \vdots\\ X\cdot f\\ f\\ X^{n-1}\cdot g\\ \vdots\\ X\cdot g\\ g\end{bmatrix}=\operatorname{Res}(f,g),$$

de donde finalmente se concluye que

$$\left(\sum_{k=0}^{m-1}c_kX^k\right)\cdot f+\left(\sum_{\ell=0}^{n-1}d_\ell X^\ell\right)\cdot g=\operatorname{Res}(f,g).$$

□

Terminamos este capítulo con algunos comentarios y propiedades adicionales vinculados a la resultante cuyas demostraciones pueden hallarse en [CLO15], [vzGJ13] y [Kri15]. Para más propiedades y resultados se puede consultar [Bou03], [Wal78] y [GKZ09].

Observación 4.6.8. Sea A un DFU con cuerpo de fracciones $\mathbb{K}$ y fijemos $\overline{\mathbb{K}}$ alguna clausura algebraica de $\mathbb{K}$. Sean $f,g\in A[X]$ de grados $n,m\geq 1$ respectivamente, y escribamos $f=a_n(X-\alpha_1)\cdots(X-\alpha_n)$, $g=b_m(X-\beta_1)\cdots(X-\beta_m)$ en $\overline{\mathbb{K}}[X]$.

1. La fórmula de Poisson:

   Se tienen las siguientes fórmulas para la resultante en función de las raíces de f y g:

   $$\operatorname{Res}(f,g) = a_n^m \cdot \prod_{i=1}^{n} g(\alpha_i) = a_n^m \cdot b_m^n \cdot \prod_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} (\alpha_i - \beta_j)$$

   La demostración clásica de estas fórmulas exhibida en [vzGJ13] se prueba para el caso en que f y g tienen todas sus raíces simples y se deduce el caso general por continuidad. Sin embargo, en [Kri15] (como un caso particular del Teorema 2.2 en [DKS05]) se demuestra directamente para el caso en que solo f no tiene raíces múltiples utilizando para ello matrices de Vandermonde, y se generaliza al caso de raíces con multiplicidad utilizando las llamadas matrices de Vandermonde generalizadas (vinculadas a la interpolación de Hermite).

2. El discriminante:

   Se define $\Delta(f)$ el discriminante de f como $\Delta(f) = \dfrac{(-1)^{\frac{n(n-1)}{2}}}{a_n}\operatorname{Res}(f,f')$, cuya propiedad fundamental es que el polinomio f tiene alguna raíz múltiple en $\overline{\mathbb{K}}$ si y solo si $\Delta(f) = 0$.

   A partir de la fórmula de Poisson y de la identidad $f' = a_n \sum_{k=1}^{n} \prod_{\substack{1\leq \ell\leq n\\ \ell\neq k}} (X - \alpha_i)$ se tiene que $\Delta(f) = a_n^{2n-2} \prod_{1\leq i<j\leq m} (\alpha_i - \alpha_j)^2$.

3. La Resultante Generalizada:

   La resultante se generaliza al caso de $n+1$ polinomios homogéneos en $n+1$ variables, y se la llama usualmente *resultante de Macaulay* ya que fue introducida por el matemático Francis Macaulay en [Mac02] y [Mac16]. Si bien existe una construcción matricial para esta resultante, la misma es mucho más compleja que la vinculada a dos polinomios homogéneos en dos variables que se sigue de homogeneizar a f y g.

Capítulo 5

Otro dominio principal que no es euclídeo

El objetivo de este capítulo es demostrar que el anillo $\mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$ es un ejemplo de dominio principal (DP) que no es dominio euclídeo (DE).

