Universidad de Granada

Álgebra I

Doble Grado de Informática y Matemáticas

Curso 2016/17

1. Anillo conmutativo

Definición (Anillo conmutativo). Un conjunto A es un anillo conmutativo si en él hay definidas dos operaciones; una aplicacion de adición y una aplicación de multiplicación, tales que cumplen las siguientes propiedades:

(*i*) Asociativa: $a + (b + c) = (a + b) + c$ $\quad a(bc) = (ab)c$

(*ii*) Conmutativa: $a + b = b + a$ $\quad ab = ba$

(*iii*) Existencia elemento neutro: $a + 0 = a$ $\quad a * 1 = a$

(*iv*) Existencia del elemento opuesto: $a + (-a) = 0$

(*v*) Distributiva del producto en la suma: $a(b + c) = ab + ac$

Definición (Grupo conmutativo). Denominamos un grupo conmutativo o abeliano a aquellos conjuntos que cumplen las propiedades asociativa, conmutativa y existencia de elemento neutro para la suma, y existencia de elemento opuesto.

Definición (monoide). Denominamos monoide a un conjunto con una operación binaria interna que cumple la propiedad asociativa y tiene un elemento neutro a izquierda y derecha. En el caso del producto, se denomina monoide multiplicativo.

Nota. Llamaremos anillo aquellos conjuntos que cumplan todas las propiedades excepto la propiedad conmutativa para la multiplicación.

Caracterización de $\mathbb{Z}_n$.

Llamaremos $R_n : \mathbb{N} \to \mathbb{Z}_n$ a la aplicación definida como:

$$R_n(a) = a - nq = a - nE(\frac{a}{n})$$

Para esta aplicación, definimos las siguientes propiedades:

- Si $0 \leq a < n - 1 \to R_n(a) = a$
- $\forall a, b \in \mathbb{N}$
    - $R_n(a + b) = R_n(R_n(a) + R_n(b))$
    - $R_n(ab) = R_n(R_n(a) * R_n(b))$

Una vez que tenemos definida una suma y producto con la aplicación R_n, definimos las suma y el producto de $\mathbb{Z}_n$.

Definición (Suma y producto en $\mathbb{Z}_n$). Se define la suma y el producto en $\mathbb{Z}_n$ de la forma:

- $a \oplus b = R_n(a + b)$
- $a \otimes b = R_n(ab)$

Es fácil verificar que $\mathbb{Z}_n$ es un anillo conmutativo con estas operaciones.

Definición (Unidad). Si A es un anillo conmutativo (a.c) $a \in A$ es una "**unidad**.º "**invertible**"si $\exists a^{-1}$ t.q. $aa^{-1} = 1$.
$U(A) = \{a \in A$ t.q. a es una unidad$\}$ = conjunto de las unidades de A.

Definición (Cuerpo). Se dice que A es un **cuerpo** si siendo un anillo conmutativo, $U(A) = A - \{0\}$, es decir, $\exists a^{-1}$ $\forall a \in A$ con $a \neq 0$.

Proposición (Asociatividad generalizada). *Sea A un anillo conmutativo, y $a_1 ... a_n$ una lista de elementos de A. La propiedad de la **asociatividad generalizada** nos dice que: $\forall m$ tal que $1 \leq m < n$ entonces:*

$$\sum_{i=1}^{n} a_i = (\sum_{i=1}^{m} a_i) + (\sum_{i=m+1}^{n} a_i)$$

$$\prod_{i=1}^{n} a_i = (\prod_{i=1}^{m} a_i)(\prod_{i=m+1}^{n} a_i)$$

Definición (Distributividad generalizada). Definimos también la distributividad generalizada en un anillo como:

$$(\sum_{i=0}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j \qquad \forall a, b \in A$$

Definición (Subanillo). Si A es un anillo conmutativo y B es un subconjunto de A. Se dice que B es un **subanillo** de A ($B \leq A$) si se verifican:

- $1, -1 \in B$
- B es cerrado para la suma y el producto.

Anillos de números cuadráticos

- $\mathbb{Z}[\sqrt{n}]$. Definimos este conjunto de la siguiente forma:

  $$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \in \mathbb{C} : a, b \in \mathbb{Z}\} \leq \mathbb{C}$$

  Podemos definir también $\mathbb{Q}[\sqrt{n}]$ de la misma forma:

  $$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} \in \mathbb{C} : a, b \in \mathbb{Q}\} \leq \mathbb{C}$$

  Se puede comprobar que $\mathbb{Z}[\sqrt{n}] \leq \mathbb{Q}[\sqrt{n}]$ y que $\mathbb{Q}[\sqrt{n}]$ es un cuerpo.

  Definición (Conjugado). Si $\alpha = a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$ se define su conjugado como $\bar{\alpha} = a - b\sqrt{n}$. Este verifica que:

  1. $\overline{(\alpha + \beta)} = \bar{\alpha} + \bar{\beta}$
  2. $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$
  3. $\alpha = \bar{\alpha} \Leftrightarrow b = 0$

  Definición (Norma). Se define entonces la Norma $N(\alpha) = \alpha\bar{\alpha} = a^2 - nb^2 \in \mathbb{Q}$. Así:

  1. $N(\alpha\beta) = N(\alpha) * N(\beta)$
  2. $N(\alpha) = 0 \iff \alpha = 0$

  Proposición. $\alpha \in a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ *es invertible* $\iff N(\alpha) \in \{-1, 1\}$

- Anillos de series.

  Definición. Si A es un anillo conmutativo y X es un símbolo que no denota ningún elemento de A. El anillo de series con coeficientes en A, denotado con A[[x]] esta definido como:

  $$A[[x]] = \{a = \textstyle\sum_{i=1}^{n} a_i x^i = a_0 + a_1 x^1 + ... + a_n x^n\} \ a_i \in A$$

  Y definimos la suma y el producto de la siguiente forma:

  $$(a + b) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

  $$(ab) = \sum_{k=0}^{n} \sum_{i=0}^{k} a_i b_{k-i}$$

Se puede probar que con estas operaciones de suma y producto, $A[[x]]$ es un anillo y $A[x]$ es un subanillo de $A[[x]]$

2. Homomorfismos

Definición. Si A, B son anillos conmutativos, una aplicacion $\varphi : A \to B$ es un homomorfismo si:

1. $\varphi(1) = 1$
2. $\varphi(a + b) = \varphi(a) + \varphi(b)$
3. $\varphi(ab) = \varphi(a)\varphi(b)$

Además, decimos que:

1. Es monomorfismo si es inyectivo.
2. Es epimorfismo si es sobreyectivo.
3. Es isomorfismo si es biyectivo.

Propiedades de los homomorfismos

- $\varphi(0) = 0$
- $\varphi(-a) = -\varphi(a)$
- $\varphi(\sum_{i=1}^{n} a_i) = \sum_{i=1}^{n} \varphi(a_i)$.

