Def: Sea R un anillo y $a,b \in R$ con $a \neq 0$. Decimos que a divide a b, $a | b$, si existe $r \in R$ tal que $ar = b$.

Lemma: Sea D un dominio entero y $a,b,x,y \in D$.

i) Si $ax = ay$ con $a \neq 0$, entonces $x = y$.

ii) Si $a | b$ y $b | a$, entonces $b = au$ para alguna unidad $u \in D$.

Dem:

i] Sup. $a \neq 0$ y $ax = ay$. Entonces $ax - ay = 0$
$\Rightarrow$ $a(x-y) = 0$. Como D es dominio entero y $a \neq 0$
entonces $x - y = 0$ ie, $x = y$.

ii] Sup. $a | b$ y $b | a$. Ent. existen $r, s \in D$ tales que
$ar = b$ y $bs = a$. Sustituyendo:

$a = bs = ars$. Si $a = 0$ ent $b = 0$ y así $a = b1$. Sup. $a \neq 0$. Por el inciso anterior $1 = rs$, es decir, r y s son unidades

Def: Sea D un dominio y $0 \neq a \in D$ un elemento que no es unidad. Decimos que a es irreducible si siempre que $a = bc$ con $b, c \in D$, se tiene que b ó c es una unidad.

Prop. Sea D un dominio entero Noetheriano. Entonces todo elemento de D es cero, una unidad o un producto (finito) de elementos irreducibles.

Dem:

Sea X el subconjunto de D que consiste de todos los elementos distintos de cero que no son unidades y que no son un producto de elementos irreducibles.

Sup. que hay elementos distintos de cero que no son unidades ni son un producto de irreducibles. Por lo tanto $X \neq \phi$. Consideremos $\Gamma = \{Da \mid a \in X\} \neq \phi$. Como D es Noetheriano, Γ tiene elementos máximos. Sea Da un maximo en Γ. Como $a \in X$, $a = bc$ donde b y c no son el cero, no son unidades y no son producto de irreducibles, i.e. $b, c \in X$. Notemos que $Da \subseteq Db \in \Gamma$

Por la maximalidad de Da, tenemos que $Da = Db$. Esto implica que $a \mid b$ y $b \mid a$. Por el lema anterior $a = bu$ con u unidad. Por lo tanto $bc = a = bu$. Como $b \neq 0$, $c = u$ $\underset{o}{\nabla}$

Def: Sea D un dominio. Un elemento $\pi \in D$ es primo si π no es unidad y siempre que $\pi | ab$ con $a, b \in D$ se tiene que $\pi | a$ ó $\pi | b$. Equivalentemente, $\pi \in D$ es primo si el ideal generado por π, $D\pi$ es un ideal primo.

Prop. Sea D un DIP y $0 \neq a \in D$. Las siguientes condiciones son equivalentes:

i) a es primo.

ii) a es irreducible.

iii) Da es un ideal máximo.

Dem:

$\underline{i \Rightarrow ii}$ Tenemos que a no es una unidad. Sup. $a = xy$ con $x, y \in D$. Entonces $a | xy$. Como a es primo, $a | x$ ó $a | y$. Por otro lado, también tenemos que $x | a$ y $y | a$. Si $a | x$

entonces, $a = xu$ con u unidad. Así $xu = xy \Rightarrow u = y$. Similarmente si $a | y$.

$\underline{ii \Rightarrow iii}$ | Sup. que a es irreducible y consideremos Da. Como a no es unidad, $Da \subsetneq D$

Sup que $Da \subseteq I \subseteq D$ con I un ideal de D. Por hipotesis existe $b \in D$ tal que $I = Db$.

Como $Da \subseteq Db$, $a = br$ con $r \in D$. Por hipotesis, b ó r es una unidad. Si b es unidad, $I = Db = D$. Si r es unidad, ent $Da = Db = I$

Por lo tanto Da es maximo.

$iii \Rightarrow i$ | Solo hay que notar que todo ideal maximo es un ideal primo.

Lema: Sea D un dominio entero.

i) Si $\pi \in D$ es primo y $\pi \mid b_1 b_2 \cdots b_m$, entonces π divide a uno de los factores b_i.

ii) Sup. $a_1 a_2 \cdots a_n = u b_1 b_2 \cdots b_m$ donde cada a_i es primo, cada b_j es irreducible y u es una unidad. Entonces $n=m$ y renumerando si es necesario, $b_i = u_i a_i$ con u_i unidad.

En $\mathbb{Z}$:

$$3 \cdot 5 = 15 = (-3)(-5)$$

$$(-1)3 = -3 \quad (-1)5 = -5$$

Dem:

i) Por induccion. Si $n=1$, el resultado es trivial. Si $n=2$, se obtiene por la definición de primo. Sup. que $n>1$, $a \mid b_1 \cdots b_n$ y $a \nmid b_n$.

Tenemos que $a \mid (b_1 \cdots b_{n-1}) b_n$. Como a es primo $a \mid b_1 \cdots b_{n-1}$. Por hip. de inducción $a \mid b_j$ p.a. j

ii) Por inducción sobre n. Sup que $n=1$, es decir, $a_1 = u b_1 \cdots b_m$. Por (i) $a_1 \mid b_j$ p.a j reordenando $a_1 \mid b_1$. Como b_1 es irreducible $b_1 = a_1 u_1$ con u_1 unidad. Sustituyendo: $a_1 = u u_1 a_1 b_2 \cdots b_m$ Cancelando: $1 = u u_1 b_2 \cdots b_m$. Esto implica que cada b_j con $2 \leq j \leq m$ es unidad ¡ Por lo tanto $1 = n = m$. Sup. $n > 1$ y el resultado es valido para $n-1$ y que $a_1 \cdots a_n = u b_1 \cdots b_m$ Tenemos que $a_1 \mid u b_1 \cdots b_m$. Por la base

de inducción, reordenando, $b_1 = a_1 u_1$ con u_1 unidad y así $a_2 \cdots a_n = u u_1 b_2 \cdots b_m$. Re-etiquetando $a_1 \cdots a_{n-1} = u u_0 b_1 \cdots b_{m-1}$. Por hip. de inducción $n-1 = m-1$ y $b_i = a_i u_i$ $1 \leq i \leq n-1$
Por lo tanto $n = m$ y cada $b_j = a_j u_j$ u_j unidad

Def: Un dominio D es un dominio de factorización única DFU si cumple:

(a) Todo elemento distinto de cero de D que no es unidad es un producto de elementos irreducibles; y

(b) Si $a_1 \cdots a_n = b_1 \cdots b_m$ con cada a_i y cada b_j irreducible, entonces $n = m$ y renumerando si es necesario, $b_i = u_i a_i$ con u_i unidad.