Proposición 5.0.1. *El anillo $A = \mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$ es un dominio íntegro.*

Demostración.
Basta ver que el polinomio $g = X^2+Y^2+1 \in \mathbb{R}[X,Y]$ es primo (= irreducible ya que $\mathbb{R}[X,Y]$ es un DFU). Como g es primitivo en $\big(\mathbb{R}[Y]\big)[X]$ por ser mónico, tomando $p = Y^2+1 \in \mathbb{R}[Y]$ que es irreducible allí por ser de grado 2 y sin raíces en $\mathbb{R}$ y por ende primo pues $\mathbb{R}[Y]$ es un DFU, por el criterio de Eisenstein 4.4.3 g resulta irreducible en $\big(\mathbb{R}[Y]\big)[X] = \mathbb{R}[X,Y]$.

□

Daremos a continuación una caracterización de las unidades del dominio íntegro estudiado. Tener presente que el morfismo $\mathbb{R} \hookrightarrow \mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$ es claramente inyectivo, por lo que notaremos directamente α a la clase en el cociente de un elemento $\alpha \in \mathbb{R}$.

Proposición 5.0.2. *Sea $A = \mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$. Entonces, $\mathcal{U}(A) = \mathbb{R}\setminus\{0\}$.*

Demostración.
Veamos que vale la doble inclusión:
($\supseteq$) Es inmediato ya que todo $\alpha \in \mathbb{R}\setminus\{0\}$ es inversible en $\mathbb{R}$.
($\subseteq$) Sea $\overline{f} \in \mathcal{U}(A)$. Entonces existe $\overline{g} \in A$ tal que $\overline{f}\cdot\overline{g} = 1$ en A.
Como $X^2+Y^2+1 \in \mathbb{R}[X,Y] = \big(\mathbb{R}[Y]\big)[X]$ es mónico, podemos escribir

$$\overline{f} = q_1(\overline{Y})\cdot\overline{X} + p_1(\overline{Y}) \quad \text{y} \quad \overline{g} = q_2(\overline{Y})\cdot\overline{X} + p_2(\overline{Y}).$$

Queremos probar que $q_1 = 0$ y que $p_1 \in \mathbb{R}\setminus\{0\}$.

Tenemos que $\overline{f} \cdot \overline{g} = 1$

$$\Leftrightarrow \quad \underbrace{(q_1q_2)(Y) \cdot X^2 + (q_1p_2 + q_2p_1)(Y) \cdot X + (p_1p_2)(Y) - 1}_{=:\, h(X,Y)} \in \langle X^2 + Y^2 + 1 \rangle,$$

lo cual a su vez equivale a que $h(X,Y) = p(Y) \cdot (X^2 + Y^2 + 1)$ ya que $\deg_X(h) \leq 2$, y por lo tanto obtenemos el sistema en $\mathbb{R}[Y]$:

$$\left\{ \begin{array}{rcl} q_1 \cdot q_2 & = & p \\ q_1 \cdot p_2 + q_2 \cdot p_1 & = & 0 \\ p_1 \cdot p_2 & = & p \cdot (Y^2 + 1) + 1 \end{array} \right. \tag{1}$$

- Caso $p \neq 0$:

En este caso, de la primera y de la tercera ecuación resulta que $p_1, p_2, q_1, q_2 \neq 0$. A su vez, de la segunda ecuación obtenemos que $q_1 \cdot p_2 = -q_2 \cdot p_1$. Luego, al multiplicar por q_1 la tercera ecuación, tenemos que

$$\begin{aligned} q_1 \cdot p_1 \cdot p_2 = q_1 \cdot p \cdot (Y^2 + 1) + q_1 \quad &\Leftrightarrow \quad -p_1^2 \cdot q_2 = q_1^2 \cdot q_2 \cdot (Y^2 + 1) + q_1 \\ &\Leftrightarrow \quad q_2 \cdot \big(-p_1^2 - q_1^2 \cdot (Y^2 + 1) \big) = q_1, \end{aligned}$$

y concluimos de este modo que $q_2 \mid q_1$ en $\mathbb{R}[Y]$. Análogamente, al multiplicar la tercera ecuación del sistema (1) por q_2, obtenemos que $q_1 \mid q_2$. Por consiguiente resulta que $q_1 \sim q_2$ en $\mathbb{R}[Y]$, y entonces existe $\lambda \in \mathbb{R} \setminus \{0\}$ tal que $q_2 = \lambda q_1$ y $p_2 = -\lambda p_1$.

