UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

GRADO DE MATEMÁTICAS

ANILLOS EUCLÍDEOS

LAURA PARDO VILLANUEVA

Departamento de Álgebra

2020/2021

TRABAJO FIN DE GRADO

Laura Pardo Villanueva
Tutor: Pascual Jara Martínez

ANILLOS EUCLÍDEOS

UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

GRADO DE MATEMÁTICAS

14 de junio de 2021

Índice general

Introducción

Sea K un anillo conmutativo y X una indeterminada sobre K. Representamos por $K[X]$ al conjunto de todos los polinomios en X con coeficientes en K, y en él consideramos las operaciones suma y producto que, junto con el polinomio constante, 1 forman un anillo conmutativo.

Existe una aplicación, gr, de $K[X]$ a $\mathbb{N}$ que a cada polinomio no nulo asocia su grado. Podemos modificar esta aplicación definiendo una nueva mediante:

$$d : K[X] \longrightarrow \mathbb{N}, \text{ definida } d(F(X)) = 2^{\mathrm{gr}(F(X))}.$$

La razón es que d es multiplicativa, si K es un dominio de integridad, mientras que gr es aditiva.

Si $F(X)$ y $G(X) \neq 0$ son polinomios, si existen polinomios $Q(X)$ y $R(X)$ y una combinación $F(X) = G(X)Q(X) + R(X)$, siendo $R(X) = 0$ ó $d(R(X)) < d(G(X))$, tenemos la **división euclídea** de $F(X)$ por $G(X)$ con cociente $Q(X)$ y resto $R(X)$. Cuando K es un cuerpo, estos polinomios $Q(X)$ y $R(X)$ son únicos en el siguiente sentido; si $F(X) = G(X)Q'(X) + R'(X)$ es otra división euclídea, entonces $0 = G(X)(Q(X) - Q'(X)) + (R(X) - R'(X))$, esto es, $R(X) - R'(X) = G(X)(Q(X) - Q'(X))$, y por tanto, como $\mathrm{gr}(R(X) - R'(X)) < \mathrm{gr}(G(X))$, se tiene $R(X) - R'(X) = 0$ y $Q(X) - Q'(X) = 0$.

Observa que esta propiedad no ocurre en otros anillos, como, por ejemplo, en el anillo $\mathbb{Z}$ de los números enteros. Dados dos enteros f y $g \neq 0$, existen números enteros q y r tales que $f = gq + r$, siendo $r = 0$ ó $|r| < |g|$. Que la unicidad de q y r no se tiene asegurada lo prueba el siguiente ejemplo: $5 = 2 \times 2 + 1 = 2 \times 3 - 1$.

En el caso de $\mathbb{Z}$ tenemos que a cada número entero asignamos un elemento de $\mathbb{N}$, su valor absoluto, mientras que en el caso de $K[X]$ no tenemos un valor asignado al polinomio cero. Para solventar este problema, de forma que la división euclídea sigua siendo una herramienta útil, vamos a asignar al polinomio cero, y al número entero 0, un valor superior a cualquier elemento de $\mathbb{N}$; para esto consideraremos, en vez de $\mathbb{N}$ el conjunto $\mathbb{N} \cup \{\infty\}$. Y como necesitamos una relación de orden (en realidad una relación de orden que sea un buen orden), vamos a considerar en $\mathbb{N} \cup \{\infty\}$ la siguiente relación:

$$\alpha \leq \beta \text{ si } \begin{cases} \alpha \leq \beta, & \text{cuando } \alpha, \beta \in \mathbb{N} \text{ ó,} \\ \text{si } \alpha = \infty \end{cases}$$

De esta forma basta asignar al polinomio cero, ó al número entero cero, el valor ∞.

Tenemos entonces que si K es un cuerpo, para cualesquiera $F, G \in K[X]$ existen polinomios Q, R tales que $F = GQ + R$, siendo $R = 0$ ó $d(R) < d(G)$, e igual para números enteros.

Estos ejemplos prueban que para estudiar la división euclídea no necesariamente tenemos que considerar $\mathbb{N}$, sino que lo más indicado es considerar un ordinal, en estos ejemplos hemos tomado $\omega + 1$. Comprobaremos que esta modificación permite extender la teoría de dominios euclídeos a anillos que no necesariamente son dominios de integridad, e incluso a anillos que no son conmutativos.

Tras una introducción a la teoría de ordinales y números ordinales, a la que dedicaremos el primer capítulo, haremos la definición de anillo euclídeo a izquierda: un anillo R es un **anillo euclídeo a izquierda** si existen un ordinal $\mathcal{O}$ y una aplicación $\delta : R \longrightarrow \mathcal{O}$ tal que $\delta(0) = \text{ínf}\{\alpha |\ \delta(a) < \alpha$ para todo $a \in D \setminus \{0\}\}$, y que que para par de elementos $a, b \in R$ existen elementos $c, r \in R$ tales que $a = cb + r$, con $r = 0$ ó $\delta(c) < \delta(b)$. Tenemos así la división euclídea a izquierda de a por b con cociente c y resto r. De igual forma se define un anillo euclídeo a derecha. Cuando $R = A$ es un anillo conmutativo, tendremos el concepto de **anillo euclídeo**.

A continuación estudiaremos las propiedades que se pueden deducir de la definición de anillo euclídeo, tanto en el caso conmutativo como en el no conmutativo, teniendo en cuenta que nuestro objeto principal de estudio lo forman los anillo conmutativos. Probaremos que

(1) Todo anillo euclídeo es una anillo de ideales principales.
(2) El producto de dos anillos euclídeos es un anillo euclídeo (esto generaliza el hecho de que el producto de dos anillos de ideales principales es un anillo de ideales principales).
(3) El anillo de matrices 2×2 sobre $\mathbb{F}_2$ es un anillo euclídeo.

La inclusión de ordinales no necesariamente numerables tiene por objeto ampliar el número de ejemplos que son anillos euclídeos; y tiene otra finalidad, ésta más práctica; mientras que el producto de anillos de ideales principales es un anillo de ideales principales, no ocurre lo mismo con el producto de anillos euclídeos, ahora bien, si ampliamos el conjunto en el que la función euclídea toma valores, obtenemos una estructura de anillo euclídeo en el producto; pero para poder hacer esto necesitamos que la función tome valores en un ordinal, no necesariamente en ω u $\omega + 1$. Este será el último resultado que incluimos en esta memoria: "*el producto de dos anillos euclídeos es un anillo euclídeo*". Existen muchos otros problemas relativos a anillos euclídeos que no vamos a tratar pero que son particularmente sugerentes; uno de ellos hace referencia a la existencia o no de anillos euclídeos que no admiten una función euclídea a $\omega + 1$; existen ejemplos de su existencia desde el inicio mismo de la teoría (ver la bibliografía); la construcción de ejemplos que sean dominios de integridad es más reciente, desafortunadamente la teoría de ordinales subyacente excede a esta exposición (ver la bibliografía).

La estructura de la memoria es la siguiente: como preámbulo a la teoría general, que es el objeto principal de esta memoria, y que exponemos en el último capítulo, el cuarto, en el capítulo dos recordamos los conceptos elementales de dominios de integridad y divisibilidad, y en el capítulo tres los conceptos de dominios euclídeos, en donde completamos la teoría desarrollada en el Grado al estudiar las relaciones entre los diversos tipos de dominios: euclídeo, de ideales principales y de factorización única. Como en el capítulo uno hemos estudiado los ordinales, podemos dar una introducción a la teoría de anillos euclídeos conociendo los resultados fundamentales de los dominios euclídeos.

Introduction

Let K be a commutative ring and X an indeterminate over K. We represent by $K[X]$ the set of all polynomials in X with coefficients in K, and in it we consider the operations sum and product that, together with the constant polynomial, 1 form a commutative ring.

There is an application, gr, from $K[X]$ to $\mathbb{N}$ that associates its degree to each non-zero polynomial. We can modify this application by defining a new one using:

$$d : K[X] \longrightarrow \mathbb{N}, \text{ defined } d(F(X)) = 2^{\mathrm{gr}(F(X))}.$$

The reason is that d is multiplicative, if K is an integrity domain, while gr is additive.

If $F(X)$ and $G(X) \neq 0$ are polynomials, if there are polynomials $Q(X)$ and $R(X)$ and a combination $F(X) = G(X)Q(X)+R(X)$, where $R(X) = 0$ ó $d(R(X)) < d(G(X))$, we have the **Euclidean division**f $F(X)$ times $G(X)$ with quotient $Q(X)$ and remainder $R(X)$. When K is a field, these polynomials $Q(X)$ and $R(X)$ are unique in the following sense; if $F(X) = G(X)Q'(X) + R'(X)$ is another Euclidean division, then $0 = G(X)(Q(X) - Q'(X)) + (R(X) - R'(X))$, that is, $R(X) - R'(X) = G(X)(Q(X) - Q'(X))$, and therefore, as $\mathrm{gr}(R(X) - R'(X)) < \mathrm{gr}(G(X))$, we have $R(X) - R'(X) = 0$ and $Q(X) - Q'(X) = 0$.

Note that this property does not occur in other rings, such as the $\mathbb{Z}$ ring of integers. Given two integers f and $g \neq 0$, there are integers q and r such that $f = gq + r$, where $r = 0$ ó $|r| < |g|$. That the uniqueness of q and r is not assured is proven by the following example: $5 = 2 \times 2 + 1 = 2 \times 3 - 1$.

In the case of $\mathbb{Z}$ we have that to each integer we assign an element of $mathbbN$, its absolute value, while in the case of $K[X]$ we do not have an assigned value to the zero polynomial. To solve this problem, so that Euclidean division continues to be a useful tool, we are going to assign the polynomial zero, and the integer number 0, a value greater than any element of $\mathbb{N}$; for this we will consider, instead of $\mathbb{N}$ the set $\mathbb{N} \cup \{\infty\}$. And since we need an order relation (actually an order relation that is a good order), we are going to consider in $\mathbb{N} \cup \{\infty\}$ the following relation:

$$\alpha \leq \beta \text{ si } \begin{cases} \alpha \leq \beta, & \text{when } \alpha, \beta \in \mathbb{N} \text{ ó,} \\ \text{si } \alpha = \infty \end{cases}$$

In this way, it is enough to assign the polynomial zero, or the integer zero, the value

∞. We then have that if K is a field, for any $F, G \in K[X]$ there are polynomials Q, R such that $F = GQ + R$, where $R = 0$ or $d(R) < d(G)$, and the same for whole numbers.

These examples prove that to study the Euclidean division we do not necessarily have to consider $\mathbb{N}$, but rather consider an ordinal, in these examples we have taken $\omega + 1$. We will verify that this modification allows us to extend the theory of Euclidean domains to rings that are not necessarily integrity domains, and even to rings that are not commutative.

After an introduction to the theory of ordinals and ordinal numbers, to which we will dedicate the first chapter, we will define a left Euclidean ring: a R ring is a **left Euclidean ring**f they exist an ordinal $\mathcal{O}$ and an application $\delta : R \longrightarrow \mathcal{O}$ such that $\delta(0) = \text{ínf}\{\alpha| \ ; \delta(a) < \alpha \ for \ all \ a \in D \setminus \{0\}\}$, and that that for a pair of elements $a, b \in R$ there are elements $c, r \in R$ such that $a = cb + r$, with $r = 0$ ó $\delta(c) < \delta(b)$. Thus we have the Euclidean division to the left of a by b with quotient c and remainder r. In the same way, a Euclidean ring is defined on the right. When $R = A$ is a commutative ring, we will have the concept of **Euclidean ring**

Next we will study the properties that can be deduced from the definition of the Euclidean ring, both in the commutative and non-commutative cases, taking into account that our main object of study is the commutative rings. We will prove that

(1) Every Euclidean ring is a ring of main ideals.
(2) The product of two Euclidean rings is a Euclidean ring (this generalizes the fact that the product of two main ideal rings is a main ideal ring).
(3) The ring of matrices 2×2 on $\mathbb{F}_2$ is a Euclidean ring.

The inclusion of ordinals not necessarily countable is intended to expand the number of examples that are Euclidean rings; And it has another purpose, this more practical one; While the product of rings of main ideals is a ring of main ideals, the same does not happen with the product of Euclidean rings, however, if we expand the set in which the Euclidean function takes values, we obtain a Euclidean ring structure in the product; but in order to do this we need the function takes values in an ordinal, not necessarily in ω u $\omega + 1$. This will be the last result we include in this report: " *the product of two Euclidean rings is a Euclidean ring* ". There are many other problems related to Euclidean rings that we will not discuss but that are particularly suggestive; one of them refers to the existence or not of Euclidean rings that do not admit a Euclidean function at $\omega + 1$; there are examples of its existence from the very beginning of the theory (see the bibliography); the construction of examples that are integrity domains is more recent, unfortunately the underlying ordinal theory exceeds this discussion (see bibliography).

The structure of memory is as follows: as a preamble to the general theory, which is the main object of this memory, and which we expose in the last chapter, the fourth, in chapter two we recall the elementary concepts of domains of integrity and divisibility , and in chapter three the concepts of Euclidean domains, where we complete

the theory developed in the Degree by studying the relationships between the various types of domains: Euclidean, main ideals and single factorization. Since we have studied ordinals in chapter one, we can give an introduction to the theory of Euclidean rings by knowing the fundamental results of the Euclidean domains.

Capítulo 1

ORDINALES

1. Conjuntos parcialmente ordenados

Dados un conjunto X y una relación de orden $\leq$ en X, el par $(X, \leq)$ se llama un **conjunto parcialmente ordenado**. Recuerda que una relación binaria $\leq$ en un conjunto X es una **relación de orden** si verifica las propiedades:

(1) **Reflexiva**. Para todo $x \in X$ se tiene $x \leq x$.
(2) **Antisimétrica**. Para todo par $x_1, x_2 \in X$, si $x_1 \leq x_2$ y $x_2 \leq x_1$, entonces $x_1 = x_2$.
(3) **Transitiva**. Para toda terna $x_1, x_2, x_3 \in X$, si $x_1 \leq x_2$ y $x_2 \leq x_3$, entonces $x_1 \leq x_3$.

Si $S \subseteq X$ es un subconjunto de un conjunto parcialmente ordenado (no siempre es necesario indicar cual es la relación de orden), tenemos los siguientes conceptos relativos a S.

(1) Un elemento $x \in X$ es una **cota superior** de S si verifica $s \leq x$ para todo $s \in S$. De igual forma se define **cota inferior**.
(2) Un elemento $s \in S$ es un **máximo** de S si es una cota superior. De igual forma se define **mínimo**.
(3) Un elemento $x \in X$ es un **supremo** de S si es un mínimo del conjunto de las cotas superiores de S. De igual forma se define **ínfimo**.

Observa que, dados S y X, la existencia de estos elementos no está asegurada; sin embargo, si existen, el máximo, el mínimo, el supremo y el ínfimo de S son únicos.

Un conjunto parcialmente ordenado es

(1) **Totalmente ordenado** si para cualesquiera dos elementos $x_1, x_2 \in X$ se tiene $x_1 \leq x_2$ ó $x_2 \leq x_1$.
(2) **Bien ordenado** si cada subconjunto no vacío tiene un elemento mínimo (o primer elemento)

Es claro que el conjunto $\mathbb{N}$ de los números naturales, con el orden usual, es un conjunto bien ordenado, por tanto totalmente ordenado. Sin embargo, el conjunto $\mathbb{Z}$ de los números enteros, aunque es totalmente ordenado, no es bien ordenado.

Amen de relaciones de orden, vamos a trabajar con relaciones de equivalencia, esto es, relaciones binarias R en un conjunto X que verifican las propiedades

(1) **Reflexiva**. Para todo $x \in X$ se tiene xRx.
(2) **Simétrica**. Para todo par $x_1, x_2 \in X$, si x_1Rx_2, entonces x_2Rx_1.
(3) **Transitiva**. Para toda terna $x_1, x_2, x_3 \in X$, si x_1Rx_2 y x_2Rx_3, entonces x_1Rx_3.

Ejemplo 1.1. Consideramos el conjunto $\mathbb{Z}$ de los números enteros y la relación de "*división*"; esto es, si $a, b \in \mathbb{Z}$ entonces $a|b$ cuando existe $x \in \mathbb{Z}$ tal que $b = xa$. Observa que esta relación verifica las propiedades reflexiva y transitiva, pero no la propiedad antisimétrica, pues $2|-2$ y $-2|2$, pero $2 \neq -2$. Podemos definir una nueva relación para números enteros:

$$aRb \text{ si } a|b \text{ y } b|a.$$

Es claro que R es una relación de equivalencia en $\mathbb{Z}$. Consideramos el conjunto cociente: $\mathbb{Z}/R$, en él tenemos una nueva relación. Si representamos por $[a]$ a la clase del número entero a, tenemos:

$$[a] \leq [b] \text{ si } a|b.$$

Para poder seguir trabajando necesitamos probar que ésta es una buena definición; esto es, que no depende de los representantes elegidos en las clases. Supongamos que $[a] = [a']$, por hipótesis existen $x, y \in \mathbb{Z}$ tales que $a' = xa$, $a = ya'$. Como consecuencia, si $a|b$, existe $z \in \mathbb{Z}$ tal que $b = za$. Tenemos entonces $b = za = zya'$, y por tanto $a'|b$, esto es, $[a'] \leq [b]$. De forma se trabajaría si tomamos otro representante de la clase $[b]$.

Una vez probado que la definición es correcta, falta ver que es una relación de orden. Las propiedades reflexiva y transitiva son inmediatas de probar. Para la propiedad antisimétrica, si $[a] \leq [b]$ y $[b] \leq [a]$, entonces $a|b$ y $b|a$, por tanto $[a] = [b]$, y se cumple la propiedad antisimétrica.

Observa que en este ejemplo se tiene una biyección entre el conjunto $\mathbb{Z}/R$ y el conjunto $\mathbb{N}$ de los números naturales, definida $f : \mathbb{N} \longrightarrow \mathbb{Z}/R$, $f(n) = [n]$ (considerando $\mathbb{N} \subseteq \mathbb{Z}$). Podemos definir en $\mathbb{N}$ la relación $a|b$ si existe $x \in \mathbb{N}$ tal que $b = xa$. Entonces f verifica: si $a|b$, entonces $f(a) \leq f(b)$.

Dados dos conjuntos parcialmente ordenados X e Y, una aplicación $f : X \longrightarrow Y$ es **creciente** (también se llama **monótona**) si para todo par de elementos $x_1, x_2 \in X$ cuando $x_1 \leq x_2$, se tiene $f(x_1) \leq f(x_2)$. En el ejemplo anterior $f : \mathbb{N} \longrightarrow \mathbb{Z}/R$ es una aplicación monótona.

Dado un conjunto parcialmente ordenado con relación de orden $\leq$, la relación de **orden estricto** asociada a $\leq$ es la relación binaria "$<$", definida:

$$a < b \text{ si } a \leq b \text{ y } a \neq b.$$

Observa que $<$ sólo verifica la propiedad transitiva, no verifica las propiedades reflexiva ni antisimétrica.

Dados dos conjuntos parcialmente ordenados X e Y, una aplicación $f : X \longrightarrow Y$ es **estrictamente creciente** (también se llama **isótona**) si para todo par de elementos $x_1, x_2 \in X$ cuando $x_1 < x_2$, se tiene $f(x_1) < f(x_2)$. En el ejemplo anterior $f : \mathbb{N} \longrightarrow \mathbb{Z}/R$ es una aplicación isótona.

2. Conjuntos bien ordenados y ordinales

La introducción de los ordinales la llevaremos a cabo a partir de los conjuntos bien ordenados. Recuerda que un conjunto bien ordenado es un conjunto parcialmente ordenado en el que cada subconjunto no vacío tiene un primer elemento; en consecuencia, todo conjunto bien ordenado es un conjunto totalmente ordenado.

