Infierno y Purgatorio
Saga de la Divina Comedia

Universidad de Murcia

Jesús González Abril

October 6, 2025

Contents

Chapter 1

Grupos

1.1 Operaciones binarias

Definition 1.1.1: Operación binaria

Sea X un conjunto. Una operación binaria en X es una aplicación $* : X \times X \to X$. Por lo general escribimos $*(a, b) = a * b$.

Remark. En general, si por el contexto se sobreentiende que una operación es binaria, se simplifica el lenguaje hablando simplemente de operaciones. De igual manera, normalmente se omite el conjunto sobre el que está definida la operación.

Definition 1.1.2: Tipos de operaciones

Una operación $*$ se dice

- **Conmutativa** si $x * y = y * x$ para todo $x, y \in X$.
- **Asociativa** si $x * (y * z) = (x * y) * z$ para todo $x, y, z \in X$.

Definition 1.1.3: Terminología sobre elementos

Un elemento $x \in X$ se dice que es:

- **Neutro por la izquierda (neutro por la derecha)** si $x*y = y$ para todo $y \in X$ ($y*x = y$ para todo $y \in X$).
- **Cancelable por la izquierda (cancelable por la derecha)** si para cada dos elementos distintos $a \neq b$ de X se verifica $x * a \neq x * b$ ($a * x \neq b * x$).
- **Neutro** si es neutro por la derecha y por la izquierda.
- **Cancelable** si es cancelable por la izquierda y por la derecha.

Supongamos que e es un elemento neutro de X con respecto a $*$. Sean x e y elementos de X. Decimos que x es simétrico de y por la izquierda y que y es simétrico de x por la derecha con respecto a $*$ si se verifica $x * y = e$. En este contexto decimos que x es:

- **Simétrico** de y si lo es por ambos lados. En tal caso decimos que x es invertible, siendo y su inverso ($y = x^{-1}$ si el inverso es único).

Example 1.1.4

Si x es cancelable por la izquierda, entonces para cualesquiera $a, b \in X$ se tiene

$$x * a = x * b \implies a = b$$

Proof

Supongamos que $x * a = x * b$, si $a = b$ ya hemos terminado. En caso contrario, a y b son elementos distintos, y, como x es cancelable por la izquierda, entonces debe ser $x*a \neq x*b$, pero eso contradice la suposición inicial, luego ha de ser $a = b$.

Example 1.1.5

Si x es cancelable por la derecha entonces, para cualesquiera $a, b \in X$ se tiene

$$a * x = b * x \implies a = b$$

Remark. Notemos que esta caracterización no es más que el contrarrecíproco de la primera definición que hemos dado de elemento cancelable.

Definition 1.1.6: Tipos de conjuntos con operaciones

Un par $(X, *)$ formado por un conjunto y una operación $*$ decimos que es un:

- **Semigrupo** si $*$ es asociativa.
- **Monoide** si es un semigrupo que tiene un elemento neutro con respecto a $*$.
- **Grupo** si es un monoide y todo elemento de X es invertible con respecto a $*$.
- **Grupo abeliano** si es un grupo y $*$ es conmutativa.

Example 1.1.7

Si tomamos la suma de elementos sobre distintos conjuntos de números obtenemos un ejemplo de cada uno de los tipos de conjuntos con operaciones:

1. $(\mathbb{N} \setminus \{0\}, +)$ es un semigrupo, ya que la suma es asociativa, pero no tiene neutro.
2. $(\mathbb{N}, +)$ es un monoide, ya que la suma es asociativa y tiene el 0 como neutro.
3. $(\mathbb{Z}, +)$ es un grupo, ya que la suma es asociativa, tiene neutro y todos los elementos tienen inverso. De hecho, como la suma es conmutativa es un grupo abeliano.

Example 1.1.8: Grupo no abeliano

Un ejemplo de grupo no abeliano es $GL_n(\mathbb{R})$ si $n \geq 2$. $GL_n(\mathbb{R})$ es el grupo de las matrices invertibles $n \times n$ con entradas reales, donde la operación es la multiplicación de matrices.

Proof

En primer lugar, es inmediato que la operación es asociativa. También es fácil ver que tiene elemento neutro, la matriz identidad I_n. Si tomamos una matriz cualquiera $A \in GL_n(\mathbb{R})$ esta ha de tener inversa, por lo que su elemento inverso es A^{-1} que claramente pertenece a $GL_n(\mathbb{R})$.
Finalmente, para ver que el grupo no es conmutativo notemos que para $n = 2$ podemos tomar las matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

ambas invertibles por tener determinante no nulo, que verifican

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

En el caso de que sea $n > 2$ podemos tomar matrices de la forma

$$A' = \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}, B' = \begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

cuyo producto no conmuta por las propiedades de la multiplicación de matrices por bloques.

Example 1.1.9

Sean A un conjunto y sea $X = A^A$ el conjunto de las aplicaciones de A en A. Probar que la composición de aplicaciones define una operación asociativa en X para la que la identidad 1_X es neutro. Esto prueba que $(A^A, \circ)$ es un monoide.

Proposition 1.1.10

Sea $*$ una operación en un conjunto X.

1. Si e es un neutro por la izquierda y f es un neutro por la derecha de X con respecto a $*$, entonces $e = f$. En particular, X tiene a lo sumo un neutro.
2. Supongamos que $(X, *)$ es un monoide y sea $a \in X$.
   (a) Si x es un simétrico por la izquierda de a e y es un simétrico por la derecha de a, entonces $x = y$. Por tanto, en tal caso a es invertible y tiene a lo sumo un simétrico.
   (b) Si a tiene un simétrico por un lado entonces es cancelable por ese mismo lado. En particular, todo elemento invertible es cancelable.

Proof

(1) Como e es neutro por la izquierda y f es neutro por la derecha tenemos

$$f = e * f = e.$$

(2a) Ahora suponemos que $(X, *)$ es un monoide. Por (1), $(X, *)$ tiene un único neutro que vamos a denotar por e. Como x es inverso por la izquierda de a e y es inverso por la derecha de a, usando la propiedad asociativa, tenemos que

$$y = e * y = (x * a) * y = x * (a * y) = x * e = x.$$

(2b) Supongamos que a es un elemento de X que tiene un inverso por la izquierda b y que $a * x = a * y$ para $x, y \in X$. Usando la asociatividad una vez más concluimos que

$$x = e * x = (b * a) * x = b * (a * x) = b * (a * y) = (b * a) * y = e * y = y.$$

Remark. Por la proposición anterior si X *es un monoide cada elemento invertible* a *tiene un único inverso que denotaremos* a^{-1}.

1.1.1 Subconjuntos y operaciones

Sea $*$ una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es cerrado con respecto a $*$ si para todo $a, b \in B$ se verifica que $a * b \in B$. En tal caso podemos considerar $*$ como una operación en B que se dice inducida por la operación en A.

- Un subsemigrupo de un semigrupo es un subconjunto suyo que con la misma operación es un semigrupo.
- Un submonoide de un monoide es un subconjunto suyo que con la misma operación es un monoide con el mismo neutro.
- Un subgrupo de un grupo es un subconjunto suyo que con la misma operación es un grupo.

1.2 Definiciones y ejemplos

Definition 1.2.1: Grupo

Un grupo es una pareja $(G, \cdot)$, formada por un conjunto no vacío G junto con una operación binaria, que denotaremos por $\cdot$, que satisface los siguientes axiomas:

1. (Asociativa) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.
2. (Neutro) Existe un elemento $e \in G$, llamado elemento neutro del grupo, tal que $e \cdot a = a = a \cdot e$, para todo $a \in G$.
3. (Inverso) Para todo $a \in G$ existe otro elemento $a^{-1} \in G$, llamado elemento inverso de a, tal que $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Si además se verifica el siguiente axioma se dice que el grupo es abeliano o conmutativo:

4. (Conmutativa) $a \cdot b = b \cdot a$, para todo $a, b \in G$.

Demostraremos ahora algunas propiedades de los grupos.

Lemma 1.2.2: Propiedades básicas de grupos

Sea $(G, \cdot)$ un grupo.