Pero así de la tercera ecuación del sistema obtenemos que $-\lambda p_1^2 = \lambda q_1^2 \cdot (Y^2 + 1) + 1$, lo cual es absurdo ya que los coeficientes principales de cada miembro de la igualdad tienen distinto signo.

- Caso $p = 0$:

El sistema (1) queda

$$\left\{ \begin{array}{rcl} q_1 \cdot q_2 & = & 0 \\ q_1 \cdot p_2 + q_2 \cdot p_1 & = & 0 \\ p_1 \cdot p_2 & = & 1 \end{array} \right.$$

De la tercera ecuación del sistema resulta que $p_1, p_2 \in \mathbb{R} \setminus \{0\}$, y a partir de esto y de las dos ecuaciones restantes se obtiene que $q_1 = q_2 = 0$, como queríamos probar.

□

Para probar que el dominio $A = \mathbb{R}[X,Y] \Big/ \langle X^2 + Y^2 + 1 \rangle$ es un DP daremos a continuación una caracterización de los ideales primos no nulos del anillo (y que de hecho resultarán maximales), la cual también será útil para concluir luego que no es un DE.

Teorema 5.0.3. *Sea $A = \mathbb{R}[X,Y] \Big/ \langle X^2 + Y^2 + 1 \rangle$ y sea $\overline{J} \trianglelefteq A$ un ideal no nulo. Entonces, $\overline{J}$ es un ideal primo si y solo si existen $a, b \in \mathbb{R}$ tales que $\overline{J} = \big\langle \overline{X} + a\overline{Y} + b \big\rangle$ o $\overline{J} = \big\langle \overline{Y} + a\overline{X} + b \big\rangle$. Más aún, todo ideal primo $\overline{J} \trianglelefteq A$ no nulo es maximal.*

Demostración.

Llamemos $I = \langle X^2 + Y^2 + 1 \rangle \trianglelefteq \mathbb{R}[X,Y]$ y consideremos $\pi_I : \mathbb{R}[X,Y] \longrightarrow \mathbb{R}[X,Y]\Big/_I$ la proyección al cociente.

($\Leftarrow$) Basta ver que los ideales de la forma $\overline{J} = \langle \overline{X} + a\overline{Y} + b \rangle$ con $a, b \in \mathbb{R}$ son maximales ya que el otro caso es análogo.

En virtud de la correspondencia dada por la proposición 1.1.14 tomemos $J = \langle X + aY + b, X^2 + Y^2 + 1 \rangle \trianglelefteq \mathbb{R}[X,Y]$ y así $I \subseteq J$ y $\overline{J} = J\Big/_I$. De este modo, por el segundo teorema de isomorfismo 1.1.15 se tiene que

$$A\Big/_{\overline{J}} \simeq \mathbb{R}[X,Y]\Big/_J,$$

y en consecuencia alcanza con ver que el anillo $\mathbb{R}[X,Y]\Big/_J$ es un cuerpo. En este cociente tenemos que $\overline{X} = -\left(a\overline{Y} + b\right)$ y entonces $\overline{X}^2 = a^2\overline{Y}^2 + 2ab\overline{Y} + b^2$, de donde se sigue que

$$\begin{aligned} 0 &= \overline{X}^2 + \overline{Y}^2 + 1 \\ &= (a^2+1)\overline{Y}^2 + 2ab\overline{Y} + (b^2+1). \end{aligned}$$

