ÁLGEBRA CONMUTATIVA

Grado en Matemáticas, Curso 2012-2013

Tema 1: Grupos

Amelia Álvarez Sánchez

Índice

1.1 Grupos y Subgrupos

Llamaremos **operación** o ley de composición interna en un conjunto X a toda aplicación $X \times X \longrightarrow X$.

Representaremos las operaciones con los símbolos $+$, $\cdot$, $*$, ..., en cuyo caso la imagen de cada pareja $(x, y) \in X \times X$ se denotará respectivamente $x + y$, $x \cdot y$, $x * y$, etc.

Definición

Una operación $G \times G \stackrel{\cdot}{\longrightarrow} G$ define una estructura de **grupo** en el conjunto G si verifica las siguientes condiciones:

Ax. 1 **Propiedad asociativa**: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in G$.

Ax. 2 Existe un elemento en G, que se llama **neutro** y se denota 1, tal que $1 \cdot a = a \cdot 1 = a$, $\forall a \in G$.

Ax. 3 Si $a \in G$, entonces existe un elemento $a^{-1} \in G$, llamado **inverso** de a, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Si además se verifica que $a \cdot b = b \cdot a$ para todo a, $b \in G$, diremos que el grupo es **abeliano** o **conmutativo**.

El conjunto de los números enteros con la suma, $(\mathbb{Z}, +)$, es el ejemplo básico de grupo conmutativo.

Notación aditiva (Caso abeliano)
Denotaremos $+$ la operación, 0 el elemento neutro, y el inverso de a lo llamaremos **opuesto** y lo denotaremos $-a$.

Notación multiplicativa
Denotaremos $\cdot$ la operación, 1 el elemento neutro, y a^{-1} el inverso de a.

Ejemplos

- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ *y* $(\mathbb{C}, +)$ *son grupos conmutativos.*
- *El conjunto* $\mathbb{R}_+$ *de los números reales positivos con el producto es un grupo abeliano. Los números complejos no nulos con el producto es un grupo abeliano, al igual que las raíces n-ésimas de la unidad, donde* $n \geq 1$.
- *Las sucesiones de números reales con la suma de sucesiones es un grupo conmutativo.*
- *Si* $(G, \cdot)$ *y* $(G', \circ)$ *son dos grupos, su producto directo* $G \times G'$ *con la operación* $(a, a') * (b, b') = (a \cdot b, a' \circ b')$ *es un grupo, que es abeliano si y sólo si lo son G y G'.*
- *Si un grupo sólo tiene un elemento, entonces es el neutro, por lo que tal grupo se denota* 0 *ó* 1*, según la operación se denote aditiva o multiplicativamente.*

Ejemplo: El grupo simétrico

Sea $\sigma : X \to Y$ *una aplicación biyectiva. Si* $y \in Y$*, existe un único elemento* $x \in X$ *tal que* $y = \sigma(x)$*, elemento que denotaremos* $\sigma^{-1}(x)$*. Obtenemos así una aplicación* $\sigma^{-1} : Y \to X$ *que también es biyectiva y verifica que* $\sigma^{-1} \circ \sigma$ *es la identidad de X y* $\sigma \circ \sigma^{-1}$ *es la identidad de Y.*

Por tanto, el conjunto de todas las biyecciones de un conjunto no vacío X en sí mismo, con la composición de aplicaciones, es un grupo cuyo elemento neutro es la identidad de X. Este grupo sólo es conmutativo cuando X tiene 1 *ó* 2 *elementos.*

Cuando X tiene un número finito n de elementos, este grupo se denota S_n *y se llama* ***grupo simétrico*** *n-ésimo. Sus elementos también reciben el nombre de* ***permutaciones*** *de n elementos.*

Supondremos siempre que $n \geq 2$*. Numerando los elementos de X podemos suponer que* $X = \{1, 2, \ldots, n\}$*, así que una permutación* $\sigma \in S_n$ *puede denotarse de la siguiente forma:*

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

donde $a_i = \sigma(i)$*. Con esta notación es evidente que el número de elementos del grupo simétrico* S_n *es el factorial* $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$*.*

También es muy usual la siguiente notación: si $a_1, \ldots, a_d$ *son números distintos entre* 1 *y n, denotaremos* $(a_1 \ldots a_d)$ *la permutación que transforma* a_i *en* a_{i+1} *(entendiendo que* a_{d+1} *es* a_1*) y deja fijos los restantes elementos. Esta notación es cómoda, pero tiene el inconveniente de que es ambigua, pues* (2135) *denota tanto un elemento del grupo* S_5 *como de los grupos* S_n *con cualquier* $n \geq 6$*. Además,* (2135) *es la misma permutación que* (1352)*,* (3521) *y* (5213)*.*

Definición

Sea $(G, \cdot)$ un grupo. Diremos que un subconjunto H de G es un **subgrupo** de G si verifica las siguientes condiciones:

(a) La operación de G induce una operación en H, es decir, $a, b \in H \Rightarrow a \cdot b \in H$.

