portada.pdf

II

Índice general

Prefacio

Estas notas cumplen un doble propósito: ser de ayuda a cualquier infortunado que se tope con ellas y servir como material de estudio a su autor.

Comenzando como una introducción a la teoría de Anillos, basado en el curso que se dicta en la USB[1], estas notas han ido creciendo hasta convertirse en lo que son hoy: una introducción al álgebra abstracta, desde los conceptos más básicos de la teoría de conjuntos y relaciones hasta la teoría de anillos.

Los prerrequisitos para leer el texto, siendo este una introducción, son mínimos. Dicho esto, no vendría mal haber visto alguna vez un poco de matemáticas 'abstractas' o 'rigurosas': como los argumentos de 'epsilon-delta' que se dan en un curso usual de cálculo, o las demostraciones axiomáticas típicas de un curso sobre geometría euclídea. En cualquier caso, lo anterior no es en absoluto un requisito por lo que el lector que no esté acostumbrado a estos temas no debe temer: este libro también es para el.

Se podrán encontrar una variedad de ejercicios de distintas fuentes, los de ellos que estén resueltos, lo están con la intención de que el lector los intente por su cuenta antes de ver la resolución propuesta. Evidentemente las respuestas dadas no serán las mas elegantes, en cuyo caso se insta al lector a enviar aquellas resoluciones que el o ella[2] considere mejores que las aquí presentes, al correo `jalb97@gmail.com`. Por último, las referencias podrán encontrarse al final del texto.

Los comentarios en el texto estarán en este formato. El lector es libre de ignorarlos, a veces serán referencias históricas, otras veces sugerencias.

[1] Universidad Simón Bolívar.

[2] O como el lector prefiera identificarse, no quiero ser acusado de lógica binaria.

Introducción

Aunque no es estrictamente necesario, sería bueno tener algo de conocimiento sobre la teoría de grupos, en la cual se estudian las propiedades generales de un conjunto con una sola operación binaria.

Nos interesa ahora pensar el caso de las estructuras algebraicas que poseen dos operaciones binarias, sus propiedades y sus aplicaciones. En este sentido, el lector no deberá sorprenderse al ver que comenzamos nuestro estudio de forma análoga al estudio de la teoría de grupos, hablando de subanillos, anillos cocientes, ideales (que son el equivalente de los subgrupos normales) y homomorfismos de anillos. En lo que concierne a la nueva operación binaria introducida, el *producto*, su estudio nos llevará al concepto de Cuerpo y eventualmente a construcciones mas específicas como los cuerpos finitos.

PARTE I

Teoría de Conjuntos

1

Introducción a los Conjuntos

> En matemáticas el arte de hacer preguntas es más valioso que resolver problemas
>
> georg cantor

El concepto central de este capítulo —y pieza fundamental en la matemática moderna— es, al menos en la superficie, tremendamente simple. Un *conjunto* es un agregado de objetos, una colección o grupo de estos objetos. Así, tenemos que la colección de los estudiantes inscritos en la Universidad Simón Bolívar es un conjunto, como también lo es la cantidad de dígitos en la expansión decimal de π.

Los conjuntos son una construcción abstracta, pensada por una cabeza humana, que consiste en agrupar todos los objetos que cumplen con una cierta propiedad. Esta propiedad puede ser en principio cualquiera, aunque más adelante daremos formas precisas de enunciar las propiedades para no caer en ambigüedades. Entonces todos los números que tienen la propiedad de ser múltiplos de dos son un conjunto, como también lo es la colección de todos los hijos que son a la vez sus propios padres (este último conjunto, aparentemente contradictorio, es *vacío*. La noción de vacío se verá mejor más adelante).

Esta noción de conjunto, en principio simple e intuitiva, irá revelando su dificultad a medida que se resuelvan problemas y se avance un poco en los conceptos.

Es interesante notar que, si nos conformamos con la definición que hemos dado hasta ahora y la tomamos como definitiva, pueden surgir contradicciones e inconsistencias. Quizás el ejemplo mas paradigmático es el siguiente, dicho en la versión del mismo que el autor de esta guía escuchó por primera vez.

Ejemplo 1.0.1 (Paradoja de Russel[1]). Existe un pueblo, en una tierra muy lejana, donde trabaja un solo barbero. Pero este barbero tiene una exigencia peculiar a sus clientes: solo afeita a aquellos que no se afeitan a ellos mismos. Todo estaría bien con nuestro barbero si no se nos ocurriese la siguiente pregunta: ¿El barbero se afeita a si mismo?

Veamos. Si el barbero se afeita a si mismo entonces, por la *propiedad* especial que cumple nuestro barbero, se sigue que el barbero no se afeita a si mismo: una contradicción.

De igual forma, si el barbero no se afeita a si mismo entonces el babero sería una persona que no se afeita a si misma y tendríamos, por la condición peculiar de nuestro barbero, que se afeita a si mismo: otra contradicción.

Tenemos que, sin importar que respuesta demos a nuestra pregunta, siempre llegamos a una contradicción: una paradoja. Los sistemas que se comportan de esta forma se suelen llamar *inconsistentes*.

La paradoja de Russel puede formularse formalmente, utilizando notación que no hemos explicado aún, de la siguiente manera: Sea $R = \{x \mid x \notin x\}$ preguntémonos si $R \in R$. Se deja como un ejercicio al lector volver después de la siguiente sección y desarrollar la paradoja de Russel en lenguaje formal.

La lección que se saca de ejemplos como la paradoja de Russel es que el conjunto nombrado no existe y que, en general, ser capaz de nombrar un conjunto no es condición suficiente para asegurar su existencia. Más aún, no tenemos hasta ahora ninguna manera de definir formalmente la noción de conjunto de tal forma que contradicciones como las del ejemplo anterior no ocurran. Por esta razón es que no intentaremos dar una noción mas formal de la idea de conjunto, en cambio daremos unos cuantos *axiomas* que describen bastante bien como esperamos que se comporte un conjunto. Y partiendo de estos axiomas construiremos el resto de nuestra teoría.

Un *axioma* es una verdad que asumiremos sin demostración.

§1.1 PROPIEDADES

En nuestra definición de conjunto aludimos a unas *propiedades* que los elementos del conjunto compartían. Tenemos ahora la tarea de establecer ciertas reglas con las que podamos enunciar estas propiedades, con el fin de evitar ambigüedades.

Las reglas que vamos a explicar son, en esencia, las de la *lógica*. Si se quiere un estudio riguroso de estas reglas será mejor remitirse a un libro de lógica matemática, aquí se hablará de los conceptos de manera informal.

La relación más básica en la teoría de conjuntos es la de *pertenencia*, que denotamos con el símbolo $\in$. La expresión $X \in Y$ se lee 'X pertenece a Y' o 'X es un miembro de Y'.

Las letras X e Y usadas en el párrafo anterior son *variables*, denotan cualquier par de conjuntos. La proposición '$X \in Y$' es verdadera o falsa dependiendo de cuales son los

[1] Bertrand Russel fue un matemático británico del siglo xx que trabajó mucho en el área de filosofía de las matemáticas.

conjuntos X e Y.

Todas las demás propiedades de la teoría de grupos se pueden expresar usando la pertenencia y algunas herramientas lógicas: identidad, conectividad y cuantificadores.

Hay veces en las que conviene expresar el mismo conjunto con variables distintas, la relación de igualdad —o identidad— de conjuntos la denotaremos con el símbolo '$=$'.

Ejemplo 1.1.1. Este ejemplo da varios hechos sobre la igualdad de conjuntos. Sean X, Y y Z tres conjuntos, entonces se cumple que:

1. $X = X$.
2. Si $X = Y$ entonces $Y = X$.
3. Si $X = Y$ y $Y = Z$, entonces $X = Z$.
4. Si $X = Y$ y $X \in Z$ entonces $Y \in Z$.
5. Si $X = Y$ y $Z \in X$ entonces $Z \in Y$.

PARTE II

Teoría de Grupos

PARTE III

Teoría de Anillos

2

Definiciones Básicas y Ejemplos

> Comunmente en las matemáticas el problema crucial es reconocer y descubrir cuales son los conceptos relevantes, una vez hecho esto esta casi la mitad del trabajo listo
>
> i. n. herstein

Nuestro punto de partida, y la pieza central la teoría de anillos, es la siguiente definición.

> Definición 2.0.1 (anillo). Un anillo $\mathcal{A}$ es un conjunto con dos operaciones binarias, $+$ y $\times$ (llamadas suma y producto), que satisface, para todo a, b, c en $\mathcal{A}$,
>
> 1. $(\mathcal{A}, +)$ es un grupo abeliano.
> 2. El producto es asociativo: $(a \times b) \times c = a \times (b \times c)$
> 3. Se cumple la propiedad distributiva:
>
> $$(a + b) \times c = (a \times c) + (b \times c) \quad \text{y,}$$
> $$c \times (a + b) = (c \times a) + (c \times b).$$

Los anillos fueron desarrollados a principios del siglo XIX, aunque no fue hasta el segundo tercio del siglo XX que adquirieron notoriedad. Cabe destacar que, las operaciones suma y producto antes descritas son abstractas, y no son aquellas a las que estamos acostumbrados en, por ejemplo, el conjunto $\mathcal{R}$ de los números reales. Otra acotación importante es que, de acuerdo con la definición anterior, siempre que se hable de un anillo $\mathcal{A}$ deben especificarse las operaciones junto con a las cuales $\mathcal{A}$ forma un anillo. Los momentos en los que se omitan estas operaciones serán solo los casos en que sean evidentes.

Diremos que un anillo $\mathcal{A}$ es *conmutativo* cuando, como cabría esperar, el producto sea conmutativo. Además, si $\mathcal{A}$ posee un elemento 1 tal que $1 \times a = a \times 1 = a$, para todo

$a \in \mathcal{A}$, diremos que $\mathcal{A}$ es unitario.

A partir de ahora, adoptaremos las siguientes convenciones. Sea $\mathcal{A}$ un anillo. El producto $a \times b$ se denotará simplemente como ab, para cuales quiera elementos $a, b \in \mathcal{A}$. La identidad aditiva será denotada por 0 y el inverso aditivo (*opuesto*) de un $a \in \mathcal{A}$ será denotado por $-a$. Estas convenciones son familiares del conjunto $\mathfrak{Z}$ de los enteros.

La condición de que $\mathcal{A}$ sea un grupo bajo la adición es natural, por otro lado, la condición de que sea abeliano puede parecer un poco forzada. Una de la razones principales de que se le pida una condición tan restrictiva es que, si el anillo es unitario, entonces la conmutatividad de la suma se ve *forzada* por la propiedad distributiva.

Para ver esto, se calcula $(1 + 1)(a + b)$ de forma artificiosa. Un anillo $\mathcal{A}$ unitario (con $1 \neq 0$) es llamado de *división* si todo elemento no nulo a de $\mathcal{A}$ posee un inverso multiplicativo, es decir, si para todo $a \in \mathcal{A}$ existe un $b \in \mathcal{A}$ tal que $ab = ba = 1$. Ahora podemos considerar la siguiente definición.

Definición 2.0.2 (cuerpo). Un cuerpo es un anillo de división conmutativo.