Así, si consideramos el polinomio $p(Y) = (a^2+1)Y^2 + 2abY + (b^2+1) \in \mathbb{R}[Y]$ resulta que $p \in J$. Notemos que p tiene grado 2 y su discriminante es $\Delta(p) = -4\left(a^2 + b^2 + 1\right) < 0$, por lo que p tiene dos raíces en $\mathbb{C} \setminus \mathbb{R}$ y son conjugadas. Si fijamos $z \in \mathbb{C} \setminus \mathbb{R}$ raíz de p y definimos el morfismo de anillos $\varphi : \mathbb{R}[X,Y] \to \mathbb{C}$ dado por la evaluación $\varphi(f) = f(-az - b, z)$ resulta inmediato que φ es un epimorfismo. Veamos que $\mathrm{Ker}(\varphi) = J$.

($\supseteq$) Es inmediato ya que $\varphi(X + aY + b) = 0$ y además $\varphi(X^2 + Y^2 + 1) = p(z) = 0$ pues z es raíz de p.

($\subseteq$) Sea $f \in \mathrm{Ker}(\varphi)$, es decir, $f \in \mathbb{R}[X,Y]$ con $f(-az - b, z) = 0$.

Pensando a f y a $X + aY + b$ como polinomios en $(\mathbb{R}[Y])[X]$ podemos escribir vía algoritmo de división

$$f = q(X,Y) \cdot (X + aY + b) + \tilde{r}(Y),$$

y a su vez dividamos a $\tilde{r}$ por p en $\mathbb{R}[Y]$ para obtener la escritura

$$f = q(X,Y) \cdot (X + aY + b) + p(Y) \cdot s(Y) + r(Y),$$

donde $r = 0$ o bien $\deg(r) < 2$.

Luego $0 = \varphi(f) = \varphi(r) = r(z)$, por lo que debe ser $r = 0$ por la condición en el grado de r ya que $z \in \mathbb{C} \setminus \mathbb{R}$. De este modo concluimos que $f = q(X,Y) \cdot (X + aY + b) + p(Y) \cdot s(Y) \in J$, y por el primer teorema de isomorfismo 1.1.13 resulta entonces que $\mathbb{R}[X,Y]\Big/_J \simeq \mathbb{C}$ que es un cuerpo, como queríamos ver.

($\Rightarrow$) Asumamos que el ideal no nulo $\overline{J} \trianglelefteq A$ es primo y en vista de la correspondencia 1.1.14 tomemos $J \trianglelefteq \mathbb{R}[X,Y]$ primo con $I \subsetneq J$ tal que $\overline{J} = J\Big/_I$ ya que $\overline{J} \neq 0$.

A partir de lo probado en la otra implicación tenemos que los ideales en A de la forma $\langle a\overline{X} + b\overline{Y} + c\rangle$ con $(a,b) \neq (0,0)$ son maximales, por lo que si probamos que existe $q = aX + bY + c \in \mathbb{R}[X,Y]$ con $(a,b) \neq (0,0)$ tal que $q \in J$ será entonces $\overline{J} = \langle \overline{q}\rangle$ de donde se concluye lo deseado.

Si $X \in J$ o $Y \in J$ es inmediato. Supongamos entonces que $X, Y \notin J$, por lo que $\overline{X}, \overline{Y} \neq 0$ en $\mathbb{R}[X,Y]\Big/_J$. Sea $f \in J \setminus I$ y llamemos $g = X^2 + Y^2 + 1 \in I$. Luego $f\left(\overline{X},\overline{Y}\right) = 0$ y $g\left(\overline{X},\overline{Y}\right) = 0$ en $\mathbb{R}[X,Y]\Big/_J$.

