Anillos.

Def. Un anillo es un triplete $(A,+,\cdot)$ donde A es un conjunto no vacío y, $+$ y $\cdot$ son operaciones de A, tales que:

i) $(A,+)$ es grupo abeliano.

ii) $(A,\cdot)$ es semigrupo.

iii) $\cdot$ es distributiva con respecto a la suma. Es decir:

$$\forall\, a,b,c\in A,\quad a\cdot(b+c)=a\cdot b+a\cdot c,\quad y$$
$$(a+b)\cdot c=a\cdot c+b\cdot c$$

El elemento neutro de A (es decir, la identidad del grupo $(A,+)$), lo denotamos por:

$$e_+=0$$

y, para cada $a\in A$, su inverso aditivo lo denotamos por $-a$, el cuál es único.

Proposición.

Sea $(A,+,\cdot)$ un anillo. Se cumple lo siguiente:

i) $0\cdot a=0=a\cdot 0$, $\forall\ a\in A$.

ii) $-(-a)=a$, $\forall\ a\in A$.

iii) $-(ab)=-a(b)=a(-b)$, $\forall\ a,b\in A$.

iv) $a(b-c)=ab-ac$ y $(b-c)a=ba-ca$, donde:

$$b-c:=b+(-c)\quad (\text{la diferencia de } b \text{ y } c).$$

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

Dem:

De (i):

Sea $a\in A$, entonces:

$a\cdot 0 + a\cdot 0 = a\cdot(0+0) = a\cdot(0) = a\cdot 0$, como $(A,+)$ es grupo, valen las leyes de cancelación. Por tanto: $a\cdot 0 = 0$.

De manera análoga $0\cdot a = 0$.

De (ii):

Es inmediato del hecho que $(A,+)$ es grupo.

De (iii):

Tenemos que: si $a,b\in A$:

$$ab + (-a)b = (a+(-a))\cdot b = (0)\cdot b = 0b = 0$$

$\Rightarrow -(ab) = (-a)b$. De forma análoga $-(ab) = a(-b)$.

De (iv):

$\forall\, a,b,c\in A$:

$$a(b-c) = ab + a(-c) = ab + (-ac) = ab - ac$$

De manera similar $(b-c)a = ba - ca$.

q.e.d.

Por abuso de notación, diremos simplemente: "sea A anillo" en lugar de: "sea $(A,+,\cdot)$ anillo".

Def. Decimos que A es un anillo finito, si A como conjunto lo es, i.e $|A|<\infty$. En caso contrario, decimos que A es un anillo infinito, y escribimos $|A|=\infty$.

Def. Sea A un anillo. Decimos que el anillo A es conmutativo, si $(A,\cdot)$ lo es.

Decimos que A es anillo con identidad, si $(A,\cdot)$ tiene elemento identidad. Si el anillo A tiene identidad, esta se denota por 1, y referiremos al anillo A como un anillo con 1.

En este caso, si $u\in A$ es invertible, i.e, u tiene inverso (mismo que debe ser únical, decimos que u es unidad de A, y al conjunto de las unidades de A se le denota por A^*. Es decir:

$$A^* = \{u \in A \mid u \text{ es invertible}\}$$

en particular $1 \in A^*$.

Obs: Si A es un anillo con identidad 1, entonces $(A^*, \cdot)$ es grupo multiplicativo.

EJEMPLOS.

1) $\mathbb{Z}$ y $\mathbb{K}$ son anillos conmutativos con 1, con operaciones estándar. Notemos que: $\mathbb{Z}^* = \{-1, 1\}$ y $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

2) Si $n \in \mathbb{Z}$, $n \geq 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un anillo con operaciones estándar de suma y producto de clases. Si $n > 0$, sabemos que:

$$\forall a,b \in \mathbb{Z},\ a \equiv b \bmod n\mathbb{Z} \iff a-b \in n\mathbb{Z}$$

En el caso que $n=0$, $a \equiv b \bmod 0\mathbb{Z} \iff a-b \in 0\mathbb{Z} \iff a=b$. Por tanto $[a] = \{a\}$. Luego $\mathbb{Z}/0\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\} = \{\{a\} \mid a \in \mathbb{Z}\}$. Además:

$$\{a\} + \{b\} = [a] + [b] = [a+b] = \{a+b\}$$
$$\{a\} \cdot \{b\} = [a] \cdot [b] = [ab] = \{ab\}$$

También:

$$(\mathbb{Z}/0\mathbb{Z})^* = \{[-1], [1]\} = \{\{-1\}, \{1\}\}$$

Cuando $n \geq 1$, $a \equiv b \bmod n\mathbb{Z} \iff a \equiv b \bmod n \iff n \mid a-b$. Y $(\mathbb{Z}/n\mathbb{Z})$ es anillo con las operaciones usuales. Tenemos además que:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$$

Con $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, φ la función de Euler.

3) $(M_{n\times n}(\mathbb{K}), +, \cdot)$ es un anillo con identidad no conmutativo para $n \geq 2$. Y

$$M_{n\times n}(\mathbb{K})^* = GL_n(\mathbb{K})$$

donde:

$$GL_n(\mathbb{K}) = \{ A \in \mathcal{M}_{n\times n}(\mathbb{K}) \mid \det(A) \neq 0 \}$$

Recordemos que $GL_n(\mathbb{K})$ tiene un subgrupo normal, a saber; $SL_n(\mathbb{K})$:

$$SL_n(\mathbb{K}) = \{ A \in GL_n(\mathbb{K}) \mid \det(A) = 1 \}$$

el cual es el Kernel del homomorfismo:

$$(GL_n(\mathbb{K}), \cdot) \xrightarrow{\det} (\mathbb{K}^*, \cdot)$$
$$A \longmapsto \det(A)$$

4) Sea A un anillo, $X \neq \phi$. Denotamos por $\mathcal{F}(X, A) = \{ f : X \to A \mid f \text{ es función} \}$. En $\mathcal{F}(X, A)$ se definen 2 operaciones: $\forall\, f, g \in \mathcal{F}(X, A)$,

$$(f+g)(a) = f(a) + g(a), \ \forall\, a \in A.$$
$$(f \cdot g)(a) = f(a) \cdot g(a), \ \forall\, a \in A.$$

Con lo cual $\mathcal{F}(X, A)$ es un anillo. Y es conmutativo (con 1) $\iff$ A lo es (con identidad $1 : X \to A$, $x \mapsto 1$).

5) Tenemos que $\mathcal{C}([0,1], \mathbb{R}) = \{ f : [0,1] \to \mathbb{R} \mid f \text{ es continua} \}$ es un anillo con las operaciones inducidas por $\mathcal{F}([0,1], \mathbb{R})$.

Obs: Si A es un anillo con 1, siempre supondremos que $1 \neq 0$. Ya que si $1 = 0$, tendríamos que: $\forall\, a \in A$:

$$a = a \cdot 1 = a \cdot 0 = 0 \Rightarrow A = \{0\}$$

Así que, si A es un anillo con 1, tendremos que:

$$|A| \geq 2 \iff 1 \neq 0$$

Def. Sea A un anillo, definimos la función

$$\mathbb{Z} \times A \longrightarrow A$$
$$(m, a) \longmapsto ma$$

donde

$$ma := \begin{cases} \underbrace{a+a+\ldots+a}_{m\text{-veces}} & \text{si } m>0. \\ 0 & \text{si } m=0. \\ (-m)(-a) & \text{si } m<0. \end{cases}$$

Se cumple que: $\forall\, a,b \in A$ y $\forall\, m,n \in \mathbb{Z}$:

i) $m(a+b) = ma+mb$.

ii) $m(a-b) = ma-mb$.

iii) $(m+n)a = ma+na$

iv) $m(ab) = ma(b) = a(mb)$.

v) $(mn)a = m(na) = n(ma)$.

Notar que, podemos tener la notación $0a$ y $1a$.

Divisores de Cero.

Def. Sea A un anillo y $a \in A$, $a \neq 0$. Decimos que a es divisor de 0 por la derecha (resp. izquierda) si $\exists\, b \in A$, $b \neq 0$ ∍ $ba = 0$ ($ab = 0$ resp.). Además, a es divisor de cero si lo es tanto por la izquierda como por la derecha, i.e $\exists\, b, c \in A$, $b, c \neq 0$ ∍

$$ab = ca = 0$$

Ejemplo.