1. (Unicidad del neutro) El neutro de G es único y lo denotaremos e. De hecho, si $a, b \in G$ satisfacen que $a \cdot b = a$ ó $b \cdot a = a$ entonces $b = e$.
2. (Unicidad del inverso) El inverso de un elemento a de G es único y lo denotaremos a^{-1}. De hecho, si e es el neutro de G y $a, b \in G$ satisfacen $a \cdot b = e$ ó $b \cdot a = e$ entonces $b = a^{-1}$.
3. (Propiedad Cancelativa) Todo elemento de G es cancelativo.
4. Para todo $a, b \in G$, las ecuaciones $a \cdot X = b$ y $X \cdot a = b$ tienen una única solución en G.
5. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof

1. Haremos solo el caso por la derecha, en efecto, si $a \cdot b = a$ entonces
$$b = e \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot a = e.$$
2. De nuevo hacemos solo el caso $a \cdot b = e$
$$a^{-1} = a^{-1} \cdot e = a^{-1} \cdot a \cdot b = e \cdot b = b.$$
3. Sea $x \in G$, entonces x debe ser cancelable puesto que en caso contrario existirían $a, b \in G$ con $a \neq b$ tales que $x \cdot a = x \cdot b$, pero entonces
$$a = e \cdot a = x^{-1} \cdot x \cdot a = x^{-1} \cdot x \cdot b = e \cdot b = b$$
una contradicción.
4. Sean $a, b \in G$ arbitrarios y x, y dos soluciones cualesquiera, entonces
$$x = e \cdot x = a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

y de igual manera

$$y = e \cdot y = a^{-1} \cdot a \cdot y = a^{-1} \cdot b$$

luego $x = y$. Para la otra ecuación se razona igual. Notemos que también hemos demostrado la existencia de una solución ($x = a^{-1} \cdot b$).

5. Basta realizar un sencillo cálculo y aplicar el apartado 2

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot b \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e.$$

1.2.1 Ejemplos

Example 1.2.3: Grupo trivial

Sea X un conjunto y consideremos la aplicación identidad $1_X : X \to X$ tal que $1_X(x) = x$ para todo $x \in X$. Entonces el conjunto $T = \{1_X\}$ con la operación de composición es un grupo $(T, \circ)$ que llamaremos el grupo trivial (lo denotaremos 1).
En general, podríamos haber definido este grupo como un único elemento $\{x\}$ con la operación descrita por $x \cdot x = x$.

En términos de grupos de transformaciones, el grupo trivial de X es el grupo de transformaciones más pequeño que podemos construir. Que en efecto se trata de un grupo es inmediato.

Example 1.2.4: Grupo simétrico

Sean X un conjunto y S_X el conjunto de todas las biyecciones de X en sí mismo. Entonces $(S_X, \circ)$ es un grupo, llamado grupo simétrico o grupo de las permutaciones de X.

En términos de grupos de transformaciones, el grupo de permutaciones de X es el grupo de transformaciones más grande que podemos construir. Probemos ahora que en efecto es un grupo.

Proof

Prescindiremos del uso de $\circ$ para simplificar la notación.

1. Asociativa: sean f, g, h biyecciones, dado $x \in X$ cualquiera

$$((fg)h)x = (fg)(h(x)) = f(g(h(x))) = f(gh(x)) = (f(gh))x \implies (fg)h = f(gh)$$

2. Neutro: basta considerar la aplicación identidad $\mathrm{id}(x) = x$.

3. Inverso: claramente el inverso de una biyección cualquiera f es su inversa f^{-1}, que verifica

$$(ff^{-1})(x) = f(f^{-1}(x)) = x$$

luego $ff^{-1} = \mathrm{id}$.

Remark. En general S_X no es un grupo abeliano.

Example 1.2.5: Producto de grupos

Si $(G, *)$ y $(H, *)$ son dos grupos, entonces el producto directo $G \times H$ es un grupo en el que la operación viene dada componente a componente:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

Más generalmente, si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el producto directo $\prod_{i \in I} G_i$ tiene una estructura de grupo en el que el producto se realiza componente a componente. Para más información ver la Definición A.5.1.

Probemos que el producto directo de dos grupos es un grupo:

Proof

1. Asociativa:

$$((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 * g_2, h_1 * h_2) \cdot (g_3, h_3) = (g_1 * g_2 * g_3, h_1 * h_2 * h_3) = \\ = (g_1, h_1) \cdot (g_2 * g_3, h_2 * h_3) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))$$

   donde hemos usado la asociatividad de los grupos G, H.

2. Neutro: basta considerar el elemento (e_G, e_H) donde e_G es el neutro de G y e_H el de H.

3. Inverso: claramente el inverso de un elemento cualquiera (g_1, h_1) es (g_1^{-1}, h_1^{-1}), que verifica
$$(g_1, h_1) \cdot (g_1^{-1}, h_1^{-1}) = (g_1 * g_1^{-1}, h_1 * h_1^{-1}) = (e_G, e_H).$$

Example 1.2.6: Tabla de Cayley

Dado un grupo finito podemos construir lo que llamaremos su tabla de Cayley (también llamada tabla de multiplicación o de suma, dependiendo del nombre que le demos a la operación del grupo). Esta tabla se obtiene disponiendo cada uno de los elementos del grupo tanto por columnas como por filas y calculando sus productos. Si el grupo tiene 2 elementos a, b la tabla será de la forma:

$\cdot$	a	b
a	$a \cdot a$	$a \cdot b$
b	$b \cdot a$	$b \cdot b$

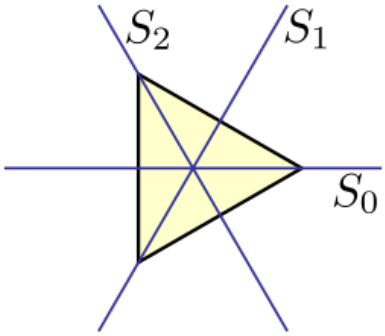
Como ejemplo concreto, la tabla del grupo $\mathbb{Z}_3$ (enteros módulo 3) es la siguiente:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

1.2.2 El grupo diédrico

Veamos ahora un grupo con especial significado geométrico. Consideremos un polígono regular de n lados y las transformaciones que lo dejan invariantes (rotaciones y reflexiones), a las que llamaremos simetrías. La composición de dos simetrías de un polígono regular es nuevamente una simetría de este objeto. Considerando la composición de simetrías como operación binaria, esto le da a las simetrías la estructura algebraica de un grupo finito.

La siguiente tabla de Cayley muestra el efecto de la composición en el grupo diédrico de orden 6, D_3 – las simetrías de un triángulo equilátero. Aquí, r_0 denota la identidad, r_1 y r_2 denotan rotaciones en sentido antihorario de 120° y 240° respectivamente, mientras que s_0, s_1 y s_2 denotan reflexiones a través de las tres líneas mostradas en la imagen adyacente.



$\circ$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Por ejemplo, $s_2 s_1 = r_1$, porque la reflexión s_1 seguida de la reflexión s_2 resulta en una rotación de 120°. El orden de los elementos que denotan la composición es de derecha a izquierda, reflejando la convención de que el elemento actúa sobre la expresión a su derecha. La operación de composición no es conmutativa.

El siguiente ejemplo abstrae y generaliza el concepto de grupo diédrico prescindiendo de la interpretación geométrica.

Example 1.2.7: Grupo diédrico

Para cada número natural positivo n definimos un grupo formado por $2n$ elementos

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

en el que la multiplicación viene dada por la siguiente regla:

$$(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$$

con notación como en el ejemplo anterior. Este grupo se llama grupo diédrico de orden $2n$.

El grupo diédrico infinito D_∞ está formado por elementos de la forma $a^n b^m$, con $n \in \mathbb{Z}$ y $m = 0, 1$ con el producto $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1+(-1)^{j_1}i_2}b^{[j_1+j_2]_2}$.

Si ahora consideramos únicamente las rotaciones que dejan invariante un polígono de n lados obtenemos otro grupo, en este caso con n elementos, cada uno de ellos correspondiente a rotar por un múltiplo de $\frac{360°}{n}$. El siguiente ejemplo abstrae este grupo de rotaciones.

Example 1.2.8: Grupo cíclico

Para cada número natural positivo n definimos un grupo C_n formado por n elementos

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

donde a es un símbolo, y en el que la multiplicación viene dada por la siguiente regla:

$$a^i a^j = a^{[i+j]_n}$$

donde $[x]_n$ denota el resto de dividir x entre n. Este grupo se llama cíclico de orden n. También definimos el grupo cíclico infinito como el conjunto $C_\infty = \{a^n : n \in \mathbb{Z}\}$, donde a es un símbolo y consideramos $a^n = a^m$ si y solo si $n = m$, y en el que el producto viene dado por $a^n \cdot a^m = a^{n+m}$.

Remark. Es fácil notar la similitud entre C_n y $\mathbb{Z}_n$, así como entre C_∞ y $\mathbb{Z}$. Más tarde formalizaremos esta intuición probando que estos grupos son equivalentes (isomorfos).

Chapter 2

Anillos

2.1 Anillos

Definition 2.1.1: Anillo

Un anillo es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ (suma) y $\cdot$ (producto) en A que verifican:

1. $(A, +)$ es un grupo abeliano.
2. $(A, \cdot)$ es un monoide.
3. Distributiva del producto respecto de la suma: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ para todo $a, b, c \in A$.

