Grupos, anillos y cuerpos

Manuel Palacios

Departamento de Matemática Aplicada

Centro Politécnico Superior

Universidad de Zaragoza *

Otoño 2002

Contents

References

[1] Merino, L. y Santos, E.: Algebra lineal con métodos elementales. *Ed. Los autores*, Universidad de Granada. 1997.

[2] Burgos (de), J.: Curso de Algebra y Geometría. *Alhambra*.

[3] Burgos, J. de: Algebra lineal. *McGraw-Hill*. 1993.

[4] Smirnov, V.: Cours de Mathématiques Superieurs; tome III. *Mir*.

[5] Gutiérrez Gómez, A. y García Castro, F.: Algebra lineal 2. *Pirámide*.

[6] García, J. y López Pellicer, M.: Algebra lineal y Geometría. *Marfil*.

[7] Castellet, M. y Llerena, I.: Algebra lineal y Geometría. *Reverté*, 1992.

[8] Anzola y Caruncho: Problemas de Algebra, tomos I y II. *Ed. los autores*.

*e-mail: mpala@posta.unizar.es

1 Grupos

Vamos a introducir el concepto de grupo proponiendo en primer lugar varios ejemplos.

Ejemplo 1 *El conjunto de las rotaciones del espacio ordinario de ángulo ϕ y eje Oz, que denotamos por R(Oz,ϕ) $\phi \in [0, 2\Pi]$.*

Las ecuaciones que describen uno cualquiera de estos giros son

$$x' = x\cos\phi - y\,\mathrm{sen}\,\phi$$
$$y' = x\,\mathrm{sen}\,\phi + y\cos\phi$$

si (x,y) son las coordenadas de un punto del plano Oxy y (x',y') son las coordenadas del punto imagen.

Podemos introducir la siguiente notación para designar el giro y su matriz 2x2 asociada

$$Z_\phi, \qquad M_\phi = \begin{pmatrix} \cos\phi & -\,\mathrm{sen}\,\phi \\ \mathrm{sen}\,\phi & \cos\phi \end{pmatrix}$$

y la operación de composición de giros definida por

$$Z_\phi * Z_{\phi'} = Z_{\phi+\phi'}$$

que se puede escribir, en términos de las matrices asociadas, como producto de éstas

$$M_\phi M_{\phi'} = M_{\phi+\phi'}$$

como podemos comprobar fácilmente.

Observamos que se verifican las siguientes propiedades fundamentales:

1) El producto de dos giros es otro giro, es decir,

$$Z_\phi * Z_{\phi'} \in R(Oz, \phi)$$

2) El producto de tres giros se puede expresar de dos formas equivalentes

$$(Z_\phi * Z_{\phi'}) * Z_{\phi''} = Z_\phi * (Z_{\phi'} * Z_{\phi''})$$

3) Existe un giro neutro (que no modifica los puntos del espacio), éste es

$$Z_0$$

4) Para cada giro Z_ϕ podemos encontrar otro $Z_{\phi'}$ que realiza la maniobra inversa, es decir, el resultado de aplicar los dos sucesivamente es

$$Z_\phi * Z_{\phi'} = Z_0 = Z_{\phi'} * Z_\phi$$

5) El producto de dos giros es independiente del orden en que se aplican, es decir,

$$Z_\phi * Z_{\phi'} = Z_{\phi'} * Z_\phi$$

Otras propiedades de este conjunto relacionadas con la operación definida se demuestran a partir de estas cinco. En general, cuando se verifican estas cinco propiedades, se dice, respectivamente, que:

1) La operación es estable para el conjunto
2) Se verifica la propiedad asociativa
3) Existe un elemento neutro en dicho conjunto
4) Todo elemento del conjunto tiene otro elemento simétrico también del conjunto.
5) Se verifica la propiedad conmutativa.

Ejemplo 2 *El conjunto de todos los giros del ejemplo 1 anterior, cuyo ángulo de giro toma los valores* $0, 2\pi/m, 4\pi/m, ..., 2(m-1)\pi/m$.

Los elementos de este conjunto pueden ser representados como antes.

Veamos ahora la definición abstracta (axiomática) del concepto de grupo.