Los angloparlantes prefieren la palabra *Campo (Field)* en vez de *Cuerpo*. Es un ejercicio interesante, aunque quizás tedioso, desglosar la definición anterior y darla en función de las propiedades nombradas. A continuación, más ejemplos.

Ejemplo 2.0.1. Los ejemplos más sencillos de anillos son los anillos *triviales* formados tomando cualquier grupo conmutativo $\mathcal{A}$ con el siguiente producto trivial, para todo $a, b \in \mathcal{A}$, $ab = 0$. Es fácil revisar que este $\mathcal{A}$ es un anillo conmutativo. En el caso de que $\mathcal{A} = \{0\}$ se obtiene el *anillo cero*, denotado por $\mathcal{A} = $.

Ejemplo 2.0.2. El conjunto de los enteros, $\mathfrak{Z}$, bajo las operaciones usuales de suma y producto es un anillo conmutativo con identidad, pero *no* un cuerpo. ¿Cuáles son los elementos de $\mathfrak{Z}$ invertibles, es decir, con inverso multiplicativo?

Ejemplo 2.0.3. Los conjuntos $\mathbb{Q}$ y $\mathbb{R}$, de los racionales y los reales, son anillos conmutativos con unidad (¿Son cuerpos?).

Ejemplo 2.0.4. El grupo cociente $\mathfrak{Z}/n\mathfrak{Z}$ es un anillo conmutativo con identidad al usar el producto *módulo n*, de las clases de equivalencia, esto es, el producto de dos elementos es la clase de su multiplicación usual.

Los ejemplos dados hasta ahora han sido todos de anillos conmutativos, los anillos no conmutativos son también un área importante del álgebra, en este sentido se tiene el siguiente ejemplo.

Ejemplo 2.0.5 (Cuarteniones Hamiltonianos). Sea $\mathcal{H}$ el conjunto de los elementos de la

forma $a + bi + cj + dk$, donde $a, b, c, d \in \mathfrak{R}$, con la suma definida 'por componentes':

$$(a + bi+cj + dk) + (a' + b'i + c'j + d'k) = \\ (a + a') + (b + b')i + (c + c')j + (d + d')k$$

y el producto definido expandiendo $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ de acuerdo con la propiedad distributiva. El producto se hace tomando en cuenta que

$$i^2 = j^2 = k^2 = -1$$

junto con las siguientes reglas multiplicativas

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,$$

y que los números reales conmutan con los elementos i, j, k. De las relaciones anteriores es claro que los cuaterniones son en efecto no conmutativos. El lector acostumbrado a la teoría de espacios vectoriales se habrá dado cuenta que los cuaterniones, así definidos, representan un espacio 4-dimensional sobre $\mathfrak{R}$ con los vectores $\{1, i, j, k\}$ como base. El hecho de que los cuaterniones son un anillo se puede ver mediante un chequeo, bastante tedioso, de las propiedades. Nótese que el elemento identidad es $1 + 0i + 0j + 0k$. Más aún, los cuaterniones son un anillo no conmutativo de división, donde el inverso de un elemento —no nulo— viene dado por

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

El álgebra no conmutativa se empezó a desarrollar en el siglo diecinueve de la mano de matemáticos como W. R. Hamilton[1], I. N. Herstein, entre otros. Se pueden obtener ejemplos interesantes de anillos considerando anillos de funciones, como lo muestra el siguiente ejemplo.

Ejemplo 2.0.6. Sea X un conjunto no vació y $\mathcal{A}$ un anillo. La colección, $\mathcal{F}$, de todas las funciones $f\colon X \to \mathcal{A}$ es un anillo con las operaciones usuales:

$$(f + g)(x) = f(x) + g(x) \quad \text{y} \quad (fg)(x) = f(x)g(x).$$

El hecho de que $\mathcal{F}$ sea un anillo se hereda directamente de $\mathcal{A}$. Más aún, $\mathcal{F}$ es conmutativo si, y solo si, $\mathcal{A}$ lo es y $\mathcal{F}$ tiene un 1 si, y solo si, $\mathcal{A}$ tiene un 1 (en cuyo caso el 1 de $\mathcal{F}$ es necesariamente la función constante $f(x) = 1$).

Si X y $\mathcal{A}$ poseen estructuras con mas propiedades, se pueden formar anillos mas complejos. Por ejemplo, si tomamos $\mathcal{A}$ como el anillo de los números reales y tomamos X

[1] Sir William Rowan Hamilton (1805–1865) fue un matemático irlandés conocido por aportes importantes en las áreas de óptica, mecánica clásica y álgebra.

como el intervalo cerrado $[0, 1]$ de $\mathcal{R}$, obtendremos el *anillo de las funciones continuas*, el cual es conmutativo y posee un 1.

Aunque sea tedioso, puede ser útil para el lector verificar todo lo que se afirma en el ejemplo anterior sobre los anillos de funciones. Puede ocurrir también que un anillo no posea identidad.

Ejemplo 2.0.7. El anillo $2\mathcal{Z}$ de los números pares, bajo la multiplicación y la suma usuales, es un anillo conmutativo *sin* identidad.

El siguiente teorema nos dará unas cuantas propiedades de los anillos que son familiares del conjunto $\mathcal{Z}$.

Teorema 2.0.1. Sea A un anillo. Entonces, para todo $a, b \in A$,

1. $0a = a0 = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$
4. Si $1 \in A$ es una identidad, entonces esta identidad es *única* y $-a = -1(a)$

En la siguiente demostración, como en muchas otras, la clave esta en pensar cuidadosamente en las propiedades que poseen los objetos con que estamos trabajando. Por ejemplo, para probar (2), se quiere ver que ese elemento actúa como inverso aditivo de (ab).

Demostración. El teorema se sigue de la propiedad distributiva y de la ley de cancelación (considerando a A como un grupo aditivo). Veamos cada una, para todo $a, b \in A$,

1. $0a = (0+0)a = 0a + 0a$ de donde, por la ley de cancelación, $0a = 0$. Igualmente para $a0 = 0$.
2. Primero, $ab + (-a)b = (a + (-a))b = 0b = 0$ y por otro lado $ab + a(-b) = a(b + (-b)) = a0 = 0$.
3. Por la parte anterior, $(-a)(-b) = -(-ab) = ab$.
4. Supongamos que existe un $1'$ tal que $1'a = a1' = a$ entonces ocurriría que $(1')1 = 1$ y $(1')1 = 1'$, lo cual es imposible, luego solo existe un elemento identidad en A. Por 2, $-a = 1(-a) = (-1)a$.

§ 2.1 DOMINIOS ENTEROS Y DIVISORES DE CERO

A diferencia del conjunto $\mathfrak{Z}$, puede ocurrir que en un anillo existan elementos no nulos a, b tales que $ab = 0$. Esto motiva la siguiente definición.

Definición 2.1.1 (divisor de cero). Sea A un anillo,

1. Un elemento no nulo a de A es un *divisor de cero* si existe un $b \in A$, no nulo, tal que $ab = 0$ o $ba = 0$.
2. Supongamos que A posee una identidad 1, con $1 \neq 0$. Un elemento $v \in A$ es llamado una *unidad* si existe un $w \in A$ tal que, $vw = wv = 1$. El conjunto de las unidades de A se denota por $A^\times$.

Los divisores de cero nos son familiares de las matrices reales. En la terminología de la definición anterior, un anillo A es un cuerpo si todos los elementos no nulos son unidades, o lo que es lo mismo, si $A^\times = A - \{0\}$.

Nótese que un divisor de cero no puede ser una unidad. En efecto, supongamos que $a \in A$ es una unidad tal que existe un $b \in A$, no nulo, para el cual $ab = 0$. Entonces, como a es una unidad, existe un $v \in A$ tal que $va = 1$, de donde se sigue que $b = 1b = (va)b = v(ab) = 0$, lo cual es una contradicción. Lo mismo ocurre si $ba = 0$. Una consecuencia de esto es que *en un cuerpo no hay divisores de cero.*

Continuamos con ejemplos, esta vez sobre divisores de cero y unidades.

Ejemplo 2.1.1. El anillo $\mathfrak{Z}$ de los enteros no posee divisores de cero, y sus únicas unidades son ± 1, es decir, $\mathfrak{Z}^\times = \{-1, 1\}$.

Ejemplo 2.1.2. Si A es el anillo de todas las funciones que van del intervalo cerrado $[0, 1]$ a $\mathfrak{R}$ entonces sus unidades son todas las funciones que no se anulan en ningun punto (para esta clase de funciones su inverso viene dado por $1/f$). Si f no es una unidad y tampoco se anula, entonces f es un divisor de cero. Esto se debe a que podemos definir la siguiente

$$g(x) = \begin{cases} 0 & \text{si } f(x) \neq 0 \\ 1 & \text{si } f(x) = 0 \end{cases}$$

que no se anula, sin embargo, $f(x)g(x) = 0$ para todo x.

Siempre que se quiera que una función cumpla un papel específico, y no se le ocurra ninguna ¡defínala por partes! A los anillos que se parecen mucho a los enteros se les da un nombre especial.

Definición 2.1.2 (dominio entero). Un anillo conmutativo con identidad es un dominio entero si no posee divisores de cero.

El hecho de que no existan divisores de cero hace que los dominios enteros posean una ley de cancelación, como explica el siguiente teorema.

Teorema 2.1.1. Supongamos que a, b y c son elementos de un anillo y que a no es un divisor de cero. Si $ab = ac$ entonces se tiene que $a = 0$ o $b = c$.

Demostración. Si $ab = ac$ entonces $a(b - c) = 0$ de donde se sigue que $a = 0$ o $b - c = 0$.

Corolario 2.1.1.1. Todo dominio entero finito es un cuerpo.

Demostración. Sea A un dominio entero finito y sea a un elemento, no nulo, de A. La función $f: A \to A$ definida por $f(x) = ax$ es inyectiva, debido a la ley de cancelación. Como A es finito esta función es sobreyectiva. En particular, existe un $b \in A$ tal que $ab = 1$, es decir, a es una unidad en A. Como lo anterior es cierto para *cualquier* $a \in A$, se sigue que A es un cuerpo.

§2.2 SUBANILLOS

Es natural considerar la noción de *subanillo*.

Definición 2.2.1 (subanillo). Un subanillo, de un anillo A, es un subgrupo de A que es cerrado bajo el producto.

También se puede pensar que un subanillo es un subconjunto que tiene el también estructura de anillo. De la definición anterior se sigue que, para mostrar que un conjunto es un subanillo, hace falta ver que es *no vacío* y *cerrado bajo la diferencia y el producto*.

Continuamos con más ejemplos, esta vez de subanillos.

Ejemplo 2.2.1. $\mathfrak{Z}$ es un subanillo de $\mathbb{Q}$ y $\mathbb{Q}$ es un subanillo de $\mathfrak{R}$. La propiedad 'ser un un subanillo de' es claramente transitiva.

Ejemplo 2.2.2. $2\mathfrak{Z}$ es un subanillo de $\mathfrak{Z}$, de la misma forma, $n\mathfrak{Z}$ es un subanillo de $\mathfrak{Z}$ para todo n.

