Divisibilidad.

De aquí en adelante, A denotará a un anillo conmutativo con identidad, a menos que se establezca lo contrario.

Def. Sea A un anillo y $a, b \in A \ni a \neq 0$. Entonces a divide a b, o b es multiplo de a, a lo que se escribe $a \mid b$, si existe $c \in A \ni b = ac$.

Proposición.

Sean $a, b, c \in A$, con $a \neq 0$. Entonces:

i) $a \mid 0$.

ii) $1 \mid a$.

iii) $a \mid 1 \iff a \in A^*$

iv) Si $a \mid b$ y $b \mid c$ $(b \neq 0) \Rightarrow a \mid (bx + cy)$ con $x, y \in A$.

v) $a \mid a$.

vi) Si $b \neq 0$ & $a \mid b$ & $b \mid c \Rightarrow a \mid c$.

vii) Si $b \neq 0$ y $a \mid b$ & $b \mid a$, con a no div. de cero entonces existe u unidad de A $\ni$ $b = au$ y $a = bu^{-1}$.

Dem:

En A definimos la sig. relación: $\forall\, a,b \in A$:

$$a \sim b \iff \exists\, u \in A^* \text{ m } a = bu$$

Tenemos que $\sim$ es rel. de equivalencia.

i) Reflexiva: $a \sim a$, pues $\exists\, 1 \in A$ m $a = a \cdot 1$, $\forall\, a \in A$.

ii) Simétrica: $\forall\, a,b \in A$, si $a \sim b$ y $b \sim a \Rightarrow \exists\, u \in A^*$ m $a = bu \Rightarrow b = au^{-1}$ $(u^{-1} \in A^*) \Rightarrow$ $b \sim a$.

iii) Transitividad: $\forall\, a,b,c \in A$, si $a \sim b$ y $b \sim c \Rightarrow \exists\, u,v \in A^*$ m $a = bu$ y $b = cv \Rightarrow$ $a = cuv$, con $uv \in A^* \Rightarrow a \sim c$.

Bajo esta relación, $a \sim b$ entonces decimos que a y b son asociados. Si $a \in A$,

$$[a] = \{au \mid u \in A^*\} = aA^*$$

$$[1] = A^*$$

Obs) Si A es dominio entero, entonces $\forall\, a,b \in A$, $a \sim b \iff a \mid b$ & $b \mid a$. En efecto, si $a \sim b$ es claro que $a \mid b$ y $b \mid a$. Recíprocamente, si $a \mid b$ & $b \mid a \Rightarrow \exists\, u,v \in A^*$ m $a = bu$ y $b = av \Rightarrow$ $a = auv \Rightarrow a(1-uv) = 0$, con $a \neq 0 \Rightarrow uv = 1 \Rightarrow u,v \in A^*$ y $u = v^{-1}$. $\therefore a \sim b$.

Def. Sean $a,b \in A \setminus \{0\}$. Se dice que $d \in A$ es un máximo común divisor de a y b, a lo que se escribe $d = (a,b)$, si

i) $d \neq 0$.

ii) $d \mid a$ y $d \mid b$.

iii) Si $d' \in A$ es tal que $d' \neq 0$, $d' \mid a$ y $d' \mid b \Rightarrow d' \mid d$.

Obs) La relación de "ser divisor" entre elementos de A es una relación reflexiva y transitiva, lo cual hace $(A, \mid)$ un conjunto preordenado, y bajo esta relación, $\forall\, a,b \in A$, $a \neq 0, b$, entonces un máximo común divisor de a & b, en caso de que exista, es un elemento maximal bajo esta relación.

Obs) Sea A un dominio entero y $a,b \in A\setminus\{0\}$. Si existe un máximo común divisor de a & b, entonces cualquier otro es asociado con éste. Es decir, si d y d_1 son máximos comunes divisores de a & $b \Rightarrow d \mid d_1$ & $d_1 \mid d \Rightarrow d \sim d_1$.

Recíprocamente, si $d=(a,b)$ y $d_1 \in A$ ∋ $d_1 \sim d$, entonces $d_1=(a,b)$, ya que si $u \in A^*$ ∋ $d_1 = du \Rightarrow d_1 \mid a$ & $d_1 \mid b$; además si $p \in A$ ∋ $p \mid a$ y $p \mid b \Rightarrow p \mid d \Rightarrow p \mid d_1$. Así que d_1 es máx-

¿. imo común divisor de a y b.