1) El conjunto $\mathcal{M}_{2\times 2}(\mathbb{R})$ es anillo no conmutativo. Sea $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. A es divisor de cero, pues: $\exists\, B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in \mathcal{M}_{2\times2}(\mathbb{R})$

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \text{ y}$$

$$BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Proposición.

Sea A un anillo. Entonces A no admite divisores de cero si y solo si las leyes de cancelación se cumplen, es decir: $\forall\, a, b, c \in A$, $a \neq 0$; si

$$ab = ac \Rightarrow b = c \quad \&$$

$$ba = ca \Rightarrow b = c$$

Dem:

$\Rightarrow$) Sean $a, b, c \in A$, $a \neq 0$ ∍ $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b + (-c)) = 0 \Rightarrow a(b - c) = 0$, Como A no admite divisores de cero y $a \neq 0$, entonces $b - c = 0 \Rightarrow b = c$.
Similarmente se prueba que si $ba = ca \Rightarrow b = c$.

$\Leftarrow$) Suponga que las leyes de cancelación se cumplen. Sea $a \in A$ ∍ $a \neq 0$, y $b \in A$ tal que $ab = 0$, como $0 = a0 \Rightarrow ab = a0$, luego como se cumplen las leyes de cancelación $\Rightarrow b = 0$. Por tanto A no admite divisores de cero.[1]

q.e.d.

Def. Sea A un anillo. Decimos que A es un dominio entero (abreviado d.e), si A es un anillo conmutativo con 1 y tal que no admite divisores de cero.

Ejemplos.

1) El anillo $\mathbb{Z}$ es un dominio entero.
2) Todo campo es anillo y, más aún, es dominio entero.
3) Si $n \geq 2$ y n es compuesto, entonces $\mathbb{Z}/n\mathbb{Z}$ no es dominio entero. Sean $r, s \in \mathbb{N}$ $\ni$ $r > 1$, $s > 1$ y $r \cdot s = n$. Luego $[r], [s] \neq [0]$, pero:
$$[r] \cdot [s] = [rs] = [n] = [0]$$
Luego $\mathbb{Z}/n\mathbb{Z}$ no es dominio entero.
Recíprocamente, si $\mathbb{Z}/n\mathbb{Z}$ admite divisores de cero, $\exists\, [r], [s] \in \mathbb{Z}/n\mathbb{Z}$ $\ni$
$$[r] \cdot [s] = [0],\ [r], [s] \neq [0]$$
entonces $[rs] = [0]$. Si n no fuera compuesto $\Rightarrow$ n es primo, luego $n \mid rs \Rightarrow n \mid r$ ó $n \mid s \Rightarrow [r] = [0]$ ó $[s] = [0]$ $\cancel{c}$. Por tanto, n es compuesto.
En resumen $\mathbb{Z}/n\mathbb{Z}$ es dominio entero $\Leftrightarrow$ n es primo.
4) No todo dominio entero es campo. Como ejemplo son los enteros $\mathbb{Z}$.
5) El anillo $M_{n\times n}(\mathbb{K})$ no es dominio entero si $n \geq 2$.

Def. Sea A un anillo, $B \subseteq A$, $B \neq \emptyset$. Decimos que B es subanillo de A, si las operaciones de A inducidas en B, hacen de B un anillo.

Proposición.

Sea A anillo, $B \subseteq A$, $B \neq \emptyset$. Las siguientes condiciones son equivalentes:

a) B es subanillo de A.

b) $\forall\ a,b \in B$, $a+b$, $-a \in B$ y $ab \in B$.

c) $\forall\ a,b \in B$, $a-b \in B$ y $ab \in B$.

Dem: ejercicio.

Proposición.

Sea A un anillo y $B \subseteq A$, $B \neq \emptyset$ finito, entonces B es subanillo de $A \iff \forall\, a, b \in B$, $a+b \in B$ y $ab \in B$.

Dem: ejercicio.

Ejemplos.

1) Si A es anillo, entonces A y $\{0\}$ son subanillos de A, llamados subanillos triviales.

2) En el anillo de los enteros $\mathbb{Z}$, $n\mathbb{Z}$ es subanillo de $\mathbb{Z}$, $n \geq 0$ (los cuáles son únicos subanillos de $\mathbb{Z}$)[2].

3) $\mathbb{Z}$ es subanillo que $\mathbb{Q}$ y $\mathbb{Q}$ es subanillo de $\mathbb{R}$.

Def. Sea A un anillo. Se define el centro de A, como

$$\text{cent}(A) = \{a \in A \mid ax = xa, \ \forall x \in A\}$$

Tenemos que $\text{cent}(A) \neq \emptyset$, pues $0 \in \text{cent}(A)$.

Obs: Si A es un anillo, A es conmutativo $\Leftrightarrow$ $\text{cent}(A) = A$.

Proposición.

Para cada A anillo, $\text{cent}(A)$ es subanillo de A.

Dem:

Sean $a, b \in \text{cent}(A)$. Si $x \in A$:

$$(a-b)x = ax - bx = xa - xb = x(a-b), \ y$$
$$(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$$

Por tanto, $a-b, ab \in \text{cent}(A)$.

q.e.d.

Obs: Si A es anillo con 1, entonces $1 \in \text{cent}(A)$, y si $x \in A^*$ y $x \in \text{cent}(A) \Rightarrow x^{-1} \in \text{cent}(A)$.

Sea B un subanillo de un anillo A. Pueden pasar las sig. situaciones:

1) A y B no tienen identidades. Digamos $A = 2\mathbb{Z}$ y $B = 4\mathbb{Z}$.

2) A con identidad y B no. $A=\mathbb{Z}$ y $B=2\mathbb{Z}$.

3) A no tiene identidad y B si la tiene. Para esto, notemos que si $A_1,\dots,A_n$ son anillos, sea $A=A_1\times\dots\times A_n$. Entonces A es anillo con operaciones usuales, tal que 0 de A es $0=(0_{A_1},0_{A_2},\dots,0_{A_n})$.

Si $a=(a_1,\dots,a_n)\in A$, su inverso aditivo $-a=(-a_1,\dots,-a_n)$. Además A es conmutativo $\Leftrightarrow A_i$ lo es, $\forall\, i\in[\![1,n]\!]$.

A tiene identidad $\Leftrightarrow A_i$ la tiene, $\forall\, i\in[\![1,n]\!]$.

Así, usamos esto para definir: $A=\mathbb{Z}\times 2\mathbb{Z}$ y $B=\mathbb{Z}\times\{0\}$.

4) Tanto A como B tienen identidades:

a) $1\in A$ y $1'\in B$ ⫪ $1\neq 1'$, digamos en $A=\mathbb{Z}\times\mathbb{Z}$, $B=\mathbb{Z}\times\{0\}$.

b) $1\in A$ y $1'\in B$ ⫪ $1=1'$, digamos $A=\mathbb{Q}$, $B=\mathbb{Z}$.

Obs: Sean A anillo y B subanillo de A tales que ambos tienen identidades $1\in A$ y $1'\in B$ con $1'\neq 1$. Entonces, $1'$ es divisor de cero de A. (B no es trivial).

Dem:

En efecto, tenemos que $1-1'\neq 0$ y:

$$1'\cdot(1-1')=1'\cdot 1-1'\cdot 1'=1'-1'=0$$

(Donde $1'\neq 0$ en B). Similarmente:

$$(1-1')\cdot 1'=1\cdot 1'-1'\cdot 1'=1'-1'=0$$

q.e.d.

Luego, si A es dominio entero y B es subanillo de A no trivial con identidad, entonces la identidad de B es la de A.

El recíproco en gral. no es cierto. Tome $A=M_{2\times 2}(\mathbb{K})$.

Def. Sea A un anillo. Decimos que A es de característica positiva, a lo que

Se escribe $car(A)>0$, si existe un $m\in\mathbb{N}$ ∍

$$ma=0,\ \forall a\in A.$$

Si esto ocurre, al mínimo entero positivo m ∍ $ma=0$, se le llama la **característica de A**, y se escribe $m=car(A)$.

Si lo anterior no ocurre, se dice que A es de característica **cero**, y se escribe:

$$car(A)=0.$$

Es decir: $\forall\, n\in\mathbb{N}$, $\exists\, a\in A$ tal que:

$$na\neq 0$$

Por lo anterior, el concepto de característica de un anillo A, es que $car(A)\geq 0$.

Proposición.

Sea A un anillo con $n=car(A)>0$. Entonces dado $m\in\mathbb{Z}$:

$$ma=0,\ \forall a\in A \iff n\mid m$$

Dem:

$\Leftarrow$) Si $m=nq$, para algún $q\in\mathbb{Z} \Rightarrow ma=(nq)a=q(na)=q0=0,\ \forall a\in A.$

$\Rightarrow$) Suponga que $ma=0,\ \forall a\in A$. Por el alg. de la div, $\exists!\, q,r\in\mathbb{Z}$ ∍

$$m=nq+r,\quad 0\leq r<n$$

Luego:

$$\begin{aligned}0&=ma\\&=(nq+r)a\\&=q(na)+ra\\&=0+ra\\&=ra\end{aligned}$$

Como n es el mínimo entero positivo para el que ocurre esto, entonces: $r=0$.
Por tanto $m=nq \Rightarrow n \mid m$.

q.e.d.

Obs: Por lo general, supondremos $car(A)=0$ ó $car(A)\geq 2$. Si $car(A)=1 \Rightarrow 1a=0$, $\forall a\in A \Rightarrow a=0$, $\forall a\in A \Rightarrow A=\{0\}$.

Obs. Sea A un anillo. :) <3

(i) A finito $\Rightarrow car(A)>0$ (pues $(A,+)$ es grupo aditivo finito, i.e $|A|a=0$, $\forall a\in A$).

(ii) Si $car(A)=0 \Rightarrow A$ es infinito.

Ejemplos.

1) $char(\mathbb{Z})=0$. Pues $\forall m\in\mathbb{N}$, $m\cdot a=(ma)\cdot 1=ma$, $\forall a\in A\setminus\{0\}$. Luego $m\cdot a \neq 0$, $\forall a\in A\setminus\{0\}$. Al igual, $char(\mathbb{K})=0$.

2) Si $n\geq 2$, $char(\mathbb{Z}/n\mathbb{Z})=n$, pues $\forall a\in\mathbb{Z}$:
$$n[a]=[na]=[0]$$
luego $char(\mathbb{Z}/n\mathbb{Z})\leq n$. Si $1\leq k<n$:
$$k[1]=[k]\neq[0]$$
luego $char(\mathbb{Z}/n\mathbb{Z})>k$, i.e $char(\mathbb{Z}/n\mathbb{Z})=n$.

Obs: Sea $\{A_i\}_{i\in I}$ una familia no vacía de anillos. Definimos $A=\prod_{i\in I} A_i=\{a \mid a=(a_i)_{i\in I},\ a_i\in A_i\ \forall i\in I\}$. Dotamos al conjunto A con 2 operaciones: Suma y producto:
$$(a_i)_{i\in I}+(b_i)_{i\in I}=(a_i+b_i)_{i\in I},\ y\ (a_i)_{i\in I}\cdot(b_i)_{i\in I}=(a_ib_i)_{i\in I}$$
$\forall (a_i)_{i\in I},(b_i)_{i\in I}\in A$. Con estas operaciones A es un anillo. Donde $0_A=(0_i)_{i\in I}$

(0_i el cero de A_i, $\forall i\in I$). Y si $(a_i)_{i\in I}\in A$, su inverso aditivo será:

$$-(a_i)_{i\in I}=(-a_i)_{i\in I}$$

Se define la suma directa de la familia de anillos $\{A_i\}_{i\in I}$ como:

$$B=\bigoplus_{i\in I}A_i=\{a=(a_i)_{i\in I}\in A \mid a_i=0_i \text{ } \cancel{\forall} \text{ } i\in I\}$$

Con las operaciones de A, B es un anillo. En efecto: veámos que las operaciones son cerradas en B.

Sean $(a_i)_{i\in I}, (b_i)_{i\in I}\in B$, entonces

$$(a_i)_{i\in I}+(b_i)_{i\in I}=(a_i+b_i)_{i\in I}\in B$$

Pues $a_i+b_i\neq 0_i$ $\cancel{\forall}$ $i\in I$, pues $(a_i)_{i\in I}, (b_i)_{i\in I}$ tienen n y m entradas distintas de cero. Luego $(a_i+b_i)_{i\in I}$ tiene a lo sumo $n+m$ entradas diferentes de cero. Luego $(a_i+b_i)_{i\in I}\in B$.

De manera similar, $(a_i)_{i\in I}\cdot(b_i)_{i\in I}=(a_ib_i)_{i\in I}\in B$ (tiene a lo sumo $\min\{n,m\}$ entradas diferentes de cero).

Además, si $(a_i)_{i\in I}\in B \Rightarrow (-a_i)_{i\in I}\in B$. Por tanto, B es subanillo de A.

3) Sea $A=\prod_{\mathbb{N}}\mathbb{Z}/n\mathbb{Z}=(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times\dots$. Tenemos por lo anterior que A es un anillo infinito y $Car(A)=n$.

4) Sea $A=\prod_{n\geq 2}\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\dots$ Entonces A es infinito y $car(A)=0$. Pues si $m\in\mathbb{N}$, entonces el elemento $a\in A$ dado como:

$$a=([0]_2,[0]_3,\dots,[0]_m,[1]_{m+1},[0]_{m+2},\dots)$$

de forma más formal:

$$\forall i\in\mathbb{N}\quad a(i)=\begin{cases}[0]_{i+1} & \text{si } i\neq m\\ [1]_{m+1} & \text{si } i=m\end{cases}$$

luego $ma=([0]_2,\dots,[m]_{m+1},\dots)\neq 0_A$, i.e $Car(A)=0$. Notemos que $1_A=$

$([1]_2, [1]_3, \dots)$ Cumple que:

$$m \cdot 1_A \neq 0, \ \forall m \in \mathbb{N}.$$

pues en la m-ésima entrada, 1_A vale $[m]_{m+1} \neq [0]_{m+1}$. Así 1_A tiene orden infinito.

Proposición.

Sea A un anillo con identidad. Entonces $car(A) > 0 \Leftrightarrow$ el orden aditivo del 1 (denotado por $o(1) = |1|$) es finito. Cuando $o(1) < \infty$, entonces $car(A) = o(1)$.

Dem:

$\Rightarrow$) Supongamos $car(A) = m > 0$. Entonces $m \cdot 1 = 0$. Luego $o(1) < \infty$. Si $n = o(1)$ entonces $n \mid m \Rightarrow n \leqslant m$.

Por otro lado, sea $a \in A$ arbitrario. Entonces:

$$na = n(a \cdot 1) = a \cdot (n1) = a \cdot 0 = 0$$

por def. de m, $n \leqslant m \Rightarrow n = m$.

$\Leftarrow$) Suponemos que $o(1) = n < \infty$. Tenemos que

$$\forall a \in A, \ na = n(1 \cdot a) = (n1) \cdot a = 0 \cdot a = 0$$

luego $car(A) = m > 0$. Por lo anterior $m \leqslant n$. Notemos que:

$$m \cdot 1 = 0 \Rightarrow n \leqslant m$$

así $n = m$.

q.e.d.

Corolario.

Sea A un anillo con identidad. Entonces $car(A) = 0 \Leftrightarrow o(1) = \infty$.

Dem:

Es inmediata de lo anterior.

q.e.d.

Proposición.

Todo dominio entero A es o bien $car(A)=0$ ó $car(A)=p$, p un número primo.

Dem:

Supóngase que $car(A)=n>0$. Además, supongamos que n es compuesto, $\exists\, r,s \in \mathbb{N}\setminus\{1\}$ m $n=r\cdot s$. Luego:

$$0=n\cdot 1=(rs)\cdot 1)=(r\cdot 1)\cdot(s\cdot 1)$$

por ser A dominio entero, $r\cdot 1=0$ ó $s\cdot 1=0$. Si $r\cdot 1=0 \Rightarrow n=car(A)=o(1)\leq r$, pero $r<n$, pues $n=rs$ $\#_c$.

De manera similar $s\cdot 1=0$ lleva a una contradicción. Por tanto n debe ser primo.

q.e.d.

Corolario.

$\forall\, n\in\mathbb{N}$, $n\geq 2$, las siguientes condiciones son equivalentes:

i) $\mathbb{Z}/n\mathbb{Z}$ es dominio entero.

ii) n es primo.

iii) $car(\mathbb{Z}/n\mathbb{Z})=n$ es número primo.

Dem:

Es inmediato de lo anterior.

q.e.d.

Notas:

1) El caso $ba = 0$ se prueba de manera similar y no es mencionada.

2)