Es un ejercicio rápido verificar el ejemplo anterior

Ejemplo 2.2.3. El anillo de todas las funciones continuas de $\mathfrak{R}$ en $\mathfrak{R}$ es un subanillo del anillo de las funciones de $\mathfrak{R}$ en $\mathfrak{R}$. El anillo de las funciones *diferenciables* es un subanillo de los dos.

Ejemplo 2.2.4. Los *cuaterniones enteros*, es decir, los elementos de la forma $a + bi +$

$cj + dk$ con $a, b, c, d \in \mathfrak{Z}$, son un subanillo de los cuaterniones reales o racionales.

Las subestructuras son muy comunes en el álgebra. El lector podrá pensar en muchos ejemplos, como los subgrupos o los subespacios.

Ejemplo 2.2.5. Si A es un subanillo, de un cuerpo C, que contiene a la identidad de C, entonces A es un dominio entero. El converso también es cierto, todo dominio entero esta contenido en un cuerpo.

§2.3 POTENCIAS Y MÚLTIPLOS

Las nociones de múltiplo y de potencias a las que estamos acostumbrados tienen una generalización natural en los anillos.

Sea a un elemento de un anillo A y $n \in \mathcal{N}$. Entonces la *enésima potencia* de a, a^n, se define mediante las condiciones inductivas

$$a^1 = a \quad \text{y} \quad a^n = a^{n-1}a$$

de esto las reglas usuales se los exponentes se siguen directamente:

$$a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad (n, m \in \mathcal{N}).$$

Nótese que si dos elementos, a, b, conmutan, entonces sus potencias también lo hacen y $(ab)^n = a^n b^n$.

En el caso de que A sea unitario y a^{-1} exista, se pueden considerar *potencias negativas* de a definidas mediante la siguiente expresión

$$a^{-n} = (-a)^n,$$

que junto con la definición de $a^0 = 1$, nos dan una definición de las potencias para todo elemento de $\mathfrak{Z}$.

Consideramos ahora el caso de los múltiplos. Para cada $n \in \mathfrak{Z}$ definimos el *múltiplo enésimo* de a, na, de manera recursiva:

$$1a = a \quad \text{y} \quad na = (n-1)a + a, \quad \text{cuando } n > 1.$$

Si definimos $0a = 0$ y $(-n)a = -(na)$ entonces la definición de múltiplo queda bien definida para cualquier entero. Los múltiplos satisfacen varias identidades fáciles de probar, para $a, b \in A$ y $n, m \in \mathfrak{Z}$:

$$(n+m)a = na + ma, \ (nm)a = n(ma),$$

y

$$n(a+b) = na + nb.$$

Además de estas reglas, hay dos propiedades mas que se siguen de la ley distributiva, estas son,

$$n(ab) = (na)b = a(nb), \quad \text{y} \quad (na)(mb) = (nm)(ab).$$

Es bueno decir que la expresión na no significa el producto en el anillo, es una abreviación de la suma.

§2.4 CARACTERÍSTICA

En los anillos pueden ocurrir cosas extrañas, por ejemplo, podría ocurrir que si $a \in A$ entonces $a + a + \cdots + a = 0$. Esto motiva la siguiente definición.

> Definición 2.4.1 (característica de un anillo). Sea A un anillo. La *característica* de A, denotada por $\operatorname{car} A$, se define como el numero natural mas pequeño tal que $na = 0$ para todo $a \in A$. Si no existe ningún entero que cumpla esa identidad (esto es, si el único entero que lo cumple es $n = 0$), entonces se dice que el anillo A es de *característica cero*.

La definición se ilustra con los siguientes ejemplos,

Ejemplo 2.4.1. Los anillos $\mathfrak{Z}$, $\mathbb{Q}$ y $\mathfrak{R}$ son de característica cero.

Ejemplo 2.4.2. El anillo $\mathfrak{Z}/n\mathfrak{Z}$ es de característica n.

Este ultimo ejemplo también es divertido—y fácil—de verificar. El siguiente teorema nos dice que, si el anillo es unitario, la característica viene completamente determinada por el 1.

> Teorema 2.4.1. Si A es un anillo con identidad, entonces la característica de A es n si, y solo si, $n1 = 0$.
>
> *Demostración.* Si $\operatorname{car} A = n$, entonces en particular se tiene que $n1 = 0$. Si hubiese un $m \in A$, con $0 < m < n$, tal que $m1 = 0$ tendríamos que
>
> $$ma = (m1)a = 0a = 0 \text{ para todo } a \in A.$$
>
> Lo que haría que $\operatorname{car} A < n$, lo cual es imposible. El recíproco se prueba de forma similar.

Terminamos esta sección con un teorema importante que relaciona la característica de un anillo con su estructura multiplicativa.

> Teorema 2.4.2. La característica de un dominio entero o es un numero primo, o es cero.

Demostración. Sea A un anillo con característica n y supongamos que n no es primo. Entonces existe una factorización no trivial $n = n_1 n_2$, con $1 < n_1, n_2 < n$. Se sigue que

$$0 = n1 = (n_1 n_2)1 = (n_1 n_2)1^2 = (n_1 1)(n_2 1).$$

Pero A no tiene divisores de cero, por lo que $n_1 1 = 0$ o $n_2 1 = 0$. Como n_1 y n_2 son ambos menores que n, entramos en contradicción con el hecho de que n es la característica de A. Por lo tanto la característica de A debe ser un numero primo.

§2.5 EJERCICIOS

A continuación hay varios ejercicios resueltos, seguidos por otros que si se dejaran enteramente al lector.

Siempre que no se especifique, A es un anillo.

Ejercicio 2.5.1. Demuestre que $(-1)^2 = 1$ en A.

Solución. Usando el teorema 1.1, se tiene que

$$(-1)^2 = (-1)(-1) = -(-1) = 1.$$

Ejercicio 2.5.2. Demuestre que si u es una unidad en A, entonces $-u$ también lo es.

Solución. Sea $v \in A$ el inverso de u. Entonces $(-u)(-v) = -(-uv) = uv = 1$, de igual forma, $(-v)(-u) = 1$ y $-u$ es una unidad.

Ejercicio 2.5.3. Sea A un anillo con identidad, y S un subanillo de A que contiene a la identidad de A. Demuestre que si u es una unidad en S, entonces también lo es en A.

Solución. Sabemos, por la definición de subanillo, que $S \subset A$. Luego, si $v \in S$ es el inverso de u, se sigue que $v \in A$. Pero como el producto en S es el mismo que en A, se tiene que necesariamente uv en S es lo mismo que uv en A. Pero esto ultimo es lo mismo que decir que u es una unidad en A.

Ejercicio 2.5.4. Demuestre que la intersección de una colección de subanillos, de un anillo dado, es también un subanillo.

Solución. Sea A un anillo cualquiera y sean $\{S_1, \cdots, S_n\}$ subanillos de A. Denotemos por $\bigcap S_i$ la intersección de los S_i con $0 < i \leqslant n$.

Sean $x, y \in \bigcap S_i$, entonces se tiene que $x, y \in S_i$ para todo $0 < i \leqslant n$, y la diferencia $(x - y)$, como todos los S_i son subanillos, esta en cada uno de ellos. Pero esto último es lo mismo que decir que $(x - y) \in \bigcap S_i$.

Sean x, y como antes, por un argumento similar al anterior, es fácil ver que $(xy) \in \bigcap S_i$ para todo $0 < i \leqslant n$. Por las dos condiciones anteriores, $\bigcap S_i$ es un subanillo de A.

Ejercicio 2.5.5. El *centro* de un anillo A es

$$\{z \in A : za = az \text{ para todo } a \in A\},$$

es decir, el conjunto de los elementos de A que conmutan con todos los elementos de A. Demuestre que el centro de un anillo es un subanillo unitario y que el centro de un anillo de división es un cuerpo. AA

Solución. Primero que todo, es evidente que si $1 \in A$ entonces 1 pertenece al centro de A.

Sean x, y en el centro de A y sea a un elemento de A. Entonces se tiene que

$$(x-y)a = xa - ya = ax - ay = a(x-y)$$

y se sigue que $x - y$ pertenece al centro de A. Consideremos ahora el producto (xy),

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

por lo que (xy) pertenece al centro de A.

En el caso de que A sea un anillo de división, entonces el centro de A es un anillo de división conmutativo, es decir, un cuerpo.

Ejercicio 2.5.6. Demuestre que si A es un dominio entero y $x^2 = 1$ para algún $x \in A$, entonces $x = \pm 1$.

Solución. Tenemos que $x^2 = 1$, o lo que es lo mismo, que $x^2 - 1 = 0$. Notemos que

$$(x+1)(x-1) = x^2 - x + x - 1 = x^2 - 1$$

y entonces tenemos que de la igualdad

$$(x+1)(x-1) = 0$$

se sigue que $(x+1) = 0$ o $(x-1) = 0$ debido a que A es un dominio entero. Pero entonces tenemos que $x = 1$ o $x = -1$.

Ejercicio 2.5.7. Demuestre que cualquier subanillo de un cuerpo que contiene a la identidad es un dominio entero.

Solución. Sea C un cuerpo y S un subanillo de C que contiene a la identidad. Sean a, b elementos no nulos de S y supongamos que $ab = 0$. Como a es un elemento de un cuerpo existe su inverso multiplicativo a^{-1} y se sigue que

$$a^{-1}ab = a^{-1}0$$

de donde $b = 0$, lo cual es una contradicción.

Ejercicio 2.5.8. Un elemento $x \in A$ es llamado *nilpotente* si $x^m = 0$ para algún $m \in \mathcal{N}$.

1. Demuestre que si $n = a^k b$, para algunos enteros a, b, entonces $\overline{ab}$ es un elemento nilpotente de $\mathfrak{Z}/n\mathfrak{Z}$.
2. Sea A el anillo de funciones de un conjunto no vacío, X, a un cuerpo C. Demuestre que A no posee elementos nilpotentes distintos de cero.

Solución. Veamos cada parte por separado,

1. Tenemos que

$$\begin{aligned}(\overline{ab})^k &= \overline{(ab)^k} = \overline{(a^k b)(b^{k-1})} \\ &= (\overline{a^k b})(\overline{b^{k-1}}) = \overline{(n)}(\overline{b^{k-1}}) \\ &= 0\overline{b^{k-1}} = 0.\end{aligned}$$

2. Supongamos que existe una $f \in A$, no nula, tal que $f^k = 0$ para algún $k \in \mathcal{N}$. Entonces ocurriría que $f(x)^k = 0$, pero como $f(x)$ es un elemento de C esto es imposible. En un cuerpo no hay elementos nilpotentes, debido a que estos son *siempre divisores de cero* (considérese la ecuación $f(x)f(x)^{k-1} = 0$).

A continuación están los ejercicios no resueltos.

Ejercicio 2.5.9. Describa el centro de $\mathcal{H}$, los cuaterniones Hamiltonianos. Demuestre que $\{a + bi \mid a, b \in \mathcal{R}\}$ es un subanillo de $\mathcal{H}$ que es un cuerpo, pero no esta contenido en el centro de $\mathcal{H}$.

