

Ejercicio 1. Se considera un conjunto R con dos operaciones internas $+$ y \cdot tal que $(R, +)$ es un grupo, \cdot es asociativa y distributiva respecto a $+$. Si \cdot posee identidad, demostrar que $(R, +, \cdot)$ es un anillo.

Equivale a probar que la operación $+$ es conmutativa. Por un lado tenemos

$$-(a + b) = -a - b, \quad -(b + a) = -b - a$$

Por tanto

$$-(a + b) + a = -a - b + a, \quad -(b + a) + a = -b$$

Restando:

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

Por tanto,

$$a + b = b + a.$$

Hemos usado que para todo elemento r de R , $-1 \cdot c = -c$.

Ejercicio 2. Sea R un anillo con identidad y $a \in R$ un elemento de R que no es divisor de cero a derecha y que tiene un inverso a izquierda. Demostrar que a es unidad en R .

Por hipótesis, si $r \in R$ es tal que $ra = 0$, entonces $r = 0$. Por otro lado, existe $s \in R$ tal que $sa = 1$. Así:

$$ara = a \implies (ar - 1)a = 0 \implies ar = 1.$$

Ejercicio 3. Demostrar que si R es un anillo con identidad y $a, b \in R$ son dos elementos de R tales que $1 - ba$ tiene un inverso a izquierda, entonces $1 - ab$ también tiene un inverso a izquierda.

Sea $r \in R$ el inverso a izquierda de $1 - ba$. Entonces

$$r(1 - ba) = r - rba = 1 \implies rba = r - 1$$

Por tanto

$$ab = a \cdot 1 \cdot b = a[r(1 - ba)]b = arb - arbab = arb(1 - ab)$$

Sea $s = 1 + arb$. Entonces

$$s(1 - ab) = (1 + arb)(1 - ab) = (1 - ab) + arb(1 - ab) = (1 - ab) + ab = 1$$

Ejercicio 4. Sea p un número primo. Demostrar que si R es un anillo con identidad de orden p^2 , entonces R es conmutativo. ¿Es cierto si R no posee identidad? Dar un ejemplo de anillo con identidad no conmutativo de orden p^3 .

Sabemos que $|Z(R)| > 1$ porque $0, 1 \in Z(R)$. Supongamos que $|Z(R)| = p$. Entonces $R/Z(R)$ es un grupo cíclico con la suma, por tener orden $p^2/p = p$. Supongamos que este grupo viene generado por $r \in R$. Sean $x, y \in R$. Queremos ver $xy = yx$. Se tiene:

$$x + Z(R) = nr + Z(R), \quad y + Z(R) = mr + Z(R)$$

para enteros positivos m, n . Por tanto,

$$x = nr + z_1, \quad y = mr + z_2$$

para elementos z_1, z_2 del centro de R . Así:

$$xy = nr \cdot mr + nrz_2 + z_1mr + z_1z_2 = nmr^2 + nrz_2 + z_1mr + z_1z_2 = mnr^2 + nrz_2 + z_1mr + z_1z_2.$$

Por otro lado

$$yx = mr \cdot nr + mrz_1 + z_2nr + z_2z_1 = mnr^2 + nrz_2 + z_1mr + z_1z_2 = xy.$$

El caso $|Z(R)| = p^2$ implica $R = Z(R)$ luego R es directamente conmutativo.

Considérese el anillo

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}_p \right\}$$

Entonces

$$e_{12}e_{11} = 0 \neq e_{12} = e_{11}e_{12}.$$

Por tanto es un ejemplo de anillo de orden p^2 sin identidad que no es conmutativo. Para un ejemplo de orden p^3 basta tomar el anillo

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\}$$

Y tenemos de la misma forma que

$$e_{12}e_{11} = 0 \neq e_{12} = e_{11}e_{12}.$$

Ejercicio 5. Sea x un elemento nilpotente de un anillo con identidad R . Prueba que $1 + x$ es una unidad de R . Deduce que si R es conmutativo, la suma de un elemento nilpotente y una unidad es una unidad. Dar un ejemplo que demuestre que

Sea x tal que $x^n = 0$ par algun entero positivo n . Sea $u = -x$. Entonces

$$(1 - u)(1 + u + \cdots + u^{n-1}) = 1 - u^n = 1$$

Como $1 - u = 1 + x$, esto demuestra que $1 + x$ es unidad.

Supongamos que R es conmutativo. Sea x nilpotente y sea $u \in R$ una unidad. Veamos que $x + u$ es una unidad. Considérese el elemento $y = -xu^{-1} \in R$. Entonces $y^n = 0$ por ser x nilpotente. Además,

$$(x + u)u^{-1}(1 + y + \cdots + y^{n-1}) = 1 - y^n = 1.$$

Esto es lo que queríamos demostrar.

Como contraejemplo para mostrar que la conmutatividad es necesaria, considérense las matrices en \mathbb{Z}_2 . En este caso, la matriz e_{12} es nilpotente dado que $e_{12}^2 = 0$. Además, la matriz

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

es unidad dado que su cuadrado es la identidad. Sin embargo, la suma de estas matrices tiene determinante 0, por lo que no es unidad.

Ejercicio 6. Se considera un elemento a de un anillo con identidad R con más de un inverso por la derecha. Demostrar que a tiene infinitos inversos a derecha en R .

Sean b_1, b_2 distintos tales que $ab_1 = ab_2 = 1$. Supongamos por reducción al absurdo que hay un número finito de inversos a derecha. Sean b_1, \dots, b_n todos ellos (distintos entre sí). Definamos $c_i := 1 - b_i a$ para $1 \leq i \leq n$. Si $c_i = c_j$, entonces

$$c_i = c_j \implies b_i a = b_j a \implies b_j a b_i = b_i a b_i \implies b_i = b_j$$

Es decir, que todos los c_i son distintos entre sí. Además, $ac_i = 0$. Por tanto $b_1 + c_i$ son inversos de a a izquierda:

$$a(b_1 + c_i) = ab_1 + ac_i = ab_1 = 1.$$

Por tanto

$$b_1, b_1 + c_1, \dots, b_1 + c_n$$

son $n + 1$ inversos de a . Falta ver que son distintos. Ello equivale a probar que los c_i son no nulos. Equivalentemente, que $1 \neq b_i a$ para todo i . Supongamos por reducción al absurdo que $b_1 a = 0$. Entonces:

$$0 = (1 - b_1 a)b_2 = b_2 - b_1(ab_2) = b_2 - b_1 \implies b_1 = b_2.$$

Esto es una contradicción dado que hemos supuesto que los b_i eran todos distintos.

Prueba alternativa: Sea $e = ba$. Entonces $e^2 = baba = b(ab)a = ba = e$. Así,

$$(1 - e)(1 - e) = 1 + e^2 - e - e = 1 + e - e - e = 1 - e$$

Definimos $e_{ij} := b^i(1 - e)a^j$, para números naturales i, j . Entonces

$$e_{ij}e_{kl} = b^i(1 - e)a^j b^k(1 - e)a^l \tag{1}$$

Notamos que

$$a^j b^k = \begin{cases} a^{|j-k|} & \text{si } j \geq k \\ b^{|j-k|} & \text{si } j < k \end{cases}$$

Además, notamos que

$$a(1 - e) = 0 = (1 - e)b$$

Concluyendo así que la parte derecha de ?? se anula salvo que $k = j$, caso en el que se tiene

$$e_{ij}e_{jl} = b^i(1 - e)a^l = e_{il}$$

En resumen:

$$e_{ij}e_{kl} = \begin{cases} 0 & \text{si } j \neq k \\ e_{il} & \text{si } j = k. \end{cases}$$

Notamos que son distintos porque, por ejemplo,

$$e_{ii}e_{ii} = e_{ii} \neq 0 = e_{ii}e_{jj}.$$

Ejercicio 7. Demostrar que si un anillo R no tiene elementos nilpotentes distintos de cero, entonces todo elemento idempotente pertenece al centro de R .

Sea $a \in R$ tal que $a^2 = a$. Sea $x \in R$. Entonces

$$xa - axa, ax - axa$$

son nilpotentes:

$$(xa - axa)^2 = xaxa - xaaxa - axaxa + axaaxa = 0.$$

Y análogamente

$$(ax - axa)^2 = 0.$$

Por hipótesis, $xa - axa = 0 = ax - axa$. Concluimos así que $ax = xa$, y por tanto $a \in Z(R)$. Esto ocurre, por ejemplo, en los anillos de división. Si en un anillo de división un elemento es nilpotente, entonces necesariamente es el 0.

Ejercicio 8. Sea S un subanillo de un anillo R . Demostrar que si R y S tiene identidad y éstas son distintas, entonces la identidad de S es un divisor de cero de R .

Se da la siguiente situación:

$$(1_R - 1_S) \cdot 1_S = 1_R 1_S - 1_S 1_S = 1_S - 1_S = 0.$$

Sin embargo, $1_R - 1_S \neq 0$ por hipótesis. Como ejemplo de esta situación, podemos considerar R y S como sigue:

$$S := \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Z} \right\}, \quad R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$$

Ejercicio 9. Sea R un anillo en el que para todo $x \in R$ existe $n_x > 1$ tal que $x^{n_x} = x$. Demostrar que R no tiene elementos nilpotentes no nulos y que si R es conmutativo con identidad, todo ideal primo es maximal.

Sea $0 \neq x \in \text{Nil}(R)$. Entonces existe un entero positivo m tal que $x^m = 0$. Supongamos que m es el menor entero positivo satisfaciendo tal propiedad. Como x es no nulo, necesariamente $m \neq n_x$. Distinguimos casos: Si $m < n_x$, entonces

$$x^{n_x} = x^m x^{n_x-m} = 0,$$

lo que supone una contradicción. Por otro lado, si $m \geq n_x$, podemos aplicar el algoritmo de la división

$$m = n_x q + r$$

para enteros q, r y $0 \leq r < n_x$. Así:

$$0 = x^m = x^{n_x q + r} = x^{q+r}$$

Dado que $n_x > 1$, necesariamente $q + r < m$. Esto contradice la propiedad de minimalidad de m . Esto nos permite concluir que el anillo no tiene elementos nilpotentes no nulos.

Para el siguiente paso del problema necesitamos usar el siguiente lema:

Lema 1. Si en el enunciado del problema suponemos que R es un dominio de integridad, entonces R es directamente un cuerpo.

Demostración. Supongamos que R es dominio de integridad. Sea x un elemento no nulo de R . Entonces $x^{n_x} - x = x(x^{n_x-1} - 1) = 0$ y dado que x es no nulo, necesariamente $x^{n_x-1} = 1$. Por tanto x es unidad. Esto implica que R es cuerpo. ■

Sea ahora P un ideal primo y que R es conmutativo. Entonces R/P es un dominio de integridad. Así, para todo elemento x de R ,

$$(x + P)^{n_x} = x + P,$$

por el lema anterior, esto implica que R/P es cuerpo. Así, P es ideal maximal.

Para próximos ejercicios será interesante tener en cuenta el siguiente lema:

Lema 2. Bajo las condiciones del ejercicio anterior, para todo x elemento de R , x^{n_x-1} pertenece al centro del anillo R

Demostración. Se tiene la siguiente situación:

$$(x^{n_x-1})^2 = x^{n_x-1} \cdot x^{n_x-1} = x^{n_x} x^{n_x-2} = x^{n_x-1},$$

por lo que x^{n_x-1} es nilpotente. Por el ejercicio 7, x^{n_x-1} pertenece al centro de R . ■

Ejercicio 10. Sea $R = \{f \in \mathbb{R}^{[0,1]} : f \text{ es continua}\}$. Demuestra que R es un anillo conmutativo con identidad y determina sus ideales maximales.

El anillo es conmutativo porque lo es \mathbb{R} . Además, su identidad es la aplicación constante 1. Vamos a determinar sus ideales maximales. Para cada $\alpha \in [0, 1]$, considérese la aplicación

$$\begin{aligned} \phi_\alpha : R &\longrightarrow \mathbb{R} \\ f &\longmapsto f(\alpha). \end{aligned}$$

Esta aplicación es un homomorfismo de anillos cuyo núcleo es

$$M(\alpha) := \ker \phi_\alpha = \{f \in R : f(\alpha) = 0\} \neq R.$$

Sea M un ideal maximal tal que para todo $\alpha \in [0, 1]$, $M \not\subseteq M(\alpha)$. Entonces para cada $\alpha \in [0, 1]$ existe una función $f_\alpha \in M$ tal que $f_\alpha(\alpha) \neq 0$. Como f es continua, considérese U_α un entorno de α contenido en $[0, 1]$ en el que f_α no se anula. Como $[0, 1]$ es compacto, podemos recubrirlo con un número finito de estos entornos $\{U_{\alpha_1}, \dots, U_{\alpha_n}\}$. Definimos

$$h := f_{\alpha_1}^2 + \dots + f_{\alpha_n}^2 \in M.$$

Entonces h no se anula en ningún punto del intervalo $[0, 1]$. Por tanto h es una unidad que está en M . Concluimos así que $M = R$. Pero esto contradice la condición de maximalidad de M . Por tanto, los ideales maximales son los de la forma $M(\alpha)$ para algún $\alpha \in [0, 1]$.

Ejercicio 11. Si $x^3 = x$ para todo elemento x de R , demostrar que $6x = 0$ para todo $x \in R$ y que R es conmutativo.

Para todo x de R , $2x = (2x)^3 = 8x^3 = 8x$ y por tanto $6x = 0$. Además, por el lema ??, x^2 pertenece al centro de R para todo x de R . Así, dados x, y elementos de R ,

$$xy = (xy)^3 = xyxyxy = x(yx)^2y = xy(yx)^2 = xy^2xyx = y^2x^2yx = y^3x^3 = yx,$$

concluyendo así que R es conmutativo.

Ejercicio 12. Sea R anillo con identidad, y sea $S = \text{Mat}_n(R)$. Demostrar que los ideales de S son exactamente los de la forma $\text{Mat}_n(I)$ para I un ideal de R . Determinar los ideales primos y maximales de S .

Sea J un ideal de S . Consideramos el siguiente subconjunto de R :

$$I := \{r \in R \mid \exists (a_{ij}) \in J : a_{11} = r\}.$$

Veamos que I es ideal de R . La suma de dos elementos de I está claramente en I . Además, al multiplicar un elemento de $a \in I$ por cualquier elemento de $r \in R$, consideramos $(a_{ij}) \in J$ tal que $a_{11} = a$, y entonces la matriz (b_{ij}) dada por $b_{ij} = ra_{ij}$ satisface $b_{11} = ra$. Así, I es un ideal de R . Veamos que $J = \text{Mat}_n(I)$ por doble inclusión.

Sea $(b_{ij}) \in \text{Mat}_n(I)$. Como $b_{ij} \in I$, por definición existe para cada $i, j \in \{1, \dots, n\}$ una matriz A_{ij} de J cuya primera entrada es igual a b_{ij} . Así,

$$B_{ij} := e_{i1}A_{ij}e_{1j}$$

es una matriz de J (por ser J ideal) con entradas todas nulas salvo la entrada i, j , que será igual a b_{ij} . Por tanto,

$$(b_{ij}) = \sum_{i,j \in \{1, \dots, n\}} B_{ij} \in J.$$

Concluimos que $\text{Mat}_n(I) \subseteq J$.

Sea ahora $(a_{ij}) \in J$. Queremos ver que todas las entradas de (a_{ij}) están en I . Para $i_0, j_0 \in \{1, \dots, n\}$ dados, la matriz

$$e_{1i_0}(a_{ij})e_{j_01}$$

tiene como primera entrada $a_{i_0j_0}$, por lo que $a_{i_0j_0} \in I$. Concluimos así con la igualdad deseada.

Ahora veamos que si I es un ideal de R , entonces $J = \text{Mat}_n(I)$ es un ideal de S . Está claro que la suma de elementos de J está en J . Asimismo, al multiplicar un elemento de J por cualquier elemento de S , obtendremos una nueva matriz cuyas entradas son sumas de elementos de la forma $r \cdot a$ con $r \in R$ y $a \in I$. Como I es ideal, $ra \in I$, luego las entradas de dicha matriz estarán en I . Por tanto J es un ideal.

De esta forma, podemos considerar una biyección $\bar{}$ de los ideales de R a los ideales de S dado por $\bar{I} = \text{Mat}(I)$

Veamos ahora cuáles son los ideales primos de S . Para ello, necesitamos usar lo que demostraremos a continuación. Supongamos que $I \subseteq J \subseteq R$ son ideales de R . Entonces obviamente $\bar{I} \subseteq \bar{J} \subseteq S$. Recíprocamente, si $I, J \subseteq R$ son ideales de R tales que $\bar{I} \subseteq \bar{J}$, entonces dado $a \in I$, podemos considerar la matriz $ae_{11} \in \bar{I} \subseteq \bar{J}$, concluyendo así que $a \in J$. En conclusión, $I \subseteq J$. Podemos resumir este resultado con las palabras “ $\bar{}$ y su inversa conservan la inclusión de ideales”.

Vamos a ver que los ideales primos de S son exactamente \overline{P} donde P es un ideal primo de R . Sea P un ideal primo de R , y supongamos que $\overline{IJ} \subseteq \overline{P}$. Sean $a \in I$, $b \in J$. Entonces $ae_{11}be_{11} = abe_{11} \in \overline{IJ} \subseteq \overline{P}$, por lo que $ab \in P$. Esto implica que $IJ \subseteq P$. Así, $I \subseteq P$ o $J \subseteq P$ por ser P primo. Como $\overline{}$ conserva la inclusión de ideales, $\overline{I} \subseteq \overline{P}$ o $\overline{J} \subseteq \overline{P}$. Concluimos que P es ideal primo de S .

Recíprocamente, si \overline{P} es ideal primo de S y I, J son ideales de R tales que $IJ \subseteq P$, entonces $\overline{IJ} \subseteq \overline{P}$. Notamos que $\overline{IJ} \subseteq \overline{I}J$, es decir, el producto de una matriz con entradas en I por una matriz con entradas en J será una matriz con entradas en IJ . Por tanto, $\overline{IJ} \subseteq \overline{P}$. Como \overline{P} es primo, necesariamente $\overline{I} \subseteq \overline{P}$ o $\overline{J} \subseteq \overline{P}$. Por tanto, $I \subseteq P$ o $J \subseteq P$. Concluimos así que P es ideal primo de R .

Para los maximales hacemos algo similar. Los maximales de S serán exactamente de la forma \overline{M} para M ideal maximal de R . En efecto, si M es un maximal de R , entonces $\overline{M} \neq S$ y si $\overline{M} \subsetneq \overline{I} \subseteq S$, entonces $M \subsetneq I \subseteq R$ y por la maximalidad de M , $I = R$, luego $\overline{I} = S$, concluyendo así que \overline{M} es maximal.

Recíprocamente, si \overline{M} es maximal en S , entonces $\overline{M} \neq S$ luego $M \neq R$; y si $M \subsetneq I \subseteq R$ entonces $\overline{M} \subsetneq \overline{I} \subseteq S$, y por la maximalidad de \overline{M} se tiene $\overline{I} = S$. Por tanto, $I = R$, concluyendo que M es maximal de R .

Ejercicio 13. Sea $R = R_1 \times \cdots \times R_n$ un producto de anillos con identidad. Demuestra que para todo ideal I de R existen ideales I_1, \dots, I_n de R_1, \dots, R_n , respectivamente, tales que $I = I_1 \times \cdots \times I_n$. ¿Es cierto el resultado si los anillos R_i no tienen identidad?

Sea J un ideal de R . Consideramos el epimorfismo de anillos “proyección” $\pi_k : R \rightarrow R_k$, y el ideal $I_k = \pi_k(J)$ para $1 \leq k \leq n$, que es un ideal de R_k . Veamos $J = I_1 \times \cdots \times I_n$. Sea $j \in J$. Entonces $\pi_k(j) \in I_k$. Así, $j \in I_1 \times \cdots \times I_n$. Sea ahora $(i_1, \dots, i_n) \in I_1 \times \cdots \times I_n$. Entonces $i_k = \pi_k(j_k)$ para algún $j_k \in J$. Sea $e_k \in R$ el elemento cuyas entradas son todas nulas salvo la entrada k -ésima, cuyo valor es 1. Este elemento existe porque todos los R_i tienen identidad. Entonces como J es ideal, $e_k j_k \in J$. Además,

$$(i_1, \dots, i_n) = \sum_{k=1}^n e_k j_k \in J.$$

Concluimos así con la igualdad de conjuntos.

Recíprocamente si I_k es un ideal de R_k para $1 \leq k \leq n$, y consideramos el subconjunto $J = I_1 \times \cdots \times I_n$ de R , es fácil ver que la suma de elementos de J está en J y que si multiplicamos un elemento de J por uno de R volvemos a caer en J . Es decir, que J es un ideal de R .

Si consideramos el anillo cero $(\mathbb{Z}_2, +, \cdot)$, y definimos $R = \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces tomando $0 \neq a \in \mathbb{Z}_2$, el ideal $\langle (a, a) \rangle$ de R no es producto de ideales de \mathbb{Z}_2 , dado que cualquier producto de ideales de \mathbb{Z}_2 es el ideal 0, mientras que el primero no el ideal cero. Por tanto, si los anillos no tienen identidad, el resultado no es cierto.

Ejercicio 14. Sea $f : R \rightarrow S$ un homomorfismo de anillos. Sea I un ideal de R y J un ideal de S . Demuestra que

1. Si f es un epimorfismo y J es maximal en S , entonces $f^{-1}(J)$ es ideal maximal de R .

2. Si f es epimorfismo y $\ker f \subseteq I$ e I es ideal maximal de R , entonces $f(I)$ es un ideal maximal de S .
3. Si J es ideal primo de S y f es epimorfismo, entonces $f^{-1}(J)$ es ideal primo de R .
4. Si f es epimorfismo, $\ker f \subseteq I$ e I es ideal primo de R , entonces $f(I)$ es ideal primo de S .

Recordamos algunas propiedades básicas de las aplicaciones y de las aplicaciones sobreyectivas. Si $f : A \longrightarrow B$ es una aplicación y $C \subseteq A$ y $D \subseteq B$, entonces

$$C \subseteq f^{-1}(f(C)), \quad f(f^{-1}(D)) \subseteq D$$

Además, si f es sobreyectiva,

$$f(f^{-1}(D)) = D,$$

y aunque no lo usaremos, si f es inyectiva

$$C = f^{-1}(f(C))$$

1. Notamos que $f^{-1}(J)$ es ideal de R . Además, si $f^{-1}(J) = R$ entonces $f(f^{-1}(J)) = J = f(R) = S$, lo que contradice la maximalidad de J . Así $f^{-1}(J) \subsetneq R$. Supongamos $f^{-1}(J) \subsetneq I \subseteq R$. Tomando imágenes,

$$J \subseteq f(I) \subseteq S$$

Supongamos que $J = f(I)$. Entonces $f^{-1}(J) = f^{-1}(f(I)) \supseteq I$, lo cual es una contradicción con que $f^{-1}(J) \subsetneq I$. Así,

$$J \subsetneq f(I) \subseteq S,$$

y por la maximalidad de J , encontramos que $f(I) = S$. Así, dado $r \in R$, $f(r) \in S$, luego $f(r) = f(i)$ para algún $i \in I$, y así $f(r) - f(i) = f(r - i) = 0$, es decir $r - i \in \ker f$. Como $\ker f \subseteq f^{-1}(J) \subsetneq I$, se tiene que $r - i \in I$, luego $r \in I$. Concluimos que $I = R$.

2. Notamos que al ser f sobreyectiva, $f(I)$ es ideal de S . Supongamos que $f(I) = S$. Entonces, razonando como anteriormente, $I = R$, lo que contradice la maximalidad de I . Así, $f(I) \neq S$. Supongamos ahora que $f(I) \subsetneq J \subseteq S$. Entonces

$$I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(J) \subseteq S.$$

Supongamos $I = f^{-1}(J)$. Entonces $J = f(f^{-1}(J)) = f(I)$, lo que contradice el hecho de que $f(I) \subsetneq J$. Por tanto, teniendo en cuenta además que $f^{-1}(J)$ es un ideal de R e I es maximal, necesariamente $f^{-1}(J) = S$.

3. Notamos que $f^{-1}(J)$ es ideal de R . Supongamos $f^{-1}(J) = R$. Entonces $J = f(f^{-1}(J)) = f(R) = S$, lo cual es una contradicción. Sean A, B ideales de R tales que $AB \subseteq f^{-1}(J)$. Entonces $f(AB) \subseteq f(f^{-1}(J)) = J$. Además, como f es homomorfismo,

$$f(A)f(B) \subseteq f(AB)$$

Luego $f(A)f(B) \subseteq J$. Tanto $f(A)$ como $f(B)$ son ideales por ser f un epimorfismo. Por la primalidad de J , $f(A) \subseteq J$ o $f(B) \subseteq J$. Concluimos así que $A \subseteq f^{-1}(f(A)) \subseteq f^{-1}(J)$ o $B \subseteq f^{-1}(f(B)) \subseteq f^{-1}(J)$. Por tanto $f^{-1}(J)$ es ideal primo.

4. Notamos que $f(I)$ es ideal por ser f epimorfismo. Además, si $f(I) = S$ entonces, como ya hemos argumentado anteriormente, $I = R$, lo que contradice la primalidad de I . Por tanto $f(I) \neq S$. Supongamos que A, B son dos ideales de S tales que $AB \subseteq f(I)$. Entonces $f^{-1}(AB) \subseteq f^{-1}(f(I))$. Veamos que $f^{-1}(f(I)) = I$. Está claro que $I \subseteq f^{-1}(f(I))$. Sea $a \in f^{-1}(f(I))$. Entonces $f(a) \in f(I)$. Sea $i \in I$ tal que $f(a) = f(i)$. Entonces $a - i \in \ker f \subseteq I$, por lo que $a \in I$. Así, se da la igualdad de conjuntos. Por otro lado, si $rs \in f^{-1}(A)f^{-1}(B)$, entonces

$$f(rs) \in f(f^{-1}(A)f^{-1}(B)) = f(f^{-1}(A))f(f^{-1}(B)) = AB,$$

es decir, $rs \in f^{-1}(AB)$. Esto demuestra que $f^{-1}(A)f^{-1}(B) \subseteq f^{-1}(AB)$, y por tanto

$$f^{-1}(A)f^{-1}(B) \subseteq f^{-1}(AB) \subseteq f^{-1}(f(I)) = I.$$

Por la primalidad de I , o bien $f^{-1}(A) \subseteq I$ o $f^{-1}(B) \subseteq I$. Tomando imágenes en ambos lados, obtenemos que $A \subseteq f(I)$ o $B \subseteq f(I)$. Esto demuestra la primalidad de $f(I)$.

Ejercicio 15. *Se considera un anillo con identidad R que satisface la siguiente propiedad: para todo $r \in R$ existe un único $s \in R$ tal que $rsr = r$. Demostrar que en este caso $srs = s$ y que R es un anillo de división.*

Tenemos la siguiente situación

$$r(srs)r = (rsr)sr = rsr = r.$$

Como s es el único elemento que satisface $rsr = r$, y además $r(srs)r = r$, necesariamente $s = srs$. Por otro lado,

$$(sr)(sr)(sr) = s(rsr)sr = srsr = s(rsr) = sr, \quad (sr) \cdot 1 \cdot (sr) = s(rsr) = sr.$$

De nuevo, por la unicidad, deducimos que $sr = 1$.