(b) El elemento neutro de G está en H, es decir, $1 \in H$.

(c) El inverso de cualquier elemento de H está en H, es decir, $a \in H \Rightarrow a^{-1} \in H$.

Ejercicios

1. Demostrar que un subconjunto H de un grupo G es subgrupo de G si y sólo si $H \neq \emptyset$ y para todo $a, b \in H$ se cumple que $a \cdot b^{-1} \in H$.
2. Sea H un subgrupo de un grupo G. Compruébese que aHa^{-1} es un subgrupo de G, para todo $a \in G$. Este subgrupo se denomina **subgrupo conjugado** de H por a.

Ejemplos

i) *Todo grupo G admite los subgrupos* $\{1\}$ *y G, llamados subgrupos triviales.*

ii) $\mathbb{Z}$, $\mathbb{Q}$ *y* $\mathbb{R}$ *son subgrupos del grupo* $(\mathbb{C}, +)$.

iii) *Las sucesiones de números racionales, con la suma de sucesiones, forman un grupo conmutativo. Las sucesiones de Cauchy y las sucesiones convergentes forman sendos subgrupos.*

iv) *Dado n un número entero, el conjunto*

$$n\mathbb{Z} = \{a \in \mathbb{Z} : a = nb \text{ para algún } b \in \mathbb{Z}\}$$

formado por los múltiplos de n es un subgrupo de $(\mathbb{Z}, +)$ *(veremos que todos sus subgrupos son así).*

v) *Subgrupos de* $(\mathbb{C}^*, \cdot)$:

- ¿$(\mathbb{Z}^*, \cdot)$?
- ¿$(\mathbb{Q}^*, \cdot)$?
- ¿$S_1 = \{z \in \mathbb{C} : |z| = 1\}$?
- ¿$B_1 = \{z \in \mathbb{C} : |z| \leq 1\}$?
- ¿μ_n[1] $= \{z \in \mathbb{C} : z^n = 1\}$?

[1] Admitiendo la notación $e^{a+bi} = e^a(\cos b + i \operatorname{sen} b)$, dado un número natural no nulo n, las raíces n-ésimas de la unidad $1 = e^{2\pi i}$ es el grupo μ_n formado por los n números complejos $e^{\frac{2\pi i}{n}k}$, $k = 0, \ldots, n-1$.

vi) *Cada elemento g de un grupo G genera un subgrupo:*

- *Con notación aditiva:* $(g) = \{ng\}_{n\in\mathbb{Z}}$, *donde*

$$ng = g + \overset{n)}{\ldots} + g \quad \text{si } n > 0,$$

$$0g = 0, \text{y}$$

$$ng = (-g) + \overset{-n)}{\ldots} + (-g) \quad \text{si } n < 0.$$

- *Con notación multiplicativa:* $(g) = \{g^n\}_{n\in\mathbb{Z}}$, *donde*

$$g^n = g \cdot \overset{n)}{\ldots} \cdot g \quad \text{si } n > 0,$$

$$g^0 = 1, \text{y}$$

$$g^n = g^{-1} \cdot \overset{-n)}{\ldots} \cdot g^{-1} \quad \text{si } n < 0.$$

vii) *Las permutaciones* σ *de n puntos en un plano que conserven distancias (es decir, tales que la distancia entre P y Q coincida con la distancia entre* σP *y* σQ*) forman un subgrupo de* S_n*, llamado* ***grupo de simetría*** *de la figura dada.*
Así, el grupo de simetría de un triángulo equilátero de vértices P_1, P_2, P_3 *es claramente* S_3*. Si el triángulo es isósceles y* P_1 *es el vértice común de los dos lados iguales, el grupo de simetría es* $\{Id, (23)\}$*, mientras que el grupo de simetría se reduce a la identidad si el triángulo es escaleno.*

Operaciones con subgrupos

Proposición (1)

- *Si* $\{H_i\}_{i\in I}$ *es una familia de subgrupos de G, entonces* $\cap_{i\in I} H_i$ *es un subgrupo de G.*
- *Si* H_1 *y* H_2 *son subgrupos de G, entonces*

$$H_1 \cup H_2 \text{ subgrupo} \iff H_1 \subseteq H_2 \text{ ó } H_2 \subseteq H_1.$$

- *Si G es abeliano y* H_1 *y* H_2 *son subgrupos de G, entonces*

$$H_1 + H_2 = \{g \in G : g = h_1 + h_2,\ h_1 \in H_1,\ h_2 \in H_2\}$$

es un subgrupo de G.

