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, por el teorema de Ruffini, los múltiplos de $(X - a)$

Entonces, lo que deducimos es que $\frac{\mathbb{R}[X]}{(X-a)} \simeq \mathbb{R}$.

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

Ahora bien, aquí no podemos usar el teorema de Ruffini tan alegremente porque $i \notin \mathbb{R}$. Consideremos los polinomios con coeficientes complejos. Ahor notamos que si i es raíz de un polinomio con coeficientes reales, entonces $-i$ también lo es, pues es su conjugado y la conjugación es un automorfismo en $\mathbb{C}$ que deja fijos los elementos de $\mathbb{R}$.

Así, si P está en el núcleo, visto sobre $\mathbb{C}$, entonces, aplicando, ahora sí, Ruffini, tenemos que es disivible por $(X-i)$ y $(X+i)$. Por tanto, P es divisible por $(X-i)(X+i) = X^2+1$. En particular, si P tiene coeficientes reales, también lo divide. O sea, $P \in Kerf \implies X^2+1|P$

Recíprocamente, si $X^2+1|P$, entonces i es raíz de $P \implies P \in Kerf$

Por tanto $Kerf = (X^2+1)$.

Y así, por el primer teorema de isomorfía

$$\frac{\mathbb{R}[X]}{(X^2+1)} \simeq \mathbb{C}$$

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.

2 Divisibilidad en dominios

2.1 Cuerpos y dominios; ideales maximales y primos

2.1.1 Sean a, b dos elementos de un anillo. Demostrar que ab es un divisor de cero si y solo si a *ó* b es un divisor de cero.

Recordemos que los divisores de cero son los elementos no regulares.

' $\Longrightarrow$ ' ab no es regular si $\exists c \neq d / abc = abd$. Si a es regular, entonces deducimos que $bc = bd$, por lo que b no puede ser regular o tendríamos $c = d$.

Si b es regular, tenemos $ac = ad$ y a no puede ser regular.

' $\Longleftarrow$ ' Supongamos, sin perder generalidad, pues suponemos los anillos conmutativos, que a no es regular.

Entonces existen $c \neq d / ac = ad \implies acb = adb \implies abc = abd$.

De esta manera, $\exists c \neq d / abc = abd$, por lo que ab no es regular.

2.1.2 Sea A un anillo finito. Demostrar que todo elemento de A es o divisor de cero o unidad. Deducir que todo dominio finito es un cuerpo.

Sea $a \in A$. Supongamos que no es unidad.

O sea que $a \cdot b \neq 1, \forall b \in A$.

Consideremos

$$\begin{array}{ccc} f : A & \to & A \\ x & \mapsto & ax \end{array}$$

Esta aplicación no es sobreyectiva. Pero como A es finito, f es sobreyectiva si y solo si es inyectiva. Como no es sobre, no es inyectiva. Por lo que existen $x \neq y / f(x) = f(y) \implies ax = ay$. O sea, que si a no es unidad, entonces no es regular (es divisor de cero).

Si a no es divisor de 0, entonces $\forall c \neq b \in A \implies ac \neq ab$. Por lo que la aplicación f será inyectiva, y será sobreyectiva. Al ser sobreyectiva, $\exists b \in A / ab = f(a) = 1$. Y a es unidad.

Para la última afirmación, si A es un dominio, entonces todos los elementos no nulos son regulares, por lo anterior, al no ser divisores de cero deben ser unidades, por tanto A es un cuerpo.

2.1.3 Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que:

(1) Si p es un ideal primo de B, entonces $f^{-1}(p)$ es un ideal primo de A

p primo $\iff \forall a', b' \in B,\ a'b' \in p \implies a' \in B$ *ó* $b' \in B$

Así, sean $a, b \in A / ab \in f^{-1}(p) \implies f(ab) \in p \implies f(a)f(b) \in p \implies f(a) \in p$ *ó* $f(b) \in p \implies a \in f^{-1}(p)$ *ó* $b \in f^{-1}(p)$

Así, $f^{-1}(p)$ es un ideal por un ejercicio del capítulo 1 y es primo como acabamos de ver.

(2) En general, no se verifica el resultado análogo para ideales maximales

Consideremos

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

tenemos que $p = (0)$ es maximal en $\mathbb{Q}$, pero $f^{-1}(p) = (0)$ no es maximal en $\mathbb{Z}$.

2.1.4 Sea I un ideal propio de un anillo A. Demostrar que las biyecciones del teorema de correspondencia llevan ideales maximales (resp. primos) de A que contienen a I a ideales maximales (resp. primos) de $\frac{A}{I}$, y viceversa.

El teorema afirma que si $J \subset K$ son ideales de A que contienen a I, entonces $\frac{J}{I} \subset \frac{K}{I}$.

También afirma que si $X \subset Y$ son ideales de $\frac{A}{I}$ entonces $\pi^{-1}(X) \subset \pi^{-1}(Y)$.

Pero también demuestra que los ideales de $\frac{A}{I}$ son de la forma $\frac{J}{I}$ con $I \subset J \lhd A$.

Juntando estos resultados, obtenemos que $J \subset K$ ideales de A que contienen a I si y solo si $\frac{J}{I} \subset \frac{K}{I}$ son ideales de $\frac{A}{I}$.

Y lo pedido sobre maximales del ejercicio se deduce inmediatamente de este último resultado.

2.1.5 Demostrar que si D es un dominio su característica es 0 o un número primo.

D es un dominio si y solo si $a, b \in D$ son no nulos, entonces $ab \neq 0$.

Sea n la característica de D. Es decir,

$$n = \min_{n \in \mathbb{N}} \{n/n1 = 0\}$$

o cero si este mínimo no existe.

Si no es cero, entonces puede ser primo o no serlo.

Si no es primo, entonces puede expresarse como producto de primos. También podemos ponerlo como $n = ap$, donde p es primo y a es el producto del resto de primos de la factorización de n. Nótese que $a, p < n$.

De esta forma, tenemos que $n1 = 0 \iff ap1 = 0 \iff a1 \cdot p1 = 0$.

Entonces, encontramos $a1, p1 \in D$ no nulos (si alguno fuera nulo, la característica no sería n), tales que $a1 \cdot p1 = 0\#$ Esto es una contradición, pues D es un dominio.

Así, vemos que la característica, si no es cero, debe ser un número primo.

2.1.6 Determinar los ideales de $\mathbb{Z}_n$. ¿Cuáles son primos y cuales maximales?

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

Pero $(n) \subset (m) \iff m|n$. Por tanto, los ideales son $m\mathbb{Z}_n$, con $m|n$.

Por el ejercicio 2.1.4, los primos y maximales de $\mathbb{Z}_n$ son los primos y maximales de $\mathbb{Z}$ que contienen a (n). Es decir, los de la forma $p\mathbb{Z}_n / p|n,\ p\ primo$

El 7 es muy pesado

2.1.8 Demostrar que si P es un ideal primo de A, entonces $P[X]$ es un ideal primo de $A[X]$ y

$$p + (X) = \{a_0 + ... + a_n X^n : a_0 \in P,\ a_1, ..., a_n \in A\}$$

es un ideal maximal de $A[X]$. ¿Puede $P[X]$ ser maximal de $A[X]$?

Por la proposición 2.6, $P[X]$ será primo si y solo si $\frac{A[X]}{P[X]}$ es un dominio.

¿Es $\frac{A[X]}{P[X]} \cong \left(\frac{A}{P}\right)[X]$?

Sea

$$\begin{array}{ccc} f : A[X] & \to & \left(\frac{A}{P}\right)[X] \\ \sum a_i X^i & \mapsto & \sum (a_i + P) X^i \end{array}$$

f es un homomorfismo suprayectivo con núcleo $P[X]$.

Así, por el primer teorema de isomorfía

$$\frac{A[X]}{P[X]} \cong \left(\frac{A}{P}\right)[X]$$

Ahora bien, como P es ideal primo de A, entonces $\frac{A}{P}$ es un dominio, esto implica que $\left(\frac{A}{P}\right)[X]$ es dominio. Pero entonces $\frac{A[X]}{P[X]}$ es dominio y así $P[X]$ es ideal primo de $A[X]$.

¿Puede $P[X]$ ser maximal de $A[X]$?

Para eso, $\frac{A[X]}{P[X]} \cong \left(\frac{A}{P}\right)[X]$ debería ser un cuerpo, pero esto no puede ser, ya que un anillo de polinomios no puede ser un cuerpo ($X^{-1} \notin A[X]$).

¿$p+(X)$ maximal?

No necesariamente... pero sí primo.

Sea

$$\begin{array}{ccc} h : A[X] & \to & \frac{A}{P} \\ a_0 + ... + a_n x^n & \mapsto & a_o + P \end{array}$$

h es un homomorfismo suprayectivo con núcleo $p+(X)$. Por el 1º trm isom:

$$\frac{A[X]}{p+(X)} \cong \frac{A}{P}$$

que es un dominio, por lo que $p+(X)$ es un ideal primo.

2.1.9 Demostrar que las siguientes condiciones son equivalentes para un anillo A:

(1) A tiene un único ideal maximal

(2) A tiene un ideal propio I que contiene todos los elementos no invertibles de A

(3) El conjunto de los elementos no invertibles de A es un ideal

(4) Para todo $a, b \in A$, $a+b \in A^* \implies a \in A^*$ ó $b \in A^*$

Un anillo que satisface estas condiciones se denomina local.

'(1) $\implies$ (2)' Sea I el ideal maximal de A. Supongamos que existe algún elemento no invertible, $x \notin I$.

Entonces $(x) \triangleleft A$ propio $\implies (x) \subset I \implies x \in I\#$ Contradicción.

Así, A tiene un ideal que contiene a todos los elementos no invertibles, y es I.

'(2) $\implies$ (3)' Si I contuviera algún invertible, entonces contendría al 1 y, por tanto, sería el total. Pero I es propio. Por tanto, I contiene a todos los no invertibles y no contiene a ningún invertible. Es decir, el conjunto de los elementos no invertibles es un ideal.

'(3) $\implies$ (4)' Por contrarrecíproco,

$$a \notin A^* \ y \ b \notin A^* \overset{A \setminus A^* \ ideal}{\implies} a+b \notin A^*$$

'(4) $\implies$ (1)' Sea $I = A \setminus A^*$. ¿I ideal?

Sean $x, y \in I \implies x, y$ no invertibles $\implies x+y$ no invertible $\implies x+y \in I$

Dado $x \in I$, $a \in A \implies ax \in I$

Por lo que I es un ideal.

¿Es maximal?

Sea J un ideal propio.

Dado $x \in J$, si x no es invertible, entonces $x \in I$.

Si x es invertible, entonces $1 \in J \implies J = A\#$ Esto no puede ocurrir, pues J es propio.

Así, $J \subset I, \forall J$ propio.

2.1.10 Demotrar que los siguientes anillos son locales (verifica las propiedades del ejercicio anterior)

(1) $\mathbb{Z}_{p^n}$, donde p es primo y $n \geq 0$

$\underline{n = 0}$ Es $\{0\}$, este caso no es cierto.

$\overline{n = 1}$ Es un cuerpo, por lo que se verifica (4) trivialmente.

$n > 1$ Los ideales propios son los $p^i\mathbb{Z}_{p^n}$, $i = 1, ..., n-1$. Pero, para todo $i > 1$, se tiene que $p|p^i$, luego $p^i\mathbb{Z}_{p^n} \subset p\mathbb{Z}_{p^n}$. Por lo que hay un único ideal maximal y se verifica (1).

2.1.11 Sea A un anillo cuya característica es un número primo p. Demostrar que la aplicación $x \mapsto x^{p^n}$es un endomorfismo de A para todo $n \in \mathbb{Z}^{\geq 0}$.

- $a, b \in A \implies p(a+b) = (a+b)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} a^{p^n} b^{p^n - i}$

  Pero este sumatorio tiene al menos un factor p en todos los sumandos excepto el primero y el último (p^n tiene $n-1$ divisores menores que él mismo, por ser p primo). Entonces

  $$p(a+b) = a^{p^n} + b^{p^n} = p(a) + p(b)$$

- $a, b \in A \implies p(ab) = (ab)^{p^n} = a^{p^n} b^{p^n} = p(a)p(b)$
- $p(1) = 1^{p^n} = 1$

Y la aplicación es un homomorfismo.

2.1.12 Demostrar que si K es un cuerpo finito con un subcuerpo F, entonces el cardinal de K es una potencia del cardinal de F.

Consideremos K espacio vectorial sobre F.

Sean $a_1, a_2, a \in F$ *y* $v_1, v_2, v \in K$. Entonces

$$a(v_1 + v_2) = av_1 + av_2 \quad (a_1 + a_2)v = a_1 v + a_2 v \quad a_1(a_2 v) = (a_1 a_2)v \quad 1 \cdot v = v$$

Por lo que efectivamente es un EV.

Sea $n = dim_F K$.

Entonces

$$_F K \simeq F^n \implies |K| = |F|^n$$

Deducir que:

(1) El cardinal de cualquier cuerpo finito es una potencia de un número primo

Sea $A = subanillo\ primo\ de\ K = \{n1_k / n \in \mathbb{Z}\}$.

$$|A| = cararterística(K) = p \implies A \simeq \mathbb{Z}_p$$

$$|K| = potencia\ de\ |A| = potencia\ de\ p$$

(2) Si K es un cuerpo finito con un subcuerpo F, entonces existen un número primo p y enteros positvios n, m tales que $n|m$, $|F| = p^n$ y $|K| = p^m$.

$F\ subcuerpo \implies F\ cuerpo\ finito \implies |F| = p^n \implies |K| = |F|^l = (p^n)^l = p^{nl} = p^m$

2.1.13 Demostrar que si K es un cuerpo finito entonces 1 y -1 son los únicos elementos de K cuyo cuadrado es 1. Usar esto para demostrar que el producto de todos los elementos no nulos de K es -1 y deducir el teorema de Wilson: Si p es un número primo entonces $(p-1)! \equiv -1 \mod p$. Demostrar también el recíproco del teorema de Wilson: si n es un entero positivo que cumple $(n-1)! \equiv -1 \mod n$ entonces n es primo.

Sea $n = |K|$. Entonces en K hay n elementos, que además tienen que ser $0, 1, 1+1, ..., 1+1+...+1 = (n-1)1$.

Como K es un cuerpo de n elementos, es isomorfo a $\mathbb{Z}_n$, con n primo por el ejercicio anterior.

Lo demostramos para $\mathbb{Z}_n$.

Si $m^2 = 1 \iff m^2 - 1 = 0 \iff (m-1)(m+1) = 0 \iff m = \pm 1$.

Para verlo en K, consideramos el isomorfismo entre los dos cuerpos, f.

Si $x \in K$ es tal que $x^2 = 1 \implies f(x^2) = f(1) = 1 \implies f(x)^2 = 1 \implies f(x) = \pm 1$

Si $f(x) = 1 \implies x = 1$

Si $f(x) = -1 \implies f(-x) = -f(x) = 1 \implies -x = 1 \implies x = -1$.

Segunda afirmación

$\forall x \in K, \exists y / xy = 1$

Así, el producto de todos los elementos será

$$1 \cdot x_1 \cdot y_1 \cdot ... \cdot x_m \cdot y_m \cdot (-1) = 1 \cdot 1 \cdot ... \cdot 1 \cdot (-1) = -1$$

Teorema de Wilson

p *primo* $\implies \mathbb{Z}_p$ *cuerpo* $\implies (p-1)! = \prod_{x \in \mathbb{Z}_p} x = -1$

Recíproco de Wilson

Supongamos que n no es primo, entonces $\mathbb{Z}_n$ no es cuerpo, y entonces $\exists x \in \mathbb{Z}_n$ no nulo y no invertible.

Entonces

$$(n-1)! = \prod_{y \in \mathbb{Z}_n} y = x \cdot \prod_{y \in \mathbb{Z}_n \setminus \{x\}} y = \textit{...sacamos todos los no invertibles...} = x_1 \cdot ... \cdot x_m \cdot \prod_{y \in \mathbb{Z}_n^*} y =$$

$$= x_1 \cdot ... \cdot x_m \cdot (-1) = -x_1 \cdot ... \cdot x_n$$

Que no es -1, pues entonces sería invertible, y los x_i serían invertibles, pero sabemos que no es así.

Luego n ha de ser primo.

2.1.14 Sean I un ideal de un anillo y $p_1, ..., p_n$ ideales primos del mismo anillo. Demostrar que si $I \subset \cup_{i=1}^n p_i$ entonces $I \subset p_i$ para algún i.

2.2 Divisibilidad

2.2.2 Demostrar que si dos elementos de un anillo son asociados, entonces uno es irreducible (resp. primo) si y solo si lo es el otro.

Por la proposición 2.15:

a, b asociados sii $(a) = (b)$

a primo sii (a) ideal primo no nulo de D sii (b) ideal primo no nulo de D sii b primo

a irreducible sii (a) ideal maximal entre los ideales principales propios no nulos de D sii (b) ideal maximal entre los ideales principales propios no nulos de D sii b irreducible

2.2.3 Sea a un elemento diferente de cero de un anillo A. Demostrar que si todos los divisores de a son unidades o asociados de a entonces a es irreducible. Demostrar que el recíproco se verifica si A es dominio pero no en general.

a es irreducible sii (a) ideal maximal entre los ideales principales propios no nulos de D.

Supongamos que no es irreducible, entonces existe un ideal principal (b) tal que $(a) \subset (b)$ de forma propia. Esto quiere decir que $b|a$, pero la hipótesis nos dice que entonces b es unidad o asociado de a.

Si es unidad, entonces $(b) = D$, por lo que no es un ideal propio

Si es asociado de a, entonces $(a) = (b)$, por lo que no está contenido propiamente

En cualquier caso, llegamos a una contradiccón, por lo que a debe ser irreducible.

Si A es dominio se verifica el recíproco

¿$a \in A$ irreducible $\implies$ los divisores de a son unidades o asociados de a?

$a\ irred \iff (a = bc \implies b \in A^*\ o\ c \in A^*)$

A dominio implica a regular

Sea $x/x|a \implies a = cx \implies c \in A^*$ *ó* $x \in A^*$

Si $x \in A^* \implies x\ unidad$✓

Si $c \in A^* \implies x \notin A^*$, pues sería $a = cx \in A^*$, pero $a \notin A^*$(pues es irreducible). En un dominio, a, x son asociados sii $\exists c \in A^* : a = cx$✓

Si no es dominio no se verifica necesariamente

..

2.2.4 Demostrar las siguientes afirmaciones para elementos $a.b$ de un anillo

(1) $i)$ $a|b \iff ii)$ $a = mcd(a,b) \iff iii)$ $b = mcm(a,b)$. En particular, $1 = mcd(a,1)$, $mcd(a,0)$ y $0 = mcm(a,0)$

'$ii) \implies i)$' Obvio

'$i) \implies ii)$' Supongamos que $a \neq mcd(a,b) \implies \exists m/m|a\ y\ m|b\ y\ a|m$

Entonces a y m son asociados, lo que quiere decir que $a = mcd \iff m = mcd\#$ Contradicción, pues suponíamos que a no era el mcd.

Por tanto, $a = mcd(a,b)$.

'$iii) \implies i)$' Obvio

'$i) \implies iii)$' Supongamos $b \neq mcm(a,b) \implies \exists M/a|M\ y\ b|M\ y\ M|b \implies M, b\ asociados \implies (b\ mcm \iff m\ mcm)\#$

Para las demás afirmaciones:

$1|a \implies mcd(a,1) = 1\ y\ mcm(a,1) = a$

$a|0 \implies a = mcd(a,0)\ y\ mcm(a,0) = 0$

(2) Si a es irreducible entonces $mcd(a,b) = 1 \iff a \nmid b$

$$\text{' } \implies \text{' } mcd(a,b) = 1 \iff \begin{cases} 1|a \\ 1|b \\ \nexists c/1|c, c|a, c|b \end{cases}$$

$$\text{Supongamos que } a|b \implies \begin{cases} a|a \\ a|b \\ 1|a \end{cases} \quad \# \text{ Contradicción con lo anterior.}$$

$$\text{' } \impliedby \text{' Supongamos } mcd(a,b) = c \implies \begin{cases} c|a \\ c|b \\ 1|c \end{cases} \implies \begin{cases} a = dc \\ b = ec \\ c = c1 \end{cases}$$

Como a es irreducible, $a = dc \implies d \in A^*$ *ó* $c \in A^*$

Si $c \in A^* \implies 1, c\ asociados \implies mcd(a,b) = 1$✓

Si $d \in A^* \implies a, c$ *asociados* $\implies a|b\#$ Esto no puede ser.

2.2.5 Demostrar las siguientes propiedades para d, m dos elementos de un dominio D y S un subconjunto de D.

(1) $d = mcd(S)$ si y solo si (d) es mínimo entre los ideales principales que contienen a S. En particular, si (S) es un ideal principal entonces cualquier generador suyo es un máximo común divisor de S, y además existe una identidad de Bezout para S.

$' \implies '$ $d = mcd(S) \iff (d|x,\ \forall x \in S \text{ y } c|x, \forall x \in S \implies c|d)$

$d|x \implies (x) \subset (d), \forall x \in S \implies (S) \subset (d)$

Sea otro e tal que $(S) \subset (e) \implies e|x, \forall x \in S$

Si $(e) \subset (d) \implies d|e$

Por tanto, $e = mcd(S)\#$ Pues el mcd es d

$' \impliedby '$ $S \subset (d) \implies \forall x \in S, x \in (d) \implies d|x, \forall x \in S$

Supongamos $d \neq mcd(S) = e \implies \begin{cases} e|x, \forall x \in S \implies (x) \subset (e) \implies S \subset (e) \\ d|e \implies (e) \subset (d) \end{cases} \implies S \subset (e) \subset (d)\#$

Segunda afirmación

Si $(S) = k$, entonces (k) es mínimo entre los ideales principales que contienen a S. Por tanto $k = mcd(S)$.

Tercera afirmación

Por la proposición 2.17.(5), si d es $mcd(S)$ y $d \in (S) = (d)$, entonces existe una identidad de Bezout para S.

(2) $m = mcm(S) \iff (m) = \cap_{s \in S}(s)$. En consecuencia, $mcm(S)$ existe si y solo si el ideal $\cap_{s \in S}(s)$ es principal, y entonces cualquier generador de este es un mcm de S.

$' \implies ' \subset' m = mcm(S) \iff \begin{cases} s|m,\ \forall s \in S \\ s|n, \forall s \in S \implies m|n \end{cases} \iff \begin{cases} (m) \subset (s), \forall s \in S \\ (n) \subset (s), \forall \in S \implies (n) \subset (m) \end{cases} \implies (m) \subset \cap_{s \in S}(s)$

$' \supset'$ Sea $x \in \cap_{s \in S}(s) \implies x = a_s s, \forall s \in S \implies s|x, \forall s \in S \implies m|x \implies x \in (m)$

$' \impliedby '$ Supongamos $m \neq mcm(S) = e \implies \begin{cases} s|e, \forall s \in S \\ s|n, \forall s \in S \implies e|n \end{cases} \implies (e) \subset \cap_{s \in S}(s) \implies (e) \subset (m) \implies \begin{cases} m|e \\ m \in \cap_{s \in S}(s) \implies s|m, \forall s \in S \end{cases} \implies e \text{ no es } mcm(S)\#$

Segunda afirmación

$\exists m = mcm(S) \iff (m) = \cap_{s \in S}(s)$ principal

Tercera afirmación

Si $(k) = \cap_{s \in S}(s) \implies k = mcm(S)$

2.2.6 Demostrar en $\mathbb{Z}\left[\sqrt{-5}\right]$:

(1) 2 y $1 + \sqrt{-5}$ son coprimos y sin embargo no hay una identidad de Bezout para $\left\{2, 1 + \sqrt{-5}\right\}$

Si $a|2$ $a|1 + \sqrt{-5} \implies \begin{cases} N(a)|N(2) = 2^2 = 4 \\ N(a)|N\left(1 + \sqrt{-5}\right) = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 6 \end{cases}$

Por tanto, ha de ser

$$a_1^2 + 5a_2^2 | 2$$

- $a_1^2 + 5a_2^2 = 2$, no hay dos enteros que puedan verificar esto

- $a_1^2 + 5a_2^2 = 1 \implies N(a) = 1 \implies a \in \mathbb{Z}\left[\sqrt{-5}\right]^*$

Por tanto, son coprimos.

Para que exista una identidad de Bezout, debe suceder que $1 \in (2, 1+\sqrt{-5})$. O sea

$$1 = 2a + \left(1+\sqrt{-5}\right) b$$

con $a, b \in \mathbb{Z}\left[\sqrt{-5}\right]$. ¿Es esto posible?

$$2\left(a_1 + a_2\sqrt{-5}\right) + \left(1+\sqrt{-5}\right)\left(b_1 + b_2\sqrt{-5}\right) = 2a_1 + 2a_2\sqrt{-5} + b_1 + b_2\sqrt{-5} + b_1\sqrt{-5} - 5b_2 = 1 \iff$$

$$\iff \begin{cases} 2a_1 + b_1 - 5b_2 = 1 \\ 2a_2 + b_2 + b_1 = 0 \end{cases} \implies 1 - b_1 + 5b_2 = -b_2 - b_1 \iff 1 + 5b_2 = -b_2 \iff 1 + 6b_2 = 0$$

Y ningún entero verifica esto.

(2) 2, $1+\sqrt{-5}$ no tienen mcm

Supongamos que sí, entonces

$$\begin{cases} 2|m \implies N(2)|N(m) \implies 4|N(m) \\ 1+\sqrt{-5}|m \implies 6|N(m) \end{cases} \implies 12 = mcm(4,6)|N(m)$$

Ahora bien, $6 = 3 \cdot 2 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$, por lo que $m|6 \implies N(m)|N(6) = 36$

Por tanto

$$12|N(m)|36 \implies N(m) \in \{12, 36\}$$

¿Puede ser 12?

$$m_1^2 + 5m_2^2 = 12 \implies m_1^2 \equiv 2 \mod 5$$

Modulo 5 los cuadrados son 1 *y* 4. Es decir, este caso no puede darse.

¿Puede ser 36?

$$m_1^2 + 5m_2^2 = 36 \implies m_1^2 \equiv 1 \mod 5$$

$m_1 \in \{-4, -1, 1, 4, 6\}$, los demás o su cuadrado se pasa de 36 o al cuadrado no son cong con 1 mod 5

$m_1 = -1, 1 \implies 5m_2^2 = 35 \implies m_2^2 = 7$. Esto no tiene solución entera

$m_1 = 6 \implies m_2 = 0$ Ok

$m_1 = -4, 4 \implies 5m_2^2 = 20 \implies m_2^2 = 4 \implies m_2 = \pm 2$ Ok

O sea $m \in \{6, \pm 4 \pm 2\sqrt{-5}\}$.

Es fácil comprobar que los múltiplos comúnes son $\left\{6, -4 + 2\sqrt{-5}, 4 - \sqrt{-5}\right\}$. Nótese que estos dos últimos son asociados.

Ahora bien, si existe el mcm, como $a = 6$ y $b = 4 - 2\sqrt{-5}$ no son asociados, solo puede ser uno de ellos, y debe dividir al otro.

Pero tenemos que $N(a) = N(b) = 36$. Si $a|b \implies b = ac \implies N(b) = N(a)N(c) \implies 36 = 36N(c) \implies N(c) = 1 \implies c = \pm 1$

Pero $b \neq \pm a$, por lo que estos números no tienen mcm.

2.2.7 Sea S un subconjunto finito de un anillo A y supongamos que para cada dos elementos distintos s, t de S se verifica que $mcd(s,t) = 1$. Demostrar que $mcm(S) \prod_{s \in S} s$

2.3 Dominios de factorización única

2.3.1 Sean D un DFU y P un conjunto de representantes de los irreducibles de D por la relación de equivalencia 'ser asociados'.

(1) Demostrar que cada elemento $a \in D$ se puede escribir de forma única como $a = u \prod_{p \in P} p^{\alpha_p}$, donde u es una unidad de D, cada $\alpha_p \geq 0$ y $\alpha_p = 0$ para casi todo $p \in P$. Llamaremos a esto la factorización de a en irreducibles de p.

Dado $a \in D$, por ser DFU, tenemos que

$$a = u \cdot p_1 \cdot ... \cdot p_n$$

y cualquier otra factorización es equivalente.

Entonces, para cada p_i, tomamos su representante en P, $\overline{p_i}$.

Entonces, para cada p_i, p_j tales que $\overline{p_i} = \overline{p_j}$, aumentamos en una unidad α_{p_i}, una vez hecho esto nos quedarán solo los representantes sin repetición y sus respectivos exponentes, digamos que hay k distintos.

Entonces

$$a = u \cdot u_1\overline{p_1} \cdot ... \cdot u_n\overline{p_n} = u \cdot u_1 \cdot ... \cdot u_n \cdot \overline{p_1}^{\alpha_{\overline{p_1}}} \cdot ... \cdot \overline{p_k}^{\alpha_{\overline{p_k}}} = v \cdot \overline{p_1}^{\alpha_{\overline{p_1}}} \cdot ... \cdot \overline{p_k}^{\alpha_{\overline{p_k}}} = v \prod_{i=1...n} \overline{p_i}^{\alpha_{\overline{p_i}}} = v \prod_{p \in P} p^{\alpha_p}$$

Donde $\alpha_p = 0, \forall p \notin \{\overline{p_1}, ..., \overline{p_k}\}$.

(2) Demostrar que si

$$\boldsymbol{a = u \prod_{p \in P} p^{\alpha_p} \quad y \quad b = v \prod_{p \in P} p^{\beta_p}}$$

son las factorizaciones de a, b es irreducibles de P entonces $a|b$ si y solo si $\alpha_p \leq \beta_p, \forall p \in P$.

$$a|b \iff b = ca \iff v \prod_{p \in P} p^{\beta_p} = cu \prod_{p \in P} p^{\alpha_p}$$

Si

$$c = w \prod_{p \in P} p^{\gamma_p}$$

Lo anterior queda

$$v \prod_{p \in P} p^{\beta_p} = wu \prod_{p \in P} p^{\gamma_p + \alpha_p} \iff \forall p \in P,\ p^{\beta_p} = p^{\gamma_p + \alpha_p} \iff \forall p \in P,\ \beta_p = \gamma_p + \alpha_p,\ para\ algún\ \gamma_p \geq 0 \iff \beta_p \geq \alpha_p$$

(3) El número de divisores de un elemento no nulo a de D es finito, salvo asociados.

Por (2), los divisores son aquellos números que tienen los coeficientes de su factorización en irreducibles de P menores o iguales que los de a.

Como son no negativos, y hay un número finito de exponentes no nulos, esta cantidad es finita.

(4) Obtener una fórmula para calcular el número de divisores de a, salvo asociados, en términos de una factorización de a.

La fórmula consiste en la cantidad de formas distintas de coger los coeficientes, es

$$\prod_{p\in P}(\alpha_p+1)$$

Por ejemplo

$$20=2^2\cdot 3$$

La fórmula da $3\cdot 2=6$.

(5) Demostrar que todo subconjunto de D tiene mcd y mcm y dar una fórmula para ambos.

$1|x,\ \forall x\in S\subset D\implies \exists mcd(S)$

Si S es finito, entonces podemos tomar el máximo de los coeficientes de cada p para cada elemento de S. Multiplicando todos estos $p^{max\{\alpha_p\}}$ obtenemos un mcm

Si es infinito, puede no haber mcm, ejemplo $\{n\in\mathbb{N}/n\ par\}$

Las fórmulas son

$$mcd(S)=\prod_{p\in P}p^{\omega_p},\qquad \omega_p=max\left\{\alpha:p^\alpha|s,\forall s\in S\right\}$$

$$mcm(S)=\prod_{p\in P}p^{\sigma_p},\qquad \sigma_p=max\left\{\alpha:p^\alpha|s,\ para\ algún\ s\in S\right\}$$

(6) Dar ejemplos de conjuntos P como los del ejercicios para $\mathbb{Z}$ y $K[X]$ con K cuerpo.

$$P(\mathbb{Z})=\{p\in\mathbb{Z}/p\ primo\}$$
$$P(K[X])=\{X^n/n\geq 0\}$$

2.3.2 Sea D un dominio y supongamos que existe una aplicación $\mu: D\to\mathbb{Z}^{\geq 0}$ que verifica las propiedades:

- $\mu(ab)=\mu(a)\mu(b),\ \forall a,b\in D$
- $\mu(a)=0\iff a=0$
- $\mu(a)=1\iff a\in D^*$

Demostrar que D es DF. Demostrar que si $\mu(a)$ es primo y diferente de $\mu(1)$ entonces a es irreducible en D.

Este no sé hacerlo

2.3.3 ¿Qué conclusión sobre el anillo $\mathbb{Z}\left[\sqrt{-3}\right]$ se extrae de la igualdad $\left(1+\sqrt{-3}\right)\left(1-\sqrt{-3}\right)=4$?

Que no es DFU, puesto que también se verifica $4=2\cdot 2$ y 2 no es asociado de ninguno de los otros dos factores. Para comprobar esto suponemos que si y veremos que no puede ser.

El 2.3.4 es muy pesado.

2.3.5 Sea $m \neq 1$ un entero libre de cuadrados y sea $R = \mathbb{Z}\left[\sqrt{m}\right]$. Se pide:

(1) Usando la igualdad $\left(m+\sqrt{m}\right)\left(m-\sqrt{m}\right) = m(m-1)$, demostrar que 2 no es primo en R.

$m(m-1)$ es par, pues si $m-1$ es impar, entonces m es par, y al revés.
Por tanto $m(m-1) = 2 \cdot k \implies 2|m(m-1) = (m+\sqrt{m})\,(m-\sqrt{m})$
Pero $2 \nmid m+\sqrt{m}$, pues si fuese así, entonces

$$m+\sqrt{m} = 2c \implies \begin{cases} m \text{ par} \implies \sqrt{m} \text{ par} \\ m \text{ impar} \implies \sqrt{m} \text{ impar} \end{cases} \implies \sqrt{m} \text{ entero\#}$$

Contradicción, pues m es libre de cuadrados.
Con $m-\sqrt{m}$ el razonamiento es el mismo.

El 2 y el 3 no me salen

---

(4) Encontrar dos factorizaciones de 4 esencialmente distintas en $\mathbb{Z}\left[\sqrt{-3}\right]$

$$\left(1+\sqrt{-3}\right)\left(1-\sqrt{-3}\right) = 4 = 2 \cdot 2$$

(5) Encontrar dos factorizaciones de 6 esencialmente distintas en $\mathbb{Z}\left[\sqrt{-6}\right]$

$$2 \cdot 3 = 6$$

$$\left(a+b\sqrt{-6}\right)\left(c+d\sqrt{-6}\right) = (ac-6bd)+(ad+bc)\sqrt{-6} = 6 \iff \begin{cases} ac-6bd = 6 \\ ad+bc = 0 \end{cases}$$

$b = 1, d = -1$

$$\begin{cases} ac+6 = 0 \\ -a+c = 0 \end{cases} \implies a = 0 = c$$

Así

$$6 = \left(\sqrt{-6}\right)\left(-\sqrt{-6}\right)$$

Los dos que faltan son parecidos

2.4 Dominios de ideales principales

2.4.1 Sea D un DIP y sean $S \subset D$ y $a, b, c \in D$. Demostrar:

(1) S tiene un mcm

Por el ejercicio 2.2.5 mcm existe sii $\cap_{s \in S}(s)$ es principal.
Como es DIP, es principal.

(2) S tiene un mcd y existe una identidad de Bezout para S

Por el 2.2.5, si (S) es principal, entonces cualquier generador suyo es mcd y admite identidad de Bezout.
Como es DIP, (S) es principal.

(3) $\boldsymbol{d = mcd\{a_1, ..., a_n\} \iff d|a_i, \forall i = 1, ..., n \ y \ \exists r_1, ..., r_n \in D / r_1a_1 + ... + r_na_n = d}$
Se deduce inmediatamente del apartado anterior.
(4) Los elementos $\boldsymbol{a_1, ..., a_n}$ son coprimos si y solo si $\boldsymbol{\exists r_1, ..., r_n \in D / r_1a_1 + ... + r_na_n = 1}$
Son coprimos sii el mcd es 1 sii existe esa identidad, por el apartado anterior.
(5) Si $\boldsymbol{d = mcd(a, b) \implies mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1}$

Por el (3), $d = mcd(a, b) \iff d|a, d|b \ y \ \exists c, d/ca + db = d \implies c\frac{a}{d} + d\frac{b}{d} = 1 \overset{(4)}{\implies} mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
(6) no me sale
(7) Si $\boldsymbol{mcd(a, b) = 1 \ y \ a|bc \implies a|c}$
Si $a \nmid c \implies a$ no es primo, pues $a|bc$ pero $a \nmid b \ y \ a \nmid c$
¿$mcd(a, c) = 1$?
Supongamos que $1 \neq d = mcd(a, c)$. Entonces

$$\begin{cases} d|a \\ d|c \implies d|bc \end{cases} \implies \begin{cases} d|a \\ d|bc \\ a|a \\ a|bc \end{cases} \overset{d \ mcd}{\implies} a|d \overset{d|a}{\implies} a, d \ asociados \overset{d|c}{\implies} a|c\#$$

Contradicción, por lo que $mcd(a, c) = 1\#$ Contradicción, pues si $mcd(a, b) = 1 = mcd(a, c) \implies \overset{(6)}{mcd}(a, bc) = 1$, pero $a|bc$.
(8) y (9) no me salen

El 2.4.2 es una proposición del capítulo 3 (prop 3.13)

2.4.3 Demostrar que si todos los ideales de un anillo A son principales e I es un ideal de A entonces todos los ideales de $\frac{A}{I}$ son principales. ¿En qué condiciones si A es un DIP se verificará que $\frac{A}{I}$ también es un DIP?

Esto se demuestra en el ejercicio 1.5.7

La segunda pregunta, al relacionarla con la primera, vemos que lo que debe verificarse es que $\frac{A}{I}$ sea dominio, o sea que I debe ser maximal o primo, por la proposición 2.24.

2.5 Dominios euclídeos

2.5.1 Demostrar que si D es un DIP entonces todo ideal se puede poner de forma única como producto de ideales maximales. ¿Qué ideales son intersección de ideales maximales?

$D \ DIP \implies D \ DFU$

Dado $0 \neq I \lhd D$, al ser DIP, tenemos que $I = (a)$.
Por ser DFU, $a = up_1 \cdot ... \cdot p_k$, donde p_i son irreducibles.
Entonces $I = (a) = (p_1 \cdot ... \cdot p_k) = (p_1)...(p_k) = P_1...P_k = (q_1...q_m)$
Y cada $(p_i) = P_i$ es ideal maximal, por ser p_i irred.

$$a = up_1...p_k = vq_1...q_m$$

$k = m$ y podemos suponer p_i asociado de q_i, luego $(p_i) = (q_i), \forall i$

2.5.2 Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo entre DI entonces o bien f es un isomorfismo o bien B es un cuerpo.

Si f no es isomorfismo, entonces f no es inyectiva, por lo que $Kerf \neq 0$.

Por el primer teorema de isomorfía

$$\frac{A}{Kerf} \simeq B \implies \frac{A}{Kerf}\ dominio \implies Kerf\ primo$$

Por la proposición 2.24, se tiene que $Kerf$ es maximal, lo que implica que $\frac{A}{Kerf}$ es cuerpo, lo que equivale a que B sea cuerpo.

2.5.3 Sea D un DIP y sea $a = p_1^{e_1}...p_k^{e_k}$ con $p_1, ..., p_k$irreducibles no asociados de D. Demostrar que

$$\frac{D}{(a)} \cong \frac{D}{(p_1^{e_1})} \times ... \times \frac{D}{(p_k^{e_k})}$$

Por ser DIP, es DFU, y entonces los irreducibles son primos.

Entonces los $p_i^{e_i}$ son coprimos, o sea $mcd(p_1^{e_1}, ..., p_k^{e_k}) = 1$. Por el ejercicio 2.4.1 (9), tenemos que $mcd \cdot mcm$ y $\prod_i p_i^{e_i}$ son asociados.

Es decir, que $1 \cdot mcm$ es asociado de $a \implies a = mcm(p_1^{e_1}, ..., p_k^{e_k}) \implies (a) = \cap_i (p_i^{e_i})$

Como son coprimos, son coprimos dos a dos, entonces $(p_i) + (p_j) = D, \forall i \neq j$.

Así, estamos en las condiciones del teorema chino de los restos. O sea, que

$$\frac{A}{(a)} = \frac{A}{\cap_i (p_i^{e_i})} \cong \frac{A}{(p_1^{e_1})} \times ... \times \frac{D}{(p_k^{e_k})}$$

2.6 El cuerpo de fracciones de un dominio

2.6.1 Sea D un dominio y sea Q su cuerpo de fracciones. Demostrar que:

(1) Si D' es un subanillo de D con cuerpo de fracciones Q', entonces Q contiene un subcuerpo isomorfo a Q'

D' subanillo de D dominio $\implies$ D' dominio

$$D \subset Q \implies D \xrightarrow{u} Q\ hom\ iny$$

$$D' \subset D \implies D' \xrightarrow{i} D\ hom\ iny$$

$$D' \xrightarrow{u \circ i} Q\ hom\ iny$$

Por la proposición 2.35, Q contiene un subcuerpo isomorfo a Q'.

(2) Si A es un subanillo de Q que contiene a D, entonces Q es un cuerpo de cocientes de A

'$\subset$' $D \subset A \implies Q(D) \subset Q(A)$

'$\supset$' Q cuerpo $\implies$ Q dominio $\implies$ A dominio

$$A \xrightarrow{u} Q\ hom\ iny$$

Por la prop 2.35, Q contiene un subcuerpo isomorfo a $Q(A) \implies Q(A) \subset Q(D)$.