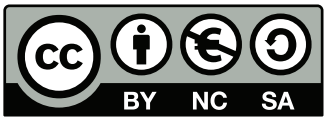
Álgebra I

LibreIM

Doble Grado de Informática y Matemáticas
Universidad de Granada

libreim.github.io/apuntesDGIIM



Álgebra I

LibreIM

Doble Grado de Informática y Matemáticas
Universidad de Granada

libreim.github.io/apuntesDGIIM

Índice

Teoría

Anillo conmutativo

Definición 1.1 (Monoide). Un monoide es un par $(X, \cdot)$, donde X es un conjunto y $\cdot$ es una aplicación $\cdot : X \times X \to X$ con las siguientes propiedades:

(*i*) Asociatividad: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall a, b, c \in X$

(*ii*) Existencia de elemento neutro: $\exists e \in X : a \cdot e = e \cdot a \ \forall a \in X$

En ocasiones, si la operación $\cdot$ queda clara por el contexto, se dirá simplemente que "X es un monoide".

Nótese que la definición de $\cdot$ implica la *clausura* de la misma, es decir, para cualesquiera $a, b \in X, a \cdot b \in X$.

Un grupo se define similarmente, como un conjunto con una operación y ciertas propiedades.

Definición 1.2 (Grupo). Un grupo es un monoide $(X, \cdot)$, con la siguiente propiedad adicional:

- Existencia de elementos inversos: $\forall a \in X \ \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$, donde e es el elemento neutro de X como monoide con $\cdot$.

Definición 1.3 (Monoide conmutativo). Un monoide $(X, \cdot)$ se dice *conmutativo* o *abeliano* si $\cdot$ es una aplicación simétrica.

Definición 1.4 (Grupo conmutativo). Un grupo $(X, \cdot)$ se dice *conmutativo* o *abeliano* si $\cdot$ es una aplicación simétrica.

Definición 1.5 (Anillo). Un anillo es una tripla $(X, +, \cdot)$ tal que:

(*i*) $(X, +)$ es un grupo conmutativo.

(*ii*) $(X, \cdot)$ es un monoide.

(iii) $\cdot$ es distributiva a izquierda y a derecha respecto de $+$:

$$\begin{cases} (a+b)\cdot c = (a\cdot c)+(b\cdot c) \\ c\cdot(a+b) = (c\cdot a)+(c\cdot b) \end{cases} \quad \forall a,b,c \in X$$

Definición 1.6 (Anillo conmutativo). Un anillo $(X,+,\cdot)$ se dice *conmutativo* o *abeliano* si $(X,\cdot)$ es un monoide conmutativo.

Nótese que en este caso, la distributividad de $\cdot$ a izquierda y a derecha son dos propiedades equivalentes.

Nota. En todas las estructuras provistas de una operación de las notadas con $\cdot$, se notará $a\cdot b = ab$.

Caracterización de $\mathbb{Z}_n$

Si $a,n \in \mathbb{Z}$, entonces existen $q,r \in \mathbb{Z},\ 0 \leq r < n$ tales que:

$$a = qn + r$$

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

$$R_n(a) = a - qn = a - nE\left(\frac{a}{n}\right)$$

Para esta aplicación, observamos 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 observadas estas propiedades de la aplicación R_n, definimos las suma y el producto de $\mathbb{Z}_n$.

Definición 1.7 (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 1.8 (Unidad). Si A es un anillo conmutativo (a.c.) $a \in A$ es "una unidad" o "invertible" si $\exists a^{-1}$ tal que $aa^{-1} = 1$.

El conjunto de las unidades de A se nota $U(A) = \{a \in A : a \text{ es una unidad}\}$.

Definición 1.9 (Cuerpo). Se dice que A es un cuerpo si siendo un anillo conmutativo, $U(A) = A - \{0\}$, es decir, $\forall a \in A \ \exists a^{-1}$ con $a \neq 0$.

Proposición 1.1 (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:

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

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

Proposición 1.2 (Distributividad generalizada). Se tiene la propiedad análoga a la asociatividad generalizada para la distributividad:

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

Definición 1.10 (Subanillo). Si A es un anillo conmutativo y $B \subseteq A$, se dice que B es un subanillo de A ($B \leq A$) si $\left(B, +\big|_{B\times B}, \cdot\big|_{B\times B}\right)$ es un anillo conmutativo y $1 \in B$.

Esto equivale a:

- $1, -1 \in B$
- 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 1.11 (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 1.12 (Norma). Si $\alpha \in \mathbb{Z}[\sqrt{n}]$ o $\alpha \in \mathbb{Q}[\sqrt{n}]$, se define 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 1.3. $\alpha = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ es invertible $\iff N(\alpha) \in \{-1, 1\}$

Anillos de series.

Definición 1.13. 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:

$$A[[x]] = \left\{ a = \sum_{n\in\mathbb{N}} a_n x^n, a_n \in A \ \forall n \in \mathbb{N} \right\}$$

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

$$(a + b) = \sum_{n\in\mathbb{N}} (a_n + b_n)x^n$$

$$(ab) = \sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$$

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

Homomorfismos

Definición 2.1. Si $(A, +, \cdot), (B, \ddagger, *)$ son anillos conmutativos, una aplicación $\varphi : A \to B$ es un homomorfismo si:

1. $\varphi(1_A) = 1_B$, donde 1_A y 1_B son los elementos neutros de $\cdot$ en A y $*$ en B, respectivamente.
2. $\varphi(a + b) = \varphi(a) \ddagger \varphi(b)$
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

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

Estas propiedades nos dicen que $\text{img}(\varphi) = \{\varphi(x) : x \in A\} \leq B$ es un subanillo.

Proposición 2.1. Si φ es monomorfismo, entonces la aplicación restringida:

$$A \to \text{img}(\varphi)$$

$$a \mapsto \varphi(a)$$

es un epimorfismo y por ello es un isomorfismo, podemos decir que $A \cong \text{img}(\varphi)$.

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

Definición 2.2 (Anillo de polinomios sobre un anillo conmutativo). Sean A un anillo conmutativo y x un símbolo que no denote ningún elemento de A. Entonces se define el anillo de polinomios sobre A (también "con coeficientes en A") como:

$$A[x] = \{a_n x^n + \cdots + a_1 x + a_0 : n \in \mathbb{N}, a_i \in A \ \forall i \in \{0, \ldots, n\}\}$$

Las operaciones de suma y producto en $A[x]$ son las usuales. Con las convenciones de que $x^0 = 1, x^1 = x$ y $\sum_{i=m}^{n} a_i = 0$ si $m > n$:

$$\begin{array}{rcl} \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i & = & \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i, \text{ con } m \leq n. \\ \left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) & = & \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k \end{array}$$

$A[x]$ es un subanillo de $A[[x]]$ (los elementos de $A[x]$ son los de $A[[x]]$ para los que $a_n = 0$ a partir de un cierto $n \in \mathbb{N}$).

Proposición 2.2 (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:

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

Proposición 2.3 (Sustitución 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 2.4 (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 2.5 (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 $\exists \psi : A \to B[x]$ que lleva $a \mapsto \psi(a) = \varphi(a)$. En efecto, basta tomar $\psi = i_{B[x]} \circ \varphi$, donde $i_{B[x]} : B \to B[x]$ es la inclusión en $B[x]$.

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

$$\begin{array}{ccc} A[x] & \to & B[x] \\ \sum_i a_i x^i & \mapsto & \sum_i \varphi(a_i) x^i \end{array}$$

es un homomorfismo, 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 $g = \sum b_i x^i \in A[x]$. Si ahora aplicamos $\Phi(f+g) = \sum \varphi(a_i + b_i) b^i$, 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, 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. Recordemos que, de la definición:

$$fg = \sum c_k x^k \text{ con } c_k = \sum_{i+j=k} a_i b_j$$

Así:

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

Desarrollamos por otro lado

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

$$=^{(2)} \sum_{i,j} \varphi(a_i b_j) b^{i+j} = \sum_n \left(\sum_{i,j : i+j=n} \varphi(a_i b_j) b^n \right)$$

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 $f(x) \in A[x]$

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

$$b \mapsto f(b)$$

Sin embargo, un polinomio es mucho más que la función de evaluación que él mismo define.

Estudiaremos el anillo de polinomios en varias variables.

Definición 2.3 (Monomio en r variables). Sean A un anillo conmutativo, $p_1, \ldots, p_r \in \mathbb{N}$ y $x_1, \ldots, x_r$ símbolos que no denoten ningún elemento de A. Entonces

$$\prod_{i=1}^{r} x_i^{p_i}$$

es un monomio en r variables con coeficientes en A. Si $p = (p_1, \ldots, p_r)$, denotamos $X^p = \prod_{i=1}^{r} x_i^{p_i}$.

Definición 2.4 (Anillo de polinomios en r variables sobre un anillo conmutativo). Sean A un anillo conmutativo y $x_1, \ldots, x_r$, con $r \in \mathbb{N}$ símbolos que no denoten ningún elemento de A. Entonces, se define el anillo de polinomios en r variables sobre A como

$$A[x_1, \ldots, x_r] = \left\{ \sum_{i=1}^{n} b_i X^{p_i} : \begin{array}{l} B = \{b_1, \ldots, b_n\} \subseteq A \\ P = \{p_1, \ldots, p_n\} \subset \mathbb{N}^r \\ n \in \mathbb{N} \end{array} \right\}$$

Es decir, el conjunto de las combinaciones lineales finitas con coeficientes en A de monomios en r variables sobre A.

Este anillo de polinomios es igual al que se puede obtener tomando anillos de polinomios sobre anillos de polinomios sucesivamente, es decir:

$$A[x_1, \ldots, x_s][x_{s+1}, \ldots, x_r] = A[x_1, \ldots, x_r]$$

para cualquier número de variables $x_1, \ldots, x_r$ y cualquier permutación de ellas.

Ilustraremos este hecho en el caso $r = 2$, $A[x][y]$.

Definimos

$$f = \sum f_i y^i,\ f_i = \sum_j a_{ij} x^j$$

Luego

$$f = \sum_i \left(\sum_j a_{ij} x^j \right) y^i = \sum_{i,j} a_{ij} x^i y^j$$

Como A es un anillo conmutativo, se tiene que $A[x][y] = A[y][x] = A[x, y]$.

Después de esto, vamos a demostrarlo en el caso general.

Proposición 2.6. Sea A un anillo conmutativo. Entonces

$$A[x_1, \ldots, x_{r-1}][x_r] \text{ y } A[x_1, \ldots, x_r]$$

son isomorfos.

Demostración. Si $f \in A[x_1, \ldots, x_{r-1}][x_r]$,

$$f = \sum_{i=0}^{n} f_i x_r^i,\ f_i = \sum_{j \in J} a_{ij} X^j,\ J = \{j_0, \ldots, j_m\} \subset \mathbb{N}^{r-1}$$

Luego

$$f = \sum_{(i,j) \in \{1,\ldots,n\} \times J} a_{ij} X^j x_r^i$$

Definimos $\Phi : A[x_1, \ldots, x_{r-1}][x_r] \to A[x_1, \ldots, x_r]$:

$$\Phi\left(\sum_{(i,j) \in \{1,\ldots,n\} \times J} a_{ij} X^j x_r^i \right) = \sum_{i=0}^{nm} b_i X^{p_i}, \quad \begin{array}{l} B = \{b_k = a_{ij} : jn + i = k\} \\ P = \{p_k = q_{ij} : q_{ij} \in \{1, \ldots, n\} \times J, jn + i = k\} \end{array}$$

Se puede comprobar que este es un isomorfismo de anillos conmutativos.

□

Proposición 2.7. Si $\varphi : A \to B$ es un homomorfismo, $\forall (b_1, ..., b_n) \in B^n$ la aplicación:

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

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

Proposición 2.8. Si $\varphi : A \to B$ es un homomorfismo, $\forall\ b \in B$ existe un único homomorfismo definido como:

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

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

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

Corolario 2.1. $A \leq B$ subanillo, $\forall b \in B$ existe un único homomorfismo

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

Nota. En la anterior definición, tendremos en cuenta que x es un elemento concreto de $A[x]$ (el polinomio de grado uno con coeficientes cero y la unidad), no un elemento cualquiera de $A[x]$.

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 2.9 (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 $r > 1$:

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

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

¿Es único?

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

□

Proposición 2.10 (Evaluación en subanillos *r* variables). Si $A\leq B, \forall b_1,\cdots,b_r\in B$ lista ordenada:

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

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

Dominio de integridad

Definición 3.1 (Dominio de integridad). Un anillo conmutativo A es un dominio de integridad si verifica la propiedad:

$$a\neq 0\ \wedge\ b\neq 0\Rightarrow ab\neq 0\ \ \forall a,b\in A$$

Equivalentemente,

$$ab=0\implies \begin{cases} a=0,\ \text{o} \\ b=0 \end{cases}\qquad \forall a,b\in A$$

Proposición 3.1 (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 $a\neq 0$, tomo $x,y\in A: b=x-y$, entonces $ab=a(x-y)=0\implies x=y\implies b=0.$ □

Definición 3.2 (Divisor de 0). $a\in A$ es divisor de 0 si $\exists b\neq 0: ab=0$.

Proposición 3.2. 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 3.3. Si A es finito, A es dominio de integridad $\iff$ A es un cuerpo

Demostración.
$\boxed{\Leftarrow}$ Trivial
$\boxed{\Rightarrow}$ $0 \neq a \in A$. Tomo $\{1, a, a^2, \dots\} = \{a^n : n \in \mathbb{N}\} \subseteq A$ Como A tiene cardinal finito y es cerrado para el producto: $\exists n, k \in \mathbb{N} : a^n = a^{n+k}$.
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 3.4. Todo D.I. es un subanillo de un cuerpo.

Antes de probar esta proposición, presentaremos otros conceptos. Comenzaremos por repasar brevemente los conceptos de relación binaria y relación de equivalencia, y definir el cociente de un conjunto por una relación de equivalencia. Esto nos servirá para construir el cuerpo de fracciones de un dominio de integridad, del que el dominio de integridad será un subanillo.

Definición 3.3 (Relación binaria). Una relación binaria en un conjunto A es un subconjunto de A^2. Si $\sim \subseteq A^2$ es una relación binaria y $(a, b) \in \sim$, se nota $a \sim b$ y se dice que "a está relacionado con b mediante $\sim$".

Definición 3.4 (Relación de equivalencia). Una relación de equivalencia en un conjunto A es una relación binaria $\sim$ en A que verifica las siguientes propiedades:

(*i*) ***Reflexividad***. $a \sim a \ \ \forall a \in A$.

(*ii*) ***Transitividad***. Si $a \sim b$ y $b \sim c$, entonces $a \sim c \ \ \forall a, b, c \in A$.

(*iii*) ***Simetría***. $a \sim b \implies b \sim a \ \ \forall a, b \in A$.

Definición 3.5 (Clase de equivalencia). Sean A un conjunto, $a \in A$ y $\sim$ una relación de equivalencia en A. Se define la clase de equivalencia de a respecto de $\sim$:

$$[a] = \{b \in A : a \sim b\}$$

Definición 3.6 (Cociente de un conjunto por una relación de equivalencia). Sean A un conjunto y $\sim$ una relación de equivalencia en A. Entonces se define el cociente de A por $\sim$:

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

Definición 3.7 (Cuerpo de fracciones de un D.I.). Sea A un dominio de integridad con $|A| \geq 2$. Consideramos

$$A \times (A - \{0\}) = \{(a, b), a, b \in A \mid b \neq 0\}$$

y en este conjunto la relación de equivalencia:

$$(a, b) \sim (c, d) \iff ad = bc$$

Definimos el cuerpo de fracciones de A como

$$\mathbb{Q}(A) = [A \times (A - \{0\})]/\sim$$

Se nota $[(a, b)] = \frac{a}{b}$ y se le llama "fracción a entre b".

Sobre él, definimos unas operaciones con las que será 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:

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

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 $\frac{a}{b}$.

Corolario 3.1.

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

Proposición 3.5 (Fracciones de denominador 1). Si A es un dominio de integridad, existe un homomorfismo

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

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

A partir de ahora usaremos la identificación $a = \frac{a}{1}$.

Proposición 3.6. Sea K un cuerpo y $A \leq K, a, b \in A$ $(b \neq 0)$.

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

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

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

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

Proposición 3.8. Si A es un D.I. $\implies$ $A[x]$ es un D.I.

Definición 3.8 (Grado de un polinomio). Si $f = \sum a_i x^i \neq 0$, entonces

$$gr(f) = n \in \mathbb{N} : a_n \neq 0 \text{ y } a_m = 0 \quad \forall m > n$$

El coeficiente a_n se denomina coeficiente líder.

Proposición 3.9. Si A es D.I., $f, g \in A[x] \implies gr(fg) = gr(f) + gr(g)$. En caso contrario, tenemos que $gr(fg) \leq gr(f) + gr(g)$.

Definición 3.9 (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) si

$$\exists c \in A : b = ac$$

Proposición 3.10. En las condiciones anteriores:

$$\exists c \in A : b = ac \tag{1}$$
$$\iff \text{La ecuación } ax = b \text{ tiene solución} \tag{2}$$
$$\iff \frac{b}{a} \in A \tag{3}$$

Demostración.

- $\boxed{(1) \iff (2)}$ Es la definición de que la ecuación $ax = b$ tenga solución.

- $\boxed{(1) \iff (3)}$

  $\boxed{\implies}$ Si a divide a $b \implies \exists c : b = ac \implies \dfrac{b}{a} = \dfrac{ac}{a} = \dfrac{c}{1} = c \in A$

  $\boxed{\impliedby}$ si $\dfrac{b}{a} \in A \implies \dfrac{b}{a} = \dfrac{c}{1} \implies b = ac$

□

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

Definición 3.10 (Asociados de un elemento de un D.I.). Sean A un dominio de integridad y $a \in A$. Entonces los elementos ua con $u \in U(A)$ se llaman *asociados de a*.

Proposición 3.11.

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

Definición 3.11. Los divisores triviales de $a \in A$ son las unidades y sus asociados.

Definición 3.12. Los divisores propios de $a \in A$ son los no triviales.

Proposición 3.12. 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.

Proposición 3.13. La divisibilidad verifica algunas propiedades:

(*i*) Reflexión: a/a

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

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

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

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

Notación: si a y b son asociados, escribiremos $a \sim b$.

Definición 3.13 (Irreducible). Sean A un dominio de integridad, $a \in A, a \neq 0, a \notin U(A)$. Se dice que a es irreducible si sus únicos divisores son los triviales

$$\begin{aligned}
&\iff \text{si } b/a \implies b \in U(A) \vee b \sim a \\
&\iff \text{si } a = bc \implies b \in U(A) \vee c \in U(A) \\
&\iff \text{si } a = bc \implies a \sim b \vee c \sim a \\
&\iff \text{si } a = bc \wedge b \notin U(A) \implies c \in U(A)
\end{aligned}$$

Dominios euclídeos

Definición 4.1 (Dominios euclídeos). Un dominio euclídeo es un dominio de integridad, A, tal que se pueda definir una función $\varphi : A - \{0\} \to \mathbb{N}$ que verifique:

(*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 $r = 0 \vee \varphi(r) < \varphi(b)$

Nota. En algunos textos, se omite la primera propiedad, dado que a partir de una función que verifique la segunda, es posible definir una que verifique ambas.

Proposición 4.1. Si A es dominio euclídeo, entonces:

$$\begin{aligned}
& b/a && (1) \\
\iff \; & \text{un resto de dividir } a \text{ entre } b \text{ es cero} && (2)
\end{aligned}$$

Demostración.

$\boxed{\Longleftarrow}$ Trivial.

$\boxed{\Longrightarrow}$ Por definición de b/a, $\implies \exists c \in A$ tal que $a = bc$ y por ser A un dominio euclídeo, $\exists q, r \in A : a = bq + r$ 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 $\varphi(r) < \varphi(b)$.

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

$$\varphi(r) = \varphi(b(c-q)) \geq \varphi(b)$$

Llegando a una contradicción.

□

Teorema 4.1 (Teorema de Euclides). $\forall a, b \in \mathbb{Z}, b \neq 0, \exists! q, r \in \mathbb{Z}$ 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 $r \neq r'$ ($\implies q \neq q'$), 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. Observemos que el caso general se puede reducir al caso $a \geq 0, b > 0$, de la siguiente forma:

- si $b < 0$, entonces se toman $b' = -b, q' = -q$, y se escribe $a = b'q' + r, 0 \leq r < |b'|$.
- si $a < 0$ y $b > 0$ (podemos asegurar que $b > 0$ por el caso anterior), se toman $a' = -a, q' = -q-1, r' = b - r$ y se escribe $a = bq' + r', 0 \leq r' < b$.

Por tanto, 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 $a - b$ (para $x = 1$).

  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 que $r < b$, por 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 $r < b$.

□

Corolario 4.1. $\mathbb{Z}$ es un dominio de Euclides con

$$\begin{aligned} \varphi &= |\cdot| : \mathbb{Z} \to \mathbb{N} \\ \varphi|_{\mathbb{N}} &= 1_{\mathbb{N}} \\ \varphi|_{\mathbb{Z}\setminus\mathbb{N}} &= -1_{\mathbb{Z}\setminus\mathbb{N}} \end{aligned}$$

Teorema 4.2 (Teorema de Euclides para polinomios). $\forall f, g \in A[x]$ 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 $n < m \implies f = g * 0 + f \implies \exists q, r \in A[x] : f = gq + r$ con $q = 0$ 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 $g = b_0$ 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 tenemos el q y r que buscábamos.
  - Si $n > 0$, haremos la inducción.
    Consideramos $x^{n-m} g(x)$ y establecemos

    $$f_1 = f - \frac{a_n}{b_m} x^{n-m} g \quad (1)$$

    Entonces, podemos ver que $gr(f_1) < n$. Por hipótesis de inducción

    $$\exists q, r \in A[x] : f_1 = gq_1 + r \quad (2)$$

    Ahora, utilizando (1) y (2):

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

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

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 4.2. 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 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 4.3 (Teorema de Euclides, enteros cuadráticos). 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 $\beta \neq 0 \quad \exists q, r \in \mathbb{Z}[\sqrt{n}] : \alpha = \beta q + r$ 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 4.1. Vamos a tratar de dividir $\alpha = 6+10i$ entre $\beta = 1+2i$ en el anillo $\mathbb{Z}[i]$. Tenemos que saber si se puede hacer dicha división o no ($\varphi(ab) \geq \varphi(a)$) 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, 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.