Como consecuencia tenemos que, si X es un subconjunto de un grupo G, la intersección de todos los subgrupos de G que contienen a X es un subgrupo de G y diremos que es el subgrupo de G **engendrado** o **generado** por X. El subgrupo de G generado por X es un subgrupo de G que contiene a X y que está contenido en cualquier otro subgrupo de G que contenga a X: *es el menor subgrupo de G que contiene a X*.

Ejemplo

El subgrupo de $\mathbb{Z}$ *generado por un entero n es*

$$(n) = n\mathbb{Z} = \{a \in \mathbb{Z} : a = nb \text{ para algún } b \in \mathbb{Z}\}$$

y el subgrupo de $\mathbb{Z}$ *generado por dos números enteros m y n es*

$$m\mathbb{Z} + n\mathbb{Z} = \{x \in \mathbb{Z} : x = am + bn,\ a, b \in \mathbb{Z}\}.$$

1.2 Aritmética Elemental

Teorema (2)

Si H es un subgrupo del grupo aditivo de los números enteros, entonces existe un único número natural n tal que $H = n\mathbb{Z}$.

Sean a, b dos números enteros. Diremos que a es **múltiplo** de b (o que b es **divisor** de a) cuando exista algún $c \in \mathbb{Z}$ tal que $a = bc$, es decir, cuando $a\mathbb{Z} \subseteq b\mathbb{Z}$.

Diremos que un número natural p mayor que 1 es **primo** cuando no pueda descomponerse en producto de dos números naturales más pequeños (es decir, cuando $p > 1$ y sus únicos divisores naturales son 1 y p).

Definición

Sean a, b dos números enteros. Diremos que un número natural es el **mínimo común múltiplo** de a y b si es un múltiplo común y divide a cualquier otro múltiplo común. Diremos que un número natural es el **máximo común divisor** de a y b si es un divisor común y es múltiplo de cualquier otro divisor común. Diremos que a y b son **primos entre sí**, cuando su máximo común divisor sea la unidad.

Si n es un número natural no nulo, $\phi(n)$ denotará el número de números naturales entre 1 y n que son primos con n. Esta función ϕ se llama **indicador de Euler**(1707-1783) y sus primeros valores son:

$$\phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2,\ \phi(7) = 6,$$
$$\phi(p) = p - 1 \text{ cuando } p \text{ es primo.}$$

Proposición (3)

Sean a y b dos números enteros. La condición necesaria y suficiente para que un número natural m sea el mínimo común múltiplo de a y b es que

$$m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}.$$

Luego el mínimo común múltiplo de dos números enteros siempre existe y es único.

Proposición (4)

Sean a y b dos números enteros. La condición necesaria y suficiente para que un número natural d sea el máximo común divisor de a y b es que

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}.$$

Por tanto, el máximo común divisor de dos números enteros siempre existe y es único.

Identidad de Bézout (1730-1783). *Sean a y b dos números enteros. Si d es el máximo común divisor de a y b, entonces existen números enteros α y β tales que*

$$d = \alpha a + \beta b.$$

Corolario (5)

La condición necesaria y suficiente para que dos números enteros a, b sean primos entre sí es que existan números enteros α, β tales que

$$1 = \alpha a + \beta b.$$

Corolario (6)

Si un número entero divide a un producto de dos números enteros y es primo con un factor, entonces divide al otro factor.

Lema de Euclides. *Si un número primo divide a un producto de números enteros, entonces divide a algún factor.*

Teorema de descomposición en factores primos. *Todo número natural mayor que* 1 *es producto de números primos. Esta descomposición es única salvo el orden de los factores.*

Corolario (7)

Todo número natural mayor que 1 *es múltiplo de algún número primo.*

Corolario (8)

Hay infinitos números primos.

Todo número natural $n \geq 2$ descompone de la siguiente forma:

$$n = p_1^{n_1} \cdots p_r^{n_r}\ , \quad n_i \geq 1$$

donde $p_1, \ldots, p_r$ son números primos distintos, y tal descomposición es única salvo el orden de los factores. Del lema de Euclides se sigue que si un número primo p divide a n, entonces $p = p_i$ para algún índice i: *Los únicos factores primos de n son* $p_1, \ldots, p_r$.