Lema 2.1. *Si X un conjunto bien ordenado y $f : X \longrightarrow X$ una aplicación estrictamente creciente (o isótona), entonces $f(x) \geq x$, para todo $x \in X$.*

DEMOSTRACIÓN. Si definimos $T = \{x \in X |\ f(x) < x\}$, vamos a ver que $T = \emptyset$. Supongamos que T es no vacío, por ser X un conjunto bien ordenado, existe el mínimo de T. Sea mín$(T) = x$. Entonces se verifica: $f(x) < x$; como f es isótona, tendríamos $f(f(x)) < f(x)$ por lo que $f(x) \in T$ y ésto es absurdo ya que $f(x) < x = \text{mín}(T)$.

Si X es un conjunto bien ordenado, un **segmento inicial** de A es un subconjunto propio, $A \subset X$, de manera que para todo $y \in A$ tenemos que todos los elementos $z < y$ están también en el subconjunto A.

Lema 2.2. *Sea X un conjunto bien ordenado, se verifica:*

(1) X no es isomorfo a ningún segmento inicial $A_x = \{y \in X |\ y < x\}$.

(2) Si $A \subseteq X$ es un segmento inicial de X, entonces $A = A_x$, para algún $x \in X$ si, y sólo si, $X \setminus A$ tiene mínimo.

DEMOSTRACIÓN. (1). Probamos que X no es isomorfo a ninguno de sus segmentos iniciales. Si existe un isomorfismo $f : X \longrightarrow A_x$ para algún $x \in X$, entonces $f(x) \in A_x$ por tanto $f(x) < x$ y estaríamos contradiciendo el Lema (2.1.).

(2). Si el segmento inicial A es de la forma $A_x = \{y \in X |\ y < x\}$, entonces $x = \text{mín}(X \setminus A_x)$. Recíprocamente, si existe $x \in X$ tal que $x = \text{mín}(X \setminus A)$, veamos que $A = A_x$. Si $y \in A$, como A es segmento inicial y $x \in X \setminus A$, tenemos que $y < x$, esto es, $y \in A_x$. por lo que $y < x$; ya que x es mínimo en $X \setminus A$ entonces $y \notin X \setminus A$ si no que $y \in A$. Para terminar, Como todo segmento inicial es propio entonces $X \setminus A \neq \emptyset$ y como X es un conjunto bien ordenado, si tomamos $x = \text{mín}(X \setminus A)$ obtenemos que $A = A_x$.

Corolario 2.3. *Si X es un conjunto bien ordenado, entonces el único isomorfismo $f : X \longrightarrow X$ es la identidad.*

DEMOSTRACIÓN.Si f es un isomorfismo, tanto f como su inversa, f^{-1}, cumplen el Lema (2.1.). Esto es, si a cualquier $x \in X$ le aplicamos el Lema (2.1.) para f^{-1}, tendríamos que $f^{-1}(x) \geq x$ y si a ésta desigualdad le aplicamos el mismo lema para f, tenemos que $x \geq f(x)$. Como el Lema (2.1.) nos dice que $f(x) \geq x$, llegamos a que $f(x) = x$, y esto quiere decir que f es la identidad.

Corolario 2.4. *Si X es un conjunto bien ordenado, para cada conjunto bien ordenado Y existe como mucho un isomorfismo $X \longrightarrow Y$.*

DEMOSTRACIÓN. Utilizamos el Corolario (2.3.); si $f : X \longrightarrow Y$ y $g : X \longrightarrow Y$ son isomorfismos, entonces se tiene que $g^{-1} \circ f : X \longrightarrow X$ es un isomorfismo, y por lo tanto la identidad. Es decir, se tiene $f = g$.

A raíz de los expuesto hasta ahora, podemos destacar el siguiente resultado sobre conjuntos bien ordenados.

Teorema 2.5. *Si X e Y son dos conjuntos bien ordenados, se verifica una de las siguientes situaciones, mutuamente excluyentes:*

(I) X e Y son isomorfos.
(II) X es isomorfo a un segmento inicial de Y.
(III) Y es isomorfo a un segmento inicial de X.

DEMOSTRACIÓN. Sabemos que, por los corolarios y lemas vistos, éstas propiedades son excluyentes dos a dos y además el isomorfismo es único. Para la demostración basta comprobar que se da una de estas situaciones. Para cada $x \in X$ definimos $A_x = \{z \in X | \, z < x\}$, y para cada $y \in Y$ definimos $A_y = \{z \in Y | \, z < y\}$. Ahora construimos un subconjunto $X' \subseteq X$ y un subconjunto $Y' \subseteq Y$ mediante:

$$X' = \{x \in X | \text{ existe } y \in Y \text{ tal que } A_x \cong A_y\},$$
$$Y' = \{y \in Y | \text{ existe } x \in X \text{ tal que } A_x \cong A_y\}.$$

Si $x \in X'$ existe $y \in Y$ y un isomorfismo $f : A_x \cong A_y$, y para cada $x' \in A_x$ tendremos un isomorfismo entre $A_{x'}$ y $A_{f(x')}$; en consecuencia X' es un segmento inicial ó $X' = X$. Si $y \in Y'$, existe $x \in X$ y un isomorfismo $f : A_x \cong A_y$, y para cada $y' < y$ tendremos un isomorfismo entre $A_{y'}$ y $A_{f^{-1}(y')}$; en consecuencia, Y' es un segmento inicial o $Y' = Y$.

Veamos que existe una aplicación inyectiva de X' a Y'; en efecto, si $A_x \cong A_{y_1}$ y $A_x \cong A_{y_2}$, entonces $A_{y_1} \cong A_{y_2}$; si $y_1 \neq y_2$, sea $y_1 < y_2$, entonces $A_{y_1} \subseteq A_{y_2}$, lo que es una contradicción. En consecuencia, $y_1 = y_2$. Llamamos $\varphi : X' \longrightarrow Y'$ a esta aplicación.

Veamos que $\varphi : X' \longrightarrow Y'$ es una aplicación monótona. Si $x_1, x_2 \in X'$ verifican $x_1 \leq x_2$, existen $y_1, y_2 \in Y'$ e isomorfismos $f_i : A_{x_i} \cong A_{y_i}$, para $i = 1, 2$, entonces $A_{y_1} \cong A_{x_1} \subseteq A_{x_2} \cong A_{y_2}$, lo que implica $y_1 \leq y_2$.

Como consecuencia, se tiene un isomorfismo $X' \cong Y'$, ya que podemos construir una aplicación inversa de φ.

Finalmente, vamos a ver que necesariamente se tiene una de las siguientes tres posibilidades:

(1) $X = X' \overset{\varphi}{\cong} Y' = Y$.
(2) Si $X' \neq X$ e $Y' = Y$, entonces X' es un segmento inicial, y existe $x \in X$ tal que $X' = A_x$ y por tanto Y es isomorfo a un segmento inicial de X.
(3) Si $X' = X$ e $Y' \neq Y$, entonces Y' es un segmento inicial, y existe $y \in Y$ tal que $Y' = A_y$ y por tanto X es isomorfo a un segmento inicial de Y.
(4) Si $X' \neq X$ e $Y' \neq Y$ existen $x \in X$ e $y \in Y$ tales que $X' = A_x$ e $Y' = A_y$, y por tanto $x \in X'$ e $y \in Y'$, lo que es una contradicción.

Ahora, la finalidad será ver si los ordinales valen para representar a los conjuntos bien ordenados, por tanto vamos a ir estudiando sus propiedades.

Un conjunto X es **transitivo** si cada elemento $x \in X$ verifica que para cada $y \in x$ se tiene $y \in X$.

Un **ordinal** (ó un **número ordinal**) es un conjunto transitivo en el que la relación definida, para cada par de elementos $x, y \in X$, por $y \in x$, es un buen orden.

Ejemplo 2.6. Para cada número natural $n \in \mathbb{N}$ definimos $n = \{0, 1, \ldots, n-1\}$. Observa que para cada $n \in \mathbb{N}$ tenemos un ordinal, ya que $\{0, 1, \ldots, n-1\}$ es transitivo, y la relación de pertenencia es un buen orden. También $\mathbb{N} = \{0, 1, 2, \ldots\}$ es un ordinal.

Ejemplo 2.7. El conjunto $\{1, 2\}$ no es un ordinal, ya que no es transitivo.

Para cada ordinal σ definimos $S(\sigma) = \sigma + 1 = \sigma \cup \{\sigma\}$.

Lema 2.8. *Para cada ordinal σ se tiene que $\sigma + 1$ es un ordinal.*

DEMOSTRACIÓN. Cada elemento de $S(\sigma)$ es ó un elemento de σ ó σ, que también es un subconjunto de $S(\sigma)$; por tanto $S(\sigma)$ es transitivo. Además como $\sigma \notin \sigma$, y $\tau < \sigma$ para todo $\tau \in \sigma$, concluimos que $S(\sigma)$ está bien ordenado.

Llamamos a $S(\sigma) = \sigma + 1$ es **siguiente** de σ.

En atención a esta definición distinguimos varios tipos de ordinales:

(1) **Ordinal sucesor**, si es de la forma $S(\sigma) := \sigma \cup \{\sigma\}$ para algún ordinal σ.
(2) **Ordinal nulo**, es $0 := \emptyset$.
(3) **Ordinal límite**, aquel que no es ni ordinal sucesor ni ordinal nulo.
(4) **Ordinal finito**, el que verifica que para todo ordinal $\tau < \sigma$ se tiene $\tau = 0$ ó τ es un ordinal sucesor.

Ejemplos 2.9. (1) Por extensión, a los ordinales finitos también se les llama **números naturales**.
(2) Todos los números naturales mayores que 0 son ordinales sucesores.
(3) El primer ordinal límite es el ordinal del conjunto de los números naturales, y la representamos por ω u ω_1.

Lema 2.10. *Si σ es un ordinal y $x \in \sigma$ un elemento, entonces x es un ordinal.*

En otras palabras, cada elemento de un ordinal es un ordinal. DEMOSTRACIÓN. Tenemos que $x = A_x$ es un subconjunto de σ. Para cada $y \in x$, por ser transitivo, tenemos que $y \in \sigma$, y por tanto y es un segmento inicial A_y. Como $y < x$, entonces $y = A_y$ es subconjunto de $A_x = x$.

Una vez visto que los elementos de un ordinal σ son también ordinales, veamos si el recíproco también es cierto. Vamos a ver que los ordinales contenidos en σ son elementos de σ.

Lema 2.11. *Sean σ y τ ordinales, si $\sigma \subset \tau$ entonces $\sigma \in \tau$.*

DEMOSTRACIÓN. Si $\sigma \subset \tau$, esto es $\tau \setminus \sigma \neq \emptyset$, por lo que habrá un primer elemento λ debido a que τ es un conjunto bien ordenado. Basta probar que $\lambda = \sigma$.

Si $x \in \lambda$ entonces $x < \lambda$ y como λ es mínimo de $\tau \setminus \sigma$, se tiene $x \in \sigma$.

Si $x \in \sigma$ entonces no se tiene $\lambda \leq x$, ya que: o bien $\lambda = x$, y entonces $\lambda = x \in \sigma$, o bien $\lambda < x$, y entonces $\lambda \in x$, y por tanto $\lambda \in \sigma$, lo que es una contradicción, porque $\lambda \notin \sigma$.

Por tanto, $x < \lambda$, esto es, $x \in \lambda$, entonces $\sigma = \lambda$.

Hemos probado que un número ordinal es un conjunto que está formado por todos sus subconjuntos propios los cuales son números ordinales.

Observación. 2.12. Para cada ordinal σ se tiene $\sigma \notin \sigma$.

Observación. 2.13. Tenemos que si σ es un ordinal con $\sigma \neq \emptyset$ entonces $\emptyset \subset \sigma$, por tanto $0 = \emptyset \in \sigma$.

Esquemáticamente, para un ordinal σ tenemos la siguiente situación:

- Si $\emptyset \subseteq \sigma$, entonces $0 = \emptyset \in \sigma$, y tenemos $1 = \{0\} \subseteq \sigma$.
- Si $\sigma = 1$ tenemos una buena descripción de σ, y en caso contrario $1 = \{0\} \subset \sigma$.
- En este segundo caso se tiene $1 \in \sigma$, y tenemos $2 = \{0, 1\} \subseteq \sigma$.
- ...
- Repitiendo el proceso llegamos a que σ es un número natural o bien $\omega_1 \subseteq \sigma$.
- Si $\omega_1 = \sigma$, tenemos una buena descripción de σ, y en caso contrario $\omega \subset \sigma$.
- En este segundo caso se tiene $\omega \in \sigma$, y tenemos $\omega + 1 \subseteq \sigma$.
- Y seguimos este proceso.

Con este esquema nos damos cuenta que los ordinales tienen el aspecto que comentábamos al principio de este capítulo.

Dicho ésto; vamos a tratar cada número ordinal como un conjunto en el cual definimos:

- un orden $\sigma < \tau$ cuando $\sigma \in \tau$, o equivalentemente $\sigma \subset \tau$,
- un orden $\sigma \leq \tau$ cuando $\sigma < \tau$ ó $\sigma = \tau$, o equivalentemente $\sigma \subseteq \tau$,

para así ver que con este orden los ordinales van a comportarse como un conjunto bien ordenado salvo por no forman un conjunto; esto es, *no existe el conjunto de todos los ordinales (Burali-Forti)*.

Teorema 2.14. *Sean σ, τ, λ ordinales, se verifica:*

(1) Si $\sigma < \tau$ y $\tau < \lambda$ entonces $\sigma < \lambda$.
(2) Si $\sigma < \tau$ entonces $\tau \not< \sigma$
(3) Para cada dos ordinales ó $\sigma \leq \tau$ ó $\tau \leq \sigma$.
(4) Si T es una colección no vacía de ordinales entonces existe α de T de manera que $\alpha \leq \alpha'$ para todo α' de T.
(5) Si X es un conjunto de ordinales entonces $\bigcup X$ es el supremo de X. Esto es, σ es un ordinal de manera que $\tau \leq \sigma$ para todo $\tau \in X$ y esto implica que $\sigma + 1$ es un ordinal que no puede estar en X y σ es el mínimo entre los ordinales σ' de manera que $\tau \leq \sigma'$ para todo $\tau \in X$

DEMOSTRACIÓN. (1) y (2) son consecuencia del Lema (2.11.). (1) se debe a la transitividad de λ y (2) sigue a (1) porque si $\sigma < \tau < \sigma$ tendríamos $\sigma < \sigma$.

(3). Para demostrarlo vamos a considerar $\sigma \cap \tau$ que obviamente es un ordinal. Por la Observación (2.12.) se tiene $\sigma \cap \tau \notin \sigma \cap \tau$. Por tanto, o bien $\sigma \cap \tau \notin \sigma$ ó $\sigma \cap \tau \notin \tau$.

Si $\sigma \cap \tau \notin \sigma$, es decir, $\sigma \cap \tau \not\subset \sigma$ entonces $\sigma \cap \tau = \sigma$, debido a que $\sigma \cap \tau \subseteq \sigma$, esto es, $\sigma \subseteq \tau$ que significa $\sigma \leq \tau$.

Si $\sigma \cap \tau \notin \tau$, es decir, $\sigma \cap \tau \not\subset \tau$ entonces $\sigma \cap \tau = \tau$ debido a que $\sigma \cap \tau \subseteq \tau$, esto es, $\tau \subseteq \sigma$ que significa $\tau \leq \sigma$.

(4). Fijamos α_0 de T. Entonces, por el Axioma de Separación, $T' = \{\alpha' \in \alpha_0 |\ \alpha \in T\}$ es un conjunto.

- Si $T' = \emptyset$ para cada $\alpha' \in T$ tenemos que $\alpha' \notin \alpha_0$ entonces $\alpha' \not< \alpha_0$, y aplicando (3) se tiene $\alpha_0 < \alpha'$, entonces $\alpha = \alpha_0$.
- Si $T' \neq \emptyset$ entonces, como α_0 tiene buen orden eso implica que α va a ser el primer elemento de T'.

Por tanto, si $\alpha' \in T$; o bien $\alpha' \in \alpha_0$ o bien $\alpha' \notin \alpha_0$.

(I) si $\alpha' \in \alpha_0$, entonces $\alpha \leq \alpha'$.
(II) si $\alpha' \notin \alpha_0$, entonces $\alpha_0 \leq \alpha'$.

Juntando (I) y (II) resulta que $\alpha < \alpha'$.

Por último; observamos que $\cup X$ es un conjunto de ordinales por el Lema (2.10.), (cada elemento de un ordinal es un ordinal) por (3) y (4) observamos también que está bien

ordenado y $\sigma = \cup X$ es un conjunto transitivo ya que si por ejemplo, $X = \{1,2,4\}$, $\cup X = 1 \cup 2 \cup 4$, entonces $4 = \{0,1,2,3\}$ y $4 \in X$ pero $4+1 = 5 \notin X$.

Luego; si $\tau \in X$ tendremos $\tau \subset \sigma$, esto es, $\tau \leq \sigma$. Sea $\sigma' \in \sigma = \cup X$ entonces $\sigma' \in \tau$ o lo que es lo mismo $\sigma' < \tau$ para algún $\tau \in X$ entonces no hay $\sigma' < \sigma$ que sea cota superior de X, es decir, no hay σ' de tal manera que $\tau \leq \sigma'$ para todo $\tau \in X$ cumpla que $\sigma' < \sigma$. Aplicando (3) tenemos que $\sigma \leq \sigma'$.

Teorema 2.15. *Los números naturales son los ordinales finitos.*

DEMOSTRACIÓN. Por el Ejemplo (2.6.), sabemos que cada número natural es ordinal y finito. Lo que hay que comprobar es que un ordinal finito es un número natural.

Sea $\mathbb{N} = \omega$ y σ un ordinal. Si σ no es natural entonces $\sigma \notin \omega$ esto es, $\sigma \not< \omega$, entonces usando el Teorema (2.14.), $\omega \leq \sigma$, esto es $\omega \subseteq \sigma$. Es decir, σ es infinito ya que contiene al conjunto infinito de los naturales. Por tanto, σ tiene que ser natural.

Llegados a este punto, podemos citar el objetivo de ésta sección con el siguiente teorema:

Teorema 2.16. *Cada conjunto bien ordenado es isomorfo a un único ordinal.*

DEMOSTRACIÓN. Hemos visto anteriormente que dados dos ordinales σ y τ ó son isomorfos ó uno es un segmento inicial del otro. Basándonos en el Corolario (2.3.); ahora podemos también decir que cada conjunto bien ordenado es isomorfo, como mucho, a un único ordinal. Veámoslo.

Sea $(X, \leq)$ un conjunto bien ordenado; sea $\leq$ una relación entre los elementos x de X, es decir, $x \in X$ y sea σ el único ordinal al que es isomorfo y sea A un subconjunto, $A \subseteq X$ formado por los elementos $x \in X$.

Definimos la relación binaria $\varphi(x,\sigma) := \{x \in A |$ existe $f : A_x \cong \sigma\}$.

Entonces si $x \in A$ y σ, σ' son dos ordinales, la relación $\varphi(x,\sigma)$ y $\varphi(x,\sigma')$ nos dice que σ y σ' son isomorfos ya que del Corolario (2.1.) precede que dos ordinales σ y σ' son isomorfos entonces $\sigma = \sigma'$ y el único isomorfismo es la identidad.

Veamos distintos puntos.

- Sea A_x un segmento inicial de A, tenemos que para todo $x \in A_x$ existe σ de manera que $f : A_x \cong \sigma$. Tomamos un $z \in A$ con $z < x$, entonces A_z es un subconjunto de A_x y, además, es segmento inicial de A_x.

- Si definimos $\tau := f(A_z)$ la imagen, diríamos que $f(A_Z \subseteq \sigma$ debido a que f define un isomorfismo que también es segmento inicial de σ, lo cual, $\tau \leq \sigma$.

- Si definimos ahora, por restricción, la función h como un isomorfismo entre A_y y τ (siendo τ un ordinal) tendríamos que la relación binaria $\varphi(z,\tau)$ y $z \in A_x$.

