Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Anexo: CUERPOS FINITOS

Mayo de 2017

Anexo: CUERPOS FINITOS

A.1. Algunas estructuras algebraicas interesantes

En este anexo introduciremos algunas estructuras algebraicas básicas, constituidas por ciertos conjuntos con una o más leyes de composición internas que cumplen unos determinados axiomas.

Definición Un **grupo** es un par $(G, +)$, donde $+$ es una ley de composición interna en G (es decir, una aplicación de $G \times G$ en G), que cumple:

1. $(a + b) + c = a + (b + c)$ $\forall a, b, c \in G$ (propiedad asociativa).
2. $\exists 0_G \in G$ tal que, $a + 0_G = 0_G + a = a$ $\forall a \in G$ (existencia de elemento neutro).
3. $\forall a \in G$ $\exists a' \in G$ tal que $a + a' = a' + a = 0_G$ (existencia de elemento opuesto).

Si además se cumple que $a + b = b + a$ $\forall a, b \in G$ (propiedad conmutativa), el grupo se dice **conmutativo**, o también **abeliano**.

Hay un único elemento en el grupo que cumple la propiedad indicada en el segundo axioma, es decir, el elemento neutro es único.

También, para cada $a \in G$, el elemento a' indicado en el tercer axioma es único. Al opuesto a' del elemento a se le suele denotar por $-a$.

Es indiferente el símbolo que se use para denotar la ley de composición interna; de hecho, se podría haber utilizado cualquier otro, como $\star, \circ$, etc. Cuando el símbolo usado es $+$, se dice que la notación es aditiva. También es habitual denotarlo por $\cdot$ (o, más brevemente, simplemente por yuxtaposición), en cuyo caso se dice que la notación es multiplicativa. En este caso, al elemento neutro se le suele denotar por 1_G (o simplemente por 1 si no hay lugar a confusión), y al elemento a' que verifica $aa' = a'a = 1$ se le suele denotar por a^{-1}, y se le llama el **inverso de** a.

Ejemplos A.1.1

1. El grupo más simple de todos es el grupo $\{0\}$ con un sólo elemento y con la

única operación posible definida por $0 + 0 = 0$, llamado grupo trivial; este grupo es abeliano.

2. El conjunto $\mathbb{Z}$ de los números enteros, con la operación habitual de suma de enteros, es un grupo abeliano. En cambio, $\mathbb{Z}$ con la operación producto habitual no es un grupo, ya que los únicos elementos que tienen inverso son 1 y -1.

3. El conjunto $\mathbb{Q}$ de los números racionales, con la operación habitual de suma, es un grupo abeliano. Con la operación producto no es grupo, ya que 0 no tiene inverso, pero si omitimos este elemento, es obvio que los números racionales no nulos con la multiplicación sí forman un grupo, el cual es abeliano.

4. El conjunto $\mathbb{R}$ de los números reales, con la operación habitual de suma, es un grupo abeliano.

5. El conjunto $\mathbb{C}$ de los números complejos, con la operación habitual de suma, es un grupo abeliano.

6. El conjunto $G = \{a, b, c, d, e, f\}$, con la operación definida por

*	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

es un grupo. No es abeliano ya que, por ejemplo, $b * d = f$, pero $d * b = e$.

Definición Un **subgrupo** de un grupo G es un subconjunto H de G que cumple:

1. $a + b \in H \ \forall a, b \in H$.
2. $0_G \in H$.
3. $-a \in H \ \forall a \in H$.

Un subgrupo H de un grupo G se dice **normal**, y se denota $H \trianglelefteq G$, si cumple

$$-a + b + a \in H, \ \forall a \in G, \forall b \in H.$$

Obviamente, si G es abeliano, todo subgrupo suyo es normal.

Si H es un subgrupo de G, la relación definida por

$$a \equiv b, \text{ si } a - b \in H$$

es de equivalencia. Dado un $a \in G$, la clase de equivalencia representada por a, es igual a $\{h+a \mid h \in H\}$. A este conjunto se le suele denotar por $H+a$, y a este tipo de conjuntos se les llama **coclases a derecha**.