Definición 3 *Llamaremos grupo al par (G,*) constituido por un conjunto no vacío G y una operación sobre él que verifica las siguientes propiedades:*

*o) * es estable en G, es decir,* $a * b \in G, \forall a, b \in G$

1) asociativa, $(a * b) * c = a * (b * c), \forall a, b, c \in G$

2) existencia de elemento neutro, $e \in G$ *tal que*

$$a * e = e * a = a, \forall a \in G$$

3) existencia de elemento simétrico, $\forall a \in G, \exists b \in G$, *tal que*

$$a * b = b * a = e$$

(el elemento simétrico de a suele denotarse por a' *ó* a^{-1}*).*

Definición 4 *Si todos los elementos del grupo (G,*) verifican la propiedad*

4) conmutativa, $a * b = b * a, \forall a, b \in G$

diremos que el grupo es conmutativo o abeliano.

Si la operación * definida en G es la adición, al elemento neutro se le suele llamar **cero**, 0, y al elemento simétrico de uno a se le llama **elemento opuesto** y se le denota por -a.

Si la operación * es la multiplicación, al elemento neutro se le suele denominar **elemento unidad**, 1, y al simétrico, **elemento inverso** y se le designa por a^{-1}.

Como hemos visto en los ejemplos, un grupo puede tener un número finito de elementos y se dice entonces grupo finito y se llama **orden del grupo** al número de elementos de ese grupo. Si tuviese infinitos elementos se diría **grupo infinito**

Ejemplo 5 *a) (* $\mathbb{Z}$*,+) es un grupo conmutativo*

b) $(Q,+)$ *y* $(Q^*, \cdot)$ *son grupos abelianos*

c) $(\mathbb{R}, +)$ *y* $(\mathbb{R}^*, \cdot)$ *son grupos abelianos*

d) el conjunto $3\ \mathbb{Z} = \{x \in Z | x = 3p, p \in \mathbb{Z}\}$ *es grupo abeliano respecto de la suma.*

e) El conjunto $M_{\mathrm{R}}(2)$ *con la suma es un grupo abeliano.*

Ejemplo 6 *El conjunto O(3) de todos los movimientos (giros y simetrías) que transforman un triángulo equilátero en sí mismo es un grupo no abeliano respecto de la composición de movimientos.*

Ejemplo 7 *El conjunto S (3) de las permutaciones de tres elementos es un grupo no abeliano respecto del producto de permutaciones.*

Pregunta: ¿Qué tienen en común los grupos de los ejemplos 6 y 7?.

Ejercicio 8 *Probar que realmente los ejemplos propuestos en 2,6 y 7 tienen estructura de grupo (abeliano, en su caso).*

Ejercicio 9 *Sea* $F = \{f_i, \quad i = 1, 2, ..., 6\}$ *el conjunto de las aplicaciones biyectivas de* $\mathbb{R}$-$\{0,1\}$ *en sí mismo definidas por* $f_1(x) = x$, $f_2(x) = 1/x$, $f_3(x) = 1 - x$, $f_4(x) = 1/(1-x)$, $f_5(x) = (x-1)/x$, $f_6(x) = x/(x-1)$. *Probar que F tiene estructura de grupo no abeliano con respecto de la operación composición de aplicaciones.*

Solución: En primer lugar, formemos la tabla del grupo:

(En esta tabla el primer elemento de la composición aparece en la primera fila y el segundo en la primera columna)

```
o | f1  f2  f3  f4  f5  f6
f1| f1  f2  f3  f4  f5  f6
f2| f2  f1  f4  f3  f6  f5
f3| f3  f5  f1  f6  f2  f4
f4| f4  f6  f2  f5  f1  f3
f5| f5  f3  f6  f1  f4  f2
f6| f6  f4  f5  f2  f3  f1
```

Observamos ahora que:

0) $\forall f_i, f_k \in F : f_i \, o \, f_k \in F$, luego F es estable

1) la composición de aplicaciones es asociativa (propiedad conocida de las apicaciones).

2) $\exists f_1 \in F$ tal que $\forall f_k \in F : f_1 \, o \, f_k = f_k \, o \, f_1 = f_k$

3) $\forall f_i \in F \quad \exists f_k \in F$ tal que $f_i \, o \, f_k = f_1 = f_k \, o \, f_i$

Además, no se verifica la propiedad conmutativa, ya que, por ejemplo,

$$f_5 \, o \, f_3 = f_2 \neq f_3 \, o \, f_5 = f_6$$

Por lo tanto, (F,o) es un grupo finito de orden 6 no abeliano. ■

Consecuencia 10 *1) El elemento neutro es único.*

2) Cada elemento del grupo posee un único simétrico.

3) El simétrico (b')' del simétrico b' de un elemento b es el propio elemento b.