Por lo tanto, si A es dominio entero, y existe un máximo común divisor de a y b, entonces el máximo común divisor es $[d]$ donde d es un máximo común divisor. En ocasiones expresamos esto como:

$$d=(a,b)=\text{mcd}\{a,b\}$$
$$[d]=(a,b)$$

Obs) Con respecto a $\mathbb{Z}$ no hay tanto problema, pues si $d \in \mathbb{Z}\setminus\{0\}$, entonces

$$[d]=d\mathbb{Z}^*=d\{1,-1\}=\{d,-d\}$$

Proposición.

Sea A un dominio entero, entonces:

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

ii) $((a,b),c)=(a,(b,c))$.

iii) $(0,a)=a$.

iv) $(a,b)=(-a,b)=(a,-b)=(-a,-b)$.

v) Si $u \in A^*$, $(u,u)=u$.

vi) $(ca,cb)=c(a,b)$

Donde las igualdades son bajo ser asociados.

Dem:

Proposición.

Sea A un dominio entero y $a,b,c \in A$ $\ni$ $a|bc$ con $(a,b)=1 \Rightarrow a|c$.

Dem:

Def. Sean $a, b \in A$ con $a \neq 0$, $b \neq 0$. Decimos que $m \in A$ es un mínimo común múltiplo de a y b, a lo que se escribe $m = [a,b] = mcm\{a,b\}$, si

i) $m \neq 0$.

ii) $a | m$ y $b | m$.

iii) Si $m' \in A \setminus \{0\}$ es tal que $a | m'$ y $b | m'$ $\Rightarrow$ $m | m'$.

Obs) Notemos que la def. de divisibilidad es equivalente a la condición: $\forall\, a, b \in A$, $a \neq 0$, $\langle b \rangle \subseteq \langle a \rangle$. Es decir:

$$a \mid b \iff \langle b \rangle \subseteq \langle a \rangle$$

Def. Sean $a_1, \dots, a_n \in A \setminus \{0\}$. Decimos que $a_1, \dots, a_n$ son **primos relativos** o **coprimos**, si $(a_1, \dots, a_n)$ es una unidad, lo que se escribe $(a_1, \dots, a_n) = 1$.

Def. Un dominio entero A se dice que es **dominio de ideales principales** (DIP), si todo ideal de A es principal, i.e $\forall\, I$ ideal de A, existe $a \in A \ni I = \langle a \rangle$.

Teorema.

En un DIP A, existe siempre el máximo común divisor de dos elementos no ambos cero. Más aún, si $a_1, \dots, a_n \in A$, no todos cero y $d = (a_1, \dots, a_n)$, entonces $d = r_1 a_1 + \dots + r_n a_n$.

Dem:

Consideremos el ideal $I = \langle a_1, \dots, a_n \rangle$. Sea $d \in A \ni I = \langle d \rangle$. Notemos que $\langle a_i \rangle \subseteq I = \langle d \rangle$, $\forall\, i \in [\![1, n]\!]$. Entonces $d \mid a_i$, $\forall\, i \in [\![1, n]\!]$.

Sea ahora $p \in A \ni p \mid a_i$ $\forall\, i \in [\![1, n]\!] \Rightarrow \langle a_i \rangle \subseteq \langle p \rangle$, $\forall\, i \in [\![1, n]\!] \Rightarrow \langle d \rangle = \langle a_1, \dots, a_n \rangle \subseteq \langle p \rangle \Rightarrow d \mid p$. Por tanto $d = (a_1, \dots, a_n)$ & $d = r_1 a_1 + \dots + r_n a_n$.

q.e.d.

Corolario.

Sea A un DIP & $a, b, c \in A \ni a \mid bc$ con $(a, b) = 1 \Rightarrow a \mid c$.

Dem:

$\exists\, r, s \in A \ni ar + bs = 1 \Rightarrow a \mid (acr + bcs) = c$.

q.e.d.

Def. Sea $p \in A$ con $p \neq 0$ & $p \notin A^*$. Entonces:

i) p es **elemento primo de A**, si: $\forall\, a, b \in A$, $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

ii) p es elemento irreducible (de A), si $\forall a,b \in A$, $p=ab \Rightarrow a\in A^*$ ó $b\in A^*$.

