Ampliación Matemática Discreta

Justo Peralta López

Universidad de Almería
Departamento de Álgebra y Análisis Matemático

Definición

Un grupo es un conjunto de elementos sobre los cuales se define una operación binaria, a la cual notaremos . para la cual se verifican las siguientes propiedades.

G1 *Asociativa:* Para cualquier $a, b, c \in G$, $(a.b).c = a.(b.c)$

G2 *Identidad o Existencia de Elemento Neutro:* Existe un elemento $e \in g$ tal que para todo $x \in g$, $e.x = x.e = x$.

G3 *Inversa:* Para todo $x \in G$, existe un $x^{-1} \in G$ tal que $x.x^{-1} = x^{-1}.x = e$

con a, b y c elementos del grupo G.

Es fácil probar que el elemento neutro e es único y que el elemento inverso para cualquier elemento del grupo también lo es. Es más, $(a.b)^{-1} = b^{-1}.a^{-1}$

G4 *Conmutativa:* Para cualquier $a, b \in G$, $a.b = b.a$

Si un grupo verifica esta última propiedad, entonces decimos que el grupo es conmutativo o abeliano.

Ejemplo

1. $(Z, +)$, el anillo de los enteros con la suma, es un grupo respecto a la suma. Su elemento neutro es el 0 y el inverso de cualquier $x \in Z$ es $-x$.
2. $(Z_p, .)$ con p un primo, también tiene estructura de grupo. En este caso, el elemento identidad es el 1.
3. $(Z_4, +)$, con la adición módulo 4 es un grupo abeliano. La adición en Z_4, viene dada por la siguiente tabla

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

4. El conjunto de todas las $(n \times n)$ matrices sobre los números reales con la multiplicación es un grupo no abeliano, mientras que con la suma de matrices si lo es.
5. El conjunto $A(x)$ de todos los polinomios de la forma $a(x) = a_0 + a_1 x + a_2 x^2 + \ldots$, con $a_i \in Z_2$, es un grupo bajo la adición. En este caso, la inversa de cualquier polinomio es el mismo.

Definiciones

1. Un elemento a, se dice que *genera* un grupo G, si $a.a = a^2, a.a.a = a^3, \ldots,$ son todos los elementos del grupo. Entonces decimos que a es el *generador* de G y G es un grupo *cíclico*.
2. Un grupo G se dice que es cíclico si existe un elemento $a \in G$ tal que para todo $b \in G$, $b = a^j$ para algún entero j. Nótese que todo grupo cíclico es conmutativo.
3. El *orden* de un elemento$x$ es n, si n es el menor entero tal que

$$x^n = e$$

.
4. El número de elementos de un grupo es el *orden del grupo* . Como se puede observar, el orden de un grupo cíclico coincide con el orden de su elemento generador.

Ejemplo

1. Un ejemplo de grupo cíclico sería $(Z_4, +)$ con el 1 como generador del grupo.
2. En el grupo multiplicativo $G = \{1, 2, 3, 4\}$, con la multiplicación efectuada módulo 5, tenemos que $\{2, 2^2 = 4, 2^3 = 3, 2^4 = 1\}$. Luego, 2 es el generador de dicho grupo, y su orden es 4.

Definición

Para $a, b \in \mathbb{Z}$ y $n > 0$ un entero positivo, decimos que a es congruente con b módulo n, y escribimos ,$a \equiv_n b$, si $n|(a - b)$, es decir, si $a = b + kn$ para algún entero k.

La relación de congruencia es una relación de equivalencia definida sobre los enteros

Definición

El grupo formado por $\{[0], [1], \ldots, [n-1]\}$, las clases de equivalencia módulo n con la operación $+$ definida por $[a] + [b] = [a + b]$ es el grupo de enteros módulo n y lo notaremos por $\mathbb{Z}_n$

Nótese que $(\mathbb{Z}_n, +)$ es un grupo cíclico generado por $[1]$

Definición

Un grupo G es finito, si su número de elementos es finito. Al número de elementos de dicho grupo es el orden del grupo y lo notamos por $|G|$.

Definición

Un subconjunto H de un grupo G es un *subgrupo* si satisface todos los axiomas de grupo.

1. Los subgrupo *triviales* de G son G y $\{e\}$.
2. La operación del subgrupo debe ser, por supuesto, la misma que la del grupo.
3. Para determinar si un subconjunto H es un subgrupo de G, no necesitamos verificar todos los axiomas de grupo. Los siguientes dos axiomas son suficientes:
   - S1 Para todo $a, b \in H$, $a.b \in H$.
   - S2 Para todo $a \in H$, $a^{-1} \in H$.

   La asociativa en H es heredada de G. Y de (S1) y (S2), podemos mostrar que la identidad existe en H.

Ejemplo

$(H = \{0, 2\}, +)$, es un subgrupo de $(Z_4, +)$.

Definiciones

1. El subgrupo de G formado por todas las potencias de un elemento $a \in G$, se llama el grupo generado por A y lo notaremos por $< a >$. Si a es finito, entonces el orden del subgrupo es el orden de a.
2. Si S es un subconjunto no vacío de G y H un subgrupo de G formado por todos los productos finitos de potencias de elementos de S, entonces H es el subgrupo generado por S y $H =< S >$.

