TEMA 1

Grupos, anillos y cuerpos

Contenidos

1. Grupos. Propiedades y tipos. Grupos cíclicos. Homomorfismos de grupos. Subgrupos normales y grupo cociente. Teorema de Lagrange.
2. Anillos y cuerpos.
3. Introducción a la teoría de codificación. Códigos de grupo.

Prerrequisitos: Teoría intuitiva de conjuntos. Funciones y sus propiedades. Operaciones con congruencias.

Objetivos: Saber reconocer y estudiar operaciones que dotan de estructura de grupo, anillo o cuerpo. Saber trabajar y operar en $\mathbb{Z}_n$ con las operaciones de suma y producto, conociendo sus propiedades en función de n. Saber trabajar y operar en el grupo de permutaciones S_n. Conocer los fundamentos de la teoría de codificación y trabajar con códigos de grupo.

En matemáticas, una *estructura algebraica* es un conjunto en el que se han establecido una o varias *operaciones*. Y una *operación interna* en un conjunto X es una regla que asigna a cada par de elementos x e y del conjunto, otro elemento z del mismo conjunto, que es el resultado de efectuar la operación entre x e y. Hablamos de operación interna porque el resultado de la operación está dentro del mismo conjunto. Por otra parte, aunque aquí decimos que la operación se aplica a dos elementos, también se pueden definir operaciones involucrando más elementos, pero en este curso solo vamos a trabajar con operaciones *binarias*. De manera formal, una operación binaria interna en un conjunto X es una función

$$\rho\colon X \times X \to X.$$

Sin embargo, cuando tratamos una función como un operador, lo habitual es utilizar un símbolo escrito de manera infija. Los símbolos habituales que se suelen utilizar son $+$, $\cdot$, $\times$, $*$,... y escribiríamos, por ejemplo, $x * y = \rho(x, y)$.

Como veremos, las características que diferencian a una estructura algebraica de otra son las propiedades de sus operadores. Por ejemplo, la primera que vamos a estudiar en este curso es la estructura de *grupo* y se caracteriza por tener una operación *asociativa*, con *elemento neutro* y *simétrico* de cada elemento.

1.1. Grupos

Definición 1.1.1 (Grupo) *Sea $*$ una operación binaria definida en un conjunto G. Se dice que $(G, *)$ es un* grupo *si se verifican las siguientes propiedades:*

1. *Asociativa: $(x * y) * z = x * (y * z)$, para todo $x, y, z \in G$.*
2. *Existencia de elemento neutro: existe un elemento $e \in G$ tal que $x*e = e*x = x$ para todo $x \in G$.*
3. *Existencia de elemento simétrico: para cada $x \in G$, existe $x' \in G$ tal que $x * x' = x' * x = e$.*

Y decimos que el grupo es abeliano *o* conmutativo *si además se verifica la propiedad*

4. *Conmutativa: $x * y = y * x$ para todo $x \in G$.*

Al trabajar con ejemplos concretos de grupos, es habitual optar por dos tipos de notaciones y nomenclaturas, la *aditiva* y la *multiplicativa*. Con la notación aditiva se usa el símbolo $+$, el elemento neutro se representa por 0 y el elemento simétrico se denomina opuesto y se denota por $-x$. Con la notación multiplicativa, se utilizan los símbolos $\cdot$ o $*$, el elemento neutro se denomina unidad, y se denota por 1, y el elemento simétrico se denomina inverso y se denota por x^{-1}.

Ejemplo 1.1.2
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$ son grupos abelianos.
- $(\mathbb{Q}^*, \cdot)$ y $(\mathbb{R}^*, \cdot)$ son grupos abelianos.
- $(\mathbb{N}, +)$ no es un grupo, ya que ningún elemento, excepto el 0, tiene opuesto. De la misma forma, $(\mathbb{N}, \cdot)$ no es un grupo, ya que ningún elemento, excepto el 1, tiene inverso.
- $(\mathbb{Z}, \cdot)$ no es un grupo, ya que ningún elemento, excepto 1 y -1, tiene inverso. □

Ejemplo 1.1.3 En el conjunto $\mathbb{Z}$ definimos la operación $x * y = x + y + 1$. Vamos a estudiar las propiedades que tiene.

- La operación es asociativa:

$$x * (y * z) = x + (y * z) + 1 = x + (y + z + 1) + 1 = x + y + z + 2$$
$$(x * y) * z = (x * y) + z + 1 = (x + y + 1) + z + 1 = x + y + z + 2$$

- $e = -1$ es elemento neutro para la operación:

$$(-1) * x = -1 + x + 1 = x; \qquad x * (-1) = x - 1 + 1 = x$$

- $x' = -x - 2$ es el elemento simétrico a x respecto del operado:

$$x * x' = x + (-x - 2) + 1 = x - x - 2 + 1 = -1 = e$$
$$x' * x = (-x - 2) + x + 1 = -x - 2 + x + 1 = -1 = e$$

- La operación es conmutativa: $x * y = x + y + 1 = y + x + 1 = y * x$.
- Por lo tanto, $(\mathbb{Z}, *)$ es un grupo abeliano. □

Vemos a continuación dos resultados con propiedades básicas en una estructura de grupo.

Teorema 1.1.4 *Sea $(G, *)$ un grupo..*

1. *El elemento neutro, e, es único.*
2. *Cada elemento tiene un único elemento simétrico.*
3. *El inverso es una operación* involutiva*, es decir, $(x^{-1})^{-1} = x$ para todo $x \in G$.*
4. *$(x * y)^{-1} = y^{-1} * x^{-1}$ para todo $x, y \in G$.*

TEOREMA 1.1.5 (CANCELACIÓN) *Sea $(G,*)$ un grupo y sean $x,y,z \in G$.*

1. *Si $x*y = x*z$, entonces $y = z$*
2. *Si $y*x = z*x$, entonces $y = z$*

Las demostraciones de estas propiedades son sencillas y se proponen como ejercicio al alumno. Por ejemplo, la demostración de las propiedades de cancelación consiste en la habitual operación de "multiplicar ambos lados" por el opuesto:

$$x*y = x*z \;\Rightarrow\; x'*(x*y) = x'*(x*z) \;\Rightarrow$$
$$\Rightarrow\; (x'*x)*y = (x'*x)*z \;\Rightarrow\; e*y = e*z \;\Rightarrow\; y = z$$

Obsérvese que, en el desarrollo, hemos usado las tres propiedades de la estructura de grupo. El mismo desarrollo es el que se usa para demostrar el siguiente teorema.