4) Se verifica la propiedad simplificativa, es decir,

$$\forall a, b, c \in G, \ si \ a * b = a * c ==> b = c.$$

*5) El simétrico ,(a * b)', del producto de dos elementos es el producto de los simétricos en orden inverso, b' * a'.*

*6) Las ecuaciones a * x = b y z * a = b tienen cada una una única solución.*

Ejercicio 11 *Probar los resultados anteriores.*

Ejercicio 12 *Resolver la ecuación*

$$x * a * b * x * c = b * x * c$$

en un grupo G.

1.1 Subgrupos.

Es interesante considerar los subconjuntos de un grupo que a su vez también tienen estructura de grupos.

Definición 13 *Un subconjunto no vacío S de un grupo G es un subgrupo (de G) si, con respecto a la misma operación de G, S también es grupo.*

Ejemplo 14 *1) El conjunto* 3 $\mathbb{Z}$ *es un subgrupo de (* $\mathbb{Z}$*,+).*

2) Sea (G,) un grupo cualquiera; el conjunto* $S = \{x \in G \,|x = a * ... * a = a^p, p \in \mathbb{Z}\}$ *es un subgrupo de G, llamado* **subgrupo monógeno** *de generador a.*

3) El conjunto del ejemplo 2 es un subgrupo del grupo del ejemplo 1

4) Los conjuntos $S_1 = \{f_1, f_2\}$ *y* $S_2 = \{f_1, f_4, f_5\}$ *son subgrupos de (F,o) (ejercicio 9)*

En todo grupo existen, al menos, dos subgrupos, $\emptyset$, G, llamados subgrupos impropios; caso de que existan, los restantes subgrupos se denominan subgrupos propios.

Teorema 15 *(de caracterización de subgrupos).- Un subconjunto S, no vacío, de un grupo G es un subgrupo si y solo si*

$$\forall a, b \in S, \text{ se verifica: } a * b' \in S.$$

Demostr.: [$\Longrightarrow$] Por ser S subgrupo, $\forall a, b \in S$, se verifica que $\exists b' \in S$ y que, por ser * operación estable en S, $a * b' \in S$.

[$\Longleftarrow$] Hemos de probar que se verifican las propiedades 0), 1), 2), 3) de la definición. Trivialmente, si * es asociativa en G también lo es en S. Tomando, en la hipótesis, b = a resulta: $a*a' = e \in S$(prop. 2)). Ahora, tomando e y a en la hipótesis, resulta: $e*a' = a' \in S$ (prop. 3)). Finalmente, tomando a y b' en la hipótesis, sale: $a * (b')' = a * b \in S$ (prop. o)). ■

Ejercicio 16 *Probar que la intersección de dos subgrupos de un grupo es otro subgrupo y que la suma de dos subgrupos de un grupo con la adición como operación es otro subgrupo.*

1.2 Clases o cogrupos.

Unos subconjuntos de un grupo que tienen especial interés, ya que conducen a la definición del concepto de grupo cociente, son los cogrupos o clases de equivalencia asociadas a un subgrupo.

Teorema 17 *Sea S un subgrupo de un grupo (G,*). Definimos la relación binaria* $\mathcal{R}$ *en G mediante*

$$a\mathcal{R}b \Longleftrightarrow a * b' \in S, a, b \in S$$

Entonces, se verifica: 1) $\mathcal{R}$ *es una relación de equivalencia.*

2) $[a] = S * a = \{x \in G | x = s * a, s \in S\}$

Demostr.:

1) reflexiva: $a\mathcal{R}a \Longleftrightarrow a * a' = e \in S$ (por ser S subgrupo, prop. 2)

simétrica: $a\mathcal{R}b \Longleftrightarrow a * b' \in S \Longleftrightarrow (a * b')' = b * a' \in S \Longleftrightarrow b\mathcal{R}a$.

transitiva: $a\mathcal{R}b$ y $b\mathcal{R}c \Longleftrightarrow a * b' \in S, b * c' \in S \Longrightarrow$ (prop. o)) $(a * b') * (b * c') = a * c' \in S \Longleftrightarrow a\mathcal{R}c$.

2) Por definición de clase de equivalencia: [a] $= \{x \in G \,|\, x\mathcal{R}a\}$. Pero $x\mathcal{R}a \Longleftrightarrow x * a' \in S \Longleftrightarrow s \in S' x = s * a$, luego: [a] $= \{x \in G \,|\, x = s * a, s \in S\} = S * a$. ■

Análogamente podríamos estudiar la relación $\tilde{\mathcal{R}}$ en G:

$$a\tilde{\mathcal{R}}b \Longleftrightarrow b' * a \in S, a, b \in S$$

y ver que

1) $\tilde{\mathcal{R}}$ es una relación de equivalencia.