Ejercicio 2.5.10. Para un elemento fijo $a \in A$ definamos $C(a) = \{r \in A \mid ra = ar\}$. Demuestre que $C(a)$ es un subanillo de A que contiene a a. Demuestre que el centro de A es la intersección de los subanillos $C(a)$, para todo $a \in A$.

Ejercicio 2.5.11. Sea A un anillo tal que, para todo $a, b \in A$, $a + b = ab$. Demuestre que A debe ser el anillo trivial, esto es, que $A = 0$.

Ejercicio 2.5.12. Un elemento a de A se llama *idempotente* si $a^2 = a$. Demuestre que un elemento, no nulo, que sea idempotente no puede ser nilpotente[2].

[2]Véase el ejercicio 2.5.8

3

Ideales

> Las matemáticas son el arte de darle
> el mismo nombre a cosas distintas
>
> henri poincaré

En esta sección estudiaremos un tipo de subanillos, llamados ideales, que poseen una mayor cerradura en su estructura multiplicativa.

La palabra *ideal* proviene de los *números ideales* desarrollados por Ernst Kummer

> Definición 3.0.1 (ideal). Sea $\mathfrak{i}$ un subconjunto, no vació, de un anillo $\mathscr{A}$. Entonces $\mathfrak{i}$ es un *ideal a ambos lados* si, y solo si,
>
> $a, b \in \mathfrak{i}$ implica que $a - b \in \mathfrak{i}$
>
> y; $r \in \mathscr{A}$ y $a \in \mathfrak{i}$ implica que los productos ra y ar están en $\mathfrak{i}$

Los ideales fueron propuestos por primera vez en 1876 por Richard Dedekind[1]en la tercera edición de su libro 'Vorlesungen über Zahlentheorie' Si la segunda condición —de la definición anterior— se debilita un poco y pedimos solamente que $ra \in \mathfrak{i}$, obtenemos la noción de un *ideal a la izquierda*. La noción de *ideal a la derecha* se define de forma simétrica.

A partir de ahora adoptaremos la convención de llamar ideal, sin mas, a los ideales a ambos lados.

Antes de continuar, algunos ejemplos:

Ejemplo 3.0.1. Consideremos el anillo $n\mathfrak{Z}$. Es fácil ver que este anillo es un ideal de $\mathfrak{Z}$ (por ejemplo, considere el caso de $2\mathfrak{Z}$, los pares).

Ejemplo 3.0.2. Consideremos el anillo formado por las funciones que van de un conjunto X, no vació, a un anillo $\mathscr{A}$. Entonces el conjunto $\mathfrak{f}_x$, de todas las funciones que se anulan en x, es un ideal.

[1]Dedekind fue un matemático alemán, conocido por sus aportes al álgebra abstracta, la definición de los números reales, la teoría de números algebraica; por nombrar algunos.

En efecto, tomemos f y g en $\mathfrak{f}_x$ y $h\colon X \to \mathscr{A}$ una función. Entonces,

$$(f-g)(x) = f(x) - g(x) = 0 - 0 = 0,$$

y también

$$(fh)(x) = f(x)h(x) = 0h(x) = 0,$$

y, de forma similar, $(hf)(x) = 0$. Y tenemos que $\mathfrak{f}_x$ es un ideal.

§ 3.1 IDEALES PROPIOS

Ejemplo 3.1.1. Los subanillos $\{\}$ y $\mathscr{A}$ son ideales. Un ideal $\mathfrak{i}$ es *propio* cuando $\mathfrak{i} \neq \mathscr{A}$. El ideal $\{0\}$ es llamado el *ideal trivial* y se denota por $\mathfrak{o}$.

Damos ahora un resultado que, aunque parezca simple, sera muy útil más adelante.

> Teorema 3.1.1. Si $\mathfrak{i}$ es un ideal propio (a izquierda o derecha, o ambos) de un anillo unitario $\mathscr{A}$, entonces ningún elemento de $\mathfrak{i}$ posee un inverso multiplicativo, es decir, $\mathfrak{i} \cap \mathscr{A}^{\times} =$.

La idea de la demostración es que, al haber un elemento invertible en I, la cerradura fuerza a que $I = A$.

> *Demostración.* Sea I un ideal de A y supongamos que existe un $a \in I$, no nulo, tal que su inverso a^{-1} existe en A. Como I es cerrado bajo la multiplicación por cualquier elemento de A, se sigue que $aa^{-1} = 1 \in A$. Luego, I contiene a $r = r1$ para todo $r \in A$; es decir, $A \subseteq I$, y tenemos la igualdad $I = A$. Esto contradice el hecho de que I era un ideal propio.

Nótese que también hemos establecido el siguiente corolario.

> Corolario 3.1.1.1. En un anillo con identidad, ningún ideal propio contiene a la identidad.

El siguiente ejemplo, que nos dará una caracterización para todos los ideales del anillo de matrices reales, es muy interesante. Veremos que *este anillo no posee ideales propios*.

El álgebra matricial... ¡Que pesadilla!

Ejemplo 3.1.2. Consideremos el anillo $M_n(\mathfrak{R})$, de matrices $n \times n$ con entradas reales. Sea E_{ij} la matriz, $n \times n$, que tiene 1 en el lugar ij y cero en el resto de lugares. Supongamos que $I \neq \{0\}$ es un ideal de $M_n(\mathfrak{R})$. Entonces I posee al menos una matriz (a_{ij}), con $a_{rs} \neq 0$. Como I es un ideal se tiene que el producto

$$E_{rr}(b_{ij})(a_{ij})E_{ss}$$

es un miembro de I, donde la matriz (b_{ij}) es escogida para tener el elemento a_{rs}^{-1} en su diagonal principal y ceros en todos los demás sitios. Es fácil verificar que este producto es igual a E_{rs}. Teniendo esto en cuenta, la relación

$$E_{ij} = E_{ir}E_{rs}E_{sj} \quad (i, j = 1, 2, \ldots, n)$$

implica que todas la matrices E_{ij}, en total n^2 de ellas, están contenidas en I. La parte crucial es que la matriz identidad, (δ_{ij}), se puede escribir como

$$(\delta_{ij}) = E_{11} + E_{22} + \cdots + E_{nn},$$

de donde se sigue que $(\delta_{ij}) \in I$ y, por el corolario anterior, $I = M_n(\mathfrak{R})$. Así, $M_n(\mathfrak{R})$ no posee ningún ideal propio.

Discutiremos ahora maneras de conseguir ideales nuevos a partir de los que ya tenemos. Para empezar con algo sencillo,

> Teorema 3.1.2. Sea $\{I_i\}$ una colección arbitraria de ideales de un anillo A, donde i toma valores en un índice de A. Entonces $\bigcap I_i$ es también un ideal de A.

¿Será un ideal la $\bigcup I_i$?

> *Demostración.* Por el ejercicio 2.5.4 sabemos que la intersección de los I_i es un subanillo. Queda por ver que pasa con la cerradura bajo el producto.
>
> Sean $x \in \bigcap I_i$ y $a \in A$, entonces el producto $ax \in I_i$ para cada i, puesto que los I_i son ideales de A. Por el mismo argumento $xa \in I_i$ para cada i.

§3.2 IDEAL GENERADO Y PRINCIPAL

Podemos pensar también en el ideal *generado* por un subconjunto de un anillo.

> Definición 3.2.1 (ideal generado). Sea A un anillo y $S \subseteq A$. El ideal generado por S, y denota por $|\mathfrak{s}|$, se define como la intersección de todos los ideales de A que contienen a S.

Al lector acostumbrado al álgebra lineal, le será imposible no pensar en la definición de *subespacio generado*. Notemos que la colección de ideales que contienen a S no es vacía, debido a que el propio anillo A es un ideal que contiene a S. Por el teorema 3.1.2 tenemos que (S) es un ideal. Vale la pena mencionar que, debido a la definición de (S), este es el ideal más pequeño que contiene a S.

Si S es finito, digamos que $S = \{a_1, \ldots, a_n\}$, entonces el ideal generado por S se denota comunmente por $(a_1, \ldots, a_n)$. Un ideal (a) generado por un solo elemento recibe

el nombre de *ideal principal*.

Vale la pena pensar en los ideales laterales generados por un solo elemento de A. El ideal derecho generado por a es llamado un *ideal derecho principal*, denotado por $(a)_r$, y definido como

$$(a)_r = \{ar + na \mid r \in A;\ n \in \mathfrak{Z}\}.$$

Cuando el anillo A es unitario, la definición anterior se reduce a todos los múltiplos a la derecha de a por elementos en A, es decir,

$$(a)_r = aA = \{ar \mid r \in A\}.$$

Es evidente que una construcción análoga a la anterior de puede hacer para definir el *ideal principal izquierdo* $(a)_l$.

Si consideremos ahora al ideal a ambos lados (a), la situación es más complicada. En este caso tenemos que, para todo $r, s \in A$ y $n \in \mathfrak{Z}$,

$$(a) = \{na + ra + as + \sum_{\text{finita}} r_i a s_i\}.$$

En el caso de que A sea unitario, la definición anterior se reduce al conjunto de todas las *sumas finitas* de la forma $\sum r_i a s_i$.

Con todo lo anterior podemos definir un nuevo tipo de anillo.

> Definición 3.2.2 (anillo principal ideal). Una anillo A es un *anillo principal ideal* si cada ideal I de A es de la forma $I = (a)$ para algún $a \in A$

Ejemplos de este tipo de anillo nos los da el siguiente

> Teorema 3.2.1. El anillo $\mathfrak{Z}$ de los enteros es un anillo principal ideal; en efecto, si I es un ideal de $\mathfrak{Z}$, entonces $I = (n)$ para algún entero n no negativo.
>
> *Demostración.* Si $I = 0$ entonces el teorema es trivialmente cierto, pues el ideal 0 es el ideal generado por el elemento $0 \in \mathfrak{Z}$. Suponemos entonces que $I \neq 0$. Ahora, si $m \in I$, entonces $-m$ también, y el conjunto I tiene enteros positivos. Sea n el menor entero positivo en I. Como I es un ideal, cada múltiplo entero de n debe pertenecer a I, y por lo tanto $(a) \subseteq I$.
>
> Para ver la otra inclusión, $I \subseteq (n)$, sea k un elemento arbitrario de I. Por el algoritmo de la división, existen enteros q y r tales que $k = qn + r$, con $0 \leqslant r \leqslant n$. Como k y qn son ambos miembros de I se sigue que $r = k - qn \in I$. Si $r > 0$, tendríamos una contradicción con el hecho de que n es el menor entero positivo de I, por lo tanto $r = 0$ y $k = qn \in (n)$. Se tiene entonces que

solo múltiplos de n pertenecen a I, por lo que $I \subseteq (n)$. La doble inclusión demuestra que $I = (n)$.

§3.3 OPERACIONES CON IDEALES

Consideraremos ahora operaciones binarias con los ideales. Dada una cantidad finita de ideales $I_1, I_2, \ldots, I_n$ de un anillo A, definimos su suma de la forma natural:

$$I_1 + I_2 + \cdots + I_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in I_i\}.$$

Se tiene que $I_1 + I_2 + \cdots + I_n$ es también un ideal (*verifíquese*) y, más aún, es el ideal más pequeño que contiene a todos los I_i.