Obs) Si A es dominio entero, entonces p elemento primo $\Rightarrow$ p elemento irreducible. En efecto, sea p elemento primo de A. Si $a,b\in A$ son tales que $p=ab \Rightarrow p\mid ab \Rightarrow p\mid a$ ó $p\mid b$.

Si $p\mid a \Rightarrow \exists\, r\in A$ $\ni$ $a=pr \Rightarrow p=ab=pbr \Rightarrow p(1-br)=0$. Como A es dominio entero $\Rightarrow 1-br=0 \Rightarrow b\in A^*$.

Similarmente, si $p\mid b \Rightarrow a\in A^*$. Por tanto p es irreducible.

La recíproca no necesariamente se cumple. Consideremos el dominio entero $\mathbb{Z}[\sqrt{-5}]$, y sea $p=1+\sqrt{-5}\neq 0$ & $N(p)=1+5=6\neq \pm 1$. Luego $p\neq 0$ & $p\notin A^*$. Sean $a+b\sqrt{-5}$, $c+d\sqrt{-5}\in A$ $\ni$

$$(a+b\sqrt{-5})\cdot(c+d\sqrt{-5})=p$$

Aplicando normas:

$$\Rightarrow (a^2+5b^2)(c^2+5d^2)=6$$

Luego $a^2+5b^2=1,2,3$ ó 6. Pero $a^2+5b^2\neq 2,3$. Así $a^2+5b^2=1,6$, luego:

$$N(a+\sqrt{-5}\,b)=1 \quad ó \quad N(c+\sqrt{-5}\,d)=1$$

$$\Rightarrow a+\sqrt{-5}\,b\in A^* \quad ó \quad c+d\sqrt{-5}\in A^*$$

i.e, p es irreducible pero no es primo.

Pero no es primo, pues:

$$(1+\sqrt{-5})=p \mid (1+\sqrt{-5})(1-\sqrt{-5})=6=2\cdot 3$$

Con $p\nmid 2$ & $p\nmid 3$, ya que si $p\mid 2 \Rightarrow \exists\, a+b\sqrt{-5}\in\mathbb{Z}[\sqrt{-5}]$ $\ni$

$$2=(1+\sqrt{-5})(a+b\sqrt{-5})$$

$$\Rightarrow 4=6(a^2+5b^2)\Rightarrow 3\mid 4 \ \text{⨳c}.$$

Similarmente, $p\nmid 3$. Por tanto $1+\sqrt{-5}$ no es elemento primo.

Proposición.

Si A es DIP, los conceptos de elemento primo y elemento irreducible son equivalentes.

Dem:

Sea $p \in A$ elemento irreducible y $a, b \in A$ ⫪ $p | ab$. Por demostrar que $p | a$ o $p | b$. Como $\langle p \rangle \neq A$ y A tiene identidad, $\exists M$ ideal maximal de A ⫪ $\langle p \rangle \subseteq M$. Expresamos $M = \langle d \rangle$ $\Rightarrow \exists c \in A$ ⫪ $p = dc$. Como p es elemento irreducible y M es maximal $\Rightarrow c \in A^* \Rightarrow p$ y d son asociados $\Rightarrow \langle p \rangle = M \Rightarrow \langle p \rangle$ es ideal primo con $ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ o $b \in \langle p \rangle \Rightarrow$ $p | a$ o $p | b$.

q.e.d.

Corolario.

$\mathbb{Z}[\sqrt{-5}]$ no es DIP.

Teorema.

Sea A un DIP y sea M ideal de A con $M \neq A$ y $M = \langle p \rangle$, $p \in A$. Entonces, las sig. condiciones son equivalentes:

i) M es maximal.

ii) M es primo.

iii) p es elemento primo.

iv) p es irreducible.

Dem:

i) $\Rightarrow$ ii): ya se tiene.

ii) $\Rightarrow$ iii): Supongamos que M es ideal primo. Sean $a, b \in A$ ⫪ $p | ab \Rightarrow ab \in \langle p \rangle = M \Rightarrow$ $a \in M$ o $b \in M \Rightarrow p | a$ o $p | b$.

iii) $\Leftrightarrow$ iv): ya se tiene.

iv) $\Rightarrow$ (i): Sea I un ideal de A $\ni$ $M \subseteq I \subseteq A$, con $I = \langle c \rangle$. Luego $\exists$ $f \in A$ $\ni$ $p = cf \Rightarrow$ $c \in A^*$ o $f \in A^*$. Si $c \in A^* \Rightarrow I = A$. Si $f \in A^* \Rightarrow p \sim c \Rightarrow \langle p \rangle = \langle c \rangle \Rightarrow M = I$. i.e M es maximal.

q.e.d.