Si $a = p_1^{a_1} \cdots p_r^{a_r}$ y $b = p_1^{b_1} \cdots p_r^{b_r}$ son descomposiciones de dos números naturales a, b en producto de primos distintos ($a_i, b_i \geq 0$), entonces

$$b \text{ es múltiplo de } a \Leftrightarrow b_i \geq a_i \text{ para todo índice } i$$

$$\text{m.c.d.}(a,b) = p_1^{d_1} \cdots p_r^{d_r}, \quad d_i = \min(\mathrm{a_i}, \mathrm{b_i})$$

$$\text{m.c.m.}(a,b) = p_1^{m_1} \cdots p_r^{m_r}, \quad m_i = \max(\mathrm{a_i}, \mathrm{b_i})$$

En particular, $ab = \text{m.c.d.}(a,b) \cdot \text{m.c.m.}(a,b)$.

Algoritmo de Euclides. *Sean $a, b, c, r \in \mathbb{Z}$. Si $a = bc + r$, entonces*

$$m.c.d.(a,b) = m.c.d.(b,r).$$

Este algoritmo permite calcular rápidamente el máximo común divisor d de dos números enteros no nulos a, b, y los coeficientes de la Identidad de Bézout. Se efectúan las divisiones:

$$a = c_1 b + r_1,\ b = c_2 r_1 + r_2,\ r_1 = c_3 r_2 + r_3,\ \ldots\ ,\ r_{n-1} = c_{n+1} r_n + 0$$

hasta que el resto sea nulo, lo que necesariamente ha de ocurrir, pues la sucesión de restos $r_1, r_2, \ldots$ es estrictamente decreciente. Según el resultado anterior, el máximo común divisor de a y b coincide con el máximo común divisor de dos términos sucesivos cualesquiera de la sucesión

$$a,\ b,\ r_1,\ r_2,\ \ldots\ ,\ r_n,\ 0.$$

Como $\text{m.c.d.}(r_n, 0) = r_n$, concluimos que el máximo común divisor d de a y b es el último resto no nulo r_n.

Ecuaciones diofánticas lineales

Ejemplo

Dados números enteros a, b, c, el algoritmo de Euclides permite hallar todas las soluciones enteras de la ecuación

$$ax + by = c.$$

Sea $d = m.c.d.(a,b)$. Según hemos visto, la condición necesaria y suficiente para que la ecuación tenga solución entera es que d divida a c.
Supongamos que $a, b \neq 0$ y que la ecuación tiene alguna solución entera (es decir, $c = dc'$ para algún $c' \in \mathbb{Z}$). Si $d = \alpha a + \beta b$, entonces $x_0 = \alpha c'$, $y_0 = \beta c'$ es una solución particular de la ecuación considerada.

Todas las soluciones enteras son

$$\begin{cases} x = x_0 + (b/d)n \\ y = y_0 - (a/d)n \end{cases}$$

donde n recorre todos los números enteros. En efecto, por sustitución directa se comprueba que son soluciones, y para cualquier otra solución x, y se tiene

$$0 = c - c = (ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0),$$

luego $a(x - x_0) = -b(y - y_0)$ y $(a/d)(x - x_0) = -(b/d)(y - y_0)$. Como b/d no divide a a/d, se sigue que b/d divide a $x - x_0$. Es decir, $x - x_0 = (b/d)n$ para algún $n \in \mathbb{Z}$, así que $y - y_0 = -(a/d)n$.

Como ejemplo vamos a resolver la ecuación diofántica $2000x - 266y = -4$.

Definición

Diremos que una aplicación $f : G \to G'$ entre dos grupos es un **morfismo de grupos** cuando para todo $a, b \in G$ se verifique

$$f(a \cdot b) = f(a) \cdot f(b).$$

Diremos que un morfismo de grupos $f : G \to G'$ es un **isomorfismo** si existe un morfismo de grupos $g : G' \to G$ tal que $f \circ g = I_{G'}$ y $g \circ f = I_G$. Diremos que tal morfismo g es el **inverso** de f y lo denotaremos f^{-1}.
Llamaremos **automorfismos** de un grupo G a los isomorfismos de G en G.

Propiedades

- Los morfismos de grupo conservan el neutro y los inversos:

$$f(1) = 1$$
$$f(a^{-1}) = f(a)^{-1}$$

- Si $f\colon G \to G'$ y $g\colon G' \to G''$ son morfismos de grupos, entonces su $g \circ f\colon G \to G''$ también es un morfismo de grupos.