2) $[\mathrm{a}]_{\tilde{\mathcal{R}}} = \mathrm{a} * \mathrm{S} = \{x \in G \,|\, x = a * s, s \in S\}$

En consecuencia, podemos dar la siguiente definición

Definición 18 *Sea $a \in G$ y S un subgrupo de G. Llamaremos clase a izquierda asociada al elemento a módulo S, al conjunto*

$a * S = \{x \in G \,|\, x = a * s, s \in S\}$

y clase a derecha asociada al elemento a módulo S, al conjunto

$S * a = \{x \in G \,|\, x = s * a, s \in S\}$

Preguntas:

¿Cúantos elementos tiene cada clase?

¿Cúantas clases a izquierda y a derecha tiene un grupo?

¿Coinciden o no las clases a izquierda y a derecha?

Ejercicio 19 *Sea G el grupo F del ejercicio 9 y sean $S_1 = \{f_1, f_2\}$ y $S_2 = \{f_1, f_4, f_5\}$, construir las clases a izquierda y a derecha módulo S_1 y S_2, respectivamente.*

Solución: Construyamos en primer lugar las clases asociadas a S_1, éstas son:

```
f1 o S1 = {f1,f2}; S1 o f1 = {f1,f2}
f2 o S1 = {f1,f2}; S1 o f2 = {f1,f2}
f3 o S1 = {f3,f5}; S1 o f3 = {f3,f4}
f4 o S1 = {f4,f6}; S1 o f4 = {f3,f4}
f5 o S1 = {f3,f5}; S1 o f5 = {f5,f6}
f6 o S1 = {f4,f6}; S1 o f6 = {f5,f6}
```

Como se observa, las clases a izquierda y a derecha no son todas iguales.

Veamos ahora con S_2:

```
f1 o S2 = {f1,f4,f5} = f4 o S2 = f5 o S2
S2 o f1 = {f1,f4,f5} = S2 o f4 = S2 o f5

f2 o S2 = {f2,f3,f6} = f3 o S2 = f6 o S2
S2 o f2 = {f2,f3,f6} = S2 o f3 = S2 o f6
```

En este caso, a pesar de que (F,o) no es grupo abeliano, las clases a izquierda y a derecha coinciden. ■

Ejemplo 20 *Clases de restos módulo 3.*

A partir del grupo abeliano ($\mathbb{Z}$, +) y del subgrupo 3 $\mathbb{Z}$ de los enteros múltiplos de tres construimos las clases a izquierda y a derecha siguientes:

$$1+3\ \mathbb{Z} = \{1+3p | p \in \mathbb{Z}\} = \{-5,-2,1,4,7,...\}$$
$$2+3\ \mathbb{Z} = \{2+3p | p \in \mathbb{Z}\} = \{-4,-1,2,5,8,...\}$$
$$3+3\ \mathbb{Z} = \{3+3p | p \in \mathbb{Z}\} = \{-3,0,3,6,9,...\} = 3\ \mathbb{Z}$$

Por ser ($\mathbb{Z}$,+) grupo conmutativo, las clases a izquierda y a derecha coinciden.

El conjunto de todas las clases (conjunto cociente de $\mathbb{Z}$ sobre 3 $\mathbb{Z}$) se denomina conjunto de las clases de restos (o residuales) módulo 3 y se denota por $\mathbb{Z}/3\ \mathbb{Z}$, o bien, $\mathbb{Z}/(3)$, o aún, $\mathbb{Z}_3$.

Pregunta: ¿qué estructura posee $\mathbb{Z}_3$?

1.3 Grupo cociente

Definición 21 *Llamaremos subgrupo normal, invariante o distinguido a todo subgrupo N de un grupo G que verifique:*

$$a * N = N * a, \forall a \in G$$

Ejemplo 22 *1) Todo subgrupo de un grupo conmutativo es subgrupo normal; 3 Z es normal.*
2) El subgrupo S_2 del ejercicio 19 es normal, en cambio, el S_1 **no** *lo es.*

Observemos que:

$$a * N = N * a, \forall a \in G \Longleftrightarrow a * N * a' = N, \forall a \in G$$

es decir,

$$\forall a \in G, \forall n_1 \in N \quad \exists n_2 \in N \text{ tal que } a * n_1 * a' = n_2 \in G$$

La importancia de los subgrupos invariantes deriva de la siguiente propiedad.

