Universidad de Granada

Álgebra I

Doble Grado de Informática y Matemáticas

Curso 2016/17

Índice

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 para la suma: $a + (-a) = 0$

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

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. $aa^{-1} = 1$.
$U(A) = \{a \in A : a \text{ es una unidad}\}$ = 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 $1 \leq m < n$ se verifican:*

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

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

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

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

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:

  $$A[[x]] = \{a = \textstyle\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x^1 + ... + a_n x^n\}\ a_i \in A$$

  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

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

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

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 (Homomorfismo de cambio de coeficientes)(1). *Dado A cualquier anillo conmutativo, conocido $A[x]$.*

Si $\varphi : A \to B$ es un 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 un anillo 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:

$$A[x] \to B[x]$$
$$\sum_i a_i x^i \to \sum_i \varphi(a_i) x^i$$

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 $c_n = \sum_{i+j=n} a_i b_j$

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

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

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

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.

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:*

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

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 $r > 1$:

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

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

¿Es único?

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

□

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 (anillo conmutativo) es un dominio de integridad si verifica la propiedad:

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

Proposición (Propiedad de simplificación). *A es un dominio de integridad $\iff$ se verifica: $ax = ay$ 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:

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

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 $A \leq K$, $a, b \in A$ $(b \neq 0)$.*

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

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

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, $f, g \in A[x] \implies gr(fg) = gr(f) + gr(g)$
  (Si no es D.I, tenemos que $gr(fg) \leq gr(f) + gr(g)$)

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):

$$\Rightarrow \exists c \in A : b = ac \tag{1}$$

$$\iff La\ \ ecuacion\ \ ax = b\ \ tiene\ \ solucion \tag{2}$$

$$\iff \frac{b}{a} \in A \tag{3}$$

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

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 $a \in A$(D.I), $a \neq 0, a \notin U(A)$ 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* $0 \leq r < |b|$

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 $a < b \implies a = b * 0 + a$, 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 $r' = r - b$) $\implies$ r' 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 $\square$

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

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

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

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

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 de inducción $\implies$ $\exists q, r \in A[x] : f_1 = gq_1 + r$, que consideraremos como (2).

    Ahora, utilizando (1) y (2):

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

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

    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.

$\square$

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

$$gr : K[x] - \{0\} \to \mathbb{N}$$

(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 $\mathbb{Z}[\sqrt{n}]$ 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 $\alpha = \beta * 0 + \alpha$
- 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 $\mathbb{Z}[i]$. 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 $q = q_1 + q_2 i$:

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

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. Ecuaciones Diofánticas en D.I.P

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, $(a,0) = a, \quad (a,1) = 1 \quad , \quad (a,u) = 1 \iff u \in U(A)$

(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. $\boxed{\implies}$ Por la propiedad de combinación lineal se confirma.

$\boxed{\impliedby}$ 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 euclídeo es un dominio de ideales principales: $DE \implies DIP$*

Demostración. Sea A un DE con función euclídea $\varphi : A - \{0\} \longrightarrow \mathbb{N}$ 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. $\square$

5.1. 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 $d = au + bv\circledast$

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

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

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

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

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).

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

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

Suponer ahora que (x,y) es cualquier solución: $\implies a'x + b'y = c'$. 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 $b'/(x-x_0) \implies \exists k \in A : (x - x_0) = kb'$. 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 $k = 22$).

6. Mínimo común múltiplo. Ecuaciones en congruencias.

Definición (Mínimo común múltiplo). Sea $a, b \in A = DI$
$m \in A$ es un mínimo común múltiplo de a y b, notando por $m = mcm(a, b) = [a, b]$
Si se verifica que el conjunto de los múltiplos comunes a ambos es igual al conjunto de múltiplos de m. Esto implica:

1. a/m *y* b/m
2. Si a/c y $b/c \Rightarrow m/c$

Del mismo modo se define para $[a_1, a_2, ..., a_r], r \in \mathbb{N}$.

Propiedades.

(i) Si $a \sim a'$ *y* $b \sim b' \Rightarrow [a, b] = [a', b']$

(ii) $[a, b] = [b, a]$

(iii) $[a, 0] = 0$

(iv) $[a, 1] = a$

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

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

Demostración del último. Supongamos que $c \neq 0$, pues si no es trivial.
Como $c/ab \implies c/[ca, cb] \implies \exists q \in A : [ac, bc] = cq \quad (1)$
Por otro lado, sea $m = [a, b]; \implies a/m \quad y \quad b/m \implies ac/mc \quad y \quad bc/mc \implies cq/mc$.
Como $c \neq 0 \implies q/m$.
Por otro lado, $ca/cq \quad y \quad cb/cq \implies$ como $c \neq 0 \implies a/q \quad y \quad b/q \implies m/q$.
Hemos llegado a que $q/m \quad y \quad m/q \implies$ son asociados $\implies q = [a, b]$.
Ahora, basta llevarnos esto a (1) en esta demostración para ver que:
$[ac, bc] = c[a, b]$ □

Proposición. *Si* A *es un DIP* $\implies \forall a, b \in A \quad \exists [a, b]$

Demostración. Consideramos $aA = (a)$, el ideal principal generado por a. De la misma forma, consideramos $bA = (b)$, el ideal principal generado por b.
Ahora, tomamos $aA \cap bA \implies$ los números que están simultáneamente en los múltiplos de ambos. Ahora, esto es cerrado para sumas y para productos, por tanto también es un ideal.
Por último, por estar en un DIP $\implies$ el ideal es principal y por tanto:
$\implies aA \cap bA = mA \implies m = [a, b]$ □