  $\varphi(\prod_{i=1}^{n} a_i) = \prod_{i=1}^{n} \varphi(a_i)$
- $\varphi(na) = n\varphi(a)$

Ya sabemos que $Im(\varphi) = \{\varphi(x) : x \in A\} \leq B$ es un subanillo.

Proposición. *Si φ es monomorfismo, entonces la aplicación restringida:*

$$A \to Im(\varphi)$$
$$a \mapsto \varphi(a)$$

es un epimorfismo y por ello es un isomorfismo, podemos decir que $A \cong Im(\varphi)$.

Nota. Se puede probar que $R_n : \mathbb{Z} \to \mathbb{Z}_n$ es un homomorfismo, llamado *Homomorfismo de reducción módulo n*

Proposición (1). *Dado A cualquier anillo conmutativo, conocido $A[x]$.*

Si $\varphi : A \to B$ es homomorfismo de anillos conmutativos, entonces:

$$\exists \varphi : A[x] \to B[x] : \varphi\left(\sum_i a_i x^i\right) = \sum_i \varphi(a_i) x^i$$

Proposición (Sustición en un polinomio)(2). *Si A es cualquier conjunto y $a \in A$ entonces: existe un homomorfismo $E_a : A[x] \to A$ tal que $E_a(\sum_i a_i x^i) = \sum_i a_i a^i$.*

Proposición (3). *Si $A \leq B$ es un subanillo y $b \in B$, la aplicación $E_b : A[x] \to B$ definida como $E_b(\sum_i a_i x_i) = \sum_i a_i b^i$ es un homomorfismo*

Proposición (Engloba a las anteriores). *Si $\varphi : A \to B$ es un homomorfismo y $b \in B$, la aplicación $\Phi : A[x] \to B$ definida como $\Phi(\sum_i a_i x_i) = \sum_i \varphi(a_i) b^i \in B$ es un homomorfismo*

Demostración. Veamos primero cómo (4) engloba a las demás:

(i) $4 \Rightarrow 3$. Se ve tomando como φ la inclusión en B

(ii) $4 \Rightarrow 2$. Tomamos esta vez como φ la identidad

(iii) $4 \Rightarrow 1$. Suponemos 4 válido. Probaremos que $\exists \varphi : A \to B[x]$ que lleva $a \to \varphi(a)$. Ahora, podemos ver que esa aplicación es como usar primero φ para ir de A a B y luego usar la inclusión de B en $B[x]$:

$$A \to B \to B[x]$$

$$a \to a \to \varphi(a)$$

De esta forma, tomamos $x \in B[x]$. Entonces:

$$\begin{gathered} A[x] \to B[x] \\ \textstyle\sum_i a_i x_i \to \sum_i \varphi(a_i) x_i \end{gathered}$$

Que es justamente el enunciado de la primera proposición.

Pasamos ahora a la demostración de la Proposición 4.

Sean $f = \sum a_i x_i$ y $g = \sum b_i x_i \in A[x]$. Entonces: $f + g = \sum c_i x_i$ con $c_i = a_i + b_i$

Si ahora aplicamos $\Phi(f + g) = \sum \varphi(c_i) b^i = \sum \varphi(a_i + b_i) b^i$.

Como φ es homomorfismo , eso es igual a: $\sum(\varphi(a_i) + \varphi(b_i)) b^i$.

Usando que B es un anillo y por ello hay distributividad, eso es igual a: $\sum(\varphi(a_i) b^i + \varphi(b_i) b^i$.

Por la asociatividad generalizada eso es igual a: $\sum \varphi(a_i) b^i + \sum \varphi(b_i) b^i = \Phi(f) + \Phi(g)$ Por lo que queda probado para la suma.

Ahora probaremos el producto:

$fg = \sum c_i x^i$ con $c_i = \sum_{i+j=n} a_i b_j$

Así:

$$\Phi(f + g) = \sum_n \varphi(c_n) b^n = \sum \varphi(\sum_{i+j=n} a_i b_j) b^n = \sum_n (\sum_{i+j=n} \varphi(a_i) \varphi(b_j)) b^n$$

Desarrollamos por otro lado

$$\Phi(f) + \Phi(g) = (\sum_i \varphi(a_i) b^i)(\sum_j \varphi(b_j) b^i) =^{(1)} \sum_{i,j} \varphi(a_i) b^i \varphi(b_j) b^j =^{(2)} \sum_{i,j} \varphi(a_i b_j) b^{i+j} =$$

$$= \sum_{n} (\sum_{i,j:i+j=n} \varphi(a_i b_j) b^n)$$

Donde en (1) hemos usado la distributividad general y en (2) hemos usado que estamos en un anillo conmutativo y que φ es un homomorfismo.

Así, hemos llegado a dos expresiones que son iguales, probando así el resultado.

□

Sabemos que cada polinomio $f(x)$ constituye una función de evaluación $f(x) \in A[x]$

$$f(x) : B \to B$$

$$b \to f(b)$$

Sin embargo, un polinomio es mucho más que la función de evaluación que él mismo define. Estudiaremos el caso $A[x_1, ..., x_r]$

Definición (Polinomios de r variables con coeficientes en A). Sea A un anillo conmutativo. Consideramos $A[x_1, ...x_r]$ inductivamente en r:
Si $r > 1$ entonces $A[x_1, ..., x_r] = A[x_1, ..., x_{r-1}][x_r]$

Demostración.

- $r = 1$:

$$f(x_1) \in A[x_1] \qquad \sum_{i \geq 0} a_i x_i \quad a_i \in A \quad \exists K : a_{i1} = 0 \;\; \forall i > K$$

- $r > 1$

$$f(x_1, ..., x_r) = \sum_{i1,...ir} a_{i1}, ..., a_{ir} x_1^{i1}, ..., x_r^{ir} : \quad \exists K : a_i, ..., a_r = 0 \iff i_s > K$$

Ahora, si vemos que:

$$f_{ir}(x_1, ..., x_{r-1}) = \sum_{i1,...ir>0} a_{i1}, ..., a_{ir} x_1^{i1}, ..., x_r^{ir-1} \in A[x_1, ..., x_{r-1}]$$