TEOREMA 1.1.6 *Si $(G,*)$ es un grupo y $a \in G$ entonces la siguiente función es biyectiva*

$$f\colon G \to G; \qquad f(x) = a*x$$

En los grupos finitos, la operación se puede especificar mediante una tabla, que se denomina *tabla de Cayley*.

EJEMPLO 1.1.7 Sea $H = \{1, \mathrm{i}, -1, -\mathrm{i}\} \subset \mathbb{C}$ y consideremos el grupo $(H,\cdot)$, con el producto habitual de números complejos, es decir, $\mathrm{i}\cdot\mathrm{i} = -1$. La tabla de Cayley del producto en este grupo es la siguiente:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

□

Como consecuencia del teorema anterior a este ejemplo, tenemos el siguiente resultado.

COROLARIO 1.1.8 *Si $(G,*)$ es un grupo finito, entonces la tabla de Cayley de la operación verifica que en cada fila y en cada columna los elementos de G aparecen exactamente una vez.*

DEFINICIÓN 1.1.9 (SUBGRUPO) *Sea $(G,*)$ un grupo y sea H un subconjunto de G no vacío. Se dice que H es un* subgrupo *de $(G,*)$ si $(H,*)$ es grupo.*

Naturalmente, para que H sea subgrupo de G, al menos tiene que contener al elemento neutro y de hecho $H = \{e\}$ constituye un subgrupo. Si H es distinto de $\{e\}$ distinto de G decimos que es un subgrupo *propio*.

Ejemplo 1.1.10

- $(\mathbb{Z}, +)$ es subgrupo propio de $(\mathbb{Q}, +)$ y de $(\mathbb{R}, +)$ y $(\mathbb{Q}, +)$ es subgrupo propio de $(\mathbb{R}, +)$.
- Si consideramos el conjunto $2\mathbb{Z} = \{2 \cdot x \ ; \ x \in \mathbb{Z}\}$, se verifica que $(2\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Z}, +)$. Podemos definir de la misma forma los subgrupos $n\mathbb{Z}$ para cada $n \in \mathbb{Z}^*$.

Teorema 1.1.11 (Caracterización de subgrupos) *Sea $(G, *)$ un grupo y sea H un subconjunto de G no vacío. Los siguientes enunciados son equivalentes.*

1. *H es un subgrupo de G.*
2. *Para todo $x, y \in H$: $x * y \in H$, $x^{-1} \in H$.*
3. *Para todo $x, y \in H$: $x * y^{-1} \in H$.*

En los grupos finitos, la caracterización de los subgrupos se simplifica:

Corolario 1.1.12 *Sea $(G, *)$ un grupo finito y sea H un subconjunto de G no vacío. $(H, *)$ es un subgrupo de $(G, *)$ si y solo si $x * y \in H$ para todo $x, y \in H$.*

Mientras que la unión de subgrupos no es en general un subgrupo, la intersección sí lo es.

Teorema 1.1.13 (Intersección de subgrupos) *Sea $(G, *)$ un grupo y sean H y K dos subgrupos de G. Entonces $H \cap K$ es un subgrupo de G.*

La demostración es una consecuencia inmediata del teorema de caracterización que hemos visto antes.

Ejemplo 1.1.14 $2\mathbb{Z}$ y $3\mathbb{Z}$ son dos subgrupos de $(\mathbb{Z}, +)$ y por lo tanto, $2\mathbb{Z} \cap 3\mathbb{Z}$ también lo es; de hecho, $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

Sin embargo, $2\mathbb{Z} \cup 3\mathbb{Z}$ no es un subgrupo de $(\mathbb{Z}, +)$, ya que la suma no es una operación interna en ese conjunto: $4 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, $9 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ y sin embargo, $4 + 9 = 13 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. □

Teorema 1.1.15 (Grupo producto) *Dados los grupos $(G, *)$ y $(H, \cdot)$, el* **producto directo** *$(G \times H, \oplus)$ es un grupo, donde la operación $\oplus$ se define como $(g_1, h_1) \oplus (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$.*

Ejemplo 1.1.16 $(\mathbb{R}\times\mathbb{R},+)$ es un grupo considerando la suma por coordenadas. En general, $(\mathbb{R}\times\cdots\times\mathbb{R},+)$ también es un grupo que se denota igualmente por $(\mathbb{R}^n,+)$. □

1.2. Los grupos $(\mathbb{Z}_n,+)$ y $(\mathbb{Z}_n^*,\cdot)$

En la asignatura de Matemática Discreta hemos introducido los conjuntos $\mathbb{Z}_n$ formados por las clases de congruencia módulo n. También hemos visto que la suma y el producto es compatible con la relación de congruencia, lo que significa que las operaciones de suma y producto son operaciones internas en $\mathbb{Z}_n$:

$$[x]_n+[y]_n=[x+y]_n, \qquad [x]_n\cdot[y]_n=[x\cdot y]_n,$$

Es más, la teoría de congruencias estudiada demuestra los siguientes resultados.

Teorema 1.2.1 *Para todo natural n mayor o igual que 2, se verifica que $(\mathbb{Z}_n,+)$ es un grupo abeliano, siendo $[0]_n$ el elemento neutro de la suma y $[-x]_n$ el elemento opuesto a $[x]_n$.*

Teorema 1.2.2 *Sea n un número natural mayor o igual que 2 y $\mathbb{Z}_n^*=\mathbb{Z}_n^*-\{[0]_n\}$.*

1. *La operación $\cdot$ es una operación interna en $\mathbb{Z}_n^*$.*
2. *$[1]_n$ es la unidad para la operación $\cdot$.*
3. *Si $\mathrm{mcd}(x,n)=1$, existe el inverso de x en $\mathbb{Z}_n^*$. En particular, si n es un número primo, $(\mathbb{Z}_n^*,\cdot)$ es un grupo abeliano.*

Ejemplo 1.2.3

1. Las tablas de Cayley para $(\mathbb{Z}_4,+)$ y $(\mathbb{Z}_5^*,\cdot)$.

$+_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\cdot_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

2. $(\{[1]_7,[2]_7,[4]_7\},\cdot)$ es subgrupo de $(\mathbb{Z}_7^*,\cdot)$: la tabla de Cayley muestra que el producto es interno en ese subconjunto

$\cdot_7$	$[1]_7$	$[2]_7$	$[4]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[4]_7$
$[2]_7$	$[2]_7$	$[4]_7$	$[1]_7$
$[4]_7$	$[4]_7$	$[1]_7$	$[2]_7$

3. $(\{[0]_6, [2]_6, [4]_6]\}, +)$ es subgrupo de $(\mathbb{Z}_6, +)$.

