Lista Anillos.

1. Pruebe que en un anillo el cero y los inversos aditivos de sus elementos son únicos.

Dem:

Sea A un anillo. Suponga que $\exists\, 0' \in A \ni$

$$0' + a = a + 0' = a, \forall a \in A$$

Entonces:

$$0 = 0 + 0' = 0' + 0 = 0'$$

Sea ahora $a \in A$. Suponga $\exists\, b \in A \ni a + b = b + a = 0$, entonces:

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

q.e.d.

2. Sea A un anillo con identidad y $a \in A$. Pruebe que las condiciones siguientes se cumplen:

   a) El elemento identidad de A es único;

   b) Si a tiene inverso multiplicativo, entonces este es único.

   c) Si a es invertible, entonces también lo es $-a$;

   d) Ningún divisor de cero de A puede tener un inverso multiplicativo en A.

Dem:

De a): Suponga $\exists\, 1' \in A \ni 1' a = a \cdot 1' = a, \forall a \in A$, entonces como $1 \in A$:

$$1 = 1 \cdot 1' = 1' \cdot 1 = 1'$$

De b): Suponga que $\exists\, b \in A \ni ab = ba = 1$. Entonces:

$$a^{-1} = a^{-1} \cdot 1 = a^{-1}(ab) = (a^{-1}a)\, b = 1 \cdot b = b$$

De c): Veamos que:

$$(-a^{-1})(-a) = -(a^{-1})(-a) = -(-a^{-1}a) = a^{-1}a = 1,$$

de forma similar $(-a)\cdot(-a^{-1}) = 1$. Así $(-a)^{-1} = -a^{-1}$.

De d): Suponga que $\exists\, a \in A$ tal que a es divisor de cero y $\exists\, c \in A \ni ac = ca = 1$. Como a es divisor de cero, $\exists\, b \in A \setminus \{0\} \ni ab = 0$. Como:

$$ac = ac + ab$$
$$\Rightarrow ac = a(c+b)$$
$$\Rightarrow cac = ca(c+b)$$
$$\Rightarrow 1c = 1(c+b)$$
$$\Rightarrow c = c+b$$
$$\Rightarrow b = 0 \quad \text{※c.}$$

Luego a no tiene inverso.

q.e.d.

3. Sea A un anillo. Pruebe que para cada $n, m \in \mathbb{Z}$ y para cada $a, b \in A$

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

   b) $(nm)a = n(ma)$;

   c) $n(a+b) = na + nb$;

   d) $n(ab) = (na)b = a(nb)$;

   e) $(na)(mb) = (nm)(ab)$.

4. Sea $\{A_i\}_{i\in I}$ una familia de anillos y $A = \prod_{i\in I} A_i$ el producto directo de la familia $\{A_i\}_{i\in I}$. Sea $B = \bigoplus_{i\in I} A_i$ la suma directa de la familia $\{A_i\}_{i\in I}$, es decir, el conjunto de todas las funciones $f \in A$ tales que $f(i) = 0$ para casi todo índice i salvo un número finito de ellos. Definimos las siguientes operaciones en A: Para cada $i \in I$ y para cada $f, g \in A$

$$(f + g)(i) = f(i) + g(i) \text{ y } (fg)(i) = f(i)g(i).$$

Pruebe que A con las operaciones antes definidas satisface lo siguiente:

a) A es anillo;

b) B es subanillo de A;

c) A (resp. B) es conmutativo si, y solo si cada A_i lo es;

d) A tiene identidad si, y solo si cada A_i lo tiene.

e) Si cada A_i tiene identidad, entonces ¿es cierto que B tiene identidad?

5. Sea X un conjunto con más de un elemento. Pruebe que la triada $(\mathcal{P}(X), \triangle, \cap)$ es un anillo conmutativo con identidad, en el que cada subconjunto propio no vacío de X es un divisor de cero.

Dem:

Primero, probaremos que $(\mathcal{P}(X), \Delta)$ es grupo abeliano. En efecto, $\mathcal{P}(X) \neq \emptyset$, y:

i) Sean $A, B, C \in \mathcal{P}(X)$, entonces:

$$\begin{aligned}
(A \Delta B) \Delta C &= (A \setminus B \cup B \setminus A) \Delta C \\
&= (A \setminus B \cup B \setminus A) \setminus C \cup C \setminus (A \setminus B \cup B \setminus A) \\
&= [(A \cap B^c) \cup (B \cap A^c)] \cap C^c \cup \{C \cap [(A \cap B^c) \cup (B \cap A^c)]^c\} \\
&= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup \{C \cap [(A^c \cup B) \cap (B^c \cup A)]\} \\
&= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup \{[(C \cap A^c) \cup (C \cap B)] \cap (B^c \cup A)\} \\
&= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup [(C \cap A^c) \cap (B^c \cup A)] \cup [(C \cap B) \cap (B^c \cup A)] \\
&= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup [(A^c \cap B^c \cap C) \cup (A^c \cap A \cap C)] \cup [(B \cap B^c \cap C) \cup \\
&\quad (A \cap B \cap C)] \\
&= (A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)
\end{aligned}$$

de forma similar: $A \Delta (B \Delta C) = (A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)$, así:

$$(A \Delta B) \Delta C = A \Delta (B \Delta C)$$

ii) Sea $A \in \mathcal{P}(X)$, $\exists\, \emptyset \in \mathcal{P}(X)$ m:

$$A \Delta \emptyset = A \setminus \emptyset \cup \emptyset \setminus A = A = \emptyset \setminus A \cup A \setminus \emptyset = \emptyset \Delta A$$

iii) $\forall\, A \in \mathcal{P}(X)$, $\exists\, A \in \mathcal{P}(X)$ m

$$A \Delta A = A \Delta A = \emptyset$$

Así, $(\mathcal{P}(X), \Delta)$ es grupo, y es abeliano pues:

$$A \Delta B = A \setminus B \cup B \setminus A = B \setminus A \cup A \setminus B = B \Delta A$$

Veamos que $(\mathcal{P}(X), \cap)$ es monoide abeliano. En efecto:

iv) $\forall\, A, B, C \in \mathcal{P}(X)$:

$$(A \cap B) \cap C = A \cap (B \cap C)$$

v) $\forall\, A \in \mathcal{P}(X)$, $\exists\, X \in \mathcal{P}(X)$ m: $A \cap X = X \cap A = A$.

Además: $\forall\ A, B \in \mathcal{P}(\mathbb{X})$:

$$A \cap B = B \cap A$$

Luego $(\mathcal{P}(\mathbb{X}), \cap)$ es monoide abeliano. Finalmente: $\forall\ A, B, C \in \mathcal{P}(\mathbb{X})$:

$$\begin{aligned}(A\cap C)\Delta(A\cap B) &= (A\cap C)\setminus(A\cap B)\cup(A\cap B)\setminus(A\cap C)\\ &= [(A\cap C)\cap(A^c\cup B^c)]\cup[(A\cap B)\cap(A^c\cup C^c)]\\ &= [(A\cap C\cap A^c)\cup(A\cap C\cap B^c)]\cup[(A\cap B\cap A^c)\cup(A\cap B\cap C^c)]\\ &= (A\cap C\cap B^c)\cup(A\cap B\cap C^c)\\ &= A\cap(B\cap C^c\cup C\cap B^c)\\ &= A\cap(B\setminus C\cup C\setminus B)\\ &= A\cap(B\Delta C)\end{aligned}$$

Luego, como $\cap$ es conmutativo, Δ es distributiva respecto a $\cap$. Luego $(\mathcal{P}(\mathbb{X}), \Delta, \cap)$ es anillo conmutativo con identidad $\mathbb{X}$.

Sea ahora $A \in \mathcal{P}(\mathbb{X})$ un subconjunto propio de $\mathbb{X}$, i.e $A \subseteq \mathbb{X}$, pero $A \neq \emptyset, \mathbb{X}$. Como $\mathbb{X}$ tiene más de un elemento, entonces A existe, y $A^c \neq \emptyset, \mathbb{X}$. Veamos que:

$$A \cap A^c = \emptyset \Rightarrow A \text{ es divisor de cero (el vacío).}$$

q.e.d.

6. Sea A un anillo y $n > 1$. Pruebe que el anillo de matrices $\mathfrak{M}_n(A)$ es un anillo no conmutativo el cual admite divisores de cero, aún cuando A pueda no tenerlos. Además, pruebe que $\mathfrak{M}_n(A)$ tiene identidad si y solo si A tiene identidad.

7. Sea A un anillo con identidad 1 sin divisores de cero (izquierdos o derechos). Pruebe que para cada $a, b \in A$ se verifica que

   a) $ab = 1$ si, y solo si $ba = 1$;

   b) $a^2 = 1$ implica que $a = 1$ o $a = -1$.

Dem:

De a):

$$ab = 1 \Leftrightarrow b = b \cdot 1 = b(ab) \Leftrightarrow b = (ba)b \Leftrightarrow 1 = ba$$

De b):

$$a^2 = 1 \Rightarrow a^2 - 1 = 0 \Rightarrow (a-1)(a+1) = 0 \Rightarrow a = 1 \text{ ó } a = -1.$$

q.e.d.

8. De condiciones necesarias y suficientes sobre n, $n \geq 1$, para que el anillo $\mathbb{Z}/n\mathbb{Z}$ sea un dominio entero.

9. Sean A un anillo, $a, b \in A$ tales que $ab = ba$, y $n \in \mathbb{N}$. Pruebe que se tiene la expresión

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

donde

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

es el coeficiente binomial usual.

10. Un elemento a de un anillo A se dice que es **idempotente** si $a^2 = a$, y **nilpotente** si $a^n = 0$ para algún $n \in \mathbb{N}$. Pruebe lo siguiente:

a) Un elemento no cero de A el cual es idempotente no puede ser nilpotente;

b) Cada elemento no cero de A el cual es nilpotente es un divisor de cero de A.

Dem:

De a): Sea $a \in A \setminus \{0\} \ni a^2 = a$ (tal elemento existe pues $1 \in A \setminus \{0\} \ni 1^2 = 1$, siendo $A \neq \{0\}$). Probaremos que $a^n = a \neq 0, \forall n \in \mathbb{N}$. En efecto: por inducción sobre n:

1) Por hip. $a^2 = a \neq 0$.

2) Suponga $\exists\, k \in \mathbb{N} \setminus \{1\} \ni a^k = a \neq 0$.

3) $a^{k+1} = a^k \cdot a = a \cdot a = a^2 = a \neq 0$.

Luego, por inducción, $a^n = a \neq 0, \forall n \in \mathbb{N}$.

De b): Si $a \in A \setminus \{0\}$ es tal que $a^n = 0$, para algún $n \in \mathbb{N}$, como $a \neq 0$ entonces $n > 1$.

Sea $m = \min\{n \in \mathbb{N} \mid a^n = 0\}$, entonces $m > 1$, y $a^m = 0$.

Tome $a^{m-1} \neq 0$, por def. de m. Luego:

$$\begin{aligned} a \cdot a^{m-1} &= a^m \\ &= 0 \end{aligned}$$

Así, a es divisor de cero.

q.e.d.

11. Sea A un anillo conmutativo con identidad de característica p primo. Pruebe que para cada $a, b \in A$ y para cada $n \in \mathbb{N}$,

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}.$$

Note que para $p = 2$, $a = -a$ para cada $a \in A$.

Dem:

Procederemos por inducción sobre n. Sean $a, b \in A$, entonces:

$$\begin{aligned} (a \pm b)^{p^1} &= (a \pm b)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} (\pm b)^k \end{aligned}$$

Como p es primo, $p \geqslant 2$. Veamos que $p \mid \binom{p}{k}, \forall\ 1 \leqslant k \leqslant p-1$. En efecto, como:

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

Como $1 \leq K \leq p-1$, entonces $K < P$ y $P < K$, luego:

$$\binom{p}{k} = p \cdot \frac{(p-1)!}{K!(p-K)!} \Rightarrow p \mid \binom{p}{k}$$

Luego:

$$\sum_{K=0}^{p} \binom{p}{K} a^{p-K} (\pm b)^K = a^p + \sum_{K=1}^{p-1} \binom{p}{k} a^{p-K} (\pm b)^K + (\pm b)^p$$

Como $p \mid \binom{p}{k}$ $\forall$ $1 \leq K \leq p-1$, $\exists$ n_K $\ni$ $\binom{p}{k} = p n_K$, por tanto:

$$(a \pm b)^{p^1} = a^p + \sum_{K=1}^{p-1} p n_K a^{p-K} (\pm b)^K + (\pm b)^p$$

Como A es de característica p, $p n_K a^{p-K} (\pm b)^K = 0$, $\forall$ $1 \leq K \leq p-1$. Luego:

$$(a \pm b)^{p^1} = a^{p^1} + (\pm b)^{p^1}$$

Si $p = 2$, entonces $2u = 0$, $\forall$ $u \in A$, luego $u = -u$, $\forall u \in A$. Así: $\pm b^p = \mp b^p$. Por tanto:

$$(a \pm b)^{p^1} = a^{p^1} \pm b^{p^1}, \quad p = 2$$

Si $p > 2$:

$$(a \pm b)^{p^1} = a^{p^1} \pm b^{p^1}$$

Suponga el resultado válido para m, i.e $\forall a, b \in A$:

$$(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}$$

Se cumple para $m+1$. En efecto:

$$\begin{aligned}
(a \pm b)^{p^{m+1}} &= (a \pm b)^{p^m \cdot p} \\
&= \left[(a \pm b)^{p^m} \right]^p \\
&= \left(a^{p^m} \pm b^{p^m} \right)^p, \text{ por lo anterior:} \\
&= \left(a^{p^m} \right)^{p^1} \pm \left(b^{p^m} \right)^{p^1} \\
&= a^{p^{m+1}} \pm b^{p^{m+1}}
\end{aligned}$$

$\forall a, b \in A$. Por inducción, se cumple $\forall$ $m \in \mathbb{N}$.

q.e.d.

12. Sea A un dominio entero. Pruebe lo siguiente:

a) El cero es el único elemento nilpotente de A;

b) La identidad multiplicativa de A es el único elemento idempotente no cero.

Dem:

De (i): Sea $a \in A$ $\ni$ $a^n = 0$, para algún $n \in \mathbb{N}$. Sea m el mínimo número natural tal que

$a^m = 0$. Si $m=1$, entonces $a=0$. Si $m>1$, $a^1 \neq 0$, así:

$$a^m = 0 \Rightarrow a \cdot a^{m-1} = 0$$

Como A es dominio entero, $a^{m-1}=0$ ó $a=0$ ~~*c~~ en ambos casos. Por tanto, $a=0$.

De (ii): Sea $a \in A \setminus \{0\}$ $\ni$ $a^2 = a$, entonces $a^2 - a = a(a-1) = 0$. Como A es dominio entero y $a \neq 0$, entonces $a-1=0$, luego $a=1$.

q.e.d.

13. Sean A un anillo con identidad y $a \in A$ nilpotente. Pruebe que $a+1$ es invertible en A.

Dem:

Sea $m \in \mathbb{N}$ el mínimo entero positivo tal que $a^m = 0$. Veamos que $a+1$ es invertible, en efecto:

$$\begin{aligned} 0 = a^m &= (a+1-1)^m. \text{ Como } a+1 \text{ y } -1 \text{ conmutan (pues } -1 \in \operatorname{cent}(A)\text{).} \\ &= \sum_{k=0}^{m} \binom{m}{k} (a+1)^k \cdot (-1)^{m-k} \\ &= (-1)^m + \sum_{k=1}^{m} \binom{m}{k} (a+1)^k \cdot (-1)^{m-k} \end{aligned}$$

podemos elegir el m impar, pues si es par, $a^{m+1} = a^m \cdot a = 0 \cdot a = 0$. Luego:

$$0 = -1 + (a+1) \cdot \underbrace{\sum_{k=1}^{m} \binom{m}{k} (a+1)^{k-1} \cdot (-1)^{m-k}}_{u}$$

$$\Rightarrow 1 = (a+1)u$$

De forma similar: $u(a+1) = 1$. Luego $a+1$ es invertible.

q.e.d.

14. Sean A un anillo y $a, b \in A$ elementos nilpotentes tales que conmutan. Pruebe que $a+b$ es elemento nilpotente de A. Demuestre que la afirmación puede ser falsa si no se suponen que los elementos a, b conmutan.

Dem:

Sean $m, n \in \mathbb{N}$ los mínimos enteros positivos tales que $a^m = 0$ y $b^n = 0$, $m, n > 1$. Entonces:

$$\begin{aligned} (a+b)^{mn} &= ((a+b)^m)^n. \text{ Como } a \text{ y } b \text{ conmutan:} \\ &= \left(\sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k} \right)^n \\ &= \left(\sum_{k=0}^{m-1} \binom{m}{k} a^k b^{m-k} + a^m \right)^n \end{aligned}$$

$$= \left(b \cdot \sum_{k=0}^{m-1} \binom{m}{k} a^{k} b^{m-k-1}\right)^{n}$$
$$= b^{n} \cdot \left(\sum_{k=0}^{m-1} \binom{m}{k} a^{k} b^{m-k-1}\right)^{n}$$
$$= 0$$

Luego, $a+b$ es nilpotente.

q.e.d.

15. Sea A un anillo. Pruebe que las siguientes condiciones son equivalentes:

   a) A no tiene elementos nilpotentes distintos de cero;

   b) Si $a \in A$ con $a^2 = 0$, entonces $a = 0$

Dem:

a) $\Rightarrow$ b):

Como A no tiene elementos nilpotentes distintos de cero: $\forall\, n \in \mathbb{N}$ y $\forall\, a \in A \setminus \{0\}$: $a^n \neq 0$, en particular $a^2 \neq 0$, $\forall\, a \in A \setminus \{0\}$. Así $a^2 = 0 \Rightarrow a = 0$.

b) $\Rightarrow$ a):

Sea $a \in A$ nilpotente y $m \in \mathbb{N}$ el mínimo entero positivo tal que $a^m = 0$. Si $m = 1$, $a = 0$. Si $m = 2$, por hip. $a = 0$. Si $m > 2$:

$$a^m = a^2 \cdot a^{m-2}$$
$$= 0$$

16. Un anillo **Booleano** es un anillo A con identidad en el cual cada elemento es idempotente. Pruebe que cualquier anillo Booleano es conmutativo. (Sugerencia: Pruebe primero que $a = -a$ para cada $a \in A$).

Dem:

Sea $a \in A$. Como a es idempotente: $a^2 = a$. Veamos que:

$$(a+a)^2 = a+a$$
$$\Rightarrow 2a^2 + 2a^2 = a+a$$
$$\Rightarrow 2a^2 + 2a = 2a^2, \text{ pues } a+a = a^2+a^2$$
$$\Rightarrow a+a = 0$$
$$\Rightarrow a = -a.$$

Sean ahora $a, b \in A$, entonces:

$$\begin{aligned} a+b &= (a+b)^2 \\ &= (a+b)(a+b) \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b \end{aligned}$$
$$\Rightarrow -ab = ba, \text{ como } ab = -ab:$$
$$\Rightarrow ab = ba$$

Luego, A es conmutativo.

q.e.d.

17. Sea A un anillo el cual posee un elemento $a \neq 0$ tal que es idempotente y no es divisor de cero (ni izquierdo, ni derecho). Pruebe que a es identidad de A.

Dem:

Sea $b \in A$. Probaremos que $ab = ba = b$. Como a es idempotente, $a^2 = a$, luego:

$$ab = a^2 b \quad \text{y} \quad ba = ba^2$$
$$\Rightarrow ab - a^2 b = 0 \quad \text{y} \quad ba - ba^2 = 0$$
$$\Rightarrow a(b - ab) = 0 \quad \text{y} \quad (b - ba)a = 0$$

Como a no es divisor de cero, entonces $b - ab = 0$ y $b - ba = 0$, por lo cual:

$$ab = ba = b$$

q.e.a.

18. Sea B un subconjunto no vacío de un anillo finito A. Pruebe que B es un subanillo de A si, y solo si las operaciones de adición y multiplicación son cerradas en B.

19. Sea A un anillo. Para cada $a \in A$, denotamos por $\mathrm{Cent}(a)$ al conjunto de todos los elementos de A que conmutan con a. Pruebe que $\mathrm{Cent}(a)$ es un subanillo de A, para cada $a \in A$, y que

$$\mathrm{Cent}(A) = \bigcap_{a\in A} \mathrm{Cent}(a).$$

Dem: Sea $a \in A$

1) $\mathrm{Cent}(a)$ es subanillo de A.

Sean $x, y \in \mathrm{Cent}(a)$. Veamos que:

$$a(x-y) = ax - ay = xa - ya = (x-y)a$$

Luego $x-y \in \mathrm{Cent}(a)$. Además:

$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$$

por tanto $xy \in \mathrm{Cent}(a)$. Así, $\mathrm{Cent}(a)$ es subanillo de A.

2) Veamos la doble contención:

$$x \in \mathrm{cent}(A) \iff ax = xa,\ \forall a \in A \iff x \in \mathrm{Cent}(a),\ \forall a \in A \iff x \in \bigcap_{a\in A} \mathrm{cent}(a).$$

q.e.d.

20. Sean A un anillo, $\{B_i\}_i$ una familia de subanillos de A y S un subconjunto de A. Pruebe lo siguiente:

a) La intersección $\bigcap_i B_i$ es un subanillo de A;

b) El conjunto $[S]$, definido como la intersección de todos los subanillos de A que contienen a S, es el mínimo (con respecto a la relación de contención) subanillo de A que contiene a S. $[S]$ es llamado el **subanillo de A generado por S**.

Dem:

De a):

Como $0 \in B_i$, $\forall i \in I$, entonces $0 \in \bigcap_{i\in I} B_i$, así $B = \bigcap_{i\in I} B_i \neq \phi$. Sean ahora $x, y \in B$, entonces:

$x, y \in B_i$, $\forall i \in I$. como B_i es subanillo de $A \Rightarrow x-y, xy \in B_i$, $\forall i \in I$. Luego:

$$x-y, xy \in B$$

Por tanto, B es subanillo de A.

De b): Sea K un subanillo de A tal que $S \subseteq K$. Probaremos que $[S] \subseteq K$. Como K es un subanillo de A que contiene a S, K está en la familia $\{B_i\}_{i\in I}$ de los subanillos de A que contienen a S. Luego:

$$\bigcap_{i \in I} B_i \subseteq K$$

$$\Rightarrow [S] \subseteq K.$$

q.e.d.

21. Sean A un anillo y B un subanillo de A. Para cada $a \notin B$, el subanillo de A generado por $B \cup \{a\}$ es denotado por $[B, a]$ o como $B[a]$. Si $a \in \mathrm{Cent}(A)$, entonces pruebe que

$$B[a] = \{b_0 + b_1 a + b_2 a^2 \cdots + b_n a^n + m a^k \mid b_i \in B \ (1 \leq i \leq n);\ n, k \in \mathbb{N}; m \in \mathbb{Z}\}.$$

Si B tiene identidad, entonces

$$B[a] = \{b_0 + b_1 a + b_2 a^2 \cdots + b_n a^n \mid b_i \in B \ (1 \leq i \leq n);\ n \in \mathbb{N}\}.$$

22. Sean A un anillo y $n \in \mathbb{N}$. Sea $B_n = \{a \in A \mid \exists\, k \in \mathbb{N} \ni n^k a = 0\}$. Pruebe que B_n es un subanillo de A.

Dem:

$B_n \neq \emptyset$, pues $0 \in B_n$ ya que $\exists\ 1 \in \mathbb{N} \ni n^1 0 = n0 = 0$. Sean $x, y \in B_n$, existen $K_1, K_2 \in \mathbb{N}$ tales que $n^{K_1} x = n^{K_2} y = 0$. Sea $K = K_1 + K_2$, entonces:

$$n^K(x-y) = (n^{K_1} n^{K_2})x - (n^{K_1} n^{K_2})y = n^{K_2}(n^{K_1}x) - n^{K_1}(n^{K_2}y) = n^{K_2}0 - n^{K_1}0 = 0$$

$$n^K(x \cdot y) = (n^{K_1} n^{K_2})(xy) = n^{K_2}(n^{K_1}x)y = n^{K_2}0 \cdot y = 0$$

$\therefore B_n$ es subanillo de A.

q.e.d.

es un subanillo de A.

23. Sea A un anillo. Pruebe lo siguiente:

a) Si existe un entero k tal que $ka = 0$ para cada $a \in A$, entonces $\operatorname{car}(A) | k$;

b) Si $\operatorname{car}(A) > 0$, entonces $\operatorname{car}(B) \leq \operatorname{car}(A)$ para cada B subanillo de A;

c) Si A es un dominio entero y B es un subanillo de A, entonces $\operatorname{car}(B) = \operatorname{car}(A)$.

Dem:

De a): Por el alg. de la div. existen $n, r \in \mathbb{Z} \ni$:

$$K = n\operatorname{car}(A) + r, \quad 0 \leqslant r < \operatorname{car}(A)$$

$\forall\, a \in A$ se cumple:

$$\begin{aligned} 0 &= Ka \\ &= (n\operatorname{car}(A))a + ra \\ &= n(\operatorname{car}(A)a) + ra \\ &= n0 + ra \\ &= ra \end{aligned}$$

Como $r < \operatorname{car}(A)$, entonces $r = 0$. Así $\operatorname{car}(A) | K$.

De b):

Sea B un subanillo de A y $\operatorname{car}(B) = n_b$. Si $\operatorname{car}(A) = n_a$ es la característica de A, entonces:

$$n_a a = 0, \ \forall\, a \in A$$

en particular:

$$n_a b = 0, \; \forall \; b \in B$$

Por la parte anterior, $n_b | n_a \Rightarrow n_b \leqslant n_a$.

q.e.d.

24. Sea A un anillo finito con elementos $a_1, \ldots, a_n$, y sea n_i el orden aditivo de a_i $(1 \leq i \leq n)$. Pruebe que la característica de A es el mínimo común múltiplo de los n_i's.

25. Sea A un anillo el cual no tiene elementos nilpotentes. Deduzca que todo elemento idempotente de A pertenece al $\text{Cent}(A)$. (Sugerencia: Si $a^2 = a$, entonces $(aba - ab)^2 = (aba - ba)^2 = 0$ para cada $b \in A$).

26. Sea A un anillo con la propiedad: Para cada $a \in A$, $a^2 + a \in \mathrm{Cent}(A)$. Pruebe que A es conmutativo. (Sugerencia: Utilice la expresión $(a+b)^2 + (a+b)$ para probar primeramente que $ab + ba \in \mathrm{Cent}(A)$ para cada $a, b \in A$).

27. Sea A un anillo con identidad tal que $\operatorname{car}(A) = n > 0$. Pruebe que si n no es número primo, entonces A tiene divisores de cero.

28. Sean $(G,+)$ un grupo abeliano y $\mathrm{End}(G)$ el conjunto de todos los endomorfismos de G. Para cada $f, g \in \mathrm{End}(G)$, definimos las operaciones $f+g$ y $f \circ g$ como siguen: Para cada $x \in G$,

$$(f+g)(x) = f(x) + g(x) \text{ y } (f \circ g)(x) = f(g(x)).$$

Pruebe que $(\mathrm{End}(G), +, \circ)$ es un anillo, y determine los elementos invertibles de $\mathrm{End}(G)$.

29. Sea G un grupo finito escrito multiplicativamente. Digamos que $G = \{g_1, \ldots, g_n\}$. Sea A un anillo arbitrario. Considérese el conjunto $A[G]$ formado por todas las sumas formales $\sum_{i=1}^{n} a_i g_i$, donde $a_i \in A$ para cada $i = 1, \ldots, n$. Dos de tales expresiones son iguales, si ellas tienen los mismos coeficientes (en A). Definimos dos operaciones sobre $A[G]$ como siguen:

$$\sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} (a_i + b_i) g_i \text{ y } \left(\sum_{i=1}^{n} a_i g_i\right)\left(\sum_{i=1}^{n} b_i g_i\right) = \sum_{i=1}^{n} c_i g_i$$

donde $c_i = \sum_{g_j g_k = g_i} a_j b_k$ para cada $i = 1, \ldots, n$. Pruebe que con respecto a estas operaciones, $A[G]$ es un anillo. $A[G]$ es llamado el **anillo grupo de G sobre A**.