- Sea O un ordinal; se cumple que O es un segmento inicial de la clase de los ordinales (todo conjunto transitivo de ordinales es un ordinal porque σ es un conjunto transitivo por hipótesis y la relación de pertenencia $\in$ sobre σ, para un buen orden estricto y todo conjunto $\neq \emptyset$ de ordinales tiene un mínimo ($\sigma \in X$ y $\sigma = \text{mín}(X)$)).
- Se define g como isomorfismo entre $A_x \subseteq A$ y el ordinal O. Sabemos que g es sobreyectiva y estrictamente creciente por tanto g es un isomorfismo.
- Si $A_x \subsetneq A$ y tomamos $x_0 = \text{mín}(A \setminus A_x)$. Se tiene que $A_x = A_{x_0}$ y como $g : A_{x_0} \longrightarrow O$ es un isomorfismo, tendríamos la relación binaria como $\varphi(x_0, 0)$ por tanto $A_x = A$.

Juntando todos los puntos vemos que g es un isomorfismo entre $(X, \leq)$ y A.

3. Aritmética de ordinales

En la teoría de conjuntos, la aritmética de los ordinales describe las operaciones que usamos normalmente con números ordinales tales como son la suma, la multiplicación y la exponenciación.

Adición.

Sean τ y σ ordinales, su suma $\tau + \sigma$ es la operación definida por recurrencia sobre σ mediante:

(I) $\tau + 0 = \tau$.

(II) $\tau + (\sigma + 1) = (\tau + \sigma) + 1$.

(III) $\tau + \sigma = \bigcup_{\sigma' < \sigma} (\tau + \sigma')$ si σ es un ordinal límite (es decir, $\tau + \sigma$ es el limite de $\tau + \sigma'$ para todo $\sigma' < \sigma$).

Observación. 3.1. Cuando aparece $+1$ tras el número ordinal, hacemos referencia a su sucesor, no a la suma con 1 aunque ambas cosas coinciden.

Observación. 3.2. La suma de los ordinales cumple con la propiedad asociativa y elemento neutro, pero no es conmutativa ni cancelativa ya que $n + \omega = \bigcup_{r \in \mathbb{N}} (n + r) = \omega$ es distinto de $\omega + n$ porque

$$\omega + n = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + (n - 1)\}.$$

y

$$\omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}.$$

Además, si $n + \omega = r + \omega$ no tiene el porqué de ocurrir que $n = r$

Multiplicación.

Sean τ y σ ordinales, su producto $\tau \cdot \sigma$ es la operación definida por recurrencia sobre σ mediante:

(I) $\tau \cdot 0 = 0$

(II) $\tau \cdot (\sigma + 1) = (\tau \cdot \sigma) + \tau$

(III) $\tau \cdot \sigma = \bigcup_{\sigma' < \sigma} (\tau \cdot \sigma')$ si σ es un ordinal límite y $\sigma \neq 0$

Observación. 3.3. A la multiplicación le ocurre lo mismo que a la suma; que no es ni conmutativa ni cancelativa ya que, por ejemplo, $\tau \cdot 2 = \tau \cdot (1+1) = \tau \cdot 1 + \tau \cdot 1 = \tau + \tau$ (siendo τ un ordinal).
Usando inducción sobre n tendríamos: $\tau \cdot n = \tau + \ldots + \tau$. Particularmente, haciendo de forma análoga a lo que hemos hecho con la suma en la Observación (3.2.), tenemos;

$$\omega \cdot n = \omega + \ldots + \omega = \{0, 1, \ldots, \omega, \omega + 1, \ldots, \omega \cdot (n-1), \omega \cdot (n-1) + 1, \ldots\}$$

y

$$\omega \cdot \omega = \{0, 1, \omega, \omega + 1, \ldots, \omega \cdot n, \omega \cdot n + 1, \ldots\}.$$

En cambio, $n \cdot \omega = \bigcup_{r \in \omega} (n \cdot r) = \omega$.

Exponenciación.

Sean τ y σ ordinales, la exponenciación τ^σ es la operación definida por recurrencia sobre σ mediante:

(I) $\tau^0 = 1$.

(II) $\tau^{\sigma+1} = \tau^\sigma \cdot \tau$.

(III) $\tau^\sigma = \bigcup_{\sigma' < \sigma} (\tau^{\sigma'})$ si σ es un ordinal límite y $\sigma \neq 0$.

Esta primera aproximación a la aritmética de ordinales se completa con una aritmética más avanzada el que el principal exponente es el siguiente resultado.

Teorema 3.4. (Teorema de la forma normal de Cantor) *Cada ordinal $\sigma \neq 0$ se representa de forma única como*

$$\sigma = \omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_t} n_t,$$

con $\alpha_1 > \cdots > \alpha_t \geq 0$, ordinales, y $n_1, \ldots, n_t \in \mathbb{N}$.

Existen otras operaciones suma y producto de ordinales que sí son asociativas, conmutativas y distributivas; una de ellas es la **suma** y el **producto natural** o de **Hessenberg**. Se representan por $\sigma \oplus \tau$ y $\sigma \otimes \tau$, respectivamente, y están definidas como sigue:

$$\sigma \oplus \tau = \sup(\{\sigma + \beta |\ \beta < \tau\} \cup \{\alpha + \tau |\ \alpha < \sigma\}),$$

$$\sigma \otimes \tau = \text{mín}\{\gamma |\ \gamma \oplus (\alpha \otimes \beta) > (\sigma \otimes \beta) \oplus (\alpha \otimes \tau)\}.$$

Si las formas normales de Cantor de σ y de τ son

$$\begin{aligned} \sigma &= \omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_t} n_t, \\ \tau &= \omega^{\alpha_1} m_1 + \cdots + \omega^{\alpha_t} m_t, \end{aligned}$$

donde algún n_i ó m_j puede ser cero, se tendría:

$$\begin{aligned} \sigma \oplus \tau &= \omega^{\alpha_1}(n_1 + m_1) + \cdots + \omega^{\alpha_t}(n_t + m_t), \\ \sigma \otimes \tau &= \textstyle\sum_{i=1}^{t} \sum_{j=1}^{t} \omega^{\alpha_i \oplus \alpha_j} n_i m_j. \end{aligned}$$

Capítulo 2

NOCIONES BÁSICAS SOBRE ANILLOS

1. Anillos

Un **anillo** es un conjunto R junto con dos operaciones $+$, suma, y $\times$, multiplicación, y un elemento $1 \in R$, verificando las siguientes propiedades:

(1) $(R, +)$ es un grupo abeliano. Representamos por 0 al elemento neutro, y lo llamamos el **cero** del anillo.
(2) $(R, \times, 1)$ es un monoide. El elemento 1 se llama el **uno** del anillo.
(3) La multiplicación es distributiva respecto a la suma:

$$a \times (b + c) = a \times b + a \times c,$$
$$(b + c) \times a = b \times a + c \times a,$$

para todos $a, b, c \in R$.

Un anillo R es un **anillo conmutativo** si la multiplicación es conmutativa. En general vamos a utilizar la letra A para referirnos a anillos conmutativos.

La primera propiedad que podemos probar en un anillo es la siguiente:

Lema 1.1. *Si R es un anillo se verifica:*

(1) Existe un único elemento cero.
(2) Existe un único elemento uno.
(3) Para cada elemento $a \in A$ se verifica $0 \times a = 0 = a \times 0$.

Por comodidad, la multiplicación $\times$ se representa, a veces como el símbolo $\cdot$, o simplemente por yuxtaposición.

Observa que si $0 = 1$ en un anillo, entonces $R = \{0\}$. Este anillo se llama el **anillo trivial**. En lo que sigue suponemos que los anillos que estudiamos son no triviales.

Veamos algunos tipos especiales de elementos de un anillo R:

(1) Un elemento $a \in R$ es **invertible a la izquierda** si existe $b \in A$ tal que $ba = 1$. Análogamente se define **elemento invertible a la derecha**. Un elemento $a \in R$ es **invertible** si es invertible a la derecha y a la izquierda.
(2) Un elemento $a \in R$ es un **divisor de cero a la izquierda** si existe $0 \neq b \in A$ tal que $ba = 0$, y análogamente se define **divisor de cero a la derecha**. Un elemento $a \in R$ es un **divisor de cero** si es un divisor de cero a la izquierda ó a la derecha.
(3) Un elemento $a \in R$ es un **elemento regular** si no es divisor de cero a izquierda ni a derecha.
(4) Un elemento $a \in R$ es **nilpotente** si existe una potencia a^n igual a cero.

Estos tipos de elementos permiten una primera clasificación de anillos.
Un anillo R es

(1) un **anillo de división** si cada elemento no nulo es invertible.
(2) un **anillo de integridad** si cada elemento no nulo es regular.
(3) un **dominio** o **dominio de integridad** si es un anillo de integridad conmutativo.
(4) un **cuerpo** si es un anillo de división conmutativo.

Dados dos anillos R y S, un **homomorfismo de anillos** de R a S es una aplicación $f : R \longrightarrow S$ que es homomorfismo para la suma, la multiplicación y el uno.

Lema 1.2. *Para cada anillo R existe un único homomorfismo de anillos de $\mathbb{Z}$ a R, definido por $f(n) = n1$, para cada $n \in \mathbb{Z}$.*

Dado un homomorfismo de anillos $f : R \longrightarrow S$ llamamos **núcleo** de f a

$$\mathrm{Ker}(f) = \{r \in R |\ f(r) = 0\},$$

y llamamos **imagen** de f a

$$\mathrm{Im}(f) = \{f(r) \in R |\ r \in R\}.$$

El núcleo $\mathrm{Ker}(f)$ verifica las siguientes propiedades:

(1) $\mathrm{Ker}(f)$ es un subgrupo aditivo.
(2) $ax, xa \in \mathrm{Ker}(f)$ para cada $x \in \mathrm{Ker}(f)$ y cada $a \in R$.

Ejemplo 1.3. Los ideales de $\mathbb{Z}$ son los subconjuntos de la forma $n\mathbb{Z} = \{nx \in \mathbb{Z} |\ x \in \mathbb{Z}\}$.

Un subconjunto $\mathfrak{A} \subseteq R$ que verifica estas dos propiedades se llama un **ideal** de R.
La imagen $\mathrm{Im}(f)$ verifica las siguientes propiedades:

(1) $\mathrm{Im}(f)$ es un subgrupo aditivo.
(2) $a + b, ab \in \mathrm{Im}(f)$ para cada $a, b \in \mathrm{Im}(f)$.
(3) $1 \in \mathrm{Im}(f)$.

Un subconjunto $T \subseteq R$ que verifica estas dos propiedades se llama un **subanillo** de R. Observa que cada subanillo es un anillo con las restricciones de las operaciones suma y multiplicación, y la inclusión $T \hookrightarrow R$ es un homomorfismo de anillos.

Observación. 1.4. Todo subanillo de un anillo de integridad es un anillo de integridad; en particular, todo subanillo de un cuerpo es un domino de integridad. Para cada anillo R el único homomorfismo de anillos $f : \mathbb{Z} \longrightarrow R$ define un entero positivo o nulo n tal que $\mathrm{Ker}(f) = n\mathbb{Z}$. Llamamos a n la característica de R. Si n es positivo, entonces n es el menor entero positivo que verifica $n1 = 0$, y si $n = 0$, entonces no existe ningún entero m tal que $m1 = 0$. El número n se llama la **característica** del anillo R.

Todo ideal $\mathfrak{A} \subseteq R$ define una relación de equivalencia en R:

$$a \sim_{\mathfrak{A}} b \text{ si } a - b \in \mathfrak{A}.$$

En el conjunto cociente $R/\sim_{\mathfrak{A}}$ se definen operaciones suma y producto

$$[a] + [b] = [a + b],$$
$$[a] \times [b] = [a \times b],$$

que, junto con $[1]$ definen una estructura de anillo de forma que la proyección $R \longrightarrow R/\sim_{\mathfrak{A}}$ es un homomorfismo de anillos. El anillo $R/\sim_{\mathfrak{A}}$ se representa, abreviadamente, como $R/\mathfrak{A}$.

Un homomorfismo de anillos $f : R \longrightarrow S$ es un **isomorfismo** si existe un homomorfismo de anillos $g : S \longrightarrow R$ tal que $fg = \mathrm{id}_S$ y $gf = \mathrm{id}_R$. Es fácil ver que f es un isomorfismo si, y sólo si, f es una aplicación inyectiva y sobreyectiva. En particular, observa que se tiene un isomorfismo entre $R/\mathrm{Ker}(f)$ e $\mathrm{Im}(F)$ (Primer teorema de isomorfía).

2. Ideales

Un subconjunto $\mathfrak{a} \subseteq R$ es un **ideal a izquierda** si verifica:

(1) $\mathfrak{a} \subseteq R$ es un subgrupo aditivo.
(2) $ax \in \mathfrak{a}$ para cada $a \in R$ y cada $x \in \mathfrak{a}$.

De la misma forma se define **ideal a derecha**.

Lema 2.1. *Para cada familia $\mathscr{F}$ de ideales a izquierda de un anillo R se verifica:*

(1) La intersección de los elementos de la familia $\mathscr{F}$ es un ideal a izquierda. Se representa por $\cap\mathscr{F}$, y es el mayor ideal a izquierda contenido en todo elemento de $\mathscr{F}$.
(2) El conjunto $\{\sum_i a_i \mid a_i \in \mathscr{F}\}$ es un ideal a izquierda de R; se representa por $\sum\mathscr{F}$, y es el menor ideal a izquierda que contiene a todo elemento de $\mathscr{F}$.

Dado un subconjunto $G \subseteq R$ definimos el **ideal a izquierda generado** por G como el ideal

$$\langle G \rangle = \cap\{\mathfrak{a} |\ G \subseteq \mathfrak{a},\ \text{y } \mathfrak{a} \text{ es un ideal a izquierda}\}.$$

Un ideal a izquierda $\mathfrak{a}$ es **finitamente generado** si existe un conjunto finito contenido en R, $\{a_1, \ldots, a_t\} \subseteq R$, tal que $\mathfrak{a} = \langle a_1, \ldots, a_t \rangle$, y es **principal** si existe un elemento $a \in R$ tal que $\mathfrak{a} = \langle a \rangle$.

Lema 2.2. *Para cada subconjunto $G \subseteq R$ el ideal a izquierda $\langle G \rangle$ generado por G tiene los siguientes elementos:*

$$\langle G \rangle = \left\{ \sum_{i=1}^{t} a_i g_i |\ a_i \in R,\ g_i \in G \right\}.$$

El ideal a izquierda $\langle G \rangle$ también se representa por RG.

Un anillo R es **noetheriano a izquierda** si cada ideal a izquierda es finitamente generado, y es un **anillo de ideales a izquierda principales** si cada ideal a izquierda es un ideal principal.

Dados dos ideales a izquierda $\mathfrak{a}$ y $\mathfrak{b}$ su **producto** $\mathfrak{ab}$ se define como el ideal a izquierda generado el conjunto $\{ab |\ a \in \mathfrak{a},\ b \in \mathfrak{b}\}$.

Un ideal a izquierda $\mathfrak{p}$ es **primo** si $\mathfrak{p} \neq R$ y para cualesquiera ideales a izquierda $\mathfrak{a}, \mathfrak{b} \subseteq R$ tales que si $\mathfrak{ab} \subseteq \mathfrak{p}$, se tiene $\mathfrak{a} \subseteq \mathfrak{p}$ ó $\mathfrak{b} \subseteq \mathfrak{p}$. Si $R = A$ es un anillo conmutativo tenemos la siguiente caracterización de ideales primos.

Lema 2.3. *Sea A un anillo conmutativo, para un ideal propio $\mathfrak{p} \subsetneq R$ son equivalentes:*

(a) $\mathfrak{p} \subseteq R$ es un ideal primo.
(b) Para cualesquiera $a, b \in R$, si $ab \in \mathfrak{p}$, entonces $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.

Un ideal a izquierda $\mathfrak{m} \subseteq R$ es un ideal **maximal** si $\mathfrak{m} \neq R$ y para cualquier ideal a izquierda $\mathfrak{a}$ tal que $\mathfrak{m} \subseteq \mathfrak{a} \subsetneq R$ se tiene $\mathfrak{a} = \mathfrak{m}$.

Lema 2.4. *Sea A un anillo conmutativo, cada ideal maximal es un ideal primo.*

Proposición 2.5. *Sea A un anillo conmutativo, para cada ideal propio $\mathfrak{p}$ son equivalentes:*

(a) $\mathfrak{p}$ es un ideal primo.
(b) $A/\mathfrak{p}$ es un dominio de integridad.

Proposición 2.6. *Sea A un anillo conmutativo, para cada ideal propio $\mathfrak{m}$ son equivalentes:*

(a) $\mathfrak{p}$ es un ideal maximal.
(b) $A/\mathfrak{p}$ es un cuerpo.

3. Construcción de anillos

Producto de anillos

Dada una familia de anillos $\{R_i | \ i \in I\}$ en el producto cartesiano $\prod_i R_i$ se definen una operación suma y una multiplicación mediante:

$$(r_i)_i + (s_i)_i = (r_i + s_i)_i,$$
$$(r_i)_i(s_i)_i = (r_i s_i)_i,$$

que junto con el elemento $1 = (u_i)_i$, siendo $u_i = 1$ para cada índice i, forma un anillo. Para cada índice $j \in I$ existen un homomorfismo de anillos:

$$p_j : \prod_i R_i \longrightarrow R_j, \qquad p_j((r_i)_i) = r_j.$$

El producto de anillos verifica la siguiente propiedad universal.

Proposición 3.1. *Para cada anillo S y cada familia de homomorfismos de anillos $f_j : S \longrightarrow R - j$ existe un único homomorfismo de anillos $f : S \longrightarrow \prod_i R_i$ verificando $f(s) = (f_i(s))_i$ para cada $s \in S$.*

Anillos de polinomios

Para cada anillo R el **anillo de polinomios** en la indeterminada X con coeficientes en R tiene como conjunto subyacente las expresiones formales $\sum_{i=0}^{t} a_i X^i$, con $a_i \in R$ junto con las siguientes operaciones suma y multiplicación:

$$\sum_{i=0}^{t} a_i X^i + \sum_{i=0}^{s} b_i X^i = \sum_{i=0}^{\text{máx}\{t,s\}} (a_i + b_i) X^i,$$

siendo $a_i = 0$ si $i > t$ y $b_i = 0$ si $i > s$.

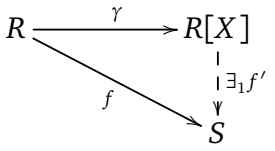
$$(\sum_{i=0}^{t} a_i X^i)(\sum_{i=0}^{s} b_i X^i) = \sum_{i=0}^{t+s} (\sum_{h+j=i} a_h + b_j) X^i,$$

y el elemento uno el polinomio constante igual a 1. En este caso tenemos un homomorfismo de anillos $\eta : R \longrightarrow R[X]$ definido $\gamma(r)$ es el polinomio constante igual a r.

El anillo de polinomios $R[X]$ está caracterizado por la siguiente propiedad universal.

Proposición 3.2. *Para cada anillo S, cada homomorfismo de anillos $f : R \longrightarrow S$ y cada elemento $b \in S$ tal que $f(r)b = bf(r)$ para cada $r \in R$ existe un único homomorfismo*

de anillos $f' : R[X] \longrightarrow S$ *tal que* $f = f'\gamma$.



Anillos de matrices

AÑADO:

Consideramos: $I = J = \{1, 2, \ldots, n\}$ conjuntos de números enteros positivos, y A una matriz. Las aplicaciones son de la forma $f : I \times I \longrightarrow \langle R, +, \cdot, 0\rangle$ cuyos elementos vienen dados por:

$$f = (a_{ij})_{n\times n} = (a_{ij})_n = A_{n\times n} = A_n = A$$

En este caso, el conjunto de éstas aplicaciones lo llamamos conjunto de matrices porque la operación producto que vamos a definir, si tiene sentido como lo que usualmente entendemos como matrices. Sea el conjunto $M_n(R) = \{(a_{ij})_{n\times n}\}$ junto con las operaciones

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})(a_{ij}) \cdot (b_{ij}) = (\sum_{j=1}^{n}(a_{ij}b_{jk})) = (d_{ij})$$

conseguimos que el conjunto $M_n(R)$ sea un anillo.