De una forma mas general, sean los $\{I_i\}$ una colecciones arbitraria, indexada, de ideales de A. Entonces tenemos que la

$$\sum I_i = \left\{ \sum_{\text{finita}} a_i \mid a_i \in I \right\}.$$

Cabe destacar que, aunque $\{I_i\}$ sea una cantidad infinita de ideales, solo se toman *sumas finitas* en la definición anterior.

Podría ocurrir el que caso de que $A = I_1 + I_2 + \cdots + I_n$, entonces ocurriría que, para todo $x \in A$, $x = a_1 + a_2 + \cdots + a_n$ con $a_i \in I_i$. Lo que no se puede garantizar es que esta representación de x sea *única*; para esto, necesitamos la siguiente definición.

> Definición 3.3.1 (suma directa interna). Sean $I_1, I_2, \cdots, I_n$ ideales de A. Llamamos a A la *suma directa interna* de $I_1, I_2, \cdots, I_n$, denotado por $A = I_1 \oplus I_2 \oplus \cdots \oplus I_n$, siempre que
>
> $$A = I_1 + I_2 + \cdots + I_n$$
>
> y
>
> $$I_i \cap (I_1 + I_2 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n) = \{0\}$$
>
> para todo i.

No casualmente esta definición recuerda a su equivalente para espacios vectoriales. El lector familiarizado con la teoría de espacios vectoriales notará que la diferencia esta en la condición 2. Con la definición anterior podemos demostrar el siguiente teorema.

> Teorema 3.3.1. Sean $I_1, I_2, \cdots, I_n$ ideales de A. Las siguientes proposiciones son equivalentes:
>
> 1. A es la suma interna directa de los $I_1, I_2, \cdots, I_n$

2. Cada elemento $x \in A$ se puede expresar de forma única como

$$x = a_1 + a_2 + \cdots + a_n \quad (a_i \in I_i).$$

Si el lector tiene dificultad para seguir esta demostración, haga primero el caso $n = 2$ y de allí verá como es el caso general.

Demostración. Empecemos asumiendo que se cumple 1, es decir, que $A = I_1 \oplus I_2 \oplus \cdots \oplus I_n$. Supongamos que x posee 2 representaciones,

$$x = a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n$$

donde $a_i, b_i \in I_i$. Entonces de esta igualdad se sigue que

$$a_1 - b_1 = (a_2 - b_2) + (a_3 - b_3) + \cdots + (a_n - b_n)$$

pero el lado izquierdo de la igualdad es un elemento en I_1 mientras que el lado derecho es un elemento en $I_2 + I_3 + \cdots + I_n$. Osea que ambos lados pertenecen a $I_1 \cap (I_2 + I_3 + \cdots + I_n) = 0$, de donde se sigue que $a_1 - b_1 = 0$. De forma análoga tenemos que

$$a_2 - b_2 = (a_1 - b_1) + (a_3 - b_3) + (a_4 - b_4) + \cdots + (a_n - b_n)$$

y, por lo mismo que antes, ambos lados de la igualdad pertenecen a $I_2 \cap (I_1 + I_3 + I_4 + \cdots + I_n) = 0$ y entonces $a_2 - b_2 = 0$.

Repitiendo este argumento n veces obtenemos

$$a_1 - b_1 = a_2 - b_2 = \cdots = a_n - b_n = 0$$

de donde se sigue, claramente,

$$a_1 = b_1,\ a_2 = b_2,\ \cdots,\ a_n = b_n$$

y queda demostrado que x posee una representación única.

Asumamos ahora que se cumple 2, es decir, que x se escribe de forma única con respecto a los $I_1, I_2, \cdots, I_n$. Supongamos que

$$x \in \{I_i \cap (I_1 + I_2 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n)\}$$

para algún $1 \leqslant i \leqslant n$. Entonces podemos expresar a x de dos formas distintas, a saber, $x = 0 + \cdots + x + \cdots + 0$ donde x esta en la posición i, y $x = x + 0 + \cdots + 0$ donde x esta en cualquier posición que no sea i. Como la representación de x es única, llegamos a la conclusión de que $x = 0$. Por último, como el argumento anterior se hizo para todo $1 \leqslant i \leqslant n$, tenemos

que

$$I_i \cap (I_1 + I_2 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n) = 0$$

y que $A = I_1 \oplus I_2 \oplus \cdots \oplus I_n$.

Si antes consideramos la suma de ideales, es natural pensar ahora en su *producto*. Supongamos que I y J son ideales de un anillo A, entonces su producto viene definido por

$$IJ = \left\{ \sum_{\text{finita}} a_i b_i \mid a_i \in I, b_i \in J \right\}.$$

De haber definido el producto como la colección, más simple, de productos de la forma ab (con $a \in I$ y $b \in J$) obtendríamos un conjunto que falla en ser un ideal (*¿Por qué?*) Con esta definición IJ es un ideal de A. En efecto, supongamos que $x, y \in IJ$ y $a \in A$; entonces,

$$\begin{aligned} x &= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \\ y &= a'_1 b'_1 + a'_2 b'_2 + \cdots + a'_m b'_m \end{aligned}$$

donde $a_i, a'_i \in I$ y $b_i, b'_i \in J$. De aquí se sigue que

$$\begin{aligned} x - y &= a_1 b_1 + \cdots + a_n b_n + (-a'1) b'_1 + \cdots + (-a'_m) b'_m \\ ax &= (aa_1) b_1 + (aa_2) b_2 + \cdots + (aa_n) b_n. \end{aligned}$$

Como los elementos $-a'_i$ y aa_i necesariamente pertenecen a I, entonces tanto $x - y$ como ax (el caso xa se prueba idénticamente) pertenecen a IJ; lo cual hace de IJ un ideal de A.

No hay dificultad en extender el producto de ideales a una colección finita cualquiera de estos. Sean los $I_1, I_2, \cdots, I_n$ ideales de A, entonces podemos definir su producto, $I_1 I_2 \cdots I_n$, como el conjunto de todas las sumas que tienen como términos $a_1 a_2 \cdots a_n$ con $a_i \in I_i$.

Nótese que, debido a la ley asociativa, la notación $I_1 I_2 \cdots I_n$ no es ambigua. En el caso especial que todos los ideales son iguales, digamos que iguales a I, tenemos la siguiente noción de potencia

$$I^n = \left\{ \sum_{\text{finita}} a_{i1} a_{i2} \cdots a_{in} \mid a_{ik} \in I \right\}.$$

Observación. Si I es un ideal derecho y S es un subconjunto no vacío del anillo A,

entonces

$$SI = \left\{ \sum_{\text{finita}} a_i r_i \mid a_i \in A; r_i \in I \right\}$$

forma un *ideal derecho* de A (*verifíquese*). En particular, si $S = \{a\}$ entonces aI esta dado por

$$aI = \{ar \mid r \in I\}.$$

La última operación de ideales que consideraremos es la de *cociente*, dada por la siguiente

> Definición 3.3.2 (cociente). Sean I y J dos ideales de un anillo A. El *cociente derecho (izquierdo)* de I por J, denotado por $I :_r J$ ($I :_l J$), consiste en todos los elementos $a \in A$ tales que $aJ \subseteq I$ ($Ja \subseteq I$). En el caso de que A sea un anillo conmutativo simplemente escribimos $I : J$.

No es para nada evidente que el cociente de ideales sea un ideal, se deja como ejercicio al lector una demostración de este hecho.

El propósito del siguiente teorema es conectar la definición anterior con las operaciones de suma y producto.

En el siguiente teorema, los subíndices i denotan una colección arbitraria de ideales.

> Teorema 3.3.2. Las siguientes relaciones se cumple para ideales de un anillo A (las letras mayúsculas indican ideales):
>
> 1. $(\cap I_i):_r J = \cap(I_i:_r J)$,
> 2. $I:_r \sum J_i = \cap(I:_r J_i)$,
> 3. $I:_r (JK) = (I:_r K):_r J$.
>
> *Demostración.* En lo que se refiere a la parte (1), tenemos que
>
> $$\begin{aligned}(\cap I_i):_r J &= \{a \in A \mid aJ \subseteq \cap I_i\} \\ &= \{a \in A \mid aJ \subseteq I_i \text{ para todo } i\} \\ &= \cap \{a \in A \mid aJ \subseteq I_i\} \\ &= \cap(I_i:_r J).\end{aligned}$$
>
> Si consideramos ahora la parte (2), nótese que la inclusión $J_i \subseteq \sum J_i$ implica

que $a(\sum J_i) \subseteq I$ si, y solo si, $aJ_i \subseteq I$ para todo i; por lo tanto,

$$\begin{aligned} I:_r \sum J_i &= \left\{a \in A \mid a\left(\sum J_i\right) \subseteq I\right\} \\ &= \{a \in A \mid aJ_i \subseteq I \text{ para todo } i\} \\ &= \cap \{I:_r J_i\}. \end{aligned}$$

Por último, para la parte (3), tenemos que

$$\begin{aligned} I:_r (JK) &= \{a \in A \mid a(JK) \subseteq I\} \\ &= \{a \in A \mid (aJ)K \subseteq I\} \\ &= \{a \in A \mid aJ \subseteq I :_r K\} \\ &= (I_r K):_r J. \end{aligned}$$

Y asi queda demostrado el teorema.

Una observación importante es que, si I es un ideal de A y J un ideal de I, entonces J no es necesariamente un ideal de A. Para ilustrar esto, esta el siguiente ejemplo.

Ejemplo 3.3.1. Consideremos el anillo, A, de las funciones continuas de $\mathscr{R} \to \mathscr{R}$. Consideremos además los conjuntos

$$\begin{aligned} I &= \{fi \mid f \in A \text{ y } f(0) = 0\}, \\ J &= \left\{fi^2 + ni^2 \mid f \in A \text{ y } f(0) = 0 \text{ con } n \in \mathfrak{Z}\right\} \end{aligned}$$

donde i es la función identidad. Un calculo rutinario prueba que J es un ideal de I, y este, a su vez, es un ideal de A. Sin embargo, J *no* es un ideal de A debido a que, mientras que $i^2 \in J$, $\frac{1}{2}i^2 \notin J$. El lector podrá verificar esto último.

§3.4 ANILLO REGULAR

Una condición que nos asegurará que casos como el del ejemplo anterior no ocurran es la de un *anillo regular* dada por la siguiente definición.

> Definición 3.4.1 (anillo regular). Un anillo A es regular si, para cada elemento $a \in A$, existe un $a' \in A$ tal que $aa'a = a$.

La noción de anillo regular se la debemos a Von Neumann[2]. En el caso de que el elemento a posea un inverso multiplicativo, entonces la condición de regularidad se satisface

[2]Von Neumann fue un matemático Americano-Húngaro, conocido por sus aportes en diversos campos de la física, las matemáticas y la computación (A jack of all trades, master of *all*).

haciendo $a' = a^{-1}$. En el caso de que A sea conmutativo la condición de regularidad se convierte en $a^2a' = a$. A a' se le llama tambien *pseudoinversa* El siguiente teorema nos da la "transitividad" en los ideales que buscábamos.