Si además $\cdot$ es conmutativo en A, decimos que $(A, +, \cdot)$ es un anillo conmutativo.

Remark.

- *El neutro de A con respecto a $+$ se llama cero y se denota 0.*
- *El neutro de A con respecto a $\cdot$ se llama uno y se denota 1.*
- *El simétrico de un elemento a con respecto a $+$ se llama opuesto y se denota $-a$.*
- *Si a es invertible con respecto a $\cdot$, su simétrico se llama inverso y se denota a^{-1}.*
- *En general para $+$ y $\cdot$ usamos la notación usual para sumas y productos*

$$a \cdot (b + c) = a(b + c) = ab + ac.$$

Como $(A, +)$ es un grupo, todo elemento de A es invertible respecto de la suma y por tanto cancelable. Diremos que un elemento de A es regular en A si es cancelable con respecto al producto. En caso contrario decimos que el elemento es singular en A o divisor de cero. El termino divisor de cero se justifica por lo siguiente. Supongamos que $x \in A$ no es cancelable respecto al producto, en tal caso existen dos elementos distintos $a \neq b$ tales que $ax = bx$. Pero entonces es inmediato que

$$(a - b)x = 0$$

sin embargo, ni $(a - b)$ ni x son cero, por lo que podemos interpretar que ambos son «divisores del cero».

2.1.1 Ejemplos de anillo

Example 2.1.2

Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos con la suma y el producto usuales. Notemos que todo elemento no nulo de $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es invertible. Sin embargo, en $\mathbb{Z}$ solo hay dos elementos invertibles (1 y -1) aunque todos los elementos son regulares menos el 0.

Proof

Demostrar que se trata de anillos conmutativos es muy sencillo, basta comprobar que se verifican todas las propiedades pertinentes.
Probaremos que en $\mathbb{C}$ todos los elementos salvo el 0 son invertibles, el resto de afirmaciones quedan como ejercicio. Sea $z = a + bi$ un número complejo cualquiera no nulo, en tal caso el número $w = \frac{a-bi}{a^2+b^2}$ verifica

$$zw = \frac{(a+bi)(a-bi)}{a^2+b^2} = \frac{a^2 - abi + abi - b(-1)}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} = 1$$

luego $w = z^{-1}$ y por tanto z tiene inverso.

Example 2.1.3: Producto de anillos

Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones definidas componente a componente:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

Obsérvese que $A \times B$ es conmutativo si y solo si lo son A y B, y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

Example 2.1.4

Dados un anillo A y un conjunto X, el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

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

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Si definimos la familia de conjuntos $\{A_i = A : i \in X\}$ entonces es inmediato que $\cup_{i\in X} A_i = A$. Recordemos ahora que el producto $\prod_{i\in X} A_i$ es el conjunto de funciones $f : X \to \cup_{i\in X} A_i$, es decir, el conjunto de funciones $f : X \to A$, luego A^X es un anillo correspondiente a un producto «infinito» del anillo A consigo mismo. Para más información ver la Definición A.5.1.

Example 2.1.5: Anillo de polinomios

Dado un anillo A, un polinomio en una indeterminada es una expresión:

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

donde $n \geq 0$ y $a_i \in A$ para todo i. El conjunto de polinomios con coeficientes en A se denota $A[X]$. La suma y producto en $A[X]$ se definen de la forma usual.

Example 2.1.6: Sucesiones

Dado un anillo A, denotamos por $A[[X]]$ el conjunto de sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. Con las operaciones:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, \ldots),$$

$A[[X]]$ es un anillo llamado anillo de series de potencias con coeficientes en A.

2.1.2 Propiedades de los anillos

Lemma 2.1.7

Sea A un anillo y sean $a, b, c \in A$. Se verifican las siguientes propiedades

1. Todo elemento de A es cancelable respecto de la suma.
2. Todo elemento invertible de A es regular en A.
3. Si $b + a = a$ entonces $b = 0$. Si $ba = a$ para todo a, entonces $b = 1$. En particular, el cero y uno son únicos.
4. El opuesto de a es único y si a es invertible, entonces a tiene un único inverso.
5. $0a = 0 = a0$.
6. $a(-b) = (-a)b = -(ab)$.
7. $a(b - c) = ab - ac$.
8. a y b son invertibles si y solo si ab y ba son invertibles. En tal caso $(ab)^{-1} = b^{-1}a^{-1}$.
9. Si $0 = 1$ entonces $A = \{0\}$.

Proof

1. Como A es un grupo respecto de la suma todo elemento tiene inverso, y por la Proposición 1.1.10 todo elemento invertible (respecto a la suma) es cancelable (respecto a la suma).
2. De nuevo por la Proposición 1.1.10 todo elemento invertible (respecto al producto) es cancelable (respecto al producto).
3. Si $b + a = a$ entonces como a es cancelable por el apartado 1, tenemos $b = 0$. Si $ba = a$ para todo a, entonces como el neutro es único $b = 1$.
4. De nuevo se sigue de la Proposición 1.1.10.

5. Basta aplicar un pequeño truco

$$0a = (0+0)a = 0a + 0a \implies 0 = 0a$$

para el caso $a0$ se procede igual.

6. Basta notar que

$$ab + a(-b) = a(b-b) = 0, ab + (-a)b = (a-a)b = 0 \implies -(ab) = a(-b) = (-a)b$$

ya que los opuestos son únicos.

7. $a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.

8. En primer lugar si a, b son invertibles entonces existen a^{-1}, b^{-1} y es fácil ver que

$$ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab, ba(a^{-1}b^{-1}) = e = (a^{-1}b^{-1})ba$$

luego ab, ba son invertibles. Para el recíproco, si ab, ba son invertibles entonces

$$a(b(ab)^{-1}) = ab(ab)^{-1} = e, ((ba)^{-1}b)a = (ba)^{-1}ba = e$$

por tanto, por la Proposición 1.1.10 ambos simétricos $b(ab)^{-1}, (ba)^{-1}b$ son iguales (ambos son a^{-1}) y a es invertible. Para ver que b es invertible se procede igual.

9. Si $0 = 1$ entonces dado $x \in A$ tenemos

$$x = x1 = x0 = 0 \implies A = \{0\}.$$

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ convenimos que $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n+1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

Lemma 2.1.8

Sea A un anillo, $a, b \in A$, y $m, n \in \mathbb{Z}$. Se verifican:

1. $n(a+b) = na + nb$.
2. $(n+m)a = na + ma$.
3. Si $n, m \geq 0$, entonces $a^{n+m} = a^n a^m$. Si a es invertible, la igualdad vale para n, m arbitrarios.
4. Si A es conmutativo y $n \geq 0$, entonces $(ab)^n = a^n b^n$. Si a y b son invertibles, la igualdad vale para todo n.

Proof

1. Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces

$$(n+1)(a+b) = (a+b) + na + nb = (n+1)a + (n+1)b.$$

2. Basta aplicar recursivamente que $(n+1)a = a + na$.
3. Basta aplicar recursivamente que $a^{n+1} = aa^n$. Si a es invertible entonces podemos usar que $a^{-n} = (a^{-1})^n$ distinguiendo casos. Por ejemplo si $n > 0, m < 0, n > m$

entonces

$$a^n a^m = a^n (a^{-1})^{-m} = a^{n+m} a^{-m} (a^{-1})^{-m} = a^{n+m}.$$

4. Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces

$$(ab)^{n+1} = ab(ab)^n = aba^n b^n = aa^n bb^n = a^{n+1} b^{n+1}.$$

Cuando a y b son invertibles, si $n < 0$

$$(ab)^n = ((ab)^{-1})^{-n} = (b^{-1}a^{-1})^{-n} = (b^{-1})^{-n} (a^{-1})^{-n} = b^n a^n.$$

2.2 Subanillos

Remark. A partir de ahora supondremos que todos los anillos que aparecen son conmutativos.

Sea $*$ una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es cerrado con respecto a $*$ si para todo $a, b \in B$ se verifica que $a * b \in B$. En tal caso podemos considerar $*$ como una operación en B que se dice inducida por la operación en A.

Definition 2.2.1: Subanillo

Un subanillo de un anillo es un subconjunto suyo que con la misma suma y producto es un anillo con el mismo uno.

Proposition 2.2.2: Caracterización de subanillos

Las siguientes condiciones son equivalentes para $B \subseteq A$:

1. B es un subanillo de A.
2. B contiene al 1 y es un anillo, luego es cerrado para sumas, productos y opuestos.
3. B contiene al 1 y es cerrado para restas y productos.