Definición

Si $f\colon G \to G'$ es un morfismo de grupos, su **núcleo** y su **imagen** son, respectivamente:

$$\operatorname{Ker} f = \{a \in G\colon\ f(a) = 1\} \subseteq G,$$
$$\operatorname{Im} f = \{x \in G'\colon\ x = f(a),\ \text{para algún } a \in G\} \subseteq G'.$$

Proposición (9)

Si $f\colon G \to G'$ es un morfismo de grupos, entonces:

(a) *f es inyectivo si y sólo si $\operatorname{Ker}(f) = 1$.*

(b) *f es isomorfismo si y sólo si f es biyectivo.*

Proposición (10)

Sea $f : G \to G'$ un morfismo de grupos.

(a) *Si H es un subgrupo de G, entonces*

$$f(H) := \{y \in G' :\ y = f(a) \text{ para algún } a \in H\}$$

es un subgrupo de G'.

(b) *Si H' es un subgrupo de G', entonces*

$$f^{-1}(H') := \{a \in G :\ f(a) \in H'\}$$

es un subgrupo de G.

En particular $\operatorname{Im} f$ es un subgrupo de G' y $\operatorname{Ker} f$ es un subgrupo de G.

Ejemplos

i) *Si H es un subgrupo de un grupo G, la inclusión $i : H \to G$, $i(a) = a$, es un morfismo de grupos inyectivo y su imagen es H.*

ii) *Si G es un grupo, existe un único morfismo de grupos $1 \to G$, que es inyectivo, y un único morfismo de grupos $G \to 1$, que es epiyectivo.*

iii) *Si G y G' son dos grupos, las proyecciones $G \times G' \to G$ y $G \times G' \to G'$ son morfismos de grupos. También lo es la aplicación $i : G \to G \times G'$, $i(g) = (g, 1)$.*

iv) *¿Morfismos de grupos $\mathbb{Z} \to \mathbb{Z}$?*

v) *Sea $(G, \cdot)$ un grupo. Cada elemento $g \in G$ define un morfismo de grupos:*

$$f_g : (\mathbb{Z}, +) \to (G, \cdot), \quad 1 \to f_g(1) = g$$

$\operatorname{Im} f_g =$

$\operatorname{Ker} f_g =$

1.4 Grupo Cociente

Relación definida por un subgrupo. Sea $(G, \cdot)$ un grupo. Cada subgrupo H define una relación

$$a \equiv b \iff a^{-1}b \in H,$$

que es de equivalencia. Respecto de esta relación, las clases de equivalencia del neutro y de un elemento cualquiera $a \in G$ son:

$[1] =$

$[a] =$

Ejemplo

$G = \mathbb{Z}$, $H = (n) = n\mathbb{Z} = [0]$
$a \equiv b \iff$
$[a] = \bar{a} =$

El conjunto cociente de G por la relación de equivalencia inducida por el subgrupo H se denotará:

$$G/H = \{aH : a \in G\}.$$

Definición

Llamaremos **orden** de un grupo a su cardinal[2]. Llamaremos **índice** de un subgrupo H en un grupo G al cardinal del conjunto cociente G/H.

¿Índice de $n\mathbb{Z}$ en $\mathbb{Z}$?

Teorema (de Lagrange)

Sea G un grupo de orden finito. Si H es un subgrupo de G, el orden de H divide al orden de G y el cociente es el índice de H en G.

$$|G/H| = |G|/|H|.$$

[2] El cardinal de un conjunto finito X es el número de elementos de X y se denota $|X|$.

Ejemplos

- *Subgrupos de* $\mu_8 = \{z \in \mathbb{C} : z^8 = 1\}$

- *Subgrupos de* S_3

Construcción del grupo cociente

Sea H un subgrupo de un grupo $(G, \cdot)$. Queremos definir una estructura de grupo en el cociente G/H de manera que la proyección canónica $\pi : G \to G/H$ sea morfismo de grupos. Es decir:

$$[a \cdot b] = [a] \cdot [b].$$

- ¿Podemos definir $[a] \cdot [b] := [a \cdot b]$?
- ¿Si $[a] = [a'] \Rightarrow [a \cdot b] = [a' \cdot b]$?
- Es decir, ¿$a \equiv a' \Rightarrow a \cdot b \equiv a' \cdot b$?

En tal caso, $H = \{g \in G : \pi(g) = \pi(1)\}$ sería el núcleo del morfismo π.