> Teorema 3.4.1. Sea A un anillo regular e I un ideal de A. Entonces cualquier ideal J de I es también un ideal de A.
>
> *Demostración.* Para comenzar, nótese que el propio I es un anillo regular. En efecto, si $a \in I$, entonces $aa'a = a$ para algún $a' \in A$. Hagamos $b = a'aa'$, es claro que b pertenece a I y posee la propiedad de que
>
> $$aba = a(a'aa')a = (aa'a)a'a = aa'a = a.$$
>
> Queremos demostrar que si $a \in J$ y $r \in A$, entonces $ar, ra \in J$. Sabemos que $ar \in I$; entonces, por lo de arriba, existe un $x \in I$ para el cual $arxar = ar$. Como $rxar$ pertenece a I y J es un ideal de I, se sigue que el producto $a(rxar)$ pertenece a J, o lo que es lo mismo, $ar \in J$. Un argumento análogo se usa para probar que $ra \in J$.

Aunque la definición 3.4.1 pueda parecer artificial, se puede usar para demostrar que el conjunto de todas las transformaciones lineales, en un espacio vectorial de dimensión finita sobre un cuerpo, forma un anillo regular. Esta aplicación en si misma seria suficiente para justificar la existencia de la definición.

§3.5 EJERCICIOS

Igual que la sección anterior, primero algunos ejercicios resueltos. Siempre que no se especifique, A es un anillo.

Ejercicio 3.5.1. Si I es un ideal derecho y J es un ideal izquierdo de un anillo A, tales que $I \cap J = \{0\}$, demuestre que $ab = 0$ para todo $a \in I, b \in J$.

Solución. No es muy complicado. Como I es un ideal a la derecha, y podemos considerar a b como un elemento de A, entonces $ab \in I$. De forma análoga, como J es un ideal a la izquierda, y podemos considera a a como un elemento de A, entonces $ab \in J$.

Pero

$$\text{si } ab \in I \text{ y } ab \in J \text{ entonces } ab \in I \cap J,$$

de donde se sigue claramente que $ab = 0$.

Ejercicio 3.5.2. Sea I un ideal de A. Demuestre que el conjunto, $C(I)$, definido por

$$C(I) = \{r \in A \mid (ra - ar) \in I \text{ para todo } a \in A\}.$$

es un subanillo de A.

Solución. Primero que nada, notemos que $C(I) \neq$, debido a que $0 \in C(I)$. Ahora, sean $r_1, r_2 \in C(I)$ queremos ver que $r_1 - r_2 \in C(I)$. Sea $a \in A$, veamos que

$$(r_1 - r_2)a - a(r_1 - r_2) = (r_1a - ar_1) - (r_2a - ar_2)$$

pero como $(r_1a - ar_1) \in I$ y $(r_2a - ar_2) \in I$, su resta también pertenece a I; por lo tanto, $r_1 - r_2 \in C(I)$.

Queremos ver ahora que $r_1r_2 \in C(I)$. Notemos que, si $a \in A$,

$$\begin{aligned}(r_1r_2)a - a(r_1r_2) &= (r_1r_2)a - a(r_1r_2) + r_1ar_2 - r_1ar_2 \\ &= r_1(r_2a) - r_1(ar_2) + (r_1a)r_2 - (ar_1)r_2 \\ &= r_1(r_2a - ar_2) + (r_1a - ar_1)r_2.\end{aligned}$$

Como I es un ideal, y usando el hecho de que $r_1, r_2 \in C(I)$, se tiene que $r_1(r_2a - ar_2) \in I$. De la misma forma $(r_1a - ar_1)r_2 \in I$. Por lo tanto, su suma, $r_1(r_2a - ar_2) + (r_1a - ar_1)r_2$, pertenece a I y $r_1r_2 \in C(I)$.

Ejercicio 3.5.3. Este ejercicio consta de dos partes,

1. Sea A un anillo y sean I, J ideales de A. Demuestre, mediante un ejemplo, que $I \cup J$ puede no ser un ideal de A.

2. Si $\{I_i\}$ $(i = 1, 2, \cdots)$ es una colección de ideales de una anillo A tal que $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, demuestre que $\cup I_i$ es también un ideal de A.

Solución. Veamos cada parte por separado

1. Tomemos el anillo de los enteros. Y consideremos los ideales $I = 2\mathfrak{Z}$ y $J = 3\mathfrak{Z}$. Entonces tenemos que $9 \in \{2\mathfrak{Z} \cup 3\mathfrak{Z}\}$ y $2 \in \{2\mathfrak{Z} \cup 3\mathfrak{Z}\}$, pero claramente $9 - 2 = 7 \notin \{2\mathfrak{Z} \cup 3\mathfrak{Z}\}$. Por lo que $2\mathfrak{Z} \cup 3\mathfrak{Z}$ no es cerrado bajo la diferencia, y no es un ideal.

   En general, la unión falla en ser un ideal por la cerradura bajo la *diferencia*. Nótese que, por otra parte, la unión siempre es cerrada bajo el producto (*¿Por qué?*).

2. Igual que antes, la unión siempre es cerrada bajo el producto. La cerradura bajo la diferencia viene garantizada por las inclusiones. En efecto, si $x, y \in \cup I_i$, se tiene que $x \in I_j$ e $y \in I_k$ con j y k enteros positivos. Si $j = k$ entonces x, y están en el mismo ideal y la cerradura es evidente. Si $j < k$ entonces $I_j \subseteq I_k$ y por lo tanto $x, y \in I_k$ y la cerradura se sigue de que I_k es un ideal. En caso de que $j > k$ se procede de forma análoga. Así, no importa en cual ideal x, y estén, siempre habrá cerradura con respecto a su diferencia. Por lo tanto $\cup I_i$ es un ideal.

   Es interesante considerar como este ejercicio depende el axioma de elección[3]. En el caso finito es claro que no hay ningún problema, pero para el caso infinito necesitamos el axioma de elección para poder asegurar que x, y pertenecen a algún I_i.

Ejercicio 3.5.4. Sea I un ideal izquierdo y J un ideal derecho del anillo A. Considere el conjunto

$$IJ = \left\{ \sum_{\text{finita}} a_i b_i \mid a_i \in I; b_i \in J \right\}.$$

Demuestre que IJ es un ideal *a ambos lados* de A y, siempre que I y J sean ellos mismos ideales *a ambos lados*, que $IJ \subseteq I \cap J$.

Solución. Veamos primero que IJ es un ideal de A. La cerradura bajo la diferencia no es muy complicada de ver ya que, si tanto $\sum a_i b_i$ como $\sum a'_i b'_i$ pertenecen a IJ, entonces

$$\sum a_i b_i - \sum a'_i b'_i = \sum a_i b_i + (-a'_i b'_i).$$

Y como $-a'_i \in I$ y $-b'_i \in J$ se tiene que la suma anterior esta en IJ. Por otro lado, sea

[3] Para una buena explicación del axioma de elección véase el capitulo del libro de Halmos [**naivesethalmos**], o el apéndice del Dummit [**abstractalgebra**].

$r \in A$, y consideremos el producto

$$r \sum a_i b_i = \sum r a_i b_i.$$

Como I es un ideal a la izquierda, el producto $ra_i \in I$, y se tiene que la suma anterior pertenece a IJ. Es claro que el caso simétrico, de $a_i b_i r$, se hace de forma análoga.

Supongamos ahora que I, J son ideales a ambos lados y consideremos el producto $a_i b_i$. Como I es un ideal, y podemos considerar a b_i como un elemento de A, tenemos que $a_i b_i \in I$. Por un razonamiento similar, se tiene que $a_i b_i \in J$. Luego $a_i b_i \in I \cap J$. Más aún, como $I \cap J$ es un ideal[4], cualquier suma finita de $a_i b_i$ pertenece a $I \cap J$. Pero esto último es lo mismo que decir que todo elemento de IJ pertenece a $I \cap J$, o, que $IJ \subseteq I \cap J$.

Ahora, algunos ejercicios no resueltos.

Ejercicio 3.5.5. Diga cual de los siguientes son ideales del anillo $\mathfrak{Z} \times \mathfrak{Z}$.

1. $\{(a, a) \mid a \in \mathfrak{Z}\}$
2. $\{(2a, 2b) \mid a, b \in \mathfrak{Z}\}$
3. $\{(2a, 0) \mid a \in \mathfrak{Z}\}$
4. $\{(a, -a) \mid a \in \mathfrak{Z}\}$

[4]Véase el teorema 3.1.2

§ 3.6 HOMOMORFISMOS DE ANILLOS

> Si la gente no cree que las matemáticas son simples, es solo porque no se dan cuenta de lo complicada que es la vida.
>
> john von neumann

En esta sección nos ocuparemos de funciones que van de un anillo en otro. En particular nos interesaran las funciones, llamadas *homomorfismos*, que preservan las operaciones.

> Definición 3.6.1 (homomorfismo). Sean A y A' dos anillos. Un *homomorfismo* es una función $f\colon A \to A'$ tal que
>
> $$f(a+b) = f(a) + f(b) \quad \text{y} \quad f(ab) = f(a)f(b)$$
>
> para todo $a, b \in A$. Un homomorfismo biyectivo es un *isomorfismo*.

La palabra homomorfismo viene del griego, "homo-morfos" que significa "misma forma". Es importante notar que, en la definición anterior, las operaciones en el lado derecho de las igualdades son las de A', mientras que las del lado izquierdo son las de A, a pesar de que usemos el mismo símbolo para denotarlas.

Si f es un homomorfismo de anillos, la imagen de f, $f(A)$, es la *imagen homomórfica* de A. En el caso de que f sea un homomorfismo de un anillo en si mismo, le llamaremos *endomorfismo*; si además f es biyectiva le llamaremos *automorfismo*.

Adoptaremos la convención de llamar al conjunto de todos los homomorfismos de A en A' como $\hom(A, A')$. En el caso de que $A = A'$ usaremos la notación $\hom(A)$.

A continuación están unos ejemplos sencillos que ayudan a ilustrar la definición anterior.

Ejemplo 3.6.1. Sea A y A' dos anillos cuales quiera y $f\colon A \to A'$ la función que envía a todo elemento de A al 0 de A'. Entonces, para todo $a, b \in A$,

$$f(a+b) = 0 = 0 + 0 = f(a) + f(b)$$

y

$$f(ab) = 0 = 00 = f(a)f(b).$$

Entonces f es un homomorfismo. Esta f, llamada el *homomorfismo trivial*, es la única

función constante que satisface la definición 3.6.1 (*¿Por qué?*).

Ejemplo 3.6.2. Consideremos los anillos $\mathfrak{Z}$ y $\mathfrak{Z}/n\mathfrak{Z}$. Definimos $f\colon \mathfrak{Z} \to \mathfrak{Z}/n\mathfrak{Z}$ mediante $f(a) = \overline{a}$; es decir, f es la función que asigna a cada entero su clase de equivalencia. El que f es un homomorfismo es consecuencia directa de la definición de las operaciones en $\mathfrak{Z}/n\mathfrak{Z}$ (*Verifíquese*).