Proof

$(1) \implies (2)$: Si B es un subanillo de A entonces contiene al 1 y es cerrado para sumas y productos. Por otro lado, como B es un anillo, tiene un cero, que de momento denotamos 0_B y cada elemento $b \in B$ tiene un opuesto en B. En realidad $0_B + 0_B = 0_B = 0 + 0_B$, con lo que aplicando la propiedad cancelativa de la suma deducimos que $0_B = 0$, o sea, el cero de A está en B y por tanto es el cero de B (el único que puede tener). Por la unicidad del opuesto, el opuesto de b ha de ser el de A, con lo que B es cerrado para opuestos.
$(2) \implies (3)$: Inmediato.
$(3) \implies (1)$: Si B contiene al 1 y es cerrado para restas, entonces $0 = 1 - 1 \in B$, y para $b \in B$, $-b = 0 - b \in B$. Además, $a + b = a - (-b) \in B$, luego B es cerrado para sumas, por tanto, es un subanillo de A.

Example 2.2.3: Subanillo impropio

Todo anillo A es un subanillo de si mismo, al que llamamos impropio por oposición al resto de subanillos, que se dicen propios.

Example 2.2.4

En la cadena de contenciones $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ cada uno es un subanillo de los posteriores.

Example 2.2.5

Si A es un anillo, el subconjunto $\{0\}$ es cerrado para sumas, productos y opuestos. Si $A = \{0\}$ entonces $\{0\}$ sería subanillo de A, pero este es el único caso en el que esto pasa pues en todos los demás casos $1 \neq 0$.
En efecto si $1 = 0$ entonces para cualquier $a \in A$, $a = 1a = 0a = 0 \implies A = \{0\}$.

Example 2.2.6

Si A y B son anillos entonces $A \times \{0\}$ es un anillo, pero no es un subanillo de $A \times B$ porque no contiene a $(1_A, 1_B)$.
De igual manera, $A \times \{1_B\}$ con las operaciones

$$(a, 1_B) + (b, 1_B) = (a + b, 1_B), \quad (a, 1_B) \cdot (b, 1_B) = (ab, 1_B)$$

es un anillo, pero no es subanillo de $A \times B$ porque las operaciones no son las inducidas por la operaciones de $A \times B$.

Example 2.2.7: Subanillo primo

Si A es un anillo entonces el conjunto:

$$\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\}$$

es un subanillo de A contenido en cualquier otro subanillo de A.
Este se conoce como el subanillo primo de A.
Observaciones:

- $\mathbb{Z}$ y los $\mathbb{Z}_n$ son sus propios subanillos primos
- Por tanto, no tienen subanillos propios

Example 2.2.8

Dado un número entero m, los conjuntos:

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$

son subanillos de $\mathbb{C}$.
Observaciones:

- Si $m > 0$, ambos son subanillos de $\mathbb{R}$
- Si m es un cuadrado perfecto, estos conjuntos coinciden con $\mathbb{Z}$ y $\mathbb{Q}$ respectivamente
- Cuando m no es cuadrado perfecto, la igualdad $a + b\sqrt{m} = 0$ implica $a = 0$ y $b = 0$

Caso particular importante:

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ con $i = \sqrt{-1}$ es el anillo de los enteros de Gauss

Example 2.2.9

Todo anillo A puede verse como un subanillo del anillo de polinomios $A[X]$ identificando los elementos de A con los polinomios constantes (del tipo $P = a_0$).

Example 2.2.10: Diagonal

Sea A un anillo y X un conjunto. Entonces la diagonal:

$$B = \{f \in A^X : f(x) = f(y) \text{ para todo } x, y \in X\}$$

(es decir, el conjunto de las aplicaciones constantes de X en A) es un subanillo de A^X.

Example 2.2.11

Sea $A = M_n(B)$, donde B es un anillo. Son subanillos:

- El conjunto de las matrices diagonales
- El conjunto de las matrices escalares: $\{aI_n : a \in B\}$
- El conjunto de las matrices triangulares superiores

Example 2.2.12

Sea $A = B \times B$, con B un anillo. Son subanillos:

- $A_1 = \{(b, b) : b \in B\}$ (la diagonal)
- $A_2 = B_1 \times B_2$, donde B_1 y B_2 son subanillos de B

Example 2.2.13

Sea A un anillo cualquiera y B un subanillo de A. Para $\alpha \in A$, el conjunto:

$$A_1 = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \geq 0, a_0, a_1, \ldots, a_n \in B\}$$

es un subanillo de A llamado subanillo generado por B y α.

Example 2.2.14

Sea $A = B[X]$, donde B es un anillo. Son subanillos:

- $A_1 = B_1[X]$, donde B_1 es un subanillo de B
- El conjunto de polinomios de grado menor o igual que un número dado n (¡cuidado! este no siempre es subanillo, ya que el producto puede aumentar el grado)

Example 2.2.15

Sea $A = \mathbb{C}$. Son subanillos:

- $A_1 = \{a + bi : a = b\} = \{(1 + i)a : a \in \mathbb{R}\}$
- $A_2 = \{ai : a \in \mathbb{R}\}$ (solo contiene a los imaginarios puros, pero ¡cuidado! verificar que contiene al 1)
- $A_3 = \{a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i : a_1, a_2, a_3, a_4 \in \mathbb{Z}\}$

No es subanillo:

- $A_4 = \{a + bi : b \geq 0\}$ (no cerrado para opuestos)

Example 2.2.16

Decimos que un entero d es libre de cuadrados si p^2 no divide a d para ningún número primo p (en particular 1 es libre de cuadrados).
Para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que:

$$\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$$

Esto no ocurre en general si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$.

2.3 Homomorfismos de anillos

Definition 2.3.1: Homomorfismo de anillos

Sean A y B dos anillos. Un homomorfismo de anillos entre A y B es una aplicación $f : A \to B$ que satisface:

1. $f(x + y) = f(x) + f(y)$
2. $f(x \cdot y) = f(x) \cdot f(y)$
3. $f(1) = 1$

Un isomorfismo es un homomorfismo biyectivo. Dos anillos A y B son isomorfos ($A \cong B$) si existe un isomorfismo entre ellos.

Remark. En la definición anterior hemos usado el mismo símbolo para las operaciones en ambos anillos, pero es importante notar que:

- *En* $f(x + y)$*, la suma se realiza en* A
- *En* $f(x) + f(y)$*, la suma se realiza en* B
- *Lo mismo aplica para el producto*

Definition 2.3.2: Tipos de homomorfismos

- Un endomorfismo es un homomorfismo de un anillo en sí mismo.
- Un isomorfismo es un homomorfismo biyectivo.
- Un automorfismo es un isomorfismo de un anillo en sí mismo.

Example 2.3.3

Si $B = \{0\}$ entonces la aplicación $f(a) = 0_B, \forall a \in A$ es un homomorfismo.

Proposition 2.3.4: Propiedades básicas

Sea $f : A \to B$ un homomorfismo de anillos. Entonces para todo $a, b, a_1, \ldots, a_n \in A$ se verifica:

1. $f(0_A) = 0_B$
2. $f(-a) = -f(a)$
3. $f(a - b) = f(a) - f(b)$
4. $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$
5. $f(na) = nf(a)$ para todo $n \in \mathbb{Z}$
6. Si a es invertible en A, entonces $f(a)$ es invertible en B y $f(a^{-1}) = f(a)^{-1}$
7. $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$

Proof

Demostremos algunas de estas propiedades:

- Para (1): $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, luego por cancelación en B, $f(0_A) = 0_B$.
- Para (2): $f(a) + f(-a) = f(a + (-a)) = f(0_A) = 0_B$, luego $f(-a) = -f(a)$.
- Para (6): Si a es invertible, $aa^{-1} = 1_A$, luego $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$, por tanto $f(a^{-1}) = f(a)^{-1}$.

Definition 2.3.5: Núcleo e imagen

Sea $f : A \to B$ un homomorfismo de anillos. Definimos:

- El núcleo de f: $\ker f = \{a \in A : f(a) = 0_B\}$
- La imagen de f: $\text{Im } f = \{f(a) \in B : a \in A\}$

Proposition 2.3.6: Propiedades del núcleo e imagen

Sea $f : A \to B$ un homomorfismo de anillos. Entonces:

1. $\ker f$ es un ideal de A
2. $\text{Im } f$ es un subanillo de B
3. f es inyectivo si y solo si $\ker f = \{0_A\}$
4. f es suprayectivo si y solo si $\text{Im } f = B$

Proof

1. Para ver que $\ker f$ es un ideal:
   - $0_A \in \ker f$ pues $f(0_A) = 0_B$
   - Si $x, y \in \ker f$, entonces $f(x+y) = f(x)+f(y) = 0_B+0_B = 0_B$, luego $x+y \in \ker f$
   - Si $x \in \ker f$ y $a \in A$, entonces $f(ax) = f(a)f(x) = f(a) \cdot 0_B = 0_B$, luego $ax \in \ker f$
2. Para la inyectividad: si f es inyectivo y $x \in \ker f$, entonces $f(x) = 0_B = f(0_A)$, luego $x = 0_A$. Recíprocamente, si $\ker f = \{0_A\}$ y $f(a) = f(b)$, entonces $f(a - b) = 0_B$, luego $a - b \in \ker f = \{0_A\}$, por tanto $a = b$.

