Lista Anillos De Div.

1. Pruebe que cada subanillo con identidad de un campo es un dominio entero.

Dem:

Sea K campo y T subanillo de K con identidad 1_T. Probaremos que T es dominio entero. Como K es campo, entonces K es anillo de división conmutativo, i.e $K^* = K\setminus\{0\}$.

Sean ahora $a, b \in T$. Si $ab = 0$ con $a \neq 0$, entonces $\exists\, a^{-1} \in K^*$ ⫪ $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Luego:

$$ab = 0 \Rightarrow (a^{-1}a)\, b = a^{-1} 0 \Rightarrow b = 0$$

Por tanto, T no admite divisores de cero. Como $T \subseteq K$, T es conmutativo y tiene identidad 1_T. Luego T es dominio entero.

q.e.d.

2. Sea A un anillo conmutativo con identidad, y sea $a \in A$, $a \neq 0$. Si a es divisor de cero de A, entonces pruebe que a no es unidad.

Dem:

Suponga que $a \in A^*$. Entonces $\exists\, u \in A$ ⫪ $au = 1$. Como a es divisor de cero, $\exists\, b \in A\setminus\{0\}$ ⫪

$$ab = 0$$

Luego:

$$\begin{aligned} au = 1 &\Rightarrow b(au) = b \\ &\Rightarrow (ab)u = b \\ &\Rightarrow 0u = b \\ &\Rightarrow b = 0 \quad \#c \end{aligned}$$

Luego, a no es unidad.

q.e.d.

3. Sea G el subconjunto de los cuaternios reales $\mathbb{H}$ dado por

$$G = \{1, -1, i, -i, j, -j, k, -k\}.$$

Pruebe que G es grupo multiplicativo.

4. Sea A un anillo con más de un elemento tal que para cada elemento a de A no cero, existe un único elemento b de A tal que $aba = a$. Pruebe lo siguiente:

a) A no admite divisores de cero;

b) $bab = b$;

c) A tiene elemento identidad;

d) A es un anillo de división.

Dem:

De a): Supongu que existen $x, y \in A\setminus\{0\} \ni xy = 0$. Como $x \neq 0$, $\exists!\, a \in A \ni xax = x$. Veamos:

$$xy = 0 \Rightarrow xyx = 0$$
$$\Rightarrow xyx + x = x$$
$$\Rightarrow xyx + xax = x$$
$$\Rightarrow x(y+a)x = x$$

Por unicidad: $y + a = a \Rightarrow y = 0$ #c. Por tanto A no admite divisores de cero.

De b):

Sea $a \in A\setminus\{0\}$, $\exists!\, b \in A \ni aba = a$. Veamos:

$$aba = a \Rightarrow ababa = aba = a \Rightarrow b = bab$$

De c):

Sea $a \in A\setminus\{0\}$ y $x \in A$, afirmamos que ab es la identidad de A, con $b \in A$ el único elemento tal que $aba = a$. Si $x = 0$, entonces $xab = abx = x$.

Si $x \neq 0$, $\exists!\, y \in A \ni xyx = x$, veamos:

5. Si A es un anillo de división, entonces pruebe que $\mathrm{Cent}(A)$ es un campo.

6. Sea A un dominio entero, y sea $\mathbb{Z}\cdot 1$ el subconjunto de A definido como:

Dem:

Como A es anillo de división, entonces A tiene identidad y $A^* = A\setminus\{0\}$. $\mathrm{Cent}(A)$ es un subanillo de A conmutativo, donde $1 \in \mathrm{Cent}(A)$. Veamos que $\mathrm{Cent}(A)^* = \mathrm{Cent}(A)\setminus\{0\}$.

Sea $x \in \mathrm{Cent}(A)\setminus\{0\} \subseteq A\setminus\{0\} = A^*$, entonces $\exists\, x^{-1} \in A \ni$

$$xx^{-1} = x^{-1}x = 1$$

Probaremos que $x^{-1} \in \mathrm{Cent}(A)$. Como $x \in \mathrm{Cent}(A)$:

$$\forall a \in A,\ ax = xa \Rightarrow \forall a \in A \quad x^{-1}axx^{-1} = x^{-1}xax^{-1}$$

$$\Rightarrow \forall a \in A \quad x^{-1}a = ax^{-1}$$

$$\Rightarrow x^{-1} \in \mathrm{Cent}(A)$$

Por tanto $x^{-1} \in \mathrm{Cent}(A) \Rightarrow \mathrm{Cent}(A)^* = \mathrm{Cent}(A)\setminus\{0\}$. Por tanto, $\mathrm{Cent}(A)$ es campo.

q.e.d.

6. Sea A un dominio entero, y sea $\mathbb{Z}\cdot 1$ el subconjunto de A definido como:

$$\mathbb{Z}\cdot 1 = \{n \cdot 1 \mid n \in \mathbb{Z}\}.$$

Pruebe que $\mathbb{Z}\cdot 1$ es un subcampo de A si, y solo si A tiene característica positiva.

Dem:

Como A es dominio entero, A es anillo conmutativo con identidad que no admite divisores de cero.

$\Rightarrow$) Suponga que $\mathbb{Z}\cdot 1$ es subcampo de A, i.e $\mathbb{Z}\cdot 1^* = \mathbb{Z}\cdot 1\setminus\{0\}$. Entonces, $\forall\, n \in \mathbb{Z}\setminus\{0\}$, $\exists\, m \in \mathbb{Z}\setminus\{0\} \ni (n\cdot 1)\cdot(m\cdot 1) = 1 \Rightarrow nm\cdot 1 = 1$.

En particular, para $2 \in \mathbb{Z}$, $\exists\, m \in \mathbb{Z} \ni 2m\cdot 1 = 1 \Rightarrow (2m-1)\cdot 1 = 0$. Sea $K \in \mathbb{N} \ni$

$$2K - 1 = |2m-1|$$

Se cumple que $(2K-1)\cdot 1 = 0$. Sea ahora $a \in A$, entonces:

$$\begin{aligned}(2K-1)\cdot a &= (2K-1)\cdot 1 \cdot a \\ &= ((2K-1)\cdot 1)\cdot a \\ &= 0 \cdot a = 0\end{aligned}$$

donde $2k-1>0$. Por tanto $car(A)>0$.

$\Leftarrow$) Suponga que $k=car(A)>0$. Probaremos que $\mathbb{Z}\cdot 1$ es subcampo de A, i.e basta probar que $(\mathbb{Z}\cdot 1)^* = \mathbb{Z}\cdot 1 \setminus \{0\}$. Como:

$$k\cdot 1 = 0$$

Sea $m\cdot 1 \in \mathbb{Z}\cdot 1\setminus\{0\}$. Entonces

7. Sea $f:\mathbb{C}\longrightarrow\mathbb{C}$ dada por $f(a+bi)=a-bi$ para cada $a,b\in\mathbb{R}$. Pruebe que f es un automorfismo de $\mathbb{C}$. Más aún, pruebe que exactamente existen dos automorfismos de $\mathbb{C}$ tales que dejan fijo a $\mathbb{R}$. (Un homomorfismo $f:\mathbb{C}\longrightarrow\mathbb{C}$ deja fijo a $\mathbb{R}$, si $f(x)=x$ para cada $x\in\mathbb{R}$).

Dem:

Sean $a,b,a_1,b_1\in\mathbb{R}$. Entonces:

$$\begin{aligned} f(a+bi+a_1+b_1i) &= f(a+a_1+(b+b_1)i)\\ &= a+a_1-(b+b_1)i\\ &= a-bi+a_1-b_1i\\ &= f(a+bi)+f(a_1+b_1i)\end{aligned}$$

$$\begin{aligned} f((a+bi)\cdot(a_1+b_1i)) &= f(aa_1+ab_1i+a_1bi-bb_1)\\ &= (aa_1-bb_1)-(ab_1+a_1b)i\\ &= (aa_1-bb_1)+(a(-b_1)+a_1(-b))i\\ &= aa_1-(-b)(-b_1)+(a(-b_1)+a_1(-b))i\\ &= (a-bi)\cdot(a_1-b_1i)\\ &= f(a+bi)\cdot f(a_1+b_1i)\end{aligned}$$

Por tanto f es homomorfismo. Claramente f es biyección, así f es automorfismo. Sea $h:\mathbb{C}\to\mathbb{C}$ un automorfismo de $\mathbb{C}$ que deja fijo a $\mathbb{R}$, i.e:

$$h(x)=x,\ \forall x\in\mathbb{R}$$

Sean $a,b\in\mathbb{R}$. Entonces:

$$\begin{aligned} h(a+bi) &= h(a)+h(bi)\\ &= h(a)+h(b)\cdot h(i)\\ &= a+bh(i)\end{aligned}$$

Pero $h(-1)=-h(1)=h(i)h(i)=-1$, pues h deja fijo a $\mathbb{R}$. Por tanto $h(i)^2=-1 \Rightarrow h(i)=\pm i$. Así, sólo pueden existir dos homomorfismos que dejan fijo a $\mathbb{R}$.

q.e.d.

8. Encuentre el centro de los cuaternios reales $\mathbb{H}$.

9. Sea A el conjunto de todas las matrices en $\mathfrak{M}_2(\mathbb{C})$ de la forma

Dem:

Recordando que:

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

9. Sea A el conjunto de todas las matrices en $\mathfrak{M}_2(\mathbb{C})$ de la forma

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$$

con $z, w \in \mathbb{C}$. Pruebe que A es un anillo de división el cual es isomorfo al anillo de división $\mathbb{H}$ de los cuaternios reales. (Sugerencia: Defina un isomorfismo de $\mathbb{H}$ sobre A que aplique respectivamente los elementos $1, i, j, k$ de $\mathbb{H}$ sobre las matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

Dem:

Sean $w, v \in \mathbb{C}$, como $\bar{w} + \bar{v} = \overline{w+v}$, entonces $(A, +)$ es grupo abeliano. Claramente (no tanto)[1], A es anillo. Veamos que es anillo de div. En efecto: $A^* = A \setminus \{0\}$, donde identificamos al 0 con:

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Con identidad $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Sea $M = \begin{pmatrix} z & \bar{w} \\ -\bar{w} & \bar{z} \end{pmatrix} \in A$, veamos que:

$$\det(M) = |z|^2 - \bar{w}^2$$

Si $z = a + bi$ y $w = c + di$, entonces:

$$\det(M) = a^2 + b^2 - (c^2 + d^2 - 2cdi)$$

Si $c, d \neq 0 \Rightarrow \det(M) \neq 0$. Si $c = d = 0$, entonces $\det(M) = 0 \Leftrightarrow a = b = 0$, i.e $M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Por ende $\det(M) \neq 0, \forall M \in A \setminus \{0\}$, así M es invertible y su inversa es:

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} \bar{z} & \bar{w} \\ -w & z \end{pmatrix} = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$$

Donde $u = \frac{\bar{z}}{\det M}$ y $v = \frac{\bar{w}}{\det(M)}$. Así $M^{-1} \in A$, i.e $M \in A^*$. Luego A es anillo de div. Defina ahora

$f:$

10. Sea K un campo y $A = \mathfrak{M}_2(K)$. Pruebe lo siguiente:

   a) El centro de A consiste de todas las matrices de la forma

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix};$$

   b) El centro de A no es un ideal de A;

   c) ¿Cuál es el centro de $\mathfrak{M}_n(B)$ donde B es un anillo de división?

11. Sea A un anillo. Pruebe lo siguiente:

   a) Si A tiene elemento identidad, entonces A es anillo de división si, y solo si A no tiene ideales propios izquierdos;

   b) Si A no tiene ideales propios izquierdos (posiblemente A no posea identidad), entonces $A^2 = \{0\}$ ó A es un anillo de división. (Sugerencia: Demuestre que $\{a \in A \mid Aa = 0\}$ es un ideal de A. Si $ab \neq 0$, entonces pruebe que $\{r \in A \mid rb = 0\} = \{0\}$. Encuentre un elemento e de A tal que $eb = b$, y e es identidad (por ambos lados)).

12. Pruebe que el anillo $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ es un dominio entero bajo las operaciones usuales, pero que no es un campo exhibiendo un ideal no trivial de A.

Dem:

Claramente A es un anillo. Veamos que es dominio entero. Sean $a,b,c,d,e,f \in \mathbb{Z}$ m $a+b\sqrt{2} \neq 0$. Veamos que si:

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (a+b\sqrt{2})(e+f\sqrt{2})$$

$$\Rightarrow (ac+2bd)+(ad+bc)\sqrt{2} = (ae+2bf)+(af+be)\sqrt{2}$$

$$\Rightarrow \begin{cases} ac+2bd-ae-2bf=0 \\ ad+bc-af-be=0 \end{cases}$$

$$\Rightarrow \begin{cases} a(c-e)+2b(d-f)=0 \\ a(d-f)+b(c-e)=0 \end{cases}$$

Si $a \neq 0 \Rightarrow a^2 > 0$. Luego:

$$\Rightarrow \begin{cases} a^2(c-e)^2+2ab(d-f)(c-e)=0 \\ a^2(d-f)^2+ab(d-f)(c-e)=0 \end{cases}$$

$$\Rightarrow a^2(c-e)^2-2a^2(d-f)^2=0$$

$$\Rightarrow (c-e)^2-2(d-f)^2=0$$

$$\Rightarrow (c-e+\sqrt{2}(d-f))(c-e-\sqrt{2}(d-f))=0 \ \ldots (1)$$

Probaremos un resultado. Si $x,y \in \mathbb{Z}$ son m $x^2-2y^2=0 \Rightarrow x=y=0$. Si $x \neq 0$, entonces $y \neq 0$, pero la ec. $x^2-2y^2=0$ no tiene sols. en $\mathbb{Z}$ no triviales, luego $x=y=0$. Por tanto, de (1):

$$c-e=d-f=0 \Rightarrow c=e \text{ y } d=f$$

$\Rightarrow c+\sqrt{2}d = e+\sqrt{2}f$, i.e A es dominio entero. Pero no es campo, pues el conjunto

$$I = \{2a+2\sqrt{2}b \mid a,b \in \mathbb{Z}\}$$

es un ideal no trivial de A.

q.e.d.

13. Sean A un anillo y $f, g : \mathbb{Q} \longrightarrow A$ homomorfismos tales que $f(r) = g(r)$ para cada $r \in \mathbb{Z}$. Pruebe que $f = g$ sobre $\mathbb{Q}$.

Dem:

Como $\mathbb{Q}$ es campo, entonces f y g son triviales, o son monomorfismos. No puede suceder que uno sea trivial y el otro sea monomorfismo, i.e ambos son triviales o son monomorfismos. Luego $\mathbb{Q} \hookrightarrow A$ bajo f y g.

Considere $f(\mathbb{Q})$ y $g(\mathbb{Q}) \subseteq A$.

14. Sea $f : A \longrightarrow B$ un homomorfismo. Supóngase que A contiene un subanillo K el cual es un campo. Pruebe que $K \subseteq \ker(f)$ ó B contiene un subanillo el cual es isomorfo a K.

15. Sea p número primo, y sea $K = \{a+b\sqrt{p} \mid a, b \in \mathbb{Q}\}$. Pruebe que K es un subcampo de $\mathbb{R}$.

de $\mathbb{R}$.

16. Pruebe las siguientes afirmaciones:

    a) El elemento identidad de un subcampo es el mismo que el del campo;

    b) Si $\{K_i\}_i$ es una familia de subcampos de un campo K, entonces $\cap_i K_i$ es también un subcampo de K;

    c) Un subanillo F de un campo K es un subcampo de K si, y solo si F contiene al menos un elemento no cero, y $a^{-1} \in F$ para cada $a \in F$;

    d) Un subconjunto F de un campo finito K es un subcampo de K si, y solo si F contiene más de un elemento, y es cerrado bajo la adición y multiplicación.

17. Pruebe que si K es un campo de característica $p \geq 0$, entonces cada subcampo de K es de característica p.

18. Sean K un campo y $p \geq 0$ su característica. Sea P_K la intersección de todos los subcampos de K. P_K es llamado el **campo primo** de K. Pruebe lo siguiente:

   a) $P_K \cong \mathbb{Z}/p\mathbb{Z}$ si $p > 0$;

   b) $P_K \cong \mathbb{Q}$ si $p = 0$.

19. Sea K un campo de característica $p > 0$, y sea $n \geq 1$. Pruebe que el conjunto

$$\{a \in K \mid a^{p^n} = a\}$$

es un subcampo de K.

20. Sean K un campo y F subcampo de K. Si f es un automorfismo de K, decimos que f **deja fijo a un elemento** a **de** F si $f(a) = a$. Pruebe lo siguiente:

a) El conjunto de todos los automorfismos de K forman un grupo con la operación de composición;

b) El conjunto de automorfismo de K que dejan fijo a los elementos de F es un subgrupo del grupo de automorfismos de K;

c) Si G es un subgrupo del grupo de automorfismos de K, entonces el conjunto

$$\{a \in K \mid f(a) = a \; \forall f \in G\}$$

es un subcampo de K llamado el **campo fijo de** K **por** G y es denotado por K^G.

Dem:

De a): Es inmediata.

De b): Sea

$$\mathcal{E} = \{ f \in Aut(K) \mid f(a) = a, \; \forall a \in F \}$$

$\mathcal{E} \neq \emptyset$ pues $id \in \mathcal{E}$. Sean $f, g \in \mathcal{E}$, entonces:

$$\begin{aligned} f \circ g^{-1}(a) &= f(g^{-1}(a)) \\ &= f(a) \\ &= a, \; \forall a \in F \end{aligned}$$

$\therefore \mathcal{E} < Aut(G)$.

De c): Probamos que K^G es subanillo de K. $K^G \neq \emptyset$, pues $f(0) = 0$, $\forall f \in G$ (por ser f automorfismo), luego $0 \in K^G$. Sean $a, b \in K^G$ y sea $f \in G$:

$$\Rightarrow f(ab) = f(a)f(b) = ab \qquad f(a-b) = f(a) - f(b) = a - b$$

Luego K^G es subanillo de K. Si $a \in K^G \setminus \{0\}$, entonces

$$f(a^{-1}) = f(a)^{-1} = a^{-1}, \text{ pues } f(a) \neq 0 \text{ y } K \text{ es campo}$$

Luego a^{-1} es dejado fijo por f. Por tanto $(K^G)^* = K^G \setminus \{0\}$, i.e K^G es subcampo de K.

q.e.d.

Notas:

1)