Entonces:

$$\sum_{ir \geq 0} f_{ir}(x_1, ..., x_{r-1}) x_r^{ir} = \sum_{ir \geq 0} (\sum_{i1,...,ir>0} a_1, ..., a_r x_1^{i1}, ..., x_{r-1}^{ir-1}) x_r^{ir} =$$

$$= \sum_{i1,...ir} a_{i1}, ..., a_{ir} x_1^{i1}, ..., x_r^{ir}$$

Ahora, definimos $g(x_1, ..., x_r) = \sum_{i1,...ir} b_{i1}, ..., b_{ir} x_1^{i1}, ..., x_r^{ir}$. Ahora, sumamos:

$$f(x_1, ..., x_r) + g(x_1, ..., x_r) = \sum_{i1,...ir} a_{i1}, ..., a_{ir} x_1^{i1}, ..., x_r^{ir} + \sum_{i1,...ir} b_{i1}, ..., b_{ir} x_1^{i1}, ..., x_r^{ir} =$$

$$= \sum_{i1,...,ir} (a_i + bi) x^{i1+ij}$$

Ahora, podemos desarrollar de la misma forma el producto y ver que:

$$(ax_1^{i1}, ..., x_r^{ir})(bx_1^{j1}, ..., x_r^{jr}) = abx_i^{i+j} x_2^{i_2+j_2} ... x_r^{i_r+j_r}$$

Por lo que queda probado nuestro resultado. □

Definición. (A[x][y])
Definimos $f = \sum f_i y^i | f_i \in A[x] : f_i = \sum_j a_{ij} x^j$
Luego, $f = \sum_i (\sum_j a_{ij} x^j) y^i = \sum_{i,j} a_{ij} x^i y^j$

Ahora, tomamos $g = \sum_{i,j} b_{ij} x^i y^j$ y sumamos:

$$f + g = \sum_{i,j} (a_{ij} + b_{ij}) x^i y^j$$

Y , si $A[x][y]$ es un anillo, vemos que la multiplicación se realiza:

$$(a_{ij} x^i y^j)(b_{mn} x^m y^n) = a_{ij} b_{mn} x^{i+m} y^{j+n}$$

Además, como es un anillo conmutativo $\Rightarrow A[x][y] = A[y][x] = A[x, y]$

Definición. $A[x_1, ..., x_n] = A[x_1, ..., x_{n-1}][x_n]$

Se puede probar que $A[x_1, ..., x_n] = A[x_{\sigma(1)}, ..., x_{\sigma(n)}]$ siendo σ una permutación de $\{1, 2, ..., n\}$

Proposición. *Si $\varphi : A \to B$ es un homomorfismo, $\forall (b_1, ..., b_n) \in B^n$ la aplicación:*

$$\Phi : A[x_1, ...x_n] \to B \iff \Phi : (\sum_{i1,...,in} a_1...a_n x^{i1}...x^{in}) = \sum_{i1,...,in} a_{i1}...a_{in} b^{i1}...b^{in} \in B$$

es un homomorfismo de anillos conmutativos. Es conocido como evaluación de un polinomio en n variables.

Proposición. *Si $\varphi : A \to B$ es un homomorfismo, $\forall b \in B \exists!$ homomorfismo definido como:*

$$\Phi : A[x] \to B : \begin{cases} \Phi(a) = \varphi(a) \forall a \in A \\ \Phi(x) = b \end{cases}$$

$$\Phi(\sum a_i x_i) = \sum \Phi(a_i x_i) = \sum \Phi(a_i)\Phi(x)^i = \sum \varphi(a_i) b^i$$

Además, ya se probó que esto es un homomorfismo de anillos conmutativos.

Corolario 1. *$A \leq B$ subanillo, $\forall b \in B\ \exists!$ homomorfismo*

$$E_b : A[x] \to B : \begin{cases} E_a(a) = a \quad \forall a \in A \\ E_b(x) = b \end{cases}$$

Nota. Si $f(x) \in A[x]$ denota un polinomio de $A[x]$, notaremos: $E_b(f(x)) = f(b)$. De la misma forma, si $f(x) = \sum a_i x^i \Rightarrow E_b(f(x)) = \sum a_i b^i$

Proposición (Evaluación en r-variables). *Si $\varphi : A \longrightarrow B$ es un homomorfismo de anillos conmutativos, y $b_1, \cdots, b_r \in B$ una lista ordenada. Entonces*

$$\exists! \phi : A[x_1, \cdots, x_r] \longrightarrow B : \begin{cases} \phi(a) = \varphi(a) \quad \forall a \in A \\ \phi(x_1) = b_1 \\ \vdots \\ \phi(x_r) = b_r \end{cases}$$

Demostración. Si $r = 1$, ya está probado. Para $r > 1$:

$$\exists \psi : A[x_1, \cdots, x_r] \longrightarrow B : \begin{cases} \psi(a) = \psi(a) \\ \psi(x_i) = b_i \forall i = 1, \cdots, r-1 \end{cases}$$

$$\exists \phi : A[x_1, \cdots, x_r] \longrightarrow B \begin{cases} \phi(a) = \psi(a) = \varphi(a) \\ \phi(x_i) = \psi(x_i) = b_i \forall i = 1, \cdots, r-1 \\ \phi(x_r) = b_r \end{cases}$$

¿Es único?

$$\phi(\sum_{i1,\cdots,ir} a_{1i} \cdots a_{ir} x_1^{i1} \cdots x_r^{ir}) = \sum_{i1,\cdots,ir} \varphi(a_{i1} \cdots a_{ir}) b_1^{i1} \cdots b_r^{ir}$$

$\square$

Proposición (Evaluación en subanillos r-variables). *Si $A \leq B, \forall b_1, \cdots, b_r \in B$ lista ordenada:*

$$\exists! E_{b_1,\cdots,b_r} : A[x_1, \cdots, x_r] \to B : \begin{cases} a \to a \\ x_i \to b_i \end{cases}$$

Se suele notar $f(x_1, \cdots, x_r) \to f(b_1, \cdots, b_r)$

3. Dominio de Integridad

Definición (Dominio de integridad). A es un dominio de integridad si verifica la propiedad:

$$a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \iff si\ ab = 0 \begin{cases} a = 0 \\ b = 0 \end{cases}$$

Proposición (Propiedad de simplificación). *A es un dominio de integridad $\iff$ $ax = ay$ con $a \neq 0 \Rightarrow x = y$*

Demostración. $\boxed{\Rightarrow}$ $a(x-y) = 0$, por ser A dominio de integridad, $x - y = 0 \Rightarrow x = y$
$\boxed{\Leftarrow}$ $ab = 0$ con $a \neq 0 \Rightarrow b = 0$ pues $a0 = 0; ab = a0; b = 0;$ □

Definición (Divisor de 0). $a \in A$ es divisor de 0 si $\exists b \neq 0 : ab = 0$

Proposición. *Si A es un dominio de integridad $\Rightarrow$ el 0 es el único divisor de 0.*

Equivalentemente: A es dominio de integridad $\iff$ no tiene divisores de cero no nulos.