Teorema. *Sea* A *un DI en el cual* $\exists (a, b) \quad \forall a, b \in A$. *Entonces,* $\exists [a, b] \quad \forall a, b \in A$ *y se verifica que:* $[a, b](a, b) = ab$

Demostración. Sean $0 \neq a, b \in A$. Llamamos $d = (a, b) \implies \begin{cases} a = a_1 d \\ b = b_1 d \end{cases}$

Podemos observar que:

$$m = \frac{ab}{d} = a_1 b = a b_1$$

De esta forma, nuestra prueba termina si comprobamos que $m = [a, b]$. Tenemos ya que claramente $a/m \quad y \quad b/m$.

Sea $m_1 = a/m_1$ y b/m_1, tenemos que probar que m/m_1. Para esto, lo que hay que probar es que $(m, m_1) = m$.
Para ello, vamos a llamarlo $k = (m, m_1) \implies k/m$. Llamo $d_1 = \frac{m}{k} \implies m =_{(1)} d_1 k$ para un cierto d_1. Guardamos la igualdad de (1) para usarla después.
Ahora, lo que bastaría probar es que $d_1 \in U(A)$:
Tenemos que a/m y $a/m_1 \implies a/k \implies k = au$. Podemos hacer lo mismo con b para ver que $k = bv$. Esto ocurre para ciertos u y v.
Ahora, usando la igualdad del principio ($m = a_1 b = ab_1$) y el (1) podemos ver que

$$\left.\begin{array}{l} m = a_1 b = kd_1 = bvd_1 \implies a_1 = vd_1 \\ m = ab_1 = kd_1 = aub_1 \implies b_1 = ud_1 \end{array}\right\} \implies \left.\begin{array}{c} a = a_1 d = vd_1 d \\ b = b_1 d = ud_1 d \end{array}\right\} \implies d_1 d/a \quad d_1 d/b$$

$\implies d_1 d/d \implies \exists x \in A : d = dd_1 x \implies 1 = d_1 x \implies d_1 \in U(A)$.
$\implies m, k$ son asociados y como k era $mcd(m, m1) \implies$ m también lo es. □

6.1. Congruencias

Sea A un anillo, $I \subset A$ un ideal. $a, b \in A$ son 'congruentes módulo I' si $a - b \in I$ (Equivalentemente, si $\exists x \in I : a = b + x$). La notaremos:

$$a \equiv bmod(I) \quad o \quad a \equiv_I b$$

Otra notación. En un DIP $I = (m) = mA$

$$a \equiv bmod(mA) \rightarrow^{notacion} a \equiv bmod(m)(\iff m/a - b \iff a - b = qm)$$

Para algún q en el último paso, y en ese caso $\iff a = b + qm$ para algún q.

Propiedades

(i) $\equiv$ es una relación de equivalencia.

- $a \equiv a$
- $a \equiv b \iff b \equiv a$ (dem:$a - b = (-1)(b - a) \in I$)
- $a \equiv b$ y $b \equiv c \implies a \equiv c$ (dem: $a - b \in I, b - c \in I \implies a - c \in I$)

(ii) $a \equiv b \iff \forall c : a + c \equiv b + c$

(iii) $a \equiv b$ y $c \equiv d \implies a + c \equiv b + d$ (dem: usando 2 y 1)

(iv) $a \equiv 0 \iff a \in I$

(v) $a \equiv b \implies \forall c : ac \equiv bc$

(vi) $a \equiv b$, $c \equiv d \implies ac \equiv bd$ (dem: 5 y luego uso 1)

(vii) $ac \equiv bcmod(mc)$ y $c \neq 0 \implies a \equiv bmod(m)$

Demostración. $ac \equiv bcmod(mc) \iff mc/(a-b)c \iff {}^{c\neq 0}m/a-b \iff a \equiv bmod(m)$ □

(viii) Si $(c,m)=1$, entonces: $ac \equiv bcmod(m) \iff a \equiv bmod(m)$

Demostración. $ac \equiv bc \implies m/(a-b)c \implies$, como $(c,m)=1 \implies m/a-b$ □

6.2. Ecuaciones en Congruencias

Proposición (Ecuaciones en congruencias). *Estudiaremos la ecuación $ax \equiv bmod(m)$ (1)*

- *Si $m=0 \implies$ la ecuación es $ax=b$*
- *Si $a=0 \implies$ la ecuación es $0x \equiv 0mod(m) \implies$ tiene solución: todo el anillo*
- $a,b \neq 0$
  1. *Si $d=(a,m)$ la ecuación tiene solución $\iff d/b$*

     Demostración. (1), tiene solución $\iff \exists x \in A : ax \equiv bmod(m) \iff \exists x \in A : m/ax-b \iff \exists x,y \in A : (ax-b)=my \iff \exists x,y \in A : ax-my=b$, que es una ecuación diofántica, que sabemos ya que tiene solución $\iff d=(a,m)$ *y* d/b □

  2. *Supongamos que tiene solución. Consideramos $a'=\frac{a}{d}$, $b'=\frac{b}{d}$ y $m'=\frac{m}{d}$.*

     Ahora, usando $(1) = da'x \equiv db'mod(dm')$, esta es equivalente a $a'x \equiv b'mod(m')$ a la que llamaremos (2). Esta es su reducida. Tiene las mismas soluciones pero $(a',m')=1$.

     Podemos hallar los coeficientes de Bezout: $u,v \in A : 1 = a'u+b'v$. Esto nos lleva a ver que:

     $$a'u \equiv 1mod(m') \implies a'ub' \equiv b'mod(m')$$

     Y así tenemos que $x_0 = ub'$ es una solución particular.

  3. *La solución general es de la forma: $x = x_0 + km' \quad k \in A$. Equivalentemente, es de la forma $x \equiv x_0 mod(m')$*

     Demostración. Si x_0 es una solución particular $\implies a'x_0 \equiv b'mod(m')$
     Si sustituimos x_0 por x pues son congruentes obtenemos: $a'x \equiv b'mod(m')$.
     Vamos a suponer que:

     $$\left.\begin{array}{r} a'x \equiv b'mod(m') \\ a'x_0 \equiv b'mod(m') \end{array}\right\} \implies a'x \equiv a'x_0 mod(m')$$

     Por la transitividad. Pero a' y m' son primos entre sí, luego $x \equiv x_0 mod(m')$ □

4. *Diremos que una solución particular x_1 es óptima si $x_1 = 0$ ó $\varphi(x_1) < \varphi(m')$ siendo φ la función euclídea de A.*
   Si x_0 es cualquier solución particular, entonces:

$$x_0 = m'q + x_1 \begin{cases} x_1 = 0 \\ o \\ \varphi(x_1) < \varphi(m') \end{cases}$$

   Y x_1 es una solución parcial óptima. En este caso, la solución general óptima es: $x \equiv x_1 mod(m')$

6.3. Sistemas de Ecuaciones en Congruencias

En este caso, vamos a abordar un problema en el que tenemos un sistema de ecuaciones en congruencias, que sabemos que se puede expresar de la forma:

$$\left.\begin{array}{r} a_1x \equiv b_1 mod(m1) \\ a_2x \equiv b_2 mod(m2) \end{array}\right\} (1) \quad \left.\begin{array}{r} x \equiv amod(m) \\ x \equiv bmod(n) \end{array}\right\} (2)$$

Teorema (Teorema Chino). *El sistema tiene solución* $\iff a \equiv bmod((m, n))$

Demostración. Sea $d = (m, n)$.
Si tomamos $x = a + km$; $\exists k : a + km \equiv bmod(n) \iff km \equiv b - amod(n) \iff d/b - a \iff b \equiv amod(d)$ □

Ahora, supuesto que tiene solución, vamos a hallar las soluciones particular y general del problema.
Si y_0 es una solución particular de $my \equiv b - amod(n)$, entonces su solución general es:

$$y = y_0 + k\frac{n}{(m, n)} \quad k \in A$$

Entonces $x_0 = a + my_0$ es una solución particular del sistema dado en (2) y por tanto la solución general de 2 viene dada por:

$$x = a + m(y_0 + k\frac{n}{(m, n)}) \quad k \in A$$
$$= a + my_0 + k\frac{mn}{(m, n)} = x_0 + k[m, n] \quad k \in A$$
$$\implies x \equiv x_0 mod[m, n]$$

Pero si $x_0 = [m, n]q + x_1$ con $x_1 = 0$ ó $\varphi(x_1) < \varphi([m, n])$ entonces tenemos que

$$x_0 \equiv x_1 mod([m, n])$$

Y obtenemos que la solución general óptima de nuestro sistema es:

$$x \equiv x_1 mod([m, n])$$

Teorema (Teorema de Ruffini). *Si $f(x) \in A[x]$, $a \in A$ entonces $f(a) =$ resto de dividir f entre $x - a$. Equivalentemente, $f = (x - a)q + r$ donde $r \in A$. Así, $f(a) = r$.*

En forma de congruencias: $f \equiv f(a) mod(x - a)$.

7. Anillos de Congruencias. Conjuntos Cocientes

Sea A un anillo cualquiera. Sea también $I \subseteq A$ un Ideal de A.
Sabemos que $a \equiv b mod(I) \iff a - b \in I$. Vamos a denotar:

$$[a] = \{b : b \equiv a mod(I)\} = \bar{a} = a + I$$

Que sabemos que es un subconjunto de A y al que llamaremos la clase de congruencia de a.
Denotaremos también:

$$A/I = \{[a] : a \in A\}$$

Propiedades:

- $[a] = [b] \iff a \equiv b mod(I)$
- $[a] + [b] = [a + b]$
- $[a][b] = [ab]$
- Si $[a] = [a']$ y $[b] = [b'] \implies \begin{cases} [a + b] = [a' + b'] \\ [ab] = [a'b'] \end{cases}$

  Demostración. $a \equiv_I a'$ y $b \equiv_I b' \implies \begin{cases} a + b \equiv_I a' + b' \\ ab \equiv_I a'b' \end{cases} \implies \begin{cases} [a + b] = [a' + b'] \\ [ab] = [a'b'] \end{cases}$ □

- $[0] = I$

Proposición. *Si $f_i : A \to B$ es un homomorfismo de anillo, $Img(g) = \{f(a) : a \in A\} \leq B$ es un subanillo. Entonces, $Ker(f) = \{a \in A : f(a) = 0\}$ es un ideal.*
Demostración. Vamos a probar que este ideal es cerrado para sumas y para múltiplos. Para ello, en ambos casos usaremos que f es un homomorfismo.

$$Si f(a) = 0 \ y \ f(b) = 0,$$

$$f(a + b) = f(a) + f(b) = 0 + 0 = 0$$

$$f(ab) = f(a)f(b) = 0 * 0 = 0$$

□

Además, f es un monomorfismo $\iff Ker(f) = 0$
Demostración. $\boxed{\Rightarrow}$ Trivial
$\boxed{\Leftarrow}$ Si $f(a) = f(b) \implies f(a - b) = 0 \implies a - b \in Ker(f)$ pero hemos dicho que $Ker(f) = 0 \implies a - b = 0 \implies a = b$ □

Teorema (Teorema de Isomorfía). *Si $f : A \to B$ es un homomorfismo, se induce un isomorfismo de anillos:*

$$A/Ker(f) \cong Im(f)$$

$$F : [a] \longmapsto f(a)$$

Además, F está bien definida: es biyectiva y, por tanto, es un isomorfismo.
Demostración. Vamos a probar que está bien definida (inyectividad y sobreyectividad) y que es un homomorfismo.

Veamos primero que si $[a] = [b] \implies f(a) = f(b)$
Si $[a] = [b] \implies a \equiv bmod(Ker(f)) \implies a = x + b$ para algún $x \in Ker(f)$
$\implies f(a) = f(b + x) = f(b) + f(x) = f(b) + 0 = f(b)$

Vamos a ver ahora que es un homomorfismo $F : [a] \mapsto f(a)$

- $F([a] + [b]) = F([a + b]) = f(a + b)$ Pero como f es un homomorfismo por hipótesis $\implies f(a) + f(b) = F[a] + F[b]$
- $F([a][b]) = F([ab]) = f(ab)$ pero f vuelve a ser un homomorfismo, luego $f(a)f(b) = F[a]F[b]$
- $F(1) = f(1) = 1$

Probamos la inyectividad:
Suponemos $F[a] = F[b] \implies f(a) = f(b) \implies f(a - b) = 0 \implies a - b \in Ker(f) \implies a \equiv bmod(Ker(f)) \implies [a] = [b]$.

Probamos la sobreyectividad:
Sea $b \in Im(f) \implies \exists a \in A : f(a) = b \implies F[a] = f(a) = b$. Como f es sobreyectiva, $\forall b \in Im(f)$, $\exists [a]$ que se aplica en b. □

Proposición. *Sea A un Dominio Euclídeo con función euclídea $\varphi : A - \{0\} \to \mathbb{N}$ tal que en A hay unicidad de cocientes y restos (Esto es: $\forall a, b \in A : b \neq 0 \implies \exists! q, r \in A : a = bq + r \begin{cases} r = 0 \\ \varphi(r) < \varphi(b) \end{cases}$). Si seleccionamos un $b \in A, b \neq 0$ tal que $\varphi(1) < \varphi(b)$ entonces:*

$\forall a \in A, R_b(a) =$ resto de dividir a entre b; $R_b(a) = r \iff \begin{cases} a \equiv rmod(b) \\ r = 0 \quad o \quad \varphi(r) < \varphi(b) \end{cases}$

Ahora, llamaremos:

$$A_b = \{R_b(a) : a \in A\} \subseteq A$$

que cumple:

1. *Si $r \in A_b \implies R_b(r) = r$*
2. *$R_b(a + a') = R_b(R_b(a) + R_b(a'))$*

   Demostración. $R_b(a + a') \equiv a + a' \equiv_b R_b(a) + R_b(a') \equiv_b R_b(R_b(a) + R_b(a'))$ □
3. *$R_b(aa') = R_b(R_b(a)R_b(a'))$*

Además, se define la suma y el producto de $r, r' \in A_b$ de la forma:

- $r + r' = R_b(r + r')$
- $rr' = R_b(rr')$

Con estas operaciones, A_b es un anillo.

Se comprueba que si $f : A \to B$ es un isomorfismo, entonces:

Si $a \in U(A), \exists a^{-1} : aa^{-1} = 1 \implies f(a)f(a^{-1}) = f(1) = 1 \implies f(a) \in U(B)$

Así, surge la aplicación: $f : U(A) \to U(B)$ isomorfismo en la que si $b \in U(B) \implies \exists b^{-1} \in B : bb^{-1} = 1$

Pero también:
$$\left.\begin{matrix}\exists a \in A : f(a) = b \\ \exists a' \in A : f(a') = b'\end{matrix}\right\} f(aa') = f(a)f(a') = bb' = 1 \implies aa' = 1 \implies a \in U(A)$$

Definición (Divisores de Cero). Si a es divisor de cero de A, $\exists a' \neq 0 : aa' = 0 \implies f(a)f(a') = 0$ con $f(a') \neq 0 \implies f(a)$ es divisor de cero en B

Análogamente, surge el isomorfismo entre los divisores de cero de dos Anillos A y B:

$$f : DivCero(A) \to DivCero(B)$$

Si b es divisor de B y $b = f(a)$ para cierto $a \in A \implies a \in$ D. Cero de A.

$\implies \exists b' \neq 0 : bb' = 0$

Luego:

Si $b' = f(a') \implies f(a)f(a') = 0 \implies f(aa') = 0 \implies aa' = 0$ y con $a' \neq 0 \implies a$ es divisor de cero de A.

Proposición. *Sea A un D.E. con función euclídea φ donde hay unicidad en cocientes y restos y si $m \in A : m \neq 0$ y $\varphi(1) < \varphi(m)$.*

Consideramos $A_m = \{R_m(a) : a \in A\}$ donde, como ya sabemos, $\begin{cases} r + r' = R_m(r + r') \\ rr' = R_m(rr') \end{cases}$

Veamos que es un homomorfismo.

Demostración. $R_m(a+b) = R_m(a) + R_m(b) = R_m(R_m(a) + R_m(b))$ donde la primera suma es en A, la segunda es en A_m y la tercera dentro del paréntesis vuelve a ser en A
$R_m(ab) = R_m(a)R_m(b) = R_m(R_m(a)R_m(b))$ luego el producto también está bien definido.
Por último: $R_m(1) = 1$ por $\varphi(1) < \varphi(m)$ □

Además, $Im(R_m) = A_m$ y $Ker(R_m) = (m) = mA = \{mx : x \in A\}$.

También hay un isomorfismo:

$$A/(m) \cong A_m$$

$$[a] \mapsto R_m(a)$$

$$[r] \leftarrow\!\shortmid r$$

De esta forma, podemos llevarnos los problemas a otros anillos para facilitar su resolución.

Proposición. *Sea $a \in A$*

(i) $[a] \in U(A/(m)) \iff (a,m) = 1$

(ii) $a \in A_m$, *entonces* $a \in U(A_m) \iff (a,m) = 1$

(iii) *Todo elemento de $A/(m)$ es una unidad o divisor de cero*

(iv) *Todo elemento de A_m es una unidad o divisor de cero*

Demostración. Vamos a probar i) y iii). Luego ii) y iv) son consecuencia del isomorfismo entre $A/(m)$ y A_m.
Sea $[a] \in U(A/(m)) \iff \exists x \in A : [a][x] = [1] \iff \exists x \in A : ax \equiv 1 mod(m) \iff mcd(a,m) = 1$.

Sea $a \in A/(m) : a \notin U(A/(m)) \implies mcd(a,m) = d \neq 1$. Ahora, sea $a = da'$ y $m = dm'$ Pero m no divide a m' pues en otro caso: $m' = mx \implies m' = dm'x \implies 1 = dx \implies d \in U(A)$, contradicción. Ahora, tomo $[a][m'] = [am'] = [da'm'] = [a'm'] = [0]$ por ser un múltiplo de m' (congruencia módulo m'), así que [a] es divisor de cero. □

Corolario 5. *En las mismas condiciones, son equivalentes:*

(i) *m es irreducible*

(ii) *A/(m) ó (A_m) es DI*

(iii) *A/(m) ó (A_m) es un cuerpo*

Demostración. $\boxed{iii) \implies ii)}$ Todo cuerpo es un dominio de integridad.
$\boxed{ii) \implies iii)}$ Supongamos $[a] \in A/(m)$ si $[a] \neq [0]$ entonces, por la proposición anterior, a es una unidad.

$\boxed{i) \implies iii)}$ Sea $[a] \in A/(m), [a] \neq [0] = 0 \implies m$ no divide a $a \implies (a,m) = 1$, como m es irreducible, sus únicos divisores son m y 1 salvo asociados $\implies [a] \in U(A/(m))$

$\boxed{ii) \implies i)}$ Supongamos que m no es irreducible $\implies m = ab$ con a y b divisores propios $\implies m$ no divide a a y m no divide a $b \implies [a] \neq 0$ y $[b] \neq 0$ en $A/(m)$ pero $[a][b] = [ab] = [m] = [0] = 0$ y como [a] y [b] son distintos de cero $\implies A/(m)$ no es DI, en contradicción con la hipótesis. □

En $\mathbb{Z}_n$ si $p \geq 2$ es un irreducible y $\mathbb{Z}_p$ es un cuerpo. En general, si K es un cuerpo y $f(x) = \sum a_i x^i \in K[x]$ es de grado $n \implies K[x]_{f(x)}$ es un cuerpo $\iff f(x)$ es irreducible, con $K[x]_{f(x)} = \{b_0 + b_1 x + ... + b_{n-1} x^{n-1} : b_i \in K\}$

En particular, si p es un irreducible de $\mathbb{Z}$ y $f(x)$ es un irreducible de $\mathbb{Z}_p[x]$ de grado $n \implies \mathbb{Z}_p[x]_{f(x)}$ es un cuerpo con p^n elementos. Lo notamos $F_p n = \mathbb{Z}_p[x]_{f(x)}$

Salvo isomorfismos es el único cuerpo con p^n elementos , al variar p y n obtenemos todos los cuerpos finitos que existen.

7.1. Ecuaciones en $\mathbb{Z}_n$

Vamos a intentar ahora encontrar una solución para una ecuación $ax = b$ en $\mathbb{Z}_n$ con $a \neq 0$.

1. Tiene solución $\iff d = (a, n)/b$
2. Si tiene solución, tiene exactamente d soluciones distintas.

Demostración. Utilizaremos el siguiente isomorfismo para simplificar esta prueba: $\mathbb{Z}_n \cong \mathbb{Z}/(n)$.