Teorema 23 *Si N es subgrupo invariante de G, la relación de equivalencia $\mathcal{R}$ asociada a N es compatible con la estructura de G.*

Demostr: Por definición, $\mathcal{R}$ es compatible con la estructura de grupo de G si y solo si

$$a\mathcal{R}b \text{ y } \tilde{a}\mathcal{R}\tilde{b} \Longrightarrow (a * \tilde{a})\mathcal{R}(b * \tilde{b}),$$

que es lo que debemos probar.

Pues bien, notemos que

$$(a * \tilde{a}) * (b * \tilde{b})' = a * \tilde{a} * \tilde{b}' * b' = a * (\tilde{a} * \tilde{b}') * (b' * a) * a' \in N$$

como se requería. ■

Estamos ahora en condiciones de definir coherentemente una operación en el conjunto cociente G/$\mathcal{R}$, que a partir de aquí denotaremos por G/N que, como sabemos, está constituido por todas las clases de equivalencia o cogrupos.

Definición 24 *En G/N, definimos la operación * mediante [a] * [b] = [a * b]*

Observemos que * está bien definida, pues, como consecuencia del teorema 23, el resultado no depende de los representantes de las clases [a], [b] elegidos.

Teorema 25 *El conjunto G/N respecto de la operación * anterior tiene estructura de grupo.*

Demostr.: Se propone como ejercicio. ■

Definición 26 *Al grupo G/N le llamaremos grupo cociente de G sobre N.*

Ejemplo 27 *El conjunto* $\mathbb{Z}_3$ *(es decir,* $\mathbb{Z}/3\ \mathbb{Z}$ *) con la suma de clases de restos inducida por la suma de* $\mathbb{Z}$ *es un grupo (conmutativo) llamado de las clases residuales módulo 3.*

Ejercicio 28 *Probar que el conjunto cociente* F/S_2 *(F y* S_2 *definidos en el ejercicio 19) es un grupo respecto de la operación inducida.*

Solución: Denotemos por [1] , [2] las dos únicas clases existentes. Se puede comprobar que la operación inducida "o" definida por

```
[1] o [2] = [f4 o f5] = [2]
[1] o [1] = [f1 o f5] = [1]
[2] o [2] = [f3 o f6] = [1]
```

no depende del representante de la clase que se tome. Fácilmente se comprueba que [1] es el elemento neutro, que [2]' = [2] y que se verifica la propiedad asociativa. ■

Ejercicio 29 *Sea G un grupo cualquiera. Probar que el centro C del grupo G (conjunto de elementos de G que verifican la propiedad conmutativa) es un grupo invariante.*

1.4 Generación de grupos

Una pregunta que surge expontaneamente es la siguiente: ¿cuál es subgrupo S más pequeño que contiene a un subconjunto no vacío C de un grupo G?

Definición 30 *Al subgrupo S anterior se le denomina subgrupo engendrado por el conunto C.*

Para construir el subgrupo S engendrado por C, basta construir la tabla de Klein del conjunto C, ampliándola sucesivamente con el elemento neutro y con los elementos no considerados que vayan saliendo, debido a que S debe ser estable para la operación. Veamos varios ejemplos.

Ejemplo 31 *Sea* $G = \mathbb{Z}_8$ *y* $C = \{2,3\}$

	0	2	3	5	7	6	1	4
0	0	2	3	5	7	$\cdots$		
2	2	4	5	7	1			
3	3	5	6	0	2			
5	5	7	0	2	4			
7	7	1	2	4	6			
$\vdots$			$\cdots$					

luego S = G

Ejemplo 32 *Sea* $G = \mathbb{Z}_8$ *y* $C = \{2,4\}$

	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

Ejemplo 33 *Sea* $G = \mathbb{Z}_8$ *y* $C = \{4\}$

	0	4
0	0	4
4	4	0

luego S = {0, 4}

1.5 Grupos monógenos y grupos finitos

Definición 34 *Se denomina grupo monógeno a todo grupo G engendrado por un solo elemento g; a este elemento g se le llama generador del grupo; se escribe*

$$G = (g) = \{g^k \mid k \in \mathbb{Z}\}$$

Ejemplo 35 *1)* $\mathbb{Z}$ *con la suma es un grupo engendrado por +1 y también por -1.*
2) $\mathbb{Z}_p$ *con la suma está engendrado por 1.*
3) $\{1, i, -1, -i\} = (i) = (-i)$

Teorema 36 *Todo grupo monógeno es isomorfo a* $\mathbb{Z}$ *o a* $\mathbb{Z}_p$

Dem.: Consultar, por ejemplo, Castellet [7]. ■

Teorema 37 *Todo subgrupo de un grupo monógeno es también monógeno*

Dem.: Consultar, por ejemplo, Castellet [7]. ■

Definición 38 *Se denomina orden de un grupo al número de sus elementos. Se denomina orden de un elemento de un grupo al orden del subgrupo engendrado por él.*