Máximo común divisor. Dominios de ideales principales. Ecuaciones diofánticas en D.I.P.

Definición 5.1 (Máximo común divisor). Sea A un anillo conmutativo. 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 $c/b \implies c/d$

Definición 5.2 (Primos relativos). Si $(a, b) = 1$, a y b se dicen *primos relativos*.

Definición 5.3 (Ideal). En un anillo conmutativo se llama ideal a un subconjunto suyo no vacío que es cerrado para la suma y que "absorbe" el producto en todo el anillo. Formalmente, 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*) $a \in I, x \in A \implies ax \in I$

Definición 5.4 (Ideal principal). Sea A un anillo conmutativo. Si $a \in A$,

$$aA = (a) = \{ax : x \in A\}$$

es el ideal principal generado por a.

Definición 5.5 (DIP: dominio de ideales principales). Un dominio de ideales principales es un dominio de integridad en el cual todo ideal es principal.

En un DIP, el máximo común divisor es único salvo asociados, y verifica algunas 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, $(a, 0) = a$, $\quad (a, 1) = 1$, $\quad (a, u) = 1 \iff u \in U(A)$

(*iv*) $((a, b), c) = (a, (b, c)) = (a, b, c)$

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

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

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

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

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

□

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

(vii) $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$

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

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

□

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

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

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

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

(xiii) 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:

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

(xiv) 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: $1 = (a, bc)$

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

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

(*xvi*) 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 5.1. Realizamos un ejemplo en el que se puede probar que, usando la Nota anterior, 3 y $(1+\sqrt{5})$ son irreducibles

Teorema 5.1. 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: $\boxed{\subseteq}$ $b \in I \implies (b) \subseteq I$.

  $\boxed{\supseteq}$ Tomamos $a \in I$, por tanto $\exists q, r \in A : a = bq + r$. Supongamos que $r \neq 0 \implies r = a - bq \in I$ con $\varphi(r) < \varphi(b)$, esto es imposible puesto que $\varphi(b)$ es el mínimo, luego $r = 0 \implies a \in (b)$.

□

Teorema 5.2. 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:
$(ax + by) + (ax' + by') = a(x + x') + b(y + y') \in I(a, b) \implies$ cerrado para la suma.
$(ax + by)z = a(xz) + b(xz) \in I(a, b) \implies$ 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 A, llamamos ecuaciones diofánticas a aquellas que son de la forma:

$$ax + by = c \quad a, b, c \in A$$

Proposición 5.1 (Lema de Euclides). Sean $a, b, c \in A$, con A un D.I.P., tales que c/ab y $(c, a) = 1$. Entonces c/b.

A continuación vamos a estudiar las soluciones de las ecuaciones diofánticas en un D.I.P., en tres pasos. Comenzaremos por dar una condición suficiente y necesaria para que una ecuación tenga solución, fácilmente verificable; en ese caso, daremos una solución particular y a partir de ella, la general.

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

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

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

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

Esta ecuación tiene las mismas soluciones que la ecuación diofántica inicial. Llamaremos a esta la ecuación "reducida".

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 particular, entonces la solución general es el conjunto de los (x, y) que hemos dado arriba.

Demostración de iii).

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

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

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 5.2 (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 5.2. 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 $k=22$).

Mínimo común múltiplo. Ecuaciones en congruencias

Definición 6.1 (Mínimo común múltiplo). Sean A un D.I., y $a, b \in A$. Entonces m es un mínimo común múltiplo de a y b,y lo notamos $m = mcm(a, b) = [a, b]$, si se verifica que m es un múltiplo común de de a y b y que el conjunto de los múltiplos comunes a ambos es igual al conjunto de múltiplos de m, formalmente:

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

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 6.1. 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 6.1. 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 ($m = a_1 b = a b_1$) y el (1) podemos ver que $\left.\begin{array}{l} m = a_1 b = k d_1 = bv d_1 \implies a_1 = v d_1 \\ m = a b_1 = k d_1 = au b_1 \implies b_1 = u d_1 \end{array}\right\} \implies$

$\left.\begin{array}{l} a = a_1 d = v d_1 d \\ b = b_1 d = u d_1 d \end{array}\right\} \implies d_1 d/a \quad d_1 d/b$

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

Congruencias

Sean 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:

$$a \equiv b \mod (I) \quad \text{o} \quad a \equiv_I b$$

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

$$a \equiv b \mod (mA) \to^{\text{notación}} a \equiv b \mod (m) \ (\iff m/a - b \iff a - b = qm)$$

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 (*ii*) y (*i*))

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

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

(*vi*) $a \equiv b, c \equiv d \implies ac \equiv bd$ (dem.: (*v*) y luego uso (*i*))

(*vii*) $ac \equiv bc \mod (mc)$ y $c \neq 0 \implies a \equiv b \mod (m)$

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

(*viii*) Si $(c, m) = 1$, entonces: $ac \equiv bc \mod (m) \iff a \equiv b \mod (m)$

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

Ecuaciones en congruencias

Proposición 6.2 (Ecuaciones en congruencias). Estudiaremos la ecuación

$$ax \equiv b \mod (m) \quad (1)$$

- Si $m = 0 \implies$ la ecuación es $ax = b$.
- Si $a = 0 \implies$ la ecuación es $0x \equiv 0 \mod (m) \implies$ 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 $\iff \exists x \in A : ax \equiv b \mod (m) \iff \exists x \in A : m/ax - b \iff \exists x, y \in A : (ax - b) = my \iff \exists x, y \in A : ax - my = b$, 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:
   $$a'u \equiv 1 \mod (m') \implies a'ub' \equiv b' \mod (m')$$
   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:

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

   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: $x \equiv x_1 \mod (m')$

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:

$$\left.\begin{array}{ll} a_1x \equiv b_1 & \mod (m1) \\ a_2x \equiv b_2 & \mod (m2) \end{array}\right\} (1) \quad \left.\begin{array}{ll} x \equiv a & \mod (m) \\ x \equiv b & \mod (n) \end{array}\right\} (2)$$

Teorema 6.2 (Teorema chino del resto). El sistema tiene solución $\iff a \equiv b \mod ((m,n))$.

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

Ahora, supuesto que tiene solución, vamos a hallar las soluciones particular y general del problema.
Si y_0 es una solución particular de $my \equiv b - a \mod (n)$, 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 6.3 (Teorema de Ruffini). Si $f(x) \in A[x]$, $a \in A$ entonces $f(a)$ es el 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: $f \equiv f(a) \mod (x-a)$.

Anillos de congruencias. Anillo cociente.

Definición 7.1 (Clase de congruencia respecto de un ideal). Sean A un anillo conmutativo, $I \subseteq A$ y $a \in A$. Si definimos la relación de equivalencia

$$a \overset{\circ}{=} b \iff a - b \in I$$

es decir, "ser congruente módulo I", entonces la clase de congruencia de a respecto de I es la clase de equivalencia de a respecto de $\overset{\circ}{=}$. La notamos

$$[a] = \bar{a} = a + I$$

Definición 7.2 (Anillo cociente). Sean A un anillo conmutativo e I un ideal suyo. Entonces se define el anillo cociente de A por I, $(A/I, \oplus, \odot)$:

$$A/I = [a] = a + I : a \in A$$
$$[a] \oplus [b] = [a + b]$$
$$[a] \odot [b] = [ab]$$

Se puede comprobar que estas operaciones están bien definidas y que con ellas A/I es un anillo conmutativo. Probaremos que están bien definidas:

$$\text{Si } [a] = [a'] \text{ y } [b] = [b'] \implies \begin{cases} [a+b] = [a'+b'] \\ [ab] = [a'b'] \end{cases}$$

Demostración.

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

□

Proposición 7.1. Si $f : A \to B$ es un homomorfismo de anillos, $\ker(f) = \{a \in A : f(a) = 0\}$ es un ideal de A.

Demostración. Vamos a probar que $\ker(f)$ es cerrado para sumas y para múltiplos. Para ello, en ambos casos usaremos que f es un homomorfismo.

$$\text{Si } a, b \in \ker(f) \implies \begin{cases} f(a+b) = f(a) + f(b) = 0 + 0 = 0 \\ f(ab) = f(a)f(b) = 0 * 0 = 0 \end{cases}$$

□

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

$$\begin{array}{rccc} F: & A/\ker(f) & \cong & \operatorname{img}(f) \\ & [a] & \mapsto & f(a) \end{array}$$

Demostración. Para probar el resultado tenemos que probar tres cosas:

(*i*) F está bien definida.

(*ii*) F es biyectiva.

(*iii*) F es un homomorfismo de anillos.

Vamos a probar que está bien definida. Es decir, que sin importar el representante de la clase de

congruencia que tomemos, el valor de la aplicación para esa clase es el mismo. Esto es, $[a] = [b] \implies F([a]) = F([b])$.

Si $[a] = [b] \implies a - b \in \ker(f) \implies f(a-b) = 0 \implies F([a]) = f(a) = f(b) = F([b])$.

Vamos a ver ahora que es un homomorfismo

- $F([a] + [b]) = F([a+b]) = f(a+b) = f(a) + f(b) = F([a]) + F([b])$
- $F([a][b]) = F([ab]) = f(ab) = f(a)f(b) = F([a])F([b])$
- $F([1]) = f(1) = 1$

Probamos la inyectividad:

$F([a]) = F([b]) \implies f(a) = f(b) \implies f(a-b) = 0 \implies a - b \in \ker(f) \implies a \equiv b \mod (\ker(f)) \implies [a] = [b]$.

La sobreyectividad es trivial por la sobreyectividad de f en su imagen.

□

Proposición 7.2. 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:

$$\forall a, b \in A : b \neq 0 \implies \exists! q, r \in A : a = bq + r \text{ y } \begin{cases} r = 0 \text{ o} \\ \varphi(r) < \varphi(b) \end{cases}$$

Si seleccionamos un $b \in A, b \neq 0$ tal que $\varphi(1) < \varphi(b)$ entonces:

$$\forall a \in A, R_b(a) = r \iff \begin{cases} a \equiv r \mod (b) \text{ y} \\ r = 0 \quad o \quad \varphi(r) < \varphi(b) \end{cases}$$

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. $R_b(a + a') = R_b(R_b(a) + R_b(a'))\ \ \forall a, a' \in A$

Demostración. $R_b(a+a') \equiv_b a + a' \equiv_b R_b(a) + R_b(a') \equiv_b R_b(R_b(a) + R_b(a'))$. □

3. $R_b(aa') = R_b(R_b(a)R_b(a'))\ \ \forall a, a' \in A$

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.

Proposición 7.3 (Isomorfismo entre unidades). Sean A y B anillos conmutativos, y $f : A \to B$ un isomorfismo. Entonces $f\big|_{U(A)} : U(A) \to U(B)$ es un isomorfismo.

Demostración. $a \in U(A) \implies \exists a^{-1} : aa^{-1} = 1 \implies f(a)f(a^{-1}) = 1 \implies f(a) \in U(B)$ y $f(a)^{-1} = f(a^{-1})$. El resto de propiedades de isomorfismo se deducen de que f es un isomorfismo. □

Proposición 7.4 (Isomorfismo entre divisores de cero). Sean A y B anillos conmutativos, y $f : A \to B$ un isomorfismo. Entonces $f\big|_{\mathrm{div}_0(A)} : \mathrm{div}_0(A) \to \mathrm{div}_0(B)$ es un isomorfismo.

Demostración. Análoga a la anterior: $a \in \mathrm{div}_0(A) \implies \exists a' \in A, a' \neq 0 : aa' = 0 \implies f(a)f(a') = 0$ y $f(a') \neq 0$. □

Proposición 7.5. Sean A un D.E. con función euclídea φ, en el que hay unicidad en cocientes y restos; y $m \in A : m \neq 0$ con $\varphi(1) < \varphi(m)$.

Consideramos $A_m = \{R_m(a) : a \in A\}$ donde, como ya sabemos,

$$r + r' = R_m(r + r')$$
$$rr' = R_m(rr')$$

Veamos que R_m es un homomorfismo.

Demostración. Notando por $\oplus$ la suma en A_m,

$$R_m(a + b) = R_m(R_m(a) + R_m(b)) = R_m(a) \oplus R_m(b)$$
$$R_m(ab) = R_m(a)R_m(b) = R_m(R_m(a)R_m(b))$$

Por último: $R_m(1) = 1$ por $\varphi(1) < \varphi(m)$. □

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

Corolario 7.1. Sean A un DE y $m \in A$. Entonces $A/(m)$ y A_m son isomorfos con

$$\begin{array}{rccc} F: & A/(m) & \cong & A_m \\ & [a] & \mapsto & R_m(a) \end{array}$$

Proposición 7.6. 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.

i) Sea $[a] \in U(A/(m)) \iff \exists x \in A : [a][x] = [1] \iff \exists x \in A : ax \equiv 1 \mod (m) \iff (a, m) = 1$.

iii) Sea $a \in A$. Entonces la aplicación dada por $x \mapsto ax$ puede ser

- Inyectiva: entonces es sobreyectiva por ser $A/(m)$ finito. Por tanto, existe $x \in A$ tal que $ax = 1$, luego a es una unidad.
- No inyectiva: entonces existen $u, v \in A,\ u \neq v$ tales que $au = av$, luego $a(u - v) = 0$ y $u - v \neq 0$.

Ahora, si esta aplicación no es sobreyectiva, entonces no puede ser inyectiva (de nuevo porque $A/(m)$ es finito), por tanto a es divisor de cero. Si es sobreyectiva, a es una unidad. Además, sabemos que los divisores de cero y las unidades de un anillo son disjuntos. □

Corolario 7.2. En las mismas condiciones, son equivalentes:

(*i*) m es irreducible.

(*ii*) $A/(m)$ (resp. (A_m)) es un D.I.

(*iii*) $A/(m)$ ó (resp. (A_m)) es un cuerpo.

Demostración.

iii) $\implies$ *ii)* Todo cuerpo es un dominio de integridad.

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 D.I., en contradicción con la hipótesis. □

Definición 7.3 (Característica de una anillo). Sea $(A, +, \cdot)$. Su característica es el menor $n \in \mathbb{N}$ tal que

$$\underbrace{1 + \cdots + 1}_{n \text{ sumandos}} = 0$$

donde 1 es el elemento neutro multiplicativo del anillo. De no existir tal número, se dice que tiene característica cero.

Proposición 7.7. La característica de un cuerpo finito es distinta de cero.

Demostración. Solo hay que observar que, de ser cero, el cuerpo tendría infinitos elementos, pues al sumar 1 (que no es el elemento neutro para la adición) se obtiene un elemento distinto. □

Proposición 7.8. Si $(F, +, \cdot)$ es un cuerpo finito, entonces su característica es un número primo.

Demostración. Sea p la característica de F. Razonando por contradicción, supongamos que $p = ab$, con a y b distintos de uno, por tanto distintos de p. Entonces $\sum_{i=1}^{a} \sum_{i=1}^{b} 1 = 0$. Como b no es la característica de F, $q := \sum_{i=1}^{b} 1 \neq 0$. Luego $q \sum_{i=1}^{a} 1 = 0$. Como a tampoco es la característica de F, $\sum_{i=1}^{a} 1$ es un divisor de cero no nulo, lo cual es una contradicción con la hipótesis de que F es un cuerpo. □

Proposición 7.9. Si F es un cuerpo finito, entonces $|F| = p^n$, con $p, n \in \mathbb{N}$ y p la característica de F.

Demostración. Por las propiedades de F como cuerpo, se puede comprobar que F es un espacio vectorial sobre $\mathbb{Z}_p$. Ahora, su dimensión es necesariamente finita, sea esta n. Entonces, si $\{v_1, \ldots, v_n\}$ es una base del espacio, sabemos que cada vector del mismo se expresa de forma única como $a_1 v_1 + \cdots + a_n v_n$, con $a_i \in \mathbb{Z}_p$, por tanto el espacio tiene p^n elementos. □

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 $K[x]_{f(x)} = \{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} : b_i \in K\}$

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.

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 $\{[x_0],\ [x_0 + n'],\ [x_0 + 2n'], ...,\ [x_0 + (d-1)n']\} \subseteq \mathbb{Z}/(n) \cong \mathbb{Z}_n, \forall r, 0 \leq r \leq d-1$. $\{x_0,\ x_0 + n',\ x_0 + 2n', ...,\ x_0 + (d-1)n'\} \subseteq \mathbb{Z}_n$

□

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

Necesitamos algunos resultados para probar esto:

Definición 8.1 (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 8.1 (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.

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

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 $[a]_n = [c]_n$?

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

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 8.1. 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, $\varphi(n) = \varphi(p_1^{e_1}) \dots \varphi(p_n^{e_n})$.

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

Teorema 8.2. Si $(a,m)=1 \implies a^{\varphi(m)}=1$ en $\mathbb{Z}_m \qquad a \in \mathbb{Z}_m$

Por tanto, $a^{\varphi(m)-1}=a^{-1}$ en $\mathbb{Z}_m$

Teorema 8.3 (Teorema de Euler). $\forall a \in \mathbb{Z}$ si $(a,m)=1 \implies a^{\varphi(m)} \equiv 1 \mod (m)$.

Teorema 8.4 (Teorema pequeño de Fermat). Si p es irreducible, $\forall a \in \mathbb{Z}, a^p \equiv a \cdot \mod (p)$

Corolario 8.2. Si p es irreducible, $\forall a \in \mathbb{Z}_p \quad a^p = a$ en $\mathbb{Z}_p$

Demostración. Partiendo de la hipótesis del teorema demostraremos el corolario:

$m=p, a \neq 0$ en $\mathbb{Z}_p$ (si $a=0$ es trivial) $\implies (a,p)=1 \implies a^{\varphi(p)}=1$ en $\mathbb{Z}_p$

$\varphi(p)=p(1-\frac{1}{p})=p-1 \implies a^{p-1}=1$ en $\mathbb{Z}_p \implies a^p=a$ en $\mathbb{Z}_p$

□

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 $\exists \sigma : \{1,...,r\} \cong \{1,...,s\}$ una permutación tal que q'_i es asociado con $q_{\sigma(i)}$

Definición 9.1 (Conjunto representativo de los irreducibles de A). Si A es un DFU, vamos a denotar $\mathcal{P}$ = un conjunto representativo de los irreducibles de A.

- $\forall p \in \mathcal{P}$, p es un irreducible
- $\forall p,q \in \mathcal{P}$, p y q no son asociados entre sí
- $\forall p$ 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 $a \in A$, $a \notin U(A), a \neq 0$, 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 9.1. 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 9.2. 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. $e(p,a) = 0 \quad \forall p \notin \{p_1, ..., p_s\}$

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

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

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

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

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

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

Proposición 9.1. En un 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.
Sea d un elemento del anillo tal que $e(p,d) = min\{e(p,a), e(p,b)\}\ \forall p \in \mathcal{P}$, es evidente que d/a,b. 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 un máximo común divisor. □

Definición 9.3 (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 9.2. (*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 $b \sim p$

(*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 9.1. 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 $(i) \implies (ii)$ es trivial. Veamos que $(ii) \implies (i)$

Lo único que falta para probar que es un DFU es probar que las factorizaciones son únicas. Sea $a = p_1 ... p_r = q_1 ... q_s$ con p_i, q_j irreducibles. Vamos a ver que $r = s$. Para ello, vamos a hacer una inducción en r.

- Caso $r = 1 \implies p_1 = q_1 ... q_s$. 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. Como no se puede dar que $s > 1 \implies s = 1 = r \implies p_1 = q_1$
- 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 $(i) \implies (iii)$ es trivial. Como (i) y (ii) son equivalentes, basta probar que $(iii) \implies (ii)$

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 producto 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:

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

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

Realizando la prueba análoga para el producto, 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 9.2. 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 distintos de cero 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 $a_1 = a,\ a_{n+1} = a'_n$. 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, podemos ver que (como a_{n+1} es divisor de a_n):

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

Y en esta cadena 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. □

Proposición 9.3. Si $\alpha \in \mathbb{Z}[\sqrt{n}]$ es un divisor propio de β en $\mathbb{Z}[\sqrt{n}]$ entonces $N(\alpha)$ es un divisor propio de $N(\beta)$ en $\mathbb{Z}$

Demostración. Como α es un divisor de β entonces $\exists \gamma \in \mathbb{Z}[\sqrt{n}] : \beta = \alpha\gamma \implies N(\beta) = N(\alpha)N(\gamma) \implies N(\alpha)/N(\beta)$.

Ahora, la norma de α no puede ser ni 1, ni -1 pues si no sería una unidad y, por tanto, no sería divisor propio; α no puede ser un asociado pues si no, γ sería un divisor propio también, luego $N(\alpha)$ tiene que ser un divisor propio de $N(\beta)$

□

Corolario 9.1. Si $N(\alpha) = \pm p$ con p un primo de $\mathbb{Z}, p \geq 2 \implies \alpha$ es irreducible en $\mathbb{Z}[\sqrt{n}]$

Corolario 9.2. Si α es primo en $\mathbb{Z}[\sqrt{n}] \implies N(\alpha) = \pm p$ ó $\pm p^2$ con $p \geq 2$ un primo de $\mathbb{Z}$. Además, si $N(\alpha) = \pm p^2 \implies \alpha\ y\ p$ son asociados en $\mathbb{Z}[\sqrt{n}]$

Demostración. Supongamos que $\alpha \in \mathbb{Z}[\sqrt{n}]$, primo. Consideramos su norma: $N(\alpha)$ que no es ni 1 ni -1 pues si no sería una unidad. Así: $N(\alpha) = p_1...p_r$ con $p_i \in \mathbb{Z}$ primos, lo que implica que $\alpha\bar{\alpha} = p_1...p_r \implies \alpha / p_1...p_r$ pero α es primo, luego $\exists i \in \{1, ..., r\} : \alpha / p_i \implies \exists p \geq 2$ primo de $\mathbb{Z}$ tal que $\alpha / p\ en\ \mathbb{Z}[\sqrt{n}]$.