Teorema

Si H es un subgrupo de G, entonces la relación R_H en G definido por aR_Hb si y solo si $a = bh$ para algún $h \in H$, es una relación de equivalencia.

A R_H se le llama congruencia a izquierda módulo H, e induce una partición de G cuyas clases de equivalencia vienen dados por

$$[a] = aH = \{ah | h \in H\}$$

Ejemplo

Sea $G = \mathbb{Z}_{12}$ y H el subgrupo $\{[0], [3], [6], [9]\}$, entonces las clases a izquierda módulo H son

$$\begin{aligned} [0] + H &= \{[0], [3], [6], [9]\} \\ [1] + H &= \{[1], [4], [7], [10]\} \\ [2] + H &= \{[2], [5], [8], [11]\} \end{aligned}$$

Como se puede observar, si H es u subgrupo de G, todas las clases de G módulo H tienen el mismo número de elementos que H. Al número de esas clases se le llama *índice* de H en G, y se suele escribir por $[G : H]$.

Teorema

El orden de un grupo finito G viene dado por el producto del orden de cualquier subgrupo H de G por $[G : H]$. En particular, el orden de H divide al orden de G y el orden de cualquier elemento $a \in G$ divide el orden de G.

Teorema

1. *Todo subgrupo de un grupo cíclico es cíclico.*
2. *En un grupo cíclico finito $< a >$ de orden m, el elemento a^k genera un subgrupo de orden $m/mcd(k, m)$.*
3. *Sea d es un divisor positivo de m, donde m es el orden de un grupo cíclico finito $< a >$, entonces $< a >$ contiene uno y solo un subgrupo de índice d. Para cualquier divisor f de m, $< a >$ contiene un subgrupo de orden f.*
4. *Sea f un divisor entero del orden de un grupo cíclico finito $< a >$. Entonces $< a >$ contiene $\phi(f)$ elementos de orden f. $\phi(f)$ es la función de Euler y representa el número de enteros n, $1 \leq n \leq f$ coprimos a f.*
5. *Un grupo cíclico finito $< a >$ de orden m contiene $\phi(m)$ generadores. Los generadores son de la forma a^r con $mcd(r, m) = 1$.*

Definición

Un subgrupo H de G es llamado *normal* si $aha^{-1} \in H$ para todo $a \in G$ y $h \in H$.

Teorema

Si H es un subgrupo normal de G, entonces G/H es un grupo respecto la operación $(aH)(bH) = (ab)H$.

Algoritmo: Orden de un elemento de un grupo

Entrada: $|G| = n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, a.
Salida: *Orden de a*

1. $t := n$
2. *For* $i = 1$ *to* k *do*
   - 2.1 $t := t/p_i^{e_1}$
   - 2.2 $a_1 := a^t$
   - 2.3 *While* $a_1 \neq 1$ *do*
     $a_1 := a_1^{p_i}$
     $t := t.p_i$
3. *Return(t)*

Ejemplo

$|\mathbb{Z}_{13}^{\star}| = 6 = 2{,}3$ y $\mathbb{Z}_{13}^{\star} = \{1, 2, \dots, 12\}$.

Elemento	1	2	3	4	5	6	7	8	9	10	11	12
Orden	1	12	3	6	4	12	12	4	3	6	12	2

Algoritmo: Generador de un grupo cíclcio

Entrada: $|G| = n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.
Salida: *Generador* α *de* G.

1. $\alpha \in G$
2. *For* $ii = 1$ *to* k *do*

2.1 $b := \alpha^{n/p_i}$
2.2 *Si* $b = 1$ *ir a 1.*

3. *Return*(α)

Público

1. Un número primo p y un entero generador g de $\mathbb{Z}_p$
2. La clave pública $y \equiv g^x \ (mod\ p)$

Privado

1. Un entero x tal que $1 < x < p - 1$.

Cifrado (Acceso a la parte pública)

1. Escoger el mensaje a cifrar $1 < M < p$.
2. Generar número aleatorio $1 < k < p - 1$ con $(k, p - 1) = 1$.
3. Generar el par (r, s) para enviar con

$$r \equiv g^k \ (mod\ p)$$

$$s \equiv My^k \ (mod\ p)$$

Descifrado (Acceso a la parte privada)

1. Obtener $C = (r, s)$
2. $M \equiv \frac{s}{r^x} \ (mod\ p)$

Ejemplo

Sea $(p, g) = (107, 32)$ los parámetros de la parte pública y $x = 74$ la clave secreta. Entonces la clave pública del receptor viene dado por

$$y \equiv 32^{74} \equiv 53 \ (mod\ 107)$$

Si el emisor A quiere enviar al receptor B de forma secreta el mensaje $M = 82$, el emisor A escoge un número aleatorio $k = 49$ comprimo con $p - 1 = 106$. Entonces el cifrado de M viene dado por $C = (r, s)$ con

$$r \equiv 32^{49} \equiv 58 \ (mod\ 107)$$

$$s \equiv 82 * 53^{49} \equiv 28 \ (mod\ 107)$$

El receptor B recupera el mensaje M a partir de $C = (58, 28)$ calculando

$$M \equiv \frac{28}{58^{74}} \equiv \frac{28}{16} \equiv 82 \ (mod\ 107)$$