(i) *$A \leq B$ y B es D.I. $\Rightarrow$ A es D.I.*

(ii) *Todo cuerpo es D.I.*

(iii) *Si $u \in U(A) \Rightarrow u$ no es divisor de 0 (Supongamos $u * b = 0 \Rightarrow u * u^{-1} * b = u^{-1} * 0 \Rightarrow b = 0$)*

Proposición. *Si $|A| < \infty$, A es dominio de integridad $\iff$ A es un cuerpo*

Demostración. $\boxed{\Leftarrow}$ Trivial
$\boxed{\Rightarrow}$ $0 \neq a \in A$. Tomo $\{1, a, a^2, \cdots, a^n\} = \{a^n : n \in N\} \subseteq A$ Como tiene cardinalidad finita: $\exists k \in N : a^n = a^{n+k}$.
Pero, por ello: $a^n = a^n a^k; a^n * 1 = a^n * a^k$, luego a^n no es 0 porque A es Dominio de integridad y por ser D.I entonces:

$$1 = a^k \begin{cases} k = 1 \Rightarrow a = 1 \\ k > 1 \Rightarrow a^{k-1} * a = 1 \end{cases}$$

Con lo que $\exists$ inverso de a $= a^{k-1}$ y como a es un elemento cualquiera, todo elemento tiene inverso, luego es un cuerpo. □

Proposición. *Todo D.I. es un subanillo de un cuerpo.*

Primero, presentaremos otros conceptos:

Definición (Cuerpo de fracciones de un D.I.). Sea A un dominio de integridad con $|A| \geq 2$. Consideramos $AxA - \{0\} = \{(a,b), a, b \in A \quad |b \neq 0\}$

Definición. Decimos que (a,b) es equivalente a (c,d): $(a,b) \sim (c,d) \iff ad = bc$

Esta relación es reflexiva, simétrica y transitiva.

Ahora, considero $a, b \in A$. Llamo $\frac{a}{b} = \{(c,d) \ \ c, d \in A : (c,d) \sim (a,b)\} \subseteq AxA - \{0\}$

Y llamo a $\frac{a}{b}$ la fracción a entre b.

Corolario 2.

$$\frac{a}{b} = \frac{u}{v} \iff av = bu \iff (a,b) \sim (u,v)$$

Demostración. $\boxed{\Rightarrow}$ $(a,b) \in \frac{a}{b} = \frac{u}{v} \Rightarrow (a,b) \sim (u,v) \Rightarrow (av = ub)$

$\boxed{\Leftarrow}$ $(a,b) \sim (u,v)$ Por la transitividad: $\frac{a}{b} \subseteq \frac{u}{v}$ y $\frac{u}{v} \subseteq \frac{a}{b} \Rightarrow \frac{a}{b} = \frac{u}{v}$ □

Ahora, llamamos $Q(A) = \{\frac{a}{b} | a, b \in A : \quad b \neq 0\}$ que es un conjunto de conjuntos, pues ya habíamos definido la fracción $\frac{a}{b}$ como un conjunto.

Sobre él, definimos unas operaciones que nos permitirán ver que es un cuerpo:

(i) Suma:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

Ahora, como la fracción $\frac{a}{b}$ es un conjunto, hay que probar que el resultado es único, es decir:

$$\frac{a}{b} = \frac{a'}{b'} \ \ y \ \ \frac{c}{d} = \frac{c'}{d'} \Rightarrow ab' = a'b \ \ y \ \ cd' = c'd$$

Hay que probar que se cumple:

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}$$

Equivalementente, tenemos que probar que se cumple:

$$b'd'(ad + cb) = bd(a'd' + c'b')$$

Desarrollamos en la izquierda:

$$b'd'(ad + cb) = b'd'ad + b'd'cb =^{(1)} a'bd'd + b'bc'd$$

Donde en (1) hemos usado la equivalencia que habíamos dado de $ab' = a'b$ y $cd' = c'd$. Ahora, desarollamos el producto de la derecha y veremos que es igual al resultado obtenido

$$bd(a'd' + c'b') = bda'd' + bdc'b' = a'bdd' + bb'c'd$$

Probando la unicidad.

(ii) Producto:
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

La unicidad del producto se hace desarrollando de la misma manera.

Para finalizar, se puede probar que es un cuerpo probando las propiedades de anillo conmutativo y que existe inverso para todo $\frac{a}{b}$.

Proposición (Fracciones de denominador 1). *Existe un homomorfismo*

$$\begin{aligned} i : & A \longrightarrow \mathbb{Q}(A) \\ & a \longmapsto \frac{a}{1} = i(a) \end{aligned}$$

Que cumple que $i(a+b) = i(a) + i(b)$ *y que* $i(ab) = i(a)i(b)$*, y además es un monomorfismo. Así,* $A \overset{i}{\cong} Img(i) = \{\frac{a}{1} : a \in A\}$ *es un isomorfismo y* $A \leq \mathbb{Q}(A)$ *con* $a = \frac{a}{1}$*. Con esta identificaión* $\frac{a}{b} = \frac{a}{1}\frac{1}{b} = ab^{-1}$

Proposición. *Sea* K *un cuerpo y* $A \leq K$*,* $a, b \in Ab \neq 0$*.*

$$\begin{aligned} &\Longrightarrow a \in K \ y \ b^{-1} \in K \implies ab^{-1} \in K \\ &\Longrightarrow \mathbb{Q}(A) \leq K \end{aligned}$$

Nota. Sea K un cuerpo. Entonces $\mathbb{Q}(K)$ es el cuerpo más pequeño que contiene a K.

Nota. $A \subseteq \mathbb{Q}(A), A = \text{D.I.} \implies \mathbb{Q}(\mathbb{Q}(A)) = \mathbb{Q}(A)$

Proposición. *Sea* K *un cuerpo,* $A \leq K$*. Si* $\forall \alpha \in K \quad \exists a \in A \quad a \neq 0 : a\alpha \in A \implies \mathbb{Q}(A) = K$

Demostración. $\alpha \in K$, $\exists a \in A \neq 0 : a\alpha = b \in A \implies \alpha = ba^{-1} = \frac{b}{a} \in \mathbb{Q}(A)$ □

Ejemplo: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\} \implies \mathbb{Q}(\mathbb{Z}[i]) = \mathbb{Q}[i]$

$$\alpha \in \mathbb{Q}[i] \implies \alpha = \frac{m}{n} + \frac{m'}{n'}i \implies \mathbb{Z}[i] \ni nn'\alpha = n'm + nm'i \in \mathbb{Z}[i]$$

Proposición. *Si* A *es un D.I.* $\implies A[x]$ *es un D.I.*

Definición (Grado de un polinomio). Si $f = \sum a_i x^i \neq 0 \implies gr(f) = n \in \mathbb{N}$ si $a_n \neq 0$ y $a_m = 0 \quad \forall m > n$

El coeficiente a_n se denomina coeficiente líder.