Análogamente, la relación definida por

$$a \equiv b \text{ si } -a+b \in H$$

es de equivalencia. Dado un $a \in G$, la clase de equivalencia representada por a, es igual a $\{a+h \mid h \in H\}$. Este conjunto se denota por $a+H$, y a estos conjuntos se les llama **coclases a izquierda**.

Si H es subgrupo normal de G, ambas relaciones son iguales, y las coclases a derecha e izquierda son iguales. En este caso, el conjunto cociente formado por las clases de equivalencia, es decir, por las coclases, se suele representar por G/H. En este conjunto cociente la operación binaria siguiente está bien definida:

$$(a+H)+(b+H)=(a+b)+H.$$

Por bien definida queremos decir que el resultado no depende de los representantes elegidos en las coclases que forman los sumandos, es decir, que si $a+H=a'+H$ y $b+H=b'+H$, entonces $(a+b)+H=(a'+b')+H$.

Con esta operación se tiene lo siguiente:

Proposición A.1.1 *$(G/H,+)$ es un grupo. Además, si G es abeliano, G/H también lo es.*

Al grupo anteriormente introducido se le llama **grupo cociente del grupo G entre el subgrupo normal H.**

Cuando no hay ambigüedad respecto al subgrupo H que se está considerando, se suele denotar la coclase $a+H$ simplemente por $\overline{a}$. Con esta notación, la operación del grupo cociente es $\overline{a}+\overline{b}=\overline{a+b}$.

Ejemplo A.1.2 Si n es un número entero, el conjunto

$$n\mathbb{Z}=\{nm \mid m \in \mathbb{Z}\}$$

es un subgrupo del grupo aditivo $(\mathbb{Z},+)$ de los enteros. Si $n>0$, las coclases de $\mathbb{Z}/n\mathbb{Z}$ son, sin repeticiones ni que falte ninguna, $\{0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$. El resultado de sumar dos coclases $\overline{a}$ y $\overline{b}$ en este cociente es $\overline{a+b}$. Para expresar el resultado en la forma indicada anteriormente, se pone $\overline{a+b}=\overline{r}$, donde r es el resto de la división de $a+b$ entre n.

Por ejemplo, en $\mathbb{Z}/7\mathbb{Z}$, se tiene que $\overline{3}+\overline{6}=\overline{9}=\overline{2}$. La tabla completa de la suma en

$\mathbb{Z}/7\mathbb{Z}$ es

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

Otra estructura algebraica importante, en la que intervienen dos leyes de composición, es la de anillo:

Definición Un **anillo** es una terna $(A, +, \cdot)$, donde $+$ y $\cdot$ son leyes de composición internas en A, que cumple:

1. $(A, +)$ es grupo abeliano.
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in A$ (propiedad asociativa).
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$ $\forall a, b, c \in A$ (propiedad distributiva).

0_A denotará al elemento neutro de la suma, y $-a$ al elemento opuesto de a. El anillo se dice **conmutativo** si $\forall a, b \in A,\ a \cdot b = b \cdot a$, y unitario si existe un elemento $1_A \in A$ que cumple $1_A \cdot a = a \cdot 1_A = a$ $\forall a \in A$.

Ejemplos A.1.3

1. El anillo $\{0\}$, con las únicas operaciones posibles $0 + 0 = 0$ y $0 \cdot 0 = 0$, es un anillo conmutativo y unitario, llamado **anillo nulo o anillo trivial**. En él, los elementos neutros de la suma y del producto coinciden (se puede ver que es el único caso en el que pasa esto).
2. Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, con sus operaciones habituales de suma y producto, son anillos conmutativos y unitarios.
3. El conjunto
$$\{a + bI \mid a, b \in \mathbb{Z}\},$$
donde I es la unidad imaginaria, es un anillo conmutativo y unitario con sus operaciones habituales como números complejos. Se le llama **anillo de los enteros gaussianos.**
4. Si A es un anillo, el conjunto
$$A[x] = \{\sum a_i x^i \mid a_i \in A\ \forall i, a_i = 0 \text{ a partir de un cierto } n_0\},$$

es un anillo con las operaciones $\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$ y $(\sum a_i x^i)(\sum b_i x^i) = (\sum c_i x^i)$, con $c_i = \sum_{j+k=i} a_j b_k$, es un anillo. Si A es conmutativo (respectivamente, unitario), entonces $A[x]$ también lo es.