2.3.1 Ejemplos importantes de homomorfismos

Example 2.3.7: Homomorfismo inclusión

Si B es un subanillo de A, la aplicación inclusión $i : B \hookrightarrow A$ dada por $i(b) = b$ es un homomorfismo inyectivo.

Example 2.3.8: Homomorfismo proyección

Si I es un ideal de A, la proyección canónica $\pi : A \to A/I$ dada por $\pi(a) = a + I$ es un homomorfismo suprayectivo con $\ker \pi = I$.

Example 2.3.9: Homomorfismo de sustitución

Sea A un anillo y $b \in A$. La aplicación $\varphi_b : A[X] \to A$ dada por:

$$\varphi_b(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1b + \cdots + a_nb^n$$

es un homomorfismo suprayectivo llamado homomorfismo de sustitución en b.

Example 2.3.10: Homomorfismo único $\mathbb{Z} \to A$

Para cualquier anillo A, existe un único homomorfismo $f : \mathbb{Z} \to A$ dado por $f(n) = n \cdot 1_A$. Este homomorfismo está determinado por la característica del anillo A.

Example 2.3.11: Conjugación en $\mathbb{C}$

La conjugación compleja $f : \mathbb{C} \to \mathbb{C}$ dada por $f(a + bi) = a - bi$ es un automorfismo de $\mathbb{C}$.

2.3.2 Propiedades de preservación

Proposition 2.3.12: Preservación de subestructuras

Sea $f : A \to B$ un homomorfismo de anillos.

1. Si A_1 es un subanillo de A, entonces $f(A_1)$ es un subanillo de B
2. Si B_1 es un subanillo de B, entonces $f^{-1}(B_1)$ es un subanillo de A
3. Si I es un ideal de B, entonces $f^{-1}(I)$ es un ideal de A

Remark. ¡Cuidado! La imagen de un ideal por un homomorfismo no necesariamente es un ideal, a menos que el homomorfismo sea suprayectivo.

Example 2.3.13: Contraejemplo

Sea $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ la inclusión. El conjunto $2\mathbb{Z}$ es un ideal de $\mathbb{Z}$, pero $i(2\mathbb{Z}) = 2\mathbb{Z}$ no es un ideal de $\mathbb{Q}$, pues por ejemplo $1 \in \mathbb{Q}$ y $2 \in 2\mathbb{Z}$, pero $1 \cdot 2 = 2 \notin 2\mathbb{Z}$ en $\mathbb{Q}$.

2.3.3 Composición y propiedades funtoriales

Proposition 2.3.14: Composición de homomorfismos

Si $f : A \to B$ y $g : B \to C$ son homomorfismos de anillos, entonces la composición $g \circ f : A \to C$ es un homomorfismo de anillos.

Proof

Queda como ejercicio.

Proposition 2.3.15: Propiedades de isomorfismos

1. La composición de isomorfismos es un isomorfismo.
2. Si $f : A \to B$ es un isomorfismo, entonces $f^{-1} : B \to A$ es un isomorfismo.
3. La relación «ser isomorfo» es una relación de equivalencia en la clase de todos los anillos.

Proof

Queda como ejercicio.

2.3.4 Homomorfismos y productos

Theorem 2.3.16: Homomorfismos en productos

Sean A, B, C anillos. Existe una biyección natural:

$$\mathrm{Hom}(A, B \times C) \cong \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, C)$$

dada por $f \mapsto (\pi_B \circ f, \pi_C \circ f)$, donde π_B y π_C son las proyecciones canónicas.

Example 2.3.17: Aplicación

Para determinar todos los homomorfismos $f : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$, basta determinar los homomorfismos $\mathbb{Z} \to \mathbb{Z}_2$ y $\mathbb{Z} \to \mathbb{Z}_3$ por separado.

2.4 Ideales y anillos cociente

Definition 2.4.1: Ideal

Un subconjunto I de un anillo A es un ideal si:

1. $I \neq \emptyset$
2. Para todo $x, y \in I$, se verifica que $x + y \in I$
3. Para todo $x \in I$ y $a \in A$, se verifica que $ax \in I$

Remark.

- *La condición* $I \neq \emptyset$ *puede sustituirse por* $0 \in I$, *ya que si* $a \in I$ *entonces* $0 = a + (-1)a \in I$
- *Si* I *es un ideal de* A, *entonces para todo* $a_1, \ldots, a_n \in A$ *y* $x_1, \ldots, x_n \in I$ *se tiene que* $\sum_{i=1}^{n} a_i x_i \in I$

Example 2.4.2: Ideales triviales

- El ideal cero: $\{0\}$
- El ideal impropio: A

Example 2.4.3: Ideales principales

Sea A un anillo y $b \in A$. El conjunto:

$$(b) = bA = \{ba : a \in A\}$$

es un ideal de A llamado ideal principal generado por b.
Observaciones:

- $(1) = A$
- $(0) = \{0\}$
- (b) es el menor ideal de A que contiene a b

Para probar esta última afirmación supongamos que I es otro ideal de A tal que $b \in I$. Entonces si $(b) \subset I$ ya que $b \in I$ e I es un ideal, luego $x \in (b) \implies x = ba,\ a \in A \implies x \in I$.

Example 2.4.4: Ideal generado por un conjunto

Sea $T \subseteq A$. El ideal generado por T es:

$$(T) = \left\{ \sum_{i=1}^{n} a_i t_i : n \geq 0, a_i \in A, t_i \in T \right\}$$

Este es el menor ideal de A que contiene a T.

Example 2.4.5: Ideales en anillos producto

Si A y B son anillos, entonces $A \times \{0\} = \{(a, 0) : a \in A\}$ es un ideal de $A \times B$.

Proof

Claramente es no vacío. Si $x, y \in A \times \{0\}$ entonces

$$x = (a, 0),\ y = (b, 0) \implies x + y = (a + b, 0) \in A \times \{0\}.$$

Si $(a', b') \in A \times B$ entonces

$$(a', b')x = (aa', 0) \in A \times \{0\}.$$

Example 2.4.6: Ideales en anillos de polinomios

Sea $A[X]$ el anillo de polinomios.

- $I = \{a_1 X + \cdots + a_n X^n : a_i \in A\}$ (polinomios sin término constante) es un ideal
- Si I es ideal de A, entonces $J = \{a_0 + a_1 X + \cdots + a_n X^n : a_0 \in I\}$ es un ideal de $A[X]$
- $I[X] = \{a_0 + a_1 X + \cdots + a_n X^n : a_i \in I\}$ es un ideal de $A[X]$

Proposition 2.4.7: Intersección de ideales

La intersección de cualquier familia de ideales de A es un ideal de A.

Proof

Si I_α es una familia de ideales y $J = \cap_{\alpha \in X} I_\alpha$ entonces $0 \in J \implies J \neq \emptyset$. Además, para todo indice α

$$x, y \in J \implies x + y \in I_\alpha \implies x + y \in J$$

y para cualquier $a \in A$

$$x \in J \implies ax \in I_\alpha \implies ax \in J.$$

Proposition 2.4.8: Ideales de $\mathbb{Z}$

Todos los ideales de $\mathbb{Z}$ son principales. Es decir, para todo ideal $I \subset \mathbb{Z}$, existe $n \in \mathbb{Z}$ tal que $I = (n)$.

Proof

Sea I un ideal de $\mathbb{Z}$. Si $I = 0$ entonces $I = (0)$ con lo que I es principal. Supongamos que $I \neq 0$ y sea $n \in I \setminus 0$. Entonces $-n \in I$, con lo que I tiene un elemento positivo, o sea $I \cap \mathbb{N} \neq \emptyset$. Como $\mathbb{N}$ está bien ordenado, $I \cap \mathbb{N}$ tiene un mínimo que denotamos como a. Como $a \in I$ se tiene que $(a) \subseteq I$.
Para ver que se da la igualdad tomamos $b \in I$ y sean q y r el cociente y el resto de la división entera de b entre a. Entonces $b = qa + r$ y $0 \leq r < a$. Pero $r = b - qa \in I$, por que I es un ideal de $\mathbb{Z}$ que contiene a a y b y $q \in \mathbb{Z}$. Como r es estrictamente menor que a y a es mínimo en $I \cap \mathbb{N}$, necesariamente $r \notin \mathbb{N}$, es decir r no es positivo. Luego $r = 0$, con lo que $b = qa \in (a)$.

Definition 2.4.9: Congruencia módulo un ideal

Sea I un ideal de un anillo A. Decimos que $a, b \in A$ son congruentes módulo I, y escribimos $a \equiv b \pmod{I}$, si $b - a \in I$.