Vamos a probarlo:

Sea la matriz $A = (a_{ij})_n$ y $B = (b_{ij})_n$ otra matriz, la suma de ambas matrices sería $A + B = (a_{ij} + b_{ij})_n$.

Si tomamos la matriz B formada por el cero del anillo; todos los elementos son cero. Esto es, $B = (0_{ij})_n$. Si hacemos $(a_{ij} + 0_{ij})_n = (a_{ij})_n$ ya que cada uno de los elementos a_{ij} y 0_{ij}, al ser el neutro el cero del anillo y estar sumando elementos del anillo, pues obtenemos el mismo elemento.

Esto significaría que $A+0 = A$ siendo $0 = (0_{ij})_n$ y también $0+A = A$ y así tendríamos un elemento neutro para la suma de matrices cuadradas. Si en lugar de poner a_{ij} ponemos los opuestos de cada uno de ellos; si hacemos la suma $A + B = (a_{ij} + (-a_{ij}))_n = (0)_n$ y tendríamos para cada elemento un opuesto y entonces la matriz B la llamaríamos $-A$ y por tanto, $A+(-A) = (-A)+A = 0$. Obviamente la asociatividad $A+(B+C) = (A+B)+C$ es inmediata y también es inmediata la conmutatividad.

Así que el conjunto de éstas matrices cuadradas de orden o de tamaño n con entradas en el anillo A, es un grupo abeliano.

Ahora probamos la asociatividad del producto.

Sea $A=(a_{ij})_n, B=(b_{jk})_n, C=(c_{kr})_n$, veamos que $(AB)C=A(BC)$.
$(AB)C=(\sum_{j=1}^n a_{ij}b_{jk})(c_{kr})_n=(\sum_{k=1}^n(\sum_{j=1}^n a_{ij}b_{jk})c_{kr}))=(\sum_{k=1}^n\sum_{j=1}^n(a_{ij}b_{jk})c_{kr}))=$
$(\sum_{j=1}^n\sum_{k=1}^n a_{ij}(b_{jk}c_{kr}))=(\sum_{j=1}^n a_{ij}(\sum_{k=1}^n b_{jk}c_{kr}))=A(BC)$.
Probamos ahora la distributividad del producto respecto a la suma por ambos lados.

Sean las matrices cuadradas $A=(a_{ij})_{n\times n}, B=(b_{jk})_{n\times n}, C=(c_{kr})_{n\times n}$. Probamos que $A(B+C)=AB+AC$ y $(A+B)C=AC+BC$ pero no lo vamos a hacer ya que es un ejercicio de cálculo a partir de las definiciones que hemos dado para cada una de éstas operaciones. Una vez que probamos éstas propiedades, podemos asegurar que el conjunto de las matrices cuadradas de orden n con entradas en un anillo cualquiera con esa suma y ese producto, es un anillo.

En particular, también podemos probar que en el caso en que el anillo del que las matrices toman sus valores, fuera un anillo unitario; esto es, $\langle R,+,\cdot,0,1\rangle$, también sería éste anillo de matrices un anillo unitario. Por último nos preguntamos; ¿cuál sería la unidad? o mejor dicho, ¿cuál sería el elemento neutro para el producto?

Definimos

$$\delta_{ij}=\begin{cases}1, \text{ si } i=j,\\ 0, \text{ si } i\neq j,\end{cases}$$

Y definimos la matriz $I=(\delta_{ij})_{n\times n}$ que es justamente el uno del anillo de las matrices cuadradas de orden n con entradas en ese anillo unitario, ya que $AI=IA=A$.

Cabe destacar que no importa el anillo de matrices cuadradas que tomemos siempre que n sea mayor que 1; esto es, siempre que $n\geq 2$. Es decir, no importa qué anillo sea que siempre tendremos divisores de cero aunque no los tenga el anillo de partida. Veámoslo.

Consideramos un anillo R que no tenga divisores de cero; $\langle R,+,\cdot,0\rangle$ anillo sin divisores de cero, y consideramos dos elementos a y b de ese anillo, ambos distintos de cero, $a,b\neq 0$. (no es necesario que los elementos sean divisores de cero). Vamos a formar matrices de orden n con $n\geq 2$.

$$\begin{pmatrix}a&0&\cdots&0\\0&0&\cdots&0\\\vdots&\cdots&&\vdots\\0&0&\cdots&0\end{pmatrix}_{n\times n}\cdot\begin{pmatrix}b&0&\cdots&0\\0&0&\cdots&0\\\vdots&\cdots&&\vdots\\0&0&\cdots&0\end{pmatrix}_{n\times n}=\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\vdots&\cdots&&\vdots\\0&0&\cdots&0\end{pmatrix}_{n\times n}=0$$

Vemos entonces que siendo las matrices $A,B\neq 0$ tenemos que $A\cdot B=0$ por lo que tenemos divisores de cero en todo anillo de matrices con $n\geq 2$, ya que si $n=1$, tendríamos que $M_1(R)\cong R$ o incluso podemos considerar que $M_1(R)=R$, por lo tanto, si no tuviera divisores de cero tampoco tendría divisores de cero el conjunto de esas matrices cuadradas de orden 1 que realmente serían los elementos del anillo.

Hablando de las unidades, podemos decir, sin adentrarnos en ello, que una vez tenemos un anillo de matrices cuadradas cuyas entradas son de un anillo unitario,

una matriz $(a_{ij})_n \in \mathscr{U}(M_n(R))$ si, y solamente si, podemos encontrar una matriz $(b_{ij})_{n\times n} \in M_n(R)$ de forma que $(a_{ij})(b_{ij}) = (b_{ij})(a_{ij}) = (\delta_{ij}) = Id$
Concluimos entonces:

- Éstas matrices cuadradas de orden n con las operaciones que vimos con entradas en R; $\langle M_n(R), +, \cdot, 0\rangle$ forman un anillo.
- Si acaso el anillo de partida fuera unitario, también sería el anillo de las matrices un anillo unitario.
- Todos éstos anillos de matrices ya sean unitarios o no, tienen divisores de cero siempre que $n \geq 2$.

Ejemplo 3.3. Si $\mathbb{F}$ es un cuerpo y $n \in \mathbb{P} = \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}$; decimos que el anillo de matrices $M_n(\mathbb{F}) \equiv \mathbb{F}^{n\times n}$ son las matrices $n \times n$ con entrada en $\mathbb{F}$ junto con las operaciones suma y producto.
Sea $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}]$, entonces, $C = AB$ si, y solamente si $c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$.
Está claro que $M_1(\mathbb{F}) = \mathbb{F}$. Para $n \geq 2$, el anillo $M_n(\mathbb{F})$ no es conmutativo. Hablando de forma más general, las mismas definiciones de suma y producto matriciales nos permiten definir $M_n(R)$ el anillo de matrices $n \times n$ con entradas en un anillo R cualquiera.

FIN DE AÑADIR

Si R es un anillo, para cada entero positivo n consideramos el R–módulo a izquierda $R^n = \oplus_{i=1}^{n} R$. Éste es un R–módulo a izquierda libre y sus endomorfismos, $\mathrm{End}_R(R^n)$, forman un anillo para las siguientes operaciones:

$$(f + g)(x) = f(x) + g(x),$$
$$(f\, g)(x) = f(g(x)),$$

para $f, g \in \mathrm{End}_R(R^n)$ y $x \in R^n$, siendo id el elemento uno.
Fijada una base $\{e_1, \ldots, e_n\}$ de R^n, para cada $f \in \mathrm{End}_R(R^n)$ y cada índice j se tiene que $f(e_j)$ se expresa como una combinación lineal, con coeficientes en R, de los elementos e_i's, por ejemplo, tendremos $f(e_j) = \sum_{i=1}^{n} a_{ij} e_i$. Podemos entonces representar f mediante la matriz

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \cdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

De forma que si representamos el elemento $x = \sum_{i=1}^{n} a_i e_i$ como la columna $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}^t$, la imagen, $f(x)$ de x, se obtiene multiplicando la matriz anterior por esta columna:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \cdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Existe una biyección entre endomorfismos $f \in \mathrm{End}_R(R^n)$ y matrices cuadradas $n \times n$, $M \in M_n(R)$, con coeficientes en R. En consecuencia, ya que $\mathrm{End}_R(R^n)$ es un anillo, existe una estructura de anillo en $M_n(R)$.

La estructura de $M_n(R)$ está íntimamente ligada a la estructura de R; por ejemplo, los ideales de $M_n(R)$ son todos de la forma $M_n(\mathfrak{A})$ para ideales $\mathfrak{A} \subseteq R$, por lo que si R es un cuerpo ó un anillo de división, los únicos ideales de $M_n(R)$ son el cero y el total (es un anillo simple). Sin embargo tiene varios ideales a izquierda y a derecha.

AÑADIR

Ejemplo 3.4. En el anillo matricial $R = M_n(\mathbb{F})$; los ideales a izquierda se encuentran clasificados a través de una serie de columnas. De hecho, si $J = \{j_1, \ldots, j_m\} \subseteq \{1, \ldots, n\}$. Sea $M_{(J)}$ todas las matrices en R en las que las entradas no nulas ocurren en las columnas indiciadas por J. Dicho de otro modo, $c = [c_{ij}] \in M_{(J)}$ si, y solamente si, $c_{ij} = 0$ para $j \notin J$ que es un subgrupo aditivo de R. Si $A \in R$, la entrada (i, j) de AC es $\sum_{k=1}^{n} a_{ik}c_{kj}$, también es cero si $j \notin J$. Por tanto, $M_{(J)}$ es un ideal a izquierda en R.

Cualquier ideal a izquierda de $R = M_n(\mathbb{F})$ es de la forma $M_{(J)}$ para algún $J \subseteq \{1, \ldots, n\}$. Como la traspuesta de AC es $(AC)^t = C^t A^t$, vemos aquí que cualquier ideal a derecha de $M_n(\mathbb{F})$ es de la forma $M_{(J)}$; todas las matrices cuyas entradas no nulas ocurren en las filas indiciadas por J.

Observamos que el ideal a izquierda $M_{(J)}$ no es un ideal a derecha salvo cuando se trata de $J = \emptyset$ y $J = \{1, \ldots, n\}$. Por lo que los únicos ideales bilaterales de $R = M_n(\mathbb{F})$ son los ideales triviales $\{0\}$ y R, esto es, el anillo de matrices $M_n(\mathbb{F})$ es simple.

ESTO DE ARRIBA LO PONDRÍA POR EL ÚLTIMO PÁRRAFO

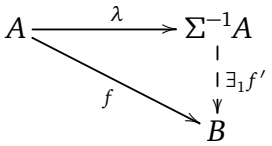
Ejemplo 3.5. Sea $\mathbb{F}^n$ el espacio vectorial de vectores con n entradas en un cuerpo $\mathbb{F}$. El anillo de matrices $R = M_n(\mathbb{F})$ actúa sobre $\mathbb{F}^n$ por $(A, x) \longmapsto Ax$ al multiplicar una matriz en R por un vector columna. Así, $\mathbb{F}^n$ es un R–módulo a izquierda. Sea $\mathbb{F}^n := \{x^t;\ x \in \mathbb{F}^n\}$ el espacio vectorial de vectores fila con n entradas en $\mathbb{F}$. El mismo anillo de matrices $R = M_n(\mathbb{F})$ actúa a la derecha sobre vectores fila por $(x^t, A) \longmapsto x^t A$, de manera que $\mathbb{F}_n$ es un R–módulo a derecha.

FIN DE AÑADIR. ¿ejemplo 3.5 lo pongo?

Por ejemplo, en el caso de $n = 2$, el anillo $M_2(K) = \begin{pmatrix} K & K \\ K & K \end{pmatrix}$ tiene a $\begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix}$ y a $\begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix}$ como ideales a izquierda, y a $\begin{pmatrix} K & K \\ 0 & 0 \end{pmatrix}$ y a $\begin{pmatrix} 0 & 0 \\ K & K \end{pmatrix}$ como ideales a derecha. Observa que todos ellos son ideales principales a izquierda ó a derecha según el caso.

Anillos de fracciones

Si A es un anillo conmutativo, para cada subconjunto $\Sigma \subseteq A$ que es **multiplicativamente cerrado**, esto es, $1 \in \Sigma$ y $ab \in \Sigma$ para cada par de elementos $a, b \in \Sigma$, existe un anillo $\Sigma^{-1}A$ y un homomorfismo de anillos $\lambda : A \longrightarrow \Sigma^{-1}A$ que verifica la siguiente propiedad universal. Para cada anillo conmutativo B y cada homomorfismo de anillos $f : A \longrightarrow B$ verificando que $f(s) \in B$ es invertible para todo $s \in \Sigma$, existe un único homomorfismo de anillos $f' : \Sigma^{-1}A \longrightarrow B$ tal que $f = f'\lambda$.



La construcción de $\Sigma^{-1}A$ se realiza como sigue:

(1) Se considera el producto cartesiano $\Sigma \times A$.
(2) En $\Sigma \times A$ se define una relación de equivalencia: $(s_1, a_1) \sim (s_2, a_2)$ si existe $s \in \Sigma$ tal que $s(s_1a_2 - s_2a_1) = 0$
(3) En el conjunto cociente, $\Sigma^{-1}A = (\Sigma \times A)/\sim$, la clase del par (s, a) se representa por $s^{-1}a$ ó por $\dfrac{a}{s}$. Se definen, en el conjunto cociente, dos operaciones:
$$(s_1^{-1}a_1) + (s_2^{-1}a_2) = (s_1s_2)^{-1}(s_2a_1 + s_1a_2),$$
$$(s_1^{-1}a_1) \times (s_2^{-1}a_2) = (s_1s_2)^{-1}(a_1a_2).$$
(4) Entonces $\Sigma^{-1}A$ es un anillo con elemento uno igual a $1^{-1}1$.
(5) La aplicación $\lambda : A \longrightarrow \Sigma^{-1}A$, definida $\lambda(a) = 1^{-1}a$ es un homomorfismo de anillos.

El anillo $\Sigma^{-1}A$ se llama el **anillo de fracciones** de A con respecto a Σ.

Ejemplo 3.6. Esta es la construcción que se usa para construir $\mathbb{Q}$ a partir del anillo de los números enteros; en este caso $\Sigma = \mathbb{Z} \setminus \{0\}$

No siempre el homomorfismo λ es inyectivo. Consideremos el siguiente ejemplo.

Ejemplo 3.7. Se considera el anillo $A = \mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$, y el subconjunto multiplicativo $\Sigma = \{1, 3\} \subseteq \mathbb{Z}_6$. En este caso tenemos que $\Sigma^{-1}A$ tiene los siguientes elementos:
$$\frac{0}{1} = \frac{2}{1} = \frac{4}{1} = \frac{0}{3} = \frac{2}{3} = \frac{4}{3}, \qquad \frac{1}{1} = \frac{3}{1} = \frac{5}{1} = \frac{1}{3} = \frac{3}{3} = \frac{5}{3}.$$
Por tanto $\mathrm{Ker}(\lambda) = \{0, 2, 4\}$. En este caso, además, $\Sigma^{-1}A$ es un cuerpo isomorfo a $\mathbb{Z}_2$.

Observación. 3.8. (1) Cuando Σ está formado por elementos invertibles se tiene $\Sigma^{-1}A \cong A$.
(2) Los anillos de fracciones son de interés cuando se estudian ideales primos, ya que si $\mathfrak{p} \subseteq A$ es un ideal primo, entonces $A \setminus \mathfrak{p}$ es un subconjunto multiplicativamente cerrado.

Capítulo 3

DIVISIBILIDAD EN DOMINIOS

En este capítulo vamos a considerar dominios de integridad, y utilizaremos frecuentemente la letra D para referirnos a ellos; para acortar a veces los nombraremos sólo como dominios.

1. Divisibilidad

Sea D un dominio de integridad, por lo tanto es un anillo conmutativo sin divisores de cero no nulos, para cada par de elementos $a, b \in D$ el elemento a **divide** al elemento b si existe un elemento $c \in D$ tal que $b = ac$, y lo representamos por $a|b$. También se dice que b es un **múltiplo** de a.

Observación. 1.1. (1) Siempre $1|a$ y $a|0$ para cada elemento $a \in D$.

(2) Por el contrario, si $a|1$, entonces a es invertible, y si $0|a$, entonces $a = 0$, para cada $a \in D$.

(3) La relación de división verifica las propiedades reflexiva y transitiva, pero no necesariamente la antisimétrica.

(4) Dos elementos $a, b \in D$ se llaman **asociados** cuando $a|b$ y $b|a$; o equivalentemente, cuando existe un elemento invertible $u \in A^\times$ tal que $b = ua$.

Proposición 1.2. *Si D es un dominio la relación "asociado", a la que representamos por $\sim$, es una relación de equivalencia, y en el conjunto cociente $D/\sim$ podemos definir la relación $[a]|[b]$ si $a|b$. Se verifica que ésta es una relación de orden en $D/\sim$.*

Dados dos elementos $a, b \in D$ de un dominio D, si $[d]$ es un ínfimo de $\{[a],[b]\}$ en $D/\sim$, resulta que se tienen las siguientes propiedades:

(1) $d|a$ y $d|b$,

(2) para cada $c \in D$ tal que $c|a$ y $c|b$ se tiene que $c|d$.

Dados dos elementos $a, b \in D$ un **máximo común divisor** de a y b es un elemento $d \in D$ que verifica las condiciones anteriores, o equivalentemente, $[d]$ es un ínfimo de $\{[a],[b]\}$ en $D/\sim$. Como consecuencia, el máximo común divisor está determinado salvo asociados.

Observa que no necesariamente tiene que existir el máximo común divisor de un par de elementos. El máximo común divisor de dos elementos a y b se representa por $\text{mcd}\{a, b\}$ ó, abreviadamente, por (a, b).

De forma similar se define el **mínimo común múltiplo** de un par de elementos $a, b \in D$, el cual se presenta por $[a, b]$ ó por $\text{mcm}\{a, b\}$.

Veamos algunos tipos de elementos de un dominio en relación a la división.

Sea D un dominio de integridad, y sea $x \in D$ un elemento distinto de cero y no invertible.

(1) x es **irreducible** en D si en cualquier factorización $x = ab$ se tiene que a es invertible ó b es invertible.
(2) x es **reducible** en D si no es irreducible.
(3) x es **primo** en D si cuando $x|ab$, se tiene $x|a$ ó $x|b$; esto es, cuando el ideal $\langle x\rangle$ es un ideal primo,

Mientras que todo elemento primo es irreducible, el recíproco no siempre es cierto.

Ejemplo 1.3. Considera el anillo $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. En este anillo tenemos las siguienes factorizaciones:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \times 3.$$

Por otro lado, la norma, definida $N(a + b\sqrt{-5}) = a^2 + 5b^2$ es multiplicativa, por lo que se verifica $N(xy) = N(x)N(y)$, para cada par de elementos $x, y \in \mathbb{Z}[\sqrt{-5}]$; entonces $2, 3 \in \mathbb{Z}[\sqrt{-5}]$ son elementos irreducibles, pero no son primos, ya que $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, pero no divide a ninguno de estos factores. Tenemos pues un ejemplo de un elemento irreducible que no es primo.

Este mismo anillo proporciona un ejemplo en el que no todo par de elementos tiene un máximo común divisor. Consideramos $x = 2(1 + \sqrt{-5})$ e $y = 6$. Es claro que 2 divide a x y a y, y lo mismo le ocurre a $1 + \sqrt{-5}$; por lo que el máximo común divisor d de x e y, si existe, debe ser un múltiplo de 2 y de $1 + \sqrt{-5}$, pero esto es imposible, ya que entonces $N(d) = 12$ que no se puede escribir en la forma $a^2 + 5b^2$ para enteros a y b.