En adelante, por simplicidad, vamos a identificar los elementos de $\mathbb{Z}_n$ con su representante tomado entre 0 y $n-1$. De esta forma, no hará falta escribir los corchetes ni los subíndices. Por ejemplo, la tabla de Cayley de la suma en $\mathbb{Z}_4$ sería

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

También podremos omitir el subíndice en los operadores si no da lugar a confusiones.

Ejemplo 1.2.4 En la asignatura de Matemática Discreta hemos aprendido a calcular el inverso de un número respecto de un módulo. Por ejemplo, 6 es inversible en $\mathbb{Z}_{17}$ y el algoritmo de Euclides, en su forma vectorial simplificada, nos permite calcular su inverso.

$$\left\lfloor \frac{17}{6} \right\rfloor = 2 \quad \rightsquigarrow \quad \begin{pmatrix} 17 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$$

$$\left\lfloor \frac{6}{5} \right\rfloor = 1 \quad \rightsquigarrow \quad \begin{pmatrix} 6 \\ 1 \end{pmatrix} - \begin{pmatrix} 5 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Por lo tanto, 3 es el inverso de 6 módulo 17. □

Ejemplo 1.2.5 En la sección dedicada a la teoría de codificación, vamos a trabajar con los grupos $(\mathbb{Z}_2^n, \oplus)$ definidos como producto directo $(\mathbb{Z}_2, +_2)$. En estos casos, omitiremos los paréntesis y las comas que separan los elementos de las tuplas. Por ejemplo, la tabla de Cayley del grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ es

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

□

1.3. Grupo simétrico

El *grupo simétrico* sobre un conjunto X, denotado por $(S_X, \circ)$, es el grupo formado por las aplicaciones biyectivas de X en sí mismo con la composición de funciones como operación interna. Si el conjunto es finito, se denomina igualmente *grupo de permutaciones* y se denota por S_n, siendo n el número de elementos del conjunto X. Concretamente, consideramos S_n como el grupo de las permutaciones del conjunto $\mathbb{N}_n = \{1, 2, \ldots, n\}$.

Las permutaciones de $\mathbb{N}_n = \{1, 2, \ldots, n\}$ se denotarán por listas de longitud n con los elementos de $\mathbb{N}_n$ sin repeticiones. Por ejemplo, $[2, 3, 1, 4]\colon \mathbb{N}_4 \to \mathbb{N}_4$ es el elemento S_4 tal que

$$[2,3,1,4](1) = 2$$
$$[2,3,1,4](2) = 3$$
$$[2,3,1,4](3) = 1$$
$$[2,3,1,4](4) = 4$$

Con esta notación, el elemento neutro, la función identidad, es $i = [1, 2, \ldots, n]$ y la composición de permutaciones y el inverso de una permutación vienen dadas por:

1. Si $\ell_1, \ell_2 \in S_n$, entonces $\ell_1 \circ \ell_2 = [c_i; i = 1, \ldots, n]$, en donde, $c_i = \ell_1(\ell_2(i))$.
2. Si $\ell \in S_n$, entonces $\ell^{-1} = [a_i; i = 1, \ldots, n]$, en donde, $a_i = k$ si y solo si $\ell(k) = i$.

Ejemplo 1.3.1 En $(S_5, \circ)$, consideramos las siguientes permutaciones

$$\sigma = [3, 4, 1, 5, 2] \qquad \rho = [5, 3, 4, 2, 1]$$

Entonces:

- $\sigma \circ \rho = [3, 4, 1, 5, 2] \circ [5, 3, 4, 2, 1] = [2, 1, 5, 4, 3]$.
- $\rho \circ \sigma = [5, 3, 4, 2, 1] \circ [3, 4, 1, 5, 2] = [4, 2, 5, 1, 3]$. Por lo tanto, la operación no es conmutativa.
- $\sigma^{-1} = [3, 4, 1, 5, 2]^{-1} = [3, 5, 1, 2, 4]$.
- $\rho^{-1} = [5, 3, 4, 2, 1]^{-1} = [5, 4, 2, 3, 1]$. □

La importancia de los grupos simétricos está en el teorema de Cayley que veremos más adelante y que establece que cualquier grupo es esencialmente un subgrupo de grupo simétrico.

1.4. Grupos cíclicos

Definición 1.4.1 (Orden de un elemento) *Sea $(G, *)$ un grupo con elemento neutro e y sea $x \in G$. El* orden *de un elemento x es el menor entero positivo n tal que*

$$\underbrace{x * \cdots * x}_{n} = e.$$

Si no existe tal entero, se dice que el elemento x tiene orden infinito.

Si utilizamos el operador de grupo con la notación multiplicativa, escribiremos

$$x^n = \underbrace{x * \cdots * x}_{n}.$$

Ejemplo 1.4.2

- En el grupo $(\mathbb{Z}_6, +_6)$, el orden de 4 es 3, ya que

$$4 +_6 4 = 2, \qquad \text{y} \qquad 4 +_6 4 +_6 4 = 0$$

- En el grupo $(\mathbb{Z}_7^*, \cdot_7)$, el orden de 2 es 3, ya que

$$2 \cdot_7 2 = 4 \qquad \text{y} \qquad 2 \cdot_7 2 \cdot_7 2 = 1$$

- En el grupo $(S_4, \circ)$, el elemento neutro o unidad es $[1, 2, 3, 4]$ y, por ejemplo, el orden de $[4, 1, 2, 3]$ es 4, ya que

$$\begin{aligned}
[4,1,2,3] \circ [4,1,2,3] &= [3,4,1,2] \\
[4,1,2,3] \circ [4,1,2,3] \circ [4,1,2,3] &= [3,4,1,2] \circ [4,1,2,3] = [2,3,4,1] \\
[4,1,2,3] \circ [4,1,2,3] \circ [4,1,2,3] \circ [4,1,2,3] &= [2,3,4,1] \circ [4,1,2,3] = [1,2,3,4]
\end{aligned}$$

□

Teorema 1.4.3 (Subgrupo generado por un elemento) *Sea $(G, *)$ un grupo y $c \in G$. El mínimo subgrupo de G que contiene a c es $\{c^n; n \in \mathbb{Z}\}$. Este subgrupo se denota $\langle c \rangle$ y se denomina subgrupo (cíclico) generado por c. Si $G = \langle c \rangle$, decimos que G es un grupo cíclico.*