Como J es un ideal primo en $\mathbb{R}[X,Y]$, por la proposición 1.1.16 sabemos que $\mathbb{R}[X,Y]\Big/_J$ es un dominio íntegro y en consecuencia podemos considerar $\mathbb{K} = \mathrm{Frac}\left(\mathbb{R}[X,Y]\Big/_J\right)$. Tenemos entonces la extensión de cuerpos $\mathbb{K}/\mathbb{R}$ y además $\mathbb{R} \subseteq \mathbb{R}[X,Y]\Big/_J \subseteq \mathbb{K}$, por lo que si consideramos el sistema polinomial

$$\left\{\begin{array}{rcl} f(X,Y) & = & 0 \\ g(X,Y) & = & 0 \end{array}\right. \qquad (*)$$

resulta que $\left(\overline{X},\overline{Y}\right)$ es una solución de (*) en $\mathbb{K}^2$.

Como $f \notin I = \langle g\rangle$ se sigue que $g \nmid f$ en $\mathbb{R}[X,Y]$, y como vimos en la proposición 5.0.1 que g es irreducible concluimos entonces que f y g no tienen factores comunes de grado positivo en $\mathbb{R}[X,Y]$.

Si $\deg_X(f) = 0$ entonces tenemos que $f \in \mathbb{R}[Y]$ y $\deg_Y(f) > 0$. Aquí resulta $f(\overline{Y})$ = 0 en $\mathbb{K}$, de donde se sigue que $\overline{Y}$ es algebraico sobre $\mathbb{R}$. Por otro lado, si pensamos $f, g \in (\mathbb{R}[X])[Y]$, como $\mathbb{R}[X]$ es un DFU y en virtud del teorema 4.6.6, se tiene que la resultante $R_Y = \mathrm{Res}(f,g,Y) \in \mathbb{R}[X]$ no es el polinomio nulo. A su vez, por el teorema 4.6.7 sabemos que existen $s,t \in \mathbb{R}[X,Y]$ tales que $R_Y = s\cdot f + t\cdot g$, por lo que al evaluar en $\left(\overline{X},\overline{Y}\right)$ obtenemos que $R_Y(\overline{X}) = 0$ en $\mathbb{K}$ ya que $f\left(\overline{Y}\right) = g\left(\overline{X},\overline{Y}\right) = 0$. Concluimos así que el elemento $\overline{X} \in \mathbb{K}$ es algebraico sobre $\mathbb{R}$. El caso $\deg_Y(f) = 0$ es análogo.

Si $\deg_X(f), \deg_Y(f) > 0$, considerando ambas resultantes $R_Y = \mathrm{Res}(f,g,Y) \in \mathbb{R}[X]$ y $R_X = \mathrm{Res}(f,g,X) \in \mathbb{R}[Y]$ concluimos también que $\overline{X}$ y $\overline{Y}$ son ambos algebraicos sobre $\mathbb{R}$.

Así, la extensión de cuerpos $\mathbb{R}\left(\overline{X},\overline{Y}\right)/\mathbb{R}$ es algebraica, y en consecuencia tenemos la torre de extensiones de cuerpos $\overline{\mathbb{R}}/\mathbb{R}\left(\overline{X},\overline{Y}\right)/\mathbb{R}$, donde sabemos que $\overline{\mathbb{R}} \simeq \mathbb{C}$. Por consiguiente, la dimensión de $\mathbb{R}\left(\overline{X},\overline{Y}\right)$ como $\mathbb{R}$-espacio vectorial es a lo sumo 2, y entonces el conjunto $\left\{\overline{X},\overline{Y},1\right\}$ resulta linealmente dependiente sobre $\mathbb{R}$. De este modo concluimos que existen $a,b,c \in \mathbb{R}$ no todos nulos tales que $a\overline{X} + b\overline{Y} + c = 0$. Notar que debe ser $(a,b) \neq (0,0)$ ya que si no resultaría también $c = 0$. Así, $a\overline{X} + b\overline{Y} + c = 0$ en $\mathbb{R}[X,Y]\Big/_J$, de donde concluimos que $aX + bY + c \in J$. □

Teniendo presente esta caracterización de los ideales primos no nulos de el dominio estudiado procedemos a demostrar que efectivamente es un DP.