Esto implica $p = \alpha\beta\ con\ \beta \in \mathbb{Z}[\sqrt{n}] \implies p^2 = N(\alpha)N(\beta) \implies N(\alpha)/p^2 \implies N(\alpha) = \pm p$ ó $\pm p^2$, como queríamos.
Si $N(\alpha) = p^2 \implies N(\beta) = 1 \implies \beta$ es una unidad $\implies \alpha$ y p son asociados □

Nota. Si estuviéramos en un DFU, ser irreducible y ser primo son equivalentes, luego estos enunciados valdrían igual para elementos primos.

Ejemplo 9.2. Factorizar $2i$ y $11+7i$ en producto de irreducibles(primos por estar en un DFU).

1. Primero, calcularemos su norma. $N(11+7i) = 11^2+7^2 = 170$
2. Factorizamos la norma en $\mathbb{Z}$. $170 = 2*85 = 2*5*17$.
3. Ahora, los factores irreducibles serán los enteros de Gauss cuya norma sea un primo o el cuadrado de un primo. Por tanto, un divisor de este número será un entero de Gauss $Z[i]$ cuya norma sea un divisor de la norma de $11+7i$, por tanto su norma será 2, 5 ó 17.
4. $N(a+bi) = a^2+b^2 = 2 \iff a = \pm 1$ y $b = \pm 1$. Los enteros de Gauss de norma 2 son: $1+i, 1-i, -1+i, -1-i$, es decir $1+i$ y sus 3 asociados.
5. Ahora, tenemos que plantearnos si $1+i/11+7i$, vemos que la división es: $11+7i/1+i = 9-2i \in \mathbb{Z}[i]$. Además, como $1+i$ tiene norma 2, que es un primo de $\mathbb{Z}$ luego ya tenemos un irreducible por el corolario 9.1.
6. Tenemos que repetir el proceso para $9-2i$.
7. Su norma es $N(9-2i) = 5*17$ pues es el de antes quitándole el irreducible cuya norma vale 2.
8. Buscamos los enteros de Gauss cuya norma valga 5. $N(a+bi) = a^2+b^2 = 5 \iff a = \pm 1$ y $b = \pm 2$ ó $a \pm 2$ y $b = \pm 1$.

   Estos son: $1+2i$ y sus asociados para el primer caso y $2+i$ y sus asociados para el segundo caso.
9. Ahora, tenemos que ver si estos dividen a $9-2i$.
   - $9-2i/2+i = \frac{16}{5} + \frac{13}{5}i \notin \mathbb{Z}[i]$
   - $9-2i/1+2i = 1-4i \in \mathbb{Z}[i]$

   Por lo que tenemos que $11+7i = (1+i)(1+2i)(1-4i)$ y ahora tenemos justo 3 irreducibles con las normas que buscábamos, luego tenemos hecha la factorización en irreducibles.

Ahora, haciendo lo mismo para $2i$ vemos que $2i = (1+i)^2$.

Ejemplo 9.3. 2. Vamos a factorizar 180 en $\mathbb{Z}[i\sqrt{2}]$. Para ello, vemos que $180 = 2^2*3^2*5$. Recordamos que en este anillo, $N(a+b\sqrt{2}) = a^2+2b^2$ y $U(\mathbb{Z}[i\sqrt{2}]) = \pm 1$

Ahora, como $N(2) = 4$, un divisor propio del 2 tendrá por norma un divisor propio del 4 en $\mathbb{Z}$. En $\mathbb{Z}$, sólo el 2 es divisor propio del 4. Por ello, tenemos que plantearnos la ecuación $a^2+2b^2 = 2$. Entonces, los únicos elementos que hay que tienen son $\sqrt{-2}$ y $-\sqrt{-2}$. Ahora vemos si alguno de estos

divide a 2:

$$\frac{2}{\sqrt{-2}} = \frac{2 * (-\sqrt{-2})}{\sqrt{-2} * (-\sqrt{-2})} = \frac{2(-\sqrt{-2})}{2} = -\sqrt{-2} \in \mathbb{Z}[i\sqrt{2}]$$

Ahora, como $N(\sqrt{-2}) = 2$ que es un primo en $\mathbb{Z} \implies \sqrt{-2}$ es un primo de $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$ y por ello $2 = -(\sqrt{-2})^2$.

Seguimos, haciendo lo mismo con el 3. $N(3) = 9$. ¿Existen a y b : $a^2 + 2b^2 = 3$? Vemos que tomando $a = \pm 1$ y $b = \pm 1$ se puede llegar a la igualdad. Es decir, tenemos los elementos: $\{1 + \sqrt{-2},\ 1 - \sqrt{-2},\ -1 - \sqrt{-2},\ -1 + \sqrt{-2}\}$.

Probamos dividiendo $3/(1 + \sqrt{-2}) = 1 - \sqrt{-2} \implies 3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ y ambos son irreducibles.

Hacemos lo mismo con el 5. Tenemos que discutir la ecuación: $a^2 + 2b^2 = 5$. Sin embargo, en este caso no hay ningún elemento que tenga solución luego 5 es primo en $\mathbb{Z}[i\sqrt{2}]$.

Por tanto, la factorización de 180 en $\mathbb{Z}[i\sqrt{2}]$ es: $180 = (\sqrt{-2})^4 * (1 + \sqrt{-2})^2 * (1 - \sqrt{-2})^2 * 5$

Ejemplo 9.4. Ejemplo de anillo que no es un DFU.

Como ejemplo, vamos a probar que $\mathbb{Z}[\sqrt{-5}]$ **no es un DFU.** En este anillo, $N(a + bi\sqrt{5}) = a^2 + 5b^2$ y $U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$

Vamos a considerar el elemento $1 + i\sqrt{5}$. Su norma es: $N(1 + i\sqrt{5}) = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 6 = 2 * 3$. ¿Es este elemento irreducible?

Vamos a plantearnos qué elementos del anillo $\mathbb{Z}$ tienen norma 2 o norma 3.

- En la ecuación $a^2 + 5b^2 = 2$ no hay soluciones en $\mathbb{Z}[i\sqrt{5}]$
- En la ecuación $a^2 + 5b^2 = 3$ tampoco hay soluciones en este anillo.

Como no tiene divisores propios, entoces este elemento es irreducible. Su conjugado, por el mismo motivo, también es un irreducible.

Ahora, por la norma de $1 + i\sqrt{5}$ hemos obtenido una factorización del 6 en producto de irreducibles. Pero el 6 también es $2 * 3$ en este anillo. Esta podría ser otra factorización en irreducibles de 6 en $\mathbb{Z}[i\sqrt{5}]$. El 2 no tiene ningún divisor propio en este anillo, pues es el único divisor de 4 en $\mathbb{Z}$ luego el 2 es irreducible en este anillo. Lo mismo ocurre con el 3.

Por tanto, tenemos dos descomposiciones del 6 en producto de irreducibles, que no son iguales ni asociados luego este anillo no puede ser un DFU.

Ahora, el 2 es un irreducible, ¿es 2 primo? Vemos que $2/6$, y $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Si fuese primo, necesitaríamos $2/1 + i\sqrt{5}$ ó $2/1 - i\sqrt{5}$ y eso no ocurre pues sus normas no se dividen en $\mathbb{Z}$ por tanto el 2 no es primo.

$\mathbb{Z}[x]$ es un DFU y no es un DIP

Vamos a estudiar ahora que este anillo es un DFU sin ser un DIP ni un DE.

Bastaría de hecho tomar los elementos 2 y x para ver que $(2, x) = 1$ y no existen los coeficientes de Bezout para estos elementos, es decir:

$$\nexists f, g \in \mathbb{Z}[x] : 1 = 2f(x) + xg(x)$$

Vamos ahora a enunciar y a demostrar el Teorema de Gauss sobre los DFU. Sin embargo, antes debemos aclarar algunos conceptos.

Definición 9.4. Si $f \in A[x]$, $gr(f) \geq 1$, se define su contenido como el m.c.d. de sus coeficientes. Lo denotamos por $c(f)$. (Si $f = \sum a_i x^i \implies c(f) = mcd(a_0, ..., a_n)$)
Se dice que f es primitivo si $c(f) = 1$. El contenido es único salvo asociados.

Lema. $c(af) = ac(f)$. Esta propiedad es consecuencia directa de que $(ab, ac) = a(b, c)$

Lema. Todo $f : gr(f) \geq 1$ se puede factorizar de la forma $f = af'$ con f' primitivo. Además, esta factorización es esencialmente única.

Demostración. Sea f un polinomio y $a = c(f)$. Entonces, $a/a_i \ \forall i$. Tomamos $a_i' = \frac{a_i}{a} \in A$. Sea también $f' = \sum a_i' x^i$. Ahora, si tomáramos $af' = \sum aa_i' x^i = f \implies a = c(f) = c(af') = ac(f') \implies c(f') = 1$ simplificando por a, luego hemos encontrado una factorización $f = af'$.

Además, podemos ver que la factorización es única, pues si $f = bg$ con $c(g) = 1$ y $f = af'$, entonces $a = c(f) = bc(g) = b \implies a = b$ y $g = f'$ □

Lema. Todo ϕ, $gr(\phi) \geq 1$ se puede factorizar de forma esencialmente única como $\phi = \frac{a}{b} f$ con f primitivo.

Demostración. Sea $\phi = \sum \frac{a_i}{b_i} x^i$. Tomamos $b = \prod b_i \implies b_i / b \ \forall i \implies b_i / ba_i \ \forall i \implies b\phi = \sum \frac{ba_i}{b_i} x^i$ Pero el numerador es un múltiplo del denominador, luego $g = \sum \frac{ba_i}{b_i} x^i \in A[x]$.

De esta forma, $b\phi = af \implies \phi = \frac{a}{b} f$.

Además, veamos que es única. Sea ahora $\phi = \frac{c}{d} f'$ con f' primitivo $\implies \frac{a}{b} f = \frac{c}{d} f' \implies daf = bcf' \implies da = bc$ y $f = f'$ □

Enunciaremos también un lema muy importante, el lema de Gauss.

Lema de Gauss. Sea A un DFU. Si tenemos $f, g \in A[x] \implies c(fg) = c(f)c(g)$. En particular, el producto de polinomios primitivos es primitivo.

Demostración. Probaremos en primer lugar que el producto de polinomios primitivos es primitivo. Sean $f = \sum a_i x^i$ y $g = \sum b_j x^j$ ambos en $A[x]$ y primitivos. Consideramos también su producto $fg = \sum c_k x^k$. Sabemos que $c_k = \sum_{i+j=k} a_i b_j$. Negaremos la tesis e intentaremos llegar a una contradicción.

Supongamos que fg no es primitivo. Entonces, $c(fg) \neq 1$. Como A es un DFU, el contenido se podrá expresar como un producto de primos (irreducibles). Existirá al menos un primo que lo divida. $\exists p$ primo

de A con $p/c(fg) \implies p/c_k \ \forall k$. Sin embargo, ese p no puede dividir a $a_i \ \forall i$ pues f es primitivo. Por la misma razón, no puede dividir a todos los b_j.

Por tanto, sea r el primer índice tal que p no divide a a_r. Tomemos también s el primer índice tal que s no divide a b_s. Ahora, vamos a fijarnos en el coeficiente c_{r+s} de fg. Este coeficiente se expresa como:

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i+j=r+s \ \ i<r} a_i b_j + a_r b_s + \sum_{i+j=r \ \ i>r} a_i b_j$$

De esta expresión, podemos ver que p/c_{r+s}, que $\forall i < r$ entonces $p/a_i b_j \implies p/\sum_{i+j=r+s} a_i b_j$ por dividir a los a_i. Ocurre lo mismo con el mismo en el término de $i > r$ pues p divide a b_j. Si despejáramos $a_r b_s$ veríamos que $p/a_r b_s$ pues divide a todos los sumandos, pero p es un primo, por tanto si divide a un producto tiene que dividir a alguno de los factores, pero como habíamos dicho que no divide a ninguno de los dos, hemos llegado a una contradicción y, por tanto, fg es primitivo.

Ahora demostraremos c(fg) = c(f)c(g). Podemos poner $f = af'$ con f' primitivo e igual con $g = bg'$. Entonces $fg = abf'g' \implies c(fg) = c(abf'g') = abc(f'g')$ pero f' y g' son primitivos luego su contenido es 1. Así, el contenido de f es a y el de g es b luego $c(fg) = c(f)c(g)$ probando así el lema. □

Lema.

(*i*) Si $a \in A$, a es irreducible en A[x] $\Leftrightarrow$ a es irreducible en A.

(*ii*) Si $gr(f) \geq 1$, f es irreducible en A[x] $\Leftrightarrow$ f es primitivo y es irreducible en K[x].

Demostración. (*i*) Una factorización de un polinomio de grado 0 será irreducible si es irreducible en A (porque U(A[x]) = U(A)).
(*ii*) $\boxed{\Rightarrow}$ Si f es irreducible, el contenido tiene que ser o una unidad o un asociado. No puede ser asociado porque... Como c(f)/f, si f es irreducible $\Rightarrow$ c(f) = 1 $\Rightarrow$ f es primitivo. Vamos a probar que es irreducible en K[x] por contradicción. Supongamos que f no es irreducible en K[x] $\Rightarrow$ f = $\phi\psi$ con $gr(\phi) \geq 1$ y $gr(\psi) \geq 1$

$$\left.\begin{array}{l}\phi = \frac{a}{b}g : g \text{ es primitivo} \\ \psi = \frac{c}{d}h : h \text{ es primitivo}\end{array}\right\} \Longrightarrow \quad f = \frac{a}{b}\frac{c}{d}gh \Rightarrow bdf = acgh$$

Aplicando contenidos sobre esta igualdad nos queda, $c(bdf) = c(acgh) \Rightarrow bdc(f) = acc(gh) \Rightarrow bd = ac \Rightarrow f = gh$ CONTRADICCIÓN f es irreducible y ninguno es unidad ya que el grado es mayor o igual que 1.

$\boxed{\Leftarrow}$ Suponemos que $f = gh$ en A[x], g y h no unidades. Entonces, $gr(g)$ y $gr(h)$ es mayor o igual que 1. (Suponemos $gr(g) = 0$, $g = a \in A; f = ah \Rightarrow 1 = ac(h) \Rightarrow g = a \in U(A) = U(A[x])$, llegamos a una contradicción con la suposición inicial).
$f = gh$ se da en K[x] y muestra que f no es irreducible en K[x], contradicción con la hipótesis. En K[x] no hay irreducibles de grado 0, las constantes tienen inverso. □

Observación: Sea $\phi \in$ K[x], $gr(\phi) \geq 1$, $\phi = \frac{a}{b}f$ con f primitivo. ϕ es irreducible en K[x] $\Leftrightarrow$ f es irreducible en A[x].

Teorema 9.3 (Teorema de Gauss). Si A es un DFU $\Longrightarrow$ $A[x]$ es también un DFU.

Demostración. Sea $f \in$ A[x], $f \neq 0$ y $f \notin$ U(A[x])=U(A)

- Caso $gr(f) = 0$. $f = a \in$ A, $a \neq 0$ y $a \notin$ U(A). Como A es un DFU, existen $p_1, ..., p_r$ irreducibles de A (también de A[x]) tales que $a = p_1...p_r$
- Caso $gr(f) \geq 1$ y f primitivo. Existen $\phi_1, ..., \phi_r \in$ K[x] irreducibles tales que $f = \phi_1...\phi_r$. $\phi_i = \frac{a_i}{b_i}f_i$: $f_i \in$ A[x], primitivo $\Longrightarrow$ $f = \frac{a}{b}f_1...f_r$ donde $a = \prod a_i$, $b = \prod b_i$ $\Longrightarrow$ $bf = af_1...f_r$ $\Longrightarrow$ $^{(1)}b = a$ $\Longrightarrow$ $f = f_1...f_r$. Por el lema anterior, como f_i son irreducibles en K[x] y, además, son primitivos, f_i son irreducibles en A[x].
- Caso general, $gr(f) \geq 1$ y f no primitivo. Tomamos $f = af'$ con f' primitivo. $c(f) = a \neq 0$, $a \notin$ U(A)

$^{(1)}$ Como f_i son primitivos

□

En lo sucesivo, vamos a notar $A \subseteq K = Q(A)$. De esta forma, también sucede $A[x] \subseteq K[x]$. También vamos a notar:

- $a, b, c.... \in A$

- $f, g, h... \in A[x]$
- $\phi, \psi, ... \in K[x]$

Corolario 9.3. Si $f \in A[x]$ es irreducible en $A[x]$ con $gr(f) \geq 1 \implies f$ es primo en $A[x]$.

Demostración. Supongamos que f/gh en $A[x] \subseteq K[x]$. Como f es irreducible en $A[x]$, lo es en $K[x]$ y $K[x]$ es un DFU por ser K un cuerpo, entonces f es primo en $K[x]$. Entonces, podemos asegurar que o bien f/g o bien f/h en $K[x]$.

Para lo que sigue, supongamos que f/g en $K[x]$ (Si quisiéramos para hacerlo para h, sólo habría que cambiar las letras). Entonces, $f\phi = g$ y $\phi = \frac{a}{b}f'$ con f' un polinomio de $K[x]$ primitivo. Esto implica:

$$\frac{a}{b}ff' = g \implies aff' = bg(1)$$

Ahora, calcularemos los contenidos aplicando el lema de Gauss. Como f y f' son primitivos,

$$ac(f)c(f') = bc(g) \implies a = bc(g)$$

Ahora, si nos llevamos esta igualdad a (1) obtenemos:

$$bc(g)ff' = bg \implies f(c(g)f') = g \implies f/g \; en \; A[x]$$

Y por tanto, obtenemos que f es primo. □

Nota. De esta forma, podemos ver por inducción que cualquier anillo de la forma $A[x_1, ..., x_r]$ es un DFU si A es un DFU.

Nota (2). En $\mathbb{Z}$ hay infinitos primos.

Vamos a intentar ahora a buscar una factorización de un $f \in A[x]$. ¿Cuándo es f irreducible?

Sabemos que $gr(f) = 0 \iff f = p \in A$ que sería irreducible si p lo es en A.

Supongamos ahora que $gr(f) \geq 1, f$ es irreducible en $A[x] \iff$ f es primitivo e irreducible en $K[x]$

Nota. Si K es un cuerpo, todo polinomio de grado 1 es irreducible.

Demostración. Supongamos que $\phi = \phi_1\phi_2 \implies 1 = gr(\phi) = gr(\phi_1) + gr(\phi_2) \implies \phi_1$ es una unidad o lo es ϕ_2, luego necesariamente ϕ es irreducible. □

Ejercicio. Factorizar $(120x + 100)^2$ en $\mathbb{Z}[x]$.

$$120x + 100 = 20(6x + 5) = 2^2 * 5 * (6x + 5)$$

Pero, $6x + 5$ es un polinomio de grado 1, primitivo en $\mathbb{Z}[x]$. Además, 2 y 5 son irreducibles en $\mathbb{Z}$, por tanto la factorización del polinomio al cuadrado es:

$$2^4 * 5^2(6x + 5)^2$$

Nota. Si K es un cuerpo, $\phi \in K[x]$ tiene un factor de grado 1 $\iff$ ϕ tiene una raíz en K

Demostración.

$$\alpha x + \beta = \alpha(x - (\frac{-\beta}{\alpha}) = \alpha(x - \gamma) \implies \alpha x + b/\phi \iff x - \gamma/\phi \iff {}^{Rufinni}\phi(\gamma) = 0$$

Donde $\gamma = \frac{-\beta}{\alpha}$ □

Proposición 9.4. Sea $f = a_0 + a_1 x + ... + a_n x^n \in A[x]$. Entonces f tiene un factor irreducible de grado 1 en $K[x]$ si y solamente si tiene una raíz en K.

Equivalentemente, $(a, b) = 1$ y $f(\frac{a}{b}) = 0 \iff bx - a/f$ en $A[x]$. En tal caso, esta posible raíz verifica que a/a_0 y b/a_n en A.

Demostración. Si tenemos que $f(\frac{a}{b}) = 0 \iff x - \frac{a}{b}/f$ en $K[x]$.

$\boxed{\Rightarrow}$ Esto implica que $f = (x - \frac{a}{b})\phi$ con $\phi = \frac{c}{d}g$ con $g \in$ A primitivo,

$$\implies f = \frac{c}{d}(x - \frac{a}{b})g = \frac{c}{bd}(bx - a)g \implies bdf = c(bx - a)g$$

Si aplicamos contenidos:

$$bdc(f) = c$$

Volviendo a la igualdad anterior:

$$f = (bx - a)(c(f)g)$$

Por tanto, $bx - a/f$ en $A[x]$.

$\boxed{\Leftarrow}$ Si $f = (bx - a)g \implies f(\frac{a}{b}) = (b\frac{a}{b} - a)g(\frac{a}{b}) = 0$ □

Criterio de la raíz: En $K[x]$ todo polinomio de grado 1 es irreducible y es asociado a uno de la forma $x - \alpha$ con $x - \alpha/\phi(x) \iff \phi(\alpha) = 0$.

Así, también en $A[x]$ los polinomios irreducibles de grado 1 son los de la forma $bx - a$ con $(a, b) = 1$ por lo que $(a, b) = 1$ y $bx - a/f(x) \iff f(\frac{a}{b}) = 0$.