Anillos Noetherianos.

Def. Sea A un anillo conmutativo con 1. Decimos que A es Noetheriano, si todo ideal de A es finitamente generado.

Obs) Todo DIP es noetheriano.

Teorema.

Sea A anillo conmutativo con identidad. Entonces, las sig. son equivalentes:

i) A es noetheriano.

ii) (Propiedad de cadena ascendente) Toda sucesión $\{I_n\}_{n \in \mathbb{N}}$ de ideales de A $\ni$ $I_n \subseteq I_{n+1}$ $\forall$ $n \in \mathbb{N}$, existe $m \in \mathbb{N}$ $\ni$ $I_k = I_m$, $\forall$ $k \geq m$.

iii) Toda familia no vacía de ideales de A tiene elementos maximales.

Dem:

i) $\Rightarrow$ ii): Sea $\{I_n\}_{n \in \mathbb{N}}$ una familia de ideales de A $\ni$ $I_n \subseteq I_{n+1}$, $\forall$ $n \in \mathbb{N}$. Definimos:

$$I := \bigcup_{n=1}^{\infty} I_n$$

Por ser $\{I_n\}_{n \in \mathbb{N}}$ una cadena, entonces I es ideal de A. Por hipótesis, $\exists$ $a_1, \dots, a_r \in A$ $\ni$

$$I = \langle a_1, \dots, a_r \rangle$$
$$= \langle r_1 a_1 + \dots + r_r a_r \mid r_i \in A \,;\, i \in [\![1, n]\!] \}$$

Por tanto, $a_i \in \bigcup_{n \in \mathbb{N}} I_n$, $\forall$ $i \in [\![1, r]\!]$. Así, $\exists$ $n_i \in \mathbb{N}$ $\ni$

$$a_i \in I_{n_i}$$

Sin pérdida de generalidad, podemos suponer que $I_{n_1} \subseteq I_{n_2} \subseteq \dots \subseteq I_{n_r}$. De aquí que:

$$a_i \in I_{n_r}, \ \forall i \in [\![1,r]\!]$$

$$\Rightarrow I = \langle a_1, \dots, a_r \rangle \subseteq I_{n_r} \subseteq I$$

$$\therefore I_{n_r} = I$$

Así $I_K = I_{n_r}, \ \forall K \geq n_r$.

ii) ⇒ iii): Sea $\mathcal{F}$ una familia no vacía de ideales de A. Sabemos que $\mathcal{F}$ es un conjunto parcialmente con la relación de contención. Suponemos que $\mathcal{F}$ no contiene elementos maximales. Como $\mathcal{F} \neq \emptyset$, elegimos $I_1 \in \mathcal{F}$. Como $\mathcal{F}$ no tiene elementos maximales, existe $I_2 \in \mathcal{F}$ m $I_1 \subsetneq I_2$. Supóngase construidos $I_1, \dots, I_n \in \mathcal{F}$ m $I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n$. Como $\mathcal{F}$ no tiene elementos maximales, $\exists$ $I_{n+1} \in \mathcal{F}$ m $I_n \subsetneq I_{n+1}$. Por inducción hemos construido una sucesión $\{I_n\}_{n \in \mathbb{N}}$ de ideales de $\mathcal{F}$ estrictamente creciente, lo cual es una contradicción. #c.

Por lo tanto, $\mathcal{F}$ debe tener elementos maximales.

iii) ⇒ i): Definimos

$$\mathcal{F} = \{ J \mid J \text{ es ideal de } A \text{ f.g. y } J \subseteq I \}$$

$\mathcal{F} \neq \emptyset$ pues $\langle 0 \rangle \in \mathcal{F}$. Así, por hip. $\mathcal{F}$ tiene elementos maximales. Sea J_0 un elemento maximal de $\mathcal{F}$. J_0 es f.g. (i.e $\exists\, b_1, \dots, b_t \in A$ m $J_0 = \langle b_1, \dots, b_t \rangle$) y $J_0 \subseteq I$. Afirmamos que $J_0 = I$. En efecto, si $J_0 \neq I$, $\exists\, a \in I$ m $a \notin J_0 \Rightarrow J_0 \subsetneq \langle b_1, \dots, b_t, a \rangle \subseteq I$ #c. Pues J_0 es maximal. Luego $J_0 = I$.