Ejemplo 1.4.4

- En $(\mathbb{C}^*, \cdot)$, el subgrupo $\mathbb{H} = (\{1, \mathrm{i}, -1, -\mathrm{i}\}, \cdot)$ esta generado por i:

$$\langle \mathrm{i} \rangle = \{\mathrm{i}, \mathrm{i}^2, \mathrm{i}^3, \mathrm{i}^4\} = \{\mathrm{i}, -1, -\mathrm{i}, 1\}$$

- En el grupo $(\mathbb{Z}_7^*, \cdot_7)$, el subgrupo generado por 2 es:

$$\langle 2 \rangle = \{2,\ 2 \cdot_7 2,\ 2 \cdot_7 2 \cdot_7 2\} = \{2, 4, 1\}$$

- En el grupo $(S_4, \circ)$, el subgrupo generado por $[4, 1, 2, 3]$ es

$$\begin{aligned}
\langle [4,1,2,3] \rangle = \{&[4,1,2,3], [4,1,2,3]^2, [4,1,2,3]^3, [4,1,2,3]^4\} = \\
&= \{[4,1,2,3], [3,4,1,2], [2,3,4,1], [1,2,3,4]\}
\end{aligned}$$

□

- El grupo $(\mathbb{Z}_7, +_7)$ es cíclico, y está generado por $[4]_7$, ya que:

$$\begin{aligned} 4 +_7 4 &= 1 \\ 1 +_7 4 &= 5 \\ 5 +_7 4 &= 2 \\ 2 +_7 4 &= 6 \\ 6 +_7 4 &= 3 \\ 3 +_7 4 &= 0 \\ 0 +_7 4 &= 4 \end{aligned}$$

  En general, todos los grupo $(\mathbb{Z}_n, +_n)$ son cíclicos.

- Es fácil demostrar que todo grupo cíclico es abeliano, aunque hay grupos abelianos que no son cíclicos, como $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$. □

1.5. Homomorfismos e isomorfismos de grupos

Definición 1.5.1 (Homomorfismo de grupos) *Dados dos grupos $(G, *)$ y $(H, \cdot)$, una función $\psi\colon G \to H$ es un* homomorfismo de grupos *si para todo $x, y \in G$ se verifica que $\psi(x * y) = \psi(x) \cdot \psi(y)$.*

Teorema 1.5.2 (Propiedes de los homomorfismos de grupos)
Sea $\psi\colon G \to H$ un homomorfismo de grupos, entonces:

1. *ψ conserva el elemento neutro: $\psi\big(e_G\big) = e_H$*
2. *ψ conserva el elemento simétrico: $\psi(a^{-1}) = \big(\psi(a)\big)^{-1}$*
3. *La imagen de cada subgrupo de G es un subgrupo de H.*
4. *La preimagen de cada subgrupo de H es un subgrupo de G*

Definición 1.5.3 (Isomorfismo de grupos) *Sean los grupos $(G, *)$ y $(H, \cdot)$. Se dice que una función $\psi\colon G \to H$ es un* isomorfismo de grupos *si es biyectiva y homomorfismo de grupos.*

Ejemplo 1.5.4 Las siguientes funcione son isomorfismos de grupo

$$\begin{array}{rccc} f\colon & (\mathbb{Z}_4, +_4) & \to & (\mathbb{Z}_5^*, \cdot_5) \\ & [0]_4 & \mapsto & [1]_5 \\ & [1]_4 & \mapsto & [2]_5 \\ & [2]_4 & \mapsto & [4]_5 \\ & [3]_4 & \mapsto & [3]_5 \end{array} \qquad \begin{array}{rccc} g\colon & (\mathbb{Z}_4, +_4) & \to & (\mathbb{Z}_5^*, \times_5) \\ & [0]_4 & \mapsto & [1]_5 \\ & [1]_4 & \mapsto & [3]_5 \\ & [2]_4 & \mapsto & [4]_5 \\ & [3]_4 & \mapsto & [2]_5 \end{array}$$

En este ejemplo, vemos que entre dos grupos isomorfos puede haber más de un isomorfismo. □

Como es habitual en matemáticas, el concepto de isomorfismo supone los grupos isomorfos son indistinguibles en cuanto a la estructura de grupo y comparten todas las propiedades asociadas a esa estructura.

TEOREMA 1.5.5 *Si $\psi\colon G \to H$ es un isomorfismo entre los grupos $(G,*)$ y $(H,\cdot)$, entonces:*

1. *$(G,*)$ es abeliano si y solo si $(H,\cdot)$ es abeliano.*
2. *$(G,*)$ es cíclico si y solo si $(H,\cdot)$ es cíclico.*
3. *Para todo $c \in G$, el orden de c coincide con el de $\psi(c)$.*
4. *La función inversa $\psi^{-1}\colon H \to G$ es un isomorfismo de $(H,\cdot)$ en $(G,*)$.*

En particular, todos los grupos cíclicos finitos son isomorfos a un grupo $(\mathbb{Z}_n,+)$ y los grupos cíclicos infinitos son isomorfos a $(\mathbb{Z},+)$. Otra caracterización de grupos mediante isomorfismos es la siguiente.

TEOREMA 1.5.6 (DE CAYLEY) *Todo grupo es isomorfo a un subgrupo de un grupo simétrico. Si un grupo es finito y tiene n elementos, entonces es isomorfo a un subgrupo de S_n.*

1.6. Clases laterales y grupos cociente

DEFINICIÓN 1.6.1 (CLASES LATERALES) *Sea H un subgrupo de $(G,*)$ y sea $x \in G$.*

- *La* clase lateral izquierda de a respecto de H *es el conjunto*

$$x * H = \{x * y; y \in H\}$$

- *La* clase lateral derecha de a respecto de H *es el conjunto*

$$H * x = \{y * x; y \in H\}$$

Dos clase laterales son, o bien iguales, o bien disjuntas y, por lo tanto, un subgrupo H induce dos particiones de G:

$$G/H = \{a * H; a \in G\} \qquad G\backslash H = \{H * a; a \in G\}$$

Por otra parte, si el grupo G es abeliano las clases laterales izquierda y derecha coincide y $G/H = G\backslash H$. Aunque no es necesario que el grupo sea abeliano para que las dos clases coincidan.