- Si A es D.I, $f, g \in A[x] \implies gr(fg) = gr(f) + gr(g)$

Definición (Divisibilidad en D.I.). Sea A un D.I. Sean $a, b \in A$. Decimos entonces que a divide a b (a es un divisor de b, b es un múltiplo de a):

$$\Longleftrightarrow \exists c \in A : b = ac \tag{1}$$
$$\Longleftrightarrow La \ ecuacion \ ax = b \ tiene \ solucion \tag{2}$$
$$\Longleftrightarrow \frac{b}{a} \in A \tag{3}$$

Demostración. $\boxed{\Longrightarrow}$ Si a divide a b $\implies \exists c : b = ac \implies \frac{b}{a} = \frac{ac}{a} = \frac{c}{1} = c \in A$
$\boxed{\Longleftarrow}$ si $\frac{b}{a} \in A \implies \frac{b}{c} = \frac{c}{1} \implies b = ac$ □

Notación: Si a divide a b, escribiremos a/b

(i) Los divisores de 1 son las unidades del anillo, los elementos del grupo $U(A)$

(ii) Las unidades son divisores de todos los elementos del anillo.

(iii) Dado $a \in A$, los elementos ua con $u \in U(A)$ se llaman *asociados de a.*

(iv) Si $u \in U(A)$, $\forall a \in A$, ua/a

Definición. Los divisores triviales de un número son las unidades y sus asociados.

Proposición. *Sean $a, b \neq 0$. Son equivalentes:*

*(*i) *a es asociado de b*

*(*ii) *b es asociado de a*

*(*iii) $a/b \wedge b/a$ *los asociados son los elementos que se dividen mutuamente*

Definición (Irreducible). Sea $a \in A, a \neq 0, a \notin U(A)$ es irreducible si sus únicos divisores son los triviales

$$\iff si \;\; b/a \implies b \in U(A) \vee b \sim a \tag{4}$$
$$\iff si \;\; a = bc \implies b \in U(A) \vee c \in U(A) \tag{5}$$
$$\iff si \;\; a = bc \implies a \sim b \vee c \sim a \tag{6}$$
$$\iff si \;\; a = bc \wedge b \notin U(A) \implies c \in U(A) \tag{7}$$

Propiedades elementales:

(i) Reflexión: a/a

(ii) Transitividad: $a/b \wedge b/c \implies a/c$

(iii) Si $a/b \vee a/c \implies a/bx + cy \;\; \forall x, y \in A$

(iv) Si $a/b \implies \;\; \forall c \;\; a/bc$

(v) Si $c \neq 0$ entonces $a/b \iff ac/bc$

4. Dominios euclídeos

Definición (Dominios euclídeos). Un dominio euclídeo es un dominio de integridad, A, tal que haya definida una función $\varphi : A - \{0\} \to \mathbb{N}$ verificando:

(i) $\varphi(ab) \geq \varphi(a)$

(ii) $\forall a, b \in A, \;\; b \neq 0 \quad \exists q, r \in A : a = bq + r$ con $r = 0 \vee \varphi(r) < \varphi(b)$

(iii) $\forall a, b \in A,\ b \neq 0 \quad \exists q \in A : a - bq = 0 \vee \varphi(a - bq) < \varphi(b)$

Nota. Si A es dominio euclídeo, entonces: $b/a \iff$ un resto de dividir a entre b es cero $\iff$ cualquier resto de dividir a entre b es 0

Demostración. $\boxed{\implies}$ Por definicion de b/a, $\implies \exists c \in A$ tal que $a = bc$ y por ser A un dominio euclídeo, $\implies \exists q, r \in A : a = bq + r$ con $r = 0 \vee \varphi(r) < \varphi(b)$. La solución es evidentemente correcta para $r = 0$, veamos que sucede para $r \neq 0$.
Supongamos $r \neq 0$, entonces $\varphi(r) < \varphi(b)$.

$$r = a - bq = bc - bq = b(c - q) \qquad c - q \neq 0$$

$$\varphi(r) = \varphi(b(c - q)) \geq \varphi(b) \implies \text{CONTRADICCIÓN}$$

□

Teorema (Teorema de Euclídes). *$\forall a, b \in \mathbb{Z}, b \neq 0, \exists q, r \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq r < b$*

Corolario 3. *$\mathbb{Z}$ es un dominio de euclídes con $\varphi = |.| : \mathbb{Z} \to \mathbb{N}$*

$$\varphi(a) \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

Pasamos a demostrar el teorema de Euclídes.
Demostración. Probaremos primero la unicidad. Supongamos

$$a = bq + r \qquad 0 \leq r < |b|$$

$$a = bq' + r' \qquad 0 \leq r' < |b|$$

distintos. Vamos a ver que $r = r'$ y $q = q'$

- Si $r \neq r'$, supongamos $r > r' \implies 0 < r - r' < |b|$ Ahora:

  $$r - r' = a - bq + a + bq' = b(q - q')$$

  $$r - r' > 0 \implies r - r' = |b(q - q')| = |b||q - q'|$$

  Pero, como $q \neq q' \implies q - q' \neq 0$ y $q, q' \in \mathbb{Z} \implies |q - q'| \geq 1$, luego:

  $$r - r' = |b||q - q'| \geq |b|$$

  Por lo que tenemos una contradicción con el comienzo de la suposición.

- Ahora, si $r = r' \implies b(q - q') = 0$ y $b \neq 0 \implies q - q' = 0 \implies q = q'$

Probamos ahora la existencia. Sean $a, b \geq 0$

- Si $a < b \implies a = 0 * b + a$, luego $q = 0$ y $r = a$, ya los tenemos
- Si $a \geq b$, llamamos $R = \{a - bx : x \in \mathbb{N} \quad a \geq bx\} \subseteq \mathbb{N}$ que es no vacío, pues está al menos $x = 1$.

  Ahora, por el Principio de buena ordenación, R tiene mínimo. Tomo $r = min(R)$.

  $r = a + bq$ para cierto $q \in \mathbb{N}$ y $r \geq 0$

  Veremos ahora que $r < b$, llegando a una contradicción.

  Supongamos $r \geq b \implies r' = r - b \geq 0 \implies r' = a - bq - b = a - b(q+1) \implies r' \in R$.

  Podemos ver que $r' < r$ (pues $r' = r - b$) $\implies$ está en R y es menor que el mínimo, luego es una contradicción y tenemos que $r < b$

Por último, vamos a probar que $0 \leq r < |b|$

Supongamos:

$$r = 0 \implies a = bq \begin{cases} -a = b(-q) \\ -a = (-b)q \\ a = (-b)(-q) \end{cases}$$

Ahora, supongamos $r > 0$:

- $-a = b(-q) - r = b(-q) - b + b - r = b(-q-1) + (b-r)$ y como $0 < r < b \implies b > b - r > 0$
- $-a = (-b)q - r = (-b)q + b - b - r = -b(q+1) + (b-r)$ y por el mismo motivo, $b > b - r > 0$
- $a = (-b)(-q) + r \implies 0 < r < b = |-b|$

De esta forma, hemos cubierto todos los casos y hemos acabado la demostración $\square$

Teorema. *$\forall f, g \in A[x]$ donde $g \neq 0$ y su coeficiente líder es una unidad de A, existen polinomios:*

$$q, r \in A[x] : f = gq + r \quad con \quad \begin{cases} r = 0 \\ gr(r) < gr(g) \end{cases}$$

y que son únicos.