Así, A es noetheriano.

q.e.d.

Teorema.

Sea A un DIP. Entonces, para cada $a \in A, a \neq 0$ & $a \notin A^*$, a se expresa como un producto finito de elementos irreducibles de A, y la descomposición es única, salvo orden y asociados.

Dem:

Sea $a \in A$ con $a \neq 0$ y $a \notin A^*$. Sea $I = \langle a \rangle$. Notemos que $I \neq A$, luego, sea $P_1 = \langle p_1 \rangle$ ideal maximal de A (Por ser DIP) $\ni$ $I \subseteq P_1$, es decir, $\langle a \rangle \subseteq \langle p_1 \rangle \Rightarrow p_1 | a \Rightarrow \exists\, a_1 \in A \ni a = p_1 a_1$. Si $a_1 \in A^*$, ya terminamos.

Si $a_1 \notin A^*$, como $a_1 \neq 0$, podemos hacer el mismo procedimiento de a para a_1, luego $\exists$ un elemento irreducible $p_2 \in A \ni p_2 | a_1 \Rightarrow \exists\, a_2 \in A \ni a_1 = p_2 a_2$.

Notar que $\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle$ & $a = p_1 p_2 a_2$. Si $a_2 \in A^*$, habremos terminado. En caso contrario, seguimos con el proceso ya que $a_2 \neq 0$ y $a_2 \notin A^*$. Así que, en el n-ésimo paso habremos construido $p_1, \dots, p_n$ elementos irreducibles y $a_1, \dots, a_n \in A \ni$

$$a = p_1 p_2 \cdot \ldots \cdot p_n a_n$$

Con $\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \ldots \subseteq \langle a_n \rangle$. Si $a_n \in A^*$, habremos terminado. En caso contrario, $a_n \neq 0$ y $a_n \in A^*$, y seguiremos con el proceso se tendrá que:

$$\langle a \rangle \subseteq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \ldots \subsetneq \langle a_n \rangle \subsetneq A$$

Luego entonces el proceso debe terminar en una cantidad finita de pasos, pues A es noetheriano.

Podemos decir que:

$$a = p_1 p_2 \cdot \ldots \cdot p_n p_{n+1} \cdot a_{n+1}$$

Donde $p_1, \dots, p_{n+1}$ son elementos irreducibles de A y $a_{n+1} \in A^*$.

Probemos la unicidad de la descomposición. Expresemos dos descomposiciones:

$$p_1 \cdot \ldots \cdot p_n = a = q_1 \cdot \ldots \cdot q_m$$

donde los p_i's & los q_i's son irreducibles. Podemos suponer $n \leq m$. Así:

$$p_1 | q_1 \cdot \ldots \cdot q_m \Rightarrow \exists\, j \in [\![1, m]\!] \ni p_1 | q_j$$

Sin pérdida de generalidad, podemos suponer que $j = 1$, i.e $p_1 | q_1 \Rightarrow \exists\, u_1 \in A \ni q_1 = u_1 p_1 \Rightarrow u_1 \in A^*$ (p_1 y q_1 son asociados). Luego,

$$p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m = p_1 q_2 \cdot \ldots \cdot q_m u_1$$

Cancelando p_1 obtenemos que

$$p_2 \cdot \ldots \cdot p_n = q_2 \cdot \ldots \cdot q_m u_1$$

Siguiendo con el proceso y sin pérdida de generalidad, $\exists\ u_1, \ldots, u_n \in A^*$ tq

$$q_i = p_i u_i,\ \forall i \in [\![1, n]\!] \ \&$$

$$1 = q_{n+1} \cdot \ldots \cdot q_m \cdot u_1 \cdot \ldots \cdot u_n$$

Como los q_i's son irreducibles, necesariamente todos deben de cancelarse, i.e $n = m$ y

$$q_i = p_i u_i,\ \forall i \in [\![1, n]\!].$$

i.e la des. es única salvo asociados.

q.e.d.

Def. Sea A anillo conmutativo con 1. Se dice que A es un **dominio de factorización única** (**DFU**) si A es dominio entero y cada elemento de A no cero se expresa como un producto finito de elementos irreducibles y la descomposición es única salvo asociados.

Obs) Todo DIP es DFU. Además todo campo es DFU (también, notemos que todo campo es DIP).

1\. El anillo $\mathbb{Z}$ es DFU.