Lemma 2.4.10: Propiedades de la congruencia

Sea I ideal de A. Para todo $a, b, c, d \in A$:

1. $a \equiv a \pmod{I}$ (reflexiva).
2. Si $a \equiv b \pmod{I}$, entonces $b \equiv a \pmod{I}$ (simétrica).
3. Si $a \equiv b \pmod{I}$ y $b \equiv c \pmod{I}$, entonces $a \equiv c \pmod{I}$ (transitiva).
4. $a \equiv b \pmod{(0)}$ si y solo si $a = b$.

Proof

1. Como $0 \in A$, dado $x \in I$ debe ser $0x = 0 \in I$, luego $a - a = 0 \in I \implies a \equiv a \pmod{I}$.
2. Si $a \equiv b \pmod{I}$, entonces
$$b - a \in I \implies (-1)(b - a) = a - b \in I \implies b \equiv A \pmod{I}.$$
3. Si $a \equiv b \pmod{I}$ y $b \equiv c \pmod{I}$, entonces
$$b - a \in I, c - b \in I \implies c - a \in I \implies a \equiv c \pmod{I}.$$
4. $a \equiv b \pmod{(0)} \iff b - a = 0 \iff a = b$.

Del Lema 2.4.10 se deduce que la relación «ser congruente módulo I» es una relación de equivalencia en A y, por tanto, las clases de equivalencia por esta relación definen una partición de A.

La clase de equivalencia que contiene a un elemento $a \in A$ es

$$a + I = \{a + x : x \in I\}$$

(en particular $0 + I = I$), de modo que

$$a + I = b + I \Leftrightarrow a \equiv b \pmod{I}$$

(en particular $a + I = 0 + I \Leftrightarrow a \in I$).

El conjunto de las clases de equivalencia se denota

$$A/I = \frac{A}{I} = \{a + I : a \in A\}.$$

Definition 2.4.11: Anillo cociente

Sea I un ideal de A. El conjunto de clases de equivalencia:

$$A/I = \{a + I : a \in A\}$$

con las operaciones:

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (ab) + I$$

es un anillo llamado anillo cociente de A módulo I.

Proposition 2.4.12: Buena definición del cociente

Las operaciones en A/I están bien definidas y dotan a A/I de estructura de anillo con:

- Elemento cero: $0 + I$
- Elemento uno: $1 + I$

Proof

Sean $a + I = a' + I$ y $b + I = b' + I$. Entonces $a - a', b - b' \in I$. Luego:

- $(a + b) - (a' + b') = (a - a') + (b - b') \in I$
- $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I$

Por tanto las operaciones están bien definidas.

Definition 2.4.13: Proyección canónica

La aplicación $\eta : A \to A/I$ dada por $\eta(a) = a + I$ es un homomorfismo sobreyectivo llamado proyección canónica.

Proof

Que la proyección es sobreyectiva es inmediato, dado $a + I \in A/I$ es inmediato que $\eta(a) = a + I$.

Example 2.4.14: Anillos $\mathbb{Z}_n$

Para $n > 0$, $\mathbb{Z}_n = \mathbb{Z}/(n)$ es el anillo cociente. Tiene exactamente n elementos: $0 + (n), 1 + (n), \ldots, (n-1) + (n)$.

Example 2.4.15: Cocientes triviales

- $A/\{0\} \cong A$
- $A/A \cong \{0\}$

Example 2.4.16: Cociente por ideales en polinomios

Sea $I = \{a_1X + \cdots + a_nX^n\} \subseteq A[X]$ (polinomios sin término constante). Entonces:

$$A[X]/I \cong A$$

mediante el isomorfismo que envía $P(X) + I$ al término constante de P.

Example 2.4.17: Cociente en productos

Sean A, B anillos, $I = A \times \{0\}$. Entonces:

$$(A \times B)/I \cong B$$

2.4.1 Caracterización de ideales maximales

Lemma 2.4.18: Caracterización de ideales impropios

Sea A un anillo. Para un ideal $I \subseteq A$, las siguientes condiciones son equivalentes:

1. $I = A$ (ideal impropio)
2. $1 \in I$
3. I contiene una unidad de A (i.e., $I \cap A^* \neq \emptyset$)

Proof

- (1) $\Rightarrow$ (2): si $I = A$, entonces $1 \in I$
- (2) $\Rightarrow$ (3): 1 es una unidad
- (3) $\Rightarrow$ (1): si $u \in I \cap A^*$, entonces $1 = uu^{-1} \in I$, luego $I = A$

2.4.2 Núcleo y teorema de correspondencia

Definition 2.4.19: Núcleo de un homomorfismo

Sea $f : A \to B$ un homomorfismo de anillos. El núcleo de f es:

$$\ker f = \{a \in A : f(a) = 0\}$$

Proposition 2.4.20: Inyectividad y núcleo

Un homomorfismo $f : A \to B$ es inyectivo si y solo si $\ker f = \{0\}$.

Proof

- Si f es inyectivo y $a \in \ker f$, entonces $f(a) = 0 = f(0)$, luego $a = 0$
- Si $\ker f = \{0\}$ y $f(a) = f(b)$, entonces $f(a-b) = 0$, luego $a - b \in \ker f = \{0\}$, por tanto $a = b$

Theorem 2.4.21: Teorema de correspondencia

Sea I un ideal de un anillo A. Las asignaciones:

$$J \mapsto J/I$$
$$X \mapsto \pi^{-1}(X)$$

definen biyecciones (una inversa de la otra) que preservan la inclusión entre:

- El conjunto de ideales de A que contienen a I
- El conjunto de todos los ideales de A/I

Proof

Basta verificar:

- Si J es ideal de A con $I \subseteq J$, entonces J/I es ideal de A/I y $\pi^{-1}(J/I) = J$
- Si X es ideal de A/I, entonces $\pi^{-1}(X)$ es ideal de A que contiene a I y $\pi^{-1}(X)/I = X$
- Las asignaciones preservan inclusiones

Example 2.4.22: Aplicación del teorema de correspondencia

En $\mathbb{Z}_n = \mathbb{Z}/(n)$, los ideales son de la forma $d\mathbb{Z}_n = (d)/(n)$ donde $d \mid n$. Además, $d\mathbb{Z}_n \subseteq d'\mathbb{Z}_n$ si y solo si $d' \mid d$.

2.5 Operaciones con ideales

Definition 2.5.1: Suma de ideales

Si I y J son ideales de A, su suma es:

$$I + J = \{x + y : x \in I, y \in J\}$$

Definition 2.5.2: Producto de ideales

Si I y J son ideales de A, su producto es:

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J, n \geq 0 \right\}$$

Remark. Más generalmente, para ideales $I_1, \ldots, I_n$*:*

- $I_1 + \cdots + I_n = \{x_1 + \cdots + x_n : x_i \in I_i\}$
- $I_1 \cdots I_n$ *está generado por productos* $x_1 \cdots x_n$ *con* $x_i \in I_i$

Proposition 2.5.3: Propiedades de las operaciones

Para ideales I, J, K de A:

1. $IJ \subseteq I \cap J$
2. $I(J \cap K) \subseteq IJ \cap IK$
3. $I(JK) = (IJ)K$
4. $I(J + K) = IJ + IK$
5. $IA = I$

Proof

Ejercicio.

Example 2.5.4: Operaciones en $\mathbb{Z}$

Sean (n) y (m) ideales de $\mathbb{Z}$. Entonces:

$$(n)(m) = (nm)$$
$$(n) \cap (m) = (\text{mcm}(n, m))$$
$$(n) + (m) = (\text{mcd}(n, m))$$

Example 2.5.5: Ideal no principal

En $\mathbb{Z}[X]$, el ideal $(2) + (X)$ (polinomios con término constante par) no es principal.

Proof

Supongamos que $(2) + (X) = (a)$ para algún $a \in \mathbb{Z}[X]$. Entonces:

- $2 = ab$ para algún b, luego $a \in \mathbb{Z}$
- Como $a \in (2, X)$, debe ser a par
- Pero entonces $X \notin (a)$, contradicción

2.5.1 Ideales primos y maximales

Definition 2.5.6: Ideal primo

Un ideal $P \subsetneq A$ es primo si para todo $a, b \in A$:

$$ab \in P \Rightarrow a \in P \text{ o } b \in P$$

Definition 2.5.7: Ideal maximal

Un ideal $M \subsetneq A$ es maximal si no existe ningún ideal I tal que $M \subsetneq I \subsetneq A$.