Demostración. Sean : $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{m} b_i x^i$ con $b_m \in U(A)$

- Si $n < m \implies f = f * 0 + f \implies \exists q, r \in A[x] : f = gq + r$ con $g = 0$ y $r = f$
- Si $n \geq m$, razonamos por inducción en $n = gr(f)$
  - Si $n = 0 \implies m = 0$ por tanto $f = a_0$ y $g = b_0$ pero con $b_0 \in U(A)$

    De esta forma:

    $$f = a_0 = \frac{a_0}{b_0} b_0 = \frac{a_0}{b_0} b_0 + 0 = g \frac{a_0}{b_0}$$

    Podemos tomar como hemos visto $q = \frac{a_0}{b_0}$ y $r = 0$ y ya tenemos el q y r que buscábamos.

  - Si $n > 0$, haremos la inducción

    Vamos a considerar que $\frac{a_n}{b_m} = a_n b_m^{-1} \in A$ Tomamos entonces x^{n-m}.

    Consideramos $x^{n-m} g(x)$ y establecemos $f_1 = f - \frac{a_n}{b_m} x^{n-m} g$. Recordaremos esto como (1).

    Entonces, podemos ver que $gr(f_1) < n$. Por hipótesis te inducción $\implies$ $\exists q, r \in A[x] : f_1 = gq_1 + r$, que consideraremos como (2).

    Ahora, utilizando (1) y (2):

    $$\implies f = f_1 + \frac{a_n}{b_m} x^{n-m} g = gq_1 + \frac{a_n}{b_m} x^{n-m} g \frac{a_n}{b_m} x^{n-m} + r =$$

    $$g(q_1 + \frac{a_n}{b_m} x^{n-m}) + r$$

    Encontramos así el q y el r que queríamos, probando la existencia.

    Vamos a probar ahora la unicidad.

    Sea $f = gq + r$ y $f = gq' + r'$ con

    $$\begin{cases} r, r' \neq 0 \\ \quad o \\ gr(r) < m \\ gr(r') < m \end{cases}$$

    Ahora, si $r \neq r' \implies r - r' \neq 0 \implies r - r' = g(q - q') \neq 0$ Vemos que $gr(r - r') = gr(g) + gr(q - q')$.

    Como $q - q' \neq 0 \implies gr(q - q') \geq 0$ y de esta forma: $gr(g) + gr(q - q') \geq gr(g) = m$.

    Sin embargo, habíamos dicho que r, r' eran ambas de grado menor que m luego $gr(r - r') < m$, llegando a una contradicción y probando así el resultado.

□

Corolario 4. *Si K es un cuerpo, entonces $K[x]$ es un D.E con función euclídea:*

$$gr : K[x] \to N$$

(función que asigna a cada polinomio su grado)

Nota. Hacemos un el ejercicio de ver si $3x^2 + 1$ es divisor de $2x^3 + 4x^2 + 4x + 3$ en $\mathbb{Z}_5[x]$. (Solución: El resto de la división es 0, con resultado de la división $= 2/3x + 4/3$)

Teorema. *Los anillos $Z[\sqrt{n}]$ para $n = 2, 3, -1, 2$ son D.E. con función euclídea:*

$$\varphi : \mathbb{Z}[\sqrt{n}] \to \mathbb{N} : \varphi(a + b\sqrt{n}) = |N(a + b\sqrt{n})| = |a^2 - nb^2|$$

Demostración. Probaremos que $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ con $\beta \neq 0 \qquad \exists q, r \in \mathbb{Z}[\sqrt{n}] : \alpha = \beta q + r$ con $r = 0$ ó $|N(r)| < |N(\beta)|$:

- Si $|N(\alpha)| < |N(\beta)|$ Basta tomar $\alpha = 0 * \beta + \alpha$
- Si $|N(\alpha)| \geq |N(\beta)|$ consideramos entonces $\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{n}]$.

  Ahora, $\frac{\alpha}{\beta} = a_1 + a_2\sqrt{n}$ con $a_1, a_2 \in \mathbb{Q}$. Esos a_1, a_2 se obtienen usando el conjugado de β.

  Sean $q_1, q_2 \in \mathbb{Z} : |a_1 - q_1| \leq 1/2$ y $|a_2 - q_2| \leq 1/2$. Esto quiere decir que q_1 y q_2 son los enteros más cercanos a a_1, a_2 respectivamente.

  Sea $q = q_1 + q_2\sqrt{n}$ y $r = \alpha - \beta q$.

  Tomo $|N(r)| = |N(\alpha - \beta q)| = |N(\beta(\frac{\alpha}{\beta} + q)| = |N(\beta)||N(\frac{\alpha}{\beta} + q)|$

  Queremos probar que: $|N(\beta)||N(\frac{\alpha}{\beta} + q)| < |N(\beta)|$.

  Equivalentemente , queremos probar que:

  $$|N(\frac{\alpha}{\beta} + q)| < 1 \implies |N(a_1 + a_2\sqrt{n} - q_1 - q_2\sqrt{n})| = |N((a_1 - q_1) + (a_2 - q_2)\sqrt{n})| =$$

  $$= |(a_1 - q_1)^2 - n(a_2 - q_2)^2| = m \in \mathbb{Q}$$

  Vamos a probarlo para los casos que habíamos anunciado en el teorema, $n = -1, -2, 2, 3$

  - $n = -1 \implies m = (a_1 - q_1)^2 + (a_2 - q_2)^2 \leq 1/4 + 1/4 = 1/2 \implies |m| < 1$
  - $n = -2 \implies m = (a_1 - q_1)^2 + 2(a_2 - q_2)^2 \leq 1/4 + 1/2 = 3/4 \implies |m| < 1$
  - $n = -2 \implies m = |(a_1 - q_1)^2 - 2(a_2 - q_2)^2| \implies -1/2 \leq m \leq 1/4 \implies |m| < 1$
  - $n = 3 \implies m = |(a_1 - q_1)^2 - 3(a_2 - q_2)^2| \implies -3/4 \leq m \leq 1/4 \implies |m| < 1$

Por lo que queda probado el resultado para esos casos.

