Universidad Complutense de Madrid

Departamento de Algebra

Estructuras Algebraicas

Julio Castellanos

2017

.

Chapter 1

Anillos

1.1 Primeras nociones

Definición 1 *Llamaremos anillo a un conjunto A con dos operaciones,* $(A, +, .)$
(+ suma, . producto),(denotaremos a.b=ab)
$+, . : A \times A \to A$ *verificando las propiedades:*
(1) Asociativa suma: $\forall\ a, b, c \in A,\ a + (b + c) = (a + b) + c$
(2) Conmutativa suma: $\forall\ a, b \in A,\ a + b = b + a$
(3) Elemento neutro existe: $0 \in A$, *tal que* $\forall\ a \in A,\ a + 0 = a$
(4) Elemento opuesto: $\forall\ a \in A$, *existe* $-a \in A$ *tal que* $a + (-a) = 0$
(5) Asociativa producto: $\forall\ a, b, c \in A,\ a(bc) = (ab)c$
(6) Distributiva suma respecto del producto:
$\forall\ a, b, c \in A,\ a(b + c) = ab + ac,\ (b + c)a = ba + ca$

Nota. propiedades (1) ... (4) nos dicen que A es grupo conmutativo.

Diremos que el anillo A es *abeliano* o *conmutativo* si $\forall\ a, b \in A,\ ab = ba$

Diremos que el anillo A es *unitario* si $\exists\ 1 \in A$ tal que $\forall\ a \in A,\ a1 = 1a = a$

EJEMPLOS:

- Anillo de los números enteros $(\mathbf{Z}, +, .)$ conmutativo y con 1.

- Múltiplos de un número n, $n\mathbf{Z}$ conmutativo y no unitario.

- Anillo de las clases módulo n, $(\mathbf{Z}_n, +, .)$, conmutativo y con $1 = \overline{1}$, $\mathbf{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

- Enteros de Gauss $(\mathbf{Z}[i], +, .)$, conmutativo y con 1
$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$, $i = \sqrt{-1}$.

- Dados A, B anillos el producto cartesiano $A \times B$ es un anillo con las operaciones $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2)$, $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$, el cero es $(0, 0)$, y si hay unidades en A y B, la unidad es $(1, 1)$.

El producto hereda propiedades de A y B, aunque no todas.

- Matrices cuadradas $M_n(\mathbf{R})$, $M_n(\mathbf{C})$, operaciones suma y producto de matrices, tiene unidad (la matriz unidad), y no es conmutativo.

- Los polinomios con coeficientes reales $\mathbf{R}[X]$, $\mathbf{R}[X, Y]$.

- Los números naturales $\mathbf{N}$ no son anillo, faltan los elementos opuestos (los negativos).

Además en cualquier anillo se verifica:
(i) $a\,0 = 0\,a = 0$, $\forall a \in A$
(ii) $(-a)b = a(-b) = -(ab)$, $\forall a, b \in A$
(ii) $(-a)(-b) = ab$, $\forall a, b \in A$

Denotaremos $a + (-b)$ como $a - b$.

Definimos para $a \in A$ y $0 \neq n \in \mathbf{N}$, $na = a + \overset{(n}{\cdots} + a$, $0a = 0$
y $(-n)a = (-a) + \overset{(n}{\cdots} + (-a)$, y $a^n = a \overset{(n}{\cdots} a$

y $\forall a, b \in A$, $\forall n, m \in \mathbf{Z}$ se verifica,:
$n(a + b) = na + nb$,
$(n + m)a = na + ma$
$(nm)a = n(ma)$

y si $ab = ba$, entonces
$(ab)^n = a^n b^n$, y $\quad (a + b)^n = \sum_{i=0,\ldots,n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i} b^i$, $\forall n \in \mathbf{N} - \{0\}$

En $\mathbf{Z}_n$, si $n = mq$ entonces $\overline{m} \cdot \overline{q} = \overline{n} = \overline{0}$, en este caso diremos que $\overline{m}$ y $\overline{q}$ son divisores de $\overline{0}$.

Definición 2 *Definimos divisores de* 0 *en un anillo* A *a los elementos* a, b *tales que* $a \neq 0$, $b \neq 0$ *y* $ab = 0$.

Definimos dominio de integridad (DI) a un anillo conmutativo con unidad, con $1 \neq 0$ *y tal que no contiene divisores de cero.*

EJEMPLOS

- $\mathbf{Z}$, $\mathbf{Q}$ son DI.

- $\mathbf{Z}_6$ no es DI, ya que $\overline{2} \cdot \overline{3} = \overline{0}$.

- $A \times B$ no es dominio de integridad, ya que $(a,0)(0,b) = (0,0)$.

En un dominio de integridad se da la propiedad cancelativa.

Proposición 1 *Sea A dominio de integridad, entonces si $a \neq 0$ y $ax = ay$ se verifica $x = y$.*

DEMOSTRACIÓN.

$ax = ay \Rightarrow a(x-y) = 0$, y por ser dominio de integridad y $a \neq 0$, entonces $x - y = 0 \Rightarrow x = y$.

Diremos que un elemento a de un anillo tiene *inverso respecto del producto* (o es *unidad*) en un anillo unitario si existe a^{-1} tal que $aa^{-1} = a^{-1}a = 1$.

Nota El conjunto de las unidades de un anillo A, U_A, es un grupo respecto del producto.

Definición 3 *Definimos cuerpo como un anillo conmutativo unitario con $1 \neq 0$ tal que todo elemento distinto de 0 tiene inverso.*

EJEMPLOS:

- Los números racionales $\mathbf{Q}$, los números reales $\mathbf{R}$, los números complejos $\mathbf{C}$, son cuerpos.

- $\mathbf{Z}$ no es cuerpo.

- $\mathbf{Z}_p$ con p primo es un cuerpo con p elementos.

Corolario 1 *Todo cuerpo es dominio de integridad.*

DEMOSTRACIÓN.

Si los elementos $a \neq 0$, $b \neq 0$ verifican $ab = 0 \Rightarrow 1 = (ab)a^{-1}b^{-1} = 0$ (contradición).

Un *subanillo* B de A, es un subconjunto $B \subset A$ que es anillo con las operaciones heredadas de A. Es decir:

$$\begin{array}{l} B \subset A \\ subanillo \end{array} \Leftrightarrow \begin{cases} \forall\, a,b \in B, a+b \in B,\ ab \in B \\ 0 \in B,\ -a \in B \end{cases} \Leftrightarrow \begin{cases} \forall\, a,b \in B, a-b \in B \\ ab \in B \end{cases}$$

EJEMPLOS:

- $\mathbf{Z}$ es subanillo de $\mathbf{Q}$, $\mathbf{Q}$ es subanillo de $\mathbf{R}$, y $\mathbf{R}$ es subanillo de $\mathbf{C}$.

1.2 Ideales y homomorfismos

A partir de ahora todos los anillos considerados serán conmutativos y unitarios.

Definición 4 *Dados A, B anillos, una aplicación $f : A \to B$ es homomorfismo de anillos si $\forall\, a_1, a_2 \in A$ se tiene:*
$f(a_1 + a_2) = f(a_1) + f(a_2),\ f(a_1 a_2) = f(a_1) f(a_2)$ *y* $f(1) = 1$

Si $f : A \to B$ es homomorfismo de anillos se verifica:
$f(0) = 0$.
$f(-a) = -f(a)$.
$f(na) = nf(a)$, $\forall\, n \in \mathbf{Z}$.

Nota. Nótese que hemos exigido que $f(1) = 1$ que no se deduce de las condiciones anteriores.

De lo anterior se deduce trivialmente que la composición de homomorfismos es homomorfismo.

Denotamos $Hom(A, B) = \{f : A \to B$, homomorfismo $\}$ es un anillo con la suma $((f + g)(a) = f(a) + g(a))$ y producto $((f \cdot g)(a) = f(a) \cdot g(a))$.

EJEMPLOS:

- La inclusión $A \subset B$ es un homomorfismo de anillos.

- $f : \mathbf{Z} \to \mathbf{Z}_n$ dado por $f(a) = \overline{k}$ si $\exists\ \lambda \in \mathbf{Z}$ con $a - \lambda n = k$, es homomorfismo.

- La inclusión $\mathbf{Z}[i] \subset \mathbf{C}$ es un homomorfismo de anillos.

Definición 5 *Dado $f : A \to B$ homomorfismo de anillos definimos:*
Imagen de f, $im(f) = \{b \in B : \exists\, a \in A,$ tal que $f(a) = b\}$
Núcleo de f, $ker(f) = \{a \in A : f(a) = 0\}$.

EJEMPLOS:

Dado $f : \mathbf{Z} \to \mathbf{Z}_n$ como antes, $im(f) = \mathbf{Z}_n$, y $ker(f) = n\mathbf{Z}$.

Nota. El núcleo es un subanillo no necesariamente unitario, en el ejemplo anterior $1 \notin n\mathbf{Z}$.

El núcleo además tiene la siguiente propiedad:
si $b \in ker(f)$ y $a \in A \Rightarrow ab \in ker(f)$,
$(\ f(ab) = f(a)f(b) = f(a)0 = 0)$.

Definición 6 *Dado A anillo, $I \subset A$ es ideal si:*
I es subanillo de A
$\forall\, x \in A, \forall\, a \in I \Rightarrow xa \in I$

Es decir:

$$I \subset A \text{ es ideal} \Leftrightarrow \begin{cases} \forall\, a, b \in I \Rightarrow a - b \in I \\ \forall\, x \in A, a \in I \Rightarrow xa \in I \end{cases}$$

EJEMPLOS:

- $\{0\}$, A son ideales de A,

de hecho si $1 \in I \Rightarrow I = A$.

- Múltiplos de $n \in \mathbf{Z}$, $n\mathbf{Z}$ son ideal.

- Múltiplos de $p(x) \in \mathbf{R}[x]$ son ideal.

- $\{f : [0,1] \to \mathbf{R}$ *continuas* $: f(1/2) = 0\}$ es ideal.

- $f : A \to B$ homomorfismo de anillos, $ker(f)$ es ideal.

Anillo cociente

Sea $I \subset A$ ideal, $\sim$ la relación $a, b \in A$, $a \sim b \Leftrightarrow a - b \in I$ es de equivalencia.

Denotamos A/I al conjunto cociente por $\sim$ y la clase de $a \in A$ como $a + I = \{a + x : \ x \in I\}$.

Nota. Las propiedades de ideal proporcionan que A/I sea anillo con las operaciones:

- Suma $(a + I) + (b + I) = (a + b) + I$.

- Producto $(a + I) \cdot (b + I) = (ab) + I$.

A/I con la suma es grupo abeliano (por ser + conmutativa).

El producto en A/I está bien definido, i.e. no depende de los representantes elegidos:

$$\left\{ \begin{array}{l} a + I = a' + I \\ b + I = b' + I \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a = a' + h, \ h \in I \\ b = b' + k, \ k \in I \end{array} \right. \Rightarrow$$

$$\left\{ \begin{array}{l} I \ ideal \\ a'k \in I, b'h \in I, hk \in I \end{array} \right. \Rightarrow \left\{ \begin{array}{l} a'k + b'h + hk = g \in I \\ ab = a'b' + g, g \in I \end{array} \right.$$

El producto en el anillo cociente A/I verifica asociativa, conmutativa y distributiva por verificarlas A.

EJEMPLOS:

$$\frac{\mathbf{Z}}{n\mathbf{Z}} \equiv \mathbf{Z}_n, \qquad \frac{\mathbf{R}[x]}{(x^2+1)\mathbf{R}[x]} \equiv \mathbf{C}$$

Operaciones con ideales

La unión de ideales no es ideal en general: $3 + 4 = 7 \notin 3\mathbf{Z} \cup 4\mathbf{Z}$.

- Suma de ideales: $I + J = \{h + k : h \in I, k \in J\}$ es ideal.

- Intersección de ideales $I \cap J$ es ideal.

$\bigcap_{i \in \Gamma} I_i$ (cualquier conjunto de indices Γ) es ideal.

- Producto de ideales $I \cdot J = \{h_1k_1 + \cdots + h_rk_r : h_i, \in I, k_i \in J\}$ es ideal.

Ideal generado por un subconjunto

Sea $\emptyset \neq S \subset A$ subconjunto, el *ideal generado* por S en A es:

$$I(S) = \{x_1h_1 + \cdots + x_rh_r : h_i, \in I, x_i \in A\} \Leftrightarrow$$

$$I(S) = \bigcap_{I_i \supset S} I_i,\ I_i \text{ ideal de } A$$

Es decir $I(S)$ es el menor ideal de A que contiene a S.

Se verifica entonces:

$I + J = I(I \cup J)$, y $I \cdot J = I(\{h_i k_i\}),\ h_i \in I, k_i \in J$.

EJEMPLOS:

- *Ideal principal*: (generado por un elemento) $bA \equiv (b) = \{ab : a \in A\}$.

- *Ideal finitamente generado*: Ideal generado por un número finito de elementos $S = \{b_1, \ldots, b_n\}$:

$I(S) \equiv (b_1, \ldots, b_n) \equiv (b_1, \ldots, b_n)A = \{x_1 b_1 + \cdots + x_n b_n : x_i \in A\}$.

Definición 7 *Llamaremos dominio de ideales principales (DIP) a un dominio de integridad en el que todos sus ideales son principales.*

EJEMPLOS:

$\mathbf{Z}$ es DIP. Si $I \subset \mathbf{Z}$ ideal, $I = (n)$ donde $n = min\{m > 0 : m \in I\}$. Basta dividir $0 < m \in I$, $m = cn + r \Rightarrow r = m - cn \in I$ y $r < n \Rightarrow r = 0$, i.e. $m \in (n)$ (análogo para $-m$).

Definición 8 *Llamaremos Anillo Noetheriano a un anillo en el que todos sus ideales son finitamente generados.*

Proposición 2 *Dados A anillo, A es cuerpo $\Leftrightarrow$*
los únicos ideales de A son (0) y (1).

DEMOSTRACIÓN.

$\Rightarrow$) A cuerpo, $(0) \neq I \subset A$ ideal, sea $0 \neq b \in I \Rightarrow bb^{-1} = 1 \in I \Rightarrow I = A$.

$\Leftarrow$) Sea $0 \neq b \Rightarrow (b) = A = (1) \Rightarrow \exists\, c \in I$ con $bc = 1$.

Ideales primos y maximales

Definición 9 *Sea A anillo:*
$\mathfrak{p} \subset A$, $\mathfrak{p} \neq A$ es ideal primo si $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.
$\mathfrak{M} \subset A$, $\mathfrak{M} \neq A$ es ideal maximal si $\forall\, I \subset A$ ideal con $\mathfrak{M} \subsetneq I \Rightarrow I = A$.

Es decir $\mathfrak{p}$ es primo si $I \cdot J \subset \mathfrak{p} \Rightarrow I \subset \mathfrak{p}$ o $J \subset \mathfrak{p}$.

$\mathfrak{M}$ es maximal si es maximal para la inclusión.

EJEMPLOS:

- El ideal $(p)\mathbf{Z}$ con p primo, es ideal primo e ideal maximal; $(n)\mathbf{Z}$ con n no primo, no es ni primo ni maximal.

- La suma de ideales primos no es primo en general, sean $I = (x^2+1), J = (y^2+1)$ ideales primos de $\mathbf{R}[x,y]$, su suma $I + J = (x^2+1, y^2+1)$ no es primo ya que $(x^2+1) - (y^2+1) = x^2 - y^2 = (y-x)(y+x) \in I + J$, pero $x \pm y \notin I + J$.

Nota. Se demuestra que todo ideal está contenido en uno maximal.

Tenemos las siguientes caracterizaciones:

Proposición 3 *Dados A anillo, $\mathfrak{p} \subset A$ ideal,*
$\mathfrak{p}$ es primo $\Leftrightarrow$ $A/\mathfrak{p}$ es dominio de integridad.

DEMOSTRACIÓN.

$\Rightarrow$) Sea $(a+\mathfrak{p})(b+\mathfrak{p}) = 0+\mathfrak{p} \Rightarrow ab \in \mathfrak{p} \Rightarrow$ (por ser $\mathfrak{p}$ primo)

$a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$, es decir $a+\mathfrak{p} = 0+\mathfrak{p}$ ó $b+\mathfrak{p} = 0+\mathfrak{p}$.

$\Leftarrow$) Sea $ab \in \mathfrak{p} \Rightarrow (a+\mathfrak{p})(b+\mathfrak{p}) = 0+\mathfrak{p} \Rightarrow$ (por ser $A/\mathfrak{p}$ DI)

$a+\mathfrak{p} = 0+\mathfrak{p}$ ó $b+\mathfrak{p} = 0+\mathfrak{p}$ es decir $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.

Nota.
A es dominio de integridad $\Leftrightarrow$ (0) es primo.

Proposición 4 *Dados A anillo, $\mathfrak{M} \subset A$ ideal*
$\mathfrak{M}$ es maximal $\Leftrightarrow$ $A/\mathfrak{M}$ es cuerpo.

DEMOSTRACIÓN.

$\Rightarrow$) Sea $a+\mathfrak{M} \neq 0+\mathfrak{M} \Rightarrow a \notin \mathfrak{M}$,

consideramos el ideal $aA + \mathfrak{M} \supsetneq \mathfrak{M} \Rightarrow$ (por ser $\mathfrak{M}$ maximal)

$aA + \mathfrak{M} = A \Rightarrow \exists\, m \in \mathfrak{M}, b \in A$ con $1 = m + ab \Rightarrow ab - 1 \in \mathfrak{M} \Rightarrow$

$ab + \mathfrak{M} = 1 + \mathfrak{M} \Rightarrow (a + \mathfrak{M})^{-1} = b + \mathfrak{M}$, luego $A/\mathfrak{M}$ es cuerpo.

$\Leftarrow$) Sea $I \supsetneq \mathfrak{M}$, $\exists\ a \in I$, $a \notin \mathfrak{M} \Rightarrow$ (por ser $A/\mathfrak{M}$ cuerpo)

$\exists\ (b + \mathfrak{M})$ con $(a + \mathfrak{M})(b + \mathfrak{M}) = 1 + \mathfrak{M} \Rightarrow$

$1 - ab \in \mathfrak{M} \subset I$ (y como $ab \in I$) $\Rightarrow 1 \in I$ y $I = A$.

Nota.
A es cuerpo $\Leftrightarrow$ (0) es maximal.

Corolario 2 *Todo ideal maximal es primo.*

DEMOSTRACIÓN.

Todo cuerpo es dominio de integridad.

- Lo contrario no es cierto , ejemplo:

Sea $(x)\mathbf{Z}[x]$ es ideal primo de $(x)\mathbf{Z}[x]$ ya que

$\mathbf{Z}[x]/(x)\mathbf{Z}[x] \equiv \mathbf{Z}$ que es DI , y no maximal pues $\mathbf{Z}$ no es cuerpo.

Nota. Siempre se tiene que $IJ \subset I \cap J$ y si los ideales I, J son *comaximales*, es decir, $I + J = A$ entonces $IJ = I \cap J$.

En efecto, Si $I + J = A$, $\Rightarrow \exists\ h \in I, k \in J$ con $1 = h + k$, y si $b \in I \cap J$ $\Rightarrow b = bh + bk \in IJ$.

Tipos de homomorfismos

Sea $f : A \to B$ homomorfismo de anillos

- f es *monomorfismo* si es homomorfismo inyectivo.

- f es *epimorfismo* si es homomorfismo suprayectivo.

- f es *isomorfismo* si es homomorfismo biyectivo.

EJEMPLOS:

- El *homomorfismo de inclusión* $i : A \hookrightarrow B$ para $A \subset B$ es inyectivo.

- El *homomorfismo de proyección* para $I \subset A$ ideal, sea $p : A \to A/I$, $p(a) = a + I$ es suprayectivo.

Proposición 5 *$f : A \to B$ homomorfismo de anillos,*
es inyectivo $\Leftrightarrow ker(f) = \{0\}$.

DEMOSTRACIÓN.

$\Rightarrow$) Sea $a \in ker(f) \Rightarrow f(a) = 0 = f(0) \Rightarrow$ (por ser f inyectiva) $a = 0$.

$\Leftarrow$) Sea $f(a) = f(b) \Rightarrow 0 = f(a) - f(b) = f(a - b) \Rightarrow$

$a - b \in ker(f) = \{0\} \Rightarrow a - b = 0 \Rightarrow a = b$.

Nota. De lo anterior se deduce que todo homomorfismo $f : F \to A$, no nulo, con F cuerpo es inyectivo.
(un cuerpo solo tiene el cero como ideal propio)

- Dos anillos A, B son *isomorfos* $(A \approx B)$ si existe un isomorfismo f entre ellos y en dicho caso $f^{-1} : B \to A$ es también isomorfismo.

Teoremas de isomorfía

Teorema 1 *1^{er} teorema de isomorfía: Sea $f : A \to B$ homomorfismo de anillos. Entonces existe un único isomorfismo $\overline{f} : A/ker(f) \to im(f)$, tal que el diagrama siguiente*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/ker(f) & \overset{\overline{f}}{\approx} & im(f) \end{array}$$

es conmutativo, i.e. $f = i \circ \overline{f} \circ p$.

DEMOSTRACIÓN.

Definimos $\overline{f} : A/ker(f) \to im(f)$ como $\overline{f}(a + ker(f)) = f(a)$.

$\overline{f}$ es homomorfismo inyectivo ya que si $0 = \overline{f}(a + ker(f)) = f(a)$

$\Rightarrow a \in ker(f) \Rightarrow a + ker(f) = 0 + ker(f)$

$\overline{f}$ es suprayectivo ya que $im(\overline{f}) = im(f)$.

$\overline{f}$ es único, ya que si existe otro f^* verificando lo mismo que $\overline{f}$, $\forall\, a \in A$ $f^*(a + ker(f)) = f(a) = \overline{f}(a + kker(f))$.

Por último $\forall\ a \in A$, $i \circ \overline{f} \circ p(a) = i \circ \overline{f}(a + ker(f)) = i(f(a)) = f(a)$.

Nota El teorema anterior nos muestra que los homomorfismos de A en cualquier anillo dependen de los posibles ideales de A.

EJEMPLO:

El homomorfismo $f : \mathbf{Z} \to \mathbf{Z}_n$, $f(a) = \overline{k}$, con $k < n$, y $a - k = \lambda n$ verifica que $ker(f) = (n)$ y $f : \mathbf{Z}/ker(f) \approx \mathbf{Z}_n$.

Teorema 2 *Teorema de la correspondencia: Sea $I \subset A$ ideal. Entonces existe una biyección φ*
$\Gamma = \{J \subset A\ ideal, J \supset I\} \overset{\varphi}{\leftrightarrow} \Upsilon = \{\overline{J} \subset A/I\ ideal\}$
y ademas si $J \supset I$:
(i) J es primo $\Leftrightarrow$ J/I es primo.
(ii) J es maximal $\Leftrightarrow$ J/I es maximal.

DEMOSTRACIÓN.

Definimos para $I \subset J \subset A$ ideal, $\varphi(J) = J/I$ que se comprueba facilmente que es ideal de A/I.

φ es inyectiva ya que si $J/I = J'/I \Rightarrow \forall\ b \in J$, $\exists\ b' \in J'$ con $b + I = b' + I$ $\Rightarrow b - b' = h \in I \Rightarrow b = b' + h \in J' \Rightarrow J \subset J'$ (análogo $J' \subset J$).

φ es suprayectiva ya que dado $\overline{J}$ ideal de A/I, $J = \{a \in A : a + I \in \overline{J}\}$ es ideal de A, $I \subset J$ y $\varphi(J) = \overline{J}$.

(i) Sea $J \supset I$ primo y $(h + I)(k + I) \in J/I$ (como $I \subset J$) $\Rightarrow hk \in J$

(J primo) $\Rightarrow h \in J$ ó $k \in J \Rightarrow h + I \in J/I$ ó $k + I \in J/I$, y J/Ies primo.

(similar en sentido contrario)

(ii) Sea $J \supset I$ maximal, si J/I no es maximal en A/I, $\Rightarrow$

$\exists\ H \subsetneq A$ ideal y $J/I \subsetneq H/I$ (y si $p : A \to A/I$) $\Rightarrow$

$J = p^{-1}(J/I) \subset p^{-1}(H/I) = H$ (J maximal) $\Rightarrow J = H \Rightarrow J/I = H/I$
(contradición)
(similar en sentido contrario)

Teorema 3 *2^o teorema de isomorfía: Sea I, J ideales de A con $I \subset J$. Entonces J/I es ideal de A/I y*

$$\frac{A/I}{J/I} \approx \frac{A}{J}$$

DEMOSTRACIÓN.

Definimos $f : A/I \to A/J$, $\forall\, a \in A$, $f(a+I) = a+J$ que es trivialmente homomorfismo suprayectivo.

f está bien definido ya que si $a + I = a' + I \Rightarrow a - a' \in I \subset J \Rightarrow a + J = a' + J$.

como el núcleo $ker(f) = \{b + I : b + J = 0 + J\} = \{b + I : b \in J\} = J/I$, $\Rightarrow J/I$ es ideal de A/I, (por el 1^{er} teorema de isomorfía) $\Rightarrow$

$$\frac{A/I}{J/I} \approx \frac{A}{J}$$

EJEMPLO:

En los enteros tenemos:

$$\frac{\mathbf{Z}/(12)}{(4)/(12)} \approx \frac{\mathbf{Z}}{(4)}$$

Teorema 4 *3^{er} teorema de isomorfía: Sea $B \subset A$, subanillo, $I \subset A$ ideal. Entonces I es ideal de $B + I$ (subanillo de A), $B \cap I$ es ideal de B, y*

$$\frac{B+I}{I} \approx \frac{B}{B \cap I}$$

DEMOSTRACIÓN.