Ejemplo 39 *En el grupo S(3), el orden de* s_4 *y* s_5 *es 3; el orden de* s_2, s_3 *y* s_6 *es 2. No hay elementos de orden 6, luego S(3) no es un grupo cíclico.*

Teorema 40 *(de Lagrange) El orden de un subgrupo S de un grupo finito G es un divisor del orden de G.*

Dem.: Consultar, por ejemplo, Castellet [7]. ■

2 Anillos

Una estructura más "fuerte" que la de grupo, con la que estamos familiarizados, es la que posee el conjunto $\mathbb{Z}$ de los números enteros respecto de la suma y el producto. Sirviéndonos ésta como ejemplo casi general, definimos axiomáticamente el concepto de anillo.

Definición 41 *Sean A un conjunto dotado de dos operaciones (leyes de composición), que denotaremos + y · , respectivamente. Diremos que (A,+, ·)esunanillo(oqueAposeeestructuradeanilloco y·) si se cumplen los siguientes axiomas:*

o) + es operación interna: $\forall a, b \in A, a + b \in A$

1) propiedad asociativa: $\forall a, b, c \in A, a + (b + c) = (a + b) + c$

2) existencia de elemento neutro (cero): $\exists 0 \in A$ *tal que* $0 + a = a + 0 = a, \forall a \in A$

3) existencia de elemento simétrico (opuesto):

$\forall a \in A \quad \exists -a \in A$ *tal que* $a + (-a) = -a + a = 0$

4) propiedad conmutativa: $\forall a, b \in A, a + b = b + a$

(es decir, A es grupo abeliano respecto de +)

o') · es operación interna: $\forall a, b \in A, a \cdot b \in A$

5) propiedad asociativa: $\forall a, b, c \in A, a \cdot (b \cdot c) = (a \cdot b) \cdot c$

6) propiedad distributiva de ·respectode+ : $\forall a, b, c \in A, a \cdot (b+c) = a \cdot b + a \cdot c \qquad (a+b) \cdot c = a \cdot c + b \cdot c$

Definición 42 *Si la multiplicación es conmutativa decimos que el anillo es conmutativo.*

Si existe elemento neutro (unidad) para la multiplicación se dice que el anillo es unitario (o con unidad).

Ejemplo 43 *1) (* $\mathbb{Z}, +, \cdot$*) es anillo conmutativo con unidad.*

2) $\mathbb{R}[x]$ *(conjunto de todos los polinomios en una indeterminada x y coeficientes números reales) con respecto de la suma y el producto de polinomios es un anillo conmutativo con unidad.*

3) El conjunto $A = \{(a, b) | \, a, b \in \mathbb{Z}\}$ *con respecto a la suma definida por (a,b)+(a',b') = (a+a',b+b') y el producto (a,b)· (a',b') = (a a',b b') tiene estructura de anillo conmutativo unitario.*

4) $M_2(\mathbb{R})$ *(conjunto de matrices cuadradas 2x2 de elementos reales) con la suma y el producto de matrices habituales es anillo unitario no conmutativo.*

5) $\mathbb{Z}_5$ *con respecto a la suma y producto de clases de restos habituales es un anillo conmutativo.*

Consecuencia 44 *1)* $a \cdot 0 = 0, \forall a \in A$

2) $0 \cdot a = 0, \forall a \in A$

3) $a \cdot b + a \cdot (-b) = 0, \forall a, b \in A$

4) $b \cdot a + (-b) \cdot a = 0, \forall a, b \in A$

5) $(-a) \cdot (-b) = a \cdot b, \forall a, b \in A$

Dem. 1): $\forall a \in A, a \cdot (b + 0) = a \cdot b + a \cdot 0 = a \cdot b$, por prop. distributiva y axioma 2), luego $a \cdot 0 = 0$.

Dem. 5): $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-a \cdot b) = a \cdot b$ por consecuencias 4), 3) y axioma 3.■

Notemos que como, en general, el producto no es conmutativo, el que se verifique una propiedad (por ejemplo consecuencia 1)) no implica que se cumpla la simétrica (por ejemplo, consecuencia 2)).