Si $f(x) = a_0 + a_1 x + ... + a_n x^n$ y si $f(\frac{a}{b}) \implies a/a_0$ y b/a_n en A.

Esto lo podríamos ver como una condición de irreducibilidad, pues si un polinomio fuera irreducible, no podría tener ninguna raíz, pues carecen de factores de grado 1.

Ejemplo 9.5. Factorizar en producto de irreducibles el polinomio $f = 6x^4 + 3x^3 - 18x^2 + 33x + 21$ en $\mathbb{Z}[x]$.

Lo primero que deberíamos hacer es buscar el contenido de este polinomio:

$$f = 3(2x^4 + x^3 - 6x^2 + 11x + 7)$$

El contenido de f es 3 y $f' = 2x^4 + x^3 - 6x^2 + 11x + 7$. 3 es un primo en $\mathbb{Z}$ y por tanto lo es en $\mathbb{Z}[x]$ y por tanto nos centramos en el primitivo asociado. Aplicamos el criterio de la raíz. Las posibles raíces que el polinomio tuviera en $\mathbb{Q}$ serían $\{\pm 1, \pm\frac{1}{2}, \pm 7, \pm\frac{7}{2}\}$. Calculamos las imágenes de estos puntos

para ver si alguno es cero:

$$f'(1) = 2+1-6+11+7 \neq 0; \quad f'(-1) = 2-1-6-11+7 \neq 0;$$

$$f'(\frac{-1}{2}) = 2*(1/2^4) - (1/2^3) - 6*(1/4) - 11*(1/2) + 7 = 0$$

Y por tanto hemos encontrado una raíz, es decir:

$$2x+1/f'(x) \; en \; \mathbb{Z}[x]$$

Ahora, dividiremos $f'(x)$ entre $2x+1$ para reducirlo. Al dividirlo nos queda cociente x^3-3x+7 y resto 0. Por tanto, f nos queda factorizado como:

$$f(x) = 3*(2x+1)*(x^3-3x+7)$$

Tenemos ya uno de grado 3, por tanto es irreducible si y solo si carece de raíces en $\mathbb{Q}$. Para ello, debemos buscar fracciones que sean divisores del 7, que son $\{\pm 1, \pm 7\}$ y haríamos sus imágenes por el polinomio x^3-3x+7 y vemos que ninguna da de resultado cero, por tanto estas no son raíces suyas y por tanto es irreducible en $\mathbb{Z}[x]$ y la factorización del polinomio en producto de primos sería justo la que acabamos de obtener.

Si nos planteamos la discusión en $\mathbb{Q}[x]$: 3 y x^3-3x+7 son mónicos, $2x+1$ no, pero podemos sacar factor común para hacerlo mónico y nos quedaría como resultado final:

$$f(x) = 6(x+\frac{1}{2})(x^3-3x+7) \quad \in \mathbb{Q}[x]$$

Ejemplo 9.6. 2. Factorizaremos el polinomio: $20x^3+10x^2-80x+30 \in \mathbb{Z}[x]$. Para resolverlo, había que observar que su contenido es 10 y que por tanto:

$$f = 2*5*(2x^3+x^2-8x+3)$$

Y por tanto habría que buscar sus raíces entre $\{\pm 1, \pm\frac{1}{2}, \pm 3 \pm \frac{3}{2}\}$ y veríamos que en $\frac{3}{2}$ el polinomio evaluado da cero, por tanto factoriza como:

$$2*5*(2x-3)(x^2+2x+2)$$

Y podemos ver que x^2+2x+2 no tiene raíces y por tanto ese es el polinomio descompuesto en primos.

Ejemplo 9.7. 3. Consideremos el polinomio: $x^4+x^3+x^2+x+1$ en $\mathbb{Z}_2[x]$. ¿Este polinomio es irreducible?. Estamos en $\mathbb{Z}_2$, luego sustituyendo el 0 y el 1 vemos que no tiene de raíces. Como no tiene raíces no tiene factores de grado 1.

Ahora, si no fuese irreducible habría que descomponerlo como 2 factores de grado 2. Si dividimos por el polinomio x^2+x+1, que es irreducible en $\mathbb{Z}_2[x]$ el resto no es 0, luego no es divisible y por tanto el polinomio inicial ya es irreducible en $\mathbb{Z}_2[x]$.

Proposición 9.5 (Criterio de Eisenstein). Sea $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$ primitivo y siendo A un DFU. Si existe un primo $p \in A$ cumpliendo alguna de estas dos:

1. $p/a_i \ \ \forall i = 0, ..., n-1$ y p^2 no divide a a_0
2. $p/a_i \ \ \forall i = 1, ..., n$ y p^2 no divide a a_n

Entonces f es irreducible.

Demostración. Vamos a demostrarlo para el primer caso, la demostración para el segundo es equivalente. Vamos a negar la tesis y veremos qué ocurre.

Supongamos que $f = (b_0 + ... + b_mx^m)(c_0 + ... + c_rx^r)$ con $r + m = n$ y $r, m \geq 1$. Entonces, $a_0 = b_0c_0$ para que fuera el producto. Como p es primo, tiene que dividir a b_0 o a c_0. Además, no puede dividir a ambos pues si no p^2 dividiría a a_0. Supongamos que p/b_0 y por tanto que no divide a c_0.

Supongamos también que p no divide a a_n pues si no, formaría parte del contenido. Además, como hemos obtenido una factorización, $a_n = b_mc_r$ y como p no divide a a_n entonces no divide ni a b_m ni a c_r.

Sea i el primer índice tal que p no divide a b_i. Es claro que $0 < i \leq m < n$, que existirá pues al menos es el último. Como lo habíamos factorizado, entonces $a_i = b_ic_0 + (b_{i-1}c_1 + ... + b_0c_i)$. Entonces, $p/b_j \ \ \forall j < i \implies p/b_ic_0$ pero p es primo luego divide o a b_i o a c_0, pero ya habíamos dicho que no dividía a ninguno de los dos anteriormente en la demostración, luego hemos llegado a una contradición. Por tanto, f es irreducible. □

Ejemplo 9.8. Podemos ver que $3x^7 - 70x^3 + 140 \in \mathbb{Z}[x]$ por el criterio de Eisenstein para el primo $p = 5$, que divide a todos los coeficientes menos al coeficiente líder pero su cuadrado $p^2 = 25$ no divide a ninguno de los coeficientes.

Ejemplo 9.9. 2. El polinomio : $y^3 + x^2y^2 + xy + x \in \mathbb{Z}[x, y]$, pues el primo $p = x$ divide a todos los coeficientes menos al líder y su cuadrado no divide a todos los coeficientes.

Proposición 9.6 (Cambio de anillo). Sean A y B dominios de integridad (así, el grado del producto es el producto de los grados). Sea $\phi : A[x] \to B[x]$ un homomorfismo en el que $gr(\phi(f)) \leq gr(f)$.

Si $f \in A[x] : gr(\phi(f)) = gr(f)$ y $\phi(f)$ no tiene divisores de grado $r \implies f$ tampoco tiene divisores de grado r

Demostración. Supongamos que $f = gh$ donde $gr(f) = n$, $gr(g) = r$ y $gr(h) = s$ con $r + s = n$. Aplicamos entonces el homomorfismo:

$$\phi(f) = \phi(gh) = \phi(g)\phi(h)$$

Y ahora, $gr(\phi(f)) = n$, $gr(\phi(g)) \leq r$ y $gr(\phi(h)) \leq s$ y entonces implica que $gr(\phi(g)) = r$ (Si $r < gr(\phi(g)) \implies r + s \neq n$, contradicción) □

Ejemplo 9.10. $x^4 + 1$ es irreducible en $\mathbb{Z}[x]$.

Si tomamos $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ que lleva $x \mapsto x + 1$ el homomorfismo de evaluación en $x + 1$. $(\phi(\sum a_i x^i) = \sum a_i (x+1)^i)$.

Así, $\phi(x^4 + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2 \in \mathbb{Z}[x]$, que es irreducible por el criterio de Eisenstein para el primo $p = 2$. Ahora, por el criterio del cambio de anillo, entonces $x^4 + 1$ es también irreducible en $\mathbb{Z}[x]$

Proposición 9.7 (Criterio de reducción módulo un primo). En las condiciones anteriores, consiste en aplicar el homomorfismo:

$$R_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x] : \quad R_p(\sum a_i x^i) = \sum R_p(a_i) x^i \in \mathbb{Z}_p[x]$$

Para utilizar este criterio, es muy útil conocer los irreducibles mónicos de los anillos $Z_p[x]$

Irreducibles mónicos de $\mathbb{Z}_p[x]$:

- de grado 2 en $\mathbb{Z}_2[x]$: $x^2 + x + 1$
- de grado 3 en $\mathbb{Z}_2[x]$: $x^3 + x + 1,\ x^3 + x^2 + 1$
- de grado 2 en $\mathbb{Z}_3[x]$: $x^2 + 1,\ x^2 + x + 2,\ x^2 + 2x + 2$

Ejemplo 9.11. Sea $f = x^4 + 3x^2 - 2x + 5 \in \mathbb{Z}[x]$. Si le aplicamos el criterio de reducción módulo un primo, en este caso el 2, el polinomio queda: $R_2(f) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ y por el criterio de reducción, como este polinomio no tiene divisores de grado ni 1 ni 3 entonces podemos asegurar que f tampoco los tiene.

Si lo volvemos a hacer para el primo $p = 3$, queda $R_3(f) = x^4 + x + 2 \in \mathbb{Z}_3[x]$, que nos da exactamente la misma información que la reducción anterior. Como conocemos los mónicos de $\mathbb{Z}_3[x]$, dividimos este polinomio entre los 3 irreducibles mónicos de $\mathbb{Z}_3[x]$ y vemos que los restos son no nulos. Así, este polinomio es irreducible en $\mathbb{Z}_3[x]$ y por el criterio de reducción módulo un primo, el polinomio primero es irreducible en $\mathbb{Z}[x]$.

Matrices sobre anillos conmutativos

Sea K un cuerpo, y consideremos $\mathcal{M}_{mxn}(K)$ y $\mathcal{M}_n(K)$. Imaginemos ahora que $A \leq K$ es un subanillo. De esta forma, podemos concebir las matrices que están en este conjunto: $\mathcal{M}_{mxn}(A)$ ó $\mathcal{M}_n(A)$.

Así, si sumáramos dos matrices que estuvieran en $\mathcal{M}_{mxn}(A)$, nos quedaría una matriz cuyas entradas están en el subanillo A. Lo mismo ocurre con la multiplicación.

Podemos considerar también el *Grupo Lineal* que se define como:

$$GL_n(K) = U(\mathcal{M}_n(K)) = \{M \in \mathcal{M}_n(K) :\ \exists M^{-1} \in \mathcal{M}_n(K)\ \ con\ \ MM^{-1} = M^{-1}M = I_n\}$$

Que sabemos que es igual al conjunto $\{M \in \mathcal{M}_n(K) : |M| \neq 0\}$. Ahora, podemos considerar, como hemos hecho anteriormente, lo mismo pero en el subanillo A.

Dada $M \in \mathcal{M}_n(A)$, si $M \in GL_n(A)$, cumplirá que $MM^{-1} = I$, tomando determinantes vemos que: $|I| = |M|\,|M^{-1}|$. El determinante de M y el determinante de M^{-1} están en A, y es un producto que da como resultado 1, por lo que podemos asegurar que $|M| \in U(A)$.

Veámoslo al revés. Si $M \in \mathcal{M}_n(A)$ con $|M| \in U(A) \implies 1/|M| \in A$. Si consideramos la adjunta de M, esta también pertenece a $\mathcal{M}_n$ y, por tanto, $M \in GL_n(A)$ pues tiene una inversa cuyas entradas están todas en el subanillo A. Con todo esto, hemos deducido la siguiente proposición:

Proposición 10.1. Sea $M \in \mathcal{M}_n(A)$, entonces $M \in GL_n(A) \iff |M| \in U(A)$

Ejemplo 10.1. El grupo lineal de $\mathbb{Z}$ es: $GL_n(Z) = \{M \in \mathcal{M}_n(A) : |M| = \pm 1\}$

Ejemplo 10.2. 2. El grupo lineal de $K[x]$ es: $GL_n(K[x]) = \{M \in \mathcal{M}_n(K[x]) : |M| = k - \{0\}\}$, donde k es un polinomio de grado 0 no nulo.

Definición 10.1 (Matrices equivalentes). Dos matrices M y N $\in \mathcal{M}_{mxn}(A)$ son equivalentes si $\exists P \in GL_m(A), Q \in GL_n(A)$ tal que

$$M = PNQ$$

Estando en un cuerpo, dos matrices serán equivalentes $\iff$ tienen el mismo rango.

Teorema 10.1 (Teorema de la forma Normal de Smith). Si A es un Dominio Euclídeo, toda matriz $M \in \mathcal{M}_{mxn}(A)$ es equivalente a una de la forma:

$$\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

con $d_1, ..., d_r \in A$ ubicados en la diagonal, donde $0 \leq r \leq min\{m, n\}$ y cada $d_i \neq 0$ y d_i / d_{i+1}. Además, estos $d_1, ..., d_r$ son únicos para la clase de equivalencia de M y se llaman los **factores invariantes** de la matriz.

Corolario 10.1. Dos matrices $M, N \in \mathcal{M}_{mxn}(A)$ son equivalentes $\iff$ tienen los mismos factores invariantes.

Sea esta matriz

$$P = \begin{pmatrix} 1 & & & \\ & \ddots & a & \\ & & & \\ & & & 1 \end{pmatrix}$$

Que tiene en la posición (i,j) un elemento $a \in A$. Entonces, esta matriz es invertible y además su inversa es igual pero cambiando a por $-a$.

Si:

$$N = \begin{pmatrix} F_1 \\ \vdots \\ F_n \end{pmatrix}$$

Y multiplicáramos P_1N, entonces quedaría $F'_k = F_k$ si $k \neq i$ con i el número de fila que contenía el elemento a y $F'_i = F_i + aF_j$. Lo mismo ocurriría con las columnas si...
FALTA CONTENIDO DE MATRICES, añadirla.

Nota. Si multiplicáramos en una matriz todos los elementos de una fila o los de una columna por una unidad del anillo, entonces la matriz inicial y la resultante son equivalentes.

Nota. Si permutamos dos filas, o dos columnas, las matrices inicial y final son equivalentes.

Definición 10.2. Una matriz $M \in \mathcal{M}_{mxn}$ que sea:

$$\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

con $d_1, ..., d_r \in A$, $d_i \neq 0$ y d_i / d_{i+1}, en las posiciones (i,i) con $1 \leq i \leq r$ y 0 en todas las demás posiciones, se dice matriz Normalizada (Smith).

Vamos a explicar ahora un método a partir del cual, teniendo una matriz cualquiera podemos obtener una matriz normalizada que es equivalente a la primera. No olvidemos que estamos trabajando en Dominios euclídeos.

Sea $A \in \mathcal{M}_{mxn}$. $A \neq 0$. Sea $\varphi : A - \{0\} \to \mathbb{N}$ la función euclídea.

Vamos a llamar $\varphi(M) = min\{\varphi(a_{ij}) : a_{ij} \neq 0\}$ Primero, tomaremos un a_{ij} donde la función euclídea tome el valor más pequeño que tome en toda la matriz. Ahora, por operaciones elementales podemos llevarlo a la posición $(1, 1)$.

Supongamos ahora que a_{11} no divide a a_{1k}, como estamos en un dominio euclídeo, podemos expresar el cociente entre ellos como:

$$a_{1k} = a_{11}q + b_{1k}$$

donde $b_{1k} \neq 0$ y $\varphi(b_{1k}) < \varphi(a_{11})$.

Ahora, realizamos la operación:

$$C_k \mapsto C_k - qC_1$$

$$\begin{pmatrix} a_{11} \dots a_{1k} \dots \\ \dots \end{pmatrix} \xrightarrow{C_k - qC_1} \begin{pmatrix} a_{11} \dots b_{1k} \dots \\ \dots \end{pmatrix}$$

Reiteramos el proceso las veces que haga falta, hasta encontrarnos una matriz que sea de la forma (b_{ij}). Ahora, si b_{11} no divide a b_{k1}, entonces este último se expresará como $b_{k1} = b_{11}q' + c_{k1}$ con $c_{k1} \neq 0$ y $\varphi(c_{k1}) < \varphi(b_{11})$

Entonces, realizamos la operación:

$$F_k \mapsto F_k - q'F_1$$

Volvemos a reiterar el procedimiento cuantas veces haga falta.

Tras una serie de pasos, llegaremos a una matriz equivalente a la original en la que b_{11}/b_{k1} y b_{11}/b_{1k} $\forall k$. Llegados a esta situación, por transformaciones elementales podemos obtener una matriz que sea del tipo:

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & & \ddots & \\ 0 & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

Donde b_{11}/c_{ij} para cada i y j. Ahora, lo que haremos es tomar la submatriz que empieza en c_{22} y volveremos a realizar el mismo proceso.

Ejemplo 10.3. Sea $A \in \mathcal{M}_{3x2}$ tal que:

$$A = \begin{pmatrix} 14 & 10 \\ 22 & 14 \\ 10 & 10 \end{pmatrix}$$

Ahora, tomamos el número que tenga φ menor, en este caso el 10 y hacemos transformaciones elementales para llevarlo a la primera posición.

$$\begin{pmatrix} 14 & 10 \\ 22 & 14 \\ 10 & 10 \end{pmatrix} \xrightarrow{C_2,\, C_1} \begin{pmatrix} 10 & 14 \\ 14 & 22 \\ 10 & 10 \end{pmatrix} \xrightarrow{C_2 - C_1} \begin{pmatrix} 10 & 4 \\ 14 & 8 \\ 10 & 0 \end{pmatrix} \xrightarrow{C_2,\, C_1} \begin{pmatrix} 4 & 10 \\ 8 & 14 \\ 0 & 10 \end{pmatrix} \xrightarrow{C_2 - 2C_1} \begin{pmatrix} 4 & 2 \\ 8 & -2 \\ 0 & 10 \end{pmatrix}$$

$$\xrightarrow{C_2, C_1} \begin{pmatrix} 2 & 4 \\ -2 & 8 \\ 10 & 0 \end{pmatrix} \xrightarrow{C_2 - 2C_1} \begin{pmatrix} 2 & 0 \\ -2 & 12 \\ 10 & -20 \end{pmatrix} \xrightarrow{F_2 + F_1} \begin{pmatrix} 2 & 0 \\ 0 & 12 \\ 10 & -20 \end{pmatrix} \xrightarrow{F_3 - F_1} \begin{pmatrix} 2 & 0 \\ 0 & 12 \\ 0 & -20 \end{pmatrix}$$

Y ahora, tendríamos que hacer lo mismo atendiendo a la submatriz resultante:

$$\begin{pmatrix} 2 & 0 \\ 0 & 12 \\ 0 & -20 \end{pmatrix} \xrightarrow{F_3 + 2F_2} \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 12 \end{pmatrix} \xrightarrow{F_3 - 3F_2} \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

Y nos queda la matriz:

$$\begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

Que es equivalente a la inicial.

Definición 10.3 (Rango de la matriz). El entero r tal que M tiene al menos un menor de orden r no nulo y todos los de orden $r+1$ son nulos se llama Rango de la matriz.

Vamos a definir ahora $\Delta_s(M) = mcd\{$ menores de orden s de M no nulos$\}$ Así, $\Delta_1(M)$ sería el máximo común divisor de todos los m_{ij} (si M está normalizada será d_1). Ahora, con esta definición, podemos decir que:

$$rg(M) = max\{s : \Delta_s(M) \neq 0\}$$

Lo que implica que si $rg(M) = r \implies \Delta_1(M), ..., \Delta_r(M)$ son $\neq 0$ y $\Delta_{r+1}(M), ...$ son nulos.

Sea $P \in \mathcal{M}_m(A)$. Construimos la matriz $PM \in \mathcal{M}_{mxn}(A)$ (tenemos la matriz $M \in \mathcal{M}_{mxn}(A)$). Si miramos el elemento de PM en la posición (k, j), este es: $\sum_{i=1}^{m} p_{ki}a_{ij}$. Así, la fila k–ésima de PM es:

$$(\sum_{i=1}^{m} p_{ki}a_{i1}, \cdots, \sum_{i=1}^{m} p_{ki}a_{in}) = \sum_{i=1}^{m} p_{ki}(a_{i1}, \cdots, a_{in})$$

Por tanto, las filas de la matriz PM son combinación lineal de la matriz M. También podemos afirmar que los menores de orden s de la matriz PM son combinación lineal de los menores de orden s de la matriz M. Entonces, $\Delta_s(M)/\Delta_s(PM)$.

Si $P \in GL_m(A) \implies \Delta_s(PM)/\Delta_s(P^{-1}PM) = \Delta_s(M) \implies \Delta_s(M) = \Delta_s(PM)$

Si $Q \in GL_n(A) \implies \Delta_s(M) = \Delta(MQ)$

Nota. $\Delta(M) = \Delta(M^t)$. Del mismo modo, $\Delta_s(MQ) = \Delta_s((MQ)^t) = \Delta_s(Q^tM^t) = \Delta_s(M^t) = \Delta_s(M)$

De las implicaciones anteriores, obtenemos como conclusión:

$\forall\ P,\ Q\ \ \Delta_s(PMQ) = \Delta_s(M)\ \ \forall s \implies$ si M y M' son equivalentes, entonces $\Delta_s(M) = \Delta_s(M')\ \forall s$

Si $M \sim M' \sim \begin{pmatrix} d'_1 & & & & & \\ & \ddots & & & & \\ & & d'_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \implies r = r'$

Tenemos que $\Delta_1(M) = d_1 = \Delta_1(M') = d'_1 \implies d_1 = d'_1$; y si lo hacemos en general vemos que:

$$\Delta_s(M) = d_1...d_s = \Delta_s(M') = d'_1...d'_s \implies d_s = \frac{\Delta_s(M)}{\Delta_{s-1}(M)} = \frac{\Delta_s(M')}{\Delta_{s-1}(M')} = d'_s$$

Nota. Si el anillo es un cuerpo $\implies d_i = 1\ \ \forall i$

A-módulo

Definición 11.1 (A-módulo). Es un conjunto no vacío M dotado de dos operacions:

- $MxM \to M$ tal que $(x, y) \mapsto x + y$ que es interna
- $AxM \to M$ tal que $(a, x) \mapsto ax$

que verifican las propiedades asociativa, conmutativa, elemento neutro y elemento opuesto. También verifican la distributiva respecto de la suma y respecto del producto, asociatividad del producto y neutro del producto.