Tenemos el siguiente resultado que nos caracteriza a los elementos irreducibles en términos de ideales principales.

Proposición 1.4. *Sea $a \in D$ un elemento no nulo y no invertible, son equivalentes:*

(a) $a \in D$ es irreducible.
(b) El ideal $\langle a \rangle$ es maximal entre los ideales principales.

PROOF (a) $\Rightarrow$ (b). Si existe un ideal principal $\langle a \rangle \subseteq \langle b \rangle \subsetneq D$, existe $c \in D$ tal que $a = bc$, por tanto c es un elemento invertible, y se tiene $\langle a \rangle = \langle b \rangle$.
(b) $\Rightarrow$ (a). Si $a = bc$ y b no es invertible, tenemos $\langle a \rangle \subseteq \langle b \rangle \subsetneq D$, y por tanto $\langle a \rangle = \langle b \rangle$. Entonces existe $d \in D$ tal que $b = ad$, y se tiene $a = adc$; como $a \neq 0$, y D es un dominio, se tiene $1 = dc$, y c es un elemento invertible. □

2. Dominios Euclídeos

A la hora de trabajar en un dominio de integridad uno de los problemas con los que nos encontramos es cómo calcular, por ejemplo, el máximo común divisor de dos elementos o cómo probar que un determinado elemento es primo o irreducible. Vamos a ver un tipo de dominios en los que tenemos algoritmos que nos ayudan en estos cálculos.

Un dominio de integridad D es un **dominio euclídeo** si existe una aplicación $\delta : D \longrightarrow \omega + 1$ que verifica:

(1) $\delta(0) = \omega$.
(2) $\delta(ab) \geq \delta(a)$, para todo par $a, b \in D$
(3) Para cada par de elementos $a, b \in D$ existen elementos $c, r \in D$ tales que $a = bc + r$, siendo $r = 0$ ó $\delta(r) < \delta(b)$.

En estas circunstancias decimos que $a = bc + r$ es la **división** de a por b, llamamos a c el **cociente** de la división, a r es **resto**, y a δ la **función euclídea**[1].

Ejemplo 2.1. (1) El anillo $\mathbb{Z}$ de los números enteros es un dominio euclídeo con función euclídea $|\ | : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$, y $|\ |(0) = \omega$.
(2) En la misma situación, para cada cuerpo K al anillo de polinomios $K[X]$ es un dominio euclídeo.
(3) Cada cuerpo K es un anillo euclídeo con función euclídea $\delta : K \longrightarrow \omega+1$ definida $\delta(0) = \omega$ y $\delta(a) = 0$ si $0 \neq a \in K$.

Como consecuencia de la definición tenemos:

Lema 2.2. *Sea D un dominio euclídeo con función euclídea δ, para cada elemento $a \in D$, se verifica:*

(1) $\delta(1) \leq \delta(a)$,
(2) $\delta(1) = \delta(a)$ si, y sólo si, a es invertible.

[1] En el siguiente capítulo veremos que podemos prescindir de la condición (2) el trabajar en dominios euclídeos.

DEMOSTRACIÓN. (1). Es consecuencia directa de la definición, ya que $a = 1a$.

(2). Dividiendo 1 por a, se tiene $1 = ac + r$. Si $r \neq 0$, entonces $\delta(r) < \delta(1)$, lo que es imposible por (1). Como consecuencia, $1 = ca$, y a es invertible. Recíprocamente, si a es invertible existe $c \in D$ tal que $1 = ac$, por tanto $\delta(a) \leq \delta(ac) = \delta(1)$, y se tiene $\delta(a) = \delta(1)$.

Podemos afinar un poco más respecto a la aritmética en un dominio euclídeo.

Lema 2.3. *Sea D un dominio euclídeo, y $a, b \in D$ elementos, se verifica:*
(1) Si $a|b$ y $\delta(a) = \delta(b)$, entonces a y b son asociados.
(2) Si $a|b$ y $b \nmid a$, entonces $\delta(a) < \delta(b)$.

DEMOSTRACIÓN. (1). Basta ver que $b|a$; dividiendo a por b se tiene $a = bc + r$. Si $r \neq 0$ entonces $\delta(r) < \delta(b)$. Por otro lado existe $d \in D$ tal que $b = ad$, y se tiene $r = a - bc = a - adc = a(1 - dc)$, por tanto $\delta(a) \leq \delta(r) < \delta(b) = \delta(a)$, lo que es una contradicción. Por tanto $a = bc$ y tenemos el resultado.

(2). Como $a|b$, se tiene $\delta(a) \leq \delta(b)$. Si se tiene la igualdad, entonces $b|a$, y como ésto no es cierto, necesariamente $\delta(a) < \delta(b)$.

Como anunciamos al inicio de esta sección, el trabajar en dominio euclídeos tiene la ventaja de que podemos hacer cálculos, esto es, existen algoritmos para trabajar con elementos; uno de estos algoritmos es el **algoritmo de Euclides** que permite calcular el máximo común divisor de un par de elementos de D.

Si D es un dominio euclídeo, dados dos elementos $a, b \in D$, supongamos que $\delta(a) \geq \delta(b)$; al hacer la división de a por b se obtiene $a = bc + r$. Es claro que $\mathrm{mcd}\{a, b\} = \mathrm{mcd}\{b, r\}$, y hemos disminuido el valor del máximo de los deltas. Como las cadenas estrictamente descendentes en un conjunto bien ordenado son finitas, reiterando el proceso llegamos a un par de elementos uno de los cuales es cero, y por tanto obtenemos el máximo común divisor de a y b. Explícitamente tenemos:

r_{-1}	$= a,$	
r_0	$= b,$	
r_1	$=$ resto de la división de $r_{-1} = a$ por $r_0 = b,$	$\delta(r_1) < \delta(r_0)$
r_2	$=$ resto de la división de $r_0 = b$ por $r_1,$	$\delta(r_2) < \delta(r_1)$
r_3	$=$ resto de la división de $r_1 = a$ por $r_2,$	$\delta(r_3) < \delta(r_2)$
$\cdots$		$\cdots$
r_t	$=$ resto de la división de $r_{t-2} = a$ por $r_{t-1},$	$\delta(r_t) < \delta(r_{t-1})$
$0 = r_{t+1}$	$=$ resto de la división de $r_{t-1} = a$ por $r_t,$	

Por otro lado, se tiene

$$\mathrm{mcd}\{a, b\} = \mathrm{mcd}\{b, r_1\} = \mathrm{mcd}\{r_1, r_2\} = \cdots \mathrm{mcd}\{r_{t_1}, r_t\} = \mathrm{mcd}\{r_t, 0\} = r_t.$$

Como consecuencia, se tiene que el máximo común divisor d de dos elementos $a, b \in D$ se expresa como una combinación lineal de a y de b; esto es, existen elementos $\alpha, \beta \in D$ tales que $d = \alpha a + \beta b$ (**identidad de Bezout**).

La siguiente conclusión es más interesante desde el punto de vista de los ideales:

Proposición 2.4. *Sea D un dominio euclídeo, para cada par de elementos $a, b \in D$ existe el máximo común divisor de a y b; además, si $d = \text{mcd}\{a, b\}$, entonces $\langle a, b\rangle = \langle d\rangle$; esto es, el ideal generado por a y b es el ideal principal generado por el máximo común divisor*

Esta propiedad sobre ideales es cierta no solo para ideales generadores por dos elementos, sino para ideales arbitrarios de un dominio euclídeo.

Un dominio de integridad D es un **dominio de ideales principales** si todo ideal es un ideal principal.

Proposición 2.5. *Todo dominio euclídeo es un dominio de ideales principales.*

DEMOSTRACIÓN. Dado un ideal no nulo $\mathfrak{a} \subseteq D$, consideramos el conjunto $\Delta = \{\delta(a) |\ a \in \mathfrak{a}\} \subseteq \omega + 1$. Como $\omega + 1$ es un conjunto bien ordenado, existe un primer elemento de Δ, sea α. Si $a \in \mathfrak{a}$ verifica $\delta(a) = \alpha$, es inmediato probar que $\mathfrak{a}$ está generado por a; esto es, $\mathfrak{a} = \langle a\rangle$, y por tanto es un ideal principal.

Podemos ahora probar que en un dominio euclídeo todo elemento irreducible es primo; basta probarlo para dominios de ideales principales.

Proposición 2.6. *Si D es un dominio de ideales principales, todo elemento irreducible es primo.*

DEMOSTRACIÓN. Primero señalamos que un elemento no nulo y no invertible $p \in D$ es primo si, y sólo si, el ideal principal $\langle p\rangle$ es un ideal primo. Por la Proposición (1.4.) se tiene que p es irreducible si, y sólo si, el ideal principal $\langle p\rangle$ es maximal entre los ideales principales. Como todos los ideales de D son principales, se tiene the si p es irreducible, entonces $\langle p\rangle \subseteq D$ es maximal, y por tanto primo, luego p es un elemento primo.

Otra consecuencia de este hecho tiene relación con los ideales primos y maximales.

Corolario 2.7. *Si D es un dominio de ideales principales, todo ideal primo no nulo es maximal.*

DEMOSTRACIÓN. Si $\mathfrak{p}$ es un ideal primo no nulo, como está generado por un elemento primo, y éste es irreducible, se tiene que p es un ideal maximal.

La teoría de dominios euclídeos y de ideales principales tiene aplicaciones a la factorización de elementos; veamos cómo son estas aplicaciones. Primero necesitamos una definición. Un dominio de integridad es un **dominio de factorización única** si

(1) cada elemento no nulo y no invertible a existe una factorización en elementos irreducibles, sea $a = q_1 \cdots q_t$.

(2) si un elemento no nulo y no invertible a tiene dos factorizaciones en elementos irreducibles, sea $a = q_1 \cdots q_t = r_1 \cdots r_s$, entonces $t = s$ y existe una permutación $\sigma \in S_t$ tal que para cada índice $i \in \{1, \ldots, t\}$ los elementos q_i y $r_{\sigma(i)}$ son asociados.

Para este tipo de dominios también todo elemento irreducible es primo.

Lema 2.8. *Si D es un dominio de factorización única, todo elemento irreducible es primo.*

Podemos reformular esta definición de dominio de factorización única utilizando factorizaciones en elementos primos.

Proposición 2.9. *Sea D un dominio de integridad, son equivalentes:*

(a) D es un dominio de factorización única.
(b) Cada elemento no nulo y no invertible tiene una factorización en elementos primos.

DEMOSTRACIÓN. Dado un elemento no nulo y no invertible y una factorización en irreducibles $a = q_1 \ldots q_t$, como existe una factorización en primos, supongamos que ésta es $a = p_1 \ldots p_s$. Como p_1 divide a $a = q_1 \cdots q_t$, existe un factor q tal que $p_1 | q$, supongamos que $q = q_1$, entonces $q_1 = p_1 p_1'$; como q_1 es irreducible, se tiene p_1' es invertible. Simplificando por p_1 en la expresión $p_1 \cdots p_s = p_1 p_1' q_2 \cdots q_s$ se obtiene $p_2 \cdots p_s = p_1' q_2 \cdots q_t$. Basta hacer inducción sobre la longitud de las factorizaciones en primos para tener el resultado.

El resultado fundamental en esta teoría es el siguiente:

Teorema 2.10. *Todo dominio de ideales principales es un dominio de factorización única.*

DEMOSTRACIÓN. Basta ver que cada elemento no nulo y no invertible tiene una factorización en primos y aplicar la Proposición (2.9.). Como en un dominio de ideales principales todo elemento irreducible es primo, basta ver que todo elemento no nulo y no invertible tiene una factorización en irreducibles. Dado $a \in D$ no nulo y no invertible, si a es irreducible ya hemos terminado; en caso contrario, existe una factorización $a = a_1 a_1'$ con a_1, a_1' no invertibles. Si a_1 es irreducible hemos encontrado un factor de a irreducible, y en caso contrario tenemos una factorización $a_1 = a_2 a_2'$ con a_2, a_2' no invertibles. Si en este proceso no encontramos a_i irreducible, construimos una sucesión $a_1, a_2, \ldots$ de elementos no invertibles de forma que $a_{i+1} | a_i$ y $a_i \nmid a_{i+1}$ para $i \geq 1$. El ideal $\langle a_1, a_2 \ldots \rangle$ es principal, por tanto existe $b \in D$ tal que $\langle a_1, a_2 \ldots \rangle = \langle b \rangle$, y por tanto un índice tal que $\langle a_1, a_2 \ldots \rangle = \langle a_i \rangle$, lo que es una contradicción. En conclusión, el elemento a tiene un factor que es un elemento irreducible.

Comenzamos de nuevo el proceso; si a es irreducible hemos terminado, en caso contrario existe un irreducible q_1 tal que $a = q_1 a_1$; si a_1 es irreducible hemos terminado,

en caso contrario existe un irreducible q_2 tal que $a_1 = q_2 a_2$, y se tiene $a = q_1 q_2 a_2$; si a_2 es irreducible hemos terminado; en caso contrario construimos q_3 y a_3, etc. Si no encontramos un a_i irreducible hemos construido una sucesión $a_1, a_2 \ldots$ de elementos de D tales que $a_{i+1} | a_i$ y $a_i \nmid a_{i+1}$ para $i \geq 1$. Al igual que antes llegamos a una contradicción, y por tanto necesariamente uno de los a_i es irreducible y tenemos una factorización en irreducibles de a.

Ejemplo 2.11. Es fácil encontrar dominios de factorización única que no son dominios de ideales; por ejemplo, el lema de Gauss nos dice que si A es un dominio de factorización única, entonces el anillo de polinomios $A[X]$ es un dominio de factorización única. Por tanto $\mathbb{Z}[X]$ es un DFU, pero $\mathbb{Z}[X]$ no es in DIP, ya que el ideal $(2, X) \subseteq \mathbb{Z}[X]$ no es principal.

Un poco más difícil es encontrar un DIP que no sea un DE. Un ejemplo sería el siguiente:

Ejemplo 2.12. El anillo $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es un DIP y no es un DE.

Capítulo 4

ANILLOS EUCLÍDEOS

El objetivo de ese capítulo es extender la teoría de dominios euclídeos a anillos que no necesariamente son un dominio de integridad e incluso no son conmutativos; en este proceso, continuando con el desarrollo hecho para dominios, veremos que podemos cambiar el conjunto bien ordenado $\mathbb{N}$ por un ordinal, que necesariamente no tiene que ser finito o numerable.

1. Anillos Euclídeos

Sea R un anillo y $\mathcal{O}$ la clase de todos los ordinales. Una **norma euclídea a derecha** en R es una aplicación $\delta : R \longrightarrow \mathcal{O}$ que satisface:

(I) $\delta(0) = \text{ínf}\{\sigma \in \mathcal{O} |\ \delta(x) < \sigma$ para todo $x \in R \setminus \{0\}\}$.

(II) Para cada $x, y \in R$, existe $q, r \in R$ de manera que $x = yq + r$ y $r = 0$ ó $r \neq 0$ y $\delta(r) < \delta(y)$.

Observación. 1.1. (1) Imponemos la condición adicional $\delta(0) = \text{ínf}\{\sigma \in \mathcal{O} |\ \delta(x) < \sigma$ para todo $x \in R \setminus \{0\}\}$ para evitar la tradicional restricción de $b \neq 0$ en el punto (II) anterior.

(2) Con q y r nos referimos al **cociente** y **resto**, respectivamente, de la división de x por y. Los llamamos así pero no están determinados de una única forma.

(3) Un **anillo euclídeo a derecha**, es un anillo R junto con una norma euclídea a derecha en R.

De la misma manera podemos definir normas euclídeas a izquierda y anillos euclídeos a izquierda. A partir de ahora, utilizaremos norma euclídea para referirnos a norma euclídea a derecha y anillo euclídeo para anillo euclídeo a derecha, y la alusión de izquierda la usaremos para normas y anillos euclídeos a izquierda.

Observación. 1.2. Si R es un anillo euclídeo, entonces es un anillo de ideales a derecha principales, y no es necesariamente un anillo de ideales a izquierda principales.

Ejemplo 1.3. Sea R el anillo $\begin{pmatrix} \mathbb{Z} & 0 \\ \mathbb{Q} & \mathbb{Q} \end{pmatrix}$ junto con la norma euclídea $\delta : R \longrightarrow \{0,1,2\}$ definida

$$\delta(x) = \begin{cases} 0, \text{ si } x \in R^{\times} \\ 1, \text{ si } x \neq 0 \text{ y } x \notin R^{\times} \\ 2, \text{ si } x = 0. \end{cases}$$

Entonces R es un anillo euclídeo a derecha, es un anillo de ideales a derecha principales, y no es un anillo de ideales a izquierda principales. Por ejemplo; si $\mathfrak{a} = \begin{pmatrix} 0 & 0 \\ \mathbb{Q} & \mathbb{Q} \end{pmatrix}$ no es un principal a izquierda principal, puesto que se tiene $\mathfrak{a} = \begin{pmatrix} 0 & 0 \\ \mathbb{Q} & \mathbb{Q} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \mathbb{Q} & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{pmatrix}$.

Como cada norma euclídea está definida por $\mathcal{O}$, podemos comparar dos de ellas. Esto es, si $\delta_1, \delta_2 : R \longrightarrow \mathcal{O}$ son normas euclídeas y definimos $\delta_1 \leq \delta_2$ cuando $\delta_1(x) \leq \delta_2(x)$ para cada $x \in R$, para cualquier familia $\{\delta_i | \ i \in I\}$ de normas euclídeas en R, tenemos que $\wedge_i \delta_i$ es una normal euclídea, (lo veremos más adelante).

Lema 1.4. *Sea R un anillo euclídeo, existe una norma euclídea δ_0 de manera que $\delta_0 \leq \delta$ para cada norma euclídea δ. Por tanto, δ_0 es la norma euclídea mínima en R.*

DEMOSTRACIÓN.Construcción de Motzkin.

Vamos a considerar los siguientes subconjuntos:

(1) $T_{-1} := \{0\}$,
(2) $T_\sigma = \{a \in R$ para cada $b \in R$ existe $q \in R, r \in T_{\tau<\sigma}$ de manera que $b = xq + r\} \cup (\bigcup_{\tau<\sigma} T_\tau)$ para cualquier $\sigma \in \mathcal{O}$.

Por lo tanto, el conjunto $\{T_\sigma\}_\sigma$ incrementa y como R es euclídeo, existe $\sigma \in \mathcal{O}$ de manera que $R = T_\sigma$. De hecho, R es euclídeo si, y solo si, existe un $\sigma \in \mathcal{O}$ tal que $R \in T_\sigma$.

Definimos pues:

$$\delta_0(a) = \text{ínf}\{\sigma | \ a \in T_\sigma\} \text{ si } a \neq 0.$$
$$\delta_0(0) = \text{ínf}\{\sigma | \ \delta(a) < \sigma \text{ para todo } 0 \neq a \in R\}.$$

Nos damos cuenta que si $\text{ínf}\{\sigma | \ T_{\sigma=R}\}$ es un ordinal límite, entonces $\delta_0(0) = \text{ínf}\{\sigma | \ T_\sigma = R\}$; al contrario, $\delta_0(0) = \text{ínf}\{\sigma | \ T_\sigma = R\} + 1$

Lema 1.5. *Sea R un anillo euclídeo, entonces $T_0 \backslash T_{-1}$ es el conjunto de todos los elementos invertibles por la derecha de R.*

DEMOSTRACIÓN. Está claro que si $a \in T_0$, para cada $b \in R$, existe $q \in R$ de manera que $b = aq$; particularmente, existe q tal que $1 = aq$. De lo contrario, si $a \in R$ es invertible por la derecha, con inverso a', para cualquier $b \in R$ tenemos que $b = a(a'b)$.

Existe un método alternativo para construir el mínimo de las normas euclídeas en un anillo euclídeo.