Teorema 5.0.4. *El anillo $A = \mathbb{R}[X,Y]\Big/_{\langle X^2+Y^2+1\rangle}$ es un DP.*

Demostración.

Sabemos por la proposición 5.0.1 que A es un dominio íntegro, y en virtud de lo que probamos recién en el teorema 5.0.3 se sigue que todo ideal primo de A es principal. Así, por el teorema 3.1.4, A resulta un DP.

□

Observación 5.0.5. Como ya sabemos que $A = \mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$ es un DP y que sus ideales primos no nulos son todos de la forma $\langle a\overline{X}+b\overline{Y}+c\rangle$ con $(a,b) \neq (0,0)$, entonces dado $\overline{p} \in A \setminus \{0\}$ se tiene que $\overline{p}$ es primo si y solo si existen $a,b,c \in \mathbb{R}$ con $(a,b) \neq (0,0)$ tales que $\overline{p} = a\overline{X} + b\overline{Y} + c$.

Para finalizar este trabajo procedemos a probar que efectivamente el dominio íntegro estudiado no es un DE.

Teorema 5.0.6. *El anillo $A = \mathbb{R}[X,Y]\Big/\langle X^2+Y^2+1\rangle$ no es un DE.*

Demostración.

Supongamos que A es un dominio euclídeo. Claramente A no es un cuerpo ya que vimos en la proposición 5.0.2 que sus unidades son $\mathbb{R} \setminus \{0\}$.

Así, en virtud de la proposición 3.2.5 y de la observación 5.0.5, sabemos que existe $\overline{p} = a\overline{X} + b\overline{Y} + c \in A$ primo (con $(a,b) \neq (0,0)$) tal que si consideramos la proyección al cociente $\pi : A \longrightarrow A\Big/\langle\overline{p}\rangle$ resulta que $\pi\big(\mathcal{U}(A)\big) = \mathcal{U}\Big(A\Big/\langle\overline{p}\rangle\Big)$.

Por la proposición 5.0.2 tenemos que $\mathcal{U}(A) = \mathbb{R} \setminus \{0\}$. En particular, esto implica que dados $\alpha, \beta \in \mathcal{U}(A)$ con $\alpha \neq \beta$ entonces $\alpha - \beta \in \mathcal{U}(A)$. Luego podemos considerar el morfismo de grupos $\psi : \mathcal{U}(A) \longrightarrow \mathcal{U}\Big(A\Big/\langle\overline{p}\rangle\Big)$ dado por $\psi(\alpha) = \pi(\alpha)$, que está bien definido ya que $\pi\big(\mathcal{U}(A)\big) = \mathcal{U}\Big(A\Big/\langle\overline{p}\rangle\Big)$, y que por el mismo motivo resulta un epimorfismo. Veamos que ψ es también un monomorfismo: sean $\alpha, \beta \in \mathcal{U}(A)$ con $\alpha \neq \beta$ y supongamos que $\psi(\alpha) = \psi(\beta)$. Se tiene así:

$$\begin{aligned} \psi(\alpha) = \psi(\beta) &\Leftrightarrow \pi(\alpha) = \pi(\beta) \\ &\Leftrightarrow \overline{p} \mid \alpha - \beta \text{ en } A, \end{aligned}$$

pero esto último es absurdo ya que $\overline{p} \in A$ es primo y como $\alpha \neq \beta$ entonces $\alpha - \beta \in \mathcal{U}(A)$. Luego ψ debe ser inyectiva. Así, ψ resulta un isomorfismo de grupos y entonces $\mathcal{U}(A) \simeq \mathcal{U}\Big(A\Big/\langle\overline{p}\rangle\Big)$.