Definición

Sea H un subgrupo de un grupo G. Diremos que H es un **subgrupo normal** de G si $aHa^{-1} \subseteq H$ para todo $a \in G$. Es decir,

$$h \in H, a \in G \Rightarrow aha^{-1} \in H.$$

Ejemplos

- *Si G es conmutativo, todo subgrupo de G es normal.*
- *El grupo de las permutaciones pares* A_n *es un subgrupo normal de* S_n.
- $H = \{Id, (2,3)\}$ *es un subgrupo de* S_3 *que no es normal.*

Proposición (11)

Sea $f : G \to G'$ *un morfismo de grupos. El núcleo de* f *es un subgrupo normal de G.*

Proposición (12)

Sea G un grupo y sea H un subgrupo de G. Las siguientes condiciones son equivalentes:

1. $aHa^{-1} \subseteq H, \forall a \in G;$
2. $aHa^{-1} = H, \forall a \in G;$
3. $aH \subseteq Ha, \forall a \in G;$
4. $aH = Ha, \forall a \in G.$

Demostración

EJERCICIO

Teorema (13)

Si H es un subgrupo normal de un grupo G, en el conjunto cociente G/H existe una única estructura de grupo tal que la proyección canónica $\pi : G \to G/H$ es morfismo de grupos. Además, $H = Ker\,\pi$.

Definición

Sea H un subgrupo normal de un grupo G. Diremos que el conjunto G/H, con la única operación para la que $\pi : G \to G/H$ es morfismo de grupos, es el **grupo cociente** de G por H y lo denotaremos también por G/H.

Ejemplos

- *Si G es un grupo conmutativo, todo subgrupo H de G es normal, y el grupo cociente G/H también es conmutativo.*
- *Dado n un número natural, $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$ y en el conjunto cocientes $\mathbb{Z}/n\mathbb{Z}$ tenemos una estructura de grupo,*

$$[a]_n + [b]_n = [a+b]_n,$$

para la cual el neutro es $[0]_n$ y el opuesto de cualquier elemento $[a]_n$ es $[-a]_n$.

Teorema (Propiedad universal del grupo cociente)

Sea H un subgrupo normal de un grupo G y sea $\pi : G \to G/H$ la proyección canónica. Si $f : G \to G'$ es un morfismo de grupos tal que $H \subseteq Ker\,f$, entonces existe un único morfismo de grupos $\phi : G/H \to G'$ tal que $f = \phi \circ \pi$:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle \phi} & \\ & G' & \end{array}$$

Propiedad universal del grupo cociente

Sea H un subgrupo normal de un grupo G.

$$\left\{ \begin{array}{c} \text{morfismos de grupos} \\ G \xrightarrow{f} G' \\ \text{tales que } H \subseteq \operatorname{Ker} f \end{array} \right\} = \left\{ \begin{array}{c} \text{morfismos de grupos} \\ G/H \xrightarrow{\phi} G' \end{array} \right\}$$

$$f \quad \mapsto \quad \exists\, \phi \,/\, f = \phi \circ \pi$$

$$f := \phi \circ \pi \quad \leftarrow \quad \phi$$

Ejercicio

Dados dos números naturales n y m, consideremos los cocientes:

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},$$

$$\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

¿Qué relación debe existir entre n y m para que exista un morfismo de grupos

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

tal que

$$f \circ \pi_n = \pi_m?$$

Teorema (de isomorfía)

Sea $f : G \to G'$ un morfismo de grupos. La aplicación

$$\phi : G/Ker\, f \longrightarrow Im\, f,\ \phi([a]) = f(a)$$

es un isomorfismo de grupos:

$$\boxed{G/Ker\, f \simeq Im\, f}$$

Corolario (14)

Si $f : G \to G'$ es un morfismo de grupos epiyectivo, entonces

$$G/Ker\, f \simeq G'.$$

Ejemplo

Consideremos el morfismo de grupos

$$\phi : \mathbb{Z} \to \mu_n,\ \phi(1) = e^{\frac{2\pi}{n} i}.$$

- $\phi(k) =$
- $Im\, \phi =$
- $Ker\, \phi =$
- $\mu_n \simeq$

Teorema (chino de los restos)

Si m, n son números enteros primos entre sí, el morfismo de grupos

$$\begin{array}{rcl} \phi : \dfrac{\mathbb{Z}}{mn\mathbb{Z}} & \to & \dfrac{\mathbb{Z}}{m\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}} \\ [a]_{mn} & \mapsto & \phi([a]_{mn}) = ([a]_m, [a]_n) \end{array}$$

es un isomorfismo:

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Observaciones

- Si $\text{m.c.d.}(m, n) = 1$, entonces:

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

  Por lo tanto, dos números enteros son congruentes módulo nm sí y sólo sí son congruentes módulo n y módulo m.
- ¡Cuidado! Si $\text{m.c.d.}(m, n) \neq 1$, el resultado anterior no es cierto. Por ejemplo:

$$\frac{\mathbb{Z}}{8\mathbb{Z}} \neq \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

¿¿¿POR QUÉ???