Proposición 1.6. *Sea $\{\delta_i | \ i \in I\}$ una familia no vacía de normas euclídeas en un anillo R, entonces, $\wedge_i \delta_i$ es una norma euclídea.*

DEMOSTRACIÓN. Para cada $x \in R$, definimos $\wedge_i \delta_i = \text{ínf}\{\delta_i | \ i \in I\}$ y demostramos que es una norma euclídea. Dados $x, y \in R$, hay un índice $i \in I$ tal que $\wedge_i \delta_i(y) = \delta_i(y)$; por lo tanto, existen $q, r \in R$ de manera que $x = yq + r$ siendo $r = 0$ ó $\delta_i(r) < \delta_i(y)$. Así tenemos que $\wedge_i \delta_i(r) \leq \delta_i(r) < \delta_i(y) = \wedge_i \delta_i(y)$.
Si δ es una norma euclídea en R, definimos el **rango** de δ como $\delta(0)$ y definimos el **rango absoluto** (o **tipo de orden euclídeo**) de R o simplemente **rango**e R como el rango de la norma euclídea mínima.

Ejemplo 1.7. Si consideramos el anillo $\mathbb{Z}$ de los números enteros; el valor absoluto, define una norma euclídea $\delta_{||}$ como sigue:

$$\delta_{||}(x) = \begin{cases} |a|, \text{ si } a \neq 0, \\ \omega, \text{ si } a = 0. \end{cases}$$

En este caso, el rango de $\delta_{||}$ es ω; que es el primer ordinal infinito.

Lema 1.8. *Si R es un anillo euclídeo y δ es una norma euclídea de R, son equivalentes:*
(a) R es trivial.
(b) δ es constante.

En este caso, el rango de R es 0.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b) Es obvio.
(b) $\Rightarrow$ (a). Si δ es constante, y dividimos 1 por 0, obtenemos que $1 = 0q + r$. Para $\delta(r) \leq \delta(0)$, es necesario que $r = 0$. Por eso, $1 = 0$ y R es el anillo trivial.
Recordemos que los anillos que tratamos son no triviales, por lo que en lo que sigue y todas las normas euclídeas serán no constantes a menos que digamos lo contrario.

Lema 1.9. *Sea R un anillo, y δ una norma euclídea no constante en R. Para cualquier $a \in R$, si $\delta(a)$ es mínimo en $\delta(R)$, entonces a es invertible por la derecha en R.*

DEMOSTRACIÓN. Si $\delta(a)$ mínimo en $\delta(R)$, entonces existen $q, r \in R$ de manera que $1 = aq + r$. Si $r \neq 0$ entonces $\delta(r) < \delta(a)$ y esto es imposible, por lo tanto, $r = 0$ y a es invertible por la derecha.

Ejemplo 1.10. Sea D un anillo de división; definimos la norma euclídea como:

$$\delta(a) = \begin{cases} 0, \text{ si } a \neq 0, \\ 1, \text{ si } a = 0, \end{cases}$$

por otro lado, si D es un anillo y lo anterior es una norma euclídea en D, entonces D es un anillo de división. En efecto, por el Lema (1.9.), cada elemento distinto de 0 es invertible por la derecha. En este caso, el rango de D es 1. Como consecuencia tenemos que D es un anillo de división si, y solo si, el rango de D es 1.

Ejemplo 1.11. (Norma euclídea mínima en $\mathbb{Z}$) Si seguimos la construcción de Motzkin de la norma euclídea mínima, tenemos:
(1) $T_{-1} = \{0\}$,
(2) $T_0 = \{-1, 0, 1\}$
(3) $T_1 = T_0 \cup \{a \in \mathbb{Z} |$ para todo $b \in \mathbb{Z}$, existe q de manera que $b = aq \pm 1\} = \{-3, -2, -1, 0, 1, 2, 3\}$
(4) ...
(5) $T_n = \{a \in \mathbb{Z} | \, |a| < 2^{n+1}\}$

En particular, $T_n / T_{n-1} = \{a \in \mathbb{Z} | \, 2^n \leq |a| < 2^{n+1}\}$. Por lo tanto, $\delta_0(a) = [log_2(a)]$ cuando $a \neq 0$. De lo contrario; $\delta_0(0) = \omega$. En consecuencia de ésto, como ya dijimos anteriormente, se tiene rango$(\mathbb{Z}) = \omega$.

Ejemplo 1.12. (Norma euclídea mínima en $K[X]$) Si K es un anillo de división y X una indeterminada sobre K para cada polinomio $P \in K[X]$. Consideramos el grado gr(P) de P. La construcción de Motzkin es la siguiente:
(1) $T_{-1} = \{0\}$
(2) $T_0 = K$
(3) $T_1 = \{x + yX \in K[X] | \, x, y \in K\}$
(4) ...
(5) $T_n = \{$polinomios de grado $n\}$.

En consecuencia, tenemos $\delta_0(P) = \text{gr}(P)$ para cada $0 \neq P \in K[X]$, y $\delta_0(0) = \omega$.
Por lo tanto, rango$(K[X]) = \omega$.

Observación. 1.13. En los Ejemplos (1.11.) y (1.12.) anteriores, observamos que los rangos son igual a ω, es decir, al primer ordinal infinito.

Módulos

Sea M un R-modulo a la derecha. Una **norma euclídea** en M es una aplicación $\delta : M \longrightarrow \mathcal{O}$ que cumple:
(1) $\delta(0) = \text{ínf}\{\sigma \in \mathcal{O} | \, \delta g < \sigma,$ para cada $g \in M \setminus \{0\}$.
(2) Para cada $g_1, g_2 \in M$, existe $q \in R$ y $r \in M$ de manera que $g_1 = g_2 q + r$ y $r = 0$ ó $r \neq 0$ y $\delta(r) < \delta(g_2)$.

Un R-modulo a la derecha M es un **modulo euclídeo** si existe una norma euclídea δ en M.

Un R-modulo a la derecha M se llama **principal** si submódulo de M sea cíclico.

Lema 1.14. *Si M es un R-módulo a la derecha euclídeo, entonces M es principal.*

Lema 1.15. *Si M es un R-módulo a la derecha euclídeo a la derecha, entonces cada submódulo $N \subseteq M$ es un módulo euclídeo.*

Lema 1.16. *Si M es un R-módulo a la derecha euclídeo, para cada submódulo $N \subseteq M$, el cociente M/N es un módulo euclídeo.*

Si $\{\delta_i |\ i \in I\}$ es una familia de normas euclídeas en un R–módulo a la derecha M, y definimos $\wedge_i \delta_i$ como $\wedge_i \delta_i(a) = \text{ínf}\{\delta_i(a)/\ i \in I\}$, para cada $a \in M$, tenemos la siguiente proposición:

Proposición 1.17. *Haciendo uso de la notación anterior; para cada familia no vacía $\{\delta_i |\ i \in I\}$ de normas euclídeas en M, tenemos que $\wedge_i \delta_i$ es una norma euclídea. En particular, en cualquier R-módulo a la derecha euclídeo existe una norma euclídea mínima, δ_0.*

DEMOSTRACIÓN. Dados $f, g \in M$ sea $\wedge_i \delta_i(f) = \delta_i(f)$, para algún índice $i \in I$. Basándonos en las hipótesis, hay un $q \in R$ y $r \in M$ de manera que $g = fq + r$, siendo $r = 0$, ó $r \neq 0$ y $\delta_i(r) < \delta_i(f)$. Por lo tanto, como si $r \neq 0$, ocurre que $\wedge_i \delta_i(r) \leq \delta_i(r) < \delta_i(f) = \wedge_i \delta_i(f)$, tenemos que $\wedge_i \delta_i$ es una norma euclídea en M.

Ejemplo 1.18. Consideramos $\mathbb{Q}$ como grupo abeliano y definimos $\delta : \mathbb{Q} \longrightarrow \mathcal{O}$ como

$$\delta(q) = \begin{cases} \omega, \text{ si } q = 0, \\ \text{máx}\{i |\ x_i \neq 0, \text{ en } |q| = \sum_{i=-\infty}^{\infty} x_i 10^i, \text{ la expansion decimal de } |q|\}. \end{cases}$$

Es decir, $\delta(q) = [log(q)]$.

Si $q_1, q_2 \in Q_{>0}$ y $\delta(q_1) \geq \delta(q_2))$ entonces $q_1 = q_2[\frac{q_1}{q_2}] + (q_1 - q_2[\frac{q_1}{q_2}])$. Por eso, $\delta(q_1 - q_2[\frac{q_1}{q_2}]) < \delta(q_1)$ y por recurrencia obtenemos $q, r \in \mathbb{Q}$ de manera que $q_1 = q_2 q + r$ verificando $r = 0$ ó $r \neq 0$ y $\delta(r) < \delta(q_2)$.

El resultado será cierto para cualquier par $q_1, q_2 \in \mathbb{Q}^*$.

En el caso particular en el que $q_2 = -1$, por el algoritmo extendido de Euclides, obtenemos la expansión en fracciones continuas de q_1.

Normas semi–multiplicativas

La condición exigida a una función euclídea en el caso clásico $\delta(a) \leq \delta(ab)$ para cualesquiera $a, b \in D$ la hemos obviado al hacer esta definición más general de norma euclídea; vamos a rescatarla, por lo que nos aparecerá un tipo especial de norma euclídea; veremos que esta condición no aporta nada cuando estudiamos la estructura de un anillo euclídeo.

Sea δ una norma euclídea en el anillo R decimos que δ es:

(1) **Semi-multiplicativa a derecha**, si para cada $x, y \in R$, tenemos que $\delta(xy) \geq \delta(x)$.
(2) **Semi-multiplicativa a izquierda**, si para cada $x, y \in R$, tenemos que $\delta(yx) \geq \delta(x)$.
(3) Si una norma es euclídea a derecha y a izquierda, se llama **norma euclídea semi-multiplicativa**.

Juntando con lo dicho anteriormente, una norma euclídea por la derecha que sea semi-multiplicativa, la llamaremos norma euclídea semi-multiplicativa.

Sea M un R-modulo a la derecha, y δ una norma euclídea en M, tenemos entonces que δ:
(4) Es **semi-multiplicativa** si para cada $g \in M$ y $x \in R$ se cumple que $\delta(xg) \geq \delta(g)$

Vamos a demostrar que asociando a cualquier norma euclídea en cualquier R-módulo a la derecha euclídeo, existe una norma euclídea semi-multiplicativa.
Sea δ una norma euclídea en M para cualquier $a \in M$, definimos:

$$\delta_1(a) = \begin{cases} \text{ínf}\{\delta(ax) |\ x \in R, \text{ si } a \neq 0 \\ \text{ínf}\{\sigma |\ \delta_1(a) < \sigma, \text{ para todo } 0 \neq a \in M, \text{ si } a = 0\}. \end{cases}$$

De la misma forma, para cada $N \subseteq M$ definimos $\delta_1(N) = \text{ínf}\{\delta(f) |\ f \in N$.
Observamos que, en general, podemos tener que $\delta_1(0) \neq \delta(0)$.

Proposición 1.19. *Con todo lo que hemos dicho, juntando los resultados, tenemos que:*

(1) Para cualquier $a \in M$, existe $a' \in aR$ de manera que $\delta(a') = \delta_1(a)$ y $a'R = aR$.
(2) Si $N_1 \subseteq N_2$ entonces ocurre que $\delta_1(N_2) \leq \delta_1(N_1)$ y $\delta_1(N_2) = \delta_1(N_1)$ cuando $N_1 = N_2$.
(3) Para cualquier $a \in M$ tenemos que $\delta_1(a) \leq \delta(a)$.
(4) δ_1 es una norma euclídea.
(5) δ_1 es semi-multiplicativo, es decir, $\delta_1(at) \geq \delta_1(a)$ para cada $a \in M$ y cada $t \in R$.
(6) δ es semi-multiplicativo si, y solo si, $\delta = \delta_1$.

DEMOSTRACIÓN. (1) y (3) son obvias por la definición.

(2). La condición suficiente está clara. De lo contrario, si $\delta_1(gt) = \delta(g)$ para cualquier $v \in R$ existe $q, r \in R$ de manera que $gv = (gt)q + r$; si $r = 0$ entonces $\delta_1(r) < \delta_1(gt) = \delta_1(g)$ pero como $r = gv - gtq \in xR$. Esto es, $\delta_1(r) \geq \delta_1(g)$, lo cual es una contradicción.

(4). Sean $g_1, g_2 \in M$ y $a \in R$ con $\delta_1(g_2) = \delta_1(g_2 a)$. Existe $q \in R$ y $r \in M$ de manera que $g_1 = g_2 aq + r$. Si $r = 0$, entonces tendríamos una división. Si $r \neq 0$ entonces tenemos que $\delta_1(r) \leq \delta(r) < \delta(ga) = \delta_1(g_2)$ y tenemos una división.

(5). Está claro que para cada $a \in M$ y cada $t \in R$, tenemos que $\delta_1(at) \leq \delta(at) \geq \delta_1(a)$.

Proposición 1.20. *Sea δ una norma semi-multiplicativa en M, para cualquier $g, f \in M$ tenemos que:*

(1) $\delta(f) \leq \delta(g)$ cuando $gR \subseteq fR$
(2) Si $gR \subseteq fR$ entonces $\delta(f) < \delta(g)$ si y solo si $gR \subsetneqq fR$

DEMOSTRACIÓN. (1). Está claro haciendo uso de la definición.
(2). Si $\delta(f) < \delta(g)$ entonces $gR \subsetneqq fR$. De lo contrario, si $gR \subsetneqq fR$ y $\delta(f) = \delta(g)$, hay $q \in R$ y $r \in M$ de manera que $f = gq + r$, donde $r \neq 0$, por hipótesis, tenemos que $\delta(r) < \delta(g) < \delta(f)$ pero $r = f + gq \in fR$, por lo que $\delta(f) \leq \delta(r)$, lo cual es una contradicción.

Observación. 1.21. La norma euclídea mínima δ_0 es siempre semi-multiplicativa, pero no todas las normas euclídeas son semi-multiplicativas.

Ejemplo 1.22. Sea $\delta : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{\omega\}$ definida como:

$$\delta(n) = 2|n| + \frac{n}{2|n|} - \frac{1}{2} = \begin{cases} 2n-1, & \text{si } n > 0 \\ -2n, & \text{si } n < 0. \end{cases}$$

y $\delta(0) = \omega$. Tenemos que δ no es una norma euclídea semi-multiplicativa. De hecho, $\delta((-1)(-1)) = \delta(1) = 1 < 2 = \delta(-1)$

Sabemos que si δ es una norma euclídea en R, los elementos $a \in R$ de manera que $\delta(a)$ es mínimo en $\delta(R)$ son invertibles por la derecha.
Podemos dar la vuelta a esta implicación bajo las condiciones de norma semi-multiplicativa.

Lema 1.23. *Sea δ una norma euclídea semi-multiplicativa en un anillo R, para cada elemento $a \in R$ son equivalentes:*

(a) a es invertible por la derecha.
(b) $\delta(a)$ es mínima en $\delta(R)$.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Lo hemos visto en el Lema (1.9.).
(a) $\Rightarrow$ (b). Si $a \in R$ es invertible por la derecha, entonces existe $y \in R$ de manera que $ab = 1$, entonces, $\delta(1) = \delta(ab) \geq \delta(a)$.
Por otro lado tenemos que para cada elemento $v \in R$ ocurre que $\delta(v) = \delta(1v) \geq \delta(1)$. En consecuencia, obtenemos que $\delta(a) = \delta(1)$ y $\delta(1)$ es mínimo en $\delta(R)$.
Si en lugar de tener un anillo, tenemos un módulo G, obtendríamos este otro lema:

Lema 1.24. *Sea δ una norma euclídea semi-multiplicativa en un R–módulo a la derecha M, para cada $g \in M$ son equivalentes:*

(a) g es un generador de M.
(b) $\delta(g)$ es mínimo en $\delta(M)$.

Ejemplo 1.25. Sea $p \in \mathbb{Z}$ un número entero positivo primo, para cualquier $n \in \mathbb{N}$, el anillo $\mathbb{Z}_{p^n}$ es euclídeo.

Cualquier elemento distinto de cero en $\mathbb{Z}_{p^n}$ tiene una única representación de la forma $p^a x$ siendo $0 \leq a < n$ y $o \leq x < p$. Definimos $\delta_0 : \mathbb{Z}_{p^n} \longrightarrow \mathcal{O}$ como:

$$\delta_0(x) = \begin{cases} 0, & \text{si } 1 \leq x < p, \\ a, & \text{si } x = p^a u \text{ y } a \neq 0,\ 1 \leq u < p, \\ n, & \text{si } x = 0 \end{cases}$$

Tenemos que δ_0 es la norma euclídea mínima en $\mathbb{Z}_{p^n}$.

Ejemplo 1.26. Sean $p_1 \dots p_s \in \mathbb{Z}$ números enteros positivos primos y $l_1 \dots l_t \in \mathbb{N}^*$. Entonces el anillo $\mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ es euclídeo.

Supongamos que $p_1 < \dots < p_s$ entonces cada elemento en $\mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ tiene una representación única que es de la forma ${p_1}^{x_1} \dots {p_s}^{x_s} a$, siendo $0 \leq x_i < l_i$ para cualquier $i = 1, \dots, s$ y a un primo relativo con $p_1, \dots, p_s$.

Vamos a definir pues;

(1) $T_{-1} = \{0\}$.

(2) $T_0 = T_{-1} \cup \{a < {p_1}^{l_1} \dots {p_s}^{l_s} |$ primo relativo con $p_1 \dots p_s\}$

(3) $T_1 = T_0 \cup \{p_i a |\ a < {p_1}^{l_1} \dots {p_s}^{l_s} |$ primo relativo con $p_1 \dots p_s\}$

Por lo que ocurre que para cualquier $b = {p_1}^{x_1} \dots {p_s}^{x_s} a \in \mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}} \setminus T_0$. Si $x_i \geq 1$, entonces tenemos que $b - p_i({p_1}^{x_1} \dots {p_i}^{x_i - 1} \dots {p_s}^{x_s} a) = 0 \in T_0$.

Si ocurre lo contrario, esto es, si $x_i = 0$ siento los índices $j \neq i$ de tal manera que $x_j = 0$, vamos a decir que $\{j_1 \dots, j_t\},\ b - p_i(\prod_{n=1}^{t} p_{jn})$ es primo relativo con $p_1 \dots p_s$ y es por esto que sabemos que $b - p_i(\prod_{n=1}^{t} p_{jn}) \in T_0$.

Si $a \in T_0$, entonces $p_i a \in T_1$ para cada p_i.

(4) $T_2 = T_1 \cup \{{p_1}^{x_1} \dots {p_s}^{x_s} a |\ \sum_{i=1}^{s} x_i = 2$ y a es un primo relativo con $p_1 \dots p_s\}$. Contamos con que para cada $b = {p_1}^{x_1} \dots {p_s}^{x_s} a \in \mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}} \setminus T_1$ ocurre que $\sum_{i=1}^{s} x_i \geq 2$.

Ahora bien, consideramos p_1^2; si $x_i \geq 2$ entonces va a existir un $q \in \mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ de manera que $b - p_1^2 q \in T_1$.

Si $x_1 = 1$, existirá un $q \in \mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ de manera que $\frac{b}{p_1} - p_1 q \in T_0$ y es por esto que $b - p_1^2 q \in T_1$.

Si $x_1 = 0$, procedemos igual que en el punto anterior, es decir, si $x_1 = 0$ existirá un $q \in \mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ de manera que $b - p_1 \in T_0$ y es por esto que $b - p_1^2 q \in T_1$.

De la misma forma razonaríamos que $p_1 p_2 \in T_2$.

Por lo tanto, el resultado es válido para todos los productos $p_i p_j$.