Ejemplo 3.6.3. Consideremos el anillo de funciones de un conjunto X a un anillo A. Definamos ϕ_a como la función dada por $\phi_a(f) = f(a)$, donde $f\colon X \to A$. Entonces ϕ_a es un homomorfismo. En efecto, nótese que

$$\begin{aligned}\phi_a(f+g) &= (f+g)(a)\\ &= f(a)+g(a)\\ &= \phi_a(f)+\phi_a(g),\end{aligned}$$

y

$$\begin{aligned}\phi_a(fg) &= (fg)(a)\\ &= f(a)g(a)\\ &= \phi_a(f)\phi_a(g).\end{aligned}$$

§ 3.6.1 Propiedades de los homomorfismos

El siguiente teorema nos da de forma mas explícita las características estructurales que preserva un homomorfismo.

> Teorema 3.6.1. Sea $f\colon A \to A'$ un homomorfismo de anillos. Entonces f preserva los *elementos distinguidos*; es decir, se cumple que
>
> $$f(0) = 0 \quad \text{y} \quad f(-a) = -f(a)$$
>
> y, en el caso de que f sea *sobreyectiva* y tanto A como A' sean unitarios, también se cumple que
>
> $$f(1) = 1 \quad \text{y} \quad f(a^{-1}) = f(a)^{-1}$$
>
> para cualquier elemento invertible a de A.
>
> *Demostración.* Veamos cada parte por separado.
>
> 1. Veamos que $f(0) = f(0+0) = f(0) + f(0)$ de donde se sigue que $f(0) = 0$.
> 2. Tenemos que $f(a) + f(-a) = f(a-a) = f(0) = 0$ por lo que $f(-a) = -f(a)$.

3. Sea $a \in A$ tal que $f(a) = 1$; entonces, $f(1) = f(a)f(1) = f(a1) = f(a) = 1$.
4. La ecuación $f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1$ implica $f(a)^{-1} = f(a^{-1})$.

Y asi queda demostrado el teorema.

Vale la pena comentar dos cosas sobre la parte (3) del teorema anterior. Primero, es evidente que

$$f(a)1 = f(a) = f(a1) = f(a)f(1)$$

para todo $a \in A$. Teniendo esto en cuenta uno podría apelar (incorrectamente) a la ley de cancelación para decir que $f(1) = 1$; lo que en realidad se necesita es el hecho de que las identidades multiplicativas son únicas. Segundo, si f no es sobreyectiva, entonces solo podemos asegurar que $f(1)$ es el neutro de $f(A)$. En este caso, el elemento $f(1)$ puede no ser una identidad de A, en efecto, podría ocurrir que $f(1) \neq 1$.

El siguiente teorema indica la estructura algebraica de las imágenes directas bajo homomorfismos. Veremos, entre otras cosas, que si f es un homomorfismo de A en A', entonces $f(A)$ es un subanillo de A'.

Teorema 3.6.2. Sea f un homomorfismo de A en A'. Entonces,

1. para cada subanillo S de A, $f(S)$ es un subanillo de A'; y
2. para cada subanillo S' de R'; $f^{-1}(S')$ es un subanillo de A.

Demostración. Veamos cada parte por separado.

1. Sean $f(a)$ y $f(b)$ en $f(S)$. Luego, tanto a como b pertenecen a S, de la misma forma que $a - b$ y ab (Pues S es un subanillo). Por lo tanto

   $$f(a) - f(b) = f(a - b) \in f(S)$$

   y

   $$f(a)f(b) = f(ab) \in f(S).$$

   Por lo que $f(S)$ es un subanillo de A'.
2. Sean a y b en $f^{-1}(S')$, entonces $f(a), f(b) \in S'$. Como S' es un subanillo, se sigue que

   $$f(a - b) = f(a) - f(b) \in S'$$

y

$$f(ab) = f(a)f(b) \in S'.$$

Lo anterior significa que $a - b$ y ab pertenecen a $f^{-1}(S)$, por lo que $f^{-1}(S)$ forma un subanillo.

Es interesante considerar que ocurre si, en el teorema 3.6.2, cambiamos la palabra "subanillo" por "ideal". En este sentido, sea I un ideal de A', $a' \in f^{-1}(I)$ y r un elemento de A; entonces $f(ra') = f(r)f(a') \in I$ de donde se sigue que ra' esta en la imagen inversa, $f^{-1}(I)$, de I. Como podemos hacer lo mismo para $a'r$, es fácil ver que la condición 2 del teorema anterior se cumple para el caso de los ideales.

Lo que no se puede garantizar, sin mayores restricciones, es la parte 1. Piénsese por ejemplo que, en general, si I es un ideal de A entonces necesitaríamos que, para todo $a' \in A'$, $a'f(a) \in f(S)$ con $a \in A$. Pero, como no hemos pedido que f sea *sobreyectiva*, no podemos garantizar que existe un $x \in A$ tal que $f(x) = a'$ y poder entonces utilizar el hecho de que I es un ideal. Podemos resumir la discusión anterior en el siguiente corolario.

> Corolario 3.6.2.1. Sea $f\colon A \to A'$ un homomorfismo de anillos. Entonces, para cada ideal I' de A' se tiene que $f^{-1}(I')$ es un ideal de A. Si además pedimos que f sea sobreyectiva, entonces —para cada ideal I de A— tenemos que $f(I)$ es un ideal de A'.

§3.6.2 Núcleo de un homomorfismo

Los elementos que un homomorfismo de anillos manda al cero son de especial interés, en este sentido se tiene la siguiente definición.

> Definición 3.6.2 (núcleo). Sea $f\colon A \to A'$ un homomorfismo de anillos. El *núcleo* de f, denotado por $\ker f$, consiste de todos los $a \in A$ tales que $f(a) = 0$.

El núcleo de un homomorfismo no es vació puesto que, como habíamos visto antes, $f(0) = 0$. Más aún, el núcleo de f es un ideal de A; como lo explica el siguiente teorema.

> Teorema 3.6.3. Sea $f\colon A \to A'$ un homomorfismo de anillos, entonces el núcleo de f es un ideal de A.
>
> *Demostración.* Como $\ker f = f^{-1}(0)$, y el $\{0\}$ es un ideal de A', el teorema se sigue directamente del corolario anterior.

Se puede pensar en el núcleo de un homomorfismo como una suerte de medidor que nos da una idea de cuanto hace falta para que nuestro homomorfismo sea un isomorfismo, o en otras palabras, de que le hace falta para ser *inyectivo*.

Teorema 3.6.4. Un homomorfismo de anillos $f\colon A \to A'$, sobreyectivo, es un isomorfismo —es decir, inyectivo— si, y solo si, $\ker f = 0$.

Demostración. Si $f\colon A \to A'$ es un isomorfismo de anillos, entonces $f(a) = 0 = f(0)$ implica que $a = 0$ y es claro que $\ker f = 0$. Por otro lado, consideremos un homomorfismo de anillos sobreyectivo, f, tal que $\ker f = 0$; entonces, para todo $a, b \in A$, $f(a) = f(b)$ implica que $f(a)-f(b) = f(a-b) = 0$, y como $\ker f = 0$, se tiene que $a - b = 0$ o, lo que es lo mismo, que $a = b$.

§ 3.6.3 Isomorfismos de anillos

Dos anillos, A y A', son isomorfos si existe un isomorfismo entre ellos; denotaremos esta relación con $A \simeq A'$. Cabe destacar que, si f es un isomorfismo, entonces f^{-1} también lo es; y la relación $\simeq$ es reflexiva.

La intuición que uno posee de dos anillos isomorfos es que ambos tienen la misma estructura —en cierto sentido son iguales—aunque los nombres que les ponemos a los elementos y las operaciones de cada anillo sean distintas.

Para ilustrar lo anterior, esta el siguiente ejemplo.

Ejemplo 3.6.4. Consideremos un anillo unitario A y la función $f\colon \mathfrak{Z} \to A$ dada por $f(n) = n1$. Veamos que, si $n, m \in \mathfrak{Z}$,

$$f(n + m) = (n + m)1 = n1 + m1 = f(n) + f(m)$$

y

$$f(nm) = (nm)1 = (n1)(m1) = f(n)f(m),$$

por lo que f es un homomorfismo.

Como el núcleo de f es un ideal de $\mathfrak{Z}$ —que es un anillo principal ideal— se sigue que

$$\ker f = \{n \in \mathfrak{Z} \mid n1 = 0\} = (p)$$

para algún p primo, no negativo. No es difícil ver que p es precisamente la característica de A. Entonces, si A es de característica cero, el anillo A posee un subanillo isomorfo a los naturales.

§ 3.6.4 Imágenes homomórficas de ideales

Hemos visto que siempre que f —un homomorfismo de anillos— sea sobreyectiva entonces cada ideal del dominio es un ideal en la imagen. Nos gustaría llegar a la conclusión de que los ideales en el dominio y rango de f están en correspondencia uno a uno. Lamentablemente, esto último en general no es cierto.

El problema esta en que, si I, J son ideales de A tales que $I \subseteq J \subseteq I + \ker f$ entonces $f(I) = f(J)$. Y dos ideales distintos tendrían imágenes iguales.

Para ver esto, considere $f(I) \subseteq f(J) \subseteq f(I + \ker f) = f(I) + 0 = f(I)$ Para remediar el problema anterior tenemos dos opciones. La primera es pedir que $\ker f = 0$ y la segunda es considerar solo los ideales que contienen al núcleo; en cualquiera de los dos casos tendríamos que $I \subseteq J \subseteq I + \ker f = I$, y por lo tanto $I = J$. La primera de las opciones lo único que hace es convertir f en un isomorfismo, en cuyo caso no es sorprendente que los ideales de los dos anillos se hallen en correspondencia uno a uno. La segunda opción es la idea central del teorema mas importante de esta sección, pero antes de el, un lema que nos será necesario.

> Lema 3.6.1. Sea $f\colon A \to A'$ un homomorfismo de anillos sobreyectivo. Si I es un ideal de A tal que $\ker f \subseteq I$, entonces $I = f^{-1}(f(I))$.
>
> *Demostración.* Primero que nada, notemos que $I \subseteq f^{-1}f(I)$ es siempre cierto, pues si $a \in I$ entonces $f(a) \in f(I)$.
>
> Sea $a \in f^{-1}(f(I))$, entonces $f(a) \in f(I)$ por definición. Como f es sobreyectiva, ha de existir un $r \in I$ tal que $f(a) = f(r)$; pero entonces $f(a - r) = 0$ por lo que $a - r \in \ker f$ que por hipótesis es un subconjunto de I. Esto último implica que $a \in I$ y que $f^{-1}(f(I)) \subseteq I$.

Ahora, el teorema prometido.