Ecuaciones Diofánticas

Sean m y n dos enteros primos entre sí. Sabemos que

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Esto significa que, para cada pareja de números enteros b, c, el sistema de congruencias

$$\begin{cases} x \equiv b & (\text{mód. } n) \\ x \equiv c & (\text{mód. } m) \end{cases}$$

siempre tiene alguna solución entera, y ésta es única módulo nm: tiene una única solución $0 \leq x < mn$.

Ejercicio

Resolver el sistema:

$$\begin{cases} x \equiv 7 & (\text{mód. } 9) \\ x \equiv 1 & (\text{mód. } 4) \end{cases}$$

1.5 Grupos Cíclicos

Sea $(G, \cdot)$ un grupo. Dado $g \in G$ tenemos definido el morfismo de grupos

$$f_g : \mathbb{Z} \to G,\ f_g(n) = g^n$$

cuya imagen es el subgrupo generado por g, (g).

Definición

Llamaremos **orden** de un elemento g de un grupo G al orden del subgrupo que genera. El orden de un elemento puede ser infinito.

El único elemento de orden 1 es el neutro del grupo.
De acuerdo con el teorema de Lagrange, si un grupo es finito, todos sus elementos tienen orden finito, puesto que divide al orden del grupo.

Proposición (15)

Sea g un elemento de un grupo G.

(a) *Si g es de orden infinito, entonces $g^n = g^m \Leftrightarrow n = m$. En particular,*

$$g^n = 1 \Leftrightarrow n = 0.$$

(b) *Si g es de orden d, entonces $g^n = g^m \Leftrightarrow n \equiv m\ (\text{mód. } d)$. En particular,*

$$g^n = 1 \Leftrightarrow n \text{ es múltiplo del orden de } g.$$

Corolario (16)

El orden de un elemento g de un grupo G es el primer número natural no nulo d tal que $g^d = 1$, si existe tal número natural, y en caso contrario es infinito.

Corolario (17)

Si G es un grupo finito de orden n, entonces $g^n = 1$ para todo $g \in G$.

Definición

Diremos que un grupo G es **cíclico** si está generado por alguno de sus elementos; es decir, si existe $g \in G$ tal que $(g) = G$, en cuyo caso diremos que g es un **generador** de G.

Por definición, un grupo G es cíclico y $g \in G$ es un generador cuando todo elemento de G es de la forma g^m para algún entero m. Todo grupo cíclico es abeliano.

Ejemplos

i) *$\mathbb{Z}$ es un grupo cíclico que tiene como generadores 1 y -1.*

ii) *El grupo μ_n de las raíces n-ésimas de la unidad es cíclico:*

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{\frac{2\pi k}{n} i}, k = 0, \ldots, n-1\}.$$

Un generador de este grupo es $e^{\frac{2\pi}{n} i}$. Los generadores de μ_n son las raíces n-ésimas primitivas de la unidad.

Ejercicios

1. El grupo $\mathbb{Z}/n\mathbb{Z}$ es cíclico, pues está generado por [1].

- Calcula el orden de un elemento $[a]$ en $\mathbb{Z}/n\mathbb{Z}$.
- Caracteriza los generadores del grupo $\mathbb{Z}/n\mathbb{Z}$.
- ¿Cuántos generadores tiene $\mathbb{Z}/n\mathbb{Z}$?

2. Determina las raíces cuartas y quintas primitivas de la unidad.

Teorema (Clasificación de grupos cíclicos)

Sea G un grupo cíclico.

(a) *Si G es infinito, entonces G es isomorfo al grupo $\mathbb{Z}$. Si g es un generador de G, la aplicación $\phi : \mathbb{Z} \to G$, $\phi(m) = g^m$, es un isomorfismo de grupos.*

(b) *Si G es finito y su orden es n, entonces G es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Si g es un generador de G, la aplicación $\phi : \mathbb{Z}/n\mathbb{Z} \to G$, $\phi([m]_n) = g^m$, es un isomorfismo de grupos.*

1.6 El grupo Simétrico S_n

El grupo simétrico n-ésimo S_n es el grupo de todas las biyecciones de un conjunto no vacío X (con n elementos) en sí mismo, con la estructura de gruopo que define la composición de aplicaciones. Sus elementos también reciben el nombre de **permutaciones** de n elementos. Supondremos siempre que $n \geq 2$.
¿Abeliano?
Numerando los elementos de X podemos suponer que $X = \{1, 2, \ldots, n\}$, así que una permutación $\sigma \in S_n$ puede denotarse de la siguiente forma:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

donde $a_i = \sigma(i)$.
El **orden** de S_n es igual a $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$.