Durante todo el apartado nos referiremos a $x, y, ...$ como elementos de M y a $a, b, ...$ como elementos de A.
Propiedades:

(*i*) Unicidad del 0 y del opuesto.

(*ii*) $0x = 0$ y $a0 = 0$

(*iii*) $(-a)x = -(ax) = a(-x)$

(*iv*) Si para una lista de elementos $(x_1, ..., x_n)$ de M con al menos 2 elementos definimos su suma simultánea $\sum_{i=1}^{n} x_i$ por inducción: $\sum_{i=1}^{n} x_i = (\sum_{i=1}^{n-1} x_i) + x_n$

(*v*) $\forall i < r < n$, entonces $\sum_{i=1}^{n} x_i = (\sum_{i=1}^{r} x_i) + (\sum_{i=r+1}^{n} x_i)$

(*vi*) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} x_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i x_j$

Si $I \leq A$ es un ideal, si tomamos $M = A/I$, entonces se verfican:

- $[x] + [y] = [x + y]$
- $a[x] = [ax] = [a][x]$

Definición 11.2 (Submódulos). Si M es un A-Módulo, un submódulo es $\emptyset \neq N \subseteq M$ que es cerrado para sumas ($x, y \in N \implies x + y \in N$) y para múltiplos($a \in A,\ x \in N \implies ax \in N$).

Con estas operaciones de suma y producto restringidas, N también es un A-módulo. Por tanto, todo submódulo es un módulo.

Proposición 11.1. Si $M_1, ..., M_r \subseteq M$ son submódulos, existe siempre un módulo que los contiene.

Se le llama submódulo suma y se representa como:

$$\sum_{i=1}^{r} M_i = \{\sum_{i=1}^{r} x_i : x_i \in M_i\}$$

Además, se puede usar la conmutatividad de la suma y la asociatividad generalizada.

Definición 11.3 (Suma directa). Se dice que la suma de $M_1, ..., M_r$ es directa y se representa:

$$\sum_{i=1}^{r} = \oplus_{i=1}^{r} M_i \; si \; (\sum_{i=1}^{r} x_i = \sum_{i=1}^{r} y_i) \; con \; x_i, y_i \in M_i \iff x_i = y_i \; \forall i$$

Definición 11.4 (Submódulo cíclico). Si $x \in M$, siempre existe un submódulo de M que es el menor submódulo que lo contiene. Más aún, que contiene al elemento x y está contenido en cualquier otro submódulo que contenga a x. Se denota como $Ax = \{ax : a \in A\}$, pues es donde están todos los múltiplos del elemento. Se le llama el submódulo cíclico de x. También se suele notar "(x)".

Definición 11.5. Si $x_1, ..., x_r \in M$, existe un módulo M que es el más pequeño módulo que los contiene. Este es:

$$\sum_{i=1}^{r} Ax_i = \{\sum_{i=1}^{r} a_i x_i : a_i \in A\}$$

Estos son combinaciones lineales de $x_1, ..., x_r$, se le llama submódulo generado por $x_1, ..., x_r$ y se representa como $(x_1, ..., x_r)$.

Nota. Si $N = (x_1, ..., x_r)$ y $N' = (y_1, ..., y_s)$, entonces

$$N \subseteq N' \iff todo \; x_i \; es \; c.lde \; y_1, ..., y_s \; \forall i$$

Y $N = N' \iff$ todo x_i es combinación lineal de $y_1, ..., y_s$ y todo y_j es combinación lineal de $x_1, ..., x_r$

Definición 11.6 (Sistema de generadores). Si $x_1, ..., x_r \in M : M = (x_1, ..., x_r)$ se dice que $x_1, ..., x_r$ es un sistema de generadores de M y se dice que M es finitamente generado.

Proposición 11.2. Si A es un dominio euclídeo, todo submódulo de un módulo finitamente generado es finitamente generado.

Definición 11.7. Un sistema de generadores $x_1, ..., x_r$ de un módulo M es una base de M si se verifica:

$$\sum_{i=1}^{r} a_i x_i = \sum_{i=1}^{r} b_i x_i \iff a_i = b_i \ \forall i$$

O, equivalentemente:

$$\sum_{i=1}^{r} a_i x_i = 0 \iff a_i = 0 \ \forall i$$

Definición 11.8 (Linealmente independientes). Un conjunto de elementos de un A-Módulo $x_1, ..., x_r$ se dice que son linealmente independientes si la única combinación lineal de ellos que da como resultado 0 es aquella en la que todos los coeficientes son cero.

Nota. En los A-módulos, es falso decir que todo A-módulo tiene una base o que todo sistema de generadores contiene a una base. Tampoco podemos siempre extender un conjunto linealmente independiente a una base.

Definición 11.9 (Módulo Libre). Un módulo que contenga una base es un módulo libre.

Definición 11.10. Si M, N son dos módulos, y $\varphi : M \to N$ una aplicación, la llamamos lineal u homomorfismo entre módulos si:

$$\left.\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(ax) &= a\varphi(x) \end{aligned}\right\} \iff \varphi(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} a_i \varphi(x_i)$$

También puede ser un monomorfismo (si y solo si su núcleo es 0), epimorfismo (es sobreyectiva) o un isomorfismo (es biyectiva).

Ejemplo 11.1. Si $m \in A$, $A/(m)$ es un A-módulo ($[a] + [b] = [a+b]$ y $a[b] = [ab]$. Si A tiene unicidad de cocientes y restos ($\mathbb{Z}, K[x]$), entonces A_m es un A-módulo con $r + r' = R_m(r + r')$ y $ar = R_m(ar)$.

Recordemos que existe un isomorfismo entre $A/(m) \cong A_m$ que lleva $[a] \mapsto R_m(a)$

Ejemplo 11.2. 2. Si $M_1, ..., M_n$ son A-módulos, su "producto"$M_1 \times ... \times M_n = \prod M_i$ es un A-módulo con $(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$ y $a(x_1, ..., x_n) = (ax_1, ..., ax_n)$

Supongamos que $M_1, ..., M_n$ son submódulos de M y que $M = M_1 \oplus ... \oplus M_n = \oplus_i M_i$ Entonces, existe:

$$\varphi : \prod_i M_i \to M = \oplus_i M_i \tag{4}$$

$$(x_1, ..., x_n) \mapsto x_1 + ... + x_n = \sum_i x_i \tag{5}$$

que es un isomorfismo.

Clasificación de los módulos finitamente generados sobre un dominio euclídeo.

Para comprenderlo mejor, vamos a ver primero un caso particular sencillo.

Módulos cíclicos

Definición 12.1 (Anulador minimal de M). Si M es cualquier módulo, entonces

$$\{a : ax = 0 \ \forall x \in M\} \subseteq A \text{ es un ideal}$$

a cuyo generador llamamos anulador minimal de M, $\mu(M)$, que es único salvo asociados.

Dado un cierto $x \in M$, podemos ver el conjunto $\{a : ax = 0\} \subseteq A$. Este también es un ideal y, a su vez, es principal. Al generador de este se le llama el anulador minimal de x y se le denota:

$$\mu(x)$$

Proposición 12.1. Si expresamos $M = (x_1, ..., x_r) = Ax_1 + ... + Ax_r \implies \mu(M) = mcm(\mu(x_1), ..., \mu(x_r))$

Demostración. $\forall i \ \mu(M)x_i = 0 \implies \forall i = 1, ..., r, \ \ \mu(x_i)/\mu(M)$.

Por tanto, si $a \in A : \mu(x_i)/a \ \forall i \implies ax_i = 0 \ \forall i \implies a\sum_i a_i x_i = \sum_i a_i(ax_i) = 0 \implies ax = 0 \ \forall x \in M \implies \mu(M)/a$ □

En particular, si estamos en un módulo cíclico (generado por un único elemento), entonces $\mu(M) = \mu(x)$ salvo asociados.

Nota. En estos casos, si $\mu(x) = 0$, la aplicación $\varphi : A \to M$ que lleva a cada elemento de A en M de forma $a \mapsto ax$, es lineal, sobreyectiva y es inyectiva, pues $\ker(\varphi) = \{0\}$ (el anulador minimal es el cero), por tanto, es un isomorfismo, $M \cong A$.

Nota. Si $\mu(M) = \mu(x) \neq 0$, la aplicación $\varphi : A/\mu(x) \to M$ tal que $[a] \mapsto ax$ está bien definida (si $a \equiv b \mod (\mu(x)) \implies a = b + q\mu(x) \implies ax = bx + q\mu(x)x = bx$), es lineal, sobreyectiva e inyectiva (si $\varphi([a]) = 0 \implies ax = 0 \implies \mu(x)/a \implies [a] = 0$) , por lo que

$$M \cong A/(\mu(M))$$

Definición 12.2 (Presentacion de M por generadores y relaciones). Sea M un A-módulo finitamente generado. Se llama entonces "Presentación de M por generadores y relaciones" a toda expresión de la forma

$$\langle x_1, ..., x_n : \sum_{i=1}^{n} a_{i1}x_i = 0, ..., \sum_{i=1}^{n} a_{im}x_i = 0 \rangle$$

Donde $(x_1, ..., x_n)$ es un sistema de generadores de M y las expresiones de la derecha son relaciones de dependencia lineal entre ellos verificadas en el módulo tales que cualquier relación de dependencia entre $x_1, ..., x_n$ es combinación lineal de las que aparecen en la presentación

Proposición 12.2. Si

$$\langle x_1, ..., x_n : \sum_{i=1}^{n} a_{i1}x_i = 0, ..., \sum_{i=1}^{n} a_{im}x_i = 0 \rangle$$

es una presentación del módulo M, a la matriz:

$$\mathcal{M}_R = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

cuyas filas son exactamente los coeficientes que aparecen en la presentación la llamamos "matriz de relaciones de los generadores de M".

Decir entonces que las combinaciones lineales de la presentación son cero, es lo mismo que decir:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Si tenemos un módulo A^n, podemos ver que este es libre y finitamente generado, además de que tiene una base (la canónica de $\mathbb{R}^n$). Vamos a considerar una aplicación $\varphi : A^n \to M$ tal que $\varphi : (a_1, ...a_n) = a_1x_1 + ... + a_nx_n$. Esta aplicación es un epimorfirmo.

Proposición 12.3.

$$\sum_{i=1}^{n} a_i x_i = 0 \iff (a_1, ..., a_n) \in \ker(\varphi)$$

En particular, que se verifiquen las relaciones de dependencia que aparecen en la presentación, significa que $F_1, ..., F_m \in \ker(\varphi)$. Y decir que cualquier relación de dependencia entre $x_1, ..., x_n$ es combinación lineal de las que aparecen en la presentación significa que si $F = (a_1, ...a_n) \in \ker(\varphi) \implies$ F es combinación lineal de $F_1, ..., F_m$, por tanto, estamos diciendo que

$$\ker(\varphi) = (F_1, ..., F_m)$$

Nota. Es importante recordar que estos sistemas de generadores pueden ser sometidos a operaciones elementales sin dejar de ser sistemas de generadores. Las operaciones pueden ser:

- Permutar dos de ellos
- Multiplicar uno por una unidad del anillo
- Sumar a uno de ellos un múltiplo de otro

Aún así, la matriz de relaciones se verá alterada y tendremos "otra presentación distinta".

Realizando estas operaciones, siempre podemos llegar a obtener la forma normal de Smith de una matriz.

Proposición 12.4. $\forall M$, existe una presentación cuya matriz de relaciones está normalizada (tiene la forma de una matriz de Smith). Es decir, es de la forma:

$$M : \langle\ y_1, ..., y_n :\ d_1 y_1 = 0\ , ...,\ d_r y_r = 0\ \rangle$$

Es más, si ahora consideráramos un nuevo epimorfismo $\varphi : A^n \to M$ tal que $\varphi(a_1, ...a_n) = \sum a_i y_i$ y

$$\ker(\varphi) = \langle\ d_1 e_1\ \ , ...,\ \ d_r e_r\ \rangle$$

con e_i el vector de la base canónica (tiene un 1 en la posición i-ésima y lo demás son ceros).

Proposición 12.5. Se puede comprobar que:

$$a y_i = 0 \implies \varphi(a e_i) = 0 \implies a e_i \in \ker(\varphi) \implies a e_i = b_1 d_1 e_1 + ... + b_r d_r e_r$$

$$\implies b_1 d_1 e_1 + ... + b_r d_r e_r - a e_i = 0$$

- si $i > r \implies a = 0 \implies \mu(y_i) = 0$.
- si $i \leq r \implies a = b_i d_i$ pues son todos linealmente independientes $\implies d_i / a \implies \mu(y_i) = d_i$

Proposición 12.6. $M \oplus_i A y_i$, todo elemento de M se expresa de forma única como combinación lineal de elementos de A

Demostración. Supongamos que $\sum a_i y_i = 0 \implies \varphi(\sum a_i e_i) = 0 \implies \sum a_i e_i \in \ker(\varphi)$
$\implies a_1 e_1 + ... + a_r e_r + ... + a_n e_n = b_1 d_1 e_1 + ... + b_r d_r e_r \implies a_i = 0\ \forall i > r$
$\implies a_i y_i = 0$

Y si $i \leq r \implies a_i = b_i d_i \implies a_i y_i = 0$ □

También podemos decir, si $d_1 = ... = d_s = 1 \implies y_1 = y_2 = ... = y_s = 0$ y, por tanto, tendríamos que:

$$M = A y_{s+1} \oplus ... \oplus A y_r \oplus ... \oplus A y_n$$

Y tenemos que $\mu(y_i) = d_i \in A$, no es cero ni unidad $\forall i = s+1, ..., r$ y cada d_i / d_{i+1} y $\mu(y_{r+1}) = ... = \mu(y_n) = 0$

Teorema 12.1 (Teorema de estructura de módulos cíclicos). En estas condiciones,

$$M \cong Ay_{s+1} \times ... \times Ay_r \times ... \times Ay_n$$

Siendo $Ay_{s+1}, ..., Ay_r$ módulos cíclicos y desde $r+1$ hasta n, Ay_j es isomorfo al propio anillo, por lo que podemos decir que:

$$M \cong Ad_{s+1} \times ... \times Ad_r \times A^{n-r}$$

A $n-r$ se le llama el rango del módulo y $d_{s+1}, ..., d_r$ es la lista de los factores invariantes del módulo M

La unicidad de estos invariantes es consecuencia de la unicidad de los invariantes de la forma normal de Smith.

Corolario 12.1. Para conocer un módulo, basta conocer la lista de sus factores invariantes y su rango.

Corolario 12.2. Si el rango de un módulo $(n-r)$ es mayor que cero, entonces $\mu(M) = 0$.

Si $n - r = 0$, entonces $\mu(M)$ es el mayor de los factores invariantes, el d_r.

A continuación, ilustraremos el teorema que hemos visto con varios ejemplos:

$\mathbb{Z}$-Módulos. Grupos abelianos.

Vamos a tratar de llevarnos los conceptos que hemos obtenido con el teorema de estructura al caso de los $\mathbb{Z}$–módulos.
Si M es un $\mathbb{Z}$-módulo, $n \in \mathbb{Z}$ con $n > 0$ y $x \in M$, entonces $nx = (\sum_{i=1}^{n} 1)x = \sum_{i=1}^{n} 1 * x = \sum_{i=1}^{n} x$. Lo mismo podemos ver si lo hacemos con n negativo.

Entonces, un $\mathbb{Z}$-módulo es un grupo abeliano. Hablaremos de aquí en adelante de grupos abelianos, aunque sabremos que es lo mismo que un $\mathbb{Z}$–módulo.

Si M es un grupo abeliano y $x \in M$, entonces $\mathbb{Z}x = (x) = \{nx : n \in \mathbb{Z}\}$. Tenemos también que $\mu(x) = d \iff dx = 0$ y $mx = 0 \implies d/m$.

Si $M = \mathbb{Z}x$ y $\mu(x) = 0 \implies M \cong \mathbb{Z}$

Teorema 12.2 (Teorema de estructura en grupos abelianos).
Para todo grupo abeliano finitamente generado M existen enteros positivos $d_1, ..., d_s$ con $d_i \geq 2$ tales que d_i/d_{i+1} y existe un $r > 0$ tal que

$$M \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_s} \times \mathbb{Z}^n$$

y a estos d_i se les llama factores invariantes del grupo abeliano y r es su rango. A la descomposición

que hemos obtenido se le llama descomposición cíclica del grupo abeliano.

Proposición 12.7. Dos grupos abelianos son isomorfos $\iff$ tienen los mismos factores invariantes y el mismo rango. Por tanto, son isomorfos $\iff$ tienen la misma descomposición cíclica.

Proposición 12.8. M es finito $\iff$ su rango es 0. En ese caso, el tamaño del grupo es el producto de sus invariantes $|M| = d_1 ... d_s$ y en tal caso $\mu(M) = d_s$

Proposición 12.9. Si el rango de un módulo M no es cero, entonces $\mu(M) = 0$

Ejemplo 12.1. Un grupo abeliano M está dado por:

$$M : \langle\, x, y, z : 12x + 26y + 13z = 0\ ,\ 6x + 12y + 6z = 0\ ,\ 6x + 26y + 13z = 0 \,\rangle$$

¿Cuál es la descomposición cíclica de este grupo?

Solución. Lo primero que habría que hacer es construir la matriz de relaciones.

$$\begin{pmatrix} 12 & 26 & 13 \\ 6 & 12 & 6 \\ 6 & 26 & 13 \end{pmatrix}$$

Y ahora buscamos su forma normal de Schmidt, para ver cuál es el rango de esta matriz.

$$\begin{pmatrix} 12 & 26 & 13 \\ 6 & 12 & 6 \\ 6 & 26 & 13 \end{pmatrix} \sim \begin{pmatrix} 6 & 12 & 6 \\ 12 & 26 & 13 \\ 6 & 26 & 13 \end{pmatrix} \sim^{C_2 - 2C_1} \begin{pmatrix} 6 & 0 & 6 \\ 12 & 2 & 13 \\ 6 & 14 & 13 \end{pmatrix}$$

Seguimos haciendo este método a llegar a una de la forma de Schmidt y nos queda la matriz:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

(comprobar si está bien).

Así, los factores invariantes de la matriz son 1 y 6, y los factores invariantes de M serán , de los obtenidos de la matriz, los que no sean unidades, por lo que en este caso es el 6. Cuidado, porque si aparecieran dos 6, los factores invariantes serían $\{6, 6\}$.

El rango de M, es el número de columnas nulas de esta matriz, que es 1.

Por tanto, la descomposición cíclica es:

$$M \cong \mathbb{Z}_6 \times \mathbb{Z}$$

□

Ejemplo 12.2. Sea

$$M : \langle x, y, z : 2x + y + 3z = 0\ ,\ 3x + 6y - 2z = 0\ ,\ 2x + 4y + 4z = 0 \rangle$$

¿Cuál es la descomposición cíclica de este grupo?

Solución. :

De nuevo, hallamos su matriz y le hacemos su forma normal de Schmidt

$$\begin{pmatrix} 2 & 1 & 3 \\ 3 & 6 & -2 \\ 2 & 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 48 \end{pmatrix}$$

Y hacemos el mismo procedimiento de antes para hallar sus invariantes (solo el 48), su rango (0) y su descomposición cíclica

$$M \cong \mathbb{Z}_{48}$$

□

Proposición 12.10. Si $(m, n) = 1 \implies \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Si $d = p_1^{e_1} ... p_r^{e_r}$ con p_i primo distintos entre sí y $e_i \geq 1$, entonces:

$$\mathbb{Z}_d \cong \mathbb{Z}_{p_1^{e_1}} \times ... \times \mathbb{Z}_{p_r^{e_r}}$$

Proposición 12.11. Si

$$M \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_s} \times \mathbb{Z}^r$$

con $d_i \geq 2$ y d_i / d_{i+1}, entonces, la descomposición de invariantes en primos estará dada por los mismos primos pero si $d_i = p_1^{e_{i1}} ... p_r e_{ir}$ y tenedremos $0 \leq e_{ij} \leq e_{i+1j}$

Así, podemos tener:

$$M \cong \prod_i^s \prod_j^k \mathbb{Z}_{p_i^{e_{ij}}} \times \mathbb{Z}^r$$

A la que llamamos descomposición cícica Primaria. En ella, la lista $p_i^{e_{ij}}$ es la lista de divisores elementales de M.

Ejemplo 12.3. Un grupo abeliano tiene como divisores elementales: $\{3, 9, 5, 25, 125y7\}$ (que son potencias de primos) y rango 0. Así, ese grupo es, en su descomposición primaria:

$$\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_{125}\mathbb{Z}_7$$

Sus invariantes serían $d_1 = 9 * 125 * 7 = 7875$, $d_2 = 3 * 5^2 = 75$, $d_3 = 5$ y ahora los ordenamos,

quedando que: $d_3 = 9 * 125 * 7 = 7875$, $d_2 = 3 * 5^2 = 75$, $d_3 = 5$, por lo que su descomposición cíclica sería:

$$\mathbb{Z}_5 \times \mathbb{Z}_{75} \times \mathbb{Z}_{7875}$$

Ejercicios

Relación 1

Ejercicio 3

¿Cuál de los siguientes conjuntos son subanillos de los anillos indicados?