5. Dado un número natural n, el conjunto $M_n(\mathbb{R})$ de matrices cuadradas de orden n cuyas entradas son números reales, es un anillo unitario con sus operaciones usuales de suma y producto de matrices. No es conmutativo, salvo en el caso $n = 1$.

A veces se suele omitir el punto en el producto, y éste se denota simplemente por yuxtaposición.

Aunque en el último ejemplo hemos mostrado, con propósitos ilustrativos, un anillo no conmutativo, en lo sucesivo supondremos, aunque no se diga explícitamente, que los anillos que consideramos son conmutativos y unitarios.

En cualquier anillo, la propiedad asociativa garantiza que el resultado de hacer $a + \cdots + a$, donde a aparece n veces, no depende de cómo se distribuyan los paréntesis al hacer la suma. A este elemento se le denota por na. Esta definición se puede extender del modo siguiente: $0a = 0_A$ y, si n es un entero negativo, $na = -((-n)a)$.

De forma similar, la asociatividad del producto garantiza que el producto $a \cdots a$, con n factores, no depende de cómo se distribuyan los paréntesis al hacer los productos parciales. A este elemento se le denota por a^n. Se conviene también que $a^0 = 1_A$.

Proposición A.1.2 *1.* $0_A a = 0_A \ \forall a \in A$.

2. $(-a)b = a(-b) = -(ab) \ \forall a, b \in A$.

3. $(-a)(-b) = ab \ \forall a, b \in A$.

4. $a(b - c) = ab - ac \ \forall a, b, c \in A$.

Definición Un elemento a de un anillo A es una **unidad** si es inversible para la multiplicación, es decir, si existe un $b \in A$ tal que $ab = 1$.

Al inverso de un elemento a se le suele denotar por a^{-1}.

Ejemplos A.1.4

1. En el anillo $\mathbb{Z}$ de los enteros los únicos elementos inversibles, es decir, las únicas unidades, son 1 y -1.

2. En el anillo de los enteros gaussianos hay exactamente 4 unidades: $1, -1, I, -I$.

3. En el anillo $\mathbb{Q}$ de los números enteros, las unidades son los elementos no nulos.

Se pueden definir potencias de exponente negativo de elementos inversibles de la siguiente forma: si a es una unidad y n es un entero negativo, $a^n = (a^{-1})^{-n}$.

Veremos ahora los objetos que son el objetivo principal de estudio en este apéndice, los cuerpos:

Definición Un **cuerpo** es un anillo no nulo K en el que todo elemento no nulo es una unidad.

Ejemplos A.1.1 *1. El conjunto $\mathbb{Q}$ de los números racionales, con las operaciones habituales, es un cuerpo.*

2. El conjunto $\mathbb{R}$ de los números reales, con las operaciones habituales, es un cuerpo.

3. El conjunto $\mathbb{C}$ de los números complejos, con las operaciones habituales, es un cuerpo.

Así como en el caso de los grupos la subestructura que nos permitía definir los grupos cocientes era la de subgrupo normal, en el de los anillos, la subestructura que nos permitirá definir los anillos cociente es la de ideal:

Definición Si A es un anillo, un **ideal** de A es un subconjunto $\mathfrak{a}$ de A que cumple:

1. $(\mathfrak{a}, +)$ es subgrupo de $(A, +)$
2. $ax \in \mathfrak{a}\ \forall a \in A, \forall x \in \mathfrak{a}$

Si un ideal $\mathfrak{a}$ de un anillo A contiene al elemento 1_A, entonces $\mathfrak{a} = A$, ya que si $a \in A$, entonces $a = a \cdot 1_A \in \mathfrak{a}$, por definición de ideal.

Ejemplos A.1.5

1. Tanto $\{0_A\}$ como A siempre son ideales de un anillo A. A éstos se les llama **ideales triviales de** A. A los que son distintos de $\{0_A\}$ y de A se les llama **ideales no triviales**, y a los que son distintos de A, **ideales propios**.
2. Si n es un número entero, el conjunto

$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$

es un ideal del anillo $\mathbb{Z}$. De hecho, éstos son todos los ideales del anillo $\mathbb{Z}$ de los enteros.