Proposición.

Sea A DFU. En A el concepto de ser elemento irreducible es equivalente, i.e es equivalente a ser elemento primo.

Dem:

Basta probar que elemento irreducible es primo. Sea $p \in A$ irreducible. Sean $a, b \in A$ tq $p | ab$. Probaremos que $p | a$ o $p | b$.

Sea $c \in A$ tq $pc = ab$. Si $a = 0$ o $b = 0 \Rightarrow p | a$ o $p | b$. Suponemos $a, b \neq 0$. Si a

$\in A^* \Rightarrow b = pca^{-1} \Rightarrow p|b$. De forma análoga, si $b \in A^* \Rightarrow p|a$. Suponemos que $a, b \neq 0$ y $a, b \notin A^*$. Entonces expresamos a a y b como un producto finito de elementos irreducibles. Sea esta factorización como:

$$a = p_1 \cdot \ldots \cdot p_t \quad y \quad b = q_1 \cdot \ldots \cdot q_s$$

$$\Rightarrow p_1 \cdot \ldots \cdot p_t \cdot q_1 \cdot \ldots \cdot q_s = pc$$

donde c es no cero y no unidad, con lo cual c tiene su propia descomposición en un producto finito de elementos irreducibles.

Como A es DFU, en particular, p es asociado a un p_i o a un q_j. Esto implica que $p|a$ o $p|b$.

Por tanto p es elemento primo.

q.e.d.

Def. Sea A un anillo conmutativo con 1. Decimos que A es un dominio euclidiano (DE) si A es un dominio entero y existe una función $\delta : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ tal que satisface las sig. propiedades:

i) $\forall\, a, b \in A \setminus \{0\}$, $\delta(ab) \geq \delta(a)$.

ii) $\forall\, a, b \in A$, con $a \neq 0$, $\exists\, q, r \in A$ m $b = qa + r$, donde $0 \leq \delta(r) < \delta(a)$ o $r = 0$.

(Algoritmo de la división).

EJEMPLOS.

1. $\mathbb{Z}$ es DE con función $\delta = |\cdot|$.
2. Si A es DE con función δ, entonces también lo es con función δ^n $(n \in \mathbb{N})$.
3. Si K es campo entonces K es DE con función $\delta : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ dada por:

$$\delta(a) = \delta(1), \ \forall\, a \in K \setminus \{0\}$$

& $\delta(1) \geq 0$. En efecto, notemos que

$$\delta(\alpha\beta) = \delta(\alpha),\ \forall\ \alpha,\beta \in K\setminus\{0\}$$

Además, sean $\alpha, \beta \in K$ con $\alpha \neq 0$, entonces tenemos que:

$$\beta = q\alpha + r \text{ donde } q = \beta\alpha^{-1}\ \&\ r = 0$$

Recíprocamente, si K es campo haciéndose DE con función $\delta : K\setminus\{0\} \to \mathbb{N}\cup\{0\}$, entonces necesariamente δ es constante y de valor $\delta(1)$. En efecto, sea $a \in K\setminus\{0\}$, se tiene:

$$\delta(1) = \delta(\alpha\alpha^{-1}) \geq \delta(\alpha) = \delta(\alpha \cdot 1) \geq \delta(1)$$

$\therefore\ \delta(\alpha) = \delta(1)$.

4. Sea $\mathbb{R}[x]$ el anillo de polinomios con coeficientes en $\mathbb{R}$ en la indeterminada x. Tenemos que $\mathbb{R}[x]$ es un dominio entero, el cual es DE con la función deg (grado del polinomio), donde el grado no está definido en el polinomio cero con:

$$\deg : \mathbb{R}[x]\setminus\{0\} \to \mathbb{N}\cup\{0\}$$

Teorema.

Todo DE es DIP.

Dem:

Sea A un anillo que es DE. Sea I un ideal de A con $I \neq \langle 0 \rangle$. Probemos que I es principal. Sea $b \in I$ tal que $b \neq 0 \Rightarrow \delta(b) \in \mathbb{N}\cup\{0\}$. Definimos

$$T := \{\delta(c) \mid c \in I,\ c \neq 0\} \subseteq \mathbb{N}\cup\{0\}$$

$T \neq \emptyset$ pues $\delta(b) \in T$. Sea $\delta(a) := \min T \Rightarrow \forall\ b \in I,\ b \neq 0$ se tiene que

$$\delta(b) \geq \delta(a),\ a \in I\setminus\{0\}$$

Afirmamos que $I = \langle a \rangle$. Es claro que $\langle a \rangle \subseteq I$. Sea $b \in I$ arbitrario. Por el algoritmo de la div $\exists\ q, r \in A$ $\ni$

$$b = qa + r$$

Donde $r = 0$ o $\delta(r) < \delta(a)$. Notemos que $r \in I$, pues $r = b - aq$, luego $\delta(r) \geq \delta(a)$.