1. $a \in \mathbb{Q} \mid 3a \in \mathbb{Z} \subseteq \mathbb{Q}$,
2. $m + 2n\sqrt{3} \mid \ m, n \in \mathbb{Z} \subseteq \mathbb{R}$,
3. $f(x) = \sum a_i x^i \in \mathbb{Z}[x] \mid a_1$es múltiplo de$2 \subseteq \mathbb{Z}[x]$,
4. $f(x) = \sum a_i x^1 \in \mathbb{Z}[x] \mid 2/a_2 \subseteq \mathbb{Z}[x]$.

Comenzamos diciendo que para que un subconjunto B sea un subanillo de un anillo A se tiene que cumplir que:

- $1, -1 \in B$ (contienen al elemento neutro para el producto y su opuesto).
- B es cerrado para la suma y el producto.

Pasemos ahora a analizar los casos descritos arriba.

i. $a \in \mathbb{Q} \mid 3a \in \mathbb{Z} \subseteq \mathbb{Q}$

Este este subconjunto no es un anillo ya que $1, -1 \in \mathbb{Q}$ no están en él, ya que no son múltiplos de 3.

ii. $m + 2n\sqrt{3} \mid \ m, n \in \mathbb{Z} \subseteq \mathbb{R}$

Con $n = 0$ y $m = 1, -1$ tenemos 1 y -1 de $\mathbb{R}$. Además, sean cuales sean n, m de $\mathbb{Z}$ este subconjunto es cerrado para la suma y el producto, dado que la suma de enteros es siempre un entero y lo mismo ocurre con el producto.

iii. $f(x) = \sum a_i x^i \in \mathbb{Z}[x] \mid a_1$es múltiplo de$2 \subseteq \mathbb{Z}[x]$

Con $a_0 = 1, -1$ y $a_i = 0, i > 0$ tenemos el elemento neutro del producto y su opuesto. Además, sean cuales sean los a_i este subconjunto es cerrado para la suma y el producto ya que para los $a_i, i \neq 1$ la suma y producto de números enteros es siempre un número entero y en el caso del a_1, la suma y producto de múltiplos de 2 es siempre un múltiplo de 2.

iv. $f(x) = \sum a_i x^1 \in \mathbb{Z}[x] \mid 2/a_2 \subseteq \mathbb{Z}[x]$

Este subconjunto no es un anillo ya que $1, -1 \in \mathbb{Z}[x]$ no están en él ya que todos sus elementos son monomios de la forma $a_i x^1$.

Relación 2

Ejercicio 1

Calcular las soluciones enteras positivas de la ecuación diofántica $138x + 30y = 12150$**.**

Tenemos la siguiente ecuación:

$$138x + 30y = 12150$$

Para resolverla deberemos calcular los coeficientes de Bezout, para ello realizamos la siguiente tabla:

138	1	0
30	0	1

Ésta es nuestra tabla inicial: ¿cómo la hemos hecho?
Bien, tenemos una ecuación con 2 incógnitas y por tanto 2 coeficientes asociados a cada incógnita. En la tabla inicial ponemos el primer coeficiente con mayor norma (en este caso, con los enteros, es el que tiene mayor valor absoluto - el 138 en este ejercicio), y el menor en la segunda fila. A continuación ponemos como podemos ver en la tabla, en la primera fila (1 0) y en la segunda (0 1). Esto siempre es fijo.

Vamos ahora con el siguiente paso: tenemos que dividir el primer coeficiente entre el segundo y el resto lo pondremos debajo de los coeficientes, es decir:

$138 = 30 \cdot 4 + 18$
El resto es 18 por lo que la tabla sería:

138	1	0
30	0	1
18		

Ahora, ¿qué ponemos en los huecos a la derecha? Muy fácil, solo tenemos que coger el cociente de la división, negarlo, multiplicarlo por el número que tiene encima y sumarlo al número que tiene dos huecos por encima. Es decir, en este caso, tenemos el -4 (el cociente 4 negado):

- Para el primero: $-4 \cdot 0 + 1 = 0 + 1 = 1$
- Para el segundo: $-4 \cdot 1 + 0 = -4$

Por lo que nos queda la siguiente tabla:

138	1	0
30	0	1
18	1	-4

El proceso se ha de repetir hasta que obtengamos en las sucesivas divisiones resto 0. Ahora hacemos la división de 30 entre 18:

$30 = 18 \cdot 1 + 12$

Con coeficientes:
- Primero: $-1 \cdot 1 + 0 = -1 + 0 = -1$
- Segundo: $-1 \cdot -4 + 1 = 4 + 1 = 5$

La tabla ahora sería:

138	1	0
30	0	1
18	1	-4
12	-1	5

Repetimos:

$18 = 12 \cdot 1 + 6$

Con coeficientes:
- Primero: $-1 \cdot -1 + 1 = 1 + 1 = 2$
- Segundo: $-1 \cdot 5 + -4 = -5 + -4 = -9$

La tabla ahora es:

138	1	0
30	0	1
18	1	-4
12	-1	5
6	2	-9

Seguimos dividiendo:

$12 = 6 \cdot 2$

Hemos llegado al resto 0, entonces paramos (no hace falta calcular aquí los coeficientes), por lo que nuestra tabla final es la siguiente:

138	1	0
30	0	1
18	1	-4
12	-1	5
6	2	-9
0		

Nota: los dos últimos coeficientes son los llamados coeficientes de Bezout (2 y -9)

El siguiente paso que debemos tomar a continuación es ver si la ecuación tiene soluciones, ¿cómo lo sabemos? Pues cogemos el número anterior del 0, en nuestro caso es el 6 (qué es el máximo común

divisor de los coeficientes originales de nuestra ecuación) y si divide al término independiente también, entonces la ecuación tiene soluciones enteras.

Dividimos todo entre 6:

$$23x + 5y = 2025$$

Podemos ver que 2025 sigue siendo entero, luego la ecuación tiene soluciones enteras. Ahora veamos como obtener todas las soluciones posibles.

Siempre se utiliza el siguiente esquema, primero va la incógnita con el primer coeficiente que se ha puesto en la tabla, nosotros hemos puesto el 138, luego va primero la "x". Entonces:

$$x = c' \cdot u + b' \cdot k$$

Donde c' es el término independiente una vez se haya dividido por el mcd, en este caso (2025), u es el último coeficiente correspondiente (izquierda para el primero, derecha para el segundo), en este caso (2), b es el coeficiente de la otra incógnita una vez dividida ya por el mcd, es decir, tiene que ser el coeficiente de la y (5); finalmente, la k es un parámetro que puede ser cualquier valor del anillo (en este caso entero).

Para el segundo coeficiente se hace lo mismo solo que con una ligera variación:

$$y = c' \cdot v - a' \cdot k$$

Se hace lo mismo pero en vez de sumar con el coeficiente contrario, resta, es la única diferencia y hay que tener cuidado con no confundirnos en esto.

Dicho esto, obtenemos nuestras ecuaciones generales:

$$x = 2025 \cdot 2 + 5 \cdot k = 4050 + 5k$$
$$y = 2025 \cdot -9 - 23 \cdot k = -18225 - 23k$$

Ahora bien, aun no hemos acabado: nos piden las soluciones enteras POSITIVAS. Luego x e y tienen que ser mayor que 0, simplemente veamos las inecuaciones:

$$x > 0 \implies 4050 + 5k > 0 \implies -810 < k$$
$$y > 0 \implies -18225 - 23k > 0 \implies -792,391... > k \implies -792 > k$$

Entonces tenemos que las soluciones enteras positivas de la ecuación que nos daban son:

$$x = 2025 \cdot 2 + 5 \cdot k = 4050 + 5k$$
$$y = 2025 \cdot -9 - 23 \cdot k = -18225 - 23k$$
$$k \in \{t \in \mathbb{Z} : -810 < t < -792\}$$

Ejercicio 2

"Cuarenta y seis náufragos cansados arribaron a una bella isla. Allí encontraron ciento veintiséis montones de cocos, de no más de cincuenta cada uno, y catorce cocos sueltos, y se los repartieron equitativamente..." (cuento del año 850 a.c.). ¿Cuántos cocos había en cada montón?

Tenemos la siguiente información:
- Hay 46 náufragos.
- Hay 126 montones de cocos (en cada montón no hay mas de 50 cocos).
- Hay 14 cocos sueltos.

Denotamos:
- x ≡ "nº de cocos que hay en cada montón"
- y ≡ "nº de cocos que le tocan a cada náufrago"

Sabemos que se repartieron equitaviamente, luego el número total de cocos que haya dividido entre el número de náufragos debe ser exacto. Esto es, el nº total de cocos (x · 126 + 14) entre el número de náufragos (46) debe dar exacto (y). La ecuación sería:

$$126x + 14 = 46y \implies 126x - 46y = -14$$

Como el ejercicio 1, procedemos a calcular el mcd y los coeficientes de Bezout:

126	1	0
-46	0	1
34	1	2
-12	1	3
10	3	8
-2	4	11
0		

Divisiones hechas:
$126 = -46 \cdot -2 + 34$
$-46 = 34 \cdot -1 + -12$
$34 = -12 \cdot -2 + 10$
$-12 = 10 \cdot -1 + -2$

Veamos facilmente que -14 es divisible entre -2, luego la ecuación tiene soluciones, veamos que tenemos:

$$-63x + 23y = 7$$

Y las siguientes ecuaciones generales:

$$x = 28 + 23k$$

$$y = 77 + 63k$$

$$k \in \mathbb{Z}$$

Ahora acotamos las soluciones, ambas incógnitas deben ser positivas y además x no puede ser más de 50:

$$x > 0 \implies 0 < 28 + 23k \implies k > -1,21... \implies k \geq -1$$

$$x \leq 50 \implies 50 \geq 28 + 23k \implies 0,95... > k \implies k \leq 0$$

$$y > 0 \implies 77 + 63k > 0 \implies -1,2... < k \implies k \geq -1$$

Podemos ver facilmente que o bien k vale 0; o bien, -1. Luego las soluciones son:

Primera solucion:
x = 28 (cocos por montón)
y = 77 (cocos a cada náufrago)

Segunda solución:
x = 5 (cocos por montón)
y = 14 (cocos a cada náufrago)

Ejercicio 3

Disponemos de 15 euros para comprar 40 sellos de correos, de 10, 40, y 60 céntimos y, al menos, necesitamos 2 de cada tipo ¿Cuántos sellos de cada clase podremos comprar?

Nombramos las siguientes variables:
- x ≡ "nº de sellos de 10 cent. comprados"
- y ≡ "nº de sellos de 40 cent. comprados"
- z ≡ "nº de sellos de 60 cent. comprados"

Disponemos de 15 euros (1500 cent.) para comprar estos 3 tipos de sellos, y además tenemos que comprar 40 sellos en total. Tenemos entocnes:

$$1500 = 10x + 40y + 60z$$

$$40 = x + y + z$$

Primero deberemos despejar una incógnita con la segunda ecuación (por ejemplo la z), quedando:

$$5x + 2y = 90$$

Hacemos la tabla:

5	1	0
2	0	1
1	1	-2
0		

Nota: siempre que nos salga mcd = 1, entonces la ecuación tiene solución.

División: $5 = 2 \cdot 2 + 1$

Ahora hacemos las ecuaciones generales (para obtener z basta sustituir x e y en la ecuación del principio):

$$x = 90 + 2k$$

$$y = -180 - 5k$$

$$z = 130 + 3k$$

$$k \in \mathbb{Z}$$

Además sabemos que cada variable mínimo debe ser 2 y como máximo 36, luego:

$$x \geq 2 \implies k \geq -44$$

$$x \leq 36 \implies k \leq -27$$

$$y \geq 2 \implies -36,4 \geq k \implies k \leq -37$$

$$y \leq 36 \implies -43,2 \leq k \implies k \geq -43$$

$$z \geq 2 \implies -42,6... \leq k \implies k \geq -42$$

$$z \leq 36 \implies -31,3.. \geq k \implies k \leq -32$$

Luego k estará acotado así:

$$k \in \{t \in \mathbb{Z} : -42 \leq t \leq -37\}$$

Ejercicio 4

Llueve y, en un mercadillo improvisado en Moscú, un paraguas nos cuesta 190 rublos. Disponemos solo de billetes de 3 rublos, y el vendedor solo de 5 rublos ¿Podremos hacer la compra-venta? ¿Cómo?

Asignamos las siguientes variables:
- x ≡ "nº de billetes de 3 rublos (pagados)"
- y ≡ "nº de billetes de 5 rublos (devueltos)"

Sabemos que 190 no es un múltiplo de 3, luego no podremos pagar exacto. Entonces sabemos claramente que tendremos que pagar más de 190 y además que nos dará una vuelta, luego la ecuacion será:

$$3x - 190 = 5y \implies 3x - 5y = 190$$

Hacemos la tabla (ojo, esta vez la y tiene mayor norma):

-5	1	0
3	0	1
-2	1	-2
1	1	2
0		

Divisiones:
- $-5 = 3 \cdot -1 + -2$
- $3 = -2 \cdot -1 + 1$

Y las ecuaciones generales:

$$y = 190 + 3k$$

$$x = 380 + 5k$$

$$k \in \mathbb{Z}$$

Acotamos k, sabiendo que tenemos que poner como mínimo el valor del paraguas (64 billetes) y que al menos tienen que devolver un billete:

$$x \geq 64 \implies -63,2 \leq k \implies k \geq -63$$

$$y \geq 1 \implies k \geq -63$$

Luego k estará acotado por:

$$k \in \{t \in \mathbb{Z} : t \geq -63\}$$

En particular podremos hacer la compra-venta con k = -63, luego las soluciones más pequeñas serían:
- x = 65 (billetes de 3 rublos entregados)
- y = 1 (billetes de 5 rublos devueltos)

Ejercicio 5

En una torre eléctrica, se nos ha roto una pata de 4 m de altura. Para equilibrarlo provisionalmente, disponemos de 7 discos de madera de 50 cm de grosor y de otros 12 de 30 cm. ¿Cuál de las siguientes afirmaciones es verdadera?
- No podremos equilibrar la torre.
- Podremos equilibrar la torre, y de una única manera.
- Podremos equilibrar la torre, y de dos únicas maneras.
- Podremos equilibrar la torre, y de más de 2 maneras distintas.

Nombramos las variables:
- x ≡ "nº de discos de 50cm"
- y ≡ "nº de discos de 30cm"

Y obtenemos la ecuación:

$$50x + 30y = 400 \implies 5x + 3y = 40$$

Hacemos la tabla:

5	1	0
3	0	1
2	1	-1
1	-1	2
0		

Divisiones hechas:
- $5 = 3 \cdot 1 + 2$
- $3 = 2 \cdot 1 + 1$

Y obtenemos las ecuaciones generales:

$$x = -40 + 3k$$

$$y = 80 - 5k$$

$$k \in \mathbb{Z}$$

Acotamos la k, sabiendo que x e y deben ser positivos o 0; y además solo podemos usar 7 discos de 50cm y 12 de 30cm como máximo:

$$x \geq 0 \implies k \geq 13,3... \implies k \geq 14$$

$$x \leq 7 \implies 15,66... \geq k \implies k \leq 15$$

$$y \geq 0 \implies k \leq 16$$

$$y \leq 12 \implies 13,6 \leq k \implies k \geq 14$$

Luego tenemos que k puede ser 14 o 15, por tanto tenemos dos soluciones:

Primera solución:
- x = 2 (discos de 50cm)
- y = 10 (discos de 30cm)

Segunda solución: - x = 5 (discos de 50cm)
- y = 5 (discos de 30cm)

Ejercicio 6

En el mes pasado, hemos gastado 13 euros y 20 céntimos en 12 llamadas telefónicas a Alemania y Francia, y solo nos cobran el establecimiento de llamada. En las llamadas a Alemania nos cobran

15 céntimos más que a las de Francia. Recordamos que han sido más las llamadas a Francia que a Alemania, pero ¿cuántas llamadas hemos hecho a cada sitio y qué nos han cobrado por cada una?

Nombramos las variables:
- x ≡ "nº de llamadas hechas a Francia"
- y ≡ "nº de llamadas hechas a Alemania"
- z ≡ "coste de una llamada a Francia"
- z + 15 ≡ "coste de una llamada a Alemania"

Tenemos las siguientes ecuaciones:

$$1320 = (z + 15)y + xz$$

$$12 = x + y$$

Despejamos x, y sustituimos, obteniendo:

$$1320 = 15y + 12z$$

Hacemos la tabla:

15	1	0
12	0	1
3	1	-1
0		

Divisiones hechas: $15 = 12 \cdot 1 + 3$

Ecuación final:

$$5y + 4z = 440$$

Ecuaciones generales, x se obtiene sustituyendo x:

$$y = 440 + 4k$$

$$z = -440 - 5k$$

$$x = -428 - 4k$$

$$k \in \mathbb{Z}$$

Ahora acotamos la k, sabiendo que el coste de llamada debe ser mayor que 0, que las llamadas deben ser positivas y menor que 12. En concreto sabemos que debe haber más llamadas a Francia que a Alemania, luego el nº máximo de llamadas de Alemania debe ser 5, y el nº de llamadas mínimas de Francia 6:

$$z < 0 \implies k < -88$$

$$y \geq 1 \implies -109,75 \leq k \implies k \geq -109$$

$$y \leq 5 \implies -108,... \geq k \implies k \leq -109$$

$$x \geq 6 \implies -108,... \geq k \implies k \leq -109$$

$$x \leq 11 \implies -109, \ldots \leq k \implies k \geq -109$$

Luego tenemos una única solución, k = -109, que nos da:
- x = 8 (llamadas a Francia)
- y = 4 (llamadas a Alemania)
- z = 105 (cent. cuesta una llamada a Francia)
- z + 15 = 120 (cent. cuesta una llamada a Alemania)

Ejercicio 7

Una persona va al supermercado y compra 12 cajas de vino, unas de blanco y otras de tinto, por 1200 euros. Si el blanco vale 30 euros más por caja que el tinto, y ha comprado el mínimo posible de tinto ¿Cuántas cajas habrá comprado de cada uno?

Nombramos las variables:
- x ≡ "nº de cajas de vino blanco"
- y ≡ "nº de cajas de vino tinto"
- z ≡ "precio por una caja de vinto tinto"
- z + 30 ≡ "precio por una caja de vino blanco"

Tenemos de esta manera dos ecuaciones:

$$1200 = (z + 30)x + yz$$

$$12 = x + y$$

Despejando la y de la segunda ecuación y sustituyendo en la primera tenemos:

$$30x + 12z = 1200$$

Hacemos la tabla:

30	1	0
12	0	1
6	1	-2
0		

Divisiones hechas: $30 = 12 \cdot 2 + 6$

La ecuación dividida sería:

$$5x + 2z = 200$$

Y las ecuaciones generales (y se obtiene sustituyendo por x):

$$x = 200 + 12k$$

$$z = -400 - 30k$$

$$y = -188 - 12k$$

$$k \in \mathbb{Z}$$

Acotando la k de manera que el precio de una caja debe ser positivo, al igual que el nº de cajas compradas (y menor que 12 - al menos debemos comprar una caja de cada tipo, y comprar 12 en total):

$$z > 0 \implies -13,33... > k \implies k \leq -14$$

$$x \geq 1 \implies -16,... \leq k \implies k \geq -16$$

$$x \leq 11 \implies -15,75 \geq k \implies k \leq -16$$

$$y \geq 1 \implies -15,75 \geq k \implies k \leq -16$$

$$y \leq 11 \implies -16,6 \leq k \implies k \geq -16$$

En concreto, tenemos que hay una única solución, k vale -16, luego las soluciones serían:
- x = 8 (cajas de vino blanco compradas)
- y = 4 (cajas de vino tinto compradas)
- z = 80 (euros vale cada caja de vino tinto)
- z + 30 = 110 (euros vale cada caja de vino blanco)

Ejercicio 8

Un vendedor en el mercado tiene un cesto de manzanas de (muy poco) más de mil. Haciendo grupos de 30 sobran 20 y haciendo grupos de 40 sobran 30. Hallar el número de manzanas que hay en el cesto.