Si $\mathfrak{a}$ es un ideal de A, entonces $(\mathfrak{a}, +)$ es un subgrupo normal del grupo aditivo, luego podemos considerar la relación de congruencia $x \equiv y$ si $x - y \in \mathfrak{a}$ y, como dijimos antes, el conjunto cociente $A/\mathfrak{a}$, con la operación $(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$ es un grupo, llamado el **grupo cociente de A entre el subgrupo $\mathfrak{a}$**. La definición siguiente de producto de clases de equivalencia es consistente y no depende de los representantes elegidos:

$$(x + \mathfrak{a})(y + \mathfrak{a}) = (xy) + \mathfrak{a}.$$

Proposición A.1.3 *Si A es un anillo y $\mathfrak{a}$ es un ideal de A, entonces $(A/\mathfrak{a}, +, \cdot)$ es anillo.*

Al anillo anterior se le llama **anillo cociente de A entre el ideal $\mathfrak{a}$**. Sus elementos neutros para la suma y el producto son $0_A + \mathfrak{a}$ y $1_A + \mathfrak{a}$, respectivamente.

A los $x + \mathfrak{a}$ se les llama también **coclases módulo $\mathfrak{a}$**, o simplemente **coclases**, y se suelen denotar, cuando no haya ambigüedad respecto al ideal que se esté considerando, poniendo simplemente una barra encima de un representante, como $\overline{x}$. Cuando $x + \mathfrak{a} = y + \mathfrak{a}$ (lo cual ocurre si y sólo si $x - y$ está en $\mathfrak{a}$), se dice que x es **congruente con y módulo $\mathfrak{a}$**, lo cual se denota por $x \equiv y \pmod{\mathfrak{a}}$.

Ejemplo A.1.6 Si, dado un número natural n, consideramos el ideal $n\mathbb{Z}$, sabemos por lo visto en los grupos cociente que

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\},$$

y que se tiene la operación suma

$$\overline{r} + \overline{s} = \overline{r + s}.$$

Al ser $n\mathbb{Z}$ un ideal, también se tiene la operación producto

$$\overline{r} \cdot \overline{s} = \overline{r \cdot s}.$$

Veremos ahora un tipo de ideales que serán muy útiles posteriormente para la construcción de cuerpos:

Definición Un ideal $\mathfrak{M}$ de un anillo A es **maximal** si es ideal propio y los únicos ideales que lo contienen son $\mathfrak{M}$ y A.

Ejemplo A.1.7

1. $6\mathbb{Z}$ no es ideal maximal de $\mathbb{Z}$, ya que $6\mathbb{Z} \subset 3\mathbb{Z}$, y $3\mathbb{Z} \neq 6\mathbb{Z}, 3\mathbb{Z} \neq \mathbb{Z}$.
2. $2\mathbb{Z}$ sí es ideal maximal de $\mathbb{Z}$, ya que $1 \notin 2\mathbb{Z}$, luego $2\mathbb{Z} \neq \mathbb{Z}$, y cualquier ideal que contenga estrictamente a $2\mathbb{Z}$ contiene un entero impar, luego también al 1, de donde se deduce que el ideal tiene que ser todo $\mathbb{Z}$.

Se pueden caracterizar los ideales maximales en términos de la estructura del anillo cociente:

Proposición A.1.4 *Un ideal $\mathfrak{M}$ de un anillo A es maximal si y sólo si $A/\mathfrak{M}$ es cuerpo.*

Generalizando lo visto en el segundo ejemplo, se tiene que los ideales maximales de $\mathbb{Z}$ son los de la forma $p\mathbb{Z}$, donde p es un número primo. De ahí se deduce lo siguiente:

Proposición A.1.5 *Un anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es cuerpo si y sólo si n es un número primo.*

La proposición anterior nos proporciona un método de construcción de cuerpos finitos de cardinal un número primo. En la sección siguiente veremos, más en general, cómo construir cuerpos con cardinal una potencia de un primo.

Ejemplo A.1.8 Como 7 es un número primo, el anillo $\mathbb{Z}/7\mathbb{Z}$ es un cuerpo con 7 elementos. Ya vimos en el ejemplo A.1.2 la tabla de la suma en este cuerpo. Veremos ahora la tabla del producto. Para confeccionarla, hay que tener en cuenta que para multiplicar $\overline{i}$ por $\overline{j}$, se hace primero el producto ij, se toma luego el resto r de la división de ij por 7, y el resultado de la multiplicación es $\overline{r}$. Por ejemplo, $\overline{5}\cdot\overline{4} = \overline{20} = \overline{6}$, ya que $20 = 2\cdot 7 + 6$. La tabla del producto es:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Cuando trabajemos en $\mathbb{Z}/n\mathbb{Z}$, si no hay ambigüedad, denotaremos a la coclase $\overline{r}$, simplemente por r.

A.2. Construcción de cuerpos finitos

En la sección anterior vimos cómo, dado un número primo p, el cociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito de cardinal p. Ahora veremos cómo se pueden construir cuerpos finitos de cardinal una potencia p^n de un primo p tomando un cociente apropiado del anillo de polinomios $\mathbb{Z}/p\mathbb{Z}[x]$ en la indeterminada x con coeficientes en $\mathbb{Z}/p\mathbb{Z}$

entre el ideal formado por los polinomios múltiplos de un polinomio irreducible de grado n. Primero necesitaremos dar algunas definiciones:

Definición Sea K un cuerpo, y sea $P(x) = \sum_i a_i x^i$ un polinomio no nulo de $K[x]$. El **grado de** $P(x)$ es el mayor entero no negativo n que cumple $a_n \neq 0$.

El grado de $P(x)$ se suele denotar por $\delta(P(x))$.

Es obvio que los polinomios de grado 0 son las unidades de $K[x]$. A estos se les llaman **polinomios constantes no nulos** (el polinomio nulo también es constante, pero no se le asigna grado).

Definición Sea K un cuerpo. Un polinomio $P(x) \in K[x]$ de grado estrictamente positivo es **irreducible** si $P(x) = Q_1(x)Q_2(x)$ implica que $\delta(Q_1(x)) = 0$ ó $\delta(Q_2(x)) = 0$.

Un polinomio no nulo $P(x)$ de $K[x]$, donde K es un cuerpo, se dice mónico si el coeficiente de $x^{\delta(P(x))}$ es 1_K (dicho coeficiente se llama **coeficiente director** de $P(x)$).Todo polinomio $P(x)$ de grado positivo de $K[x]$, donde K es un cuerpo, se puede descomponer de forma única, salvo por el orden de los factores, en la forma

$$P(x) = aP_1(x) \cdots P_m(x),$$

donde $m \in \mathbb{N}, a \in K$ y los polinomios $P_1(x), \ldots, P_m(x)$ son mónicos e irreducibles.

Ejemplos A.2.1

1. El polinomio $x^2 + \overline{1}$ no es irreducible en $\mathbb{Z}/2\mathbb{Z}[x]$, ya que $x^2 + \overline{1} = (x + \overline{1})^2$, pero $x + \overline{1}$ no es un polinomio constante.
2. En cambio, el polinomio $x^2 + x + \overline{1}$ sí es irreducible en $\mathbb{Z}/2\mathbb{Z}[x]$.

Cuando se trabaja en $\mathbb{Z}/p\mathbb{Z}[x]$ es habitual, cuando no hay ambigüedad, omitir las barras; así, los dos polinomios de los ejemplos se denotarían simplemente por $x^2 + 1$ y $x^2 + x + 1$.

Si K es un cuerpo y $P(x) \in K[x]$, el conjunto

$$(P(x)) = \{P(x)Q(x) \mid Q[x] \in K[x]\}$$

es un ideal, llamado el **ideal generado por el polinomio** $P(x)$. Dado un $Q(x) \in K[x]$, a la coclase $Q(x) + (P(x))$ del anillo cociente $K[x]/(P(x))$ se la suele denotar simplemente por $\overline{Q(x)}$ cuando no hay ambigüedad respecto al ideal $(P(x))$ considerado.

Proposición A.2.1 *El ideal $(P(x))$ es maximal si y sólo si el polinomio $P(x)$ es irreducible.*

De aquí, utilizando la proposición A.1.4, se deduce lo siguiente:

Corolario A.2.2 *El anillo cociente $K[x]/(P(x))$ es cuerpo si y sólo si el polinomio $P(x)$ es irreducible.*

Ejemplo A.2.2 El cociente $\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$ es un cuerpo. Si $P(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ y $R(x)$ es el resto de la división de $P(x)$ entre x^2+x+1 (¡Cuidado!, la división es en $\mathbb{Z}/2\mathbb{Z}[x]$), entonces $\overline{P(x)} = \overline{R(x)}$ (aquí las barras representan coclases módulo $(P(x))$), luego

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1) = \{\overline{a+bx} \mid a, b \in \mathbb{Z}/2\mathbb{Z}\},$$

y está claro que en esta representación no hay repeticiones. Por lo tanto,

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$$

es un cuerpo finito con 4 elementos. Para sumar, por ejemplo, $\overline{x}$ y $\overline{x+1}$, se hace

$$\overline{x} + \overline{x+1} = \overline{2x+1} = \overline{1}.$$

Para multiplicar los mismos elementos, se hace

$$\overline{x} \cdot \overline{x+1} = \overline{x(x+1)} = \overline{x^2+x} = \overline{1},$$

ya que $x^2 + x = (x^2+x+1) + 1$.

Para garantizar la existencia de cuerpos de orden potencia de un primo usaremos lo siguiente:

Proposición A.2.3 *Si p es un número primo y $n \in \mathbb{N}$, entonces existe por lo menos un polinomio $P(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ irreducible de grado n.*

De ahí se deduce lo siguiente:

Proposición A.2.4 *Si p es un número primo y $n \in \mathbb{N}$, entonces existe un cuerpo finito de orden p^n.*

No podemos realmente aspirar a una mayor generalidad en los cardinales de los cuerpos finitos, como vemos en la siguiente proposición.

Proposición A.2.5 *Si K es un cuerpo finito, entonces $|K| = p^n$ para algún número primo p y algún número natural n.*

Para cada primo p y cada exponente n hay esencialmente un único cuerpo de orden p^n. Definiremos primero qué queremos decir con 'esencialmente uno'.

Definición Si F, K son dos cuerpos, una aplicación $f : F \longrightarrow K$ es un **isomorfismo** si es biyectiva y además satisface

1. $f(x+y) = f(x) + f(y)\ \forall x, y \in F$,
2. $f(x \cdot y) = f(x) \cdot f(y)\ \forall x, y \in F$.

Cuando existe un isomorfismo entre dos cuerpos F y K, se dice que éstos son **isomorfos**, y se denota por $F \simeq K$. Intuitivamente, esto quiere decir que tienen la misma estructura, es decir, que son indistinguibles desde el punto de vista de las propiedades algebraicas que afectan a la suma y el producto, y que se distinguen tan sólo en la forma de denotar sus elementos.

Proposición A.2.6 *Si F, K son dos cuerpos finitos del mismo cardinal, entonces F y K son isomorfos.*

De lo visto en las proposiciones A.2.4 y A.2.6 se deduce lo siguiente:

Proposición A.2.7 *Para cada número primo p y cada número natural n hay un único cuerpo de orden p^n, salvo isomorfismos.*

Dicho cuerpo se suele denotar por $\mathbb{F}_{p^n}$.

A.3. Ejemplos de cuerpos finitos

En esta sección veremos algunos ejemplos de cuerpos finitos de orden pequeño. Para construir un cuerpo de orden p^n es necesario conocer un polinomio irreducible de grado n con coeficientes en $\mathbb{Z}/p\mathbb{Z}$. Por lo general, no hay un único polinomio irreducible de grado n en $\mathbb{Z}/p\mathbb{Z}[x]$ aunque, por lo visto en la proposición A.2.6, todos ellos dan lugar a cuerpos isomorfos.

Dentro de los polinomios irreducibles $P(x)$, interesan especialmente aquellos que cumplen que las potencias $\overline{x}^i$ permiten obtener todos los elementos no nulos del cuerpo $\mathbb{Z}/p\mathbb{Z}[x]/(P(x))$. Dichos polinomios se llaman **primitivos**. El conocer estos polinomios es importante en algunas áreas de la Teoría de Códigos, como por ejemplo cuando se estudian los códigos BCH.

Por ejemplo, el polinomio $x^2 + 1 \in \mathbb{Z}/3\mathbb{Z}[x]$ es irreducible, pero no es primitivo, ya que al hacer las potencias de $\overline{x}$ obtenemos:

$\overline{x}^0 = \overline{1}$,

$\overline{x}^1 = \overline{x}$,

$\overline{x}^2 = \overline{2}$,

$\overline{x}^3 = \overline{2x}$,

$\overline{x}^5 = \overline{1}$,

y de ahí en adelante se van repitiendo cíclicamente los mismos cuatro elementos. Por lo tanto, al hacer potencias de $\overline{x}$ sólo se obtienen $\overline{1}, \overline{x}, \overline{2}, \overline{2x}$, y no se consiguen todos los 8 elementos no nulos del cuerpo.

En cambio, el polinomio $x^2 + 2x + 2 \in \mathbb{Z}/3\mathbb{Z}$, además de irreducible es primitivo, ya que las potencias de $\overline{x}$ dan:

$\overline{x}^0 = \overline{1}$,

$\overline{x}^1 = \overline{x}$,

$\overline{x}^2 = \overline{x+1}$,

$\overline{x}^3 = \overline{2x+1}$,

$\overline{x}^4 = \overline{2}$,

$\overline{x}^5 = \overline{2x}$,

$\overline{x}^6 = \overline{2x+2}$,

$\overline{x}^7 = \overline{x+2}$,

y en este caso sí obtenemos los 8 elementos distintos de cero del cuerpo. Al seguir haciendo potencias, estos 8 elementos se van repitiendo cíclicamente.

Proposición A.3.1 *Si p es un número primo y n es un número natural, hay por lo menos un polinomio primitivo de grado n en $\mathbb{Z}/p\mathbb{Z}[x]$.*

Por lo general, no hay un sólo polinomio primitivo de grado n en $\mathbb{Z}/p\mathbb{Z}[x]$. Por ejemplo, en $\mathbb{Z}/2\mathbb{Z}[x]$ hay dos polinomios primitivos de grado 3: $1+x+x^3$ y $1+x^2+x^3$.

En la tabla siguiente damos un ejemplo de un polinomio primitivo de grados 2,3,4,5 para los primos 2,3,5,7,11,13.

	$n=2$	$n=3$	$n=4$	$n=5$
$p=2$	x^2+x+1	x^3+x^2+1	x^4+x+1	$x^5+x^4+x^3+x^2+1$
$p=3$	x^2+2x+2	x^3+2x^2+x+1	$x^4+x^3+2x^2+2x+2$	$x^5+x^4+2x^3+x^2+x+1$
$p=5$	x^2+3x+3	x^3+4x+3	x^4+4x^2+x+2	$x^5+2x^4+3x^3+x^2+4x+2$
$p=7$	x^2+x+3	x^3+3x^2+4	x^4+3x^2+4x+3	$x^5+x^4+5x^3+2x^2+4$
$p=11$	x^2+4x+7	x^3+2x^2+6x+9	x^4+4x^2+x+2	$x^5+x^4+9x^3+3x^2+5x+5$
$p=13$	$x^2+4x+11$	x^3+7x^2+2x+6	x^4+4x^2+x+2	$x^5+x^4+x^3+11x^2+8x+6$

Para terminar, veamos un ejemplo de cómo podemos utilizar los datos de la tabla para calcular el inverso en un cuerpo finito. Consideramos un cuerpo de orden 8, utilizando el polinomio primitivo x^3+x^2+1 de dicha tabla, es decir, tomemos

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^3+x^2+1).$$

Vamos a calcular el inverso de $\overline{x^2+1}$. Como x^2+1 y x^3+x^2+1 son primos entre sí en $\mathbb{Z}/2\mathbb{Z}[x]$, utilizando el algoritmo de Euclides extendido obtenemos

$$1=(x^2+x+1)(x^2+1)-x(x^3+x^2+1),$$

luego el inverso de $\overline{x^2+1}$ es $\overline{x^2+x+1}$.