Se comprueba facilmente que I es ideal de $B+I$ (subanillo de A) y $B \cap I$ es ideal de B.

Definimos el homomorfismo $f : B \to B + I/I$ por $\forall\, b \in B$, $f(b) = b + I$.

($I \not\subseteq B$ en general) $\Rightarrow$ la imagen $im(f) = (B + I)/I$.

El núcleo $ker(f) = \{b \in B : b + I = 0 + I\} = \{b \in B : b \in I\} = B \cap I$,

(por el 1^{er} teorema de isomorfía) $\Rightarrow$

$$\frac{B}{B \cap I} \approx \frac{B+I}{I}$$

EJEMPLO:

En los enteros tenemos que $(4)+(6)=(2)$, $(4)\cap(6)=(12)$ y

$$\frac{(4)+(6)}{(6)} \approx \frac{(4)}{(4)\cap(6)}$$

Cuerpo de fracciones

Sea D un dominio de integridad, consideramos en $D\times(D\setminus\{0\})$ la relación

$(a,b)\sim(c,d) \Leftrightarrow ad-bc=0$

que se comprueba trivialmente que es de equivalencia, consideramos el conjunto cociente

$$\frac{D\times(D\setminus\{0\})}{\sim}$$

y denotamos la clase de (a,b) por a/b y definimos las operaciones:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

($bd\neq 0$ por ser D DI), que están bien definidas.

El cero es $0/b$, la unidad es a/a y el inverso de a/b $(a\neq 0)$ es b/a

Con esas operaciones $D\times(D\setminus\{0\})/\sim$ es un cuerpo,
el cuerpo de fracciones de D, $cf(D)$.

El homomorfismo $\varphi : D\to cf(D)$, $\varphi(a)=a/1$ es inyectivo y permite considerar D como subanillo de $cf(D)$ identificando $a\equiv a/1$.

Nota. El cuerpo de fracciones de D es el mínimo cuerpo que contiene a D.

EJEMPLO:

- $\mathbf{Q}$ es el cuerpo de fracciones de $\mathbf{Z}$.

- El cuerpo de fracciones de $\mathbf{Q}[x]$ es
$\{p(x)/q(x) \mid p(x), 0\neq q(x)\in\mathbf{Q}[x]\}\equiv\mathbf{Q}(x)$.

1.3 Anillos de polinomios

Dado un anillo A vamos a construir el anillo de polinomios en una indeterminada con coeficicentes en A, $A[x]$.

Definición 10 *Definimos* $A[x] = \{(a_0, a_1, \ldots, a_n, 0, \ldots) : a_i \in A\}$, *es decir el conjunto de las sucesiones de elementos de* A *con todos los elementos* 0 *salvo un número finito. Diremos que* a_i *es el coeficiente de grado* i *del polinomio.*

Definimos en $A[x]$ las siguientes operaciones:

- Suma: $(a_0, a_1, \ldots, a_n, 0, \ldots) + (b_0, b_1, \ldots, b_m, 0, \ldots) =$
$= (a_0 + b_0, a_1 + b_1, \ldots, a_m + b_m, a_{m+1}, \ldots, a_n, 0, \ldots)$ si $m \leq n$.

- Producto: $(a_0, a_1, \ldots, a_n, 0, \ldots)(b_0, b_1, \ldots, b_m, 0, \ldots) =$
$= (c_0, c_1, \ldots, c_{n+m}, 0, \ldots)$, con $c_k = \sum_{i=0}^{i=k} a_i b_{k-i}$

con $0 = (0, 0, \ldots, 0, \ldots)$, $1 = (1, 0, \ldots, 0, \ldots)$, y

$-(a_0, a_1, \ldots, a_n, 0, \ldots) = (-a_0, -a_1, \ldots, -a_n, 0, \ldots)$

Proposición 6 $A[x]$ *es un anillo conmutativo y con unidad*

DEMOSTRACIÓN.

Se sigue de las propiedades del anillo A.

Nota. Con esta definición es claro que dos polinomios son iguales si y solo si lo son todos los coeficientes del mismo grado de ambos.

Para obtener la notación usual, denotamos:
$a \equiv (a, 0, \ldots, 0, \ldots)$, para $a \in A$
$x \equiv (0, 1, 0, \ldots, 0, \ldots)$ (llamaremos a x indeterminada).

Entonces $x^k = (0, 0, \ldots, 1^{(k+1}, 0, \ldots)$, $ax^k = (0, 0, \ldots, a^{(k+1}, 0, \ldots)$ y por tanto

$(a_0, a_1, \ldots, a_n, 0, \ldots) = a_o + a_1 x + \cdots + a_n x^n$

Y tenemos
$a_o + a_1 x + \cdots + a_n x^n = b_o + b_1 x + \cdots + b_m x^m \Leftrightarrow n = m$ y $a_i = b_i \; \forall \; i$

Llamaremos a a_0 término constante y a a_n coeficiente principal.

Grado de un polinomio

Sea $0 \neq p(x) \in A[x]$, $p(x) = a_o + a_1x + \cdots + a_nx^n$, definimos *grado* de $p(x)$, $deg(p(x)) = n$, si n es el máximo de los i con $a_i \neq 0$.

Consideraremos $deg(0) = -\infty$, donde $-\infty$ verifica $\forall\ n \in \mathbf{N}$, $-\infty < n$, $-\infty + n = -\infty$, y $(-\infty) + (-\infty) = (-\infty)$.

El grado verifica: Sean $p(x) = a_o + a_1x + \cdots + a_nx^n$,
$q(x) = b_o + b_1x + \cdots + b_mx^m$

- $deg(p(x) + q(x)) \leq max\{deg(p(x)), deg(q(x))\}$

- $deg(p(x)q(x)) \leq deg(p(x)) + deg(q(x))$, y la igualdad

$deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ se da si $a_nb_m \neq 0$

Nota. Obsérvese que en un dominio de integridad se tiene siempre la igualdad anterior para el grado del producto.

Teorema 5 *Si D es dominio de integridad $\Rightarrow$ $D[x]$ es dominio de integridad, y las unidades de $D[x]$ son las de D.*

DEMOSTRACIÓN.

Sea $p(x)q(x) = 0 \Rightarrow -\infty = deg(p(x)q(x)) = deg(p(x)) + deg(q(x)) \Rightarrow$

$deg(p(x)) = -\infty$ ó $deg(q(x)) = -\infty \Rightarrow p(x) = 0$ ó $q(x) = 0$

$\Rightarrow D[x]$ es DI.

Sea $p(x)q(x) = 1 \Rightarrow deg(p(x)) = deg(q(x)) = 0 \Rightarrow$

$p(x) = a \in D$ y $q(x) = b \in D$, y a, b son unidades en D.

En $\mathbf{Z}_4[x]$ (no dominio de integridad) $\overline{2}x + \overline{1}$ es unidad, ya que
$(\overline{2}x + \overline{1})(\overline{2}x + \overline{1}) = \overline{4}x^2 + \overline{4}x + \overline{1} = \overline{1}$.

Algoritmo de división

Al dividir dos polinomios $p(x), q(x)$ sobre un anillo, en general, no podemos anular el coefeciente principal de $p(x)$ con el de $q(x)$, ejemplo:

En $\mathbf{Z}[x]$, para $3x+2$ dividido entre $2x+3$, no existe a entero con $a \cdot 2 = 3$, i.e. $3x + 2 \neq a(2x + 3) + r$ para todo entero a.

El siguiente algoritmo corrige en parte esta situación.

Teorema 6 *Sea $p(x), q(x) \in D[x]$, $q(x) \neq 0$. Sean $deg(q(x)) = m$ y b_m el coeficiente principal de $q(x)$. Entonces*
$\exists\, k \in \boldsymbol{N}$, $c(x), r(x) \in D[x]$ *con* $deg(r(x)) < deg(q(x))$ *verificando*

$$b_m^k p(x) = c(x)q(x) + r(x).$$

DEMOSTRACIÓN.

Si $deg(p(x)) < deg(q(x))$ entonces $p(x) = 0 \cdot q(x) + p(x)$.

Sean $deg(p(x)) \geq deg(q(x)) = m$, $p(x) = a_0 + a_1 + \cdots + a_n x^n$,
$q(x) = b_0 + b_1 + \cdots + b_m x^m$, $m \leq n$,
consideramos inducción en $deg(p(x))$:

si $deg(p(x)) = 1$, $p(x) = a_0 + a_1 x$, $q(x) = b_0 + b_1 x$ y

$b_1(a_0 + a_1 x) = a_1(b_0 + b_1 x) + (a_0 b_1 - a_1 b_0)$.

Supongamos cierto para $deg(p(x)) < n$, y consideramos $deg(p(x)) = n$

$b_m p(x) - a_n x^{n-m} q(x) = p_1(x)$, con $deg(p_1(x)) < n$ (hip. de inducción)

$\exists\, k_1 \in \mathbf{N}$, $c_1(x), r(x) \in D[x]$ con $deg(r_1(x)) < deg(q(x))$ verificando

$$b_m^{k_1} p_1(x) = c_1(x)q(x) + r(x) \quad \Rightarrow$$

$$b_m^{k_1}(b_m p(x) - a_n x^{n-m} q(x)) = c_1(x)q(x) + r(x) \quad \Rightarrow$$

$$b_m^{k_1+1} p(x) = (b_m^{k_1} a_n x^{n-m} + c_1(x))q(x) + r(x),$$

y si $k = k_1 + 1$, $c(x) = (b_m^{k_1} a_n x^{n-m} + c_1(x))$, tenemos

$$b_m^k p(x) = c(x)q(x) + r(x)$$

con $deg(r(x)) < deg(q(x))$.

Nota. En el algoritmo anterior es claro que $c(x)$ y $r(x)$ no son únicos en general.

Corolario 3 *Si F es cuerpo y $p(x), q(x) \in F[x]$, $q(x) \neq 0$. Entonces*
$\exists\, c(x), r(x) \in F[x]$ *únicos con* $deg(r(x)) < deg(q(x))$ *verificando*

$$p(x) = c(x)q(x) + r(x)$$

DEMOSTRACIÓN.

Como b_m tiene inverso, tenemos $p(x) = c(x)q(x) + r(x)$,

y si $p(x) = c(x)q(x) + r(x) = c'(x)q(x) + r'(x) \Rightarrow$

$(c(x) - c'(x))q(x) = (r'(x) - r(x))$, y si $c(x) \neq c'(x)$ (F es DI) $\Rightarrow$

$deg((c(x) - c'(x))q(x)) \geq deg(q(x)) \Rightarrow$

$deg((r'(x) - r(x)) \geq deg(q(x))$ contradición, salvo que

$r'(x) = r(x)$, y $c'(x) = c(x)$.

Teorema 7 *Si F es cuerpo entonces $F[x]$ es dominio de ideales principales.*

DEMOSTRACIÓN.

Sea $(0) \neq I \subset F[x]$ ideal $\Rightarrow \exists\, q(x) \neq 0$ con $deg(q(x))$ mínimo para I.

Sea $p(x) \in I$ por el algoritmo de división, $\exists\, c(x), r(x) \in D[x]$

con $deg(r(x)) < deg(q(x))$ y $p(x) = c(x)q(x) + r(x)$, $\Rightarrow$

$r(x) = p(x) - c(x)q(x) \in I$ y $deg(r(x)) < deg(q(x))$

(por la definición de $q(x)$, su grado es mínimo en I) $\Rightarrow$

$r(x) = 0$, $p(x) = c(x)q(x)$ y entonces $I = (q(x))F[x]$.

- Si el anillo base A de los polinomios no es cuerpo, entonces $A[x]$ no es dominio de ideales principales en general:

EJEMPLO:

Sea $\mathbf{Z}[x]$, el ideal $(2, x)\mathbf{Z}[x]$, no es principal.

Si $(2, x) = (p(x))$, $2 = c(x)p(x)$, y por los grados, $p(x) = a \in \mathbf{Z} \Rightarrow$

$x = aq(x)$ contradición, salvo $a = \pm 1$, i.e. $(2, x) = (1) = \mathbf{Z}$,

pero $\mathbf{Z}[x]/(2, x) \approx \mathbf{Z}_2$, $\Rightarrow (2, x) \neq (1)$.

Raíces de un polinomio

Sean $A \subset B$ anillos, llamaremos *homomorfismo de sustitución* a:

sea $u \in B$, $f_u : A[x] \to B$, con $f_u(p(x)) = p(u) = a_0 + a_1 u + \cdots + a_n u^n$, que es trivialmente homomorfismo.

Definición 11 *Sean $A \subset B$ anillos, y $p(x) \in A[x]$, $a \in B$ es raíz de $p(x)$, si $p(a) = 0$.*

Teorema 8 *Sea $p(x) \in A[x]$, $a \in A$, entonces $p(x) = c(x)(x-a) + p(a)$*

DEMOSTRACIÓN.

Por el algoritmo de división a $p(x)$ y $x - a$ con coeficiente principal $1 \Rightarrow$

$p(x) = c(x)(x-a) + r$, $r \in A$, (ya que $deg(r) < 1$) y
$p(a) = c(x)(a-a) + r = r$.

Corolario 4 *$a \in A$ es raíz de $p(x) \in A[x] \Leftrightarrow x - a$ es factor de $p(x)$,i.e. $(x-a)|p(x)$ (divide).*

Diremos que $\alpha \in A$ raíz de $p(x)$ tiene *multiplicidad* $mult(\alpha) = m$ si $p(x) = c(x)(x-a)^m$, con m máximo.

Teorema 9 *Sean D dominio de integridad, $p(x) \in D[x]$ de grado n, y sean $\alpha_1, \ldots, \alpha_r$ las raíces de $p(x)$ en D. Entonces*

$$\sum_{i=1}^{r} mult(\alpha_i) \leq n$$

DEMOSTRACIÓN.

Consideramos inducción en $deg(p(x))$. Sea $n = 1$ $p(x) = a_0 + a_1 x$

si $\alpha \in D$ es raíz de $p(x)$, entonces por el corolario anterior

$p(x) = a(x-\alpha)$, y $a_0 + a_1 x \neq a(x-\alpha)^2$ (por el grado), luego $mult(\alpha) = 1$,

y no existe otra raíz $\beta \in D$, $\alpha \neq \beta$, ya que $p(\beta) = a(\beta - \alpha) \neq 0$.

Supongamos cierto para $deg(p(x)) < n$ y α_1 raíz de $p(x)$, $mult(\alpha_1) = m_1$

por el corolario anterior aplicado m_1 veces $p(x) = (x-\alpha_1)^{m_1} q(x)$,

donde α_1 no es raíz de $q(x)$, ya que $mult(\alpha_1) = m_1$, y

si $q(x)$ no tiene mas raíces en D, entonces α_1 es la única raíz de $p(x)$ y

$$mult(\alpha_1) \leq deg(p(x)),$$

si $q(x)$ tiene raíces $\alpha_2, \ldots, \alpha_r$ en D, que también lo son de $p(x)$, y como $deg(q(x)) < deg(p(x))$ por la hipótesis de inducción

$$\sum_{i=2}^{r} mult(\alpha_i) \leq deg(q(x)) = deg(p(x)) - m_1$$

(D es DI), y se tiene

$$\sum_{i=1}^{r} mult(\alpha_i) \leq deg(p(x)).$$

- Si A no es DI el número de raíces puede ser superior al grado del polinomio:

EJEMPLO:

En $\mathbf{Z}_6[x]$, $x^3 - x$ tiene como raices $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$.

Proposición 7 *Sea,* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \boldsymbol{Z}[x]$, *y* $a/b \in \boldsymbol{Q}$ *una raíz de* $f(x)$ *en* $\boldsymbol{Q}$. *Si* a, b *son primos entre sí se tiene que* $a|a_0$ *y* $b|a_n$.

DEMOSTRACIÓN.

$f(a/b) = a_0 + a_1(a/b) + \cdots + a_n(a/b)^n = 0$, multiplicando por b^n,

$0 = b^n a_0 + a_1 b^{n-1} a + \cdots + a_n a^n = b^n a_0 + a_n a^n + ab(a_1 b^{n-2} + \cdots + a_{n-1} a^{n-2})$

$\Rightarrow b^n a_0 = a(-a_n a^{n-1} - b(a_1 b^{n-2} + \cdots + a_{n-1} a^{n-2})) \Rightarrow a|b^n a_o$,

y como $(a, b) = 1 \Rightarrow a|a_0$ (analogamente $b|a_n$).

Anillos de polinomios con varias indeterminadas

Definición 12 *Definimos el anillo de polinomios* $A[x_1, \ldots x_n]$ *con* n *indeterminadas con coeficientes en el anillo* A *inductivamente por*

$$A[x_1, x_2] \equiv (A[x_1])[x_2], \ldots, \; A[x_1, \ldots, x_n] \equiv (A[x_1, \ldots, x_{n-1}])[x_n].$$

Es decir $A[x_1, \ldots, x_n] \equiv A[x_1][x_2] \cdots [x_{n-1}][x_n]$, y los polinomios de $A[x_1, \ldots, x_n]$ se expresan como suma de monomios

$$p(x_1, \ldots x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

donde $a_{i_1,\ldots,i_n} \in A$ son los coeficientes.

Nota. Con esta definición es claro que dos polinomios son iguales si y solo si, lo son todos los coeficientes de ambos.

Corolario 5 *Si D es dominio de integridad $\Rightarrow$ $D[x_1, \ldots, x_n]$ es dominio de integridad, y las unidades de $D[x_1, \ldots, x_n]$ son las de D.*

DEMOSTRACIÓN.

Se deduce del teorema similar para una indeterminada.

Nota Si $n \geq 1$, $A[x_1, \ldots, x_n]$ no es en general un dominio de ideales principales, aunque A fuera cuerpo.

EJEMPLO:

Sea $\mathbf{Q}[x_1, x_2]$, el ideal (x_1, x_2) no es principal:

Si $(x_1, x_2) = (p(x_1, x_2)) \Rightarrow x_1 = q_1(x_1, x_2)p(x_1, x_2)$, $\Rightarrow$

$$1 = deg_{x_1}(x_1) = deg_{x_1}(q_1(x_1, x_2)) + deg_{x_1}(p(x_1, x_2))$$

$\Rightarrow p(x_1, x_2) = a(x_2)x_1 + b(x_2)$ y como $x_2 = q_2(x_1, x_2)p(x_1, x_2)$

$$0 = deg_{x_1}(x_2) = deg_{x_1}(q_2(x_1, x_2)) + deg_{x_1}(p(x_1, x_2))$$

$\Rightarrow deg_{x_1}(a(x_1, x_2)x_1 + b(x_2)) = 0$

$\Rightarrow a(x_1, x_2) = 0 \Rightarrow x_1 = q_1(x_1, x_2)b(x_2) \Rightarrow b(x_2) = cte.$ (contradición).

Nota Existe un algoritmo (mucho mas complicado que para el caso de una indeterminada) para un tipo de división de polinomios en varias indeterminadas dado por las bases de Gröbner.

1.4 Divisibilidad. Dominios Euclídeos

Vamos a estudiar la divisibilidad en un dominio de integridad.

Definición 13 *Dados $a, b \in A$ anillo, diremos que a divide a b, $a|b$, si $\exists\, c \in A$ y $b = ac$ (b es múltiplo de a).*

Se tiene en A que $a|b \Leftrightarrow (b) \subset (a)$.

Se tiene que $u \in A$ es unidad $\Leftrightarrow u|1$.

Definición 14 *Diremos que $a, b \in A$ son asociados, ($a \sim b$) si $a|b$ y $b|a$, y entonces $a = ub$ donde $u \in A$ es unidad (tiene inverso).*

- Las unidades de A son los asociados de 1.

- Diremos que a a es un *factor propio* de b si $a|b$ y b no divide a a y a no es unidad.

Definición 15 *Sea A anillo, decimos que d es máximo común divisor de a y b, $mcd(a, b) = d$ (ó $(a, b) = d$), si $d|a$, $d|b$, y si $\exists\, d' \in A$ con $d'|a$, $d'|b$ entonces $d'|d$.*

Nótese que el *mcd* es el máximo respecto de la relación de divisibilidad (en general no tenemos relaciones de orden para cualquier anillo A).

EJEMPLOS:

- En $\mathbf{Z}$ es el máximo común divisor usual.

Existen anillos donde no es posible considerar máximo común divisor:

- Sea el dominio de integridad $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} :\ a, b \in \mathbf{Z}\} \subset \mathbf{C}$,

consideramos $2(1 + \sqrt{-5}), 6 \in \mathbf{Z}[\sqrt{-5}]$, y tenemos que

$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$, se tiene que

2 y $(1 + \sqrt{-5})$ son ambos factor común de $2(1 + \sqrt{-5})$ y 6,

pero 2 no divide a $1 + \sqrt{-5}$, y $1 + \sqrt{-5}$ no divide a 2.

Notas (1) El máximo común divisor es único salvo producto por unidades. Es decir podríamos escribir $mcd(a, b) \sim d$.

(2) Diremos que $a, b \in A$ son *primos entre si* cuando $mcd(a, b) \sim 1$.

El máximo común divisor verifica las siguientes propiedades:

(1) Definimos el máximo común divisor $(a_1, \ldots, a_r) \sim d$ si d verifica $(a_1, a_2) \sim d_1$, $(d_1, a_3) \sim d_2$,...,$(d_{r-1}, a_r) \sim d$.
Se verifica similar al caso de dos elementos que $d|a_1, \ldots, d|a_r$ y si $d'|a_1, \ldots, d'|a_r$ entonces $d'|d$.

(2) $((a, b), c) \sim (a, (b, c))$.

(3) $c(a, b) \sim (ca, cb)$

Dominio euclídeo

Vamos a considerar dominios donde exista división entera similar a la de los números enteros.

Definición 16 *Un dominio de integridad D es dominio euclídeo (DE), si existe una aplicación $\delta : D \setminus \{0\} \to \boldsymbol{N}$ (función de grado) verificando si $a, b \in D$, con $b|a$, $\delta(b) \leq \delta(a)$, y tal que $\forall\ a, b \in D$, $b \neq 0$, $\exists\ c, r \in D$ verificando $a = bc + r$ y si $r \neq 0$ entonces $\delta(r) < \delta(b)$.*

EJEMPLOS:

- $(\mathbf{Z}, \delta = |\ |)$, ($|\ |$ valor absoluto) es dominio euclídeo.

- $(F[x], \delta = deg)$, F cuerpo, es dominio euclídeo.

- $(\mathbf{Z}[i], \delta = |\ |)$, ($|\ | = \|\ \|^2$, $\|\ \|$ norma) es dominio euclideo.

Para ver esto último sean $a + ib, c + id \in \mathbf{Z}[i]$, consideramos

$$\frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} = \frac{(a+ib)(c-id)}{c^2+d^2} = \alpha + i\beta,\ \alpha, \beta \in \mathbf{Q}$$

y sean $h, k \in \mathbf{Z}$ tales que $|\alpha - h| \leq 1/2,\ |\beta - k| \leq 1/2 \Rightarrow$

$\alpha = h + \alpha',\ \beta = k + \beta'$ con $|\alpha| \leq 1/2,\ |\beta| \leq 1/2, \Rightarrow$

$a + ib = (c + id)(\alpha + i\beta) = (c + id)((h + \alpha') + i(k + \beta')) =$

$= (c + id)(h + ik) + (c + id)(\alpha' + i\beta') = (c + id)(h + ik) + (r_1 + ir_2)$,

con $r_1, r_2 \in \mathbf{Z}$, ya que $r_1 + ir_2 = a + ib - (c + id)(h + ik) \in \mathbf{Z}[i]$,

y se tiene que

$|r_1 + ir_2| = |(c + id)(\alpha' + i\beta')| \leq |(c + id)|((1/2)^2 + (1/2)^2) < |(c + id)|$

En un dominio euclídeo podemos verificar facilmente si un elemento divide a otro.

Proposición 8 *Dados $a, b \in D$ dominio euclídeo, si $a|b$ y $\delta(a) = \delta(b)$, entonces a y b son asociados.*

DEMOSTRACIÓN.

Consideramos $a = bc + r$ con $\delta(r) < \delta(b)$, si $r \neq 0$, como $a|b$, $b = aa' \Rightarrow$

$r = a - bc = a(1 - a'c)$, es decir $a|r \Rightarrow \delta(a) \leq \delta(r) < \delta(b)$

(y como $\delta(a) = \delta(b)) \Rightarrow r = 0$, $b|a \Rightarrow a$ y b son asociados.

Lo contrario no es cierto, en $\mathbf{Z}[i]$, $\delta(3+4i) = \delta(5) = 25$ y no son asociados.

Corolario 6 *$a \in D$, D dominio euclídeo, $a \neq 0$ es unidad $\Leftrightarrow \delta(a) = \delta(1)$*

DEMOSTRACIÓN.

$\Rightarrow$) como a es unidad $a|1 \Rightarrow \delta(a) \leq \delta(1)$, y $1|a$ y $\delta(1) \leq \delta(a)$.

$\Leftarrow$) $1|a \Rightarrow$ y $\delta(a) = \delta(1) \Rightarrow a \sim 1$ es decir a es unidad.

Teorema 10 *D es dominio euclídeo $\Rightarrow D$ es dominio de ideales principales.*

DEMOSTRACIÓN.

(Similar a la de anillos de polinomios)
Sea $(0) \neq I \subset D$ ideal $\Rightarrow \exists\, 0 \neq q \in I$ con $\delta(q)$ mínimo para I.