Definición 1.6.2 (Subgrupo normal) *Sea H un subgrupo de un grupo $(G, *)$. Se dice que H es un* subgrupo normal *si para cada $x \in G$ se tiene que $x * H = H * x$.*

Un subgrupo normal permite definir el *grupo cociente*, de forma análoga al *conjunto cociente* respecto de una relación de equivalencia: $G/H = G\backslash H$ por definición y podemos definir la operación $(a * H) \circledast (b * H) = (a * b) * H$.

Teorema 1.6.3 *Si H es subgrupo normal de $(G, *)$, entonces $(G/H, \circledast)$ es un grupo con la operación*

$$(a * H) \circledast (b * H) = (a * b) * H,$$

siendo $e * H = H$ el elemento neutro.

Si tomamos dos elementos x, y, de una misma clase lateral, entonces $x*H = y*H$ y por lo tanto $(x * H) \circledast (y^{-1} * H) = e * H = H$. Entonces, $(x * y^{-1}) * H = H$ y deducimos que $x * y^{-1} \in H$.

Corolario 1.6.4 *Si H es subgrupo normal de $(G, *)$, entonces x, y son elementos de una misma clase lateral si y solo si $x * y^{-1} \in H$.*

Ejemplo 1.6.5 Ya hemos visto que $3\mathbb{Z}$ es un subgrupo de $(\mathbb{Z}, +)$ y dado que este grupo es abeliano, el subgrupo es normal. Este subgrupo tiene 3 clases laterales

$$0 + 3\mathbb{Z}, \qquad 1 + 3\mathbb{Z}, \qquad 2 + 3\mathbb{Z}$$

Entonces, el grupo cociente $\mathbb{Z}/3\mathbb{Z}$ es isomorfo a $\mathbb{Z}_3$; la siguiente función es un isomorfismo

$$\begin{array}{rccc} f\colon & (\mathbb{Z}/3\mathbb{Z}, \oplus) & \to & (\mathbb{Z}_3, +_3) \\ & 0 + 3\mathbb{Z} & \mapsto & 0 \\ & 1 + 3\mathbb{Z} & \mapsto & 1 \\ & 2 + 3\mathbb{Z} & \mapsto & 2 \end{array}$$

En general, los grupos $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ y $(\mathbb{Z}_n, +_n)$ son isomorfos para cada natural n mayor que 2. □

Los grupos $(\mathbb{Z}_2^n, \oplus)$ son conmutativos y, por lo tanto, sus subgrupos son normales. En esto se basa la teoría de la codificación que vamos a estudiar más adelante.

Si $(G, *)$ es un grupo finito y H un subgrupo, entonces cada clase lateral de H tiene el mismo número de elementos. Como además, el conjunto de clases laterales es una partición de G, obtenemos como consecuencia el siguiente resultado.

Teorema 1.6.6 (Lagrange) *Si H es un subgrupo de un grupo finito $(G, *)$, entonces el cardinal de H divide al cardinal de G.*

Una consecuencia del teorema de Lagrange es que el orden de cada elemento de G es un divisor de su cardinal y, por lo tanto, los grupos con un cardinal primo son necesariamente cíclicos. Naturalmente, el recíproco no es cierto; por ejemplo, $(\mathbb{Z}_n, +_n)$ es cíclico aunque su cardinal n, no sea primo.

1.7. Anillos y cuerpos

Como sabemos, en los conjuntos numéricos con los que trabajamos habitualmente, disponemos de dos operaciones, una multiplicativa y otra aditiva, y las dos están relacionadas por la *propiedad distributiva*. La estructura más básica de un conjunto con dos operaciones relacionadas con esta propiedad es la de *anillo*.

Definición 1.7.1 (Anillo) *Se dice que $(A, +, \cdot)$ es un* anillo *si $+$ y $\cdot$ son dos operaciones binarias en A tales que:*

1. *$(A, +)$ es grupo abeliano.*
2. *La operación $\cdot$ es asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
3. *La operación $\cdot$ es distributiva respecto de $+$:*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

4. *Decimos que el anillo es* conmutativo *si la operación $\cdot$ es conmutativa. En general, $x, y \in A$ se dicen* permutables *si $x \cdot y = y \cdot x$; por lo tanto, un anillo es conmutativo si cada par de elementos es permutable.*
5. *Decimos que el anillo es* unitario *si la operación $\cdot$ tiene unidad. En este tipo de anillos, algunos elementos pueden tener inverso, a esos elementos se les denomina* elementos invertibles.

Ejemplo 1.7.2

1. $(m\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, pero no es unitario.
2. $(\mathbb{Z}_m, +_m, \cdot_m)$ es un anillo conmutativo y unitario, pero no contiene elementos invertibles distintos de 1.
3. El conjunto de las matrices cuadradas con la suma y producto habituales, $(\mathcal{M}_{n\times n}(\mathbb{R}), +, \cdot)$, forman un anillo unitario. Sabemos que este anillo no es necesariamente conmutativo y que tiene elementos invertibles y elementos que no son invertibles. □

Teorema 1.7.3 *Sea $(A, +, \cdot)$ un anillo. Para todo $a, b \in A$ se verifica:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Definición 1.7.4 (Divisor de cero) *Si $(A, +, \cdot)$ es un anillo. Decimos que un elemento de A, $x \neq 0$, es* divisor de cero *si existe $y \neq 0$ tal que $x \cdot y = 0$ o bien $y \cdot x = 0$.*

Ejemplo 1.7.5

- En $(\mathbb{Z}_{36}, +_{36}, \cdot_{36})$, el elemento 4 es un divisor de cero, ya que $4 \cdot_{36} 9 = 0$.
- En $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \cdot)$, la matriz $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ es un divisor de cero, ya que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

□

Definición 1.7.6 (Cuerpo) *Un anillo $(K, +, \cdot)$ se dice que es un* **cuerpo** *si $(K - \{0\}, \cdot)$ es un grupo abeliano.*

Definición 1.7.7 (Subanillo/Subcuerpo) *Sea $(A, +, \cdot)$ un anillo (resp. cuerpo) y sea B un subconjunto de A no vacío. Se dice que B es* subanillo *(resp. subcuerpo) de A si B es anillo (resp. cuerpo) con las mismas operaciones que A.*

Los conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos con la suma y el producto habituales. $\mathbb{Q}$ es subcuerpo de $\mathbb{R}$ y este es, a su vez, subcuerpo de $\mathbb{C}$.

Definición 1.7.8 (Isomorfismo) *Dados anillos (resp. cuerpos) $(A, +, \cdot)$ y $(B, *, \bullet)$ son* isomorfos *si existe una función $\varphi\colon A \to B$ que es biyectiva y* homomorfismo de anillos*, es decir, verifica las siguientes propiedades*

$$\varphi(a_1 + a_2) = \varphi(a_1) * \varphi(a_2) \qquad \varphi(a_1 \cdot a_2) = \varphi(a_1) \bullet \varphi(a_2)$$

Ejemplo 1.7.9 Otros cuerpos de gran importancia en computación, y concretamente en criptografía y codificación, son los cuerpos $(\mathbb{Z}_p, +_p, \cdot_p)$, en donde p es un número primo. De hecho, ya sabemos que $\mathbb{Z}_n$ es cuerpo si y solo si n es primo, porque si n es compuesto, el anillo contiene elementos no invertibles. Sin embargo, estos no son los únicos cuerpos finitos; se sabe que, para cada número primo p y cada $n \in \mathbb{Z}^+$, existe exactamente un cuerpo, salvo isomorfismo, con p^n elementos. □

1.8. Introducción a la teoría de codificación

Cuando transmitimos información a través de algún canal (cable, radio, wifi,...) el mensaje puede distorsionarse por diversas circunstancias; incluso los mejores sistemas de telecomunicaciones tienen una tasa de error distinta de cero. Cuando guardamos un archivo en un disco duro y lo leemos poco después, podemos encontrarnos con que el archivo se ha distorsionado; por ejemplo, debido a defectos microscópicos en el material del disco. Este tipo de errores, pueden llevar, en muchos casos, a graves consecuencias.

La *Teoría de la codificación* es el área de la computación que se encarga de analizar estos problemas y minimizar sus consecuencias. Concretamente, en esta sección vamos a ver como se pueden abordar con las herramientas que nos da el álgebra y específicamente la teoría de grupos.

En general, un mensaje es una cadena de símbolos de un determinado alfabeto y en el caso concreto de comunicación digital, este alfabeto estará formado por los dígitos 0 y 1, es decir, los elementos del grupo $(\mathbb{Z}_2, \oplus)$. También se pueden utilizar alfabetos no binarios y símbolos de algún cuerpo finito, aunque en este curso nos concentraremos en el caso binario.

Un ejemplo sencillo de codificación sería el siguiente. Como decíamos, la comunicación de información consiste en transmitir cadenas de ceros y unos y normalmente eso se hace en lotes o paquetes de una determinada longitud. Supongamos que x es uno de estos lotes, es decir una cadena de ceros y unos. Pues bien, en lugar de transmitir simplemente la cadena x, lo que podemos hacer es transmitirla dos veces, es decir, enviamos xx. Si durante la transmisión se produce alguna distorsión, el receptor recibirá una cadena $x_1x_2 \neq xx$. Este sistema básico se completaría haciendo que el receptor calcule $\sum(x_1 \oplus x_2) = d$; si $d = 1$ podemos estar seguros que $x_1 \neq x_2$ y que ha habido algún problema y el sistema podría requerir que se vuelva a enviar el mensaje; si $d = 0$ no podemos afirmar que el mensaje se haya transmitido correctamente, pero hemos reducido considerablemente la probabilidad.

El sistema anterior se podría mejorar haciendo que el paquete se envíe por triplicado, xxx. En este caso, si el receptor recibe la cadena $x_1x_2x_3$, puede "decodificar" el mensaje considerando que $x = x_1 \oplus x_2 \oplus x_3$. Obsérvese que si en la transmisión solo se ha producido un error, ese será exactamente el que diferencie x de x_1 y podremos corregirlo.

Ese es el objetivo de la teoría de la codificación, diseñar sistemas algebraicos que permitan saber si se ha producido un error en la comunicación e incluso corregirlo.

En lo sucesivo, nos referiremos a cada bloque del mensaje como *palabra*, es decir, un elemento de $\mathbb{Z}_2^m$ que por simplicidad escribiremos sin paréntesis ni comas entre los números. Los mensajes siempre se dividirán en palabras de la misma longitud.

Una *función de codificación* (m, n) es una función inyectiva $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$, en donde $n > m$. De esta forma, para cada palabra $x \in \mathbb{Z}_2^m$, la imagen $\mathcal{C}(x)$ es la *palabra codificada* que se transmite. El conjunto imagen, $\mathrm{Im}(\mathcal{C})$ se denomina *codigo* y sus elementos se denomina *palabras clave*.

El *peso (de Hamming)* de una palabra x es el número de unos que contiene y se denota $|x|$. La *distancia (de Hamming)* entre dos palabras de la misma longitud es el peso de la diferencia:

$$\delta(u, v) = |u \oplus v|$$

Por ejemplo,

$$|10001| = 2, \qquad \delta(11011, 10101) = |01110| = 3$$

El número de errores cometidos en la transmisión de una palabra x es la distancia entre la palabra transmitida y la palabra recibida. Las palabras clave serán las palabras correctamente recibidas, y el resto de las palabras del codominio de la función de codificación serán las posibles palabras recibidas si se produce algún error en la transmisión. Por esta razón, una buena función de codificación será aquella que maximice las distancias entre palabras clave.

Algunas propiedades destacadas de la distancia son las siguientes: para cualesquiera $x, y, z \in \mathbb{Z}_2^m$

1. $\delta(x, y) = \delta(y, x)$
2. $\delta(x, y) \geq 0$
3. $\delta(x, y) = 0 \iff x = y$
4. $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Si $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ es una función de codificación (m, n), decimos que $\mathcal{C}(x)$ se ha transmitido con *a lo sumo k errores* si $1 \leq \delta(\mathcal{C}(x), v) \leq k$, en donde, v es la palabra recibida al enviar la palabra clave $\mathcal{C}(x)$. Se dice que la función $\mathcal{C}$ *detecta a lo sumo k errores* si al enviar una palabra con a lo sumo k errores, no se recibe una palabra clave. La *mínima distancia* de una función de codificación es por tanto

$$\min\big\{\delta(\mathcal{C}(x), \mathcal{C}(y)) \mid x, y \in \mathbb{Z}_2^m,\ x \neq y\big\}$$

Teorema 1.8.1 *Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ una función de codificación (m, n), entonces:*

1. *$\mathcal{C}$ permite detectar a lo sumo k errores si y solo si la mínima distancia de $\mathcal{C}$ es al menos $k + 1$.*
2. *$\mathcal{C}$ permite corregir a lo sumo k errores si y solo si la mínima distancia de $\mathcal{C}$ es al menos $2k + 1$.*

Ejemplo 1.8.2 La minima distancia de la función de codificación $\mathcal{C}\colon \mathbb{Z}_2^4 \to \mathbb{Z}_2^9$ definida a continuación es 3,

$$\mathcal{C}(x) = xxb, \qquad \text{en donde } b = \begin{cases} 0, & |x| \text{ es par} \\ 1, & |x| \text{ es impar} \end{cases}$$

y por lo tanto, esta función de codificación detecta $3 - 1 = 2$ errores. □

Definición 1.8.3 (Código de grupo o lineal) *Decimos que una función de codificación $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ es un* código de grupo *o un* codigo lineal*, si es un homomorfismo de grupos.*

Si trabajamos con códigos de grupo, el conjunto $\mathrm{Im}(\mathcal{C})$ es un subgrupo de $\mathbb{Z}_2^n$, y esto permite simplificar el cálculo de la distancia mínima, ya que

$$|\mathcal{C}(x) \oplus \mathcal{C}(y)| = |\mathcal{C}(x \oplus y)| = |\mathcal{C}(z)|, \qquad \text{para algún } z \in \mathbb{Z}_2^m,$$

y de ahí se deduce el siguiente resultado.

Teorema 1.8.4 *Si $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ es un código de grupo, entonces la mínima distancia de $\mathcal{C}$ coincide con el mínimo peso de las palabras clave no nulas. Es decir,*

$$\text{mín}\{\delta(\mathcal{C}(x), \mathcal{C}(y)); x, y \in \mathbb{Z}_2^m, x \neq y\} = \text{mín}\{|\mathcal{C}(x)|; x \in \mathbb{Z}_2^m, x \neq 0\}$$

Por ejemplo, en un código de grupo (m, n) en lugar de hacer $\dfrac{m(m-1)}{2}$ comparaciones, solo tendremos que hacer $m - 1$ cálculos de peso.

Ejemplo 1.8.5 Consideremos la siguiente matriz 2×4 cuyos elementos están en $\mathbb{Z}_2$,

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Con el producto habitual de matrices (considerando la suma y el producto en $\mathbb{Z}_2$), podemos definir la siguiente función

$$\mathcal{C}_\mathcal{G}\colon \mathbb{Z}_2^2 \to \mathbb{Z}_2^4, \qquad \mathcal{C}_\mathcal{G}(x) = x\mathcal{G}$$

Es decir,

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 0000 \\ \mathcal{C}_\mathcal{G}(01) &= 0101 \\ \mathcal{C}_\mathcal{G}(10) &= 1011 \\ \mathcal{C}_\mathcal{G}(11) &= 1110 \end{aligned}$$

Las propiedades del producto de matrices permite demostrar fácilmente que esta función es un código de grupo $(2, 5)$. Teniendo en cuenta el teorema anterior, la distancia mínima de este código es

$$\text{mín}\{|\mathcal{C}(x)|; x \in \mathbb{Z}_2^m, x \neq 0\} = \text{mín}\{|0101|,\ |1011|,\ |1110|\} = 2$$

Y por lo tanto, este código puede detectar $2 - 1 = 1$ error pero no puede corregir ninguno. □

En la practica, es suficiente trabajar con códigos de grupo definidos como en ejemplo anterior, usando matrices de la forma

$$\mathcal{G} = \big(I_m \mid A\big)$$

en donde I_m es la matriz identidad $m \times m$ y A es una matriz $m \times (n - m)$. En este caso, la salida de la función responde al siguiente esquema

$$\mathcal{C}(b_1 b_2 \dots b_m) = \underbrace{b_1 b_2 \dots b_m}_{\text{mensaje}} \underbrace{c_1 c_2 \dots c_{n-m}}_{\text{sim. control}}$$

Definición 1.8.6 (Matriz generadora $\mathcal{G}$ de un código de grupo)
Sean $m, n \in \mathbb{Z}$, con $m < n$. Una matriz generadora $\mathcal{G}$ *es una matriz $m \times n$ con entradas en $\mathbb{Z}_2$ tal que las primeras m columnas forman la matriz identidad: $\mathcal{G} = \big(I_m \mid A\big)$. La función $\mathcal{C}_\mathcal{G} \colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ definido por $\mathcal{C}_\mathcal{G}(x) = x\mathcal{G}$ es el código de grupo definido por la matriz generadora.*

La segunda parte del problema que estamos abordando es la decodificación de los mensajes recibidos. Si la palabra recibida es una palabra clave, quiere decir que el mensaje se ha recibido sin errores y los primeros bits coinciden con palabra original. Pero si la palabra recibida no es una palabra clave, buscaremos la palabra clave más próxima y que la consideraremos la palabra decodificada. En el siguiente ejemplo, vamos a ver una forma simple, pero ineficiente, de buscar esta palabra usando la tabla de descodificación, que se construye con las clases laterales del grupo $\text{Im}(\mathcal{C})$.

Ejemplo 1.8.7 Sea la función de codificación $\mathcal{C}_\mathcal{G} \colon \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$ dada por la matriz generadora $\mathcal{G}$

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 00000 \\ \mathcal{C}_\mathcal{G}(01) &= 01011 \\ \mathcal{C}_\mathcal{G}(10) &= 10110 \\ \mathcal{C}_\mathcal{G}(11) &= \underbrace{11101}_{\mathcal{W}=\text{Im}\,(\mathcal{C})} \end{aligned}$$

Si recibimos una palabra que no es clave y el error se ha producido en el primer bit, la palabra recibida estará en la clase lateral $00001 \oplus \mathcal{W}$; si recibimos una palabra

que no es clave y el error se ha producido en el segundo bit, la palabra recibida estará en la clase lateral $00010 \oplus \mathcal{W}$; así, sucesivamente, podemos situar todas las posibles palabras recibidas en alguna clase lateral del código, que podemos visualizar en una tabla como la mostrada a continuación para este ejemplo

$\mathrm{Im}(\mathcal{C}) = \mathcal{W}$	00000	01011	10110	11101
$00001 \oplus \mathcal{W}$	00001	01010	10111	11100
$00010 \oplus \mathcal{W}$	00010	01001	10100	11111
$00100 \oplus \mathcal{W}$	00100	01111	10010	11001
$01000 \oplus \mathcal{W}$	01000	00011	11110	10101
$10000 \oplus \mathcal{W}$	10000	11011	00110	01101
$00101 \oplus \mathcal{W}$	00101	01110	10011	11000
$10001 \oplus \mathcal{W}$	10001	11010	00111	01100

De esta forma, sabemos que la palabra clave más cercana a una recibida es la que aparece en la primera fila de la columna en donde aparece la palabra recibida. Por ejemplo, si recibimos la palabra $v = 11110$, la palabra clave más cercana es 10110 y consideraremos que ese era el mensaje original, es decir, ese será el mensaje decodificado.

Continuando con el ejemplo, supongamos que queremos enviar un mensaje formado por las palabras

00 01 10 11 11 01 00

Lo codificamos con la matriz $\mathcal{G}$ y enviamos las siguientes palabras

00000 01011 10110 11101 11101 01011 00000

Sin embargo, el mensaje se distorsiona y se recibe

00000 00011 11100 11101 10101 11101 01000

Hemos indicado en rojo los bits que no son correctos; vemos que algunas palabras tienen tres errores, otras dos errores y otras solo uno. Al decodificar el mensaje usando la tabla de descodificación como hemos dicho antes, obtenemos

00000 01010 11101 11101 11101 11101 00000

Y eliminando los tres últimos dígitos, los de control, nos queda el siguente mensaje:

00 01 11 11 11 11 00

Podemos ver que las palabras en las que el envío solo había provocado un error se han corregido con la decodificación, pero las palabras en las que el envío provocó más de dos errores, no se han podido corregir. Esto ya sabíamos que podía ocurrir, puesto que la distancia mínima del código es $3 = 2 \cdot 1 + 1$ y por lo tanto, puede corregir a los sumo un error. □

En el ejemplo anterior, hemos necesitado construir la tabla de codificación para poder decodificar el mensaje recibido. Sin embargo, al trabajar con códigos de grupo, podemos utilizar las propiedades del homomorfismo que define el código para decodificar los mensajes de forma más simple.

Teorema 1.8.8 (Matriz de verificación de paridad) *Dada una matriz generadora* $\mathcal{G} = \big(I_m \mid A\big)$*, consideramos la matriz*

$$\mathcal{H} = \begin{pmatrix} A \\ I_{n-m} \end{pmatrix},$$

que se denomina matriz de verificación de paridad asociada es la matriz $\mathcal{G}$*. Entonces, el producto* $\mathcal{G}\mathcal{H}$ *es la matriz nula de tamaño* $m \times (n-m)$ *y es la única matriz que lo verifica. Es decir,* w *es una palabra clave del codico* $\mathcal{C}_\mathcal{G}$ *si y sólo si* $w\mathcal{H}$ *es el elemento neutro de* $\mathbb{Z}_2^{n-m}$*.*

Si $v \in \mathbb{Z}_2^n$, entonces $v\mathcal{H} \in \mathbb{Z}_2^{n-m}$ de denomina *síndrome* de v y el teorema anterior establece que el síndrome de las palabras claves es el elemento neutro. Para el resto de las palabras, las recibidas con errores de transmisión, el síndrome será la herramienta para decodificarlas.

En primer lugar, observamos que todos los elementos de una clase lateral tienen el mismo síndrome. Si $x\mathcal{H} = y\mathcal{H}$, entonces $(x \oplus y)\mathcal{H} = 0$ y por el teorema anterior, $x \oplus y$ es una palabra clave, es decir, $x \oplus y \in \mathrm{Im}(\mathcal{C}_\mathcal{G})$ y en consecuencia x e y están en la misma clase lateral. De la misma forma, si x e y están en la misma clase lateral de $\mathrm{Im}(\mathcal{C}_\mathcal{G})$, entonces $x \oplus y$ es una palabra clave y por lo tanto, $(x \oplus y)\mathcal{H} = 0$ y $x\mathcal{H} = y\mathcal{H}$. Esto demuestra el siguiente resultado.

Corolario 1.8.9 *Dos palabras están en la misma fila de la tabla de decodificación si y sólo si tienen el mismo síndrome.*

Por lo tanto, conociendo el síndrome, sabemos en qué clase lateral (fila de la tabla) está la palabra que queremos decodificar y solo tendríamos que saber cual es la palabra clave más cercana. Para ello, basta sumarle el elemento de su misma clase que tenga menor peso, esa palabra se denomina *lider* de la clase. Con este método, no necesitamos escribir toda la tabla de descodificación, basta determinar los posibles síndromes y el líder de la clase lateral correspondiente a ese síndrome; o mejor dicho, los líderes de cada clase y el correspondiente síndrome.

Ejemplo 1.8.10 Con el código de grupo dado por

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

y usando la equivalencia

000	001	010	011	100	101	110	111
A	C	E	N	O	R	S	T

Queremos saber cuál es el mensaje que nos han querido transmitir si hemos recibido la siguiente secuencia de palabras codificadas.

101110 100001 101011 111011 010011 011110 111000 100001

Empezamos escribiendo la matriz de verificación de paridad

$$\mathcal{H} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

para ir determinando los líderes de cada clase y el correspondiente síndrome. Esto lo hacemos recorriendo los elementos de $\mathbb{Z}_2^6$ en orden ascendente según el peso, multiplicando por la matriz de verificación hasta obtener los $2^{6-3} = 8$ síndromes posibles. Como vemos, en este caso, los seis elementos de peso 1 son líderes de seis clases distintas, ya que sus síndromes son distintos. El primer elemento de peso 2 sería 000011, que tiene síndrome 011 que ya estaba en la tabla; pasaríamos al 000101 que tiene síndrome 101 y que también estaba en la tabla; seguimos así hasta llegar a 100010 que nos da el último síndrome para completar la tabla, el 111.

Líderes	Síndromes
000000	000
000001	001
000010	010
000100	100
001000	110
010000	011
100000	101
100010	111

Esta tabla sustituye a la tabla de decodificación que usamos en el primer ejemplo y con ella vamos a decodificar el mensaje inicial de este ejemplo.

La primera palabra recibida es 101110. Calculamos su síndrome, $101110\mathcal{H} = 101$, al que, según la tabla anterior le corresponde el líder 100000. Por lo tanto, la palabra

decodificada es

$$100000 \oplus 101110 = 001110 \quad \rightsquigarrow \quad 001 \quad \rightsquigarrow \quad \text{C}$$

Hacemos lo mismo con todas las palabras

Recibida	Síndrome	Líder	Rec.⊕Líder	Mensaje
101110	101	100000	001110	001 ⇝ C
100001	100	000100	100101	100 ⇝ O
101011	000	000000	101011	101 ⇝ R
111011	011	010000	101011	101 ⇝ R
010011	000	000000	010011	010 ⇝ E
011110	011	010000	001110	001 ⇝ C
111000	000	000000	111000	111 ⇝ T
100001	100	000100	100101	100 ⇝ O

□