Lemma 2.5.8: Caracterizaciones

1. P es primo si y solo si A/P es un dominio de integridad
2. M es maximal si y solo si A/M es un cuerpo
3. Todo ideal maximal es primo

Example 2.5.9: Ejemplos en $\mathbb{Z}$

- Los ideales primos de $\mathbb{Z}$ son (0) y (p) con p primo
- Los ideales maximales de $\mathbb{Z}$ son (p) con p primo

2.6 Teoremas de isomorfía

Theorem 2.6.1: Primer teorema de isomorfía

Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un isomorfismo:

$$A/\ker f \cong \operatorname{Im} f$$

Theorem 2.6.2: Segundo teorema de isomorfía

Sea A un anillo y $I \subseteq J$ ideales de A. Entonces:

$$\frac{A/I}{J/I} \cong \frac{A}{J}$$

Theorem 2.6.3: Tercer teorema de isomorfía

Sea A un anillo, B un subanillo de A e I un ideal de A. Entonces:

$$\frac{B}{B \cap I} \cong \frac{B + I}{I}$$

Theorem 2.6.4: Teorema chino de los restos

Sea A un anillo y $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces:

$$\frac{A}{I_1 \cap \cdots \cap I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$$

Appendix A

Teoría de conjuntos

A.1 Conjuntos y clases

Introducimos de manera informal en esta sección la teoría de conjuntos de von Neumann-Bernays-Gödel (denotada NBG). Para más información consultar **[?]**. Las nociones primitivas en esta teoría son las de clase, pertenencia e igualdad. Intuitivamente consideramos que una clase es una colección A de objetos tal que dado un objeto cualquiera x podemos determinar si este pertenece a la clase ($x \in A$) o no ($x \notin A$).

Los axiomas de la teoría se formulan en terminos de estas nociones primitivas y del cálculo de predicados lógicos de primer orden (es decir, las afirmaciones construidas usando conectores de tipo *y, o, negación, implica*, y cuantificadores $\forall, \exists$). Por ejemplo, se asume que la igualdad tiene las siguientes propiedades para cualesquiera clases A, B, C:

$$A = A, \quad A = B \implies B = A, \quad (A = B) \wedge (B = C) \implies A = C, \quad (A = B) \wedge (x \in A) \implies x \in B.$$

Por otro lado, el **axioma de extensionalidad** afirma que dos clases con los mismos elementos son iguales:

$$(x \in A \iff x \in B) \implies A = B.$$

Una clase A es un conjunto si y solo si existe una clase B tal que $A \in B$. Por tanto, un conjunto es un tipo particular de clase. Una clase que no es un conjunto se llama una clase propia. Informalmente un conjunto es una clase «pequeña», mientras que una clase propia es «grande». El **axioma de formación** de clases asegura que para cualquier enunciado $P(y)$ de primer orden involucrando a la variable y existe una clase A tal que

$$x \in A \iff (x \text{ es un conjunto} \wedge x \text{ es verdadero})$$

en tal caso denotamos a la clase A como $\{x : P(x)\}$, llamada clase de todos los x tal que se cumple $P(x)$. En ocasiones podemos describir una clase listando sus elementos: $\{a, b, c\}$.

Example A.1.1: C

nsideremos la clase $M = \{X : X \text{ es un conjunto y } X \notin X\}$. La afirmación $X \notin X$ tiene sentido como predicado, de hecho muchos conjuntos la satisfacen (por ejemplo, el conjunto de todos los libros no es un libro). Veamos que M es una clase propia. En efecto, si M fuera un conjunto, entonces tendríamos que $M \in M$ o $M \notin M$. Pero por la definición de M, $M \in M$ implica $M \notin M$ y $M \notin M$ implica $M \in M$. Así, en ambos casos, la suposición de que M es un conjunto lleva a una contradicción: $M \in M$ y $M \notin M$.

Una clase A es una subclase de una clase B, $A \subset B$ si

$$\forall x \in A, x \in A \implies x \in B$$

por el axioma de extensionalidad y las propiedades de la igualdad tenemos

$$A = B \iff (A \subset B) \wedge (B \subset A).$$

Una subclase A de un conjunto B es un conjunto en sí misma, y en tal caso decimos que es un subconjunto.

El conjunto vacío $\emptyset$ es el conjunto sin elementos, es decir, $\forall x, x \notin \emptyset$. Como la afirmación $x \in \emptyset$ es siempre falsa tenemos de manera trivial que $\emptyset \subset B$ para cualquier clase B. Se dice entonces que A es una subclase propia de B si $A \subset B$ pero $A \neq \emptyset, A \neq B$.

El **axioma de partes** establece que para cualquier conjunto A la clase $\mathcal{P}(A)$ de todos sus subconjuntos es ella misma un conjunto, que usualmente llamamos las partes de A.

A.2 Uniones, intersecciones, complementos

Una familia de conjuntos indexada por una clase (no vacía) I es una colección de conjuntos $\{A_i : i \in I\}$. Dada una familia su unión e intersección son las clases:

$$\cup_{i\in I} A_i = \{x : x \in A_i \text{ para algún } i \in I\}$$
$$\cap_{i\in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}$$

Si I es un conjunto entonces las construcciones anteriores son conjuntos.

Si A y B son clases su diferencia es la subclase de B

$$B \setminus A = \{x : x \in B, x \notin A\}.$$

A.3 Aplicaciones

Dadas dos clases A, B la definición de aplicación es idéntica a la ya conocida para conjuntos. Se dan por conocidos los conceptos ya conocidos de dominio, rango, restricciones, etc. Dos aplicaciones son iguales si tienen el mismo dominio, rango y asignan el mismo valor a cada elemento de su dominio común.

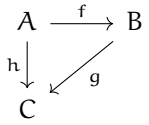
Dada una clase A la aplicación identidad en A (denotada $1_A : A \to A$) es la aplicación dada por $a \mapsto a$. Si $S \subseteq A$, la aplicación $1_A|_S : S \to A$ se llama la aplicación inclusión de S en A.

Sean $f : A \to B$ y $g : B \to C$ aplicaciones. La composición de f y g es la aplicación $A \to C$ dada por

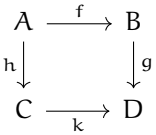
$$a \mapsto g(f(a)), \quad a \in A.$$

La aplicación compuesta se denota $g \circ f$ o simplemente gf. Si $h : C \to D$ es una tercera aplicación, es fácil verificar que $h(gf) = (hg)f$. Si $f : A \to B$, entonces $f \circ 1_A = f = 1_B \circ f : A \to B$.

Un diagrama:



se dice que es conmutativo si $gf = h$. De manera similar, el diagrama:



es conmutativo si $kh = gf$. Frecuentemente se trabaja con diagramas más complicados compuestos por varios triángulos y cuadrados como los anteriores. Tal diagrama se dice conmutativo si todo triángulo y cuadrado en él es conmutativo.

Las nociones de inyectividad y sobreyectividad son las usuales. Una aplicación $f : A \to B$ se dice inyectiva si

$$\forall a, a' \in A, \quad a \neq a' \implies f(a) \neq f(a').$$

Una aplicación f es sobreyectiva si $f(A) = B$; es decir,

$$\forall b \in B, \quad b = f(a) \text{ para algún } a \in A.$$

Una aplicación f se dice biyectiva si es a la vez inyectiva y sobreyectiva. Se sigue inmediatamente de estas definiciones que, para cualquier clase A, la aplicación identidad $1_A : A \to A$ es biyectiva.

Enunciamos ahora el siguiente teorema que permite caracterizar las nociones anteriores en aplicación de inversas por la derecha e izquierda.

Theorem A.3.1

Sea $f : A \to B$ una aplicación, con $A \neq \emptyset$.

1. f es inyectiva si y solo si existe una aplicación $g : B \to A$ tal que $gf = 1_A$.
2. Si A es un conjunto, entonces f es sobreyectiva si y solo si existe una aplicación $h : B \to A$ tal que $fh = 1_B$.

La aplicación g del teorema anterior se llama una inversa por la izquierda de f, y h se llama una inversa por la derecha de f. Si una aplicación $f : A \to B$ tiene inversas por ambos lados entonces

$$g = g1_B = g(fh) = (gf)h = 1_A h = h$$

y la aplicación $g = h$ se llama la inversa de f. Este argumento también muestra que la inversa de una aplicación (si existe) es única. Por el Teorema A.3.1, si A es un conjunto y $f : A \to B$ una aplicación, entonces

$$f \text{ es biyectiva} \iff f \text{ tiene inversa por ambos lados}$$

La única inversa de una biyección f se denota f^{-1}; claramente f es una inversa de f^{-1}, por lo que f^{-1} también es una biyección.