□

EJEMPLO: Vamos a tratar de dividir $\alpha = 6 + 10i$ entre $\beta = 1 + 2i$ en el anillo . Para ello, tenemos que saber si se puede hacer dicha división o no y para ello averiguaremos la norma de ambos números.

$$|N(6 + 10i)| = 36 + 100 = 136$$
$$|N(1 + 2i)| = 1 + 4 = 5$$

Como $1 + 2i$ tiene una norma menor que la norma $6 + 10i$ podemos hacer la división, para ello primero dividiremos como si fuesen numeros complejos normales para hallar nuestro número cociente que será de la forma $q = q_1 + q_2i$:

$$\frac{6+10i}{1+2i} = \frac{(6+10i)(1-2i)}{(1+2i)(1-2i)} = \frac{6-12i+10i+20}{5} = \frac{26-2i}{5} = \frac{26}{5} - \frac{2}{5}i$$

Tenemos que $5 < \frac{26}{5} < 6$ y 5 es más cercano a $\frac{26}{5}$ que 6 escogemos $q_1 = 5$ y por el mismo razonamiento $q_2 = 0$, de forma que $q = 5 + 0i = 5$. A continuación, para hallar el resto r hacemos la siguiente operación:

$$r = \alpha - \beta \cdot q = 6 + 10i - (1 + 2i)(5) = 6 + 10i - 5 - 10i = 1$$

Finalmente, comprobamos que no nos hemos equivocado:

$$(6 + 10i) = 5(1 + 2i) + 1|N(1)| < |1 + 2i| \implies 1 < 5$$

Viéndose así que el ejemplo está correcto.

5. Máximo Común divisor. Dominios de Ideales principales

Definición (Máximo común divisor). Dados $a, b \in A$ decimos que un elemento $d \in A$ es un mcd de a y b ($d = (a, b)$) si el conjunto de los divisores comunes a a y a b coinciden con el conjunto de los divisores de d. Esto es:

(i) d/a y d/b

(ii) Si c/a y $c/b \implies c/d$

Propiedades:

(i) $(a, b) = (b, a)$

(ii) Si $a \sim a'$ asociados y $b \sim b'$ también, $\implies (a, b) = (a', b')$

(iii) $(a,b)=a \iff a/b$. En particular, $(a,0)=a \quad , \quad (a,1)=1 \quad , \quad (a,u)=1 \iff u \in U(A)$

(iv) Si $(a,b)=1$, a y b se dicen primos relativos

(v) $((a,b),c)=(a,(b,c))=(a,b,c)$

(vi) $(ac,bc)=c(a,b)$

Demostración. Primero, llamamos $(ac,bc)=e$ y $(a,b)=d$.
Si a,b o c son 0, se verifica trivialmente. Si no lo son:

$$\left.\begin{aligned} d/a &\implies dc/ac \\ d/b &\implies dc/bc \end{aligned}\right\} \implies dc/e \implies \exists u \in A : e = dcu$$

$$\left.\begin{aligned} e/ac &\implies \exists x \in A : ac = ex \implies ac = dcux \implies = a = dux \\ e/bc &\implies \exists y \in A : bc = ey \implies bc = dcuy \implies b = duy \end{aligned}\right\} \implies \left.\begin{aligned} du/a \\ du/b \end{aligned}\right\} du/d$$

$$\implies \exists v \in A : d = duv \overset{d\neq 0}{\implies} 1 = uv \implies u \in U(A) \implies e \sim dc$$

□

(vii) Si c/a y $c/b \implies (\frac{a}{c}, \frac{b}{c}) = \frac{(a,b)}{c}$

(viii) $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$

(ix) Si $a/bc \implies a/(a,b)c$

Demostración. Supongamos que $\exists x \in A : bc = ax \implies (a,b)c = (ac,bc) = (ac,ax) = a(c,x) \implies a/(a,b)c$

□

(x) Si a/bc y $(a,b)=1 \implies a/c$

(xi) Si a/c y b/c y $(a,b)=1 \implies ab/c$

(xii) Si $(a,b)=1$ y $a/bc \implies a/c$

(xiii) Si a/c , b/c y $(a,b)=1 \implies ab/c$

(xiv) Si $a/c \implies \exists x : c = ax$. Y $b/c \implies b/ax$ con $(a,b)=1 \implies b/x \implies \exists y : x = by$
Entonces:

$$\begin{cases} c = ax \\ x = by \end{cases} \implies c = aby \implies ab/c$$

(xv) Si $(a,b)=1$ y $(a,c)=1 \iff (a,bc)=1$

Demostración. $\boxed{\implies}$ Sabiendo que: $(ac,bc)=c(a,b)=c$

Tenemos que: $1=(a,c)=(a,(ac,bc))=((a,ac),bc)=(a(1,c),bc)=(a,bc)$, por tanto: $1=(a,bc)$

$\boxed{\impliedby}$ $1=(a,bc)=(a(1,c),bc)=((a,ac),bc)=(a,(ac,bc))=(a,c(a,b))=(\frac{a}{(a,b)}(a,b),c(a,b)=(a,b)(\frac{a}{(a,b)},c)=1 \implies (a,b)\in U(A) \implies (a,b)=1 \implies (a,c)\in U(A) \implies (a,c)=1$ □

(xvi) $(a, b) = (a - kb, b)\ \forall k \in A$

(xvii) Si d/b, $d/a \iff d/(a - kb)$

Demostración. $\boxed{\Longrightarrow}$ Por la propiedad de combinación lineal se confirma.

$\boxed{\Longleftarrow}$ Igual que la otra implicación pero tomando $a = (a - kb) + kb$ □

Nota. En $\mathbb{Z}[\sqrt{n}]$ si α es un divisor propio de $\beta \implies N(\alpha)$ es un divisor propio de $N(\beta)$ en $\mathbb{Z}$.

Ejemplo: Realizamos un ejemplo en el que se puede probar que , usando la Nota anterior, 3 y)$1 + \sqrt{5}$) son irreducibles

Definición (Ideal/Ideal Principal). En un anillo se llama ideal a un subconjunto suyo no vacío que es cerrado para la suma y para múltiplos. Dicho de otra manera:
Si A es un anillo conmutativo, un subconjunto $\emptyset \neq I \subseteq A$, es un ideal si:

(i) $a, b \in I \implies a + b \in I$

(ii) $a \in I \implies ax \in I$

Si $a \in A$, $aA = (a)$ =$\{ax : x \in A\}$ es el ideal principal generado por a.

Definición ([DIP: Dominio de ideales principales). Un DIP es un anillo en el cual todo ideal es principal.