Por tanto $r=0$. Así

$$b = qa$$

$\Rightarrow I \subseteq \langle a \rangle$. $\therefore I = \langle a \rangle$.

q.e.d.

Obs) Si A es DE, δ cumple:

i) $\delta(a) \geq \delta(1)$, $\forall a \in A\setminus\{0\}$.

ii) Si $a,b \in A\setminus\{0\}$ y $a \sim b \Rightarrow \delta(a) = \delta(b)$, ya que $\exists u \in A^*$ ⫪ $a = bu$ o $b = au^{-1}$

$\Rightarrow \delta(a) \geq \delta(b)$ y $\delta(b) \geq \delta(a) \Rightarrow \delta(a) = \delta(b)$.

iii) Si $a \in A\setminus\{0\}$, entonces $a \in A^* \Leftrightarrow \delta(a) = \delta(1)$.

Proposición.

El dominio entero $\mathbb{Z}[\sqrt{n}]$ es dominio euclidiano para $n = -2, -1, 2, 3$.

Dem:

Definimos $\delta : \mathbb{Z}[\sqrt{n}]\setminus\{0\} \to \mathbb{N}\cup\{0\}$ dada como:

$$\delta(\alpha) = |N(\alpha)|, \forall \alpha \in \mathbb{Z}[\sqrt{n}]\setminus\{0\}$$

Afirmamos que $\mathbb{Z}[\sqrt{n}]$ es DE con función δ. Tenemos que $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{n}]\setminus\{0\}$ se tiene que

$$\delta(\alpha\beta) = |N(\alpha)N(\beta)| \geq |N(\alpha)| = \delta(\alpha)$$

Ahora, probemos el algoritmo de la división. Sean $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ con $\alpha \neq 0$. P.D que $\exists$ $q, r \in \mathbb{Z}[\sqrt{n}]$ ⫪

$$\beta = q\alpha + r$$

donde $r = 0$ o $\delta(r) < \delta(\alpha)$. Para ello, tenemos que $\frac{\beta}{\alpha} \in \mathbb{Q}[\sqrt{n}]$. Lo expresamos:

$$\frac{\beta}{\alpha} = x + y\sqrt{n},\ x,y \in \mathbb{Q}.$$

Sean $a,b \in \mathbb{Z}$ ⫪ $|x-a| \leq \frac{1}{2}$ y $|y-b| \leq \frac{1}{2}$. Denotamos por $q = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, y sea

$r := \beta - q\alpha \in \mathbb{Z}[\sqrt{n}]$. Si $r=0$, entonces habremos terminado. Supongamos que $r \neq 0$.

Notemos que:

$$\delta(r) < \delta(\alpha) \iff |N(r)| < |N(\alpha)| \iff |N(\beta - q\alpha)| < |N(\alpha)| \iff \left|\frac{N(\beta-q\alpha)}{N(\alpha)}\right| < 1$$

$$\iff |N(\beta - q\alpha)N(\alpha^{-1})| < 1 \iff |N(\beta\alpha^{-1} - q)| < 1 \iff |(x-a)^2 - (y-b)^2 n| < 1 \iff$$

$$-1 < (x-a)^2 - (y-b)^2 n < 1$$

Así que, probemos que $-1 < (x-a)^2 - (y-b)^2 n < 1$

1) $n = -2, -1$.

$$-1 < 0 \leq (x-a)^2 - (y-b)^2 n = (x-a)^2 + (y-b)^2(-n) \leq \frac{1}{4} + \frac{(-n)}{4} \leq \frac{1}{4} + \frac{2}{4} < 1$$

2) $n = 2, 3$.

$$-1 < -\frac{3}{4} < -(y-b)^2 n \leq (x-a)^2 - (y-b)^2 n \leq (x-a)^2 + \frac{2}{4} \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$$

$\therefore \mathbb{Z}[\sqrt{n}]$ es DE para $n = -2, -1, 2, 3$.

q.e.d.