1. $\exists x \in Z_n : ax = b \iff \exists [x] \in \mathbb{Z}/(n) : [a][x] = [b] \iff \exists x \in \mathbb{Z}/(n) : ax \equiv_n b \iff d/b$. Quedando probado 1.
2. Para demostrar 2., suponemos que d/b.
   Sean $a' = \frac{a}{b}, b' = \frac{b}{d}, n' = \frac{n}{d}$. Recuperamos la propiedad anterior, $a'x \equiv b'mod(n')$.
   De este expresión obtenemos la solución óptima: $x_0 : a'x_0 \equiv b'mod(n'), 0 \leq x_0 < n'$.
   Siendo la solución general, $x \equiv x_0 mod(n')$.
   Ahora, si $x = x_0 + kn' \quad k \in \mathbb{Z}$, los x que satisfacen nuestro problema original son los restos de estos elementos: $\{x_0,\ x_0 + n',\ x_0 + 2n', ...,\ x_0 + (d-1)n'\}$, si $k \in \mathbb{Z}, 0 \leq k < d \implies x_0 + kn' < \frac{n}{d} + (d-1)\frac{n}{d} = \frac{dn}{d} = n$. Por tanto, estas son las únicas soluciones.

   Podemos expresar las soluciones como $\{[x] \in \mathbb{Z}/(n) : x = x_0 + kn', k \in \mathbb{Z}\}$. Si $k \in \mathbb{Z}\ y\ k = qd + r\ con\ 0 \leq r < d,\ x_0 + kn' = x_0 + (qd + r)n' = x_0 + rn' + qdn' = x_0 + rn' + qn \implies [x_0 + kn'] = [x_0 + rn']$. Las soluciones de la ecuación original serán $\{[x_0],\ [x_0 + n'],\ [x_0 + 2n'], ...,\ [x_0 + (d-1)n']\} \subseteq \mathbb{Z}/(n) \cong \mathbb{Z}_n, \forall r, 0 \leq r \leq d-1$.
   $\{x_0,\ x_0 + n',\ x_0 + 2n', ...,\ x_0 + (d-1)n'\} \subseteq \mathbb{Z}_n$

□

8. Función de Euler.

$$\varphi : \mathbb{N} - \{0\} \longrightarrow \mathbb{N}$$

definida de la siguiente forma $\forall n \geq 1$:

$$\varphi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n \text{ y } (m, n) = 1\}|$$

Que es igual al número de naturales menores que n y primos con él.

Proposición. *Si* $(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$

Necesitamos algunos resultados para probar esto:

Definición (Anillo producto.). Si A y B son anillos:

$$A \times B = \{(a,b) : a \in A, b \in B\}$$

Donde se definen:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

$U(A \times B) = U(A) \times U(B)$

Nota. Un anillo producto nunca es un cuerpo.

Teorema (Versión clásica del teorema chino del resto.). *Si* $(m,n) = 1 \implies \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \iff \mathbb{Z}_{|(mn)} = \mathbb{Z}_{|(m)} \times \mathbb{Z}_{|(n)}$

Demostración.

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_{|(m)} \times \mathbb{Z}_{|(n)} \text{ es un homomorfismo de anillos.}$$
$$a \longmapsto ([a]_m, [a]_n)$$

Probaremos que es sobreyectivo:

$([b]_m, [c]_n)$ ¿$\forall b, c \in \mathbb{Z} \quad \exists a \in \mathbb{Z} : [a]_m = [b]_m$ y $[a]_n = [c]_n$?

¿$\forall b, c \in \mathbb{Z} \quad \exists a \in \mathbb{Z} : \begin{cases} a \equiv bmod(m) \\ a \equiv cmod(n) \end{cases}$? $\iff b \equiv cmod(m,n) \implies b \equiv_1 c$

Sí es sobreyectiva.

$ker(f) = (mn)$, pues m y n son primos entre sí. Ahora, como f es sobreyectiva, por el teorema de isomorfía tenemos el resultado. □

Corolario 6. *Si* $(m,n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$

Demostración. $\varphi(mn) = |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_{|m} \times \mathbb{Z}_{|n})| = |U(\mathbb{Z}_{|m}) \times U(\mathbb{Z}_{|n})| = \varphi(m)\varphi(n)$ □

Nota. Como sabemos (aunque no lo hayamos probado), si $n \in \mathbb{N}, n = p_1^{e_1} \dots p_n^{e_n}$ con $p_i \neq p_j$, p_i primo de $\mathbb{Z}$ (irreducible). Así, $\varphi(n) = \varphi(p_1^{e_1}) \dots \varphi(p_n^{e_n})$.

$\varphi(p^e) = p^e(1 - \frac{1}{p}) = p^e - p^{e-1}$

9. AQUI FALTA MAS CONTENIDO

10. Dominio de Factorización Única (DFU)

Un Dominio de Integridad A es llamado un DFU si $\forall a \in A, a \neq 0$ y $a \notin U(A)$, entonces $\exists$ irreducibles $q_1, ..., q_r \in A : a = q_1 ... q_r$ tales que la factorización es esencialmente única en el sentido de que si $q'_1, ..., q'_s \in A$ con q_j irreducible $\implies r = s$ y $\exists \sigma : \{1, ..., r\} \cong \{1, ..., r\}$ una permutación tal que si q'_i es asociado con $q_{\sigma(1)}$

Definición (Conjunto representativo de los irreducibles de A). Si A es un DFU, vamos a denotar $\mathcal{P} =$ un conjunto de representativos de los irreducibles de A. Entonces, $\forall p \in \mathcal{P}$ con p irreducible, entonces $\forall p, q \in \mathcal{P}$ no son asociados entre sí y $\forall p$ irreducible de A $\exists q \in \mathcal{P} : p \sim q$

Supongamos ahora que estamos en un DFU y hemos seleccionado un conjunto $\mathcal{P}$.

Si tenemos un $a \in A, a \notin U(A), a \neq 0$ entonces por definición existirán $q_1, ..., q_r \in A$ irreducibles tales que $a = q_1, ..., q_r$. Entonces, $\forall i = 1, ..., r \exists p_1, ..., p_r \in \mathcal{P} : q_i = u_i p_i$ con $u_i \in U(A)$. Así, a se puede expresar como: $a = (u_1...u_r)p_1...p_r$ pero todos los u_i son unidades del anillo, luego $\exists p_1, ..., p_r \in \mathcal{P}$ y$u \in U(A) : a = u(p_1...p_r)$. Esta descomposición es esencialmente única pero de forma más fuerte que antes. Además, es única salvo orden de escritura de los p_i

Ejemplo: En $\mathbb{Z}$ el -6 se puede escribir como $(-1) * 2 * 3$ ó como $(-1) * 3 * 2$

Estos p_i pueden repetirse, así que si agrupamos en términos obtenemos:

$\forall a \in A, a \neq 0 \exists p_1, ..., p_s \in \mathcal{P}$ con $p_i \neq p_j$, $e_1, ..., e_s \in \mathbb{Z}$ y $u \in U(A) : a = u(p_1^{e_1}...p_s^{e^s})$

Definición. Si $p \in \mathcal{P}$ y $a \in A, a \neq 0$ denotamos $e(p, a)$ como:

(*i*) exponente con que p aparece en la factorización de a, si aparece. $e(p_i, a) = e_i \quad i = 1, ..., s$

(*ii*) 0 en otro caso. $e(p, a) = 0 \quad \forall p \notin \{p_1, ..., p_r\}$

Vamos a asumir a partir de ahora que $a^0 = 1$ en cualquier anillo. Así, podemos ver que:

$$a \in A, \quad a = u(\prod_{p \in \mathcal{P}} p^{e(p,a)})$$

Propiedades:

(*i*) $e(p, ab) = e(p, a) + e(p, b)$.

Demostración. Con el a anterior y $b = v(\prod_{p \in \mathcal{P}} p^{e(p,b)})$. Entonces $ab = uv(\prod_{p \in \mathcal{P}} p^{e(p,a)+e(p,b)})$ □

(*ii*) $a, c \neq 0$ y $a/c \iff \forall p \in \mathcal{P}, \quad e(p, a) \leq e(p, c)$

Demostración. $\boxed{\Rightarrow}$ $\exists b : c = ab \implies \forall p \in \mathcal{P}, \quad e(p, c) \leq e(p, ab) = e(p, a) + e(p, b) \geq e(p, a)$

$\boxed{\Leftarrow}$ ¿Existe un b tal que $ab = c$?

Si c es: $c = v(\prod_{p \in \mathcal{P}} p^{e(p,b)})$

Si tomamos $b = (u^{-1}v)(\prod_{p\in\mathcal{P}} p^{e(p,c)-e(p,a)})$ Y multiplicamos por a por c, obtenemos b. □

Proposición. *En cualquier DFU existen mcd y mcm de cualesquiera elementos. Así:*

$$\forall a, b \neq 0 \quad (a,b) = (\prod_{p\in\mathcal{P}} p^{min\{e(p,a),e(p,b)\}})$$

$$[a,b] = (\prod_{p\in\mathcal{P}} p^{max\{e(p,a),e(p,b)\}})$$

Demostración. Probaremos el caso del mcd, el caso de mcd se hace de la misma forma. Vamos a llamar $d = (a,b)$. d divide a a porque $e(p,d) = min\{e(p,a), e(p,b)\}$ y por tanto a b también. Ahora, si tenemos un divisor común cualquiera , digamos $c \implies c/a$ y $c/b \implies e(p,c) \leq e(p,a), e(p,b) \implies e(p,c) \leq e(p,d) \implies c/d$ luego d es el máximo común divisor. □

Definición (Elemento Primo). Si A es un D.I. un elemento $p \in A, p \notin U(A), p \neq 0$ es llamado "primo"si se verifica la siguiente propiedad:

Si p no divide a un elemento a ni a un elemento b $\implies$ p no divide a su producto. Equivalentemente: si $p/ab \implies p/a$ o p/b

Proposición. (i) *Todo primo es irreducible en cualquier anillo A*

(ii) *Si A es un DFU, entonces todo irreducible es primo.*

Demostración. *(i)* Sea p un elemento primo. Supongamos que $p = ab$, producto de dos elementos, bastaría ver que uno de ellos es un asociado solo. Ahora, como $p/p \implies p/ab \implies p/a$ o $p/b \implies a \sim p$ o $b \sim p \implies$

(ii) $p \in \mathcal{P}$, veamos que p es primo.

Supongamos que p/ab. Veamos que p divide a a o a b. Si $p/ab \implies e(p,ab) \geq 1$ pero sabemos que $e(p,ab) = e(p,a) + e(p,b) \implies e(p,a) \geq 1$ o $e(p,b) \geq 1$. Si ocurre lo primero, p/a y si ocurre lo segundo p/b luego si p divide a un producto, entonces p divide a uno de los dos elementos del producto.

□

Teorema. *Sea A un D.I. Entonces, son equivalentes:*

(i) *A es un DFU*

(ii) a) *Todo elemento no nulo ni unidad de A factoriza como producto de irreducibles*

b) *Todo irreducible de A es primo*

(iii) a) *Idem*

b) $\forall a, b \in A$, $\exists$ $mcd(a,b)$

Demostración. Que 1 $\implies$ 2 es trivial. Veamos que 2 $\implies$ 1

Sea $a = p_1...p_r = q_1...q_s$ con p_i, p_q irreducibles. Vamos a ver que $r = s$. Para ello, vamos a hacer una inducción en r.

- Caso $r = 1 \implies p_1 = q_1...q_r$. Ahora, ¿puede ser $s > 1$?. Los q no son unidades, pues son irreducibles, por tanto si s fuese mayor que 1 serían los divisores propios de p_1 pero eso no puede ocurrir porque p_1 es irreducible. No puede ocurrir, por tanto $s = 1 = r \implies p_1 = q_1$
- Si $r > 1$ y usando la hipótesis de inducción, entonces $s > 1$.

  Nos fijamos en p_1, que es claro que divide a $a \implies p/(q_1...q_s) \implies {}^{p_1\ primo} \exists j : p_1/q_j$ y reordenando podemos suponer que p_1/q_1.

  Esto implica que $p_1 \sim q_1 \implies \exists u \in U(A) : q_1 = up_1$. Ahora nos podemos llevar la expresión a la igualdad de a($a = p_1...p_r = q_1...q_s$) $\implies p_1...p_r = up_1q_2...q_s$ y podemos reducir dividiendo por p_1 y nos queda $p_2...p_r = uq_2...q_s$.

  Ahora, usando la hipótesis de inducción, nos queda en cada lado $r-1$ elementos y $s-1$ elementos y por tanto $r-1 = s-1 \implies r = s$

Ahora, que 1 $\implies$ 3 es trivial. Como 1 y 2 son equivalentes, basta probar que 3 $\implies$ 2

Queremos probar que todo irreducible es primo. Sea p un irreducible. Supongamos que p no divide ni a a ni a b. Probaremos que entonces, no divide al producto ab

Es fácil ver que $(p, a) = 1$ y que $(p, b) = 1$. Ahora, por la propiedad del mcd que asegura que:

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

Entonces $(p, ab) = 1 \implies$ p es primo relativo con el producto por tanto p no divide al produco y así p es primo. □

Lema previo: En un DIP, toda cadena ascendente de ideales es estacionaria. En otras palabras, si A es un DIP, $I_1 \subseteq I_2 \subseteq ... \subseteq I_n$ es una sucesión de ideales creciente respecto a la inclusión(cada uno está incluido en el siguiente). $\implies \exists m : I_m = I_{m+1} = ... = I_{m+k} \quad k \geq 1$.

Demostración del lema. Podemos ver que:

$$I = U_{n \geq 1} I_n = \{a \in A : \exists n \ con \ a \in I_n\} \quad \forall a, b \in I \implies \exists n : a, b \in I_n$$

$$\implies a + b \in I_n \implies a + b \in I$$

Por ello, I es un ideal y por estar en un DIP, es principal $\implies \exists a \in A : I = (a) = \{ax : x \in A\}$. Que es no vacío, pues $a \in I$.

Si $a \in I$, en particular estará en alguno de los I_i de la unión: $\implies \exists m : a \in I_m \implies (a) \subseteq I_m$, pero $I = (a) \subseteq I_m \subseteq I_{m+k} \subseteq I \implies I_i = I_j$ para todo i y j.

□

Teorema. *Todo DIP es un DFU (Lo cual implica que todo DE es un DFU)*

Demostración. Tenemos que probar que en un DIP todo elemento se puede descomponer como producto de irreducibles. Para ello, vamos a negar la tesis. Supongamos que estamos en un DIP y que en ese anillo existen elementos que no son unidades y no se pueden descomponer como producto de irreducibles.

Supongamos que a es un elemento de esa 'clase'. Entonces $\exists\ a'$ divisor propio de a que también es de esa 'clase de elementos'.

Podemos asegurar que a no es un irreducible, pues no admite factorización en irreducibles y si fuera irreducible, él mismo sería una factorización como irreducibles. $\implies \exists b, c : a = bc$ con b y c divisores propios. Entonces, uno de los dos (b ó c) no puede admitir una factorización como producto de irreducibles, pues si no, a admitiría esa factorización. Entonces, llamamos a' a b o a c según sea el que no admita esa factorización.

Ahora, vamos a construir una sucesión $\{a_n\} \in A$ con $a_1 = a$. Cada elemento siguiente, es un divisor propio del anterior y es de la 'clase' que establecimos al principio (no es cero, ni una unidad, ni se puede factorizar en producto de irreducibles). Esto implica que $a_{n+1} = a'_n$ y a_{n+1} no es sociado con a_n.

Si consideramos los ideales principales generados por los elementos de esta sucesión, y podemos ver que (como a_{n+1} es divisor de a_n:

$$\implies (a_1) \subset (a_2) \subset ... \subset (a_n) \subset (a_{n+1})$$

Y en esta acena no hay igualdades, pues si $(a_n) = (a_{n+1}) \implies a_{n+1} \in (a_n) \implies a_n/a_{n+1}$ y esto no puede ocurrir.

Pero esto contradice el lema que hemos visto anteriormente, por tanto hemos probado así que todos los elementos deben tener una factorización y por tanto estamos en un DFU. $\square$