> Teorema 3.6.5 (de correspondencia). Sean A y A' anillos y $f\colon A \to A'$ un homomorfismo sobreyectivo. Entonces hay una correspondencia uno-a-uno entre los ideales de A que contienen al núcleo y los ideales de A'. Más específicamente, si $I \in A$ es un ideal, y $\ker f \subseteq I$; entonces la correspondencia viene dada por $f(I) = I'$ con I' un ideal de A'.
>
> *Demostración.* Veremos primero que la correspondencia dada es en efecto sobreyectiva. Es decir, queremos producir—dado un ideal $I' \in A'$—un ideal $I \in A$, con $\ker f \subseteq I$, tal que $f(I) = I'$. Tomemos $I = f^{-1}(I')$. Por el corolario 3.6.2.1 sabemos que este I es un ideal de A, y, como $0 \in I'$,
>
> $$\ker f = f^{-1}(0) \in f^{-1}(I').$$

Como f es sobreyectiva —por hipótesis— entonces

$$f(I) = f^{-1}(f(I')) = I'.$$

Veremos ahora que la correspondencia es inyectiva. Sean I, J ideales de A, con $\ker f \subseteq I$ y $\ker f \subseteq J$, tales que $f(I) = f(J)$. Entonces, por el lema anterior,

$$I = f^{-1}(f(I)) = f^{-1}(f(J)) = J.$$

§ 3.6.5 Ideal incrustado

Para dar el siguiente teorema importante de esta sección, necesitamos la siguiente definición.

Definición 3.6.3 (ideal incrustado). Decimos que un anillo A esta *incrustado* en un anillo A' si existe un subanillo, S', de A' tal que $A \simeq S'$.

Un ejemplo rápido ayudará a ilustrar la definición.

Ejemplo 3.6.5. Consideremos los cuerpos $\mathfrak{R}$ y $\mathfrak{C}$, de los reales y los complejos respectivamente. Entonces la función $f\colon \mathfrak{R} \to \mathfrak{C}$ dada por $f(a) = a + 0i$ es un isomorfismo de $\mathfrak{R}$ a un subanillo de $\mathfrak{C}$. Esta es la extensión clásica de $\mathfrak{R}$ a $\mathfrak{C}$.

El hecho de que f —del ejemplo anterior— es un isomorfismo no es difícil de ver, la inyectividad y la sobreyectividad son evidentes; de igual forma es evidente que preserva sumas y productos. Por otro lado, como $(a - b) + 0i$ y $(ab) + 0i$ están en $\mathfrak{C}$ entonces el conjunto de los complejos con parte imaginaria cero es en efecto un subanillo de $\mathfrak{C}$. En general, si un anillo A esta incrustado en un anillo A' diremos que A' es una *extensión* de A y que A puede *extenderse* a A'. Existen casos interesantes en los que un anillo A se puede extender a otro que tiene propiedades no presentes en A. Como un ejemplo, demostraremos que cualquier anillo puede incrustarse en un anillo con identidad.

Teorema 3.6.6 (de extensión de dorroh). Cualquier anillo puede incrustarse en un anillo unitario.

Demostración. Sea A un anillo y consideremos el producto cartesiano

$$A \times \mathfrak{Z} = \{(a, n) \mid a \in A; n \in \mathfrak{Z}\}.$$

Definamos la suma y el producto de la siguiente manera

$$\begin{aligned}(a, n) + (b, m) &= (a + b, n + m)\\ (a, n)(b, m) &= (ab + ma + nb, nm),\end{aligned}$$

entonces $A \times \mathfrak{Z}$ es un anillo con estas operaciones —la demostración de

este hecho no es complicada, aunque si tediosa. Nótese que este anillo que hemos definido posee un elemento neutro dado por $(0, 1)$.

Ahora, consideremos el subconjunto $A \times \{0\}$ de $A \times \mathfrak{Z}$, formado por los elementos de la forma $(a, 0)$. Este subconjunto es un subanillo de $A \times \mathfrak{Z}$. Por último, considérese la función $f\colon A \to A \times \{0\}$ dada por $f(a) = (a, 0)$. Tanto la inyectividad como la sobreyectividad de f son evidentes, además

$$f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b)$$

y

$$f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a)f(b)$$

por lo que f es un isomorfismo de A en $A \times \{0\}$.

El proceso anterior incrusta cualquier anillo A en $A \times \mathfrak{Z}$, un anillo unitario.

Es sensato preguntarse que ocurre con el proceso descrito en el teorema anterior cuando el anillo A es unitario. En este caso, el elemento unidad de A no hace mas que introducir divisores de cero en el anillo extendido.

Aunque el teorema anterior nos permitiría reducir nuestro estudio a anillos unitarios preferiremos, de ahora en adelante, *no* suponer que un anillo es unitario a menos de que sea necesario.

§ 3.6.6 Extensión de homomorfismos

Nos interesa ahora resolver el problema de extender funciones. El siguiente teorema discute un situación en la que es posible extender un homomorfismo, de un subanillo al anillo completo, conservando las operaciones.

Teorema 3.6.7. holaaa

§ 3.6.7 Ejercicios

4

Ideales Primos y Máximos

> El arte de hacer matemáticas es conseguir ese caso especial que contiene todos los gérmenes de la generalidad
>
> David Hilbert

Nos dedicaremos a estudiar ciertos tipos especiales de ideales: primos y máximos. En general, hablaremos de anillos conmutativos y unitarios debido a que nuestras hipótesis nos obligarán a ello.

§ 4.1 IDEAL MÁXIMO

Comenzamos con la siguiente definición.

> Definición 4.1.1 (ideal máximo). Un ideal I de un anillo A es *máximo* siempre que $I \neq A$ y que si J es un ideal de A tal que $I \subset J \subseteq R$ entonces $J = R$.

Dicho de otra manera, un ideal máximo es aquel que no esta contenido en ningún ideal propio de A y que es distinto de A.

Normalmente es complicado demostrar que un ideal es máximo solamente con la definición anterior, por esto el siguiente teorema es importante: nos dará una forma de identificar los ideales máximos sin necesidad de construir un argumento sobre conjuntos y contenciones.

> Teorema 4.1.1. Sea A un anillo conmutativo con unidad. Entonces I es un ideal máximo de A si, y solo si, A/I es un cuerpo.
>
> *Demostración.* Supongamos que I es un ideal máximo de A. Observemos que si A es conmutativo y unitario, entonces A/I también es conmutativo y unitario siempre que $I \neq A$, que es el caso cuando I es máximo. Sea $(a+I) \in A/I$ con $a \notin I$ de tal forma que $a + I$ no sea nulo. Supongamos que $a + I$

no posee inverso multiplicativo en A/I. Entonces el conjunto

$$(A/I)(a+I) = \{(r+I)(a+I) \mid r+I \in A/I\}$$

no contiene al elemento $1+I$. Es fácil ver que $(A/I)(a+I)$ es un ideal de A/I, además, es un ideal propio debido a que $a \notin I$ y $(1+I) \notin (A/I)(a+I)$.

Si ϕ: $A \to A/I$ es el homomorfismo natural, entonces el conjunto

$$\phi^{-1}((A/I)(a+I))$$

es un ideal propio de A que contiene a I. Pero esto es una contradicción debido a que I es máximo. Se sigue que el elemento $a+I$ debe necesariamente tener inverso en A/I y que A/I es un cuerpo.

Supongamos ahora que A/I es un cuerpo. Si J es un ideal de A tal que $I \subset J \subset A$, y ϕ: $A \to A/I$ es el homomorfismo natural, entonces $\phi(J)$ es un ideal de A/I tal que $\{0+M\} \subset \phi(J) \subset A/I$. Pero esto último es una contradicción, pues los cuerpos no tienen ideal propios. Se sigue que si A/I es un cuerpo entonces I es máximo.

El siguiente ejemplo ayudará a ilustrar un poco el teorema anterior.

Ejemplo 4.1.1. Como $\mathfrak{Z}/n\mathfrak{Z}$ es un cuerpo si, y solo si, n es primo; se sigue que un ideal $n\mathfrak{Z}$ de $\mathfrak{Z}$ es máximo si, y solo si, n es un número primo.

§ 4.2 IDEAL PRIMO

Nos interesa ahora pensar en como son los ideales I de un anillo conmutativo y unitario A, tales que A/I es un dominio entero. Después de un poco de inspección, la respuesta es sencilla: A/I es un dominio entero si, y solo si,

$$(a+I)(b+I) = I$$

implica que $a+I = I$ o $b+I = I$, debido a que I es el cero de A/I. Pero esto último implica que $a \in I$ o $b \in I$. La siguiente definición formaliza la discusión anterior.

> Definición 4.2.1 (ideal primo). Un ideal I de un anillo conmutativo y unitario es *primo* si, y solo si, $ab \in I$ implica que $a \in I$ o $b \in I$ con a y b elementos de A.

En cualquier dominio entero el conjunto $\{0\}$ es siempre un ideal primo, como cabría esperar.

La discusión anterior a la definición constituye la demostración del siguiente teorema.

Teorema 4.2.1. Sea A un anillo unitario y conmutativo, y sea I un ideal de A. Entonces I es primo si, y solo si, A/I es un dominio entero.

Corolario 4.2.1.1. Todo ideal máximo es un ideal primo.

Demostración. Sea A un anillo unitario y conmutativo y sea I un ideal máximo de A. Como I es máximo, A/I es un cuerpo. En particular, A/I es un dominio entero e I es un ideal primo.

A modo de resumen tenemos que, si A es un anillo unitario y conmutativo,

1. Un ideal I de A es máximo si, y solo si, A/I es un cuerpo.
2. Un ideal J de A es primo si, y solo si, A/J es un dominio entero.
3. Todo ideal máximo de A es primo.

Sobre LaTeX y esta guía

Este apéndice pretende lograr dos cosas: explicar, mas o menos, como fue hecha esta guía —para aquellos interesados en estas cosas— y decir una o dos cosas sobre tipografía.

Primero, ¿cómo se hizo esta guía? La respuesta a la pregunta es fácil: con LaTeX. Mas específicamente, con TeXLive y TeXStudio. Para el que no tenga idea de que son estas palabras mágicas, la explicación es sencilla, LaTeX es un sistema de tipografía para computadoras y es además software *libre*.

Para los que no sepan sobre el software libre, revisen `https://www.fsf.org/about/what-is-free-software`. Como es software libre, existen varias *distribuciones* de —formas de empaquetar y distribuir— LaTeX, TeXLive es una de ellas. TeXStudio, por otra parte, es un editor de texto. Vale la pena decir que, teniendo en cuenta lo variado que es el mundo de los editores de texto, cualquiera sirve para crear documentos en LaTeX: desde uno simple como `GNU nano` hasta algunos mas grandes y complejos.

En lo que respecta a la tipografía de esta guía, hay algunas cosas que me gustaría decir: cuales son las fuentes y una que otra cosa acerca del formato.

Para obtener el código fuente de este documento, y tener así todos los demás detalles, véase `ALGOAKI`. De no funcionar el link, pueden enviarme un correo a la dirección que esta en el prefacio.

Por último, y en lo que respecta a la tipografía en general, daré dos recomendaciones rápidas y unas cuantas referencias bibliográficas. La primera recomendación es usar márgenes grandes, pues ayudan a leer mejor, y la segunda es ser *minimalista*: usar la menor cantidad de herramientas para obtener el efecto deseado en el texto. Para los interesados en el tema, que tiene mucho de interesante, recomiendo el libro-web de Butterick [**typobutterick**] y el libro —físico, pero se puede encontrar en `libgen.io`— de Bringhurst [**typobringhurst**].