1) $\mathbb{Z}[i]$ es DE.

Teorema (de Wilson)

Sea $p \in \mathbb{N}$, $p \geq 2$. p es número primo $\iff (p-1)! \equiv -1 \text{ mód } p$.

Dem:

Aplicaremos lo siguiente. Si G es grupo finito abeliano, entonces

$$\prod_{a \in G} a = \prod_{\substack{a \in G \\ |a|=2}} a$$

Usando el grupo $(\mathbb{Z}/p\mathbb{Z})^*$ multiplicativo probaremos la equivalencia.

$\Rightarrow$) Suponga p primo. $\Rightarrow |(\mathbb{Z}/p\mathbb{Z})^*| = \varphi(p) = p-1$.

$$\Rightarrow (\mathbb{Z}/p\mathbb{Z})^* = \{[1], \dots, [p-1]\}$$

$$\Rightarrow [(p-1)!] = [1] \cdot \ldots \cdot [p-1]$$

Sea $k \in \mathbb{N}$, $1 \leq k \leq p-1$. Notemos que

$$[K]^2 = [1] \iff p \mid K^2-1 \iff p \mid (K+1)(K-1) \iff p \mid K+1 \text{ o } p \mid K-1 \iff K = 1 \text{ o } K = p-1$$

$$\therefore [(p-1)!] = [p-1] = [1]$$

$$\Rightarrow (p-1)! \equiv -1 \text{ mód } p.$$

($\Leftarrow$) Es inmediata.

q.e.d.

Proposición.

Sea $p \in \mathbb{N}$ primo de la forma $4n+1$. Entonces, existe un $x \in \mathbb{Z}$ tq

$$x^2 \equiv -1 \text{ mód } p$$

Dem:

Como $p = 4n+1 \Rightarrow (p-1)/2 = 2n$, i.e $\frac{p-1}{2}$ es par. Sea

$$x := 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \in \mathbb{Z}$$

Luego $x^2 = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot 1 \cdot \ldots \cdot \frac{p-1}{2} = 1 \cdot \ldots \cdot \frac{p-1}{2} \cdot (-1) \cdot \ldots \cdot \frac{-(p-1)}{2}$

$$\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} (p-1)(p-2) \cdot \ldots \cdot \left(p - \frac{p-1}{2}\right) \text{ mod } p$$

$$\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right)\left(p - \left(\frac{p-1}{2} - 1\right)\right) \cdot \ldots (p-2) \cdot (p-1) \text{ mód } p$$

$$\equiv (p-1)! \text{ mód } p \equiv -1 \text{ mod } p$$

q.e.d.

Teorema.

Sea $p \in \mathbb{N}$ número primo de la forma $4n+1$. Entonces p es suma de dos cuadrados.

Dem:

Afirmamos que p no es elemento primo en $\mathbb{Z}[i]$. Supóngase que p es elemento primo de $\mathbb{Z}[i]$. Sea $m \in \mathbb{Z}$ tq

$$pc = m^2 + 1$$

para algún $c \in \mathbb{Z}$ (por la prop. anterior). Luego:

$$pc = (m-i)(m+i) \text{ en } \mathbb{Z}[i]$$

$$\Rightarrow p \mid (m-i)(m+i) \text{ en } \mathbb{Z}[i]$$

$\Rightarrow p \mid m-i$ o $p \mid m+i$ en $\mathbb{Z}[i] \Rightarrow \exists\, \alpha \in \mathbb{Z}[i]$ m

$$m-i = \alpha p \quad o \quad m+i = \alpha p$$

$$\Rightarrow \alpha p = m \pm i$$

Si $\alpha = r + is \in \mathbb{Z}[i] \Rightarrow ps \pm 1$ #cr pues p es primo. Así que p no es elemento primo en $\mathbb{Z}[i]$, en part. no es irreducible. Luego, p se expresa de la forma:

$$p = (a+bi)(c+di)$$

Donde $(a+bi), (c+di) \notin (\mathbb{Z}[i])^*$.

$$\Rightarrow p^2 = (a^2+b^2)(c^2+d^2)$$

$\Rightarrow p = a^2+b^2 = c^2+d^2$. Por tanto, p es suma de dos cuadrados.

q.e.d.

Obs) Todo primo de la forma $4n+3$ no es suma de dos cuadrados

$$4n+3 = a^2+b^2$$

Notas: