Grupos y Anillos - Ejercicios

Jose Antonio Lorencio Abril

2019/2020

Contents

Introducción

En este documento voy a recopilar todos los ejercicios de la asignatura que me parezcan interesantes. Intentaré hacerlos con rigurosidad y precisión, mencionando las proposiciones utilizadas.

Los ejercicios que piden demostrar lemas anteriores, por lo general, no los voy a incluir, pues normalmente son sencillos o han sido resueltos en clase.

1 Anillos

1.1 Operaciones binarias

Los tres primeros ejercicios de esta sección son bastante sencillos, pesados y repetitivos. Voy a comenzar por el cuarto.

1.1.4 Demostrar que si a, b son elementos invertibles en un monoide entonces ab, a^{-1} también son invertibles y $(a^{-1})^{-1} = a$. Deducir que el conjunto de los elementos invertibles de un monoide forma un grupo con la operación del monoide.

Como a y b son invertibles, existen a^{-1} y b^{-1}. Así, $b^{-1}a^{-1}$ está en el monoide, que podemos llamar X. Sea e el neutro de X.

Entonces

$$(ab)(b^{-1}a^{-1}) \overset{X \ monoide}{=} a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

Por lo que tenemos que ab es invertible, con inverso $b^{-1}a^{-1}$.

Por otro lado

$$aa^{-1} = e = a^{-1}a$$

Por lo que a^{-1} es invertible y su inversa es a. Por la proposición 1.2, a^{-1} tiene a lo sumo un inverso, por tanto, $(a^{-1})^{-1} = a$.

Vamos a ver la última parte del enunciado.

- Asociatividad: $ab = ba$, pues $a, b \in X$, que es monoide.
- Elemento neutro: $1 = 1 \cdot 1 \implies 1 \ invertible \implies 1 \in Y = \{x \in X / x \ invertible\}$
- Invertibilidad: $\forall y \in Y$ se tiene que y es invertible, por definición de Y.

El siguiente también es sencillo, solo hay que echar la cuenta y ver qué deben cumplir $*$ y $\circ$ en cada caso:

- $\#$ asociativa si $*, \circ$ asociativas
- $\#$ conmutativa si $*, \circ$ conmutativas
- $\#$ tiene neutro si $*, \circ$ tienen neutro y $N_{\#} = (N_*, N_\circ)$
- Los elementos invertibles respecto $\#$ son los que su primera coordenada es invertible respecto $*$ y la segunda respecto $\circ$

1.1.6 Demostrar que si $(X, *)$ es un monoide finito entonces los elementos cancelativos por la izquierda de X son exactamente los que tienen un simétrico por la izquierda. Dar un ejemplo de un elemento cancelativo de un monoide conmutativo que no tenga simétrico.

Por la proposición 1.2, sabemos que si un elemento tiene simétrico por un lado, entonces es cancelable por ese mismo lado.

Este ejercicio nos dice que en los monoides finitos son simétricos y los cancelables son equivalentes.

Supongamos $X = \{e, x_1, ..., x_n\}$ donde e es el neutro.

Y supongamos que x_i es cancelativo por la izquierda. Definamos ahora $f_i : X \to X$ con $f_i(a) = x_i a$.

Entonces, x_i es cancelativo por la izquierda si, y solo si, f_i es inyectiva, ya que si no lo fuera, existirían $a \neq b \in X / x_i a = x_i b$, por lo que no podríamos cancelar x_i.

Ahora bien, como X es finito, f_i inyectiva implica f_i suprayectiva ya que f_i inyectiva $\implies |f_i(X)| \geq |X|$ y $f_i(X) \subset X \implies |f_i(X)| \leq |X|$, por tanto $|f_i(X)| = |X|$, y al ser finitos son el mismo y f_i es sobreyectiva.

Por ser suprayectiva, $\exists a \in X / x_i a = f_i(a) = e \implies x_i$ tiene simétrico por la derecha $\overset{prop\ 1.2}{\implies} x_i$ cancelativo por la derecha $\overset{razonando\ como\ antes}{\implies} x_i$ tiene simétrico por la izquierda.

Es decir, el resultado es más fuerte aún de lo que nos dice el enunciado, pues tenemos que la invertibilidad en un monoide finito es equivalente a la cancelatividad por un lado.

El ejemplo pedido podría ser $(\mathbb{N}, \cdot)$, con cualquier elemento distinto de 1.

|———|

El séptimo ejercicio estuvimos pensándolo en clase y no conseguimos llegar a una conclusión clara.

1.2 Anillos

1.2.2 Sea $m \in \mathbb{Z}$. Demostrar que si m no es un cuadrado en $\mathbb{Z}$, entonces tampoco es un cuadrado en $\mathbb{Q}$.

Supongamos que $m = \left(\frac{a}{b}\right)^2 \iff a^2 = mb^2$

Descomponiendo m como producto de factores primos, queda

$$m = \pm p_1^{e_1} \cdot ... \cdot p_k^{e_k}$$

Con $p_1, ..., p_k$ primos distintos.

Nótese que el signo ha de ser positivo, pues suponemos que es un cuadrado de un racional: $m = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$.

Ahora bien, como m no es un cuadrado en $\mathbb{Z}$, debe tener algún exponente impar, $\exists i / e_i$ *es impar*.

Reordenando, podemos hacer que sea e_1.

Por otro lado, a^2, b^2 tienen todos los exponentes de su factorización pares, pues son cuadrados.

Ahora bien, teniendo en cuenta la igualdad del comienzo, mb^2 debe tener todos los exponentes de su factorización pares (es igual a a^2). Pero los exponentes de la factorización de mb^2 son:

$$\begin{cases} e_i + b_i & \forall i / \forall i / p_i \in Fact(n), p_i \in Fact(b) \\ e_i & \forall i / p_i \in Fact(n), p_i \notin Fact(b) \\ b_i & \forall i / p_i \notin Fact(n), p_i \in Fact(b) \end{cases}$$

Si $p_1 \in Fact(b)$, entonces $e_1 + b_1$ es impar, esto es una contradiccón.

Pero si $p_1 \notin Fact(b)$, entonces e_i sigue siendo impar, lo que sigue suponiendo una contradicción.

En cualquier caso, vemos como mb^2 tiene algún exponente impar y m no puede ser cuadrado en $\mathbb{Q}$.

|———|

El tercer ejercicio es sencillo, basta pensar en un anillo que no sea conmutativo y encontraremos un ejemplo de esto fácilmente. Se puede comprobar rápidamente, por ejemplo, que en el anillo $\mathcal{M}_2(\mathbb{R})$ de las matrices reales 2×2, tomando

$$a = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} b = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

obtenemos el contraejemplo requerido.

1.3 Subanillos

El primer ejercicio de este apartado es sencillo, basta comprobar las propiedades de subanillo en cada caso.

1.3.2 Decimos que un entero d es libre de cuadrados si p^2 no divide a d para ningún número primo p (en particular 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. ¿Ocurre lo mismo si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$?

Si m es libre de cuadrados, es claro.

Si no es así, entonces $\exists p_1$ primo tal que $p_1^2 \mid m$ y consideramos $d_1 = \frac{m}{p_1^2}$. Entonces:

- Dado $a+b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, tenemos que $a+b\sqrt{m} = a+b\sqrt{d \cdot p_1^2} = a+bp_1\sqrt{d} \implies a+b\sqrt{m} \in \mathbb{Q}[\sqrt{d}]$
- Dado $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, tenemos que $a + b\sqrt{d} = a + b\sqrt{\frac{m}{p_1^2}} = a + \frac{b}{p_1}\sqrt{m} \implies a + b\sqrt{d} \in \mathbb{Q}[\sqrt{m}]$

Y tendríamos el resultado si d fuese libre de cuadrados. De no ser así, iteramos el proceso y, es obvio que llegaría un momento en que encontraríamos $d_n \geq 1$ libre de cuadrados, de forma que

$$m = p_1^2 p_2^2 \cdot ... \cdot p_n^2 \cdot d_n$$

La igualdad de ambos conjuntos se demuestra reproduciendo las cuentas anteriores pero con todos estos primos en lugar de solo con uno.

Respecto a la última pregunta, vemos que $\mathbb{Z}[\sqrt{m}] \subset \mathbb{Z}[\sqrt{d}]$, pero la otra implicación no se cumple, ya que $\frac{b}{p_1 \cdot ... \cdot p_n}$ puede no ser entero.

1.4 Homomorfismos de anillos

1.4.2 Demostrar que la composición de dos homomorfismos de anillos es un homomorfismo de anillos

- $(g \circ f)(1) = g(f(1)) \overset{f\ hom}{=} g(1) \overset{g\ hom}{=} 1$
- $(g \circ f)(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y)$
- $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$

Y vemos como la composición es un homomorfismo.

1.4.3 Demostrar que la relación "ser isomorfos" en la clase de los anillos es de equivalencia

- Reflexividad
$$id:\ X \to X \quad es\ homomorfismo\ biyectivo \implies X \cong X$$
- Transitividad
$$\begin{cases} X \cong Y & \implies X \overset{g\ isom}{\to} Y \\ Y \cong Z & \implies Y \overset{f\ isom}{\to} Z \end{cases} \implies X \overset{f\circ g\ isom}{\to} Z \implies X \cong Z$$
- Simetría
$$X \cong Y \implies X \overset{g\ isom}{\to} Y \implies Y \overset{g^{-1}\ isom}{\to} X \implies Y \cong X$$

1.4.4 Sean $f_1 : A \to B_1$, $f_2 : A \to B_2$ dos homomorfismos de anillos. Demostrar que la aplicación

$$f_1 \times f_2 : A \to B_1 \times B_2$$
$$(f_1 \times f_2)(a) = (f_1(a), f_2(a))$$

es el único homomorfismo de anillos tal que $\pi_{B_i} \circ (f_1 \times f_2) = f_i,\ i = 1, 2$. Demostrar que $(f_1, f_2) \mapsto f_1 \times f_2$ define una biyección $Hom(A, B_1) \times Hom(A, B_2) \to Hom(A, B_1 \times B_2)$.

Que es un homomorfismo es simplemente comprobar las tres propiedades, lo que se hace fácilmente.

Para ver la unicidad, supongamos que existe otro homomorfismo, g, tal que $\pi_{B_i} \circ g = f_i$. Entonces

$$(\pi_{B_i} \circ g)(a) = f_i(a) \iff \pi_{B_i}(g(a)) = f_i(a) \iff \pi_{B_i}(g(a)_1, g(a)_2) = f_i(a) \iff$$
$$\iff g(a)_i = f_i(a)$$

Esto sucede $\forall a \in A \implies g_i = f_i \implies g = f_1 \times f_2$, y vemos como esta es la única forma que puede tener esta aplicación.

Veamos la última afirmación:

- Inyectividad
$$f_1 \times f_2 = g_1 \times g_2 \implies (f_1(x), f_2(x)) = (g_1(x), g_2(x)), \forall x \implies \begin{cases} f_1(x) = g_1(x) \\ f_2(x) = g_2(x) \end{cases} \quad \forall x \implies (f_1, f_2) = (g_1, g_2)$$
- Sobreyectividad: Dado $g \in Hom(A, B_1 \times B_2)$, entonces
$$(\pi_1 \circ g, \pi_2 \circ g) \in Hom(A, B_1) \times Hom(A, B_2)$$
y la imagen por la aplicación del enunciado es g.

1.4.5 Sea $f : A \to B$ un homomorfismo de anillos y sea $b \in B$.

1. **Demostrar que la aplicación $f_b : A[X] \to B$ dada por $f_b(a_0 + a_1X + ... + a_nX^n) = f(a_0) + f(a_1)b + ... + f(a_n)b^n$ es el único homomorfismo de anillos $A[X] \to B$ que extiende f y asocia X con b.**

   $f_b(a_0 + ... + a_nX^n + c_0 + ... + c_mX^m) = f(a_0) + ... + f(a_n)b^n + f(c_0) + ... + f(c_m)b^m = f_b(a_0 + ... + a_nX^n) + f_b(c_0 + ... + c_mX^m)$

   $f_b(A \cdot C) = f_b(\sum_{i=0}^{n+m}(\prod_{j=0}^{i} a_jc_{i-j})X^i = \sum_{i=0}^{n+m} f(\prod_{j=0}^{i} a_jc_{i-j})b^i = \sum_{i=0}^{n+m}(\prod_{j=0}^{i} f(a_jc_{i-j}))b^i = \sum_{i=0}^{n+m}(\prod_{j=0}^{i} f(a_j)f(c_{i-j}))b^i =$

   $= (\sum_{i=0}^{n} f(a_i)b^i)(\sum_{i=0}^{m} f(c_i)b^i) = f_b(A)f_b(C)$

   $f_b(1) = f(1) = 1$

   Y vemos como efectivamente es un homomorfismo.

   Supongamos ahora que g es otro homomorfismo que extiende f y asocia X con b. Entonces, en particular, coinciden en los polinomios de grado 0, pero entonces son iguales, y esta es la única forma que pueden tener.

2. **Demostrar que la siguiente aplicación es biyectiva**

$$\begin{array}{ccc} \boldsymbol{Hom(A,B) \times B} & \to & \boldsymbol{Hom(A[X],B)} \\ \boldsymbol{(f,b)} & \mapsto & \boldsymbol{f_b} \end{array}$$

   Inyectividad:

$$f_b = g_a \implies f_b(C) = g_a(C), \forall C \in A[X] \implies f(c_0) + ... + f(c_n)b^n = g(c_0) + ... + g(c_n)a^n$$

   Humm... no veo claro cómo seguir a partir de aquí.

1.5 Ideales y anillos cociente

1.5.2 Sea I un ideal de $\mathbb{Z}$ distinto de 0. Demostrar que I tiene un entero positivo y si a es el menor entero positivo de I entonces $I = (a)$. Concluir que todos los ideales del anillo $\mathbb{Z}$ son principales. Demostrar además que si n, m son dos números enteros entonces $(n) \subset (m)$ si y solo si $m|n$.

Como $I \neq 0$, entonces $\exists b \neq 0 \in \mathbb{Z}/b \in I$.

- Si $b > 0$, ya lo tenemos.
- Si $b < 0 \overset{I \text{ ideal}}{\implies} 0 < b^2 \in I$, y lo tenemos.

Sea ahora $a = \min\{x \in I : x > 0\}$, ¿tendremos $I = (a)$?

$'\supseteq'$ Si $b = k \cdot a$, entonces $b \in I$, por ser I ideal.

$'\subseteq'$ Supongamos que $I \nsubseteq (a) \iff \exists b \in I / b \notin (a)$. Podemos poner $b = c \cdot a + r, \quad 0 < r < a$.

Entonces, tenemos que $c \cdot a \in I$, y por tanto $r = b - c \cdot a \in I$.# Pero esto es una contradicción, ya que $0 < r < \min\{x \in \mathbb{Z} : x > 0\}$. Por lo que ha de ser $I \subseteq (a)$.

Para la última afirmación:

$' \implies ' (n) \subset (m) \implies \forall k, \exists l / kn = lm$, en concreto, para $k = 1$, se tiene que $\exists l / n = lm \implies m|n$

$' \impliedby ' m|n \implies n = lm \implies kn = klm$

Así, dado un múltiplo de n, lo podemos escribir como múltiplo de m. Esto quiere decir que $(n) \subset (m)$.

1.5.3 Si n es un entero positivo, demostrar que los ideales de $\mathbb{Z}_n$ son precisamente los de la forma $m\mathbb{Z}_n$, donde $0 < m|n$, y además $m\mathbb{Z}_n \subset m'\mathbb{Z}_n \iff m'|m$.

Por el teorema de correspondencia, los ideales de $\mathbb{Z}_n = \frac{\mathbb{Z}}{(n)}$, por el teorema de correspondencia, son los ideales de $\mathbb{Z}$ que contienen a (n), modulo (n).

Por el ejercicio anterior, $(n) \subset (m) \iff m|n$. Además, este mismo ejercicio nos dice que podemos tomar $m > 0$.

Entonces, los ideales de $\mathbb{Z}_n$ son $\frac{(m)}{(n)} / m|n$, pero $\frac{(m)}{(n)} = m\mathbb{Z}_n$.

Veamos la última afirmación

$$m'|m \iff (m) \subset (m') \iff \frac{(m)}{(n)} \subset \frac{(m')}{(n)} \iff m\mathbb{Z}_n = m'\mathbb{Z}_n$$

1.5.4 Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que si I es un ideal de B, entonces $f^{-1}(I)$ es un ideal de A. Demostrar que si I es un ideal de A y f es suprayectiva, entonces $f(I)$ es un ideal de B. Dar un ejemplo de un homomorfismo de anillos $f : A \to B$ en el que la imagen por f de un ideal de A no sea ideal de B.

Veamos que $f^{-1}(I)$ es un ideal de A.

- $I \neq \emptyset \implies f^{-1}(I) \neq \emptyset$, esto se debe a que $0 \in I$ y $f^{-1}(0) = 0 \in f^{-1}(I)$
- $x, y \in f^{-1}(I) \implies f(x), f(y) \in I \implies f(x) + f(y) \in I \implies f(x + y) \in I \implies x + y \in f^{-1}(I)$
- $x \in f^{-1}(I), a \in A \implies f(x) \in I, f(a) \in B \implies f(a)f(x) \in I \implies f(ax) \in I \implies ax \in f^{-1}(I)$

Y tenemos el resultado.

Prosigamos con la siguiente afirmación:

- $I \neq \emptyset \implies f(I) \neq \emptyset$
- $x, y \in f(I) \implies f^{-1}(x), f^{-1}(y) \in I \implies f^{-1}(x) + f^{-1}(y) \in I \implies f\left(f^{-1}(x) + f^{-1}(y)\right) \in f(I) \implies f\left(f^{-1}(x)\right) + f\left(f^{-1}(y)\right) \in f(I) \implies x + y \in f(I)$
- $x \in f(I), b \in B \implies f^{-1}(x) \in I$ *y como f es suprayectiva* $\exists a \in A / f(a) = b \implies af^{-1}(x) \in I \implies f\left(af^{-1}(x)\right) \in f(I) \implies f(a)f\left(f^{-1}(x)\right) \in f(I) \implies bx \in f(I)$

Y tenemos el resultado.

El ejemplo pedido al final puede ser

$$\begin{array}{ccc} f:\mathbb{Z} & \to & \mathbb{Q} \\ n & \mapsto & n \end{array}$$

Claramente es un homomorfismo, pero $f(\mathbb{Z}) = \mathbb{Z} \not\trianglelefteq \mathbb{Q}$.

1.5.5 Sean A, B dos anilos. Describir los ideales de $A \times B$ en función de los ideales de A y de B. Determinar todos los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

Los ideales de $A \times B$ son de la forma $I \times J / I \trianglelefteq A,\ J \trianglelefteq B$. O sea

$$Ideales(A \times B) = \{I \times J / I \trianglelefteq A,\ J \trianglelefteq B\}$$

$'\supseteq'$ Es muy obvio, ya que tenemos que comprobar que son ideales coordenada a coordenada.

$'\subseteq'$ Sea $K \trianglelefteq A \times B$, podemos definir

$$K_1 = K \cap (A \times 0) = I \times 0,\ \textit{donde } I \trianglelefteq A$$

$$K_2 = K \cap (0 \times B) = 0 \times J,\ \textit{donde } J \trianglelefteq B$$

Y $K = K_1 \cup K_2 = I \times J$.

Por tanto, para ver cuáles son los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, debemos ver los ideales de cada uno. Por el ejercicio 1.5.3, tenemos que los ideales de $\mathbb{Z}_{12}$ son de la forma $m\mathbb{Z}_{12},\ m|12$ y los de $\mathbb{Z}_{18}$ son $k\mathbb{Z}_{18},\ k|18$.

Es decir, los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ son

$$\{m\mathbb{Z}_{12} \times k\mathbb{Z}_{18} / m \in \{0,1,2,3,4,6\},\ k \in \{0,1,2,3,6,9\}\}$$

1.5.6 Demostrar que si p, q son dos primos distintos entonces no hay ningún homomorfismo de $\mathbb{Z}_p$ a $\mathbb{Z}_q$ ni de $\mathbb{Z}_q$ a $\mathbb{Z}_p$. ¿Cuántos homomorfismos hay de $\mathbb{Z}_4$ a $\mathbb{Z}_2$? ¿Y de $\mathbb{Z}_2$ a $\mathbb{Z}_4$?

Las características son, respectivamente, p y q.

Entonces, si $f : \mathbb{Z}_p \to \mathbb{Z}_q$ es un homomorfismo, sabemos que $f(1) = 1$ y que f conserva inversos, también sabemos que $nf(a) = f(na)$.

Así, tenemos que $f(q) = f(q \cdot 1) = qf(1) = q = 0$, pero q es invertible en $\mathbb{Z}_p$, pues p es primo, por lo que $\mathbb{Z}_p$ es cuerpo y $p \nmid q \implies q \in \mathbb{Z}_p^*$, pero $f(q) = 0 \notin \mathbb{Z}_q^*$. Por tanto, no puede f ser un homomorfismo.

Al contrario se hace exactamente igual.

De $\mathbb{Z}_4$ *a* $\mathbb{Z}_2$, los invertibles deben ir al 1 inevitablemente, y el 0 debe ir al 0.

Es decir, ha de ser $f(3) = f(-1) = f(1) = 1$.

El 2, en principio, podría ir tanto al 0 como al 1, pero tenemos que $1 = f(3) = f(2+1) = f(2) + f(1) = f(2) + 1$, de donde ha de ser $f(2) = 0$.

Por tanto, solo hay un homomorfismo.

De $\mathbb{Z}_2$ *a* $\mathbb{Z}_4$, el 1 debe ir al 1, y el 0 al 0. Pero $0 = f(0) = f(1+1) = f(1) + f(1) = 2\#$

Es decir, no existe ningún homomorfismo entre estos dos anillos.

1.5.7 Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo de anillos y todos los ideales del anillo A son principales, entonces todos los ideales de B son principales.

Sea J un ideal de B, entonces, por 1.5.4, tenemos que $f^{-1}(J)$ es un ideal en A, pero, entonces $f^{-1}(J) = (a)$ es un ideal principal. Es decir, $f^{-1}(J) = (a) = \{ka : k \in A\}$. Entonces, $J = f((a)) = \{f(ka) : k \in A\} = \{f(k)f(a) : k \in A\} \overset{f\ supra}{=} \{mf(a) : m \in B\} = (f(a)) = (b)$.

Así, vemos como todo ideal de B es principal.

1.5.8 Sea $f : A \to B$ un homomorfismo suprayectivo de anillos. Demostrar que existe una correspondencia biunívoca, que conserva la inclusión, entre el conjunto de los ideales de B y los ideales de A que contienen a $Kerf$.

0 es un ideal en $B \implies Kerf$ es un ideal en A, por el ejercicio 1.5.4.

Todos los ideales de B contienen al 0, por lo que todos los ideales de la forma $f^{-1}(J)$, siendo J un ideal de B, contienen a $Kerf$.

Es decir, si $J \trianglelefteq B \implies Kerf \subset f^{-1}(J) \trianglelefteq A$ (!)

Además, si $Kerf \subset I \trianglelefteq A \overset{f \ supra}{\implies} f(I) \trianglelefteq B$

Es decir, que la correspondencia será f vista como función de conjunto

$$\begin{array}{ccc} \overline{f} : \{I \trianglelefteq A / Kerf \subset I\} & \to & \{J \trianglelefteq B\} \\ I & \mapsto & f(I) \end{array}$$

Por (!) tenemos que es sobreyectiva.

Supongamos que no es inyectiva, entonces existen $f(I) = \overline{f}(I) = \overline{f}(K) = f(K)$ con $I \neq K$, o sea, existen $i \in I - K, k \in K - I$ tales que $f(i) = f(k)$. Pero, entonces $f(i) - f(k) = 0 \implies f(i-k) = 0 \implies i - k \in Kerf \implies i - k \in I \implies i - k - i = -k \in I \implies k \in I\#$ Esto es una contradiccón, pues se supone que $k \notin I$.

Así, vemos que es biunívoca (por tanto, conserva la inclusión).

1.5.9 Sea X un conjunto y $*$ una operación en X. Una congruencia en X con respecto a $*$ es una relación de equivalencia $\sim$en X que verifique la siguiente condición para todo $a, a', b, b' \in X$:

$$a \sim a' \quad y \quad b \sim b' \implies a * b \sim a' * b'$$

En tal caso definimos la siguiente operación $*$ en el conjunto cociente $\frac{X}{\sim}$, donde $\overline{a}$ representa la clase de equivalencia en $\frac{X}{\sim}$ que contiene a a:

$$\overline{a} * \overline{b} = \overline{a * b}$$

Demostrar las siguientes propiedades para $\sim$ una congruencia en X con respecto a $*$:

(a) Si $(X, *)$ es un semigrupo entonces $(\frac{X}{\sim}, *)$ es un semigrupo y si además $(X, *)$ es un monoide o un grupo entonces $(\frac{X}{\sim}, *)$ también lo es.

Semigrupo

$$(\overline{a} * \overline{b}) * \overline{c} = \overline{a * b} * \overline{c} = \overline{\overline{a * b} * c}$$

$$\overline{a} * (\overline{b} * \overline{c}) = \overline{a} * \overline{b * c} = \overline{a * \overline{b * c}}$$

¿Son estas dos expresiones iguales?

Lo serán si, y solo si, $\overline{a * b} * c \sim a * \overline{b * c}$.

Pero $\overline{a * b} * c \sim (a * b) * c = a * (b * c) \sim a * \overline{b * c}$, como queríamos.

Las otras dos comprobaciones son también sencillas.

(b) Si A es un anillo y $\sim$ es una relación de equivalencia en A entonces $\sim$ es una congruencia respecto de la suma y el producto de A si y solo si el conjunto $I = \{a \in A / a \sim 0\}$ es un ideal de A.

Este ejercicio lo vimos con Álvaro, la implicación a la izquierda es falsa.

$' \implies '$ Dados $a, b \in I \implies a \sim 0, b \sim 0 \implies a + b \sim 0 + 0 = 0 \implies a + b \in I$

Dados $a \in I, x \in A \implies a \sim 0, x \sim x \implies ax \sim 0x = 0 \implies ax \in I$

$I \neq \emptyset$, porque $0 \sim 0$.

$'\Longleftarrow'$ Es falso. Contraejemplo:

$$a \sim b \iff \begin{cases} a, b \in I \\ a, b \notin I \end{cases}$$

En $\mathbb{Z}$, $I = (3)$. Tenemos que $2 \sim 2, 1 \sim 2$ pero $2 + 1 \nsim 2 + 2$

1.6 Operaciones con ideales

El primero es demostrar una proposición, y el segundo la verdad es que es bastante aburrido. Voy a hacer un par de apartados.

1.6.2 Si I, J, K son ideales de un anillo A, demostrar que:

(a) $IJ \subset I \cap J$

$$IJ = \{x_1y_1 + ... + x_ny_n / x_1, ..., x_n \in I, y_1, ..., y_n \in J\}$$

$$\begin{cases} x_i \in I \\ y_i \in J \end{cases} \forall i \implies \begin{cases} x_iy_i \in I \\ x_iy_i \in J \end{cases} \forall i \implies x_iy_i \in I \cap J, \forall i \implies \sum_i x_iy_i \in I \cap J$$

Y vemos como $IJ \subset I \cap J$

(d) $I(J + K) = IJ + IK$

$$a \in I(J+K) \iff a = \sum_i x_ib_i,\ x_i \in I,\ b_i \in J+K \iff a = \sum_i x_i(y_i+z_i),\ x_i \in I, y_i \in J, z_i \in K \iff$$

$$\iff a = \sum_i x_iy_i + \sum_i x_iz_i,\ x_i \in I, y_i \in J, z_i \in K \iff a \in IJ + IK$$

1.7 Los teoremas de isomorfía y chino de los restos

1.7.1 Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \to \mathbb{R}$ dado por $P(x) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \to \mathbb{C}$, dado por $P(X) \mapsto P(i)$?

El primer teorema de isomorfía muestra que

$$\frac{\mathbb{R}[X]}{Ker f} \simeq Im f$$

Entonces, podemos hacer varias observaciones:

1. Aplicando el homomorfismo a los polinomios constantes podemos ver que $Im f = \mathbb{R}$
2. $Ker f$ son todos aquellos polinomios que tienen a a como raíz

Entonces, lo que deducimos es el conjunto de los polinomios que no tiene a a como raíz es isomorfo a $\mathbb{R}$.

En el segundo caso, vamos a hacer observaciones similares:

1. Aplicando el homomorfismo a los polinomios de la forma $a + bX$, vemos que $Im f = \mathbb{C}$.
2. $Ker f$ son todos aquellos polinomios que tienen a i como raíz

Así, tenemos que el conjunto de los polinomios que no tienen a i como raíz es isomorfo a $\mathbb{C}$.

1.7.2 Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si $I_1, ..., I_n$son ideales de un anillo A tales que la aplicación $f : A \to \prod_{i=1}^{n} \frac{A}{I_i}$, dada por $f(a) = (a + I_1, ..., a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1), \forall i \neq j$.

¿$1 \in I_i + I_j$?

Como f es sobreyectiva, entonces $\exists a \in A / f(a) = (0 + I_1, ..., 1 + I_i, ..., 0 + I_j, ..., 0 + I_n)$

Esto quiere decir que

$$\begin{cases} 1 - a \in I_i \\ a \in I_j \end{cases} \implies 1 = (1 - a) + a \in I_i + I_j$$

Y tenemos el resultado.