Si definimos

$$T_n = T_{n-1} \cup \{{p_1}^{x_1} \dots {p_s}^{x_s} a | \sum_{i=1}^{s} x_i = n \text{ y } a \text{ es un primo relativo con } p_1 \dots p_s\}$$

para todo $n = 3, \dots, \sum_{i=1}^{s} l_i - 1$, entonces obtendríamos la norma euclídea mínima en $\mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$ con $\delta(0) = \sum_{i=1}^{s} l_i$ y $\delta({p_1}^{x_1} \dots {p_s}^{x_s} a) = \sum_{i=1}^{s} x_i$.
Posiblemente, haya mas normas euclídeas en $\mathbb{Z}_{{p_1}^{l_1} \dots {p_s}^{l_s}}$, como por ejemplo, las que están definidas por el producto $\mathbb{Z}_{{p_1}^{l_1} \times \dots \times {p_s}^{l_s}}$.

Llegados a este punto; nos preguntamos: ¿Podríamos extender éste resultado para anillos no integrales y factorizaciones en ellos?.

Problema 1.27. *Sea D un dominio euclídeo y con δ_0 la norma euclídea mínima tal que $\delta_0(D)$ tiene $\mathbb{N}$ como un segmento inicial.*
Sea $\wp$ el conjunto de representantes de elementos primos y $\nu_p(a)$ la mayor potencia de p en la factorización de a.
En esta situación tenemos que $\delta_0(a) \geq \sum\{\nu_p(a) | \, p \in \wp\}$ para todo $0 \neq a \in D$.

Solución 1.28. Lo hacemos por inducción en $\sum \nu_p(a)$. Si $\sum \nu_p(a) = 0$ entonces a es invertible, lo cual implica que $\delta_0(a) = 0$.
Supongamos pues que $\sum \nu_p(a) < s \in \mathbb{N}$ y sea $a \in R$ de manera que $\sum_{\nu_p(a)} = s$, entonces va a existir una factorización $a = p_1 \dots p_t a'$ con $p_i \in \wp$ y $a' \in R$ invertible.
Como desde $p_2 \dots p_s a'$ es un propio factor de a y $\sum \nu_p(p_2 \dots p_s a') = s - t$ entonces ocurre que $\delta(a) > \delta(p_2 \dots p_s a') \geq s - 1$.

Proposición 1.29. *Sea A un dominio de ideales principales, que tiene solo un conjunto finito de representantes de elementos primos $\wp = \{p_1 \dots p_s\}$ entonces $\delta_0(a) = \sum\{\nu_p(a) | \, p \in \wp\}$ define la norma euclídea mínima de R.*

DEMOSTRACIÓN. Denotamos por $\nu_i = \nu_{p_i}$ la valoración definida por p_i para cualquier índice $i = 1, \dots, s$. Sea $x, y \in R$ de tal manera que $x \neq yR$ y consideramos cualquier $a \in \bar{x} \in R/yR$. Si $\nu_i(a) \geq \nu_i(y)$ para cualquier índice i, entonces $y | a$, y $x \in yR$ lo cual es una contradicción.
Entonces; para todo $a \in \bar{x}$, existirá una partición $\wp = \wp_1 \cup \wp_2$ con $\wp_1 = \{p \in \wp | \; \nu_p(a) < \nu_p(y)\}$ y $\wp_2 = \{q \in \wp | \; \nu_q(a) \geq \nu_q(y)\}$.

(1) Para cualquier $q \in \wp_2$, sea $f = \nu_q(a) \geq \nu_q(y) = g$ y $a = q^f a', y = q^g y'$, entonces $q \nmid y'$. Por lo tanto, existe $c_q \in R$ de manera que $y' c_q \equiv q^{f-g} a' (\mod q)$. Si multiplicamos por q^g tenemos $y c_q \equiv a (\mod q^{g+1})$.

    Para cualquier $q \in \wp_2$ consideramos la ecuación de congruencias $X \equiv (1 - c_q) (\mod q)$ y variando q tendríamos el sistema de congruencias $X \equiv (1 - c_q) (\mod q) | \; q \in$

$\wp_2$. Por el teorema chino del resto, existe un $c \in R$ de manera que $c \equiv (1-c_q)($ mód $q^{g+1})$ para cualquier $q \in \wp_2$. En consecuencia de esto, tenemos que $b = a + yc$ es otra representación de $\bar{x}$ y satisface que $q^g | b$. Además tenemos que: $y = a+yc \equiv a+y(1-c_q)($ mód $q^{g+1}) = a+y-yc_q \equiv a+y-a($ mód $q^{g+1}) = y($ mód $q^{g+1})$.

Por tanto, $\nu_q(b) = \nu_q(y) = g$.

(2) Para cualquier $p \in \wp_1$, con $f = \nu_p(a) < \nu_p(y) = g$ ya que $\bar{b} = \bar{a}$ si $n = \nu_p(b) \geq \nu_p(y) = g$.

Entonces $b - a = p^n b' - p^f a = p^f(p^{n-f} b' - a')$ es múltiplo de $y = p^g y'$ y con $f < g$, entonces, $p|(p^{n-f} b' - a')$ y esto es una contradicción.

En consecuencia, tenemos que $\nu_p(b) < \nu_p(y)$.

De ésta manera, encontramos $b \in \bar{x}$ tal que $\sum_p \nu_p(b) < \sum_p \nu_p(y)$.

El Ejemplo (1.26.) podría ser un ejemplo de éste resultado en el caso de un anillo que no es de integridad.

Corolario 1.30. *Sea D un dominio de ideales principales que posee solamente un conjunto finito de representantes de elementos primos $p_1, \ldots, p_s$. Entonces para cualquier elección $(t_1, \ldots, t_s) \in (\mathbb{N}^*)^s$ tenemos:*

(1) $S_{(t_1,\ldots,t_s)}(a) = \sum_i \nu_{p_i}(a) t_i$ define una norma euclídea de D la cual es un mínimo entre las normas aditivas siempre que $(t_1 \ldots t_s) = (1, \ldots, 1)$.

(2) $S_{[t_1,\ldots,t_s]}(a) = \sum_i t_i^{\nu_{p_i}(a)}$ define una norma euclídea de D la cual es un mínimo entre las normas multiplicativas siempre que $(t_1 \ldots t_s) = (1, \ldots, 1)$.

Corolario 1.31. *Sea D un dominio de integridad y δ_1, δ_2 normas euclídeas aditivas. No necesariamente $\delta_1 \wedge \delta_2$ es aditiva.*

Corolario 1.32. *Sea D un dominio de integridad y δ_1, δ_2 normas euclídeas multiplicativas. No necesariamente $\delta_1 \wedge \delta_2$ es multiplicativa.*

Podemos incluso tratar casos no conmutativos como el siguiente:

Problema 1.33. *Sea C un cuerpo y $D = M_2(C)$ el anillo de las matrices cuadradas 2×2 con coeficientes en C. Vamos a demostrar que D es un anillo euclídeo. Para ello definimos*

$$\delta(x) = \begin{cases} 0, & \text{si } x \text{ es invertible,} \\ 1, & \text{si } x \neq 0 \text{ y no es invertible,} \\ 2, & \text{si } x = 0, \end{cases}$$

y probamos que es una norma euclídea semi–multiplicativa. De hecho, es la norma euclídea mínima.

Solución 1.34. Queremos ver que δ es una norma euclídea, por lo tanto, tenemos que ver que para dos matrices x e y de rango 1, existen $q, r \in D$ de manera que $x = yq + r$, siendo $r = 0$ ó $\delta(r) < \delta(y)$.

Sea $x = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$ una matriz de rango uno entonces podemos suponer que la segunda columna es múltiplo de la primera.

Si $\begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = c \begin{pmatrix} x_{12} \\ x_{22} \end{pmatrix}$ entonces $x \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_{11} & 0 \\ x_{21} & 0 \end{pmatrix}$.

Ahora suponemos que ocurre lo mismo con la matriz y. Esto es, si $y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$ entonces existe una matriz $x \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ de tal manera que $y \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y_{11} & 0 \\ y_{21} & 0 \end{pmatrix}$.

Juntamos lo obtenido y tenemos que $x = \begin{pmatrix} x_{11} & 0 \\ x_{21} & 0 \end{pmatrix}$ e $y = \begin{pmatrix} y_{11} & 0 \\ y_{21} & 0 \end{pmatrix}$. Así que pueden ocurrir dos cosas:

(1) Que exista $s \in C$ de manera que $\begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = s \begin{pmatrix} y_{11} \\ y_{21} \end{pmatrix}$. Y en este caso tendríamos que $x = y \begin{pmatrix} s & 0 \\ 0 & 0 \end{pmatrix}$, que es una división exacta.

(2) Que no exista $s \in C$ tal que $\begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = s \begin{pmatrix} y_{11} \\ y_{21} \end{pmatrix}$. Y en este caso entonces tendríamos que $x = y \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} x_{11} & y_{11} \\ x_{21} & y_{21} \end{pmatrix}$ que es una división con resto en una matriz invertible.

En cualquiera de los dos casos ocurre que existen $q, r \in D$ de manera que $x = yq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(y)$.

Lo que haremos será considerar el caso general, entonces estaríamos en la siguiente situación: $x \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = y \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} q + r$ por lo tanto, $x = y \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} q \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} + r \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$.

- Si $r = 0$ tendríamos que $r \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = 0$ y si r es invertible entonces $r \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ es invertible.

Los otros casos se resuelven con el mismo razonamiento.

Ahora bien, para demostrar que δ es una norma euclídea semi–multiplicativa, para cualquier $x, y \in D$, tenemos que:

- Si $xy = 0$ ocurre que $\delta(xy) \geq \delta(x)$.
- Si $xy \neq 0$ es invertible, ocurre que x e y son invertibles y por tanto, $\delta(xy) = 0 = \delta(x)$.
- Si xy no son invertibles, entonces, o bien x no es invertible y por tanto $\delta(xy) = 1 = \delta(x)$ o bien x es invertible y entonces $\delta(xy) = 1 > 0 = \delta(x)$.

Por último, si $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ entonces $2 = \delta(a^2)$ y $\delta(a)\delta(a) = 1$ por tanto son distintos ya que $2 \neq 1$ y queda demostrado que δ no es multiplicativo.

Dijimos anteriormente que hay ejemplos de normas euclídeas en $\mathbb{Z}$ que no son semi-multiplicativas, así que vamos a mostrar otro ejemplo de dichas normas.

Ejemplo 1.35. (Norma euclídea no semi-multiplicativa en $\mathbb{Z}$) Sea $\delta : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{\omega\}$ la aplicación definida como:

$$\delta(n) = \begin{cases} |n|, & \text{si } n \neq 5, 0 \\ 13, & \text{si } n = 5 \\ \omega, & \text{si } n = 0 \end{cases}$$

Primero de todo es ver que δ es una norma euclídea. Dados $x, y \in \mathbb{Z}$, tenemos un único problema que surge cuando $6 \leq |y| \leq 13$. Y en este caso, la división clásica euclídea $x = yq + r$ con $0 \leq r < |y| \leq 13$ funciona siempre que $r \neq 5$. Vemos que pasa si $r = 5$. En este caso, realizamos una modificación: $x = |y|q + r = |y|(q+1) + (5 - |y|)$ y tendríamos que $\delta(5 - |y|) < \delta(y)$.
Con $\delta(10) = 10 < 13 = \delta(5)$ tendríamos que δ es no semi-multiplicativa.

Observación. 1.36. Como consecuencia de la Proposición (1.19.), la norma euclídea mínima definida por la construcción de Motzkin en el Lema (1.4.) o la Proposición (1.6.) es semi-multiplicativa.

Veamos algunas propiedades que posee la norma euclídea mínima.

Proposición 1.37. *Sea δ_0 la norma euclídea mínima en el anillo euclídeo R, y definimos:*

$$R_{(\sigma)} = \{a \in R |\ \delta(x) \leq \sigma\}. R_{(\sigma)} = \{a \in R |\ \delta(x) < \sigma\}.$$

Entonces $R_{(\sigma)}$ es la unión de $\{0\}$ y $\{y \in R |\ R_\sigma \longrightarrow R/yR$ es sobreyectiva$\}$

DEMOSTRACIÓN. Está claro que para cualquier $y \in R_{(\sigma)} \setminus R_\sigma$ la aplicación $n : R_\sigma \longrightarrow R/yR$ es sobreyectiva. Para todo $x \in R$, la clase $x + yR$ es la imagen del resto de la

división de x por y. De lo contrario, si $n : R_\sigma \longrightarrow R/yR$ es sobreyectiva y $\delta(y) > \sigma$, podemos definir una nueva norma euclídea tal que así:

$$\delta(a) = \begin{cases} \delta_0(a), & \text{si } a \neq y, \\ \delta, & \text{si } a = y \end{cases}$$

Por tanto, $\delta < \delta_0$, lo que es una contradicción.

En consecuencia de esto, $\delta_0(y) \leq \sigma$, e $y \in R_{(\sigma)}$.

Esto significa que existe un método de inducción transfinito para construir la norma euclídea mínima.

Este resultado puede ser reformulado para la norma euclídea mínima en un D-modulo a la derecha M, y puede caracterizarse como sigue:

Proposición 1.38. *Sea δ una norma euclídea en M, son equivalentes:*

(1) δ es mínimo.
(2) Para todo $g \in M$ y cualquier ordinal $\sigma < \delta(g)$, existe $g_\sigma \in M \setminus gR$ de manera que $\delta(g_\sigma - g_q) \geq \sigma$ para todo $q \in R$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Definimos $\delta' : G \longrightarrow \mathcal{O}$ como:

$$\delta'(a) = \begin{cases} \delta(a), & \text{si } a \neq g, \\ \sigma, & \text{si } a = g, \end{cases}$$

Tenemos entonces que δ es mínimo y $\delta'(g) < \delta(g)$ entonces δ' no es una norma euclídea.

Por tanto existe $g_\sigma \in G \setminus gD$ de tal manera que $\delta(g_\sigma - g_q) \geq \sigma$.

(b) $\Rightarrow$ (a). Supongamos que existe una norma euclídea δ' de tal manera que $\delta' < \delta$ entonces existe $g \in M$ tal que $\delta'(g) < \delta(g)$.

Tomamos g de manera que si $\delta'(a) < \delta(g)$ entonces $\delta(a) \leq \delta'(a)$.

Si llamamos $\sigma = \delta'(g)$, existe $g_\sigma \in G \setminus gD$ tal que $\delta(g_\sigma - g_q) \geq \sigma = \delta'(g)$ para todo $q \in D$.

Por otra parte, la división de g_σ por g respecto de la norma δ' nos da un elemento $q \in D$ que cumple que $\delta'(g_\sigma - g_q) < \delta'(g) = \sigma < \delta(g)$. Por lo tanto, $\delta(g_\sigma - g_q) \leq \delta'(g_\sigma - g_q) < \sigma$, lo que es una contradicción.

Producto directo de anillos euclídeos

Con todo lo dicho, vamos a nombrar la proposición a la cual queríamos llegar, que es el tercer y último objetivo que tocamos en éste trabajo:

Proposición 1.39. *El producto de un número finito de anillos euclídeos es un anillo euclídeo.*

DEMOSTRACIÓN. Sean D_1, D_2 anillos euclídeos con normas euclídeas $\delta_i : D_i \longrightarrow \mathcal{O}_i$ con $i = 1, 2$. Consideramos $\mathcal{O}' = \mathcal{O}_1 \times \mathcal{O}_2$ y $\mathcal{O} = \mathcal{O}' + \mathcal{O}'$ como el producto y la suma respectivamente con las inclusiones $j_1, j_2 : \mathcal{O}' \longrightarrow \mathcal{O}$, $j_1(\sigma) < j_2(\tau)$, $\forall\ \sigma, \tau \in \mathcal{O}'$.
Definimos $j : D = D_1 \times D_2 \longrightarrow \mathcal{O}$ por:

$$\delta'(x_1, x_2) = \begin{cases} j_1(\delta_1(x_1), \delta_2(x_2)), & \text{si } x_1 \neq 0, \\ j_2(\delta_1(0), \delta_2(x_2)), & \text{si } x_1 = 0. \end{cases}$$

Podemos afirmar entonces que δ es una norma euclídea.
Por lo que si $(x_1, x_2), (y_1, y_2) \in D$, tendríamos que diferenciar entre los siguientes casos:

(1) $y_1 \neq 0$ entonces $x_1 = y_1 q_1 + r_1$, $x_2 = y_2 q_2 + r_2$.

- Si $r_1 \neq 0$ entonces $(x_1, x_2) = (y_1, y_2)(q_1, q_2) + (r_1, r_2)$ y $\delta(r_1, r_2) < \delta(y_1, y_2)$.
- Si $r_1 = 0$ entonces $(x_1, x_2) = (y_1, y_2)(q_1 - 1, q_2) + (y_1, r_2)$ y $\delta(y_1, r_2) < \delta(y_1, y_2)$.

(2) $y_1 = 0$, entonces $x_1 = r_1$, $x_2 = y_2 q_2 + r_2$.

- Si $r_1 \neq 0$, entonces $(x_1, x_2) = (0, y_2)(q_1, q_2) + (r_1, r_2)$ y $\delta(r_1, r_2) < \delta(0, y_2)$.
- Si $r_1 = 0$ entonces $(x_1, x_2) = (0, y_2)(q_1 - 1, q_2) + (0, r_2)$ y $\delta(0, r_2) < \delta(0, y_2)$.

Observación. 1.40. Podemos usar $\delta : D \longrightarrow \mathcal{O}_1 \times \mathcal{O}_2$ como usamos j_2 solo cuando la primera componente es cero.

AÑADIR

Antes de citar los siguientes ejemplos, necesitamos dos definiciones:

Definición 1.41. Sea $x_1 \subseteq x_2 \subseteq \ldots \subseteq x_n \subseteq \ldots$ una cadena de ideales, entonces si existe un $n \in \mathbb{N}$ tal que $x_n = x_{n+k}$ para todo $k \in \mathbb{N}$ decimos que el anillo es **noetheriano**.

Definición 1.42. Sea $x_1 \supseteq x_2 \supseteq \ldots \supseteq x_n \supseteq \ldots$ una cadena de ideales, entonces si existe un $n \in \mathbb{N}$ tal que $x_n = x_{n+k}$ para todo $k \in \mathbb{N}$ decimos que el anillo es **artiniano**.

Definición 1.43. Sea D un anillo y sea x un elemento del anillo, $x \in D$, dicho elemento se llama **nilpotente** si existe un número entero positivo, n, tal que $x^n = 0$.

DESPUES DE LA OBSERVACIÓN 1.38:

Ejemplos 1.44. 1. Vamos a considerar el anillo $A = \mathbb{Z} \times \mathbb{Z}$ y vamos a considerar un anillo euclídeo conmutativo arbitrario con un número finito de elementos invertibles y con una norma euclídea en $\mathbb{N}$. Esto es, tenemos la aplicación $\delta : A \longrightarrow \mathbb{N} \cup \{\omega\}$; para todo $n \in N$ el subconjunto $\delta^{-1}(n)$ es finito. Sea $A_{(n)} = \{x \in A \mid \delta(x) \leq n\}$ y $A_n = \{x \in A \mid \delta(x) < n\}$. Haciendo uso del Lemma (1.9.), $A_{(0)}$ es finito.

Supongamos entonces que A_n es finito y probamos que $A_{(n)}$ es finito para cualquier $n \geq 1$. Para cualquier $y \in A_{(n)} \setminus A_n$ tenemos que $\delta(y) = n$ y una aplicación sobreyectiva: $A_n \longrightarrow A/yA$ por lo tanto A/yA es finito. Particularmente; cualquiera que sea $y \in A_{(n)} \setminus A_n$ tendríamos un número finito de cocientes distintos de la forma A/yA.

Ahora consideramos la familia $\{x_i \ / \ i \in I\}$ de todos los ideales yA con $\delta(y) = n$ de manera que $A/x_i \cong A/x_i =: Y$ es finito, entonces definimos $x = \cap_i x_i$, por lo tanto, tendríamos la aplicación de un anillo inyectivo: $A/x \longrightarrow \prod_i \frac{A}{x_i} \cong Y^I$. Por lo que Y es finito, es artiniano y tiene un número finito de ideales máximos: $r_1, \ldots, r_s$ que satisfacen:

(I) Y/r_j es finito, por lo tanto es un cuerpo finito si $|Y/r_j| = z_j$ entonces $y^{z_j} - y \in r_j$ para todo $y \in Y$.