Nombramos las siguientes variables:
- x ≡ "nº de grupos de 30 manzanas"
- y ≡ "nº de grupos de 40 manzanas"
- z ≡ "nº de manzanas totales"

Tenemos las siguientes ecuaciones:

$$z = 30x + 20$$

$$z = 40y + 30$$

Luego igualando las ecuaciones tenemos:

$$3x - 4y = 1$$

Hacemos la tabla:

-4	1	0
3	0	1
-1	1	1
0		

Divisiones hechas: $-4 = 3 \cdot -1 + -1$

La ecuación final sería:

$$-3x + 4y = -1$$

Y las ecuaciones generales (sustituyendo luego z, por alguna):

$$y = -1 - 3k$$

$$x = -1 - 4k$$

$$z = -10 - 120k$$

$$k \in \mathbb{Z}$$

Acotamos x e y (los grupos deben ser positivos y al menos 1), y las manzanas totales (z) más de 1000:

$$x \geq 1 \implies -0,5 \geq k \implies k \leq -1$$

$$y \geq 1 \implies -0,33... \geq k \implies k \leq -1$$

$$z > 1000 \implies k < -8,41 \implies k \leq -9$$

Luego k será:

$$k \in \{t \in \mathbb{Z} : t \leq -9\}$$

En concreto, la solución mínima k = -9, tenemos:
- z = 1070 (manzanas en total)
- x = 35 (grupos de 30 manzanas)
- y = 26 (grupos de 40 manzanas)

Ejercicio 10 - 2 en K[x]

2. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo Z_3[x], de los polinomios $x^4 + x^3 - x - 1$ y $x^5 + x^4 - x - 1$. Encontrar todos los polinomios f (x) y g(x) en Z_3[x], con grado de g(x) igual a 7, tales que $(x^4 + x^3 - x - 1)$ f(x)+$(x^5 + x^4 - x - 1)$ g(x) = $x^4 + x^2 + 1$

Máximo común divisor

$x^5 + x^4 - x - 1$	1	0
$x^4 + x^3 - x - 1$	0	1
$x^2 - 1$	1	-x
0		

Las divisiones realizadas han sido :

• $(x^5 + x^4 - x - 1)/(x^4 + x^3 - x - 1)$

Cociente: x
Resto: $x^2 - 1$

• $(x^4 + x^3 - x - 1)/(x^2 - 1)$

Cociente: $x^2 + x + 1$
Resto: 0

Así, el máximo común divisor es $x^2 - 1$

Mínimo común múltiplo

Usamos que [a,b]=$\frac{ab}{(a,b)}$

$(x^5 + x^4 - x - 1)(x^4 + x^3 - x - 1) = x^9 + 2x^8 + x^7 - x^6 - x^3 + x^2 + 2x + 1$

$(x^9 + 2x^8 + x^7 - x^6 - x^3 + x^2 + 2x + 1)/(x^2 - 1) = x^7 - x^6 - x^5 + x^4 - x^3 + x^2 + x - 1$

Por lo tanto, el mínimo común múltiplo es $x^7 - x^6 - x^5 + x^4 - x^3 + x^2 + x - 1$

Ecuación diofántica

Dividiendo por el máximo común divisor la ecuación para obtener al reducida (vemos que tiene solución) queda:

$(x^2 + x + 1)$ f(x)+$(x^3 + x^2 + x + 1)$ g(x) = $x^2 + 2$

Aplicando la igualdad de Bezout (a partir de los cálculos del máximo común divisor):

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

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

Obtenemos como solución particular:

$f_0(x) = -x^3 - 2x$

$g_0(x) = x^2 + 2$

La solución general quedaría:

$f(x) = -x^3 - 2x + k(x)(x^3 + x^2 + x + 1)$

$g(x) = x^2 + 2 - k(x)(x^2 + x + 1)$

Para cumplir la condición g(x) igual a 7 observamos que el grado de k(x) tiene que ser igual a 5. De este modo, todas soluciones pedidas son las que se obtienen a partir de la general para todos los k(x) de $Z_3[x]$ tal que gr(k(x)) = 5.

Ejercicio 15 - 1 en $\mathbb{Z}[\sqrt{n}]$

En el anillo $\mathbb{Z}[\sqrt{n}]$ calcular
a) mcd$(2 - 3\sqrt{-2}, 1 + \sqrt{-2})$, mcm$(2 - 3\sqrt{-2}, 1 + \sqrt{-2})$.
b) En $\mathbb{Z}[\sqrt{n}]$, calcula mcd$(3 + \sqrt{3}, 2)$ y mcm$(3 + \sqrt{3}, 2)$.

a) Calcularemos primero el mcd, para ello usaremos el método de la tabla que venimos haciendo desde siempre (ver ejercicio 1 de esta relación). Sin embargo, para calcular la norma tendremos que multiplicar el número por su conjugado, en general:

$N(a + b\sqrt{n}) = (a + b\sqrt{n}) \cdot (a - b\sqrt{n}) = x^2 - b^2 n$

Bien, ahora veamos quien tiene mayor norma:
$N(2 - 3\sqrt{-2}) = 4 - 9 \cdot (-2) = 4 + 18 = 22$
$N(1 + \sqrt{-2}) = 1 - 1 \cdot (-2) = 3$

Y hacemos la tabla, pero ¿cómo sacamos el resto y el cociente en $\mathbb{Z}[\sqrt{n}]$? Usemos de ejemplo la división que vamos a tener que hacer:

$$\frac{2 - 3\sqrt{-2}}{1 + \sqrt{-2}}$$

Lo que tenemos que hacer es multiplicar por el conjugado del denominador:

$$\frac{(2 - 3\sqrt{-2})(1 - \sqrt{-2})}{(1 + \sqrt{-2})(1 - \sqrt{-2})} = \frac{-4 - 5\sqrt{-2}}{3}$$

Hemos llegado a un número del tipo $a + b\sqrt{n}$, ahora tenemos que sacar el cociente. Para hacerlo solo debemos sacar la parte entera redondeando, es decir:

$\frac{-4}{3} = -1,333 \implies a = -1$
$\frac{-5}{3} = -1,666 \implies b = -2$
Luego el cociente será: $q = -1 - 2\sqrt{-2}$
Ahora para calcular el resto, sabemos que es el dividendo menos el divisor por el cociente, luego:

$$r = 2 - 3\sqrt{-2} + (1 + \sqrt{-2})(-1 - 2\sqrt{-2}) = -1$$

Hemos acabado, la tabla sería:

$2 - 3\sqrt{-2}$	1	0
$1 + \sqrt{-2}$	0	1
-1	1	$1 + 2\sqrt{-2}$
0		

Concluimos que el mcd$(2 - 3\sqrt{-2}, 1 + \sqrt{-2})$ = -1, ahora para hallar el mcm simplemente tenemos que: $mcm(a, b) = \frac{ab}{mdc(a,b)}$. Luego:

$$[2 - 3\sqrt{-2}, 1 + \sqrt{-2}] = \frac{(2 - 3\sqrt{-2})(1 + \sqrt{-2})}{-1} = -8 + \sqrt{-2}$$

b) Realizamos el mismo proceso que en a). Calculamos las normas:
$N(3 + \sqrt{3}) = 9 - 3 = 6$
$N(2) = 4$

La tabla quedaría:

$3 + \sqrt{3}$	1	0
2	0	1
$-1 - \sqrt{3}$	1	$-2 - \sqrt{3}$
0		

La primera división sería:

$$\frac{3 + \sqrt{3}}{2} \implies q = 2 + \sqrt{3}, r = -1 - \sqrt{3}$$

Y la segunda:

$$\frac{2}{-1 - \sqrt{3}} = 1 - \sqrt{3} \implies q = 1 - \sqrt{3}, r = 0$$

Luego $mcd(3 + \sqrt{3}, 2) = 1 - \sqrt{3}$, y entonces:

$$mcm(3 + \sqrt{3}, 2) = \frac{(3 + \sqrt{3})(2)}{1 - \sqrt{3}} = -2\sqrt{3}$$

Ejercicio 16 - 2 en $\mathbb{Z}[\sqrt{n}]$

Probar que en el anillo $\mathbb{Z}[\sqrt{2}]$ el entero cuadrático $2+\sqrt{2}$ y su conjugado $2-\sqrt{2}$ son asociados. ¿Quiénes son su máximo común divisor y su mínimo común múltiplo?

Bien, sabemos que dos elementos de un anillo son asociados si uno se divide al otro; es decir, x y y son asociados si x divide a y, e y divide a x.

Veamos la norma de ambos elementos:
- $N(2+\sqrt{2}) = 4-2 = 2$
- $N(2-\sqrt{2}) = 4-2 = 2$

Da igual cual dividamos entre cual, como vemos:

$$\sqrt{2+\sqrt{2}}2 - \sqrt{2} = 3 + 2\sqrt{2}$$

$$\sqrt{2-\sqrt{2}}2 + \sqrt{2} = 3 - 2\sqrt{2}$$

Vemos que efectivamente son asociados, ya que uno se divide al otro. En este caso el máximo común divisor puede cogerse como cualquiera de los dos, y el mínimo común múltiplo sería el contrario al que hemos elegido.

Ejercicio 17 - 3 en $\mathbb{Z}[\sqrt{n}]$

a) Determinar un entero de Gauss $\alpha \in \mathbb{Z}[i]$, tal que al dividirlo por 3 da resto i, mientras su resto al dividirlo 3 + 2i es 1 + i.

a) Simplemente realizamos las siguientes ecuaciones:

$$\alpha = 3x + i$$

$$\alpha = (3+2i)y + (1+i)$$

E igualando:

$$3x + (-3-2i)y = 1$$

Sacamos la norma:
- $N(-3-2i) = 9+4 = 13$
- $N(3) = 9$

Hacemos la tabla:

-2-2i	1	0
3	0	1
i	1	1+i
0		

Divisiones hechas: 3-2i = (1-i)3 + i

La ecuación final sería:

$$(-3i)x + (-2+3i)y = -i$$

Como nos pide un entero de Gauss, basta que saquemos una solución particular, obteniendo:

$$y = -i$$

$$x = 1 - i$$

$$\alpha = 3 - 2i$$

b)

Relación 3

Ejercicio 1

Discutir, usando congruencias, la validez de las siguientes afirmaciones:

1) 320^{207} **y** 2^{42} **dan el mismo resto al dividirlos por 13.**

Tenemos que reducir ambos números, hacemos las bases.

$320^{207} \equiv 8^{207} mod(13) \equiv (2^3)^{207} mod(13) \equiv 2^{621}$

Ahora, calculamos los restos de las potencias de 2, hasta ver cuándo se repite uno de los restos:

- $2^1 \equiv_{13} 2$
- $2^2 \equiv_{13} 4$
- ...
- $2^{13} \equiv_{13} 2$

Ahora, como nos ha salido que la potencia es 13, aplicamos la función φ de Euler a 13 para ver con qué número tienen que ser las potencias congruentes.

$$\varphi(13) = 12$$

Por último, como tenemos los dos números en la misma base, tenemos que ver si los exponentes son congruentes módulo 12.

$$621 \equiv_{12} 42 \implies 9 \equiv_{12} 6$$

Por lo que no son congruentes módulo 12, luego los dos números iniciales no dan el mismo resto al dividirlos por 13.

2) $5^{2n+1} + 2^{2n+1}$ **es divisible por 7 cualquiera que sea el entero** $n \geq 1$

Tenemos que ver si $5^{2n+1} + 2^{2n+1} \equiv_7 0$ para $n \geq 1$. Pero $5 \equiv_7 -2$, luego:

$$5^{2n+1} + 2^{2n+1} \equiv_7 -(2)^{2n+1} + 2^{2n+1} \equiv_7 0$$

Luego siempre es divisible por 7 para cualquier entero.

4)Las dos últimas cifras del número 7^{355} **son 4 y 3.**

Para esto, bastaría ver si $7^{355} \equiv 43 mod(100)$. Para ello, vamos a facilitar el cálculo usando la función φ de Euler. $\varphi(100) = 100 * 1/2 * 4/5 = 40$.

Esto implica que $7^{40} \equiv 1 mod(100)$

Vamos a reducir el 7^{355} con módulo 40. Si dividimos 355 entre 40 nos queda un resto de 35, luego $7^{355} \equiv 7^{35} mod(100)$.

Ahora, vamos a calcular las potencias de 7 para ver cuándo se repite el resto al ir añadiendo exponentes.

- $7 \equiv_{100} 7$
- $7^2 \equiv 29 mod(100)$
- $7^3 \equiv 43 mod(100)$
- ...
- $7^5 \equiv_{100} 7$

Luego $7^{35} \equiv_{100} 7^3 \equiv_{100} 43$, pues ya habíamos obtenido ese 43 como resultado de hacer las congruencias de las potencias sucesivas de 7.

4) $3 * 5^{2n+1} + 2^{3n+1}$ **es divisible por 17 cualquiera que sea el entero** $n \geq 1$

Tenemos que volver a ver en este caso, si el número es congruente con 0 módulo 17. Ahora, quitando el n+1 en el 5:

$$3 * 5^{2n+1} + 2^{3n+1} \equiv_{17} 0 \implies 15 * 5^{2n} + 2^{3n+1}$$

Y seguimos desarrollando.

$$15 * 5^{2n} + 2^{3n+1} \equiv \implies -2^{2n} + 2^{3n+1} \equiv_{17} -2 * 8^n + 2^{3n+1} = -2 * 2^{3n} = -(2)^{3n+1} + 2^{3n+1} = 0$$

6) Un número es divisible por 4 si y solo si el número formado por sus dos últimas cifras es múltiplo de 4.

Vamos ver si : $a_n a_{n-1} ... a_1 a_0 \iff a_1 a_0 \equiv_4 0$.

El número vendrá dado: $a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10 + a_0$.

Pero, tomando todas la demás cifras menos las dos últimas, su suma es congruente con 0 módulo 4, luego basta ver si los dos últimos es congruente con 0 módulo 4, pero eso es el enunciado, luego queda probado.

Ejercicio 4

Una banda de 13 piratas se reparten N monedas de oro, pero le sobran 8. Dos mueren, las vuelven a repartir y sobran 3. Luego se ahogan 3 y sobran 5. ¿Cuál es la mínima cantidad posible N de monedas?

$$\begin{cases} N \equiv 8 \bmod(13) \\ N \equiv 3 \bmod(11) \\ N \equiv 5 \bmod(8) \end{cases}$$

Resolvemos el sistema formado por la primera y la tercera ecuación:

$N \equiv 8 \bmod(13) \rightarrow N = 8 + 13 \cdot x$

Sustituimos en la tercera ecuación

$8 + 13 \cdot x \equiv 5 \bmod(8) \rightarrow 5 \cdot x \equiv 5 \bmod(8) \Rightarrow x \equiv 1 \bmod(8)$ (Podemos simplificar el 5 porque $(5,8) = 1$)

$x_0 = 1 \Rightarrow N_0\ 8 + 13 \cdot 1 = 21$ (Solución óptima)

$N \equiv 21 \bmod(8 \cdot 13) = 21 \bmod(104)$

Ahora, resolvemos el sistema con la ecuación anterior y la segunda del sistema inicial

$N \equiv 21 \bmod(104) \rightarrow 21 + 104 \cdot x$

$21 + 104 \cdot x \equiv 3 \bmod(11) \Rightarrow 10 + 5 \cdot x \equiv 3 \bmod(11) \Rightarrow 5 \cdot x \equiv -7 \bmod(11) \Rightarrow 5 \cdot x \equiv 4 \bmod(11)$

Figura 1: mcd

11	1	0
5	0	1
1	1	-2
0		

$1 = 1 \cdot 11 + 5 \cdot (-2) \rightarrow 5 \cdot (-2) \equiv 1 \bmod(11)$

Multiplicamos por 4 y así obtendremos una solución particular

$5 \cdot (-8) \equiv 4 \bmod(11) \Rightarrow x_0 = -8$

Sustituimos y nos queda $N_0 = -811$

$N \equiv -811 \bmod(1144) = 333 \bmod(1144)$ (donde $1144 = [11,104]$)

$N = 333 + 1144 \cdot k$

Solución: La cantidad mínima de monedas sería cuando k vale 0. Entonces el número de monedas es 333

Ejercicio 6

Antonio, Pepe y Juan son tres campesinos que principalmente se dedican al cultivo de la aceituna. Este año la producción de los olivos de Antonio fue tres veces la de los de Juan y la de Pepe cinco veces la de los de Juan. Los molinos a los que estos campesinos llevan la aceituna, usan recipientes de 25 litros el de Juan, 7 litros el de Antonio y 16 litros el de Pepe. Al envasar el aceite producido por los olivos de Juan sobraron 21 litros, al envasar el producido por Antonio sobraron 3 litros y al envasar el producido por Pepe sobraron 11 litros. Sabiendo que la producción de Juan está entre 1000 y 2000 litros ¿cual fue la producción de cada uno de ellos?.

Vamos a plantear primero el problema. Llamamos:

1. A = 3J; P = 5J
2. La capacidad es: J = 25, A = 7 y P = 16.
3. Sobran: J = 21, A = 3, y P = 11.

Así, el sistema a plantear es:

- $J \equiv 21 mod(25)$
- $A \equiv 3 mod(7) \equiv 3J$
- $P \equiv 11 mod(16) \equiv 5J$

Por lo que el sistema resultante es

$$\left.\begin{array}{r} x \equiv 21 mod(25) \\ 3x \equiv 3 mod(7) \\ 5x \equiv 11 mod(16) \end{array}\right\}$$

Tenemos que hacer transformaciones hasta llegar a dejar la x sola en cada una de las ecuaciones en congruencia. Si las hacemos, la transformación es:

$$\left.\begin{array}{r} x \equiv 21 mod(25) \\ 3x \equiv 3 mod(7) \\ 5x \equiv 11 mod(16) \end{array}\right\} \Longrightarrow \begin{cases} x \equiv 21 mod(25) \\ x \equiv 1 mod(7) \\ x \equiv 15 mod(16) \end{cases}$$

Y este es el sistema final a resolver. Para ello, resolvemos dos primero y luego resolvemos esos dos con el siguiente. Resolvemos el de las dos primeras:

Vemos que la primera ecuación es : $x = 21 + y * 25$ lo quenos lleva a la congruencia: $21 + y * 25 \equiv 1 mod(7) \Longrightarrow 4y \equiv 1 mod(7) \Longrightarrow y \equiv 2 mod(7)$ por tanto la solución óptima es $y_0 = 2$ y ahora si $y = 2$, eso implica que (volviendo a la x que habíamos despejado) $x_0 = 21 + 50 = 71$ y si volvemos a expresarlo como congruencias nos queda $x \equiv 71 mod(175)$.

Hemos reducido una ecuación, ahora tendríamos que volver a resolver el sistema

$$\begin{cases} x \equiv 71 mod(175) \\ x \equiv 15 mod(16) \end{cases}$$

Ejercicio 11 - 1 parte K[x] y $\mathbb{Z}\sqrt{n}$

(1). Probar el teorema de Ruffini: *si $f(x) \in A[x]$, entonces $f(a)$ es igual al resto de dividir $f(x)$ entre $x-a$.*

Demostración.
Si A es un Dominio Euclídeo y $f(x) \in A[x]$, entonces $\exists q, r \in A$ tales que
$f(x) = q(x-a) + r$, donde r es el resto al dividir $f(x)$ por $x-a$. Entonces, evaluamos f en a, y tenemos que $f(a) = (a-a)q + r = r$, como queríamos demostrar. □

Nota. La tesis del teorema también puede expresarse como la siguiente congruencia: $f(x) \equiv f(a)\ mod\ (x-a)$.

(2). Encontrar un polinomio $f(x) \in \mathbb{Q}[x]$ de grado 3 tal que:

- $f(0) = 6$
- $f(1) = 12$
- $f(x) \equiv (3x+3)\ mod\ (x^2+x+1)$

Solución. Primero, reescribimos las condiciones del enunciado en términos de congruencias, usando el teorema de Ruffini:

- $f(x) \equiv 6\ mod\ (x)$
- $f(x) \equiv 12\ mod\ (x-1)$
- $f(x) \equiv (3x+3)\ mod\ (x^2+x+1)$

Para resolver este sistema de tres congruencias, lo reducimos en primer lugar a un sistema de dos congruencias, tomando las dos primeras.

Nos centramos en la ecuación $f(x) \equiv 6\ mod\ (x)$, que ya está resuelta: su solución general es $f(x) = 6 + g(x) \cdot x$, con $g(x) \in \mathbb{Q}[x]$. Sustituyendo en la segunda ecuación, nos quedaría $6 + g(x) \cdot x \equiv 12\ mod\ (x-1)$. Resolvamos ahora esta congruencia:

Primero simplificamos la expresión, llegando a $g(x) \cdot x \equiv 6\ mod\ (x-1)$. Calculemos ahora el mcd $(x, x-1)$, calculando además los coeficientes de Bezout:

r	**u**	**v**
x	1	0
$x-1$	0	1
1	1	-1

Vemos que $(x, x–1) = 1$, y haciendo uso de la identidad de Bezout, nos queda que $1 = \mathbf{1}\cdot x+\mathbf{(–1)}\cdot(x–1)$. Como esta forma es la de las soluciones de una ecuación en congruencia, deducimos que $1 \cdot x \equiv 1 \ mod\ (x-1)$, y multiplicando por 6 tenemos que $6 \cdot x \equiv 6 \ mod\ (x-1)$. Si comparamos esta expresión con la ecuación original, es evidente que $g_0(x) = 6$ es una solución particular. Entonces, $f_0(x) = 6 + 6x$ es una solución particular del sistema, y la solución general será:

$$f(x) \equiv f_0(x)\ mod\ ([x, x+1]) \Rightarrow f(x) \equiv 6 + 6x\ mod\ (x^2 - x) \tag{6}$$

Pasamos ahora a resolver, del mismo modo, el sistema formado por la tercera ecuación original, y la ecuación (6).

La solución general de (6) es $f(x) = (6 + 6x) + h(x) \cdot (x^2 - x)$, con $h(x) \in \mathbb{Q}[x]$. Sustituyendo en la tercera ecuación y simplificando, nos quedaría $h(x) \cdot (x^2 - x) \equiv –3 – 3x\ mod\ (x^2 + x + 1)$. Resolvamos ahora esta congruencia, calculando para ello $(x^2 – x, x^2 + x + 1)$, y los coeficientes de Bezout:

r	**u**	**v**
$x^2 – x$	1	0
$x^2 + x + 1$	0	1
$–2x – 1$	1	-1
$\frac{3}{4}$	$\frac{1}{2}x + \frac{1}{4}$	$\frac{-1}{2}x + \frac{3}{4}$

Vemos que $(x^2 – x, x^2 + x + 1) = \frac{3}{4}$, y haciendo uso de la identidad de Bezout, nos queda lo siguiente:

$$\frac{3}{4} = \mathbf{(\frac{1}{2}x + \frac{1}{4})} \cdot (x^2 - x) + \mathbf{(-\frac{1}{2}x + \frac{3}{4})} \cdot (x^2 + x + 1)$$

Dividimos ahora la ecuación por $\frac{3}{4}$, y tenemos que:

$$1 = \left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) + \left(-\frac{2}{3}x + 1\right) \cdot (x^2 + x + 1)$$

Como esta forma es la de las soluciones de una ecuación en congruencia, deducimos que:

$$\left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) \equiv 1\ mod\ (x^2 + x + 1)$$

y ahora multiplicamos por $–3x – 3$:

$$(–3x – 3) \cdot \left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) \equiv –3x – 3\ mod\ (x^2 + x + 1)$$

Si comparamos esta expresión con la ecuación original, es evidente que una solución particular es $g_0(x) = (–3x – 3) \cdot (\frac{2}{3}x + \frac{1}{3}) = –2x^2 – 3x – 1$. Podemos calcular una solución partícular óptima, ya que esta no lo es, sin más que calcular su resto al dividirla por $x^2 + x + 1$, que es $1 – x$. Entonces, $f_0(x) = 6 + 6x + (1 – x)(x^2 – x) = –x^3 + 2x^2 + 5x + 6$ es una solución particular del sistema, y la solución general será:

$$f(x) \equiv f_0(x)\ mod\ ([x^2 - x, x^2 + x + 1]) \Rightarrow f(x) \equiv –x^3 + 2x^2 + 5x + 6\ mod\ (x^4 - x)$$

Entonces, el polinomio pedido sería justamente $f(x) = –x^3 + 2x^2 + 5x + 6$, y podemos comprobar que, efectivamente, se cumplen las condiciones del enunciado.