Teorema. *Todo dominio euclideo es un dominio de ideales principales: DE $\implies$ DIP*

Demostración. Sea A un DE con función euclidea $\varphi : A - \{0\} \longrightarrow \mathbb{N}$ y $I \subseteq A$ un ideal:

- Caso $I = \{0\} = (0) = 0A \implies$ trivial
- Consideremos $I \neq \{0\}$, $\emptyset \neq \{\varphi(x) : x \in I, x \neq 0\} \subseteq \mathbb{N}$, sea $\varphi(b)$ el mínimo de este conjunto, donde $b \in I, b \neq 0 \implies I = (b)$. Probamos esto con la doble inclusión:
  $\boxed{\subseteq}$ $b \in I \implies (b) \subseteq I$
  $\boxed{\supseteq}$ $a \in I$; $\exists q, r \in A : a = bq + r$. Supongamos que $r \neq 0 \implies r = a - bq \in I$ con $\varphi(r) < \varphi(b)$, esto es imposible puesto que b es el mínimo, luego $r = 0 \implies a \in (b) \implies I \subseteq (b)$

□

Teorema. *Si A es un DIP, $\forall a, b \in A \quad \exists d = (a, b)$. Además, $\exists u, v \in A : d = au + bv$. A esta igualdad se le llama Identidad de Bezout, y u y v son los coeficientes de Bezout, que no son únicos.*

Demostración. Sea $\emptyset \neq I(a, b) = \{ax + by : x, y \in A\} \subseteq A$

Vemos que:
$(ax + by) + (ax' + by') = a(x + x') + b(y + y') \implies$ cerrado para la suma.
$(ax + by)z = a(xz) + b(xz) \implies$ cerrado para el producto

Ahora, como es un ideal $\implies \exists d \in A : I(a, b) = (d)$ con $(d) = \{dx : x \in A\}$. $d \in I(a, b) \implies \exists u, v \in A : d = au + bv$.

Ahora, veamos que d es mcd de a y b.
$a \in I(a,b) \implies a \in (d) \implies d/a$
$b \in I(a,b) \implies b \in (d) \implies b/d$

Por lo que d es divisor común. Ahora, sea $c : c/a$ y $c/b \implies c/(au + bv = d) \implies c/d$. Hemos encontrado así un divisor común que es dividido por cualquier divisor común, por tanto es el mcd. □

Ecuaciones diofánticas en D.I.P.

En cualquier anillo, llamamos ecuaciones diofánticas a aquellas que son de la forma:

$$ax + by = c$$

(i) Sea $d = (a,b) \implies$ entonces la ecuación tiene solución $\iff d/c$

(ii) Supongamos que tiene solución. Supongamos también que $d = au + bv)\circledast$

$$\frac{a}{d} = a' \quad , \quad \frac{b}{d} = b' \quad , \quad \frac{c}{d} = c' \implies da'x + db'y = dc' \implies d(a'x + b'y) = dc'$$

$$\implies a'x + b'y = c'$$

Esta ecuación tiene las mismas soluciones que la ecuación diofántica inicial. Llamaremos a esta la ecuación 'reducida'.
$\circledast \quad d/a, \quad d/b \implies a = a'u + b'v$. Podemos hallar así los coeficientes de Bezout.

Como $c' = a'(c'u) + b'(c'v)$ y ahí tenemos una solución particular. Conociendo esta, podemos hallar TODAS las soluciones. Si llamamos$x_0 = c'u$ e $y_0 = c'v$

(iii) Solución general

$$\begin{cases} x = x_0 + kb' \\ y = y_0 - kb' \end{cases} \quad k \in A$$

Si (x_0, y_0) es la solución, entonces la solución general es el conjunto de los (x, y) que hemos dado arriba

Demostración de iii).

$$a'x + b'y = a'(x_0 + kb') + b'(y_o - kb') = a'x_0 + a'kb' + b'y_0 - a'kb' =$$

$$a'x_0 + b'y_0 = c'$$

Suponer ahora que (x,y) es cualquier solución: $\implies \quad a'x + b'y0c'$. Por hipótesis: $a'x_0 + b'y_0 = c'$. Si restamos esas dos ecuaciones queda: $a'(x - x_0) + b(y - y_0) = 0 \implies a'(x - x_0) = b(y_0 - y)$. Denotamos a esta ecuación como 3.

Ahora, $b'/(a'(x - x_0)$ pero b' y a' son primos entre sí, luego $b'/(x - x_0) \implies \quad \exists k \in A : (x - x_0) = kb'$. Llamamos a esta ecuación 1, y además despejando en ella vemos $x = x_0 + kb'$, una solución de x.

Análogamente, podemos ver que $a/(b(y_0 - y) \implies a/(y_0 - y) \implies \exists h \in A : y_0 - y = a'h \implies y = y_0 - ha'$, solución de y. Llamamos a esa ecuación la 2.

Falta probar que $k = h$, pero sustituyendo las ecuaciones 1 y 2 en 3, vemos que $a'kb' = b'ha' \implies k = h$

□

Proposición (Algoritmo de Euclides para el cálculo del MCD). *Supongamos que tenemos dos elementos a, b y queremos hallar su mcd.*

- *Si $b = 0 \implies (a, b) = (a, 0) = a$. Igual si $a = 0$*
- *Si $a \neq 0 \neq b$*

  Construimos una sucesión: $r_1, r_2, \cdots, r_n, \cdots, r_m, r_{m+1} = 0$.
  Recordamos que A es un D.E con función euclídea $\varphi : A - \{0\} \to \mathbb{N}$
  Si $\varphi(a) \geq \varphi(b) \implies r_1 = a$ y $r_2 = b$. En el otro caso, lo hacemos al revés, es decir $r_1 = b$ y $r_2 = a$.
  Si $r_{n-1} \neq 0 \implies r_n =$ resto de dividir r_{n-2} entre $r_{n-1} \implies$

$$r_{n-2} = r_{n-1}q_{n-2} + r_n \begin{cases} r_n = 0 \\ \varphi(r_n) \leq \varphi(r_{n-1}) \end{cases}$$

  La idea es ir reduciendo de la forma:

$$(a, b) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = \cdots = (r_m, r_{m+1}) = (r_m, 0) = r_m$$

  Obteniendo los cocientes de la forma:

$$\begin{cases} r_{n-2} = au_{n-2} + bv_{n-2} \\ r_{n-1} = au_{n-1} + bv_{n-1} \\ r_{n-2} - r_{n-1}q_{n-2} = r_n = a(u_{n-2} - q_{n-2}u_{n-1}) + b(r_{n-2} - q_{n-2}v_{n-1)} \\ \cdots \\ d = r_m = au + bv \end{cases}$$

Ejemplo: Un agricultor lleva al mercado 80 sandías y 30 melones. La venta le ha sido rentable, pues ha vendido cada pieza por más de 3 euros, que es lo que le costó producirlos. Vuelve a casa con 600 euros. Calcular precio de sandías y melones.
(El ejercicio se resuelve resolviendo la ecuación diofántica $80x + 30y = 600$, hallando primero la solución general que viene dada por $x = -60 + 3k$; $y = 180 - 8k$ y luego tomando que x e y tienen que ser mayores que 3, viendo que la solución es que $k = 22$).