Sea $p \in I$ por el algoritmo de división, $\exists\, c, r \in D$

con $\delta(r) < \delta(q)$, si $r \neq 0$ y $p = cq + r$, $\Rightarrow$

$r = p - cq \in I$ y $\delta(r) < \delta(q)$

(por la definición de q, su grado es mínimo en I) $\Rightarrow$

$r = 0$, $p = cq$ y entonces $I \subseteq (q)D$.

Lo contrario no es cierto en general, hay dominios de ideales principales que no son dominios euclídeos

EJEMPLO:

El dominio $D = \{(a+b/2)+(b/2)\sqrt{-19} : \ a, b \in \mathbf{Z}\}$ es dominio de ideales principales y no es dominio euclídeo (la demostración excede en dificultad a este curso).

Algoritmo de Euclides

Vamos a demostrar que un dominio euclídeo existe máximo común divisor dando un algoritmo para su cálculo.

Teorema 11 *Sea* (D, δ) *dominio euclídeo, entonces* $\forall\ a, b \in D - \{0\}$ *si* $a = bc + r$, $r \neq 0$ *con* $\delta(r) < \delta(b)$, $mcd(a, b) \sim mcd(b, r)$.

DEMOSTRACIÓN.

Sean $mcd(a, b) \sim d$, y $a = bc + r$ con $\delta(r) < \delta(b) \Rightarrow$

$r = a - bc$, y como $d|a$, $d|b \Rightarrow d|r$,

y si $d'|b$, $d'|r \Rightarrow d'|a = bc + r \Rightarrow d'|d$, y $mcd(b, r) \sim d$

Vamos a construir el *algoritmo de Euclides* para obtener el máximo común divisor $mcd(a, b)$. Consideramos

$a = bc_1 + r_1$ con $\delta(r_1) < \delta(b)$, si $r_1 \neq 0$
$b = r_1c_2 + r_2$ con $\delta(r_2) < \delta(r_1)$, si $r_2 \neq 0$
$r_2 = r_1c_3 + r_3$ con $\delta(r_3) < \delta(r_2)$, si $r_3 \neq 0$
$\cdots$
$r_{n-3} = r_{n-2}c_{n-1} + r_{n-1}$

y como $\delta(r_1) > \delta(r_2) > \delta(r_3) > \cdots$, existirá un $r_n = 0$, $n \leq \delta(b) - 1$,
y por tanto $r_{n-2} = r_{n-1}c_n$, y por el teorema anterior
$d \sim (a, b) \sim (b, r_1) \sim (r_1, r_2) \sim \cdots \sim (r_{n-2}, r_{n-1}) \sim r_{n-1}$.

Como consecuencia del algoritmo anterior
$d = r_{n-1} = r_{n-3} - r_{n-2}c_{r-1}$ y como
$r_{n-2} = r_{n-4} - r_{n-3}c_{r-2}$, $r_{n-3} = r_{n-5} - r_{n-4}c_{r-3}$,
sustituyéndolos en la fórmula anterior, en un proceso recursivo obtenemos
$d = r_{n-1} = r_{n-3} - r_{n-2}c_{r-1} = \cdots = \lambda a + \mu b$

Llamaremos a $d = \lambda a + \mu b$, identidad de Bezout, si $mcd(a, b) = 1$ entonces $\exists \lambda, \mu$, y $1 = \lambda a + \mu b$.

Ecuaciones diofánticas

Consideramos la ecuación diofántica $ax + by = c$ en $\mathbf{Z}$, la ecuación tiene solución si y solo si $mcd(a, b)|c$:

Sea $d = mcd(a, b)$, con $c = c'd$

con el algoritmo de euclides $\exists \lambda, \mu \in \mathbf{Z}$ con $d = \lambda a + \mu b$

entonces $(c'\lambda)a + (c'\mu)b = c'd = c$, da una solución a la ecuación, la solución no es única.

Las soluciones son de la forma $c'\lambda + tb, c'\mu - ta$, $t \in \mathbf{Z}$:

en efecto, sean $a'd = a, b'd = b$, tenemos $\lambda a + \mu b = 1$, si k, t verifican
$(\lambda + k)a' + (\mu + t)b' = 1$ como $\lambda a' + \mu b' = 1 \Rightarrow ka' + tb' = 0 \Rightarrow ka' = -tb'$
como $mcd(a', b') = 1 \Rightarrow a' \mid t$ y $b' \mid k \Rightarrow k'b'a' = -t'a'b' \Rightarrow k' = t'$
luego $(\lambda + t'b')a' + (\mu - t'a')b' = 1 \Rightarrow (\lambda + t'b')a + (\mu - t'a')b = d \; \forall t'$ luego
para $t'd$ tenemos $(\lambda + t'db')a + (\mu - t'da')b = d \Rightarrow$
$(\lambda + t'b)a + (\mu - t'a)b = d$, y
multiplicando por c' tenemos $(\lambda^* + t^*b)a + (\mu^* - t^*a)b = c$

Teorema chino del resto

Teorema 12 *Dados n, m primos entre sí se verifica*
$\boldsymbol{Z}_{mn} \approx \boldsymbol{Z}_m \times \boldsymbol{Z}_n$.

DEMOSTRACIÓN.

Dados m, n primos entre sí $\Rightarrow mcd(m, n) = 1 \Rightarrow \exists\, a, b$ y $1 = am + bn$
consideramos $x = \beta am + \alpha bn \Rightarrow x \equiv \alpha(m)$ y $x \equiv \beta(n)$, ya que
$x - \alpha = \beta am + \alpha bn - \alpha = \beta am + \alpha(bn - 1) = \beta am + \alpha(-am) \in (m)$

entonces $f : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ dada por
$c + (mn) \to (c + (m), c + (n))$
es isomorfismo y $f^{-1}(\alpha + (m), \beta + (n)) = x + (mn)$.

Dominio de ideales principales

En un dominio de ideales principales, D, $a, b \in D$, $a|b \Leftrightarrow (b) \subset (a)$.

Definición 17 *Dados $a, b \in A$ definimos el mínimo común múltiplo $mcm(a,b) = m$ ($[a,b] = m$), si $a|m$, $b|m$, y si $\exists\, m' \in A$ con $a|m'$, $b|m'$ entonces $m|m'$.*

EJEMPLOS:

- En $\mathbf{Z}$ es el mínimo común múltiplo usual.

Existen anillos donde no es posible considerar mínimo común multiplo (el considerado anteriormente):

- Sea el dominio de integridad $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} :\ a, b \in \mathbf{Z}\} \subset \mathbf{C}$,

consideramos $2, 1+\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}]$, como $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3$,

se tiene que 6, $2(1 + \sqrt{-5})$ son múltiplos de 2, y $(1 + \sqrt{-5})$,

pero 6 no divide a $2(1 + \sqrt{-5})$, y $2(1 + \sqrt{-5})$ no divide a 6, y como $2, 1+\sqrt{-5}$ son irreducibles (ver mas adelante) no pueden ser otros los posibles mcm.

En un dominio de ideales principales existe máximo común divisor y mínimo común multipo

Por ser dominio de ideales principales la suma de ideales, y el producto de ideales es un ideal principal.

(i) $(d) = (a) + (b) \Rightarrow (a) \subset (d)$, $(b) \subset (d) \Rightarrow d|a$, $d|b$,

y si $d'|a$, $d'|b \Rightarrow (a) \subset (d')$, $(b) \subset (d') \Rightarrow (d) = (a) + (b) \subset (d') \Rightarrow d'|d$.

(ii) $(m) = (a) \cap (b) \Rightarrow (m) \subset (a)$, $(m) \subset (b) \Rightarrow a|m$, $b|m$,

y si $a|m'$, $b|m' \Rightarrow (m') \subset (a)$, $(m') \subset (b) \Rightarrow$

$(m') \subset (a) \cap (b) = (m) \Rightarrow m|m'$.

Nota En un DIP se verifica que el $mcd(a,b) = d$ es $d = \lambda a + \mu b$, (identidad de Bezout).

Corolario 7 *En un dominio euclideo existe mínimo común multiplo.*

1.5 Dominios de factorizacion única

Vamos a estudiar los anillos que, como los enteros, admiten descomposición de sus elementos en producto de irreducibles.

Definición 18 *Diremos que $q \in A$ $q \neq 0$, es irreducible si q no es unidad, y si $q = ab$, entonces a ó b son unidades.*

EJEMPLOS:

- Los números primos en $\mathbf{Z}$ son irreducibles.

- $x^2 + 1$ en $\mathbf{R}[x]$ es irreducible (no tiene raíces en $\mathbf{R}$).

A partir de este punto consideraremos todos los anillos dominios de integridad.

Definición 19 *Dado $a \in D$ (DI), $a = p_1 p_2 \cdots p_s$ es una factorización en irreducibles esencialmente única si los p_i son irreducibles, y si $a = q_1 q_2 \cdots q_r$ entonces $s = r$ y existe una permutación γ de $\{1, 2, \ldots, s\}$ y se verifica que $\forall\, i \in \{1, 2, \ldots, s\}$, $p_i \sim q_{\gamma(i)}$.*

EJEMPLO:

- La factorización en $\mathbf{Z}$.

Definición 20 *D (DI) es Dominio de factorización única (DFU) si todo elemento que no sea unidad admite una facorización en irreducibles esencialmente única.*

EJEMPLO:

- $\mathbf{Z}$ es DFU con la factorización en primos. En este caso el único asociado a p, distinto de p, es $-p$.

Existen dominios de integridad que no son de factorización única ya que la factorización no es esencialmente única. Consideramos:

- El dominio de integridad $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : \ a, b \in \mathbf{Z}\} \subset \mathbf{C}$ no es DFU.

Para demostrarlo veamos primero que las unidades son $1, -1$.

Consideramos la norma $|a + b\sqrt{-5}| = a^2 + 5b^2 \in \mathbf{Z}$, que verifica

$|(a + b\sqrt{-5})(c + d\sqrt{-5})| = |a + b\sqrt{-5}||c + d\sqrt{-5}|$,

entonces $u \in \mathbf{Z}[\sqrt{-5}]$ es unidad si $\exists\, v \in \mathbf{Z}[\sqrt{-5}]$ con $uv = 1$

$\Rightarrow 1 = |uv| = |u||v| \Rightarrow |u| = 1 \Rightarrow a^2 + 5b^2 = 1 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$.

Sean las factorizaciones $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$, aplicando la norma podemos ver que

$1+\sqrt{-5}, 1-\sqrt{-5}, 2, 3$ son irreducibles, y

$1+\sqrt{-5} \nsim 2$, $1+\sqrt{-5} \nsim 3$, $1-\sqrt{-5} \nsim 2$, $1-\sqrt{-5} \nsim 3$.

Existen dominios de integridad que no son de factorización única ya que no existe factorización finita en irreducibles:

- Sea $\mathbf{Q}[\{x^{1/n}\}, n \in \mathbf{N}]$ (expresiones polinomicas en potencias de los $x^{1/n}$, entonces $x = x^{1/2}x^{1/2} = x^{1/2}x^{1/4}x^{1/4} = x^{1/2}x^{1/4}x^{1/8}x^{1/8} = \cdots$ no admite factorización finita.

Definición 21 *$p \in D$ es primo si p no es unidad, y si $p|ab$ entonces $p|a$ ó $p|b$.*

EJEMPLO:

- En $\mathbf{Z}$ los primos e irreducibles son los primos.

- En $\mathbf{Z}[\sqrt{-5}]$, 2 no es primo ya que $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$

y 2 no divide a $1+\sqrt{-5}$, ni a $1+\sqrt{-5}$ y es irreducible.

- En $\mathbf{Z}[i]$ si un primo es suma de cuadrados $p = a^2 + b^2 = (a+ib)(a-ib)$ no sería irreducible, por ejemplo $2, 5$.

Proposición 9 *Todo primo $p \neq 0$ es irreducible.*

DEMOSTRACIÓN.

Supongamos p primo y sea $p = p_1p_2 \Rightarrow p|p_1p_2$ (p primo) $\Rightarrow p|p_1$ ó $p|p_2$, y si suponemos $p|p_1$ como $p_1|p \Rightarrow p \sim p_1$ y por tanto p_2 es unidad.

Nota En general todo irreducible no es primo: En el ejemplo anterior $2 \in \mathbf{Z}[\sqrt{-5}]$ es irreducible y no es primo.

Proposición 10 *Si D es DFU, entonces todo irreducible $p \neq 0$ es primo.*

DEMOSTRACIÓN.

Sea $p \neq 0$ irreducible y $p|ab$, con $a = p_1p_2\cdots p_s$, y $b = q_1q_2\cdots q_r$ y
p_i, q_j irreducibles $\Rightarrow pc = ab$ con $c = c_1\cdots c_k$, c_i irreducibles, y
$pc_1\cdots c_k = p_1p_2\cdots p_sq_1q_2\cdots q_r$ (como D es DFU) $\Rightarrow$
$\exists\, p_i$ ó q_j con $p \sim p_i$ ó $p \sim q_j \Rightarrow p|a$ ó $p|b$.

Proposición 11 *Si D es DFU, entonces, y $p \in D - \{0\}$ $(p) \subset D$ es ideal primo $\Leftrightarrow$ p es irreducible (o primo).*

DEMOSTRACIÓN.

$\Rightarrow$) Si $p|ab \Rightarrow ab \in (p) \Rightarrow$ ((p) primo) $a \in (p)$ o $b \in (p) \Rightarrow p|a$ o $p|b$.

$\Leftarrow$) Sea $ab \in (p) \Rightarrow ab = cp \Rightarrow p|ab \Rightarrow$ (p primo) $p|a$ o $p|b \Rightarrow a \in (p)$ o $b \in (p)$.

La antepenúltima propiedad nos permite caracterizar los DFU.

Teorema 13 *Sea D dominio de integridad tal que todo elemento admite una factorización en irreducibles, entonces:*

D es DFU (la factorización es esencialmente única) $\Leftrightarrow$ todo irreducible es primo.

DEMOSTRACIÓN.

$\Rightarrow$) Es una de las proposiciones anteriores.
$\Leftarrow$) Sea $0 \neq a \in D$ no unidad, y $a = p_1 p_2 \cdots p_s$, los p_i irreducibles,
una factorización, veamos que es esencialmente única:
hacemos inducción en el número de factores s, sea $s = 1$,
es decir a irreducible, si $a = q_1 q_2 \cdots q_r$, los q_i irreducibles $\Rightarrow q_1|a \Rightarrow$
(a irreducible) $a = q_1 u$, $(u = q_2 \cdots q_r)$, irreducible y $a \sim q_1$.
Supongamos que es esencialmente única para $s - 1$ factores,
y sea $a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$, los p_j, q_i irreducibles, $\Rightarrow$
$p_1|q_1 q_2 \cdots q_r$ y como p_1 es primo $\Rightarrow p_1|q_1$ ó $p_1|q_2 \cdots q_r$, esto último $\Rightarrow$
$p_1|q_2$ ó $p_1|q_3 \cdots q_r$, siguiendo el proceso tenemos $p_1|q_1$ ó $p_1|q_2$ ó $\ldots$ ó $p_1|q_r$,
supongamos $p_1|q_k$ (irreducibles) $\Rightarrow q_k = u p_1$, u unidad $\Rightarrow$
$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_{k-1} \cdot u p_1 \cdot q_{k+1} \cdots q_r \Rightarrow$
$b = p_2 \cdots p_s = q_1 q_2 \cdots q_{k-1} \cdot q_{k+1} \cdots q_r$ tiene una factorización con $s - 1$
elementos y por la hipótesis de indución $s - 1 = r - 1$, (luego $r = s$)
y existe una permutación γ de $\{2, \ldots, s\}$ y se verifica que
$\forall\, i \in \{2, \ldots, s\}$ $p_i \sim q_{\gamma(j)}$ que junto con $p_1 \sim q_k$ da el resultado.

Proposición 12 *Si D es DFU, entonces $\forall\ a, b \in D$ existe $mcd(a, b)$ y $mcm(a, b)$.*

DEMOSTRACIÓN.

Similar a $\mathbf{Z}$ el $mcd(a,b)$ es el producto de los irreducibles comunes a a y b con el menor exponente, y el $mcm(a,b)$ es el producto de los irreducibles comunes y no comunes con el máximo exponente.

Corolario 8 *Sea D es DFU, entonces $\forall\ a,b \in D$, si $d = mcd(a,b)$, $m = mcm(a,b)$, entonces $dm = ab$.*

Corolario 9 *Sea D es DFU, si $a|bc$, y $mcd(a,b) = 1$, entonces $a|c$.*

La existencia de mcd nos da un criterio para DFU.

Teorema 14 *Sea D dominio de integridad tal que todo elemento admite una factorización en irreducibles, entonces:*

D es DFU (la factorización es esencialmente única) $\Leftrightarrow \forall\ a,b \in D$ existe $mcd(a,b)$.

DEMOSTRACIÓN.

$\Rightarrow$) Visto en la proposición anterior.

$\Leftarrow$) Por la caracterización dada, veamos que todo irreducible es primo,
sea q irreducible con $q \not| a$, $q \not| b \Rightarrow$
(q irreducible) $(q,a) \sim 1$ y $(q,b) \sim 1 \Rightarrow$
$(qb, ab) \sim b$, y como $(b,1) \sim 1$, $\Rightarrow (qb,q) \sim q \Rightarrow$
$1 \sim (q,b) \sim (q,(qb,ab)) \sim ((q,qb),ab) \sim (q,ab) \Rightarrow q \not| ab$.

Teorema 15 *Todo dominio de ideales principales es dominio de factorización única (DIP $\Rightarrow$ DFU).*

DEMOSTRACIÓN.

Veamos en primer lugar que todo elemento de D admite factorización en irreducibles.

Supongamos $\exists\ a \in D$ que no admite factorización en irreducibles, veamos entonces que existe una sucesión infinita $\{a_n\}_{n\in\mathbf{N}}$, con $a_{n+1}|a_n$:

Sea $a = a_o = a_1 b_1$, a_1, b_1 no son unidades, y a_1 ó b_1 no admiten factorización finita en irreducibles, (supongamos a_1) y $a_1|a_0$,

supongamos existen $a_0, \dots a_n$ verificandolo
a_n no admite factorización en irreducibles, luego $a_n = a_{n+1}b_{n+1}$
y podemos suponer a_{n+1} no admite factorización en irreducibles $\Rightarrow$
continuando el proceso, existe $\{a_n\}_{n\in\mathbf{N}}$, con $a_{n+1}|a_n$.

Entonces existe una cadena creciente infinita de ideales
$(a_0)D \subsetneq (a_1)D \subsetneq (a_2)D \subsetneq \cdots (a_n)D \subsetneq (a_{n+1})D \subsetneq \cdots$,

pero $I = \bigcup_{i\geq 0}(a_i)D$ es un ideal de D (fácil comprobación) $\Rightarrow$

$I = (a)D$ y $\exists\ k$ con $a \in (a_k)D \Rightarrow$
$a = a_k c$ y $a_k = ac' \Rightarrow a = ac'c \Rightarrow c'c = 1$, c, c' son unidades e

$I = \bigcup_{i\geq 0}(a_i)D = (a)D = (a_k)D \Rightarrow (a_k)D = (a_{k+1})D = \cdots \Rightarrow a_k \sim a_{k+1}$,
contradición con que a_k no admite factorización en irreducibles.

La factorización es esencialmente única por la caracterización anterior, ya que en un DIP existe mcd.

Corolario 10 *Todo dominio euclídeo es dominio de factorización única.*

Corolario 11 *En un DE y en un DIP* $mcd(a, b) \cdot mcm(a, b) = ab$.

Nota DE $\Rightarrow$ DIP $\Rightarrow$ DFU $\Rightarrow$ DI, y las implicaciones en sentido contrario no se dan.

- DI $\not\Rightarrow$ DFU, ejemplo: $\mathbf{Z}[\sqrt{-5}]$.

- DFU $\not\Rightarrow$ DIP, ejemplo: $\mathbf{Z}[x]$, (se demostrará mas adelante).

- DIP $\not\Rightarrow$ DE, ejemplo: $\{(a + b/2) + (b/2)\sqrt{-19} :\ a, b \in \mathbf{Z}\}$.

Proposición 13 *Si D es DIP, entonces*
(p) es ideal primo $\Leftrightarrow$ (p) es ideal maximal.

DEMOSTRACIÓN.

Ya sabemos que todo ideal maximal es primo.
Sea (p) ideal primo $\Rightarrow$ (por lo anterior) p es irreducible, y supongamos
$\exists\ (a) \subsetneq D$ con $(p) \subset (a) \Rightarrow p = ab$
y como p es irreducible b es unidad y $(p) = (a)$.

Corolario 12 *Sea F cuerpo, y $p(x) \in F[x]$ irreducible, entonces $F[x]/(p(x))F[x]$ es cuerpo.*

DEMOSTRACIÓN.

F cuerpo $\Rightarrow$ $F[x]$ DE $\Rightarrow$ $F[x]$ DIP $\Rightarrow$ $(p(x))$ ideal primo y maximal $\Rightarrow$ $F[x]/(p(x))F[x]$ cuerpo.

Nota Con lo anterior podemos construir cuerpos finitos. Por ejemplo $\mathbf{Z}_p[x]/(q(x))$, p primo, $q(x)$ irreducible de grado d es un cuerpo con p^d elementos.

1.6 Factorialidad de anillos de polinomios

Vamos a demostrar que los anillos de polinomios con coeficientes en un DFU son también DFU.

Definición 22 *Dado D DFU, llamaremos contenido de $f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$, a $c(f) = mcd(a_0, a_1, \ldots, a_n)$. Diremos que $f(x)$ es primitivo si $c(f) = 1$.*

Nota (i) Todo polinomio $f(x) = c(f)f_1(x)$, con $f_1(x)$ primitivo,
ya que si $c(f) = c$, $f_1(x) = a'_0 + a'_1x + \cdots + a'_nx^n$, $a_i = ca'_i$, y
$c = (a_0, a_1, \ldots, a_n) = (ca'_0, ca'_1, \ldots, ca'_n) = c(a'_0, a'_1, \ldots, a'_n)$
$\Rightarrow (a'_0, a'_1, \ldots, a'_n) = 1$.
(ii) Si $f(x) = c_1f_1(x) = c_2f_2(x)$, con $f_1(x), f_2(x)$ primitivos $\Rightarrow$
$c_1 \sim c_2$ y $f_1(x) = uf_2(x)$, u unidad en D, es decir $f_1(x) \sim f_2(x)$ en $D[x]$.
Para comprobarlo consideremos $f_2(x) = a''_0 + a''_1x + \cdots + a''_nx^n \Rightarrow$
$c_1 = c_1(a'_0, a'_1, \ldots, a'_n) \sim (a_0, a_1, \ldots, a_n) = (c_2a''_0, c_2a''_1, \ldots, c_2a''_n) \sim c_2 \Rightarrow$
$c_2 = uc_1$, u unidad y $f(x) = c_1f_1(x) = uc_1f_2(x) \Rightarrow f_1(x) = uf_2(x)$

EJEMPLO:

En $\mathbf{Z}[x]$, $8x^2+6x+10 = 2(4x^2+3x+5)$, tiene contenido 2 y $4x^2+3x+5$ es primitivo.

Vamos a extender el contenido a polinomios sobre el cuerpo de fracciones.

Proposición 14 *Sea D es DFU, K cuerpo de fracciones de D, y $f(x) \in K[x]$, entonces $f(x) = \alpha f_1(x)$, $\alpha \in K$, $f_1(x) \in D[x]$ primitivo, y la factorización es única salvo producto por unidades de D.*

DEMOSTRACIÓN.

$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in K[x]$, $\alpha_i = a_i/b_i$, $a_i, b_i \in D$, $b_i \neq 0$,

sea $b = \prod_{i=0}^{n} b_i \neq 0$, $bf(x) \in D[x]$ y $bf(x) = cf_1(x)$, con $c \in D$

y $f_1(x) \in D[x]$ primitivo, luego $f(x) = (c/b)f_1(x)$, con $\alpha = c/b \in K$.

Sean $f(x) = (a/b)f_1(x) = (a'/b')f_2(x)$, $a/b, a'/b' \in K$

y $f_1(x), f_2(x) \in D[x]$ primitivos $\Rightarrow ab'f_1(x) = a'bf_2(x)$ en $D[x]$

$\Rightarrow f_1(x) \sim f_2(x)$ en $D[x]$, y $ab' = u(a'b)$, con u unidad en $D \Rightarrow$

$(a/b) = u(a'/b')$

Nota Como en polinomios con coeficientes en D, tenemos para los polinomios sobre el cuerpo de fracciones de D el contenido de un polinomio $f(x) = \alpha f_1(x)$, con $\alpha = a/b \in K$ y $f_1(x)$ primitivo.

Corolario 13 *Si $f(x), g(x)$ son primitivos en $D[x]$ y asociados en $K[x]$ ($K = cf(D)$), entonces son asociados en $D[x]$.*

DEMOSTRACIÓN.

Sea $f(x) = \alpha g(x)$, $\alpha = a/b \in K \Rightarrow bf(x) = ag(x)$ en $D[x] \Rightarrow (f(x), g(x)$ primitivos) $a \sim b$ en $D \Rightarrow a = ub$, u unidad en $D \Rightarrow \alpha = a/b = u$ unidad en D.

Proposición 15 *(Lema de Gauss) En $D[x]$ con D DFU el producto de polinomios primitivos es primitivo.*

DEMOSTRACIÓN.

Sean $f(x), g(x)$ primitivos en $D[x]$ tales que $f(x)g(x)$ no sea primitivo

$\Rightarrow \exists\, p \in D$ irreducible (primo) con $p \not| f(x)$, $p \not| g(x)$, y $p | f(x)g(x)$

$\Leftrightarrow f(x)g(x) \in (p)D[x]$, $f(x) \notin (p)D[x]$ y $g(x) \notin (p)D[x]$,

es decir, $(p)D[x]$ no es ideal primo, pero

$$\frac{D[x]}{(p)D[x]} \approx \frac{D}{(p)D}[x]$$

es DI, ya que $(D/(p)D)$ es DI, pues $0+(p)$ no tiene divisores de cero por ser p irreducible.

Proposición 16 *Sea D DFU, si $f(x) \in D[x]$ tiene grado positivo y es irreducible en $D[x]$, entonces es irreducible en $K[x]$ ($K = cf(D)$).*

DEMOSTRACIÓN.

$f(x) \in D[x]$ con $deg(f(x)) \geq 1$ e irreducible en $D[x] \Rightarrow f(x)$ es primitivo,

sea $f(x) = \gamma_1(x)\gamma_2(x)$, $\gamma_1(x), \gamma_2(x) \in K[x]$, de grados $\geq 1 \Rightarrow$

$f(x) = c(\gamma_1)c(\gamma_2)f_1^*(x)f_2^*(x)$, con $f_1^*(x), f_2^*(x) \in D[x]$ primitivos,

$c(\gamma_1), c(\gamma_2) \in K \Rightarrow f_1^*(x)f_2^*(x)$ es primitivo (lema de Gauss) $\Rightarrow$

$f(x) \sim f_1^*(x)f_2^*(x)$ en $D[x] \Rightarrow f(x) = uf_1^*(x)f_2^*(x)$ (u unidad), $\Rightarrow$

$f(x)$ es reducible en $D[x]$, contradición.

Teorema 16 *Si D es DFU, entonces $D[x]$ es DFU.*

DEMOSTRACIÓN.

Veamos en primer lugar que todo $f(x) \in D[x]$ admite una factorización en irreducibles:

$f(x) = c(f)f_1(x)$ con $f_1(x)$ primitivo, si $f_1(x)$ no es irreducible,

$f_1(x) = q(x)p(x)$, $deg(q(x)) < deg(f_1(x))$, $deg(p(x)) < deg(f_1(x))$

y son primitivos y si no son irreducibles podemos factorizarlos $\Rightarrow$
(en un numero finito de pasos)

$f_1(x) = q_1(x)q_2(x)\cdots q_r(x)$ con $r \leq deg(f_1(x)$, y los $q_i(x)$ irreducibles,

por otra parte $c(f) = p_1p_2\cdots p_s$, los p_i irreducibles (D DFU) $\Rightarrow$

$f(x) = c(f)f_1(x) = p_1p_2\cdots p_sq_1(x)q_2(x)\cdots q_r(x)$ en $D[x]$.

Veamos ahora que la factorización es esencialmente única: sean

$f(x) = p_1 p_2 \cdots p_s q_1(x) q_2(x) \cdots q_r(x) = p'_1 p'_2 \cdots p'_t q'_1(x) q'_2(x) \cdots q'_m(x)$

como los $q_i(x), q'_i(x)$ son irreducibles en $D[x]$, son primitivos $\Rightarrow$

$q_1(x)q_2(x)\cdots q_r(x)$, y $q'_1(x)q'_2(x)\cdots q'_m(x)$ son primitivos (lema de Gauss)

$\Rightarrow$ asociados en $D[x] \Rightarrow$

$q_1(x)q_2(x)\cdots q_r(x) = uq'_1(x)q'_2(x)\cdots q'_m(x)$, u unidad,

$q_i(x), q'_i(x)$ son irreducibles en $D[x]$ y grado $\geq 1 \Rightarrow$

$q_i(x), q'_i(x)$ son irreducibles en $K[x]$, $K = cf(D)$ (proposición anterior)

$\Rightarrow$ (como $K[x]$ es DFU) las dos factorizaciones son esencialmente únicas

$\Rightarrow r = m$ y existe una reorganización de indices con $q_i(x) \sim q'_i(x)$ en $K[x]$

$\Rightarrow$ (por un corolario anterior) $q_i(x) \sim q'_i(x)$ en $D[x]$

por último como $p_1 p_2 \cdots p_s \sim p'_1 p'_2 \cdots p'_t$ en D(como D es DFU)
las dos fatorizaciones son esencialmente únicas $\Rightarrow$

$s = t$ y despues de una reorganización de los indices $c_i \sim c'_i$.

Corolario 14 *Si D es DFU, entonces $D[x_1, \ldots, x_n]$ es DFU.*

DEMOSTRACIÓN.

D DFU (por el teorema anterior) $\Rightarrow D[x_1]$ es DFU

(por el teorema anterior) $\Rightarrow (D[x_1])[x_2]$ es DFU

$\Rightarrow \cdots \Rightarrow$ (por el teorema anterior)

$(\cdots((D[x_1])[x_2])\cdots)[x_n] = D[x_1, \ldots, x_n]$ es DFU.

Nota.

$F[x]$ tiene infinitos polinomios irreducibles:
Sean s polinomios irreducibles, veamos que $f(x) = p_1(x)\cdots p_s(s) + 1$
es irreducible, ya que si no lo es, existe $p_i(x)$ irreducible y
$p_i(x)|f(x) = p_1(x)\cdots p_s(s) + 1$ y $p_i(x)|p_1(x)\cdots p_s(s) \Rightarrow$
$p_i(x)|1$, que no es posible.

EJEMPLOS:

- $\mathbf{Z}[x]$ es DFU.

- $\mathbf{Q}[x_1, \ldots, x_n]$ es DFU.

Para acabar estableceremos que los anillos de polinomios sobre un cuerpo son noetherianos, es decir todos sus ideales son finitamente generados.

Teorema 17 *(de la base de Hilbert) Sea A anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ es noetheriano.*

1.7 Criterios de irreducibilidad

Vamos a estudiar la irreducibilidad en anillos de polinomios sobre un DFU y sobre su cuerpo de fracciones. Supondremos en esta sección que D es un DFU, y $K = cf(D)$.

Si un polinomio $f(x) \in D[x]$ tiene raíz $\alpha \in D$, factoriza $f(x) = (x-\alpha)g(x)$ en $D[x]$, y no será irreducible. Vamos a ver en primer lugar cuáles son las posibles raíces de un polinomio.

Proposición 17 *Sean D DFU, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$, y $a/b \in K = cf(D)$ una raíz de $f(x)$ en K. Si a, b son primos entre sí se tiene que $a|a_0$ y $b|a_n$.*

DEMOSTRACIÓN.

Análoga a la de polinomios en $\mathbf{Z}$ sección 1.3.

Nota (i) Los polinomios de grado 1 en $D[x]$ con coeficiente principal 1 son irreducibles ya que solo se podrían factorizar en polinomios de grado 1.

(ii) $f(x) \in D[x]$ mónico de grado 2, ó 3 es irreducible $\Leftrightarrow$ no tiene raíces en D.

Si $f(x)$ es reducible como es mónico los factores tienen que ser de grado positivo y mónicos, y por tanto uno de ellos de grado 1 $\Rightarrow$ $f(x)$ tiene una raiz en D.

iii) $f(x) \in D[x]$ de grado 2, ó 3 es irreducible en $K[x] \Leftrightarrow (K = cf(D))$ no tiene raíces en K.

En $\mathbf{Z}[x]$, $(x^2+1)^2$ es reducible sin raices.

Proposición 18 *$f(x) \in D[x]$ de grado ≥ 1, entonces $f(x)$ es irreducible en $D[x] \Leftrightarrow f(x)$ es irreducible en $K[x]$ y $c(f) = 1$.*

DEMOSTRACIÓN.

Visto en la sección anterior.

Cambiando por traslación la indeterminada tenemos

Proposición 19 *$f(x) \in D[x]$ de grado ≥ 1, entonces son equivalentes:*

(i) $f(x)$ es irreducible en $D[x]$.

(ii) $f(x+a)$ es irreducible en $D[x]$ $\forall\, a \in D$.

(iii) $\exists\, a \in D$ y $f(x+a)$ es irreducible en $D[x]$.

DEMOSTRACIÓN.

(i) $\Rightarrow$ (ii) Si $\exists\, a \in D$ con $f(x+a) = g(x)h(x) \Rightarrow$

$f(x) = f(x+a-a) = g(x-a)h(x-a) \Rightarrow f(x)$ es reducible en $D[x]$.

(ii) $\Rightarrow$ (iii) Evidente.

(iii) $\Rightarrow$ (i) Si $f(x) = g(x)h(x) \Rightarrow \forall\, a \in D$ $f(x+a) = g(x+a)h(x+a) \Rightarrow$

$f(x+a)$ es reducible en $D[x]$, $\forall\, a \in D$.

Si un polinomio es irreducible también lo es si se considera el polinomio en "sentido contrario".

Proposición 20 *$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in D[x]$ es irreducible en $D[x] \Leftrightarrow g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ es irreducible en $D[x]$.*

DEMOSTRACIÓN.

Si $g(x) = h(x)k(x)$ en $D[x] \Rightarrow g(1/x) = h(1/x)k(1/x)$, $deg(h(x)) = r$

$\Rightarrow x^n g(1/x) = x^n h(1/x)k(1/x) = x^r h(1/x)x^{n-r}k(1/x)$, y como

$x^n g(1/x) = x^n(a_0(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_{n-1}(1/x) + a_n) = f(x)$,

si $h^*(x) = (x^r h(1/x))$, y $k^*(x) = (x^{n-r}k(1/x)) \Rightarrow f(x) = h^*(x)k^*(x)$.

Analogamente en sentido contrario.

Proposición 21 *(Criterio de Eisenstein) Sea D DFU, y* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in D[x]$, $n \geq 1$ *y primitivo. Supongamos que existe* $p \in D$ *irreducible verificando* $p|a_0$, $p|a_1$, ..., $p|a_{n-1}$, $p \not| a_n$, $p^2 \not| a_0$, *entonces* $f(x)$ *es irreducible en* $D[x]$.

DEMOSTRACIÓN.

Supongamos $f(x)$ reducible, es decir existen polinomios primitivos con

$a_0 + a_1x + \cdots + a_nx^n = (b_0 + b_1x + \cdots + b_sx^s)(c_0 + c_1x + \cdots + a_{n-s}x^{n-s})$

y como $p|a_0 = b_0c_0 \Rightarrow$ (p primo) $p|b_0$, ó $p|c_0$,

y como $p^2 \not| a_0$ podemos suponer $p|b_0$, y $p \not| c_0$,

como $a_1 = b_0c_1 + b_1c_0$, y $p|a_1$, $p|b_0$, $p \not| c_0 \Rightarrow p|b_1$

supongamos $\exists\ k$ con $p|b_0, p|b_1 \ldots, p|b_{k-1}$, y $p \not| b_k$

como $p|a_k = b_0c_s + \cdots + b_{k-1}c_1 + b_kc_0 \Rightarrow p|c_0$

contradición que nos da que $p|b_s \Rightarrow p|a_n = b_sc_{n-s}$ (contradición), y $f(x)$ es irreducible.

Por lo anterior para el polinomio recíproco, tenemos el criterio

Proposición 22 *(Criterio de Eisenstein *) Sea D DFU, y* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in D[x]$, $n \geq 1$ *primitivo. Supongamos que existe* $p \in D$ *irreducible verificando* $p|a_n$, $p|a_{n-1}$, ..., $p|a_1$, $p \not| a_o$, $p^2 \not| a_n$, *entonces* $f(x)$ *es irreducible en* $D[x]$.

Nota Podemos usar los criterios anteriores en los polinomios $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{Q}[x, y] = (\mathbf{Q}[x])[y]$, o con mas indeterminadas.

EJEMPLOS:

- $x^5 + 4x^3 + 10x^2 + 2x + 6 \in \mathbf{Z}[x]$ es irreducible con $p = 2$ por el criterio de Einsestein.

- $q(x, y) = y^3 + x^2y^2 + x^2 + xy^2 + 2y + 2xy - 1 \in \mathbf{Z}[x, y]$ es irreducible por el criterio de Einsestein con $p(x) = x + 1$ irreducible y

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

Proposición 23 *(Criterio modular) Sea* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \boldsymbol{Z}[x]$, $n \geq 1$ *y primitivo. Supongamos que existe* $p \in \boldsymbol{Z}$ *primo con* $p \not| a_n$, *y tal que* $\overline{f(x)} = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_{n-1}x^{n-1} + \overline{a}_nx^n$ *con* $\overline{a}_i = a_i + (p) \in \boldsymbol{Z}_p$ *es irreducible en* $\boldsymbol{Z}_p[x]$, *entonces* $f(x)$ *es irreducible en* $\boldsymbol{Z}[x]$.

DEMOSTRACIÓN.

Por redución al absurdo, supongamos que $f(x) = g(x)h(x)$ en $\mathbf{Z}[x]$,

entonces para todo primo $p \not| a_n$, $\overline{a}_m \neq \overline{0}$, y como $a_n = b_mc_{n-m}$

(b_m, c_{n-m} coeficientes principales de $g(x)$ y $h(x)$ respectivamente)

$\Rightarrow p \not| b_m$, $p \not| c_{n-m}$, y $\overline{b}_m \neq \overline{0}$, $\overline{c}_{n-m} \neq 0$, y

$\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$ en $\mathbf{Z}_p[x]$ es reducible para todo primo p.

EJEMPLO:

Sea $x^4 + 6x^3 + 4x^2 + 7x + 5 \in \mathbf{Z}[x]$, módulo 2 en $\mathbf{Z}_2[x]$ es $X^4 + x + 1$
que no tiene raíces en $\mathbf{Z}_2$, y la única descomposición posible en $\mathbf{Z}_2[x]$ sería:
$x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ con $a, b \in \{0, 1\} = \mathbf{Z}_2$ lo cual no es posible

Irreducibles en Z[i]

Los irreducibles en $\mathbf{Z}[i]$ son de la forma siguiente:

(i) $\pm p$, $\pm pi$, si p primo en $\mathbf{Z}$, con $p \equiv 3(4)$

(ii) $a + bi$ con norma $|a + bi|$ irreducible en $\mathbf{Z}$

La demostración se sigue de los siguientes resultados:

(i) $2 \neq p \in \mathbf{Z}$ primo en $\mathbf{Z}$ es irreducible en $\mathbf{Z}[i] \Leftrightarrow$
$p \neq a^2 + b^2 = (a + ib)(a - ib) \Leftrightarrow p \equiv 3(4)$

(ii) Pequeño teorema de Fermat:
sea $p \in \mathbf{Z}$ primo, y $b \in \mathbf{Z}$ y p no divide a b, $\Rightarrow b^p \equiv b(p)$.

Chapter 2

Grupos

2.1 Primeras nociones

Definición 23 *Llamaremos grupo a un conjunto G con una operación*
$(\cdot$ producto),(denotaremos $a \cdot b = ab)$
$\cdot : G \times G \to G$ verificando las propiedades:
(i) Asociativa : $\forall\ a, b, c \in A$, $a(bc) = (ab)c$
(ii) Elemento neutro: existe $1 \in G$ y $\forall\ a \in G$, $a \cdot 1 = a \cdot 1 = a$
(iii) Elemento inverso: $\forall\ a \in G$, existe $a^{-1} \in G$ y $aa^{-1} = a^{-1}a = 1$

Nota El grupo G es conmutativo o abeliano, si $\forall\ a, b \in G$, $ab = ba$ y en dicho caso denotaremos la operación por la suma $+$ y el elemento neutro por 0.

EJEMPLOS:

- Son grupos abelianos, los de los números $(\mathbf{Z}, +)$, $(\mathbf{Z}_n, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q} \setminus \{0\}, \cdot)$, $(\mathbf{R} \setminus \{0\}, \cdot)$, $(\mathbf{C}\setminus\{0\}, \cdot)$

- Matrices cuadradas $M_n(\mathbf{R})$, $M_n(\mathbf{C})$, con determinante distinto de cero con el producto de matrices, con elemento neutro la matriz unidad, es grupo no conmutativo.

- Grupo de las permutaciones, no conmutativo

Sea X un conjunto (finito o no) consideramos

$S_X \equiv \{\varphi : X \to X | \varphi \text{ biyección}\}$

S_X con la composición de aplicaciones $\gamma \circ \varphi \equiv \gamma\varphi$, es un grupo y denotaremos por $I \equiv$ *identidad* y el producto de permutaciones lo consideraremos de

derecha a izquierda.
$S_X \equiv$ *Grupo Simétrico* o *Grupo de las permutaciones* de X

Consideremos $X = \{1, 2, \ldots, n\}$ tenemos S_n el grupo de las permutaciones de n elementos y $|S_n| = n!$.

Denotamos $\gamma \in S_n$

$$\gamma \equiv \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \ , \ \gamma(i) = a_i, \ \ a_i \in \{1, 2, \ldots, n\}$$

- Grupo diédrico del cuadrado D_4 formado por las transformaciones del plano que dejan fijo un cuadrado, simetría, τ, y rotación de $\pi/2$, σ.

$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, con $\sigma^4 = 1$, $\tau^2 = 1$, y $\tau\sigma\tau\sigma = 1$.

D_4 no es abeliano, ya que $\sigma\tau = \tau\sigma^3 \neq \tau\sigma$.

Notas (i) El elemento neutro de un grupo es único.

(ii) El inverso de todo elemento es único

(iii) $\forall\ a \in G\ (a^{-1})^{-1} = a$

(iv) $\forall\ a, b \in G\ (ab)^{-1}) = b^{-1}a^{-1}$

(v) Propiedades cancelativas si $ac = bc \Rightarrow a = b$, y también si $ca = cb \Rightarrow a = b$.

Podemos considerar la potencia, $a \in G$, $n \in \mathbf{N}$, definimos $a^n = a \cdot \overset{(n}{\cdots} \cdot a$, y suponemos $a^0 = 1$, $\forall\ n \in \mathbf{Z}$, $a^{-n} = (a^{-1})^n$ y tenemos:

(i) $a^n a^m = a^{n+m}$, $\forall\ n, m \in \mathbf{Z}$,.

(ii) $(a^n)^m = a^{nm}$, $\forall\ n, m \in \mathbf{Z}$,.

(iii) En general $(ab)^n \neq a^n b^n$, $\forall\ n \in \mathbf{Z}$, se da la igualdad si $ab = ba$.

Definición 24 *Diremos que un grupo G es finito si su número de elementos es finito. A dicho número de elementos le llamaremos orden del grupo, y lo denotamos por $|G|$.*

EJEMPLOS:

- $(\mathbf{Z}_n, +)$, S_n son grupos finitos.

Definición 25 *Diremos que $H \subset G$ es subgrupo de G si es un grupo con la operación de G, denotaremos $H < G$.*

Es decir

$$H \subset G \text{ es subgrupo} \Leftrightarrow \left\{ \begin{array}{l} \forall\, h,k \in H \Rightarrow hk \in H \\ 1 \in H \\ \forall\, h \in H, h^{-1} \in H \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} \forall\, h,k \in H \\ hk^{-1} \in H \end{array} \right.$$

Si H es subgrupo de G y $1 \neq H \neq G$ diremos que H es subgrupo propio.

- Intersección de subrupos $H \cap K$ es subgrupo.

$\bigcap_{i\in\Gamma} H_i$ (cualquier conjunto de indices Γ) es subgrupo.

Notas (i) La unión de subgrupos no es subgrupo en general: en $\mathbf{Z}$, $(3)\mathbf{Z} \cup (4)\mathbf{Z}$ no es un subgrupo.

(ii) El producto de subgrupos definido $HK = \{hk | h \in H, k \in K\}$ no es subgrupo en general, daremos condiciones para que lo sea mas adelante.

En D_4, $\{1, \tau\sigma\}\{1, \tau\} = \{1, \tau\sigma, \tau, \tau\sigma\tau\}$, no es grupo ya que $\tau\tau\sigma = \sigma$ no pertenece al conjunto.

$H \subset G$ finito, es subgrupo $\Leftrightarrow \forall\, h,k \in H \Rightarrow hk \in H$

Subgrupo generado por un subconjunto

Sea $S \subset G$ subconjunto, el *subgrupo generado* por S en G es:

$$< S >= \bigcap_{H_i \supset S} H_i,\ H_i \textit{ subgrupo de } G$$

Es decir $< S >$ es el menor subgrupo de G que contiene a S.

Si $< S >= G$ diremos que S es el conjunto de generadores de G.

Un grupo G es finitamente generado si $< S >= G$ y S es finito , es decir $G =< a_1, \ldots, a_n >$ (el grupo no tiene por que ser finito).

Proposición 24 *Si $S \subset G$ es un conjunto no vacio, entonces*

$$< S >= \{a_1^{n_1} \cdots a_s^{n_s} | s, \in \boldsymbol{Z}, a_i \in S, 1 \leq i \leq s\}$$

.

Definición 26 *Diremos que un subgrupo $H \subset G$ es cíclico si* $H =< a >= \{a^n | n \in \boldsymbol{Z}\}$.

EJEMPLOS:

- $(\mathbf{Z}, +)$ es cíclico, $\mathbf{Z} =< 1 >$.

- $(\mathbf{Z}_n, +)$ es cíclico, $\mathbf{Z}_n =< \overline{1} >$.

- Las raices complejas de la unidad $U_n = \{\alpha \in \mathbf{C} | \alpha^n = 1\}$ es un grupo cíclico con el producto.

Proposición 25 *Todo grupo cíclico $< a >$ es abeliano.*

DEMOSTRACIÓN.

Dados $a^n, a^m \in < a >$, $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.

Proposición 26 *Todo subgrupo de un grupo cíclico $< a >$ es cíclico.*

DEMOSTRACIÓN.

$H \subset < a >$, subgrupo es $H =< a^m >$.

Definición 27 *Definimos orden de $a \in G$ como $o(a) = | < a > |$, es decir el mínimo $n \in \boldsymbol{N}$ con $a^n = 1$.*

Propiedades del orden de un elemento

(i) $o(a) = 1 \Leftrightarrow a = 1$.

(ii) $o(a) = o(a^{-1})$.

(iii) $o(bab^{-1}) = o(a)$.

(iv) $o(ab) = o(ba)$.

(v) $o(a) = \infty \Leftrightarrow \forall\, m, n \in \mathbf{Z}$, $m \neq n$, se tiene $a^m \neq a^n$.

(vi) $o(a) < \infty \Leftrightarrow \exists\, m, n \in \mathbf{Z}$, $m \neq n$, con $a^m = a^n \Leftrightarrow$
$\exists\, 0 \neq k \in \mathbf{Z}$, tal que $a^k = 1$.

(vii) Si $o(a) = r$, $a^k = 1 \Leftrightarrow k$ es múltiplo de r.

(viii) Si $o(a) = r$, $o(b) = s$, y $ab = ba \Rightarrow o(ab)|mcm(r, s)$.

(ix) Si $o(a) = r$, $o(b) = s$, $mcd(r, s) = 1$, y $ab = ba \Rightarrow o(ab) = rs$.

(x) Si $o(a) = r$, entonces

$$o(a^k) = \frac{r}{mcd(r, k)},$$

en particular si $d|r$, se tiene $o(a^d) = r/d$.

Dejamos la demostración para el lector.

Definición 28 *Llamaremos centro de* G *a* $C(G) = \{g \in G | xg = gx, \forall\ x \in G\}$

$C(G)$ es un subrupo abeliano de G. En cierto sentido es el mas grande subgrupo abeliano de G.

$$G \text{ es abeliano} \Leftrightarrow C(G) = G$$

2.2 Congruencias módulo un subgrupo

Sea $H < G$. En G definimos las relaciones módulo H: dados $a, b \in G$

- $a \sim_H b$ si $a^{-1}b \in H$ (por la derecha)

- $a_H \sim b$ si $ab^{-1} \in H$ (por la izquierda)

Proposición 27 *Las relaciones* $a \sim_H b$, $a_H \sim b$ *son de equivalencia.*

Las clases de equivalencia por las relaciones son:

$[a] \sim_H = \{ah | h \in H\} = aH$, $[a]_H \sim = \{ha | h \in H\} = Ha$,

y los conjuntos cocientes

$$\frac{G}{\sim_H} = \{aH | a \in G\}, \quad \frac{G}{_H \sim} = \{Ha | a \in G\}$$

Dadas dos clases aH, bH, $aH = bH \Leftrightarrow b^{-1}a \in H$ o $a^{-1}b \in H$

Proposición 28 *Si $H < G$ se verifica:*

(i) $card(aH) = |H| = card(Ha)\ \forall\ a \in G$

(ii) $card(\frac{G}{\sim_H}) = card(\frac{G}{H\sim})$.

DEMOSTRACIÓN.

(i) Sea $\varphi : H \to aH$ definida por $\varphi(h) = ah$, es una biyección, $\Rightarrow$

$card(aH) = |H|$, (analogamente $|H| = card(Ha)$.

(ii) Se deduce de (i).

Llamaremos *índice* de G en H, denotado por $[G : H]$ a $card(\frac{G}{\sim_H})$

Teorema 18 *Teorema de Lagrange Si $H < G$, entonces*

G es finito $\Leftrightarrow$ H y $[G : H]$ son finitos,

y en dicho caso $|G| = [G : H]|H|$,

en particular si G es finito $|H|$ divide a $|G|$.

DEMOSTRACIÓN.

$\Rightarrow$) evidente.

$\Leftarrow$) $G = \bigcup_{i=1}^{r} a_i H$ (union disjunta de clases) siendo $[G : H] = r$, como cada clase tiene $|H| = s$ elementos $\Rightarrow |G| = [G : H]|H| = rs$ finito.

Nota El teorema anterior no asegura la existencia para cada divisor del orden de G de un sugrupo con dicho orden.

Teorema 19 *Pequeño teorema de Fermat. Sea $p \in \boldsymbol{Z}$ primo se verifica que $\forall a \in \boldsymbol{Z}\ a^p \equiv a(p)$.*

DEMOSTRACIÓN.

$\mathbf{Z}_p \backslash \{0\}$ tiene $p - 1$ elementos y es un grupo respecto del producto

$\Rightarrow$) $\forall a \in \mathbf{Z}$, $| < \overline{a} > | \mid p - 1 \Rightarrow \overline{a}^{p-1} = \overline{1} \Rightarrow \overline{a}^p = \overline{a} \Rightarrow a^p \equiv a(p)$

Corolario 15 *G grupo, $H, K < G$ finitos con $mcd(|H|, |K|) = 1 \Rightarrow$*

$H \cap K = \{1\}$.

Corolario 16 *teorema de los índices. Dados dos subgrupos H, K de G con $K \subset H \subset G$, se verifica:*

$[G : K]$ *es finito* $\Leftrightarrow$ $[G : H]$ *y* $[H : K]$ *son finitos,*

y en dicho caso $[G : K] = [G : H][H : K]$,

DEMOSTRACIÓN.

($\Rightarrow$) Supongamos $[G : K] < \infty$, como $xK \subseteq xH \Rightarrow [G : H] < \infty$

y como $\{xK | x \in H\} \subseteq \{xK | x \in G\} \Rightarrow [H : K] \leq [G : K] < \infty$

($\Leftarrow$) Supongamos $[G : H] = r$, $[H : K] = s$ finitos $\Rightarrow$ existen $g_1, \ldots, g_r \in G$, $h_1, \ldots, h_s \in H$

y $G = \bigsqcup_{i=1}^{r} g_i H$, $H = \bigsqcup_{j=1}^{s} h_j K$, (uniones disjuntas) $\Rightarrow$

$G = \bigsqcup_{i,j} g_i h_j K$ $r.s$ clases ($g_i H = \bigsqcup g_i(h_j K)$, y $g_i(h_j K) = g_i h_j K$) $\Rightarrow$

$[G : K] = [G : H][H : K] = rs$ que es finito.

Nota

Si G es finito el resultado anterior se deduce del teorema de Lagrange, ya que:

$| G | = [G : H] | H | = [G : H][H : K] | K |$ y

$| G | = [G : K] | K |$

Subgrupos normales

Los cocientes $\frac{G}{\sim_H}$, $\frac{G}{H\sim}$ no son en general grupos con la operación heredada de G. Para que lo sea es necesario considerar un subgrupo especial, subgrupo normal.

Definición 29 *Diremos que $K < G$ es normal en G si $\forall\, a \in G$, $aK = Ka$. Denotaremos $K \lhd G$.*

Nota (i) Si G es abeliano todo subgrupo es normal

(ii) La condición $aK = Ka$ no quiere decir que dado $k \in K$ $ak = ka$, sino que existe $k' \in K$ y $ak = k'a$.

Son equivalentes con K normal:

- $aKa^{-1} = K$, $\forall\ a \in G$.

- $aKa^{-1} \subseteq K\ \forall\ a \in G$.

- $aka^{-1} \in K\ \forall\ a \in G,\ k \in K$.

La demostración se deja para el lector.

EJEMPLO:

$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$, $H = \{1, \tau\}$ no es normal en D_4,

ya que $\sigma H = \sigma\{1, \tau\} = \{\sigma, \sigma\tau\}$ y $H\sigma = \{1, \tau\}\sigma = \{\sigma, \tau\sigma\}$,

y como $\sigma\tau\sigma\tau = 1$, $\sigma^4 = 1$, y $\tau^2 = 1 \Rightarrow \tau\sigma = \sigma^3\tau \neq \sigma\tau \Rightarrow$

$\sigma H \neq H\sigma$.

$< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\}$ es normal en D_4, ya que $D_4 =< \sigma, \tau >$, y $\tau\sigma\tau = \sigma^3 \in < \sigma >$.

Proposición 29 *(i) Si* $G =< a_1, \ldots, a_n >$ *es finitamente generado, entonces*

$K \lhd G \Leftrightarrow a_i k a_i^{-1} \in K$, *o* $a_i^{-1} k a_i \in K$, $\forall\ i$, *y* $\forall\ k \in K$.

(ii) Si $K =< k_1, \ldots, k_n >$ *es finitamente generado, entonces*

$K \lhd G \Leftrightarrow a k_i a^{-1} \in K$, $\forall\ i$, *y* $\forall\ a \in G$.

DEMOSTRACIÓN.

(i) Sea $a = a_{i_1} a_{i_2} \cdots a_{i_s} \Rightarrow aka^{-1} = (a_{i_1} a_{i_2} \cdots a_{i_s}) k (a_{i_1} a_{i_2} \cdots a_{i_s})^{-1} =$

$a_{i_1} a_{i_2} \cdots a_{i_s} k a_{i_s}^{-1} \cdots a_{i_2}^{-1} a_{i_1}^{-1} = (a_{i_1}(a_{i_2}(\cdots(a_{i_s} k a_{i_s}^{-1})\cdots)a_{i_2}^{-1})a_{i_1}^{-1}) \Rightarrow$

$(a_{i_s} k a_{i_s}^{-1}) \in K \Rightarrow \cdots \Rightarrow (a_{i_2}(\cdots(a_{i_s} k a_{i_s}^{-1})\cdots)a_{i_2}^{-1}) \in K \Rightarrow$

$(a_{i_1}(a_{i_2}(\cdots(a_{i_s} k a_{i_s}^{-1})\cdots)a_{i_2}^{-1})a_{i_1}^{-1}) \in K$.

(ii) Analogamente a (i).

Llamaremos grupo *simple* si no tiene subgrupos normales propios distintos del $\{1\}$.

Proposición 30 *Sea H, K subgrupos de G. Entonces*

$HK < G \Leftrightarrow HK = KH$.

DEMOSTRACIÓN. (se deja al lector)

Corolario 17 *Si H es subgrupo de G, de indice $[G : H] = 2$, entonces K es normal en G.*

DEMOSTRACIÓN.

Si $[G : H] = 2$, los cocientes $\frac{G}{\sim_H} = \{H, aH\}$, $\frac{G}{H\sim} = \{H, Ha\}$, verifican $G = H \cup aH = H \cup Ha$, uniones disjuntas, $\Rightarrow aH = Ha \Rightarrow H$ es normal.

Corolario 18 *Si $K \lhd G$, $H < G \Rightarrow HK < G$, y $KH < G$.*

Proposición 31 *Sea $H \lhd G$, $K \lhd G \Rightarrow HK \lhd G$, $KH \lhd G$.*

Grupo cociente

Analogamente con el caso conmutativo consideramos el grupo cociente por un subgrupo normal.

Teorema 20 *Sea G grupo y K subgrupo normal de G, entonces el cociente $G/\sim_H = G/_H \sim$ es un grupo con la operación $(aK)(bK) = (ab)K$, $\forall\ a, b \in G$. El grupo se denota por G/K y se llama grupo cociente módulo K.*

DEMOSTRACIÓN.

Como la operación está definida por los representantes de las clases, veamos que está bien definida,

sea $aK = a'K$, $bK = b'K \Leftrightarrow a'a^{-1} = k_1 \in K$, $b'b^{-1} = k_2 \in K \Leftrightarrow$

$a' = k_1 a$, $b' = k_2 b \Rightarrow a'b' = k_1 a k_2 b \Rightarrow$ (K normal)

dado ak_2, existe k_3 y $ak_2 = k_3 a \Rightarrow a'b' = k_1 k_3 ab \Rightarrow$

$a'b'(ab)^{-1} \in K \Rightarrow a'b'K = abK$.

Nota El elemento neutro del cociente es la clase del 1, $1K = K$, y el inverso de aK es $a^{-1}K$.

EJEMPLO:

Sean $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$, y $< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\} \lhd D_4$,

$D_4/ < \sigma >= \{< \sigma >, < \sigma > \tau\} = \{\{1, \sigma, \sigma^2, \sigma^3\}, \{\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}\}$,

es un grupo con dos elementos el neutro y otro de orden 2, es el mismo que $\mathbf{Z}_2$.

Nota (i) Si G es abeliano cualquier cociente es abeliano y lo contario no es cierto como puede verse con el ejemplo anterior, $D_4/ < \sigma >$ es abeliano por tener solo dos elementos, y D_4 no lo es.

(ii) Si $G =< a >$ es cíclico el cociente $G/K =< aK >$ es cíclico, pero el reciproco no es cierto como prueba el ejemplo anterior $D_4/ < \sigma >$ es cíclico por tener solo dos elementos, y D_4 no lo es.

(iii) Si G es finito, cualquier cociente es finito, el reciproco no es cierto, $\mathbf{Z}/ < n >= \mathbf{Z}_n$ es finito, de orden n y $\mathbf{Z}$ no lo es.

2.3 Teoremas de isomorfía

Definición 30 *Dados G, G' grupos, una aplicación $f : G \to G'$ es homomorfismo de grupos si $\forall\, a_1, a_2 \in G$ se tiene:*
$f(a_1 a_2) = f(a_1) f(a_2)$

Si $f : G \to G'$ es homomorfismo de grupos se verifica:
$f(1) = 1$
$f(a^{-1}) = (f(a))^{-1}$

De lo anterior se deduce trivialmente que la composición de homomorfismos es homomorfismo.

EJEMPLOS:

- La inclusión $H \subset G$ es un homomorfismo de grupos.

- $f : \mathbf{Z} \to \mathbf{Z}_n$ dado por $f(a) = \overline{k}$ si $\exists\ \lambda \in \mathbf{Z}$ con $a - \lambda n = k$, es homomorfismo.

Definición 31 *Dado $f : G \to G'$ homomorfismo de grupos definimos:*
Imagen de f, $im(f) = \{a' \in G' : \exists a \in G, \text{ y } f(a) = a'\}$
Núcleo de f, $ker(f) = \{a \in G : f(a) = 1\}$.

Nota El núcleo $ker(f)$ es un subgrupo normal de G, ya que

si $x \in ker(f)$, $\forall\, a \in G$, $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a) \cdot 1 \cdot (a^{-1}) =$

$f(a)(f(a))^{-1} = 1 \Rightarrow axa^{-1} \in ker(f)$.

EJEMPLOS:

Dado $f : \mathbf{Z} \to \mathbf{Z}_n$ como antes, $im(f) = \mathbf{Z}_n$, y $ker(f) = n\mathbf{Z}$.

Sea $f : G \to G'$ homomorfismo de grupos

- f es *monomorfismo* si es homomorfismo inyectivo

- f es *epimorfismo* si es homomorfismo suprayectivo

- f es *isomorfismo* si es homomorfismo biyectivo

EJEMPLOS:

- El *homomorfismo de inclusión* $i : H \hookrightarrow G$ para $H \subset G$ es inyectivo

- El *homomorfismo de proyección* para $K \lhd G$ subgrupo normal, sea $p : G \to G/K$, $f(a) = aK$ es suprayectivo.

Proposición 32 *$f : G \to G'$ homomorfismo de grupos,*
es inyectivo $\Leftrightarrow$ $ker(f) = \{1\}$

DEMOSTRACIÓN.

$\Rightarrow$) Sea $a \in ker(f) \Rightarrow f(a) = 1 = f(1) \Rightarrow$ (por ser f inyectiva) $a = 1$

$\Leftarrow$) Sea $f(a) = f(b) \Rightarrow 1 = f(a)(f(b))^{-1} = f(ab^{-1}) \Rightarrow$

$ab^{-1} \in ker(f) = \{1\} \Rightarrow ab^{-1} = 1 \Rightarrow a = b$

Nota. Lo anterior implica que todo homomorfismo $f : G \to G'$ con $f(G) \neq \{1\}$, y G grupo simple es inyectivo.

- Dos grupos G, G' son *isomorfos* ($G \approx G'$) si existe un isomorfismo f entre ellos y en dicho caso $f^{-1} : G' \to G$ es también isomorfismo.

Teoremas de isomorfía

Teorema 21 1^{er} *teorema de isomorfía: Sea* $f : G \to G'$ *homomorfismo de grupos. Entonces existe un único isomorfismo* $\overline{f} : G/ker(f) \to im(f)$*, tal que el diagrama siguiente*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/ker(f) & \overset{\overline{f}}{\approx} & (im(f) \end{array}$$

es conmutativo, i.e. $f = i \circ \overline{f} \circ p$

DEMOSTRACIÓN.

Definimos $\overline{f} : G/ker(f) \to im(f)$ como $\overline{f}(a(ker(f)) = f(a)$.

$\overline{f}$ es homomorfismo inyectivo ya que si $1 = \overline{f}(a(ker(f))) = f(a)$

$\Rightarrow a \in ker(f) \Rightarrow a(ker(f)) = 1(ker(f))$

$\overline{f}$ es suprayectivo ya que $im(\overline{f}) = im(f)$.

$\overline{f}$ es único, ya que si existe otro f^* verificando lo mismo que $\overline{f}$, $\forall\ a \in G$ $f^*(a(ker(f))) = f(a) = \overline{f}(a(ker(f)))$.

Por último $\forall\ a \in G$, $(i \circ \overline{f} \circ p)(a) = (i \circ \overline{f})(a(ker(f))) = (i \circ f)(a) = f(a)$.

Nota El teorema anterior nos muestra que los homomorfismos de G en cualquier grupo dependen de los posibles subgrupos normales de G.

EJEMPLO:

El homomorfismo $f : \mathbf{Z} \to \mathbf{Z}_n$, $f(a) = \overline{k}$, con $k < n$, y $a - k = \lambda n$ verifica que $ker(f) = (n)$ y $f : \mathbf{Z}/ker(f) \approx \mathbf{Z}_n$.

Teorema 22 *Teorema de la correspondencia: Sea* $K \lhd G$ *(subgrupo normal). Entonces existe una biyección* φ

$\Gamma = \{H < G,\ H \supset K\} \overset{\varphi}{\leftrightarrow} \Upsilon = \{\overline{H} < G/K\ \}$

y además si $H \supset K$*,* H *es normal* $\Leftrightarrow$ H/K *es normal*

DEMOSTRACIÓN.

Definimos para $K \subset H \subset G$ subgrupo, $\varphi(H) = H/K$ que se comprueba facilmente que es subgrupo de G/K

φ es inyectiva ya que si $H/K = H'/K \Rightarrow \forall\ b \in H,\ \exists\ b' \in H'$ con $bK = b'K$

$\Rightarrow b^{-1}b' = h \in K \Rightarrow b' = bh \in H \Rightarrow H' \subset H$ (análogo $H \subset H'$)

Sea $H \lhd G$, $aKhKa^{-1}K = aha^{-1}K \Rightarrow$ como $aha^{-1} = h' \in H$,

$aKhKa^{-1}K \in H/K$

(similar en sentido contrario)

Teorema 23 *2^o teorema de isomorfía: Sea K, H subgrupos normales de G con $K \lhd H$. Entonces H/K es subgrupo normal de G/K y*

$$\frac{G/K}{H/K} \approx \frac{G}{H}$$

DEMOSTRACIÓN.

Definimos $f : G/K \to G/H\ \forall\ a \in G,\ f(aK) = aH$ que es trivialmente homomorfismo suprayectivo.

f esta bien definido ya que si $aK = a'K \Rightarrow a(a')^{-1} \in K \subset H \Rightarrow aH = a'H$.

y como el núcleo $ker(f) = \{bK : bH = 1H\} = \{bK : b \in H\} = H/K, \Rightarrow$ H/K es subgrupo normal de G/K, (por el 1^{er} teorema de isomorfía) $\Rightarrow$

$$\frac{G/K}{H/K} \approx \frac{G}{H}$$

Teorema 24 *3^{er} teorema de isomorfía: Sea $H < G$, $K \lhd G$. Entonces $K \lhd HK$ (subgrupo de G), $H \cap K \lhd H$, y*

$$\frac{H}{H \cap K} \approx \frac{HK}{K}$$

DEMOSTRACIÓN.

Se comprueba facilmente que $K \lhd HK$ (subgrupo de G) y $H \cap K \lhd H$

definimos el homomorfismo $f : H \to G/K$ por $\forall\ h \in H\ f(h) = hK$

($K \not\subseteq H$ en general) $\Rightarrow$ la imagen $im(f) = (HK)/K$

el núcleo $ker(f) = \{h \in H : hK = 1K\} = \{h \in H : h \in K\} = H \cap K$
(por el 1^{er} teorema de isomorfía) $\Rightarrow$

$$\frac{H}{H \cap K} \approx \frac{HK}{K}$$

Grupos cíclicos

Sea $G =< a >= \{a^n | n \in \mathbf{Z}\}$ cíclico. Vamos a ver que hay dos tipos de grupos cíclicos, Consideramos el homomorfismo

$\varphi : \mathbf{Z} \to G$, $\varphi(n) = a^n$, suprayectivo $\Rightarrow$ (primer teorema de isomorfía)

$\mathbf{Z}/ker(\varphi) \approx G$, y tenemos dos casos:

(i) $ker(\varphi) = \{0\}$, es decir $a^n \neq 1$, $\forall\, n \in \mathbf{Z}$, y $G \approx \mathbf{Z}$,

$G =< a >= \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ grupo cílico infinito.

(ii) $ker(\varphi) = n\mathbf{Z} \neq \{0\}$, es decir $\exists\, n \in \mathbf{Z}$, con $a^n = 1$, y $G \approx \mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$,

con n mínimo tal que $a^n = 1$, es decir $o(a) = n$,

$G =< a >= \{1, a, a^2, \ldots, a^{n-1}\}$, grupo cíclico finito..

2.4 Grupo Simétrico

Sea X un conjunto (finito o no) consideramos

$S_X \equiv \{\varphi : X \to X | \varphi \; biyeccion\}$
S_X con la composición de aplicaciones $\gamma \circ \varphi \equiv \gamma\varphi$, es un grupo y denotaremos por $I \equiv$ *identidad* y el producto de permutaciones lo consideraremos de derecha a izquierda.
$S_X \equiv$ *Grupo Simétrico* o *Grupo de las permutaciones* de X

Consideremos $X = \{1, 2, \ldots, n\}$ tenemos S_n el grupo de las permutaciones de n elementos y $|S_n| = n!$.

A lo largo de esta sección estudiaremos el grupo simétrico S_n

Denotamos $\gamma \in S_n$

$$\gamma \equiv \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \;,\; \gamma(i) = a_i, \;\; a_i \in \{1, 2, \ldots, n\}$$

Definición 32 *Llamaremos ciclos a las permutaciones* $\sigma \equiv (k_1, k_2, \ldots, k_r)$, $k_i \in \{1, 2, \ldots, n\}, r \leq n$, *donde* $\sigma(k_i) = k_{i+1}$, $\sigma(k_r) = k_1$, *y* $\sigma(j) = j$, $\forall j \in \{1, 2, \ldots, n\}$, $j \notin \{k_1, k_2, \ldots, k_r\}$

Tenemos $(k_1, k_2, \ldots, k_r) = (k_r, k_1, \ldots, k_{r-1}) = \cdots = (k_2, k_3, \ldots, k_1)$,

el orden del ciclo $\sigma \equiv (k_1, k_2, \ldots, k_r)$ es r y $\sigma^{-1} = (k_r, k_{r-1}, \ldots, k_1)$

Llamaremos *trasposición* a un ciclo de orden 2, (k_1, k_2), y se tiene $(k_1, k_2)^{-1} = (k_1, k_2)$

Diremos que dos ciclos $(k_1, k_2, \ldots, k_r)$, $(q_1, q_2, \ldots, q_s)$ son disjuntos si $\{k_1, k_2, \ldots, k_r\} \cap \{q_1, q_2, \ldots, q_s\} = \emptyset$

Nota Dos ciclos disjuntos conmutan entre sí y el orden del producto de dos ciclos disjuntos es el mínimo común múltiplo de los ordenes de los ciclos.

EJERCICIOS

(i) Para toda $\gamma \in S_n$, $\gamma(k_1, k_2, \ldots, k_r)\gamma^{-1} = (\gamma(k_1), \gamma(k_2), \ldots, \gamma(k_r))$.

(ii) $(i, j) = (1, i)(1, j)(1, i)$.

(iii) $(1, i, j) = (1, 2, j)^2(1, 2, i)(1, 2, j)$, para todo $j > 2$.

A continuación vamos a ver que las permutaciones son composición de ciclos disjuntos como se ve con el siguiente ejemplo

Ejemplo 1 *En* S_9 *tenemos descomposición*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 1 & 9 & 6 & 8 & 2 & 5 \end{pmatrix} = (134)(278)(59)$$

Teorema 25 *Toda permutación es composición de ciclos disjuntos, univocamente determinados salvo el orden en la composición.*

DEMOSTRACIÓN.

Sea $\gamma \in S_n$. Fijado $i \in \{1, 2, \ldots, n\}$ consideramos el primer ciclo de la composición:

$\sigma_1 \equiv (\gamma(i), \gamma^2(i), \ldots, \gamma^r(i) = i)$, $r < n$, (si $r = n$ hemos terminado)

Consideremos $j \in \{1, 2, \ldots, n\} \setminus \{\gamma(i), \gamma^2(i), \ldots, \gamma^r(i) = i\}$, y el segundo ciclo de la descomposición es

$\sigma_2 \equiv (\gamma(j), \gamma^2(j), \ldots, \gamma^s(j) = j)$

Continuando de manera similar, como n es finito obtendremos

$\gamma = \sigma_k \cdots \sigma_2 \sigma_1$

Los ciclos anteriores son disjuntos, ya que si $\gamma^m(i) = \gamma^h(j)$ con $h \leq m$, $\gamma^{m-h}(i) = j$, y entonces $j \in \{\gamma(i), \gamma^2(i), \ldots, \gamma^r(i) = i\}$ que no es posible.

Por el procedimiento anterior $\forall m \in \{1, 2, \ldots, n\}$ si $\gamma(m) = m'$, el ciclo $(\ldots, m, m', \ldots)$ pertenece a la descomposición y esta univocamente determinado por γ y m. Por tanto solo puede variar el orden de las σ_j en la descomposición.

Dado que $(k_1, k_2, \ldots, k_r) = (k_1, k_r)(k_1, k_{r-1}) \cdots (k_1, k_3)(k_1, k_2)$ tenemos

Corolario 19 *Toda permutación es composición de trasposiciones.*

En la anterior composición ni el número ni las trasposiciones son únicas. Por ejemplo

$(i, j) = (1, i)(1, j)(1, i)$.

Otra descomposición de un ciclo en producto de trasposiciones sería

$(k_1, k_2, \ldots, k_r) = (k_1, k_2)(k_2, k_3) \cdots (k_{r-1}, k_r)$

Por lo anterior el número de trasposiciones en la descomposión de una permutación no es único, pero si lo es su paridad, es decir, el hecho de que este número sea par o impar.

Llamaremos *paridad* de un producto de trasposiciones a el caracter *par o impar* de su número.

Teorema 26 *La paridad de cualquier descomposición de una permutación $\gamma \in S_n$ en producto de trasposiciones es siempre la misma*

DEMOSTRACIÓN.

Dado que el ciclo $\sigma \equiv (k_1, k_2, \ldots, k_r) = (k_1, k_r)(k_1, k_{r-1}) \cdots (k_1, k_3)(k_1, k_2)$, definimos $N(\sigma) = r - 1$ (número de trasposiciones en la anterior descomposición)

Si una permutacion $\gamma \in S_n$ es $\gamma = \sigma_k \cdots \sigma_2 \sigma_1$, definimos
$N(\gamma) = N(\sigma_k) + \cdots + N(\sigma_2) + N(\sigma_1) = (r_k - 1) + \cdots + (r_2 - 1) + (r_1 - 1)$, si $o(\sigma_i) = r_i$
(notese que $N(I) = 0$).

Sea $\gamma = \alpha_1 \alpha_2 \cdots \alpha_m$ una descomposición en producto de trasposiciones, entonces

$N(\gamma \alpha_m \cdots \alpha_2 \alpha_1) = N(I) = 0$
Veamos cuanto es $N(\gamma\alpha)$ donde α es una trasposición.
Se verifican las siguientes descomposiciones:

(1) $(a, c_1, \ldots, c_h, b, d_1, \ldots, d_k)(a, b) = (b, c_1, \ldots, c_h)(a, d_1, \ldots, d_k)$
(2) $(a, c_1, \ldots, c_h)(b, d_1, \ldots, d_k)(a, b) = (a, d_1, \ldots, d_k, b, c_1, \ldots, c_h)$

Y por tanto si $\alpha = (a, b)$,
$N(\gamma\alpha) = N(\gamma) - 1$, si a, b están en un mismo ciclo de γ (fórmula (1))
$N(\gamma\alpha) = N(\gamma) + 1$, si a, b están en distintos ciclos de γ (fórmula (2))
$N(\gamma\alpha) = N(\gamma) + 1$, si a, b no están en algún ciclo de γ.

Por tanto si s de las trasposiciones están en el mismo ciclo tenemos
$N(\gamma \alpha_m \cdots \alpha_2 \alpha_1) = N(\gamma) + s(-1) + (m - s)(+1) =$, luego $N(\gamma) + m = 2s$ par, y por tanto $N(\gamma)$ y m tienen la misma paridad.
□

Con el teorema anterior podemos dar la siguiente

Definición 33 *La paridad de una permutación $\gamma \in S_n$ es el caracter par o impar de cualquier descomposición de γ en producto de trasposiciones.*

Nota. El conjunto de todas Las permutaciones pares A_n forman un subgrupo de S_n, dado que el producto de dos permutaciones pares es par (suma de pares) y que la identidad $I = (a, b)(a, b)$ es tambien par (las impares no lo forman).

Veamos que el número de elementos de A_n es la mitad que el número de elementos de S_n.

Definimos $\varepsilon : S_n \to \{1, -1\} \approx \mathbf{Z}_2$, por $\varepsilon(\gamma) = 1$ si la permutacón es par y $\varepsilon(\gamma) = -1$ si la permutación es impar.
Por lo anterior $\varepsilon(\gamma) = (-1)^m$ si γ es producto de m trasposiciones. Por tanto

$\varepsilon(\gamma\gamma') = \varepsilon(\gamma)\varepsilon(\gamma')$

Por ejemplo un ciclo σ de orden r es $\varepsilon(\sigma) = (-1)^{r-1}$, es decir σ es par si su orden es impar y viceversa.

Definición 34 *Llamaremos grupo alternado A_n al conjunto de todas las permutaciones pares de S_n.*

Corolario 20 *El grupo alternado A_n es un subgrupo normal de S_n y su orden es $\mid A_n \mid = (1/2) \mid S_n \mid$.*

DEMOSTRACIÓN.

$\varepsilon : S_n \to \{1, -1\} \approx \mathbf{Z}_2$ es un homomorfismo suprayectivo. El núcleo de ε es A_n, y por lo tanto $A_n \lhd S_n$. Por el primer teorema de isomorfia
$S_n/ker(\varepsilon) \approx \mathbf{Z}_2$, y por el teorema de Lagrange

$$\mid S_n \mid / \mid A_n \mid \simeq \mid \mathbf{Z}_2 \mid = 2$$

□

A_4 no es simple, ya que $\{I, (12)(34), (13)(24), (14)(23)\} \lhd A_4$.
En los demas casos no existen subgrupos normales de A_n

Teorema 27 *(Lema de Abel) A_n es simple para todo $n \geq 5$.*

(demostración no elemental)

Teorema 28 *(Teorema de Cayley)*
G finito de orden $n \Rightarrow G$ es isomorfo a un subgrupo de S_n.

DEMOSTRACIÓN.

Sea $\varphi : G \to S_G \approx S_n$ dado por $\varphi(g) : G \to G$ definida por $\varphi(g)(x) = gx$, donde $\varphi(g)$ es biyección, φ es monomorfismo, y por tanto su imagen es isomorfa a un subgrupo de S_n.

2.5 Algunos grupos finitos

En esta sección daremos algunos ejemplos de grupos finitos.

Proposición 33 *Sea $|G| = p$ con p primo, entonces G es cíclico.*

DEMOSTRACIÓN.

Sea $a \in G$, $a \neq 1 \Rightarrow < a > < G$ y por el teorema de lagrange $o(a)|p \Rightarrow o(a) = p$ y $G =< a >$ cíclico, mas aún $G \approx \mathbf{Z}_p$.

Grupos de orden ≤ 8.

Consideramos grupos G con orden n, $2 \leq n \leq 8$

- $n = 2, 3, 5, 7$, G es isomorfo a $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$, $\mathbf{Z}_7$.

- $n = 4$, sea $a \in G$, $a \neq 1$, $< a > < G$, $o(a)|4$. Tenemos dos casos:

(i) $0(a) = 4 \Rightarrow G =< a > \approx \mathbf{Z}_4$.

(ii) No hay elementos de orden $4 \Rightarrow G = \{1, a, b, c\}$

con $o(a) = o(b) = o(c) = 2$, y $a = a^{-1}$, $b = b^{-1}$, $c = c^{-1}$, y

por tanto $ab = c$, ya que si $ab = a \Rightarrow b = 1$ y si $ab = b \Rightarrow a = 1$.

Entonces $G = \{1, a, b, ab\}$ y como $o(ab) = 2 \Rightarrow abab = 1 \Rightarrow ababb = b \Rightarrow$

$aaba = ab \Rightarrow ba = ab$, y G es abeliano, con

$G \approx \mathbf{Z}_2 \times \mathbf{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})\}$.

- $n = 6$, supongamos

(i) Existe $a \in G$ con $o(a) = 6 \Rightarrow G =< a > \approx \mathbf{Z}_6$.

(ii) Supongamos existe $a \in G$, con $o(a) = 3$, (y no hay de orden 6), entonces

$< a >= \{1, a, a^2\} \lhd G$ (por ser de índice 2) $\Rightarrow$

$G/ < a >= \{< a >, b < a >\}$, $b \in G$, $b \notin < a > \Rightarrow$

$G = \{1, a, a^2\} \cup \{b, ba, ba^2\}$, y falta determinar cuanto vale ab.

Si $ab = a \Rightarrow b = 1$, si $ab = a^2 \Rightarrow b = a$, si $ab = b \Rightarrow a = 1$,

si $ab = ba$, es abeliano y $o(a) = 6$. Por tanto $ab = ba^2$.

Falta determinar b^2, si $b^2 = a$, ó $b^2 = a^2$, entonces $o(b) = 6$.

Si $b^2 = ba \Rightarrow a = b$ y si $b^2 = ba^2 \Rightarrow a^2 = b$

luego $b^2 = 1$, y $G = \{1, a, a^2, b, ba, ba^2\}$, con $a^3 = 1$, $b^2 = 1$, $ab = ba^2$,

es decir $G \approx D_3$ no abeliano.

Como S_3 no es abeliano y tiene elementos de orden $3 \Rightarrow G \approx D_3 \approx S_3$.

Si todos los elementos tienen orden 2, G es abeliano,

y no puede tener 6 elementos, contendría $\{1, a, b, ab, c, d\}$ y faltaría cd,

y no hay mas grupos de orden 6.

- $n = 8$, los ordenes de los elementos son $1, 2, 4, 8$.

(i) Existe $a \in G$ con $o(a) = 8 \Rightarrow G =< a > \approx \mathbf{Z}_8$.

(ii) Supongamos existe $a \in G$, con $o(a) = 4$, (y no hay de orden 8), entonces

$< a >= \{1, a, a^2, a^3\} \lhd G$ (por ser de índice 2) $\Rightarrow$

$G/ < a >= \{< a >, b < a >\}$, $b \in G$, $b \notin < a > \Rightarrow$

$G = \{1, a, a^2, a^3\} \cup \{b, ba, ba^2, ba^3\}$, y falta determinar cuanto vale ab.

Por un proceso análogo al caso $n = 6$, se prueba que hay dos casos

(a) $ab = ba$, abeliano, (b) $ab = ba^3$,

Caso (a) $ab = ba$, G abeliano, y $b^2 = 1$, ó $b^2 = a^2$,

si $o(b) = 2$, $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$,

y si $b^2 = a^2 \Rightarrow o(ba) = 2$ y tomando $ba \leftrightarrow b$, y

$G = \{1, a, a^2, a^3, ba, baa, baa^2, baa^3\} = \{1, a, a^2, a^3, ba, ba^2, ba^3, b\}$, y

$G \approx \mathbf{Z}_4 \times \mathbf{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{2}, \overline{0}), (\overline{3}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1}), (\overline{2}, \overline{1}), (\overline{3}, \overline{1})\}$.

Caso (b) $ab = ba^3$, hay dos casos,

primero $b^2 = 1$, $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\} \approx D_4$

con $a^4 = 1$, y $ab = ba^3$.

segundo $b^2 = a^2$, $o(b) = 4$ y $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\} \equiv Q_8$

con $a^4 = 1$, y $ab = ba^3$, el grupo de los cuaternios, con el producto de matrices

$$Q_8 \equiv \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$$

(iii) Todos los elementos tienen orden 2, el grupo es abeliano, y

$G \approx \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 = \{(\overline{0}, \overline{0}, \overline{0}), (\overline{1}, \overline{0}, \overline{0}), (\overline{0}, \overline{1}, \overline{0}), (\overline{0}, \overline{0}, \overline{1}),$

$(\overline{1}, \overline{1}, \overline{0}), (\overline{1}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{1}, \overline{1})\}$.

Grupos diedrales

Los grupos diedrales D_n son grupos de transformaciones del plano que dejan fijo un poligono regular de n lados.

Suponemos En $\mathbf{R}^2$ el poligono inscrito en la circunferencia de radio 1, y uno de sus vértices es $P_0 = (1, 0)$. Denotamos por σ la rotación con centro O y ángulo $2\pi/n$ y por τ la simetría respecto al eje OX (que contiene el $(1, 0)$).

Sea $\sigma^r(P_k) = P_j$, con $0 \leq r \leq n-1$, $j \leq n-1$, $j \equiv (r+k)(mod\ n)$.

Denotamos $P_k = (a_k, b_k)$, $a_k = cos(k2\pi/n)$, $b_k = sen(k2\pi/n) \Rightarrow$

$\tau(P_k) = (a_k, -b_k) = P_j$, con $j = n - k$, ya que

el ángulo $2(n-k)\pi/n = 2\pi - (2k\pi/n)$, y por tanto

$a_{n-k} = cos(2(n-k)\pi/n) = cos(2k\pi/n) = a_k$,

$b_{n-k} = sen(2(n-k)\pi/n) = -sen(2k\pi/n) = -b_k$.

Veamos que $D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$,

los elementos son distintos, para $i, j \leq n-1$, $i \neq j$, $\sigma^i \neq \sigma^j$, y $\tau\sigma^i \neq \tau\sigma^j$,

y si $\tau\sigma^i = \sigma^j \Rightarrow \tau = \sigma^{j-i}$ que nunca es posible.

Por último veamos que solo hay $2n$ transformaciones en D_n,

sea $\rho \in D_n$, y sea $\rho(P_0) = P_k$, hay n posibilidades de elegir k, y

si P_j es un vértice consecutivo a P_0, y ρ conserva la distancia $\Rightarrow$

$\rho(P_j)$ será consecutivo con $\rho(P_0)$, y hay dos posibilidades de ello $\Rightarrow$

(como P_0, P_j son una base $\mathbf{R}^2$), que solo hay $2n$ transformaciones .

2.6 Acción de un grupo sobre un conjunto

En esta sección estableceremos una relación entre un grupo y un conjunto que nos permitirá, entre otras cosas, reflejar las propiedades del grupo sobre el conjunto. La utilizaremos para contar elementos de grupos finitos, y para cuestiones de normalidad.

Definición 35 *Definimos una acción de un grupo G sobre un conjunto X, a una aplicación $\rho : G \times X \to X$, $\rho(g, x) = gx$, verificando:*
(i) $1x = x$
(ii) $g'(gx) = (g'g)x$

Nota Dada una acción ρ de G en X, para todo $g \in G$ se tiene una aplicación $\rho_g : X \to X$, $\rho_g(x) = gx$.

EJEMPLO:

El grupo de las rotaciones actuando sobre el plano $\mathbf{R}^2$.

La aplicación antes definida verifica:

Proposición 34 *Dado G prupo y X conjunto se tiene:*

(i) La aplicación ρ_g es una permutación de X, y $\widehat{\rho} : G \to P(X)$,
($P(X)$ permutaciones de X), definido por $\widehat{\rho}(g) = \rho_g$ es un homomorfismo de grupos.

(ii) Existe una biyección:
$\{\rho$, *acciones de G en $X\} \overset{\varphi}{\leftrightarrow} \{f : G \to P(X)$ homomorfismos de grupos$\}$,*

definida φ por $\rho \to \widehat{\rho}$, y φ^{-1} por $f \to \widetilde{f}$, donde la acción $\widetilde{f}$ es $\widetilde{f}(g, x) = f(g)(x)$.

DEMOSTRACIÓN.

(i) ρ_g es una permutación de X, ya que su inversa es $\rho_{g^{-1}}$,

y $\rho_{g^{-1}}\rho_g(x) = \rho_{g^{-1}}(g) = (g^{-1}g)x = 1x = x$
(analogamente para el otro sentido).

Comprobemos que $\widehat{\rho}$ es un homomorfismo de grupos, es decir

$\rho_{g_1 g_2} = \rho_{g_1} \circ \rho_{g_2}$, es decir $\forall\, x \in X$,

$\rho_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \rho_{g_1}(g_2x) = \rho_{g_1}(\rho_{g_2}(x)) = (\rho_{g_1} \circ \rho_{g_2})(x)$.

(ii) $\widetilde{f}$ es $\widetilde{f}(g,x) = f(g)(x)$ es una acción,

$\widetilde{f}(gg',x) = f(gg')(x) = (f(g) \circ f(g'))(x) = \widetilde{f}(g, \widetilde{f}(g',x))$.

Veamos la biyección, primero $\widehat{\widetilde{f}} = f$, es decir $\forall\ g \in G$, $\forall\ x \in X$,

$(\widehat{\widetilde{f}}(g))(x) = \widetilde{f}(g,x) = f(g)(x)$

y también $\widetilde{\widehat{\rho}} = \rho$, es decir $\forall\ g \in G$, $\forall\ x \in X$,

$\widetilde{\widehat{\rho}}(g,x) = \widehat{\rho}(g)(x) = \rho(g,x)$.

Nota Llamaremos a un homomorfismo $f : G \to P(X)$ una *representación* de G en X.

Definición 36 *Una acción ρ de G en X es fiel o efectiva si la representación asociada $\widehat{\rho} : G \to P(X)$ es monomorfismo, es decir $\forall\ x \in X$, $gx = x \Leftrightarrow g = 1$.*

Como $\widehat{\rho}$ monomorfismo $\Leftrightarrow ker(\widehat{\rho}) = \{1\} \Rightarrow$

$\rho_g = 1_X \Leftrightarrow g = 1$ es decir $\forall\ x \in X$, $\rho_g(x) = gx = x \Leftrightarrow g = 1$.

Definición 37 *Una acción ρ de G en X es transitiva si $\forall\ x, y \in X$, $\exists\ g \in G$ con $gx = y$.*

EJEMPLOS:

- *Acción por conjugación*, sea G un grupo y $H < G$ subgrupo, definimos una acción de H en G, $i(h,g) = hgh^{-1}$, (acción por conjugación).

La representación asociada es $i : H \to Aut(G)$, definida $i_h(g) = hgh^{-1}$ que se comprueba que es automorfismo de G.

En general no es efectiva, ya que el núcleo de la acción es

$\{h \in H | hgh^{-1} = g\} = \{h \in H | hg = gh,\ \forall\ g \in G\} = H \cap C(G)$,

- *Acción por traslación*, Sea G grupo y $H < G$, definimos una acción de H en G, $\lambda(h,g) = hg$ (acción de traslación por la izquierda).

Es efectiva, ya que si $hg = g \Rightarrow h = 1$.

Si $H = G$, entonces la acción por traslación es transitiva, pues dados $x, y \in G$, $x^{-1}y \in G$, y $x(x^{-1}y) = y$

- *Acción sobre los subgrupos de un grupo.* La acción de H en G por conjugación da una acción de H en el conjunto de subgrupos de G por conjugación, sea $\Gamma_G = \{K < G\}$ definida por

$\rho : H \times \Gamma_G \to \Gamma_G$, $\rho(h, K) = hKh^{-1}$,

que es un subgrupo de G, ya que $hkh^{-1}hk'h^{-1} = hkk'h^{-1}$.

Acciones en cocientes

Veamos como se comportan las acciones de los ejemplos anteriores al pasar al cociente.

Definición 38 *Sean $K < G$, $H < G$, diremos que K es estable por conjugación de $H \Leftrightarrow i(K) = hKh^{-1} = K$, $\forall\, h \in H$.*

- *Acción por conjugacion*:
Si K es estable por conjugación de H la acción por conjugación de H en G induce una acción por conjugación de H en $G/\sim_K$ (si $K \lhd G$ en G/K), ya que:

definimos para gK, $i_h(gK) = hgKh^{-1} = hgh^{-1}hKh^{-1} = hgh^{-1}K$,

es decir $i_h(gK) = i_h(g)i_h(K) = i_h(g)K$.

- *Acción por traslación*: Sea cualquier $K < G$ induce una acción por traslación de H en $G/\sim_K$ (si $K \lhd G$ en G/K), ya que:

definimos para gK, $\lambda_h(gK) = (\lambda_h(g))K$, puesto que $h(gK) = (hg)K$.

Si $H = G$ La acción de G en $G/\sim_K$ por traslación es transitiva,

dados gK, $g'K$, $(g'g^{-1})gK = g'K$.

El núcleo de la acción es $ker(\lambda) = \{h \in H | h(gK) = gK)$, $\forall\, g \in G$,

$hgk = gk' \Leftrightarrow h = gk'k^{-1}g^{-1} = gk''g^{-1}$, $\forall\, g \in G$, es decir

$$ker(\lambda) = H \cap (\bigcap_{g \in G} gKg^{-1}).$$

Proposición 35 *Sea G un grupo finito, y p el menor primo que divide al orden de G, entonces todo subgrupo de G de índice p es normal en G.*

DEMOSTRACIÓN

Sea $H < G$, y $[G : H] = p$, consideremos la acción de G en el cociente $G/\sim_H$ por traslación por la izquierda,

sea $K = \bigcap_{g\in G} gHg^{-1}$ (normal), el núcleo de la acción,

veamos que $K = H$.

G actúa sobre $G/\sim_H \Rightarrow G/K$ actúa sobre $G/\sim_H$ y es efectiva $\Rightarrow$

$G/K \hookrightarrow P(G/\sim_H)$ es inyectiva y $|G/K|$ divide a $p!$, y

como sabemos que $[G : K]$ divide al orden de G, y

no hay ningún primo $< p$ (por definición de p),

todo divisor primo de $[G : K]$ es $\geq p$ (y no menor a p) $\Rightarrow [G : K] = p$

como $K \subset H \Rightarrow [G : K] \geq [G : H] = p \Rightarrow p = [G : K] = [G : H][H : K]$

$\Rightarrow [H : K] = 1 \Rightarrow H = K$, y H es normal en G.

Proposición 36 *Sea G un grupo finito simple, y $H < G$ con $[G : H] = m$ entonces existe $f : G \to A_m$ homomorfismo inyectivo.*

DEMOSTRACIÓN

Sea la acción $\rho : G \times G/\sim_H \to G/\sim_H$ por traslación $\rho(g, g'H) = gg'H$

$\Rightarrow \exists\ f = \widehat{\rho} : G \to P(G/\sim_H) \approx S_m$ homomorfismo $\Rightarrow f(G) \subset S_m$

(G es simple) $ker(f) = \{1\} \Rightarrow f$ es inyectivo,

entonces si $f(G) \not\subseteq A_m \Rightarrow K = f(G) \cap A_m \subset A_m \Rightarrow$
$f(G)$ tiene la mitad de permutaciones pares y la mitad impares
$\Rightarrow [f(G) : K] = 2 \Rightarrow$

$K \lhd f(G)$, y como $f(G)$ es simple $\Rightarrow K = \{1\}$ y $f(G) \subset A_m$

Orbitas de una acción

dada una acción ρ de G en X, la *órbita* de $x \in X$ es $\Theta_x = \{gx | g \in G\}$

EJEMPLO

Si $H < G$ actúa sobre G por traslación λ por la izquierda, la órbita de $a \in G$ es $\Theta_a = \{ha | h \in H\} = Ha$ la clase de a módulo H.

Nota Si la acción ρ de G en X es transitiva entonces hay una sola órbita, es decir $\Theta_x = X$

Definición 39 *Dada una acción ρ de G en X, llamaremos estabilizador de $x \in X$, a $I_\rho(x) = \{g \in G | gx = x\}$ (denotaremos también por $I(x)$).*

$I_\rho(x)$ es un subgrupo de G, ya que

si $g_1, g_2 \in I_\rho(x)$, $g_1 g_2 x = g_1 x = x$,

y si $gx = x \Rightarrow g^{-1}gx = g^{-1}x \Rightarrow x = g^{-1}x$ y $g^{-1} \in I_\rho(x)$.

Diremos que $x \in X$ es *fijo* por la acción si $I_\rho(x) = G$, todos los elementos del grupo lo dejan fijo. Entonces su órbita es $\Theta_x = \{x\}$.

El estabilizador de un elemento nos determina el número de elementos de una órbita.

Proposición 37 *Dada una acción de G en X, existe una biyección entre la órbita Θ_x y $G/\sim I_\rho(x)$, y $card(\Theta_x) = [G : I_\rho(x)]$, y si G es finito, entonces $|G| = card(\Theta_x)|I_\rho(x)|$.*

DEMOSTRACIÓN

Definimos $\varphi : G/\sim I_\rho(x) \to \Theta_x$, por $\varphi(gI_\rho(x)) = gx$, que es suprayectiva,

y como $gx = g'x \Leftrightarrow x = g^{-1}g'x \Leftrightarrow g^{-1}g' \in I_\rho(x) \Leftrightarrow gI_\rho(x) = g'I_\rho(x)$,

φ está bien definida y es inyectiva.

Si G es finito por el teorema de Lagrange

$|G| = [G : I_\rho(x)]|I_\rho(x)| = card(\Theta_x)|I_\rho(x)|$.

La siguiente proposición nos muestra que el centralizador determina el núcleo de la acción.

Proposición 38 *Dada una acción de G en X, el núcleo de la acción es $ker(\widehat{\rho}) = \bigcap_{x \in X} I_\rho(x)$*

DEMOSTRACIÓN

$ker(\widehat{\rho}) = \{g \in G | \rho_g = 1_X\} = \{g \in G | gx = x, \ \forall \ x \in X\}$,

y como $I_\rho(x) = \{g \in G | gx = x\} \Rightarrow ker(\widehat{\rho}) = \bigcap_{x \in X} I_\rho(x)$.

EJEMPLOS

- Consideramos la acción de G en G por conjugación, entonces si $g \in G$

$I(g) = \{a \in G | aga^{-1} = g\} = \{a \in G | ag = ga\} \equiv C_G(g)$,

llamado *centralizador* de g en G.

- Si $H < G$, denotamos $C_H(g) \equiv H \cap C_G(g)$, *centralizador* de g en H, que es el estabilizador $I(g)$ por la acción de conjugación de H en G.

- Consideramos la acción de $H < G$ en $\Gamma_G = \{K < G\}$ por conjugación,

$I(K) = \{h \in H | hKh^{-1} = K\} = \{h \in H | hK = Kh\} \equiv N_H(K)$,
normalizador de K en H

- Si G actua sobre Γ_G por conjugación $I(K) \equiv N(K)$,
normalizador de K en G,

$K \lhd N(K)$, y es el máximo subgrupo de G, en el que K es normal.

y se verifica $N(K) = G \Leftrightarrow K \lhd G$.

Ecuación de órbitas

Sea ρ una acción de G en X, definimos la relación:

$x \sim_\rho y \Leftrightarrow \exists\, g \in G$ con $gx = y$

La relación es de equivalencia y el conjunto cociente $X/\sim_\rho$ que denotamos por X/G, tiene como clases las órbitas por ρ, Θ_x, por tanto

$$card(X) = \sum_{\Theta_x \in X/G} card(\Theta_x)$$

Si X es finito, sea $X_0 = \{x \in X | \Theta_x = \{x\}\}$ el conjunto de los puntos fijos por la acción, entonces

$$card(X) = card(X_0) + \sum_{i=1}^{s} card(\Theta_i)$$

donde $\{\Theta_1, \ldots, \Theta_s\}$ son las órbitas con más de un elemento, y por el resultado anterior

$$card(X) = card(X_0) + \sum_{i=1}^{s} [G : I(x_i)]$$

conocida como la *ecuación de órbitas*.

Corolario 21 *Si G es un p-grupo, p primo ($|G| = p^r$), y G actúa sobre X conjunto finito, entonces*

$$card(X) \equiv card(X_0)(mod\ p).$$

DEMOSTRACIÓN

Supongamos que hay puntos fijos, $card(X_o) \neq 0$.

Sea $x_i \in G$ con $[G : I(x_i)] > 1$, (por el teorema de Lagrange)

$[G : I(x_i)]||G| = p^r \Rightarrow p|[G : I(x_i)] \Rightarrow p| \sum_{i=1}^{s} [G : I(x_i)] \Rightarrow$

$card(X) \equiv card(X_0)(mod\ p)$.

Corolario 22 *Sea H p-subgrupo, p primo, de G finito, entonces:*

$$[N(H) : H] \equiv [G : H](mod\ p)$$

DEMOSTRACIÓN

Sea la acción de H en $X = G/\sim_H$ por traslación por la izquierda, el estabilizador

$I(gH) = \{h \in H | h(gH) = gH\} = \{h \in H | g^{-1}hgH = H\} =$

$\{h \in H | g^{-1}hg \in H\}$, la órbita de g tiene un solo elemento si

$I(g) = H$, es decir si $\forall\ h \in H$, $g^{-1}hg \in H \Rightarrow g \in N(H) \Rightarrow$

$X_0 = N(H)/\sim_H \Rightarrow$ (ecuación de orbitas)

$card(G/\sim_H) = card(N(H)/\sim_H) + \sum orb(\Theta_i) \Rightarrow$

$[G : H] = [N(H) : H] + \sum [H : I(x_i)]$, con $[H : I(x_i)] = p^{r_i} \Rightarrow$

$[N(H) : H] \equiv [G : H](mod\ p)$

Ecuación de clases

Es un caso especial de la ecuación de órbitas. Sea G actuando por conjugación sobre G.

El conjunto de los puntos fijos $G_0 = \{g \in G | xgx^{-1} = g, \forall\ x \in G\} =$

$\{g \in G | xg = gx, \forall\ x \in G\} = C(G)$, centro de G,

$I(x_i) = \{g \in G | gx_ig^{-1} = x_i\} = \{g \in G | gx_i = x_ig\} = Z(x_i)$,

centralizador de $x_i \Rightarrow$ (ecuación de orbitas)

$$|G| = |C(G)| + \sum_{i=1}^{s} [G : Z(x_i)]$$

llamada *ecuación de clases*, donde $x_1, \ldots, x_s$ son representantes de las clases de conjugación con más de un elemento.

Proposición 39 *El centro de un p-grupo es* $C(G) \neq \{1\}$.

DEMOSTRACIÓN

Sea $|G| = p^n$, p primo, G actúa sobre G por conjugación y la ecuación de clases

$|G| = |C(G)| + \sum_{i=1}^{s} [G : Z(x_i)]$, y como $[G : Z(x_i)] = p^{k_i}$

es tal que $|G|$, $\sum_{i=1}^{s} [G : Z(x_i)]$ son múltiplos de $p \Rightarrow$

$|C(G)|$ es múltiplo de p, $1 \in C(G) \Rightarrow 0 \neq |C(G)| \geq p$, y $|C(G)| \neq \{1\}$.

2.7 Teoremas de Sylow

Dado un grupo finito G, los resultados siguientes nos dicen si p^m divide al orden de G, cuando existen p^i-subgrupos de G y en algunos casos cual es su número.

Teorema 29 *de Cauchy (no conmutativo). Sea* G *un grupo finito,* $|G| = n$, *con* $p^m | n$, p *primo, entonces* $\exists\ x \in G$ *con* $o(x) = p$, *es decir* $\exists\ H < G$ *con* $|H| = p$.

DEMOSTRACIÓN

Sea $X = \{(x_1, \ldots, x_p) \in G^p | x_1 \cdots x_p = 1\}$,

como $(x_1 \cdots x_{p-1})x_p = 1 \Rightarrow (x_1 \cdots x_{p-1})^{-1} = x_p$,

y por tanto los elementos de X son los mismos que las posibles

$(p-1)$-tuplas $(x_1, \ldots, x_{p-1})$, es decir $card(X) = n^{p-1}$.

Hacemos un acción de $\mathbf{Z}_p$ sobre X, dado $0 \leq k < p$,

$(\overline{k}, (x_1, \ldots, x_p)) \to (x_{k+1}, \ldots, x_p, x_1, \ldots, x_k)$

que se comprueba facilmente que es acción.

Los puntos fijos son $X_0 = \{(x, \overset{p}{\ldots}, x) | x^p = 1\}$

y como $\mathbf{Z}_p$ es un p-grupo por un resultado anterior,

$card(X) \equiv card(X_o)(mod\, p) \Rightarrow (card(X) = n^{p-1}$, y $p|n)$

$card(X_0)$ es múltiplo de p, y como $(1, \overset{p}{\ldots}, 1) \in X_0$,

es decir $card(X_0) > 1$, y entonces

existe $1 \neq x \in G$ con $(x, \overset{p}{\ldots}, x) \in X_0$, es decir $x^p = 1$.

Por tanto $< x >= H < G$ con $|H| = p$.

Sea G un grupo finito, $|G| = n$, con $p^r|n$, p primo, definimos *p-subgrupo de Sylow* de G es un subgrupo $P < G$ con $|P| = p^r$ con r máximo.

Teorema 30 *1^{er} teorema de Sylow. Sea G un grupo finito, $|G| = n$, con $p^r|n$, p primo, r máximo, entonces existen subgrupos H_i, $i = 1, \ldots, r$, con $|H_i| = p^i$, y $H_1 \lhd H_2 \lhd \cdots \lhd H_r$.*

DEMOSTRACIÓN

Hacemos inducción en r, para $r = 1$ por el teorema de Cauchy.

Supongamos cierto para $r - 1$, entonces existen existen subgrupos

H_i, $i = 1, \ldots, r-1$, con $|H_i| = p^i$, y $H_1 \lhd H_2 \lhd \cdots \lhd H_{r-1}$,

como $p^r|n \Rightarrow p|[G : H_{r-1}] \Rightarrow$ (como $[N(H) : H] \equiv [G : H](mod\, p)$)

$p|[N(H_{r-1}) : H_{r-1}]$, luego el grupo cociente $N(H_{r-1})/H_{r-1}$

tiene un subgrupo H_r/H_{r-1} de orden p, con $H_r < N(H_{r-1}) \Rightarrow$

$|H_r| = |H_{r-1}|p = p^r$, y $H_{r-1} \lhd H_r$.

El teorema nos dice en particular que existen p-sugrupos Sylow para todo primo p divisor del orden de G.

Corolario 23 *Los conjugados de un p-subgrupos de Sylow son p-subgrupos de Sylow.*

DEMOSTRACIÓN

Para todo $g \in G$ si $P < G$ es de Sylow, $|gPg^{-1}| = |P|$.

Corolario 24 *Si G tiene un único p-subgrupo de Sylow, entoces es normal.*

DEMOSTRACIÓN

Si $P < G$ es de Sylow, por lo anterior p,ara todo $g \in G$, gPg^{-1} es de Sylow, y como solo hay uno, $gPg^{-1} = P \Rightarrow P \lhd G$.

Teorema 31 *2^{do} teorema de Sylow. Sean G un grupo finito, $|G| = n$, H un p-subgrupo de G, y S un p-subgrupo de Sylow de $G \Rightarrow \exists\ x \in G$ tal que $H \subset xSx^{-1}$. En particular, si P y S son p-subgrupos de Sylow de G, $\exists\ x \in G$ tal que $P = xSx^{-1}$, es decir son conjugados.*

DEMOSTRACIÓN

Sea la acción de H en $X = G/\sim_S$ por traslación por la izquierda

xS es invariante por la acción $\Leftrightarrow hxS = xS\ \forall\ h \in H \Leftrightarrow$

$\forall h \in H, x^{-1}hxS = S \Leftrightarrow x^{-1}hx \in S,\ \forall\ h \in H \Leftrightarrow$

$h \in xSx^{-1}\ \forall\ h \in H \Leftrightarrow H \subset xSx^{-1}$.

Veamos que hay invariantes:

$card(X) = [G : S]$, y $card(X) = card(X_0) + \sum[H : I(x_iS)]$,

y como H es un p-subgrupo $\Rightarrow$

$[G : S] \equiv card(X_0)(mod\ p)$, y $p \not| [G : S]$ (por ser S Sylow) $\Rightarrow$

$card(X_0)$ no es divisible por $p \Rightarrow X_0$ no es vacío y $\exists\ x \in G$ con $H \subset xSx^{-1}$.

Por último si P, S son p-subgrupos de Sylow, $|P| = |S|$,

y como $\exists\ x \in G$ con $P \subset xSx^{-1} \Rightarrow |P| = |xSx^{-1}|$ y por tanto $P = xSx^{-1}$.

Corolario 25 *Sea G grupo finito, entonces:*
P es el único p-subgrupo de Sylow de $G \Leftrightarrow P \lhd G$.

DEMOSTRACIÓN

$\Rightarrow$) visto anteriormente.

$\Leftarrow$) Si $P \lhd G \Rightarrow \forall g \in G$, $gPg^{-1} = P \Rightarrow$ solo hay uno de Sylow.

Teorema 32 *3^{er} teorema de Sylow. Sean G un grupo finito, $|G| = n$, y n_p el número de p-subgrupos de Sylow de G, entonces:*
(i) $n_p = [G : N(S)]$ para todo S p-subgrupos de Sylow de G.
(ii) $n_p|[G : S]$ para todo S p-subgrupos de Sylow de G.
(iii) $n_p \equiv 1(mod\ p)$.

DEMOSTRACIÓN

(i) Por el 2^{do} teorema de Sylow, G actúa sobre $\Gamma_G = \{H < G\}$ por conjugación $\Rightarrow$

$n_p = card(\Theta_S)$ ($\Theta_S \equiv$ órbita de S p-subgrupo de Sylow),

ya que los p-subgrupos de Sylow son conjugados, el estabilizador

$I(S) = \{g \in G | gSg^{-1} = S\} = N(S) \Rightarrow n_p = [G : I(S)] = [G : N(S)]$.

(ii) Como $S \subset N(S) \subset G$, $[G : S] = [G : N(S)][N(S) : S] \Rightarrow$

$n_p = [G : N(S)]|[G : S]$.

(iii) Sea ahora $X = \{T < G | T\ es\ de\ Sylow\}$, y consideramos que S de Sylow, actúa sobre X por conjugación $\Rightarrow$

$X_0 = \{T \in X | sTs^{-1} = T,\ \forall\ s \in S\} = \{T \in X | S \subset N(T)\}$,

veamos que $X_0 = \{S\}$,

sea $T \in X_0 \Rightarrow S, T$ son p-subgrupos de Sylow, $S \subset N(T), T \subset N(T)$,

son normales en N(T), luego por el 3^{er} teorema de isomorfía en $N(T) \Rightarrow$

$ST/T \approx S/S \cap T \Rightarrow |ST| = p^m|T| \Rightarrow m = 0$ y $ST = T \Rightarrow$

$S \subset T \Rightarrow S = T$.

Entonces como $[S : I(T_i)]$ es potencia de p, y

$card(X) = card(X_0) + \sum[S : I(T_i)] \Rightarrow n_p = card(X) \equiv 1(mod\ p)$.

EJEMPLO Sea G un grupo con $2^2 \cdot 7$ elementos, por el 1 teorena de Sylow,

existen subgrupos de G, H_1, $\mid H_1 \mid = 2$, H_2, $\mid H_2 \mid = 2^2$, H_3, $\mid H_3 \mid = 7$,

por el 3 teorema de Sylow, $n_2 \mid \frac{|G|}{|H_2|} = \frac{2^2 7}{2^2} = 7$, y

$n_2 \equiv 1 mod(2) \Rightarrow n_2 = 1$ o 7,

$n_7 \mid \frac{|G|}{|H_3|} = \frac{2^2 7}{7} = 4$, y $n_7 \equiv 1 mod(7) \Rightarrow n_7 = 1$ y H_3 es normal en G,

además, $H_4 = H_1 H_3$ con $\mid H_4 \mid = 14$ es subgrupo de G,

y G tiene subrupos de todos los ordenes posibles, 1,2,4,7,14,28.

2.8 Grupos dados por generadores y relaciones

Vamos a construir grupos de la manera mas general posible. Comenzamos con el grupo de las palabras.

Sea S un conjunto, consideramos $S' = S \times \{1\}$, y denotamos $(s, 1) = s'$. Llamaremos símbolos a $S \cup S'$.

Formamos $G^*(S) = \{sucesiones\ finitas\ de\ simbolos\ de\ S \cup S'\}$,
denotamos $e \equiv$ sucesion vacía, ω palabra, $l(\omega)$ longitud de la palabra.

Queremos que s' sea el "inverso" de s, es decir ss' y $s's$ sean la palabra vacia.

Llamaremos *palabra reducida*, $\rho(\omega)$ a la palabra que no tiene términos cancelables ss', $s's$ y e.

Denotaremos $G(S) \subset G^*(S)$, a las palabras reducidas.

$\rho : G^*(S) \to G(S)$ aplicación, y es la identidad sobre $G(S)$, es decir
$\rho(\omega) = \omega \Leftrightarrow \omega$ es reducida.

Consideramos la operación *concatenación de palabras*:

$\cdot : G(S) \times G(S) \to G(S)$, $\omega \cdot \alpha = \rho(\omega\alpha)$

(donde $\omega\alpha$ es escribir una palabra detrás de la otra)

Proposición 40 *$G(S)$ es un grupo llamado grupo libre generado por S o grupo de las palabras.*

DEMOSTRACIÓN.

Se verifican las siguientes propiedades:
- Asociativa.
- El elemento neutro es la palabra vacia e.
- El inverso del simbolo s es $s' = s^{-1}$, es decir se tiene
$\rho(ss') = \rho(s's) = \rho(e) = \emptyset$,

por tanto si $\omega = s_{i_1} \cdots s_{i_r}$, $\omega^{-1} = s'_{i_r} \cdots s'_{i_1}$.

Todo elemento $\omega \in G(S)$ se puede escribir

$\omega = s_{i_1}^{e_1} \cdots s_{i_r}^{e_r}$, $s_{i_1}, \ldots, s_{i_r} \in S$, $e_i = \pm 1$, con

$e_{j+1} \neq -e_j$, si $s_{i_{j+1}} = s_{i_j}$, $1 \leq j < r$.

$S \subset G(S)$, y S genera $G(S)$.

Proposición 41 *Propiedad universal. Sea S un conjunto, G un grupo y $f : S \to G$ aplicación $\Rightarrow$ existe un único homomorfismo $\varphi : G(S) \to G$ tal que $\varphi(s) = f(s)$, $\forall s \in S$, y $im(\varphi) =< f(S) >$.*

DEMOSTRACIÓN.

Definimos $\varphi : G(S) \to G$ por $\varphi(s) = f(s)$, y $\varphi(e) = 1$ (neutro de G), $\varphi(s^{-1}) = (f(s))^{-1}$.

φ es homomorfismo, y es único puesto que está definido en el conjunto de generadores.

Teorema 33 *Sea $S \subset G$ un conjunto de generadores de G. Entonces existe un subrupo normal $K \lhd G(S)$ que verifica*

$G \simeq G(S)/K$.

DEMOSTRACIÓN.

Consideramos la inclusión $i : S \hookrightarrow G$, como en la proposición anterior, y existe $\varphi : G(S) \to G$ homomorfimo suprayectivo, y por el primer teorema de isomorfía $G \approx G(S)/ker(\varphi)$.

Llamaremos relaciones a los elementos de $ker(\varphi)$, es decir $\omega \in G(S)$, con $\omega = 1$, es decir $s_{i_1}^{n_1} \cdots s_{i_r}^{n_r} = 1$, $n_i \in \mathbf{N}$.

Nota El isomorfismo $G \approx G(S)/ker(\varphi)$ describe G por sus generadores y relaciones.

EJEMPLOS:

- Para D_4 los generadores son $S = \{\sigma, \tau\}$, y las relaciones son el subgrupo normal K de $G(S)$ generado por $\{\sigma^4, \tau^2, (\tau\sigma)^2\}$ y $D_4 \approx G(\{\sigma, \tau\})/K$.

- S_n está generado por permutaciones $\sigma_i = (i, i+1)$, $i = 1, \ldots, n-1$, verificando las relaciones

$\sigma_i^2 = 1$, $\sigma_i\sigma_j = \sigma_j\sigma_i$, si $|j - i| > 1$ (son disjuntas), $(\sigma_i\sigma_{i+1})^3 = 1$,

ya que $\sigma_i\sigma_{i+1} = (i, i+1, i+2)$.

2.9 Producto directo de grupos

Vamos a considerar el producto directo de grupos. En primer lugar consideramos un número finito de grupos.

Sean $G_1, \ldots, G_r$ grupos, su producto cartesiano $G_1 \times \cdots \times G_r$,
con la operación $(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$
(cada producto $a_i b_i$ en G_i)

Entonces $G_1 \times \cdots \times G_r$ es un grupo llamado *producto directo*,
el neutro es $(1, \ldots, 1)$, y el inverso de $(a_1, \ldots, a_n)$ es $(a_1^{-1}, \ldots, a_n^{-1})$.

Si todos los G_i son abelianos, entonces el producto directo es abeliano, y tambien lo podemos denotar $G_1 \oplus \cdots \oplus G_r$ y llamarlo suma directa.

Si todos los grupos son iguales denotamos $G \times \overset{(r}{\cdots} \times G \equiv G^r$

Homomorfismos desde el producto y sobre el producto

Sean G, y $G_1, \ldots, G_r$, grupos, $f_i : G \to G_i$ homomorfismos

La aplicación $f = (f_1, \ldots, f_r) : G \to G_1 \times \cdots \times G_r$, definida por
$f(a) = (f_1(a), \ldots, f_r(a))$, es homomorfismo de grupos y
es el único homomorfismo de grupos que verifica que:

$$\begin{array}{ccc} G & \overset{f}{\to} & G_1 \times \cdots \times G_r \\ & {\scriptstyle f_i}\searrow & \downarrow{\scriptstyle p_i} \\ & & G_i \end{array}$$

es un diagrama conmutativo, i.e. $p_i \circ f = f_i$
donde $p_i(a_1, \ldots, a_r) = a_i$ es la proyección i-esima (suprayectiva).

Sean G , $G_1, \ldots, G_r$, grupos, (G abeliano) y $\varphi_i : G_i \to G$ homomorfismos entonces la aplicación
$\varphi : G_1 \times \cdots \times G_r \to G$, definida por $\varphi(a_1, \ldots, a_r) = \varphi_1(a_1) \cdots \varphi(a_r)$ es un homomorfismo de grupos

y es el único homomorfismo de grupos que hace

$$\begin{array}{ccc} G_1 \times \cdots \times G_r & \overset{\varphi}{\to} & G \\ {\scriptstyle u_i}\uparrow & \nearrow{\scriptstyle \varphi_i} & \\ G_i & & \end{array}$$

conmutativo el diagrama, i.e. $g \circ u_i = g_i$.
donde $u_i(a_i) = (1, \ldots, 1, a_i, 1, \ldots, 1) = a_i$ (inyectivo).

Producto de grupos cíclicos finitos

Sean $G_1, \ldots, G_r$ grupos cíclicos, con $|G_i| = n_i$, el producto
$P = G_1 \times \cdots \times G_r$ es un grupo de orden $m = n_1 \cdots n_r$.

Proposición 42 *$G_1 \times \cdots \times G_r$ es cíclico $\Leftrightarrow$ los ordenes de los G_i, $i = 1, \ldots, r$, n_i son primos entre sí.*

En este caso si $G_i =< a_i >$, y $(a_1, \ldots, a_r)$ es un generador del producto

DEMOSTRACIÓN.

Como $(1, \ldots, 1, a_i, 1, \ldots, 1)$, $(1, \ldots, 1, a_j, 1, \ldots, 1)$ conmutan,

$(1, \ldots, 1, a_i, 1, \ldots, 1)(1, \ldots, 1, a_j, 1, \ldots, 1) = (1, \ldots, 1, a_i, 1, \ldots, 1, a_j, 1, \ldots, 1)$

y $o(1, \ldots, 1, a_i, 1, \ldots, 1, a_j, 1, \ldots, 1) = mcm(n_i, n_j)$, $\Rightarrow$

$o(a_1, \ldots, a_r) = mcm(n_1, \ldots, n_r)$, y si los n_i's son primos entre sí

$o(a_1, \ldots, a_r) = n_1 \cdots n_r$, es decir el orden de $G_1 \times \cdots \times G_r$ $\Rightarrow$

$G_1 \times \cdots \times G_r =< (a_1, \ldots, a_r) >$ es cíclico.

Producto directo interno de grupos

Sea G grupo, y H, K subgrupos de G, consideramos $H \times K$ y nos preguntamos cuando dicho producto es isomorfo a G.

Definimos $\varphi : H \times K \to G$, por $\varphi(h, k) = hk$,

φ es homomorfismo $\Leftrightarrow hk = kh$, $\forall\, h \in H$, $\forall\, k \in K$

φ es suprayectiva $\Leftrightarrow HK = G$

$ker(\varphi) = \{(x, x^{-1}) | x \in H \cap K\}$, y $ker(\varphi) = \{1\} \Leftrightarrow H \cap K = \{1\}$

Definición 40 *Dados $H, K < G$ diremos que G es producto directo interno de H, y K si el homomorfismo $\varphi : H \times K \to G$, $\varphi(h, k) = hk$ es isomorfismo, $G \approx H \times K$.*

Por lo anterior G es producto directo interno de H, y $K \Leftrightarrow$ se verifican las condiciones:

(i) $\forall\ k \in K\ hk = kh$, $\forall\ h \in H$,$hk = kh$.

(ii) $H \cap K = \{1\}$.

(iii) $G = HK$.

Nota Si G es producto directo interno de $H, K < G\ \forall\ g \in G$, $g = hk$ de manera única.

Si G es abeliano escribiremos $G \approx H \oplus K$, y lo llamaremos *suma directa interna*.

EJEMPLOS:

- Sean $\mathbf{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, $H = \{\overline{0}, \overline{2}, \overline{4}, \}$, $K = \{\overline{0}, \overline{3}\}$,

$H+K = \{\overline{0}, \overline{2}, \overline{4}, \}+\{\overline{0}, \overline{3}\} = \{\overline{0}+\overline{0}, \overline{0}+\overline{3}, \overline{2}+\overline{0}, \overline{2}+\overline{3}, \overline{4}+\overline{0}, \overline{4}+\overline{3} = \overline{1}\} = \mathbf{Z}_6$,

y $H \cap K = \{\overline{0}\}$, y como los elementos conmutan, $\mathbf{Z}_6$ es producto (suma) directo interno de H y K.

- En $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, sean $H = \{1, \sigma, \sigma^2, \sigma^3\}$, $K = \{1, \sigma^2, \tau, \tau\sigma^2\}$, se verifica $D_4 = HK$, pero $\sigma\tau \neq \tau\sigma$, y $H \cap K = \{1, \sigma^2\}$, luego D_4 no es producto directo interno de H y K.

- En $D_6 = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\}$, sean $H = \{1, \sigma^3\}$, $K = \{1, \sigma^2, \sigma^4, \tau, \tau\sigma^2, \tau\sigma^4\}$, se verifica que $H \cap K = \{1\}$, los elementos de H conmutan con los elementos de K, y entonces $D_6 = HK$, y $D_6 \approx H \times K$ como producto directo interno.

La condición de conmutar respecto del producto de los elementos de dos subgrupos, se da con las siguientes condiciones

Proposición 43 *Sean $H, K \triangleleft G$, entonces:*
$H \cap K = \{1\} \Leftrightarrow$ *los elementos de H y los de K conmutan*

DEMOSTRACIÓN.

$H, K \triangleleft G \Rightarrow hkh^{-1} \in K$, $kh^{-1}k^{-1} \in H \Rightarrow hkh^{-1}k^{-1} \in H \cap K = \{1\}$
$\Rightarrow hk = kh$.

En general, si consideramos mas de dos subgrupos, sean $H_1, \ldots, H_r$ subgrupos de G,

Definición 41 *Diremos que G es producto directo interno de los H_i, si el homomorfismo $\varphi : H_1 \times \cdots \times H_r \to G$, $\varphi(h_1, \ldots, h_r) = h_1 \cdots h_r$ es isomorfismo, $G \approx H_1 \times \cdots \times H_r$.*

Las condiciones para que φ se isomorfismo son:

(i) φ es homomorfismo $\Leftrightarrow h_i h_j = h_j h_i$, $\forall\ h_i \in H_i$, $h_j \in H_j$, $i \neq j$.

(ii) Si φ es homomorfismo, φ es inyectivo $\Leftrightarrow H_j \cap (H_1 \cdots H_{j-1}) = \{1\}$.

(inyectivo $\equiv h_1 \cdots h_r = h'_1 \cdots h'_r \Leftrightarrow h_i = h'_i$, $\forall\ i$)

(iii) φ es suprayectivo $\Leftrightarrow H_1 \cdots H_r = G$

(es decir $\forall\ g \in G$, $g = h_1 \cdots h_r$, $h_i \in H_i$).

Vamos a comprobarlo:

(i) $\Rightarrow$) Suponemos φ homomorfismo, y $i < j$,
$(1, \ldots, 1, h_j, 1, \ldots, 1)(1, \ldots, 1, h_i, 1, \ldots, 1) =$
$(1, \ldots, 1, h_i, 1, \ldots, 1, h_j, 1, \ldots, 1) \Rightarrow$

$\varphi((1, \ldots, 1, h_j, 1, \ldots, 1)(1, \ldots, 1, h_i, 1, \ldots, 1)) =$
$\varphi(1, \ldots, 1, h_j, 1, \ldots, 1)\varphi(1, \ldots, 1, h_i, 1, \ldots, 1) = h_j h_i$,

y $\varphi(1, \ldots, 1, h_i, 1, \ldots, 1, h_j, 1, \ldots, 1) = h_i h_j \Rightarrow h_j h_i = h_i h_j$, $\forall\ i, j$.

$\Leftarrow$) Supongamos $h_j h_i = h_i h_j$, $\forall\ i, j$,

$\varphi(h_1, \ldots, h_r)(h'_1, \ldots, h'_r) = \varphi(h_1 h'_1, \ldots, h_r h'_r) = h_1 h'_1 \cdots h_r h'_r =$

$(h_1 \cdots h_r)(h'_1 \cdots h'_r) = \varphi(h_1, \ldots, h_r)\varphi(h'_1, \ldots, h'_r)$,
por la conmutatividad de los h_i con los h_j.

(ii) $\Rightarrow$) Sea $h_j = h_1 \cdots h_{j-1} \Rightarrow h_1 \cdots h_{j-1} h_j^{-1} = 1 \Rightarrow$

$\varphi(h_1, \ldots, h_{j-1}, h_j^{-1}, 1, \ldots, 1) = 1 \Rightarrow h_1 = \cdots = h_{j-1} = h_j^{-1} = 1 \Rightarrow$

$H_j \cap (H_1 \cdots H_{j-1}) = 1$.

$\Leftarrow$) Sea $\varphi(h_1, \ldots, h_{r-1}, h_r) = 1 \Rightarrow$

$h_1 \cdots h_{r-1} h_r = 1 \Rightarrow h_1 \cdots h_{r-1} = h_r^{-1} \Rightarrow h_r^{-1} \in H_r \cap (H_1 \cdots H_{r-1}) = \{1\}$

$\Rightarrow h_r = 1$, y recursivamente para $(h_1, \ldots, h_{r-1}, 1)$ y siguientes obtenemos $h_i = 1$ para todo i, y la inyectividad.

(iii) Es evidente.

2.10 Grupos abelianos finitamente generados

En esta sección estudiaremos los grupos abelianos G generados por un número finito de generadores $S = \{x_1, \ldots, x_n\}$. Denotaremos la operación de G como la suma.

Consideramos en el grupo libre generado por S, $G(S)$ la relación de conmutatividad, como $\omega \in G(S)$ es

$\omega = x_{i_1}^{e_1} \cdots x_{i_r}^{e_r}$, $x_{i_j} \in S$, $e_i = \pm 1$,

al ser conmutativo se agrupan las potencias y

$\omega = x_1^{m_1} \cdots x_n^{m_n}$, $m_i \in \mathbf{Z}$, que en notacion suma es
$\omega = m_1 x_1 + \cdots + m_n x_n$, $m_i \in \mathbf{Z}$ y por tanto

L es un *grupo libre conmutativo generado por* $S = \{x_1, \ldots, x_n\} \Leftrightarrow L \approx \mathbf{Z}^n$

basta con asociar $x_i \leftrightarrow e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$.

Un grupo abeliano libre finitamente generado va a estar caracterizado por su número de generadores minimal, es decir que no se pueda suprimir uno de ellos.

Lema 1 *Sean $d_1, \ldots, d_n \in \boldsymbol{Z}$, se tiene:*

$$\frac{\boldsymbol{Z}^n}{< d_1 e_1, \ldots, d_n e_n >} \approx \boldsymbol{Z}_{d_1} \oplus \cdots \oplus \boldsymbol{Z}_{d_n}.$$

DEMOSTRACIÓN:

Definimos un homomorfismo de $\mathbf{Z}^n$ en $\mathbf{Z}_{d_1} \oplus \cdots \oplus \mathbf{Z}_{d_n}$, por
$e_i \to (\overline{0}, \ldots, \overline{0}, \overline{1}, \overline{0}, \ldots, \overline{0})$,
y por el primer teorema de isomorfía tenemos el resultado.

Proposición 44 *Si L grupo abeliano es $L \approx \boldsymbol{Z}^n$, y $L \approx \boldsymbol{Z}^m$, entonces $n = m$ (es decir $\boldsymbol{Z}^n \approx \boldsymbol{Z}^m \Leftrightarrow n = m$).*

DEMOSTRACIÓN:

Sea $2L = \{2x | x \in L\} < L$, si $L \approx \mathbf{Z}^n$ sean $x_i \leftrightarrow e_i \Rightarrow$

$2L \approx < 2e_1, \ldots, 2e_n >$, y $L/2L \approx \mathbf{Z}^n / < 2e_1, \ldots, 2e_n >$,

por el lema anterior

$$\frac{\mathbf{Z}^n}{< 2e_1, \ldots, 2e_n >} \approx \mathbf{Z}_2 \oplus \cdots \oplus \mathbf{Z}_2,$$

entonces $L/2L$ tiene 2^n elementos,

si suponemos $L \approx \mathbf{Z}^m$, $L/2L$ tendría 2^m elementos, luego $n = m$.

Sea G un grupo finitamente generado por $S = \{x_1, \ldots, x_n\}$, entonces como grupo generado por un número finito de generadores tenemos:

$$G \approx \frac{\mathbf{Z}^n}{H}$$

donde H es el grupo de las relaciones finitamente generadas, y podemos suponer que los generadores de H son;

$\{(a_{i1}, \ldots, a_{in})\}, i = 1, \ldots, r$, con $a_{i1}x_1 + \cdots + a_{in}x_n = 0, i = 1, \ldots, r$.

Llamaremos *rango de un grupo libre* al número n de generadores (minimal).

En esta sección demostraremos que:

$$G \approx \frac{\mathbf{Z}^n}{H} \approx \mathbf{Z}^{n-s} \oplus \mathbf{Z}_{d_1} \oplus \cdots \oplus \mathbf{Z}_{d_s}.$$

Torsión de un grupo.

Estudiaremos a continuación en un grupo abeliano la relación que incluye un solo elemento.

Definición 42 *Sea G grupo abeliano, $a \in G$ es de torsión si $o(a) < \infty$, es decir $\exists\ m \in \boldsymbol{N}$ con $ma = 0$. Llamaremos a $T(G) = \{a \in G$ de torsion$\}$ subgrupo de torsión de G.*

Definición 43 *Sea G grupo abeliano, G es libre de torsión si $T(G) = \{0\}$, es decir si $ma = 0$, con $a \neq 0 \Rightarrow m = 0$.*

Nota Todo grupo abeliano libre L es libre de Torsión, ya que al ser isomorfo a $\mathbf{Z}^n$ el orden de todo elemento no es finito.

EJEMPLO:

- Dado $\mathbf{Z} \oplus \mathbf{Z}_n$, su torsion $T(\mathbf{Z} \oplus \mathbf{Z}_n) = \mathbf{Z}_n$

En general, si G es suma directa interna, $G = L \oplus F$ con $L < G$ libre y $F < G$ finito, entonces $T(G) = F$, ya que si $x = x_1 + x_2 \in G$, $0 = mx = m(x_1 + x_2) = mx_1 + mx_2 \Rightarrow mx_1 = 0 \Rightarrow x_1 = 0$, ya que $mx_2 \neq -mx_1$ por ser suma directa interna y $L \cap F = \{0\}$.

La ausencia de elementos de torsión caracteriza los grupos libres.

Lema 2 *Sean $\{x_1, \ldots, x_r\}$ sistema de generadores de G abeliano, y existe una relación $m_1x_1 + \cdots + m_rx_r = 0$, $n_i \in \boldsymbol{Z} \Rightarrow$ existe $\{x'_1, \ldots, x'_r\}$ sistema de generadores de G, y $\exists\ q \in \boldsymbol{N}$ y i con $qx'_i = 0$.*

DEMOSTRACIÓN:

Si $r = 1$ el resultado es trivial.

Supongamos dos índices $1, 2$, y que $|m_1| \geq |m_2| \geq 0 \Rightarrow$
$m_1x_1 + m_2x_2 = (m_1 - m_2)x_1 + m_2(x_1 - x_2) = (m_1 + m_2)x_1 + m_2(x_2 - x_1)$

y $|m_1 - m_2|$ o $|m_1 + m_2| < |m_1| \Rightarrow$

existe $\{x_1, x_2 + x_1, \ldots, x_r\}$ o $\{x_1, x_2 - x_1, \ldots, x_r\}$ y relaciones

$(m_1 + m_2)x_1 + m_2(x_2 + x_1) + m_3x_3 + \cdots + m_rx_r = 0$, o

$(m_1 + m_2)x_1 + m_2(x_2 - x_1) + m_3x_3 + \cdots + m_rx_r = 0$

y para una de las dos la suma de los valores absolutos de los coeficientes

es menor que $m = |m_1| + |m_2| + \cdots + |m_r| > 0$.

Demostraremos el resultado por induccion en m,

primer caso, sea $m = 2$, la relación es $x_1 + x_2 = 0$, entonces

$x_1 + x_2 = (1 - 1)x_1 + (x_2 + x_1) = 0 \Rightarrow x_2' = x_2 + x_1 = 0$, con $q = 1$.

Supongamos cierto para coeficientes con suma de valores absolutos $< m$,

Veamos que es cierto para m, por lo anterior $\{x_1', \ldots, x_r'\}$, con $x_1' = x_1$,

$x_2' = x_2 - x_1$ o $x_2' = x_2 + x_1$, $x_i' = x_i$ para el resto es tal que

la suma de valores absolutos de las posibles relaciones son $< m$,

y por la hipótesis de inducción es cierto el resultado.

Teorema 34 *Sea E un grupo abeliano finitamente generado, entonces E es libre $\Leftrightarrow$ E es libre de torsión*

DEMOSTRACIÓN:

$\Rightarrow$) trivial.

$\Leftarrow$) Sea $\{x_1, \ldots, x_r\}$ un sistema de generadores de E con r mínimo,

veamos que no puede haber ninguna relación entre ellos:

si existe $m_1x_1 + \cdots + m_rx_r = 0$, por el lema anterior,

existe $\{x_1', \ldots, x_r'\}$ y $\exists\, q,\ i$, con $qx_i' = 0$, y como E es libre de torsión,

$x_i' = 0$ y existe un sistema de generadores con $r - 1$ elementos,

contradición con r mínimo.

Proposición 45 *Sea G grupo abeliano finitamente generado, $T(G)$ su torsión, sea $L' = G/T(G)$ y sean $\{e_1, \ldots, e_r\}$ tales que sus clases $\{\overline{e}_1, \ldots, \overline{e}_r\}$ generan L, sea $L =< e_1, \ldots, e_r >$, entonces G es suma directa interna $G = L \oplus T(G)$.*

DEMOSTRACIÓN:

$L' = G/T(G)$ es libre de torsión y finitamente generado $\Rightarrow$

(por el teorema anterior) L' es libre, y trivialmente L es libre.

$G = L + T(G)$, ya que $x \in G$, $\overline{x} = a_1\overline{e}_1 + \cdots + a_r\overline{e}_r \Rightarrow$

$x = a_1e_1 + \cdots + a_re_r + \omega$, con $\omega \in T(G)$, y como L es libre,

es libre de torsión, y $L \cap T(G) = \{0\}$,

y la suma es directa interna $G = L \oplus T(G)$.

Definición 44 *Sea G abeliano finitamente generado, entonces llamaremos rango de G a el rango del grupo libre $G/T(G)$.*

EJEMPLO:

- Dado $\mathbf{Z}^2 \oplus \mathbf{Z}_n$, su rango es 2.

Teoremas de estructura

Sea G abelianos finitamente generado por $\{x_1, \ldots, x_n\}$, entonces existe un homomorfismo

$\varphi : \mathbf{Z}^n \to G$ definido por $\varphi(e_i) = x_i$ suprayectivo, y por el primer teorema de isomorfía

$$\frac{\mathbf{Z}^n}{ker(\varphi)} \approx G$$

por tanto, para determinar G tenemos que saber determinar los subgrupos de un grupo libre. Veamos como se pueden expresar los subgrupos de un grupo libre.

Proposición 46 *Sea L un grupo abeliano libre de rango r y $L' < L \Rightarrow$ existe una base $\{e_1, \ldots, e_r\}$ de L, un $s \in \boldsymbol{N}$, con $s \leq r$, y $d_1, \ldots, d_s \in \boldsymbol{N}$, tales que $\{d_1e_1, \ldots, d_se_s\}$ es una base de L' y $d_i|d_{i+1}$, $1 \leq i < s$.*

DEMOSTRACIÓN:

Hacemos inducción en r, para $r = 1$, $G \approx \mathbf{Z}$ y sus subgrupos son $< de_1 >$, $e_1 = 1$.

Supongamos cierto para $r - 1$, y supongamos $V = \{v_1, \ldots, v_r\}$ base de

L, y $L' \subset < v_2, \ldots, v_r >$, entonces es cierto por hipótesis de inducción.

Supongamos ahora $L' \not\subset < v_2, \ldots, v_r >$, para toda base de L,

dada una base V definimos $p_v : L \to \mathbf{Z}$, $p_v(x = n_1v_1 + \cdots + n_rv_r) = n_1$,
y se tiene $p_v(L') \subset \mathbf{Z}$, y es no nulo ya que

$p_v(L') = 0 \Rightarrow L' \subset < v_2, \ldots, v_r >$, luego

para toda base de L, $\exists\, d_v$ con $p_v(L') =< d_v >$.

Consideremos V con d_v mínimo para L', y denotamos $d_v \equiv d_1$,

si $x' \in L$ es $x' = d_1v_1 + n'_2v_2 + \cdots + n'_rv_r$, podemos ver que

$d_1 | n'_j$, $2 \leq j \leq r$, y $\exists\, x \in L$ con $x' = d_1x$,

dividimos n'_j por d_1, $n'_j = c_jd_1 + k_j$ con $0 \leq k_j < d_1$, $0 \leq j \leq r \Rightarrow$

$x' = d_1(v_1 + c_2v_2 + \cdots + c_rv_r) + k_2v_2 + \cdots + k_rv_r$

y como $\{v_1 + c_2v_2 + \cdots + c_rv_r, v_2, \ldots, v_r\}$ es base de L y d_1 es mínimo $\Rightarrow$

$k_2 = \cdots = k_r = 0$ y $d_i | n'_j$, $0 \leq j \leq r$, y $x' = d_1x$.

Sea ahora $e'_1 \in L'$, verificando $p_v(e'_1) = d_1$, y sea $e_1 \in L$ con $e'_1 = d_1e_1 \Rightarrow$

$p_v(e_1) = 1$, y $\{e_1, v_2, \ldots, v_r\}$ es una base de L.

Veamos que $L' = (L' \cap < v_2, \ldots, v_r >) \oplus < d_1e_1 >$
(suma directa interna).

Es evidente que $L' = (L' \cap < v_2, \ldots, v_r >) \cap < d_1e_1 >= \{0\}$.

Comprobemos que $L' = (L' \cap < v_2, \ldots, v_r >) + < d_1e_1 >$,

sea $x' \in L'$, por definición de d_1, $\exists\, k$ con $p_v(x') = kd_1 \Rightarrow kd_1e_1 \in < d_1e_1 >$,

y $x' - kd_1e_1 \in (L' \cap < v_2, \ldots, v_r >)$ ya que

$x' - kd_1e_1 \in L'$ y $p_v(x' - kd_1e_1) = o \Rightarrow x' = (x' - kd_1e_1) + kd_1e_1$.

Por hipótesis de indución existe una base $\{e_2, \ldots, e_r\}$ de $< v_2, \ldots, v_r >$,
($\{e_1, \ldots, e_r\}$ es una base de L),

y existe $s \leq r$ y enteros positivos $d_2, \ldots, d_r$ con $d_i | d_{i+1}$, $2 \leq i \leq s-1$,

con $\{d_2e_2, \ldots, d_re_r\}$ base de $L' \cap < v_2, \ldots, v_r >$, entonces

como $L' = (L' \cap < v_2, \ldots, v_r >) \oplus < d_1e_1 >$, $\Rightarrow$

$\{d_1e_1, \ldots, d_se_s\}$ base de L'.

Para terminar basta ver que si $s > 1 \Rightarrow d_1|d_2$,

se demuestra tomando $x' = d_1e_1 + d_2e_2 \in L'$ y $p_e(x') = d_1$,

y por lo anterior d_1 divide al resto de los de x'.

Hemos visto anteriormente que $\frac{\mathbf{Z}^n}{ker(\varphi)} \approx G$, y como $ker(\varphi) < \mathbf{Z}^n$ por la proposición anterior

existen $d_1, \ldots, d_s \in \mathbf{N}$, tales que $\{d_1e_1, \ldots, d_se_s\}$ es una base de $ker(\varphi)$,

y $d_i|d_{i+1}$, $1 \leq i < s$. Entonces analogamente a lo anterior

$$\frac{\mathbf{Z}^n}{ker(\varphi)} \approx \mathbf{Z}^{n-s} \oplus \mathbf{Z}_{d_1} \oplus \cdots \oplus \mathbf{Z}_{d_s}.$$

Con lo anterior hemos demostrado el teorema siguiente:

Teorema 35 *Teorema de estructura de grupos abelianos finitamente generados. Sea G un grupo abeliano finitamente generado, entonces existen $d_1, \ldots, d_s \in \boldsymbol{N}$, únicos con $d_i|d_{i+1}$, $1 \leq i < s$, y*

$$G \approx \boldsymbol{Z}^{n-s} \oplus \boldsymbol{Z}_{d_1} \oplus \cdots \oplus \boldsymbol{Z}_{d_s}.$$

DEMOSTRACIÓN:

Por lo anterior falta ver solo la unicidad de los d_i.

Llamaremos a $d_1, \ldots, d_s$ *coeficientes de torsion* o *factores invariantes*, y $n - s$ es el rango de G

Teorema 36 *Teorema de estructura de grupos abelianos finitos. Sea G un grupo abeliano finito, entonces existen $d_1, \ldots, d_s \in \boldsymbol{N}$, únicos con $d_i|d_{i+1}$, $1 \leq i < s$, y*

$$G \approx \boldsymbol{Z}_{d_1} \oplus \cdots \oplus \boldsymbol{Z}_{d_s}.$$

Sabemos que si $d_j = p_{1j}^{k_{1j}} \cdots p_{rj}^{k_{rj}}$, con p_{ij} primos, tenemos

$$\mathbf{Z}_{d_j} \approx \mathbf{Z}_{p_{1j}^{k_{1j}}} \oplus \cdots \oplus \mathbf{Z}_{p_{rj}^{k_{rj}}}.$$

donde los $p_{rj}^{k_{rj}}$ solo dependen de d_j, y por tanto son únicos para G.

Llamaremos a $\{p_{rj}^{k_{rj}}\}$, $0 \leq j \leq s$, los *divisores elementales* del grupo finitamente generado (o finito) G y son únicos.

EJEMPLO:

Los distintos grupos salvo isomorfismos de un grupo con $n = 2^3 \cdot 5^2 \cdot 7$ elementos vienen determinadas por los posibles factores invariantes para n, que son:
$2^3 \cdot 5^2 \cdot 7$; $2^3 \cdot 5 \cdot 7, 5$; $2^2 \cdot 5^2 \cdot 7, 2$; $2^2 \cdot 5 \cdot 7, 2 \cdot 5$ $2 \cdot 5^2 \cdot 7, 2, 2$, $2 \cdot 5 \cdot 7, 2 \cdot 5, 2$, que dan

$$\mathbf{Z}_{2^3 \cdot 5^2 \cdot 7},\ \mathbf{Z}_{2^3 \cdot 5 \cdot 7} \oplus \mathbf{Z}_5,\ \mathbf{Z}_{2^2 \cdot 5^2 \cdot 7} \oplus \mathbf{Z}_2,\ \mathbf{Z}_{2^2 \cdot 5 \cdot 7} \oplus \mathbf{Z}_{2 \cdot 5},$$
$$\mathbf{Z}_{2 \cdot 5^2 \cdot 7} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2,\ \mathbf{Z}_{2 \cdot 5 \cdot 7} \oplus \mathbf{Z}_{2 \cdot 5} \oplus \mathbf{Z}_2,$$

Cálculo de sus coeficientes de torsión a partir de la presentación.

EJEMPLO:

Sean $G := \mathbf{Z}_{10} \times \mathbf{Z}_5$ y $S := \{e_1 = (1,0), e_2 = (0,1)\}$. Cada elemento $g \in G$ se escribe como $g = (\overline{x}_1, \overline{x}_2)$, donde $\overline{x}_1$ es la clase del entero x_1 en $\mathbf{Z}_{10}$ y $\overline{x}_2$ es la clase del entero x_2 en $\mathbf{Z}_5$. Por tanto $g = x_1 e_1 + x_2 e_2$, donde

$$e_1 = (\overline{1}, \overline{0}),\ \ e_2 = (\overline{0}, \overline{1}),$$

lo que implica, puesto que G no es cíclico, que S es un sistema generador minimal de G. Consideremos el homomorfismo suprayectivo

$$f : \mathbf{Z}^2 = \mathbf{Z} \times \mathbf{Z} \to G,\ (a,b) \mapsto ae_1 + be_2.$$

Por el primer teorema de isomorfía, $\mathbf{Z}^2 / \ker f \cong G$, y vamos a determinar el núcleo de f, que se denomina subgrupo de relaciones o subgrupo de sicígeas de G respecto de S y se denota $R_S(G)$. Denotamos $r_1 = (10,0)$ y $r_2 = (0,5)$, que evidentemente pertenecen a $\ker f$. Recíprocamente,

$$(a,b) \in \ker f \iff ae_1 + be_2 = (0,0) \iff (\bar{a},\bar{b}) = (\overline{0},\overline{0})$$
$$\iff \exists\, \alpha, \beta \in \mathbf{Z}, a = 10\alpha, b = 5\beta$$
$$\iff (a,b) = (10\alpha, 5\beta) = \alpha(10,0) + \beta(0,5) = \alpha r_1 + \beta r_2,$$

luego $\ker f = \langle r_1, r_2 \rangle$. Lo anterior se abrevia diciendo que

$$G := \langle e_1, e_2 :\ 10e_1 = 0, 5e_2 = 0 \rangle,$$

que nos da una presentación de G por generadores y relaciones con matriz de G respecto del sistema generador minimal S como

$$M_S(G) = \begin{pmatrix} 10 & 0 \\ 0 & 5 \end{pmatrix}$$

y observese que matriz codifica la presentación de G. Estas notaciones indican que G está generado por los elementos e_1, e_2, cuyos órdenes son 10 y 5 respectivamente.

Nota Sean G un grupo abeliano con notación aditiva y un sistema generador

$$S := \{x_1, \ldots, x_n\}$$

de G. Sean $\lambda_2, \ldots, \lambda_n \in \mathbf{Z}$ y denotamos

$$y_1 := x_1 + \sum_{j=2}^{n} \lambda_j x_j \quad \& \quad y_j := x_j \quad \forall\ 2 \leq j \leq n.$$

Entonces, el conjunto $T := \{y_1, \ldots, y_n\}$ es también un sistema generador de G, ya que

$$x_1 = y_1 - \sum_{j=2}^{n} \lambda_j y_j \in \langle T \rangle.$$

Veamos ahora en qué consiste el proceso inverso al seguido en el ejemplo anterior; se trata de reconocer un grupo abeliano finito a partir de una presentación suya.

EJEMPLO: Consideremos el grupo abeliano

$$G = \{x_1, x_2, x_3 : 6x_1 - 9x_2 - 3x_3 = 0,\ 24x_1 + 9x_2 + 9x_3 = 0,$$
$$42x_1 + 45x_2 + 27x_3 = 0\}$$

por tanto $S := \{x_1, x_2, x_3\}$ es un sistema generador de G y el subgrupo $R_S(G)$ de $\mathbf{Z}^3$ está generado por las relaciones

$$\{r_1 = (6, -9, 3),\ r_2 = (24, 9, 9),\ r_3 = (42, 45, 27)\}.$$

A lo largo del ejemplo modificaremos el sistema generador S de modo que la matriz de G respecto de otro sistema generador nos permita reconocer el grupo. En cada paso veremos cómo se refleja en la matriz el cambio de sistema generador. Inicialmente,

$$M_S(G) = \begin{pmatrix} 6 & -9 & -3 \\ 24 & 9 & 9 \\ 42 & 45 & 27 \end{pmatrix}$$

es importante observar que uno de los coeficientes de la matriz divide a los restantes. Este coeficiente es -3 y modificamos el sistema generador para que dicho coeficiente ocupe el lugar de la fila primera y la columna primera. Para ello definimos $y_1 := -x_3, y_2 := x_1, y_3 := x_2$. Por la Observación anterior el conjunto $S_1 = \{y_i : i = 1, 2, 3\}$ es un sistema generador de G y se cumple

$$\begin{cases} 3y_1 + 6y_2 - 9y_3 = 0 \\ -9y_1 + 24y_2 + 9y_3 = 0 \\ -27y_1 + 42y_2 + 45y_3 = 0 \end{cases}$$

en consecuencia,

$$M_{S_1}(G) = \begin{pmatrix} 3 & 6 & -9 \\ -9 & 24 & 9 \\ -27 & 42 & 45 \end{pmatrix}$$

el conjunto

$$S_2 = \{z_1 := y_1 + 2y_2 - 3y_3, z_2 := y_2, z_3 := y_3\}$$

es un sistema generador de G, y sacando factor común en la primera ecuación se tiene $3(y_1 + 2y_2 - 3y_3) = 0$, es decir, $3z_1 = 0$. Las ecuaciones segunda y tercera anteriores se leen

$$-9(y_1 + 2y_2 - 3y_3) + 42y_2 - 18y_3 = 0, \quad -27(y_1 + 2y_2 - 3y_3) + 96y_2 - 36y_3 = 0$$

como $3z_1 = 0$ también $9z_1 = 0$ y $27z_1 = 0$, por lo que las ecuaciones anteriores se reescriben como

$$\begin{cases} 3z_1 & & & = & 0 \\ & 42z_2 & - \; 18z_3 & = & 0 \\ & 96z_2 & - \; 36z_3 & = & 0 \end{cases}$$

y la matriz de G respecto del sistema generador S_2 es

$$M_{S_2}(G) = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 42 & -18 \\ 0 & 96 & -36 \end{pmatrix}.$$

esto implica que $G = \mathbf{Z}_3 \times H$ donde H es el grupo generado por z_2 y z_3, que cumplen las relaciones.

$$\begin{cases} 42z_2 - 18z_3 = 0 \\ 96z_2 - 36z_3 = 0 \end{cases} \rightsquigarrow \begin{cases} 18(2z_2 - z_3) + 6z_2 = 0 \\ 36(2z_2 - z_3) + 24z_2 = 0 \end{cases}$$

el conjunto $T := \{\zeta_1 = z_2, \zeta_2 := 2z_2 - z_3\}$ genera el grupo H y

$$\begin{cases} 6\zeta_1 + 18\zeta_2 = 0 \\ 24\zeta_1 + 36\zeta_2 = 0 \end{cases}$$

por tanto, la matriz de H respecto del sistema generador T es

$$M_T(H) = \begin{pmatrix} 6 & 18 \\ 24 & 36 \end{pmatrix}$$

también el conjunto $U := \{u_1 := \zeta_1 + 3\zeta_2, u_2 := \zeta_2\}$ genera H y estos generadores cumplen

$$\begin{cases} 6u_1 = 0 \\ 36u_2 = 0. \end{cases}$$

en consecuencia,

$$M_H(U) = \begin{pmatrix} 6 & 0 \\ 0 & 36 \end{pmatrix},$$

lo que implica que $H \cong \mathbf{Z}_6 \times \mathbf{Z}_{36}$. Finalmente,

$$G \cong \mathbf{Z}_3 \times H \cong \mathbf{Z}_3 \times \mathbf{Z}_6 \times \mathbf{Z}_{36}$$

por lo que los coeficientes de torsión del grupo G son $3, 6$ y 36.