(II) r_j es nilpotente por tanto existe $t_j \in \mathbb{N}$ de manera que $r_j^{t_j} = 0$

Si consideramos todos los ideales máximos $r_j' t$ entonces todo elemento $y \in Y$ verifica que $\prod_{j=1}^{s}(y^{z_j} - y)^{t_j} = 0$. Particularmente, todo elemento de Y es una raíz del polinomio $P(X) = \prod_{j=1}^{s}(X^{z_j} - X)^{t_j}$.

Lo mismo ocurre para Y^I y para A/x.

Sea $H = A/x$ y $p \subseteq H$ un ideal primo, entonces todos los elementos de H/p son resto de $P(X)$ y H/p es finito, por tanto también es cuerpo y $p \subseteq H$ es un ideal

maximal. Decimos entonces que todo ideal primo es maximal. Dado que H es noetheriano, entonces H es artiniano con cuerpo residual finito por lo que H es finito.

Finalmente; si consideramos la correspondencia entre el ideal de H y los ideales de A que contienen a x, entonces existen muchos de ellos, es decir, la familia $\{x_i \mid i \in I\}$ es finita.

2. Supongamos que existe la norma euclídea $\delta : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{N} \cup \{\omega\}$. Sea $n \in \mathbb{N}$ tal que $\delta(1,0) = n$. Por lo tanto, existe una aplicación sobreyectiva $A_n \longrightarrow \frac{\mathbb{Z}\times\mathbb{Z}}{((1,0))}$, lo cual es una CONTRADICCIÓN.

Sean G_1 y G_2 $D-modulos$ por la derecha. Si G_1 y G_2 son principales; su producto $G_1 \times G_2$ no tiene por qué ser necesariamente principal. Consideramos, por ejemplo, el producto $\mathbb{Z}_2 \times \mathbb{Z}_2$. De hecho, si G es un $D-modulo$ por la derecha, el producto directo $G \times G$ nunca es principal porque no es cíclico.

En el siguiente teorema se caracteriza esos pares de módulos principales G_1 y G_2, tales que su producto $G_1 \times G_2$ es principal.

Sean G_1 y G_2 $D-modulos$ por la derecha, entonces ocurre que G_1 y G_2 no tienen subfactores isomorfos distintos de cero.

Una condición aritmética necesaria; es que para cualquier $g_2 \in G_2$, $g_1, g_1' \in G_1$ tenemos que; $Ann(g_2) + (g_1' D : g_1) = D$. Por lo cual, $Ann(g_1) + Ann(g_2) = D$ para cualquier $g_1 \in G_1, g_2 \in G_2$. Siendo Ann el nucleo de la aplicación, al que llamamos anulador que es de la forma: $Ann(G) = \{m \in D \ / \ mg = 0 \ \forall \ g \in G\}$.

Obtenemos así el siguiente resultado:

Teorema 1.45. *Sean G_1, G_2 $D-modulos$ principales por la derecha. Entonces:*

1. *$G_1 \times G_2$ es principal.*
2. *G_1 y G_2 no tienen subfactores isomorfos distintos de cero.*

Son equivalentes.

DEMOSTRACIÓN. $a) \Rightarrow b)$ Sea T un subfactor común de G_1 y G_2. Dado que T es un subfactor de G_1, existe un cociente G_1/X_1 tal que T 4se isomorfo a un submodulo de G_1/X_1. Por lo que T es isomorfo al cociente del submodulo de G_1.

DIAGRAMA

De la misma forma, existe un submodulo $B_2 \subseteq G_2$ de manera que T es cociente de B_2. En éstas condiciones, tenemos que $B_1 \times B_2 \subseteq G_1 \times G_2 \subseteq$ tiene un cociente isomorto a $T \times T$. Por eso, $G_1 \times G_2$ no es principal.

$b) \Rightarrow a)$ Si G_1, G_2 no tienen subfactores isomorfos distintos de cero, entones $\mathscr{L}(G_1 \times G_2) \cong \mathscr{L}(G_1) \times \mathscr{L}(G_2)$ por lo que para cualquier submodulo $F \subseteq G_1 \times G_2$ existen

submódulos $F_1 \subseteq G_1$ y $F_2 \subseteq G_2$ de manera que $F = F_1 \times F_2$ y solo tenemos que demostrar que el producto de dos módulos cíclicos es un módulo cíclico.

Sea $G_1 = g_1 D$ y $G_2 = g_2 D$; por hipótesis tenemos que $Ann(g_1) + Ann(g_2) = D$. Y existe un isomorfismo $G_i = g_i D \cong D/Ann(g_i)$ para $i = 1, 2$.

Existe la aplicación del monomorfismo canónico $D/Ann(g_1) = Ann(g_2) = D$ y aplicamos el Teorema Chino del Resto. Por lo tanto, $G_1 \times G_2$ es un módulo cíclico.

En efecto, sea $x_1, x_2 \in D$, con $D = Ann(g_1) + Ann(g_2)$, existe $a_{i,j} \in D$ de manera que $a_{1,1}, a_{2,2} \in Ann(g_1), a_{1,2}, a_{2,1} \in Ann(g_2)$ $a_{1,1} + a_{1,2} = x_1, a_{2,1} + a_{2,2} = x_2$.

Por lo tanto, $a_{1,2} + a_{2,1} - x_2 = a_{1,2} - a_{2,2} \in Ann(g_2)$.

Hemos caracterizado cuando el producto de dos $D - modulos$ principales por la derecha es principal.

Podemos demostrar también que el producto directo de dos $D - modulos$ euclídeos por la derecha, es un módulo euclídeo.

Teorema 1.46. *Sean G_1, G_2 $D - modulos$ principales por la derecha. Entonces:*

1. *$G_1 \times G_2$ es un módulo euclídeo.*

2. *G_1 y G_2 son módulos euclídeos y no tienen subfactores simples distintos de cero.*

Son equivalentes.

DEMOSTRACIÓN. $a) \Rightarrow b)$ Si $G_1 \times G_2$ es euclídeo, entonces G_1 y G_2 son euclídeos y, por lo tanto, es principal, entonces G_1 y G_2 no tienen subfactores simples distintos de cero.

$b) \Rightarrow a)$ Supongamos que G_i es euclídeo con la norma euclídea $\delta_i : G_i \longrightarrow \mathcal{O}$ siendo $\mathcal{O}_i = Im(\delta_i)$.

Consideramos el producto $\mathcal{O}_1 \times \mathcal{O}_2$ y la suma, es decir, la unión disjunta $\mathcal{O}_0 = (\mathcal{O}_1 \times \mathcal{O}_2) \ \forall \ (\mathcal{O}_1 \times \mathcal{O}_2)$ con las inclusiones:

$j_1 : (\mathcal{O}_1 \times \mathcal{O}_2) \longrightarrow \mathcal{O}_0$ y $j_2 : (\mathcal{O}_1 \times \mathcal{O}_2) \longrightarrow \mathcal{O}_0$ que satisfacen $j_1(a) < j_2(b)$ para cualquier $a, b \in \mathcal{O}_1 \times \mathcal{O}_2$.

Definimos $\delta : G_1 \times G_2 \longrightarrow \mathcal{O}_0$ como sigue:

$$\delta(g_1, g_2) = \begin{cases} j_1(\delta_1(g_1), \delta_2(g_2)) \ si \ g_1 \neq 0 \\ j_2(\delta_1(0), \delta_2(g_2)) \ si \ g_1 = 0 \end{cases}$$

Sean $(g_1, g_2), (f_1, f_2) \in (G_1 \times G_2)$ tales que $(g_1, g_2) \notin (f_1, f_2)D$.

Existe $q_i \in D$ y $r_i \in G_i$ para $i = 1, 2$ de manera que $g_i = f_i q_i + r_i$.

Tenemos pues $Ann(f_1) + Ann(f_2) = D$ por lo que existe $l_i \in Ann(f_i)$, para $i = 1, 2$ tales que $l_1 + l_2 = 1$. Tenemos las siguientes posibilidades:

- $f_1 \neq 0$ y $r_1 \neq 0$. Considerando $q = l_2q_1 + l_2q_2$ tenemos que $(f_1, f_2)q + (r_1, r_2) = (f_1l_2q_1, f_2l_1q_2) + (r_1, r_2) = (f_1q_1, f_2q_2) + (r_1, r_2) = (g_1, g_2)$ y $\delta(r_1, r_2) < \delta(f_1, f_2)$.
- $f_1 = 0$ y $r_1 = 0$. Considerando $q = l_2(q_1 - 1) + l_2q_2$ tenemos que $(f_1, f_2)q + (f_1, r_2) = (f_1l_2(q_1-1), f_2l_1q_2)+(f_1, r_2) = (f_1q_1, f_2q_2)+(0, r_2) = (g_1, g_2)$ y $\delta(f_1, r_2) < \delta(f_1, f_2)$.
- $f_1 = 0$ y $r_1 \neq 0$. Si consideramos $q = q_2$ tenemos que $(0, f_2)q + (g_1, r_2) = (0, f_2q_2) + (g_1, r_2) = (g_1, f_2q_2 + r_2) = (g_1, g_2)$ y $\delta(g_1, r_2) < \delta(0, f_2) = \delta(f_1, f_2)$.
- $f_1 = 0$ y $r_1 = 0$ entonces $q_1 = 0$ y si consideramos $q = q_2$ tenemos que $(0, f_2)q + (0, r_2) = (0, f_2q_2) + (0, r_2) = (0, f_2q_2 + r_2) = (g_1, g_2)$ y $\delta(0, r_2) < \delta(0, f_2) = \delta(f_1, f_2)$.

Sea ahora A un anillo conmutativo y sea $R = A$ un dominio integral:

Corolario 1.47. *Si R es un dominio integral, entonces el rango de R es indescomponible.*

Corolario 1.48. *Si R es un dominio integral, y no es anillo de división, el rango de R es mayor o igual a ω.*

Ejemplo 1.49. Sean D_1, D_2 anillos euclídeos con las normas euclídeas aditivas δ_1, δ_2 respectivamente.

En general, tenemos que $D_1 \times D_2$ no es aditiva.

Por la Proposición (**??**) tenemos que

$$\delta(x_1, x_2) = \begin{cases} j_1(\delta_1(x_1), \delta_2(x_2)) \; si \; x_1 \neq 0 \\ j_2(\delta_1(0), \delta_2(x_2)) \; si \; x_1 = 0 \end{cases}$$

Si cogemos $(x_1, x_2), (y_1, y_2) \in D_1 \times D_2$, entonces: $\delta((x_1, x_2)(y_1, y_2)) = \delta(x_1y_1, x_2y_2) = j_1(\delta_1(x_1y_1), \delta_2(x_2y_2)) = j_1(\delta_1(x_1) + \delta_1(y_1), \delta_2(x_2) + \delta_2(y_2)) = j_1(\delta_1(x_1), \delta_2(x_2) + j_1(\delta_1(y_1), \delta_2(y_2) = \delta(x_1, x_2) + \delta(x_2, y_2)$.

De lo contrario, si $x_1y_1 = 0$ y $x_1, y_1 \neq 0$, entonces: $\delta((x_1, x_2)(y_1, y_2)) = \delta(x_1y_1, x_2y_2) = j_2(\delta_1(0), \delta_2(x_2y_2))$; $\delta(x_1, x_2)+\delta(y_1, y_2) = j_1(\delta_1(x_1), \delta_2(x_2))+j_1(\delta_1(y_1), \delta_2(y_2))$ y son diferentes.

Del mismo modo, si cogemos $x_1 = 0$ y $x_2 \neq 0$, entonces, $\delta((0, x_2)(y_1, y_2)) = \delta(0, x_2y_2) = j_2(\delta_1(0), \delta_2(x_2y_2))$; $\delta(0, x_2) + \delta(y_1, y_2) = j_2(\delta_1(0), \delta_2(x_2)) + j_1(\delta_1(y_1), \delta_2(y_2))$ y son diferentes.

Vamos a ver que la existencia de una norma euclídea aditiva implica la exitencia de una norma multiplicativa. Si R es trivial o es un anillo de división, se mantiene el resultado.

En otro caso, si δ es una norma aditiva euclídea, en un dominio integral, existe un ordinal $\sigma > 1$ tal que $a \longmapsto \sigma^{\delta(a)}$ es una norma multiplicativa euclídea.

Proposición 1.50. *Sea D un anillo y sea δ una norma euclídea, existe un ordinal σ tal que δ_σ es una norma multiplicativa, y $\delta \leq \delta_\sigma$*

DEMOSTRACIÓN. Si D es un anillo de división entonces una norma euclídea aditiva δ es el mínimo y es multiplicativa.

Supongamos que D no es un anillo de división;y sea λ el rango de δ. Existe un $a \in R$ y un ordinal σ tal que $\delta(a) = \sigma \geq 1$.

Si para todo $a \in R$, distinto de cero y no invertible, tenemos $\delta(a) = 1$, entonces $\lambda = 2$ y $a^2 = 0$. De lo contrario, $\delta(a^2) = \delta(1) \bigoplus \delta(a) = 2$ de la misma forma $ab = 0$ para todo $a, b \in R$ no nulo y no invertible. En esta situación tenemos que δ es también multiplicativo.

En el caso en el cual existe $a \in R$ tal que $\delta(a) = r > 1$ tenemos la aplicación h del cociente que envía $D^*/_\delta$ a $\mathcal{O}_1 = \{\sigma \mid 1 \leq \sigma \leq \lambda\}$ siendo $a\ _\delta$ y siendo $\delta(a) = \delta(b)$ definidas como $h([a]) = \delta(a)$.

Del mismo modo consideramos $\mathcal{O}_2 = \{\sigma \mid 1 \leq \sigma \leq 2^\lambda\}$. Ambos, $\mathcal{O}_1$ y $\mathcal{O}_2$ son monoides, el primero con la suma natural y el segundo con el producto natural. Además, para cualquier $\tau \in \mathcal{O}_2$, la aplicación $h_\sigma : \sigma \longmapsto \tau^\sigma$ es una aplicación monoide de $\mathcal{O}_1$ a $\mathcal{O}_2$ con $h_\tau(1) = \tau$ el cual es constante cuando $\tau = 1$ y uno a uno en otro caso (estrictamente creciente o isótona).

En particular, la composición $\delta_\sigma : D^*/_\delta \xrightarrow{h} \mathcal{O}_1 \xrightarrow{h_\tau} \mathcal{O}_2$ verifica que $\delta_\tau(ab) = \delta_{tau}(a) \odot \delta_{tau}(b)$ cuando $ab \neq 0$.

Para mostrar que δ_τ define una norma euclídea cuando $\tau \neq 1$, sea $x, y \in R$, existe $q, r \in R$ de manera que $x = yq + r$. Si $r \neq 0$ entonces $\delta(r) < \delta(y)$ por tanto $\delta_\tau(r) < \delta_\tau(y)$ cuando $r, y \neq 0$. Si $y = 0$ entonces $r = x$ y $\delta(r) < \delta(0) = \delta(y)$. Para finalizar; es suficiente definir $\delta_\tau(0) = Inf\{\gamma \mid \delta_\tau(a) < \gamma,\ a \neq 0\} \leq 2^\lambda$.

Obviamente, $\delta < \delta_\sigma$ porque para cualquier $a \in R^*$ tenemos que $\delta(a) < \tau^{\delta(a)}$.

Bibliografía

[1] A. J. Bevelacqua, *A family of non–euclidean PIDs*, Amer. Math. Montly **123** (2016), 939-939.
Construye dominios, cocientes de anillos de polinomios, que son DIP y no son DE. Un ejemplo es $\mathbb{R}[X,Y]/(X^2+Y^2+1)$.

[2] P. L. Clark, *A note on euclidean order types*, Order **32** (2015), 157–178.
Estudia anillos euclídeos en relación con ordinales.

[3] C. J. Conidis, *Higher euclidean domains*, College of Staten Island (2015).
Construye dominios euclídeos de rango infinito arbitrario, basado en la teoria de anillos euclídeos de Samuel y extendiendo resultados de Hiblot.

[4] C. J. Conidis, P. P. Nielsen and V. Tombs, *Transfinitely valued euclidean domains have arbitrary indecomposable order type*, arXiv:1703.02631v2 (2018). Comm. Algebra **47(3)** (2019), 1105–1113.
Nueva exposición de [3].

[5] J. J. Hiblot, *Des anneaux euclidiens dont le plus petit algorithme nest pas valeurs finies*, C.R. des Sciences A **281** (1975), 411–414.
Construye, basado en la teoria de anillos euclídeos de Samuel, dominios euclídeos de rango ω^2.

[6] M. Harper, $\mathbb{Z}[\sqrt{14}]$ is euclidean. Canad. J. Math. **56(1)** (2004), 55–70.
Prueba que $\mathbb{Z}[\sqrt{14}]$ *es un DE mediante una modificación de la construcción de Motzkin.*

[7] N. Jacobson, Basic Algebra I, Freeman, (1985).
En él aparece la teoría básica sobre dominios de integridad.

[8] A. V. Jategaonkar, *Rings with transfinite left division algorithm*, Bul. Amer. Math. Soc. **75** (1969), 559–561.
Estudia el caso no conmutativo.

[9] P. Jara, Notas de trabajo 14. Álgebra conmutaiva. Álgebra conmutativa avanzada, Granada, (2018).
Se estudian ordinales y anillos euclídeos con valores en ordinales.

[10] M. A. Jodeit, *Uniqueness in the divisioin algorithm*, Amer. Math. Monthly **74(7)** (1967), 835–836.
Prueba que un DE tiene resto de la división único si, y sólo si, es un cuerpo o un anillo de polinomios con coeficientes en un cuerpo.

[11] F. Lemmermeyer, *The euclidean algorithm in algebraic number fields*, Expo. Math. **13** (1995), 385–416.
Una de las finalidades de la introducción del algoritmo de la división es poder realizar el cálculo del máximo conmún divisor de dos números y en consecuencia estudiar la factorización en elementos irreducibles o en elementos primos, y es en los anillos de enteros algebraicos en donde podemos obtener gran número de ejemplos. En estos anillos el primer candidato a función euclídea es la norma; por esto tiene sentido si se pueden caracterizar los anillos de enteros algebraicos para los que la norma es una función euclídea; también aquellos otros anillos para los que existe una función euclídea diferente de la norma. Se prueba que para números positivos, sólo para $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ *el anillo de enteros de la extensión* $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ *verifica que la norma es una función euclídea. Por ejemplo, en el anilo de enteros de la extensión* $\mathbb{Q}(\sqrt{14})/\mathbb{Q}$ *la norma no es una función euclídea, pero existe una función euclídea ya que es un DE.*

[12] H. L. Lenstra, Lectures on Euclidean Rings, University of Bielefeld (1974).
Buena y anema exposición de la teoría de anillos euclídeos de Samuel. Estudia el caso de módulos.

[13] J. Liu and M. Chen, *Euclidean modules*, Math. Notes **95(6)** (2014), 937–946.
Estudia módulos euclídeos.

[14] T. Motzkin, *The euclidean algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
Construye el algoritmo euclídeo minimal de un anillo euclídeo; lo que entre otros permite probar que ciertos anillo no son euclídeos.

[15] P. Samuel, About euclidean rings, J. Algebra **19** (1971), 282–301.
Inicia el estudio de anillos euclídeos utilizando ordinales.

[16] J. C. Wilson, *A principal ideal ring that is not a euclidean ring*, Math. Magazine **46(1)** (1973), 34–38.
Utilizando la construcción de Motzkin se prueba que el anillo $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ *es un DIP y no es un DE.*

[17] K. S. Williams, *Note on non–euclidean principal ideal domains*, Math. Magazine (1975), 176–177
Prueba que los únicos anillos de enteros algebraicos de $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$ *que son DIP y no son DE se obtienen para* $d = 19, 43, 67$ *y 163. Por otro lado los únicos que son DE se obtienen para* $d = 1, 2, 3, 7$ *y 11.*