Definición 45 *Sea $(A,+,\cdot\ )$ un anillo unitario; diremos que $a \in A$ es un elemento inversible de A si posee elemento inverso (respecto de $\cdot$), es decir, si $\exists a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$*

Ejemplo 46 *1) En $\mathbb{Z}_5$ todos los elementos menos el [0] poseen inverso.*
2) En $(\mathbb{Z},+,\cdot\ )$ solo son inversibles 1 y -1

Algunos autores llaman unidades de un anillo unitario a todos los elementos inversibles (¡no confundirlas con el elemento unidad o elemento neutro para el producto!).

En un anillo unitario cualquiera A suele escribirse: $na \in A, \forall a \in A, \forall n \in \mathbb{Z}$, entendiendo que

n a = a+a+...+a = 1.a+1.a+...+1.a = (1+1+...+1) a

Definición 47 *Llamaremos característica de un anillo unitario al menor número natural no nulo que verifique $na = 0, \forall a \in A$*

Si no existe n verificando la condición anterior, diremos que A es un anillo de característica nula.

Ejemplo 48 *1) $\mathbb{Z}$ tiene característica nula*
2) $\mathbb{Z}_5$ tiene característica 5.

Observemos que en cualquier anillo no es cierto que

$$a \cdot b = 0 \text{ y } b \neq 0 \Longrightarrow a = 0$$

Por ejemplo, en el anillo $M_2(\mathbb{R})$ se cumple:

$$A = \begin{bmatrix} 2 & 0 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 3 & 1 \end{bmatrix}, \quad AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

siendo cada una de las matrices factores distintas de la matriz nula. En general, se puede dar la siguiente

Definición 49 *Se denominan divisores de cero a aquellos elementos no nulos de un anillo A que verifican $a \cdot b = 0$*

Si existen tales elementos en A, se dice que A posee divisores de cero.

Si A no posee divisores de cero y es conmutativo le llamaremos anillo de integridad o anillo íntegro; si, además, posee elemento unidad le llamaremos dominio de integridad.

Ejemplo 50 *1) Los pares (0,1) y (1,0) son divisores de cero del anillo A del ejemplo 3.3 3)*
2) Las matrices A y B anteriores son divisores de cero de $M_2(\mathbb{R})$.

Ejemplo 51 *1) $(\mathbb{Z},+,\cdot\ )$ es un dominio de integridad*
2) $(Q,+,\cdot\ )$, $(\mathbb{R},+,\cdot\ )$, $(\mathbb{C},+,\cdot\ )$ son dominios de integridad
3) $\mathbb{Z}_5$ es dominio de integridad
4) $\mathbb{Z}_6$ no es dominio de integridad.

Ejercicio 52 *Probar que el conjunto $\mathbb{R}[x]$ de todos los polinomios en una indeterminada con coeficientes reales es un dominio de integridad con respecto a la suma y al producto de polinomios. ¿Cúales son los elementos inversibles?.*

La importancia de los dominios de integridad estriva en la posibilidad de simplificar respecto del producto; esta es la analogía más interesante entre estos anillos y el de los números enteros.

Propiedad 53 *En un dominio de integridad D, se verifican las propiedades simplificativas del producto: a.x = a.y ==¿ x = y x.a = y.a ==¿ x = y, ∀a ∈ D∗ y recíprocamente.*

Demostr.: [⟹] a.x = a.y ¡==¿ a.x-a.y = 0 ¡==¿ a.(x-y)=0 ⟹ x = y. [⟸] Supongamos que se puede simplificar respecto del producto. Sea a.x = 0 con a ≠ 0 y x ≠ 0 ==¿ a.y = a.y + a.x = a.(x+y) ==¿ (prop.simplif.) y = y + x ==¿ x = 0 contra la hipótesis; luego no existen divisores de cero en D. ■

Ejercicio 54 *Resolver el sistema de ecuaciones siguiente en el dominio de integridad* $\mathbb{Z}_5$

```
[3] x + [2] y = [0]
[2] x + [1] y = [1]
```

2.1 Subanillos

Los subconjuntos de un anillo que realmente tienen interés son los que también tienen estructura de anillo.

Definición 55 *Sea S ⊂ A anillo. Diremos que S es un subanillo de A si con respecto a las mismas operaciones de A tiene también estructura de anillo.*

Teorema 56 *(de caracterización).- La condición necesaria y suficiente para que un subconjunto S de un anillo A sea un subanillo es que*

$$\forall a, b \in S : a - b \in S \text{ y } a.b \in S$$

Demostr.: se propone como un sencillo ejercicio. ■

Subanillos muy especiales de un anillo, porque permiten definir la estructura de anillo cociente, son los "ideales".