A su vez, a partir de la demostración del teorema 5.0.3 sabemos que el ideal $\langle\overline{p}\rangle \trianglelefteq A$ es un ideal maximal y que $A\Big/\langle\overline{p}\rangle \simeq \mathbb{C}$, de donde se sigue que $\mathcal{U}\left(A\Big/\langle\overline{p}\rangle\right) \simeq \mathbb{C} \setminus \{0\}$ como grupos.

A partir de todo lo anterior obtenemos que $\mathbb{R} \setminus \{0\} \simeq \mathcal{U}\Big(A\Big/\langle\overline{p}\rangle\Big) \simeq \mathbb{C} \setminus \{0\}$ como grupos, y en particular esto implica que existe $\phi : \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{R} \setminus \{0\}$ isomorfismo de grupos. Como $\phi(1) = 1$ por ser morfismo, debe ser entonces $\phi(-1) \neq 1$, y como además

$1 = \phi(1) = \phi\big((-1)^2\big) = \phi(-1)^2$ en $\mathbb{R}$, concluimos que necesariamente $\phi(-1) = -1$. Sin embargo, de este modo llegamos a que $-1 = \phi(-1) = \phi\left(i^2\right) = \phi(i)^2$ en $\mathbb{R}$, que es claramente absurdo.

Así, A no puede ser un DE.

□

Bibliografía

[Bou03] Nicolas Bourbaki. *Algebra II, Chap. IV*. Springer Science & Business Media, edition 2003.

[BT71] W S Brown and J F Traub. *On Euclid's Algorithm and the Theory of Subresultants*. J. Assoc. Comput. Mach. 18, 1971.

[Cam88] Oscar A. Cámpoli *A Principal Ideal Domain That Is Not a Euclidean Domain*. The American Mathematical Monthly, 1988.

[CLO15] David A. Cox, John B. Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer Science & Business Media, fourth edition, 2015.

[Col67] George Collins. *Subresultants and Reduced Polynomial Remainder Sequences*. J. ACM 14, 1, 1967.

[DF04] David. S Dummit and Richard M Foote. *Abstract Algebra*. John Wiley & Sons, Inc., 2004.

[DKS05] Carlos D'Andrea, Teresa Krick, and Agnes Szanto. *Multivariate subresultants in roots*, 2005.

[GKZ09] Israel M. Gelfand, Mikhail Kapranov, and Andrei Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Springer Science & Business Media, 2009.

[Kri15] Teresa Krick. *Resultante, subresultantes y sumas de Sylvester*. http://mate.dm.uba.ar/~krick/LaResultante.pdf, 2015.

[Lan02] Serge Lang. *Algebra*. Springer, 3 edition, 2002.

[Mac02] Francis Macaulay. *On some formulae in elimination*. Proc. London. Math. Soc. 3, 1902.

[Mac16] Francis Macaulay. *The algebraic theory of modular systems*. Cambridge U. Press, 1916.

[mat14] Quotient of polynomials, pid but not euclidean domain? https://math.stackexchange.com/questions/864212/quotient-of-polynomials-pid-but-not-euclidean-domain, 2014.

[Motz49] Theodore Motzkin. *The Euclidean Algorithm*. Bulletin of the American Mathematical Society, 1949.

[Rot23] Joseph J Rotman. *Advanced Modern Algebra*. American Mathematical Society, third edition, 2023.

[SK90] Igor Shafarevich and Aleksej Kostrikin. *Algebra I*. Springer, 1990.

[ST01] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. CRC Press, 2001.

[Syl53] James Joseph Sylvester. *On a Theory of the Syzygetic Relations of Two Rational Integral Functions*. Philosophical Transactions of the Royal Society of London, Part III, 1853.

[vzGJ13] Joachim von zur Gathen and Gerhard Jürgen. *Modern Computer Algebra*. Cambridge University Press, 2013.

[Wal78] Robert J Walker. *Algebraic Curves*. Springer, 1978.

[Wil73] Jack C. Wilson. *A Principal Ideal Ring That Is Not a Euclidean Ring*. Mathematics Magazine, 1973.