Ejercicio 13 - 3 parte K[x] y $\mathbb{Z}\sqrt{n}$

Determinar los polinomios $f(x) \in \mathbb{Q}[x]$ de grado menor o igual que tres que satisfacen el sistema de congruencias

$$\left.\begin{aligned} f(x) &\equiv x-1 \ mod(x^2+1) \\ f(x) &\equiv x+1 \ mod(x^2+x+1) \end{aligned}\right\}$$

En primer lugar, reescribimos la primera ecuación para sustituirla en la segunda.

$$f(x) \equiv x-1 \ mod(x^2+1) \implies f(x) = x-1+(x^2+1)g(x)^{\circledast}$$

Reemplazando lo obtenido, tenemos:

$$x-1+(x^2+1)g(x) \equiv x+1 \ mod(x^2+x+1)$$

Pasamos el x-1 restando:

$$(x^2+1)g(x) \equiv 2 \ mod(x^2+x+1)$$

Resolvemos esta ecuación, que tendrá solución si, y solo si, $(x^2+1,\ x^2+x+1)/2$. Así, hallamos el mcd a través de la tablita correspondiente:

x^2+x+1	1	0
x^2+1	0	1
x	1	-1
1	$-x$	$x+1$
0		

Obtenemos de esta forma que $(x^2+1,\ x^2+x+1) = 1$, que divide a 2, por tanto, habrá solución. Partiendo de la identidad de Bezout: $1 = (x^2+x+1)(-x)+(x^2+1)(x+1)$, la transformamos en una ecuación en congruencia (si vemos la ecuación como $(x^2+x+1)(x) = (x^2+1)(x+1)-1$, por la definición de congruencia) $(x^2+1)(x+1) \equiv 1 \ mod(x^2+x+1)$, multiplicando por 2, encontramos la g(x) buscada: $(x^2+1)(2x+2) \equiv 2 \ mod(x^2+x+1)$. $g(x) = 2x+2$.

Sustituyendo en $^{\circledast}$ el polinomio g(x) recién encontrado llegaremos a f_0(x), solución parcial del sistema.

$$f_0(x) = x-1+(x^2+1)g(x) = x-1+(x^2+1)(2x+2) = 2x^3+2x^2+3x+1$$

La solución general será

$$f(x) \equiv f_0(x) mod[x^2+1,\ x^2+x+1]$$

Calculamos el mcm:

$$[x^2+1,\ x^2+x+1] = \frac{(x^2+x+1)(x^2+1)}{1} = x^4+x^3+2x^2+x+1$$

Como el ejercicio pide aquellos polinomios de grado menor o igual que tres, nos basta con la solución parcial, ya que otras soluciones eran polinomios de grado superior al buscado.

Solución: $f_0(x) = 2x^3+2x^2+3x+1$

Ejercicio 15 - 5 parte K[x] y $\mathbb{Z}\sqrt{n}$

En el anillo $Z[\sqrt{3}]$, resolver la congruencia.

$$(1+\sqrt{3})x \equiv 9-4\sqrt{3}\ mod(2\sqrt{3})$$

Primero calculamos el máximo común divisor de $(1+\sqrt{3})$ y $(2\sqrt{3})$.

$$N(1+\sqrt{3}) = \sqrt{1+(\sqrt{3})^2} = \sqrt{1+3} = 2$$

$$N(2\sqrt{3}) = \sqrt{(2\sqrt{3})^2} = 2\sqrt{3}$$

Como $N(1+\sqrt{3}) < N(2\sqrt{3})$ pondremos primero $2\sqrt{3}$

$2\sqrt{3}$	1	0
$1+\sqrt{3}$	0	1
0		

Sabemos que el resto es 0 puesto que:

$$\frac{2\sqrt{3}}{1+\sqrt{3}} = \frac{(2\sqrt{3})(1-\sqrt{3})}{(1+\sqrt{3})(1-\sqrt{3})} = \frac{2\sqrt{3}-6}{1-3} = \frac{2\sqrt{3}-6}{-2} = 3-\sqrt{3}$$

Por lo tanto, el cociente de esta división es $3-\sqrt{3}$ y de resto cero. Quedando el mcd de $(1+\sqrt{3})$ y $(2\sqrt{3})$ es $(1+\sqrt{3})$. Veamos si $(1+\sqrt{3})$ divide $9-4\sqrt{3}$.

$$\frac{9-4\sqrt{3}}{1+\sqrt{3}} = \frac{(9-4\sqrt{3})(1-\sqrt{3})}{(1+\sqrt{3})(1-\sqrt{3})} = \frac{9-9\sqrt{3}-4\sqrt{4}+4(\sqrt{3})^2}{1-(\sqrt{3})^2} = \frac{21-13\sqrt{3}}{-2} = \frac{13\sqrt{3}-21}{2} = \frac{13}{2}\sqrt{3}-\frac{21}{2}$$

El cociente la division es $q = 6$ y el resto es:

$$r = (9-4\sqrt{3}) - 6\cdot(1+\sqrt{3}) = 9-4\sqrt{3}-6-6\sqrt{3} = 3-10\sqrt{3} \neq 0$$

Como $(1+\sqrt{3})$ no divide $9-4\sqrt{3}$. Esta ecuación no tiene solución.

Ejercicio 16 - 6 parte K[x] y $\mathbb{Z}\sqrt{n}$

En el anillo $\mathbb{Z}[i]$, resolver el siguiente sistema de congruencias:

$$\begin{cases} x \equiv i & mod\ (3) \\ x \equiv 1+i & mod\ (3+2i) \\ x \equiv 3+2i & mod\ (4+i) \end{cases}$$

Resolución.

Empezaremos resolviendo el sistema:

$$\begin{cases} x \equiv i & mod\ (3) \\ x \equiv 1+i & mod\ (3+2i) \end{cases}$$

Para ello hallaremos la solución particular de $x \equiv i\ mod\ (3)$. Como i es una unidad del anillo, entonces $\forall a \in \mathbb{Z}[i] \Rightarrow (a,i) = i$. Los coeficientes de Bezout son $0*3+1*i=1$ de manera trivial. Entonces la solución general de la primera ecuación sería $x = i+3*k$.

Ahora sustituimos x en la segunda ecuación, y nos queda la ecuación $i+3k \equiv 1+i\ mod(3+2i)$ de manera equivalente $3k \equiv 1\ mod\ (3+2i)$. Ahora sacaremos los coeficientes de Bezout de 3 y 3+2i.

	3+2i	3
3+2i	1	0
3	0	1
-i	1	-1-i

Por ello, sabemos que $3*(-1-i) \equiv -i\ mod(3+2i)$. Una solución particular será $k = (-1-i)*-i = (i-1)$. La solución general para k será por lo tanto $k = (i-1)+(3+2i)*k'$.

Sustituimos la particular de k en la primera resolución y hallaríamos $M = [3, 3+2i]$ para ver cada cuanto debemos hacer la repetición. Para calcular el mcm recordaremos que $(a,b)*[a,b] = ab \Rightarrow \frac{ab}{(a,b)} = [a,b]$. Entonces para nuestro caso particular $[3, 3+2i] = \frac{9+6i}{-i} = 9i-6$. Así pues la solución será:

$$x = i+3(i-1)+k''(9i-6) = 4i-3+k''(9i-6)$$

Ahora cogemos el sistema:

$$\begin{cases} x \equiv 4i-3\ \ mod\ (9i-6) \\ x \equiv 3+2i\ \ mod\ (4+i) \end{cases}$$

Para resolverlo y hallar (por fin) la solución final haremos lo mismo: hallar la solución general de la primera ecuación (ya resuelta) y sustituir en la segunda, mcm de los módulos y terminamos.

Solución primera ecuación: $4i-3+k''(9i-6)$.

Sustituimos segunda: $4i-3+k''(9i-6) \equiv 3+2i\ \ mod\ (4+i) \rightarrow (9i-6)k'' \equiv 6-2i\ \ mod\ (4+i)$

Hallamos coeficientes de bezout y mcd:

	9i-6	4+i
9i-6	1	0
4+i	0	1
2i	1	1-2i
i	-2	4i-1

Enunciamos solución particular y un indicio de la general: Como $(9i-6)(-2) \equiv i \ mod\ (4i-1) \Rightarrow (9i-6)(-2)(-6i-2) \equiv i(-6i-2)\ mod\ (4i-1) \Rightarrow (9i-6)(12i+4) \equiv (6-2i)\ mod\ (4i-1) \Rightarrow k'' = (12i+4)+[9i-6, 4+i]k'''$

Calculamos [9i-6,4+i]: $\frac{30i-33}{i} = 30 - 33i$

Solución general: $(12i + 4) + (30 - 33i)k'''$

Relación 4

Ejercicio 1

Resuelve las ecuaciones siguientes en los anillos que se indican:

1) 12x = 8 en el anillo $\mathbb{Z}_{20}$.

Lo primero es comprobar si tiene solución. Para ello, tenemos que ver si $(20, 12) = 4(5, 3) = 4$ divide a 8, que sabemos que sí.

Ahora, planteamos la ecuación en congruencias:

$$12x \equiv 8 mod(20) \implies 3x \equiv 2 mod(5) \implies x \equiv 4 mod(5)$$

Luego una solución particular de nuestro problema es 4. Además, es la óptima pues $R_{20}(4) = 4$.

Ahora, las soluciones vendrán dadas por $4 + k * 5$ en $\mathbb{Z}_{20}$, luego son $\{4, 9, 14, 19\}$.

2) 19x = 42 en el anillo $\mathbb{Z}_{50}$.

Para empezar, tiene solución si, y solo si, $(19, 50) = 1$ divide a 42, como resulta evidente a simple vista y lo que nos indica también que nuestro problema tiene exactamente una solución. Como de buenas a primeras no se ve ningún método de simplificación factible para llegar hasta nuestra solución y como estamos en un Dominio de Ideales Principales(DIP) podemos usar la Identidad de Bezout hallada a partir del Algoritmo de Euclides.

r	u	v
50	1	0
19	0	1
12	1	-2
7	-1	3
5	2	-5
2	-3	8
1	8	-21

Explicaremos en este caso como se obtienen los coeficientes de Bezout para el resto 7 dejando claro que los demás restos se sacarán de forma recusirva utilizando el mismo método. Al dividir 19 entre 12 tenemos que:

$$19 = 12(+1) + 7 \implies 7 = 19(+1) + 12(-1) \implies 7 = 19(+1) + (50(+1) + 19(-2))(-1) \implies$$
$$\implies 7 = 50(-1) + 19(+3)$$

A continuación, como $1 = 50(8) + 19(-21)$ tenemos que $19(-21) \equiv 1 mod(50)$ luego solo tendríamos que multiplicar por 42 y tendríamos que $19(-21 * 42) \equiv 42 mod(50)$.

Luego, la conclusión es que $x = -21 * 42 \equiv_{50} 29 * 42 = 1218 \equiv_{50} 18$.

4) 5^{30} **x = 2 en** $\mathbb{Z}_7$

Podemos despejar un poco la ecuación viendo que:

$$5^{30} \equiv_7 -2^{30} = 2^{30}$$

Ahora, como 2 y 7 son primos entre sí, usamos la función φ de Euler y vemos: $2^{\varphi(7)} = 2^6 \equiv_7 1$

Luego resulta que $2^{30} \equiv_7 2^6 \equiv_7 1$

Por lo que $x_0 = 2$ y la solución es $x = 2$

Ejercicio 2

Determina cuántas unidades y cuántos divisores de cero tienen los anillos:

Antes de empezar hemos de tener en cuenta que en estos anillos todos los elementos son o unidades o divisores de cero sólo tenemos que restarle al cardinal del anillo el número de unidades para obtener el número de divisores de cero.

1) $\mathbb{Z}_{125}$

Para ello, basta calcular $|U(\mathbb{Z}_{125})| = \varphi(125) = 125 \cdot (1 - \frac{1}{5}) = 100$, luego como tiene **100 unidades**, tiene **25 divisores de cero**.

2) $\mathbb{Z}_{72}$

Calculamos $\varphi(72) = 72 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 36 \cdot \frac{2}{3} = 24$, hay un total de **24 unidades y 48 divisores de cero**.

3) $\mathbb{Z}_{88}$

Siguiendo el proceso de antes calculamos la función φ de Euler, la cual nos permitirá obtener el número de unidades de este anillo.

Así pues calculamos:

$\varphi(88) = 88 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{11}) = 40$, es decir, $|U(\mathbb{Z}_{88})|$ = **40 unidades** y por tanto hay $88 - 40$ = **48 divisores de cero**.

Recordaremos que los valores de λ *en* $\varphi(\alpha)$ *del tipo* $(1 - \frac{1}{\lambda})$ *son los divisores irreducibles de* α

4) $\mathbb{Z}_{1000}$

Volvemos a hacer lo mismo, $\varphi(1000) = 1000 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5})$ =**400 unidades** y por tanto hay **600 divisores de cero**.

Ejercicio 3

Determina si la igualdad a = b es cierta en los siguientes casos:

Como la interpretación de los paréntesis puede dar lugar a malinterpretaciones consideraremos en los dos primeros apartados la base como un número elevado a otro, y en los dos siguientes consideraremos una base que está elevada a un exponente el cual es base de otra potencia.

1) a $= (9^{55})^9$ **y b** $= (7^{70})^{55}$ **en el anillo** $\mathbb{Z}_{21}$

Partiremos de que $9^{55^9} = 9^{495}$, pero (como 9 y 21 son primos relativos) podemos calcular la función φ de Euler para saber cuantas unidades hay en el anillo y ver "con qué frecuencia se repiten los valores de las potencias"

Entonces: $\varphi(21) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$

Y esto quiere decir que $9^{495} \equiv_{21} 9^{R_{12}(495)} \equiv_{21} 9^3$

Calculamos este valor:

$9^1 \equiv_{21} 9 \quad ; \quad 9^2 \equiv_{21} 18 \quad ; \quad 9^3 \equiv_{21} \mathbf{15 = a}$

Y ahora hacemos lo propio para b $= 7^{70^{55}}$
b es congruente con $7^{10^{55}}$ (usamos $\varphi(21)$ para esto) y $7^{10^{55}} \equiv_{21} 7^{550} \equiv_{21} 7^{R_{12}(550)} \equiv_{21} 7^{16}$

Pero $7^1 \equiv_{21} 7^2 \equiv_{21} ... \equiv_{21} 7^{16} \equiv_{21} \mathbf{7 = b} \Rightarrow$ **a** $\neq$ **b**

2) a $= (2^5)^{70}$ **y b** $= (5^{70})^2$ **en el anillo** $\mathbb{Z}_{21}$

Podemos hacer uso de la función φ del ejercicio anterior, pues estamos en el mismo anillo, así sólo tenemos que repetir el mismo proceso

$2^{350} \equiv_{21} 2^{R_{12}(350)} \equiv_{21} 2^2 \equiv_{21} 4 =$ **a**

Y por su parte para b:

$5^{70^2} \equiv_{21} 5^{140} \equiv_{21} 5^{R_{12}(140)} \equiv_{21} 5^5 \equiv_{21} 17 =$ **b**

Luego: **a** $\neq$ **b**

3) a $= 12^{55^{70}}$ **y b** $= 10^{70^{55}}$ **en el anillo** $\mathbb{Z}_{22}$

Empezaremos calculando la función $\varphi(22)$ que nos será de utilidad en los siguientes ejercicios:

$\varphi(22) = 22 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{11}) = 10$

$a = 12^{55^{70}} = (3 \cdot 4)^{55^{70}} = 3^{55^{70}} \cdot 4^{55^{70}}$

Calculamos por separado cuánto vale cada uno de estos:

$3^{55^{70}}$ $\rightarrow$ Como 3 es primo relativo con 22 podemos hacer uso de la función $\varphi(22)$, por lo que con el teorema de Euler obtenemos que:

$3^{\varphi(22)} \equiv 1 mod(22)$

Y de esto deducimos que:

$3^{55^{70}} \equiv_{22} 3^{R_{\varphi(22)}(55^{70})}$

Aquí entonces tenemos que hallar cuál es la solución de $R_{10}(55^{70}) = R_{10}(5^{70})$. Pero rápidamente observamos que $5^1 \equiv_{10} ... \equiv_{10} 5^n \equiv_{10} 5$ y por tanto $R_{10}(5^{70}) = 5$

En este momento ya podemos calcular cuánto vale $3^{55^{70}}$, que es congruente con 3^5

$$3^1 \equiv_{22} 3 \quad ; \quad 3^2 \equiv_{22} 9 \quad ; \quad 3^3 \equiv_{22} 5 \quad ; \quad 3^4 \equiv_{22} 15 \quad ; \quad 3^5 \equiv_{22} 1$$

Y hacemos lo propio con $4^{50^{70}}$:

No podemos proceder como en lo anterior haciendo uso de la función φ de Euler, pues 4 y 22 no son primos relativos. En su lugar hay que operar de una manera más "rudimentaria", hallando con qué frecuencia se repiten las potencias de 4 en este anillo.

$$4^1 \equiv_{22} 4 \quad ; \quad 4^2 \equiv_{22} 16 \quad ; \quad 4^3 \equiv_{22} 20 \quad ; \quad 4^4 \equiv_{22} 14 \quad ; \quad 4^5 \equiv_{22} 12 \quad ; \quad 4^6 \equiv_{22} 4$$

De esto sacamos que se repiten cada 5, o visto de otra manera, esto quiere decir que $4^{55^{70}} \equiv_{22} 4^{R_5(55^{70})}$, pero como $R_5(55) = 0 \Rightarrow 4^{55^{70}} \equiv_{22} 4^5$

Uniendo ambos resultados vemos que el producto de esto nos queda $1 \cdot 12 = 12 =$ **a**

Y ahora calculamos *b*:

$10^{70^{55}} = 5^{70^{55}} \cdot 2^{70^{55}}$

Repetimos el mismo o procedimiento, calculamos por separado el valor de cada uno de los términos y luego multiplicamos. Siguiendo el criterio de "si son primos relativos con 22 podemos usar la función φ de Euler y si no tendremos que estudiar las repeticiones en las potencias".

De este modo obtenemos:

$2^{70^{55}} \equiv_{22} 2^{R_{10}(70^{50})} \Rightarrow \equiv_{22} 2^{10} \equiv_{22} 12$ *(Mediante repeticiones en las potencias)*

$5^{70^{55}} \equiv_{22} 5^{R_{\varphi(22)}(70^{55})} \equiv_{22} 5^{10} \equiv_{22} 1$ *(Mediante la función φ de Euler)*

Con lo que concluimos que el producto es:

$$12 \cdot 1 = 12 = \mathbf{b}$$

Afirmando en este caso que **a y b son iguales**

4) a $= 5^{5^{70}} \cdot 11^{5^{70}}$ **y b** $= 10^{70^{22}}$ **en el anillo** $\mathbb{Z}_{22}$

Volvemos a hacer lo mismo que antes. Calculamos primero el valor de a:

$5^{5^{70}} \equiv_{22} 5^{R_{\varphi(22)}(5^{70})} \equiv_{22} 5^5 \quad ; \quad$ (*Observamos que* $R_{\varphi(22)}(5^{70}) = 5$)

Luego $5^5 \equiv_{22} 1$

$11^{5^{70}} \equiv_{22} ? \rightarrow$ No podemos usar $\varphi(22)$ pues 11 y 22 no son primos relativos, pero rápidamente apreciamos

que:

$11^x \equiv_{22} 11 \; \forall \; x \in \mathbb{N}$

Obteniendo como resultado **a = 11 · 1 = 11**

Para b calculamos el producto de:

$2^{70^{22}} \equiv_{22} 2^{R_{10}(70^{22})} \equiv_{22} 2^{10} \equiv_{22} 12$

(Como 2 y 22 son primos estudiamos las repeticiones de las potencias de 2 en $\mathbb{Z}_{22}$*)*

$5^{70^{22}} \equiv_{22} 5^{R_{10}(70^{22})} \equiv_{22} 1$

Con lo que nos queda **1 · 12 = 12 = b**

Y finalizamos concluyendo que **a** $\neq$ **b**

Ejercicio 5 - 2 en anillos de restos de K[x]

Sea $\mathcal{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$ **el anillo de restos del anillo** $\mathbb{Z}_3[x]$ **módulo** $x^2 + 1$**.**

Vamos primero a describir los polinomios que hay:

$$\mathcal{F}_9 = \mathbb{Z}_3[x]_{x^2+1} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Por tanto, este anillo tiene 9 polinomios:

1) Argumentar que $\mathcal{F}_9$ **es un cuerpo**

Para ello, tenemos que ver si $x^2 + 1$ es un irreducible en $\mathbb{Z}_3[x]$. Vemos si tiene raíces, dándole los valores 0, 1 y 2 y vemos que en ningún caso el resultado es cero, por tanto es irreducible por la afirmación: Si $f(x)$ no es irreducible $\exists x - a : x - a / f \implies f(a) = 0$

Entonces, $\mathcal{F}_9$ es un cuerpo.