Definición

Diremos que una permutación $\sigma \in S_n$ es un **ciclo** si $\sigma = (a_1 \ldots a_d)$ para ciertos elementos distintos $a_1, \ldots, a_d$, $d \geq 2$. Los ciclos de orden 2 se llaman **trasposiciones**.

¿Orden de $\sigma = (a_1 \ldots a_d)$?

Diremos que dos ciclos $(a_1 \ldots a_d)$ y $(b_1 \ldots b_k)$ de S_n son **disjuntos** cuando $a_i \neq b_j$ para todo par de índices i, j.

Lema (18)

Si dos ciclos σ y τ son disjuntos, entonces $\sigma\tau = \tau\sigma$.

Teorema (19)

Toda permutación $\sigma \in S_n$ distinta de la identidad descompone en producto de ciclos disjuntos. Salvo el orden de los factores, esta descomposición es única.

Corolario (20)

Todo ciclo de orden d es producto de $d-1$ trasposiciones. Por tanto, toda permutación es producto de trasposiciones.

Definición

Sea $\sigma = \alpha_1 \ldots \alpha_r$ la descomposición de una permutación $\sigma \neq id$ en producto de ciclos disjuntos y denotemos d_i el orden de α_i, $1 \geq i \geq r$. El lema anterior nos permite suponer $d_1 \geq d_2 \geq \ldots \geq d_r$ y diremos que $d_1, \ldots, d_r$ es la **forma** de la permutación σ.

Proposición (21)

El orden de cualquier permutación de forma $d_1, \ldots, d_r$ es el mínimo común múltiplo de $d_1, \ldots, d_r$.

Definición

Sea G un grupo. Diremos que dos elementos x, y de G son **conjugados** si existe $a \in G$ tal que $y = axa^{-1}$.

Proposición (22)

Sean $\sigma, \tau \in S_n$. La condición necesaria y suficiente para que σ y τ sean conjugados es que tengan la misma forma.

Signo de una permutación

Sea Δ el siguiente polinomio con coeficientes enteros:

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_j - x_i).$$

Dada $\sigma \in S_n$, los factores de $\Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \prod_{i<j}(x_{\sigma(j)} - x_{\sigma(i)})$ coinciden, eventualmente salvo el signo, con los de $\Delta(x_1, \ldots, x_n)$. Luego

$$\Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \pm\Delta(x_1, \ldots, x_n).$$

Definición

Llamaremos **signo** de una permutación $\sigma \in S_n$ al número entero $sgn(\sigma)$ tal que

$$\Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = sgn(\sigma) \cdot \Delta(x_1, \ldots, x_n).$$

Por definición, el signo de una permutación es 1 ó -1.

Dada una permutación σ, diremos que el par i, j está en inversión con respecto a σ si $i < j$ y $\sigma(i) > \sigma(j)$. Luego

$$sgn(\sigma) = (-1)^{\text{nº de pares en inversión}}.$$

Proposición (23)

El signo de cualquier producto de permutaciones es el producto de los signos de los factores. El signo de toda trasposición es -1.

Corolario (24)

El signo de toda permutación de forma $d_1, \ldots, d_r$ es

$$(-1)^{d_1+\ldots+d_r-r}.$$

Ejercicio

Calcula el signo de $\sigma = (a_1, \ldots, a_d)$.

Corolario (25)

Sea $\sigma = \tau_1 \ldots \tau_m$ una descomposición de una permutación σ en producto de trasposiciones. Si $sgn(\sigma) = 1$, entonces m es par. Si $sgn(\sigma) = -1$, entonces m es impar.

Definición

Llamaremos permutaciones **pares** a las de signo 1 e impares a las de signo -1.

Las permutaciones pares de S_n forman un subgrupo normal de S_n, ya que son el núcleo del morfismo de grupos $sgn : S_n \to \{\pm 1\}$. Este subgrupo se denota A_n y recibe el nombre de **subgrupo alternado**. El índice de A_n en S_n es 2 porque $S_n/A_n \simeq \{\pm 1\}$; así que el teorema de Lagrange permite concluir que el orden de A_n es $n!/2$.