Definición 57 *Llamaremos ideal a izquierda I de un anillo A a todo subconjunto I de A que verifique:*

$$\forall a, b \in I : a - b \in I$$

$$\forall a \in I, \forall x \in A : \quad x.a \in I, \quad (A.I \subset I)$$

Análogamente se puede definir el concepto de ideal a derecha cambiando x.a por a.x. Entonces, un ideal bilátero es todo ideal a izquierda y a derecha.

Ejemplo 58 *1) p* $\mathbb{Z}$ *(conjunto de los enteros múltiplos de p) es un subanillo de* $\mathbb{Z}$*.*
2) 2 $\mathbb{Z}$ *(conjunto de los enteros múltiplos de 2) es un ideal (bilátero) de* $\mathbb{Z}$*.*

Definición 59 *Diremos que el ideal I del anillo unitario A es ideal principal si existe un elemento i ∈ A tal que ∀x ∈ I, ∃y ∈ A verificando x = y.i*
Al elemento i se le denomina base del ideal y entonces se escribe I = (i).

Ejemplo 60 *El conjunto 5* $\mathbb{Z}$ *de los enteros múltiplos de 5 es un ideal principal de* $\mathbb{Z}$*, y así, 5* $\mathbb{Z}$ *= (5).*

Otras consideraciones sobre anillos y homomorfismos de anillos pueden ser consultados en la bibliografía citada al principio de este capítulo.

3 Cuerpos.

El conjunto de los números reales R representa un modelo de estructura algebráica con dos operaciones internas muy conocido, por lo que únicamente recordaremos la definición de la estructura abstracta de la que R es ejemplo y algunas de sus propiedades más sobresalientes.

Definición 61 *Llamaremos cuerpo, K, a todo anillo (K,+,.) unitario, conmutativo y tal que todo elemento distinto del cero posea inverso. Es decir, que verifique:*
**) (K,+) es grupo abeliano*
**) (K*,·) es grupo abeliano*
**) propiedad distributiva:* $\forall a, b, c \in A$: $a.(b+c) = a.b + a.c$

Ejemplo 62 *1)* $(\mathbb{R},+,.)$, $(Q,+,.)$, $(\mathbb{C},+,.)$ *son cuerpos (conmutativos).*
2) $\mathbb{Z}_5$ *es cuerpo, pero* $\mathbb{Z}_6$ *no lo es.*

Propiedad 63 *1) Un cuerpo no posee divisores de cero.*
2) Todo dominio de integridad finito es un cuerpo.
3) Los únicos ideales de un cuerpo K son 0 y K
4) En todo cuerpo K son válidas las reglas del cálculo con fracciones con denominadores no nulos.

(Otras cuestiones sobre esta estructura pueden consultarse en la bibliografía recomendada).

Ejercicio 64 *(El cuerpo de fracciones de un dominio de integridad) (En este ejercicio se muestra un procedimiento para construir un cuerpo a partir de un dominio de integridad, de la misma forma a como se construye el cuerpo de los números racionales a partir de los números enteros).*
Sea (A,+,.) un dominio de integridad. En el conjunto A x A definimos dos operaciones + y . mediante*
(a,b)+(c,d) = (a..d+b.c,b.d)
(a,b).(c,d) = (a.c,b.d)
1) Probar que $A \times A^*$ *es anillo unitario conmutativo.*
Se define ahora la relación binaria R en A x A mediante:*
(a,b) R (a',b') $\Longleftrightarrow$ *a.b' = a'.b*
2) Probar que R es compatible con + y . de $A \times A^*$
3) Construir el conjunto cociente $A \times A^*/R$ *que denotaremos por K.*
Se definen en K otras operaciones + y . mediante:
[(a,b)] + [(c,d)] = [(a d + b c, b d)]
[(a,b)] . [(c,d)] = [(a c, b d)]
4) Probar que (K,+,.) es un cuerpo conmutativo.
Sea $i:(A,+,.) \longrightarrow (K,+,.)$, $a \longrightarrow i(a) = [(a,1)]$
5) Probar que i es un homomorfismo de anillos inyecctivo.
6) Probar que cualquier otro cuerpo K' para el que se pueda encontrar otro monomorfismo $m:A \longrightarrow K'$ *contiene a K.*

(Para más detalles sobre esta construcción consultar [6]

Ejercicio 65 *¿Cómo construirías el cuerpo de los números racionales a partir del dominio de integridad de los números enteros? (Desarrolla el procedimiento expuesto en el ejercicio anterior).*

Ejercicio 66 *A partir del dominio de integridad K[x] de todos los polionomios en una indeterminada con coeficientes en un cuerpo K, construir su cuerpo de fracciones.*