Remark. La caracterización de biyectividad como existencia de una inversa es válida incluso cuando A es una clase propia

A.4 Relaciones

El **axioma de formación de pares** establece que para dos conjuntos (elementos) a, b, existe un conjunto $P = \{a, b\}$ tal que $x \in P$ si y solo si $x = a$ o $x = b$; si $a = b$, entonces P es el conjunto unitario $\{a\}$. El par ordenado (a, b) se define como el conjunto $\{\{a\}, \{a, b\}\}$; su primera componente es a y su segunda componente es b. Es fácil verificar que $(a, b) = (a', b')$ si y solo si $a = a'$ y $b = b'$. El producto cartesiano de las clases A y B es la clase

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Nótese que $A \times \emptyset = \emptyset = \emptyset \times B$.

Una subclase R de $A \times B$ se llama una relación en $A \times B$. Por ejemplo, si $f : A \to B$ es una aplicación, el grafo de f es la relación $R = \{(a, f(a)) : a \in A\}$. Como f es una aplicación, R tiene la propiedad especial:

$$\text{cada elemento de } A \text{ es la primera componente de uno y solo un par ordenado en } R. \qquad (*)$$

Recíprocamente, cualquier relación R en $A \times B$ que satisfaga $(*)$ determina una única aplicación $f : A \to B$ cuyo grafo es R (definiendo $f(a) = b$, donde (a, b) es el único par ordenado en R

con primera componente a). Por esta razón es habitual identificar una aplicación con su grafo, es decir, definir una aplicación como una relación que satisface $(*)$.

Otra ventaja de este enfoque es que permite definir funciones con dominio vacío. Dado que $\emptyset \times B = \emptyset$ es el único subconjunto de $\emptyset \times B$ y satisface trivialmente $(*)$, existe una única aplicación $\emptyset \to B$. También es claro por $(*)$ que solo puede haber una aplicación con rango vacío si el dominio también es vacío.

A.5 Productos

En esta sección solo tratamos con conjuntos. No hay clases propias involucradas.

Consideremos el producto cartesiano de dos conjuntos $A_1 \times A_2$. Un elemento de $A_1 \times A_2$ es un par (a_1, a_2) con $a_i \in A_i$, $i = 1, 2$. Así, el par (a_1, a_2) determina una aplicación $f : \{1, 2\} \to A_1 \cup A_2$ mediante: $f(1) = a_1$, $f(2) = a_2$. Recíprocamente, toda aplicación $f : \{1, 2\} \to A_1 \cup A_2$ con la propiedad de que $f(1) \in A_1$ y $f(2) \in A_2$ determina un elemento $(a_1, a_2) = (f(1), f(2))$ de $A_1 \times A_2$. Por lo tanto, no es difícil ver que hay una correspondencia biyectiva entre el conjunto de todas las aplicaciones de este tipo y el conjunto $A_1 \times A_2$. Este hecho nos lleva a generalizar la noción de producto cartesiano como sigue.

Definition A.5.1: Producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por un conjunto (no vacío) I. El producto (cartesiano) de los conjuntos A_i es el conjunto de todas las aplicaciones $f : I \to \bigcup_{i \in I} A_i$ tales que $f(i) \in A_i$ para todo $i \in I$. Se denota $\prod_{i \in I} A_i$.

Si $I = \{1, 2, \ldots, n\}$, el producto $\prod_{i \in I} A_i$ a menudo se denota por $A_1 \times A_2 \times \cdots \times A_n$ y se identifica con el conjunto de todas las n-tuplas ordenadas $(a_1, a_2, \ldots, a_n)$, donde $a_i \in A_i$ para $i = 1, 2, \ldots, n$, como en el caso mencionado anteriormente donde $I = \{1, 2\}$. Una notación similar es a menudo conveniente cuando I es infinito. A veces denotaremos la aplicación $f \in \prod_{i \in I} A_i$ por $(a_i)_{i \in I}$ o simplemente (a_i), donde $f(i) = a_i \in A_i$ para cada $i \in I$.

Si algún $A_i = \emptyset$, entonces $\prod_{i \in I} A_i = \emptyset$, ya que no puede haber una aplicación $f : I \to \bigcup A_i$ tal que $f(i) \in A_i$. Si $\{A_i : i \in I\}$ y $\{B_i : i \in I\}$ son familias de conjuntos tales que $B_i \subset A_i$ para cada $i \in I$, entonces toda aplicación $I \to \bigcup B_i$ puede considerarse como una aplicación $I \to \bigcup_{i \in I} A_i$. Por lo tanto, consideramos $\prod_{i \in I} B_i$ como un subconjunto de $\prod_{i \in I} A_i$.

A.5.1 Caracterización del producto

Sea $\prod_{i \in I} A_i$ un producto cartesiano. Para cada $k \in I$, definamos una aplicación $\pi_k : \prod_{i \in I} A_i \to A_k$ mediante $f \mapsto f(k)$, o en la otra notación, $(a_i) \mapsto a_k$. π_k se llama la proyección canónica del producto sobre su k-ésima componente. Se deja como ejercicio probar que si cada A_i es no vacío, entonces cada π_k es sobreyectiva.

El producto $\prod_{i \in I} A_i$ y sus proyecciones son precisamente lo que necesitamos para el siguiente teorema

Theorem A.5.2: Propiedad universal del producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por I. Entonces existe un conjunto D, junto con una familia de aplicaciones $\{\pi_i : D \to A_i : i \in I\}$, con la siguiente propiedad: para cualquier conjunto C y familia de aplicaciones $\{\varphi_i : C \to A_i : i \in I\}$, existe una única aplicación $\varphi : C \to D$ tal que $\pi_i \varphi = \varphi_i$ para todo $i \in I$. Además, D está determinado de manera única salvo biyección.

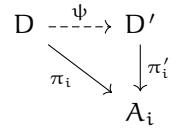
La última frase significa que si D' es un conjunto y $\{\pi_i' : D' \to A_i : i \in I\}$ una familia de aplicaciones que tienen la misma propiedad que D y $\{\pi_i\}$, entonces existe una biyección $D \to D'$.

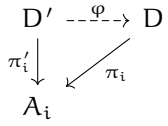
(Existencia) Sea $D = \prod_{i \in I} A_i$ y sean las aplicaciones π_i las proyecciones sobre las i-ésimas componentes. Dado C y las aplicaciones φ_i, definamos $\varphi : C \to \prod_{i \in I} A_i$ por $c \mapsto f_c$, donde $f_c(i) = \varphi_i(c) \in A_i$. Se sigue inmediatamente que $\pi_i \varphi = \varphi_i$ para todo $i \in I$. Para mostrar que φ es única, supongamos que $\varphi' : C \to \prod_{i \in I} A_i$ es otra aplicación tal que $\pi_i \varphi' = \varphi_i$ para todo $i \in I$ y demostremos que $\varphi = \varphi'$. Para ello, debemos mostrar que para cada $c \in C$, $\varphi(c)$ y $\varphi'(c)$ son el mismo elemento de $\prod_{i \in I} A_i$, es decir, $\varphi(c)$ y $\varphi'(c)$ coinciden como funciones en I: $(\varphi(c))(i) = (\varphi'(c))(i)$ para todo $i \in I$. Pero por hipótesis y la definición de π_i, tenemos para todo

$i \in I$:

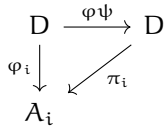
$$(\varphi'(c))(i) = \pi_i \varphi'(c) = \varphi_i(c) = f_c(i) = (\varphi(c))(i).$$

(Unicidad) Supongamos que D' (con aplicaciones $\pi'_i : D' \to A_i$) tiene la misma propiedad que $D = \prod_{i \in I} A_i$. Si aplicamos esta propiedad (para D) a la familia de aplicaciones $\{\pi'_i : D' \to A_i\}$ y también la aplicamos (para D') a la familia $\{\pi_i : D \to A_i\}$, obtenemos (únicas) aplicaciones $\varphi : D' \to D$ y $\psi : D \to D'$ tales que los siguientes diagramas son conmutativos para cada $i \in I$:





Combinando estos, obtenemos para cada $i \in I$ un diagrama conmutativo:



Así, $\varphi\psi : D \to D$ es una aplicación tal que $\pi_i(\varphi\psi) = \pi_i$ para todo $i \in I$. Pero por la demostración anterior, hay una única aplicación con esta propiedad. Como la aplicación $1_D : D \to D$ también satisface $\pi_i 1_D = \pi_i$ para todo $i \in I$, debemos tener $\varphi\psi = 1_D$ por unicidad. Un argumento similar muestra que $\psi\varphi = 1_D$. Por lo tanto, φ es una biyección por (13), y $D = \prod_{i \in I} A_i$ está determinado de manera única salvo biyección.

Nótese que el enunciado del Teorema A.5.2 no menciona elementos; involucra solo conjuntos y aplicaciones. Establece que el producto $\prod_{i \in I} A_i$ se caracteriza por una cierta propiedad universal que cumplen todas las aplicaciones. Esta propiedad se resume en el siguiente diagrama conmutativo: