Ayudantia 20

Profesor: Cristóbal Rivas
Ayudantes: Benjamin Martinez, Javier Pavez

Viernes 11 de Noviembre 2022

Ejercicios para la ayudantía.

Ejercicio 20.1. Juguemos con numeritos.

a) Demostrar que 3 es irreducible pero no primo en $\mathbb{Z}[\sqrt{-5}]$.

Demostración. 0°Para este ejercicio asumiremos el Ejercicio 20.11. Esto quiere decir que usaremos de la función $N : \mathbb{Z}[\sqrt{-5}] \setminus \{0\} \longrightarrow \mathbb{N}$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ con $a, b \in \mathbb{Z}$. Además usaremos la propiedad de que $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{-5}]\setminus\{0\}$.

1° Demostraremos que es irreducible.

Supongamos que $3 = xy$ con $x, y \in \mathbb{Z}[\sqrt{-5}]$, queremos demostrar que o bien x es invertible o bien y es invertible.

Definitivamente ni x ni y pueden ser cero. Luego, podemos usar 0° y tener (1).

$$9 = N(3) = N(xy) = N(x)N(y) \tag{1}$$

De ahí deducimos que $(N(x), N(y)) \in \{(1, 9), (3, 3), (9, 1)\}$. Procederemos a trabajar por casos, con el fin de demostrar lo querido. Veremos que los casos (1, 9) y (9, 1) satisfacen lo querido y que el caso (3, 3) no puede suceder.

Si $N(x) = 1$ o $N(y) = 1$, como 1 es el valor mínimo que puede tomar N, por el Lema 2.67. de los apuntes del curso tendremos que x o y es invertible y obtenemos lo que queremos.

Si $N(x) = 3 = N(y)$, consideramos $x = a + b\sqrt{-5}$ con $a, b \in \mathbb{Z}$. Obtenemos (2).

$$3 = N(x) = a^2 + 5b^2 \tag{2}$$

Una rápida inspección de valores enteros nos muestra que no existen $a, b \in \mathbb{Z}$ que satisfagan (2). Luego, $N(x) \neq 3$ y por lo tanto los únicos casos posibles satisfacen lo que queremos. O sea, 3 es irreducible en $\mathbb{Z}[\sqrt{-5}]$.

Para mostrar que 3 no es primo, encontraremos $x, y \in \mathbb{Z}[\sqrt{-5}]$ tal que 3 divide a xy pero no divide ni a x ni a y.

Consideramos $x = 1 + \sqrt{-5}$ e $y = 1 - \sqrt{-5}$. Calculando tendremos (3).

$$3 \mid 6 = xy \tag{3}$$

Por lo que solo nos falta verificar que 3 a ninguno divide.

Supongamos que 3 divide a x o a y. Esto significa que existen $t, s \in \mathbb{Z}[\sqrt{-5}]$ tal que $3t = x$ o $3s = y$. Aplicando nuestra función N tendremos (4) y (5).

$$9N(t) = N(3)N(t) = N(3t) = N(x) = 6 \tag{4}$$

$$9N(s) = N(3)N(s) = N(3s) = N(y) = 6 \tag{5}$$

Dado que la imagen de N son los naturales, deducimos que (4) y (5) no pueden suceder. Por lo tanto 3 no divide nia x ni a y y por ende no es primo en $\mathbb{Z}[\sqrt{-5}]$.

Concluimos que 3 es irreducible pero no primo en $\mathbb{Z}[\sqrt{-5}]$. □

b) Dar dos factorizaciones de 72 en números irreducibles dentro de $\mathbb{Z}$. ¿Por qué esto no contradice el hecho de que sea un DFU?

Demostración. Calculando se comprueba que (6) y (7) son factorizaciones de 72.

$$48 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \tag{6}$$
$$48 = 2 \cdot 2 \cdot (-3) \cdot 2 \cdot (-3) \tag{7}$$

Dado que la cantidad de números irreducibles en (6) y (7) es la misma, dado que -1 es invertible y por ende -3 y 3 son asociados. Podemos concluir que las dos factorizaciones respetan la definición de DFU.

Podemos visualizarlo de la siguiente manera. Denotamos los irreducibles y los invertibles de la siguiente manera.

$p_1 = 3$, $p_2 = 3$, $p_3 = 2$, $p_4 = 2$, $p_5 = 2$.
$q_1 = -3$, $q_2 = -3$, $q_3 = 2$, $q_4 = 2$, $q_5 = 2$.
$u_1 = -1$, $u_2 = -1$, $u_3 = 1$, $u_4 = 1$, $u_5 = 1$.

Obtenemos (8), (9) y luego la relación que deben cumplir.

$$72 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \tag{8}$$
$$72 = q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 \tag{9}$$

$$\begin{aligned} p_1 &= u_1 \cdot q_1 \\ p_2 &= u_2 \cdot q_2 \\ p_3 &= u_3 \cdot q_3 \\ p_4 &= u_4 \cdot q_4 \\ p_5 &= u_5 \cdot q_5 \end{aligned}$$

Donde los u_i son invertibles y p_i, q_i son los irreducibles. O sea, p_i es asociado con q_i. □

c) Encontrar un $MCD(5, -1+3i)$ en $\mathbb{Z}[i]$. Además encontrar una factorizacion en irreducibles de cada uno.

Demostración. 0° Para este ejercicio de nuevo asumiremos el Ejercicio 20.11. Esto quiere decir que usaremos de la función $N : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$, $a + bi \mapsto a^2 + b^2$ con $a, b \in \mathbb{Z}$. Además usaremos la propiedad de que $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[i] \setminus \{0\}$.

1° Si d es un divisor de 5 y de $-1+3i$. Entonces existen $t, s \in \mathbb{Z}[i]$ tal que $dt = 5$ y $ds = -1 + 3i$.

Aplicando N tenemos.
$N(d)N(t) = N(dt) = N(5) = 25$.
$N(d)N(s) = N(ds) = N(-1+3i) = 10$.

Luego, $N(d)$ divide a 25 y a 10. Nuestra hipótesis es que si $d = MCD(5, -1+3i)$ entonces $N(d) = 5$.

Ahora buscaremos un número tal que la imagen de N es 5 y divida a 5 y a $-1+3i$.

Después de unos intentos, encontramos a $1+2i$. Nos damos cuenta que $(1+2i)(1-2i) = 5$ (divide a 5), $(1+2i)(1+i) = -1+3i$ (divide a $-1+3i$) y $N(1+2i) = 5$. Por lo que demostraremos que es un máximo común divisor.

Notemos que $1+2i = 5 \cdot i + (-1) \cdot (-1+3i)$. Si x divide a 5 y a $-1+3i$, tendremos que $\frac{5}{x}, \frac{-1+3i}{x} \in \mathbb{Z}[i]$. Luego,

$$\frac{1+2i}{x} = \frac{5}{x} \cdot i + \frac{-1+3i}{x} \cdot (-1) \in \mathbb{Z}[i]$$

Y por lo tanto x divide a $1+2i$. Esto demuestra que $1+2i$ es un máximo común divisor de 5 y $-1+3i$. □

Definición 20.1. Sea A un anillo conmutativo. Un ideal propio P de A se dice ideal primo, si para todo $a \cdot b \in P$ se tiene que $a \in P$ o $b \in P$.

Sea A un anillo. Diremos que A es Booleano si $x^2 = x$ para todo $x \in A$, es decir, si todos sus elementos son idempotentes.

Ejercicio 20.2. Sea A un anillo Booleano conmutativo con unidad. Demuestre:

a) $2x = 0$ para todo $x \in A$.

Demostración. Consideramos $x + x \in A$. Como A es Booleano, tendremos (10).

$$(x+x)^2 = (x+x) \tag{10}$$

Desarrollando (10) obtenemos (11).

$$x^2 + 2x^2 + x^2 = x + x \tag{11}$$

Usando Booleanidad en (11) obtenemos (12).

$$x + 2x + x = x + x \tag{12}$$

Finalmente, restando en ambas parte de la igualdad de (12) concluimos (13).

$$2x = 0 \tag{13}$$

Agregado: Dado que $2x = 0$, es lo mismo que decir $x + x = 0$. Por lo que agregamos que $x = -x$ para todo $x \in A$. □

b) Sean a, $b \in A$, demuestre que existe $c \in A$ tal que $(a) + (b) = (c)$.

Demostración. Dado a y b fijos, consideramos $c = a + b + ab$. Demostraremos la igualdad pedida por doble contención. Pero primero recordemos las definiciones.

$$\begin{aligned} (c) &:= \{ct \mid t \in A\} && (14)\\ (a)+(b) &:= \{z+w \mid z \in (a) \wedge w \in (b)\} && (15)\\ &:= \{ax+by \mid x,\, y \in A\} && (16) \end{aligned}$$

1° Probaremos que $(c) \subset (a)+(b)$, o sea, todo elemento de (c) está en $(a)+(b)$. Para eso, debemos poder escribir todo elemento de (c) como un elemento de $(a)+(b)$. Esto quiere decir, poder escribir $ct = ax + by$ para todo $t \in A$ y algunos x, $y \in A$.

Pero en realidad, solo falta ver que $c \in (a)+(b)$. Ya que como $(a)+(b)$ es un ideal, si $c \in (a)+(b)$ entonces $ct \in (a)+(b)$ para todo $t \in A$, por lo tanto por (14) se tiene $(c) \subset (a)+(b)$.

Ahora si demostremos la inclusión. Recordemos que $c = a+b+ab = a(1+b)+b$. Luego, por (16) tenemos que $c \in (a)+(b)$ y concluimos lo pedido.

2° $(a)+(b) \subset (c)$. Para esta inclusión, debemos notar que solo hace falta mostrar que a, $b \in (c)$. Ya que como (c) es un ideal, tendriamos que ax, $by \in (c)$ para todo x, $y \in A$. Luego, como (c) es un ideal, $ax + by \in (c)$ para todo x, $y \in A$. Por (16) tendriamos que $(a)+(b) \subset (c)$.

Ahora demostremos la inclusión. Sabemos que $c = a+b+ab \in (c)$. Luego, $a \cdot (a+b+ab) \in (c)$ y $(a+b+ab) \cdot b \in (c)$. Lo anterior es equivalente a decir que $a^2 + ab + a^2b \in (c)$ y $ab + b^2 + ab^2 \in (c)$. Dado que A es Booleano tendremos que $a + 2ab = a + ab + ab \in (c)$ y $2ab + b = ab + b + ab \in (c)$. Finalmente, por el Ejercicio 20.2. a), obtenemos que $a = a + 0 \in (c)$, $b = 0 + b \in (c)$ y concluimos que $(a)+(b) \subset (c)$.

Ahora podemos concluir que $(a)+(b) = (a+b+ab)$. □

Nota mental: Por inducción puede probar que con a_1, ..., $a_n \in A$, existe $c \in A$ tal que $(a_1)+\cdots+(a_n) = (c)$. Esto no significa que todo ideal de A sea principal, ya que pueden haber ideales de A que no se puedan escribir como suma finita de ideales principales.

c) Si $\mathfrak{p}$ es un ideal primo de A, entonces es un ideal maximal de A. Más aun $A/\mathfrak{p}$ es un cuerpo de dos elementos.

Demostración. Primero veremos que $A/\mathfrak{p}$ tiene dos elementos. Luego que es un cuerpo. Y finalizaremos concluyendo que $\mathfrak{p}$ es maximal.

1° Sea $x + A \in A/\mathfrak{p}$, veremos que $x + A = 0 + A$ o $x + A = 1 + A$.

Como A es Booleano, tendremos que $x^2 = x$. Esto significa que $x^2 + A = x + A$. Por operaciones en el cociente obtenemos (17).

$$(x+A)^2 = (x+A)(x+A) = x \cdot x + A = x^2 + A = x + A \tag{17}$$

Restando $x + A$ en (17) tendremos (18).

$$(x+A)^2 - (x+A) = 0 + A \tag{18}$$

En la parte izquierda de la igualdad en (18), podemos factorizar por $x + A$ y tener (19).

$$(x+A)[(x+A) - (1+A)] = 0 + A \tag{19}$$

Ahora nos acordamos del ejercicio 4. de la ayudantía 19. Como $\mathfrak{p}$ es un ideal primo, tendremos que $A/\mathfrak{p}$ es un dominio de integridad. Como es un dominio de integridad, por definición no tiene divisores de cero. Así, de (19) obtenemos que $x + A = 0 + A$ o $(x + A) - (1 + A) = 0 + A$. O de manera equivalente, obtenemos que $x + A = 0 + A$ o $x + A = 1 + A$. Y concluimos lo pedido.

2° Lo que realmente nos dice 1°, es que $A/\mathfrak{p}$ tiene a lo más dos elementos. Pero $A/\mathfrak{p}$ no puede tener un elemento. Ya que de tenerlo, necesariamente $A = \mathfrak{p}$ por el teorema de

correspondencia; pero al ser $\mathfrak{p}$ un ideal primo, este es propio. Así podemos concluir que necesariamente $A/\mathfrak{p}$ tiene dos elementos.

3° Dado que $A/\mathfrak{p}$ es un dominio de integridad y tiene dos elementos. Por el Ejercicio 15.1. de la ayudantía 15 concluimos que $A/\mathfrak{p}$ es un cuerpo.

4° Finalmente, como $A/\mathfrak{p}$ es un cuerpo, el Lema 18.1. de la ayudantía 18 nos dice que $\mathfrak{p}$ es un ideal maximal. □

d) Si además A es un dominio de integridad, deducir que todo elemento primo es maximal.

Demostración. Sea $p \in A$ un elemento primo.

Consideramos el ideal generado por p. Primero demostraremos que es propio y luego que es un ideal primo.

1° Como p es un elemento primo, tendremos que p no es invertible. Dado que no es invertible, tendremos que p no divide a uno. Lo anterior significa que $px \neq 1$ para todo $x \in A$. Luego, por definición de (p) se tiene que $1 \notin (p)$. Y así se deduce que $(p) \subsetneq A$.

2° Recordemos la Definición 20.1. Sean x, $y \in A$ tal que $xy \in (p)$, queremos demostrar que $x \in (p)$ o $y \in (p)$.

Por definición de (p), se tiene que existe $t \in A$ tal que $pt = xy$. Lo anterior significa que p divide xy. Por definición de elemento primo, tendremos que p divide a x o p divide a y. Es decir, existe un $t \in A$ tal que $pt = x$ o $pt = y$. Concluyendo que $x \in (p)$ o $y \in (p)$. Por lo tanto (p) es un ideal primo.

3° Dado que (p) es un ideal primo, tendremos por el Ejercicio 20.2. c) que (p) es un ideal maximal.

4° Finalmente mostraremos que p es un elemento irreducible.

Sean x, $y \in A$ tal que $p = xy$, queremos demostrar que x o y es invertible. El que $p = xy$, significa que $p \in (x)$. Por el Ejercicio 20.2. b) 1° podemos deducir que $(p) \subset (x)$. Y dado que (p) es un ideal maximal, nos quedan dos casos.

4.1° $(x) = A$. En este caso ganamos al tiro. Este caso implica que $1 \in (x)$. Por definición de ideal principal, tendremos que existe $t \in A$ tal que $xt = 1$. Pero eso no es más que decir que x es invertible. Y llegamos a lo que queríamos.

4.2° $(x) = (p)$. En este caso tendremos que $x \in (p)$, por lo que existe $s \in A$ tal que $ps = x$. Recordemos que por hipótesis $p = xy$, remplazando ahí nos queda que $p \cdot 1 = p = psy$. Usando la ley de cancelación obtenemos que $1 = sy$. Deduciendo que y es invertible.

Concluimos que en cualquier caso, o x o y es invertible y por lo tanto p es un elemento irreducible. □

Ejercicio 20.3. Sean A un anillo con más de un elemento y R un DI. Demuestre los siguientes enunciados.

a) $A[x]$ el anillo de polinomios con coeficientes en A, no es un cuerpo.

Demostración. La demostración consiste de dos casos. Primero veremos cuando A no es un anillo con unidad. Luego, cuando A es un anillo con unidad.

1° Si $A[x]$ no es un anillo con unidad, inmediatamente vemos que no es un cuerpo. Primero veremos que si $A[x]$ es un anillo con unidad, entonces A es un anillo con unidad. Considerando la contraposición lógica de la implicancia anterior y lo dicho al principio,

tendremos las siguientes implicancias: Si A no es un anillo con unidad, entonces $A[x]$ no es un anillo con unidad, entonces $A[x]$ no es un cuerpo.

2° Supongamos existe $u \in A[x]$ tal que $u \cdot p(x) = p(x) \cdot u = p(x)$ para todo $p(x) \in A[x]$. Inmediatamente tendremos que $u \cdot a = a \cdot u = a$ para todo $a \in A$. Por lo que demostraremos que $u \in A$ y por lo tanto que A es un anillo con unidad.

Para empezar, sabemos que $u \in A[x]$ debe tener la siguiente forma.

$$u = \sum_{i=0}^{n} a_i x^i \tag{20}$$

Donde $n \in \mathbb{N}_0$ y $a_i \in A$ para todo i.

Consideremos $b \in A$ fijo pero cualquiera. Por hipótesis tenemos que $b \cdot u = u \cdot b = b$. Remplazando (20) tendremos que $b \cdot (\sum_{i=0}^{n} a_i x^i) = (\sum_{i=0}^{n} a_i x^i) \cdot b = b$. Multiplicando tenemos que $\sum_{i=0}^{n} (b \cdot a_i) x^i = \sum_{i=0}^{n} (a_i \cdot b) x^i = b$. Por definición de polinomios, necesariamente tendremos (21).

$$b \cdot a_i = a_i \cdot b = 0 \text{ para todo } i \in [1, n] \text{ y } b \cdot a_0 = a_0 \cdot b = b. \tag{21}$$

3° Dado que b era cualquier elemento de A, (21) se cumple para todo $b \in A$. Inmediatamente tenemos que a_0 es un neutro multiplicativo. Como (21) se satisface para todo elemento de A, tendremos que $a_i = a_0 \cdot a_i = 0$ para todo $i \in [1, n]$. Concluimos que $u = a_0 \in A$ y obtenemos lo que queríamos.

4° Podemos concluir que si A no es un anillo con unidad, entonces $A[x]$ no es un cuerpo.

5° Veamos ahora el caso cuando $A[x]$ si es un anillo con unidad. Quien está leyendo podrá aseverar que el neutro de $A[x]$ es realmente el neutro de A, que denotaremos por 1. Para demostrar que no es un cuerpo, veremos que existe un elemento no invertible.

6° Probaremos que un elemento sin inverso multiplicativo es x. Sea $p(x) \in A[x]$ un elemento cualquiera. Tendremos que $p(x)$ es de la forma $\sum_{i=0}^{n} c_i x^i$, donde $n \in \mathbb{N}_0$ y $c_i \in A$ para todo i. Multiplicando tenemos que $(\sum_{i=0}^{n} c_i x^i) \cdot x = \sum_{i=0}^{n} c_i x^{i+1} = \sum_{i=1}^{n+1} c_{i-1} x^i = \sum_{i=0}^{n+1} c_{i-1} x^i$, donde $c_{-1} = 0$. De la definición de polinomios, deducimos que $x \cdot p(x) \neq 1$. Ya que $0 \neq 1$ al tener A más de un elemento. Por lo tanto no existe elemento tal que al multiplicar por x tengamos 1. Concluimos que x no es invertible y por lo tanto $A[x]$ no es un cuerpo.

□

b) Deducir que todo dominio de integridad está contenido en un dominio euclideano que no es un cuerpo.

Demostración. Sabemos que podemos ver a R como un subanillo del cuerpo $Frac(R)$. Luego, por el ejercicio anterior sabemos que $Frac(R)[x]$ no es un cuerpo. Finalmente, por la Proposición 2.65. de los apuntes, tenemos que $Frac(R)[x]$ es un dominio euclideano, ya que $Frac(R)$ es un cuerpo. □

c) $Frac(R)[x] \subsetneq Frac(R[x])$.

Demostración. 0° Primero veamos la çontención". Probaremos que existe un homomorfismo de anillos inyectivos que va de $Frac(R)[x]$ a $Frac(R[x])$. Antes unos preliminares.

1° Los elemento de $Frac(R)$ son de la forma $[a, b]_2$ tal que $a \in R$, $b \in R \setminus \{0\}$ y $[-, -]_2$ es la clase de equivalencia de un elemento en $R \times R \setminus \{0\}$.

2° Los elemento de $Frac(R[x])$ son de la forma $[p(x), q(x)]_1$ tal que $p(x) \in R[x]$, $q(x) \in R[x] \setminus \{0\}$ y $[-,-]_1$ es la clase de equivalencia de un elemento en $R[x] \times R[x] \setminus \{0\}$.

3° Además podemos considerar las clases de equivalencia $[a, b]_1$ tal que $a \in R$ y $b \in R \setminus \{0\}$. Lo anterior no significa necesariamente que $[a, b]_1 = [a, b]_2$.

4° Finalmente, debemos notar que un polinomio en $Frac(R)[x]$, se ve de la forma $p(x) = \sum_{i=0}^{n} [a_i, b_i]_2 x^i$; donde $n \in \mathbb{N}_0$ y $a_i \in R$, $b_i \in R \setminus \{0\}$ para todo i.

5° Ya hechos los preliminares, consideraremos $\psi : Frac(R)[x] \longrightarrow Frac(R[x])$, $\sum_{i=0}^{n} [a_i, b_i]_2 x^i \mapsto \sum_{i=0}^{n} [a_i x^i, b_i]_1 = [\sum_{i=0}^{n} y_i a_i x^i, b_1 \cdots b_n]$, donde $y_i \cdot b_i = b_1 \cdots b_n$. Y probaremos que es la función buscada. Notemos que $y_i \in R$ por la ley de cancelación.

6° Está bien definida. Como puede tomar cualquier elemento del dominio y siempre caer en el codominio, verificaremos la regla de asignación. Sean $\sum_{i=0}^{n} [a_i, b_i]_2 x^i$, $\sum_{i=0}^{n} [c_i, d_i]_2 x^i \in Frac(R)[x]$.

Por definición de polinomio, $\sum_{i=0}^{n} [a_i, b_i]_2 x^i = \sum_{i=0}^{n} [c_i, d_i]_2 x^i$ si y solo si $[a_i, b_i]_2 = [c_i, d_i]_2$ para todo i.

Por definición de la clase de equivalencia 2, $[a_i, b_i]_2 = [c_i, d_i]_2$ si y solo si $a_i \cdot d_i - b_i \cdot c_i = 0$.

Dado que a_i, b_i, c_i, $d_i \in R \subset R[x]$ con R un D.I., $a_i \cdot d_i - b_i \cdot c_i = 0$ si y solo si $x^i \cdot a_i \cdot d_i - x^i \cdot b_i \cdot c_i = 0$ si y solo si $(a_i x^i) \cdot d_i - b_i \cdot (c_i x^i) = 0$ si y solo si $(a_i x^i) \cdot d_i = b_i \cdot (c_i x^i)$.

Ya que $R[x]$ es un D.I., $(a_i x^i) \cdot d_i = b_i \cdot (c_i x^i)$ si y solo si $(d_1 \cdots d_n)(y_i a_i x^i) = (z_i c_i x^i)(b_1 \cdots b_n)$ si y solo si $(d_1 \cdots d_n)(y_i a_i) x^i = (z_i c_i)(b_1 \cdots b_n) x^i$. Donde $y_i \cdot b_i = b_1 \cdots b_n$ y $z_i \cdots d_i = d_1 \cdots d_n$.

Como todos los "si y solo si"anteriores son para todo i, por definición de polinomios y distributividad tenemos; $(d_1 \cdots d_n)(y_i a_i) x^i = (z_i c_i)(b_1 \cdots b_n) x^i$ para todo i si y solo si $(\sum_{i=0}^{n} (d_1 \cdots d_n)(y_i a_i) x^i) = (\sum_{i=0}^{n} (z_i c_i)(b_1 \cdots b_n) x^i)$ si y solo si $(d_1 \cdots d_n) (\sum_{i=0}^{n} y_i a_i x^i) = (\sum_{i=0}^{n} z_i c_i x^i) (b_1 \cdots b_n)$.

ya que $R[x]$ es un anillo, $(d_1 \cdots d_n) (\sum_{i=0}^{n} y_i a_i x^i) = (\sum_{i=0}^{n} z_i c_i x^i) (b_1 \cdots b_n)$ si y solo si $(d_1 \cdots d_n) (\sum_{i=0}^{n} y_i a_i x^i) - (\sum_{i=0}^{n} z_i c_i x^i) (b_1 \cdots b_n) = 0$.

Por definición de la clase de equivalencia 1, $(d_1 \cdots d_n) (\sum_{i=0}^{n} y_i a_i x^i) - (\sum_{i=0}^{n} z_i c_i x^i) (b_1 \cdots b_n) = 0$ si y solo si $[\sum_{i=0}^{n} y_i a_i x^i, b_1 \cdots b_n]_1 = [\sum_{i=0}^{n} z_i c_i x^i, d_1 \cdots d_n]_1$.

Finalmente por definición de ψ, $[\sum_{i=0}^{n} y_i a_i x^i, b_1 \cdots b_n]_1 = [\sum_{i=0}^{n} z_i c_i x^i, d_1 \cdots d_n]_1$ si y solo si $\psi(\sum_{i=0}^{n} [a_i, b_i]_2 x^i) = \psi(\sum_{i=0}^{n} [c_i, d_i]_2 x^i)$.

Por lo que concluimos que ψ está bien definida y por lo tanto es una función. Pero además, dado todos los si y solo si, también probamos inyectividad.

7° Así solo nos falta mostrar que ψ es un homomorfismo de anillos. Sean $\sum_{i=0}^{n} [a_i, b_i]_2 x^i$, $\sum_{i=0}^{m} [c_i, d_i]_2 x^i$ $Frac(R)[x]$.

Denotamos $[e_i, f_i] = [a_i, b_i]$ si $i \in [1, n]$ y $[e_i, f_i] = [c_{i-n}, f_{i-n}]$ si $i \in [1 + n, m + n]$.

$$\begin{aligned}
\psi(\sum_{i=0}^{n} [a_i, b_i]_2 x^i + \sum_{i=0}^{m} [c_i, d_i]_2 x^i) &= \psi(\sum_{i=0}^{n+m} [e_i, f_i]_2 x^i) \\
&= \sum_{i=0}^{n+m} [e_i x^i, f_i]_1 \\
&= \sum_{i=0}^{n} [a_i x^i, b_i]_1 + \sum_{i=0}^{m} [c_i x^i, d_i]_1 \\
&= \psi(\sum_{i=0}^{n} [a_i, b_i]_2 x^i) + \psi(\sum_{i=0}^{m} [c_i, d_i]_2 x^i)
\end{aligned}$$

Lo que demuestra que ψ preserva la suma.

Si quien esté leyendo demuestra que ψ preserva la multiplicación, habremos demostrado lo querido y se conlcuye la demostración.

8° Para demostrar que la contención es propia, solo hay que mencionar que $Frac(R[x])$ es un cuerpo y $Frac(R)[x]$ no es un cuerpo. □

d) Si $R \subset A \subset Frac(R)$, entonces $Frac(A) = Frac(R)$.

Demostración. Dado que $R \subset A \subset Frac(R)$, tendremos que A es un D.I. Ahora consideramos la Proposición 2.47. de los apuntes de la clase.

Como $A \subset Frac(R)$, por la proposición tendremos que $Frac(A) \subset Frac(R)$.

Como $R \subset A \subset Frac(A)$, por la proposición tendremos que $Frac(R) \subset Frac(A)$.

Concluimos que $Frac(R) = Frac(A)$. □

Ejercicios para la casita.

Ejercicio 20.4. Recuerde que un anillo se dice Booleano si todos sus elementos son idempotentes. Demuestre.

a) Todo anillo Booleano es conmutativo.

b) Existe un anillo Booleano de infinitos elementos.

Ejercicio 20.5. (En colaboración con Emir Molina T.). Sean $(G, +)$ un grupo y $(A, +, \cdot)$ un anillo. Si existe un isomorfismo de grupos $\psi : (G, +) \longrightarrow (A, +)$. Demostrar que $(G, +, *)$ es un anillo, donde $*$ se define como sigue.

$$\begin{aligned} * : G \times G \longrightarrow G,\ (a,\ b) &\mapsto \psi^{-1}(\psi(a)\psi(b)) \\ a * b &= \psi^{-1}(\psi(a)\psi(b)) \end{aligned}$$

Hint:
Recordar que $\psi(a)$, $\psi(b) \in A$ para todo a, $b \in G$.
Recordar que como ψ es biyectiva, $\psi^{-1} : A \longrightarrow G$ es una función bien definida. Más aun, recordar que como ψ es un isomorfismo de grupos, entonces ψ^{-1} también es un isomorfismo de grupos.

Ejercicio 20.6. Sea L un cuerpo de característica p. Demostrar que $\mathbb{Z}/p\mathbb{Z}$ es isomorfo a un subcuerpo de L.
Nota: Sea L un cuerpo. Diremos que un subconjunto $B \subset L$ es un subcuerpo, si es un subanillo y además un cuerpo.

Ejercicio 20.7. Encontrar el máximo común divisor y mínimo común múltiplo de $3 + 2i$ y $5 + i$ en $\mathbb{Z}[i]$.

Ejercicio 20.8. Sean L, M cuerpos. Sea $\psi : L \longrightarrow M$ un isomorfismo de cuerpos. Demostrar que $\varphi : L[x] \longrightarrow M[x]$, $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \psi(a_i) x^i$ es un isomorfismo de anillos.

Ejercicio 20.9. Sean K, L, F, M cuerpos tal que L es una extensión de K y M es una extensión de F. Sea $\psi : L \longrightarrow M$ un isomorfismo de cuerpos. Sea $\alpha \in L$ algebraico sobre K, demostrar que $\psi(\alpha) \in M$ es algebraico sobre F.

Ejercicio 20.10. Sea A un anillo y $S := \{xy - yx \mid x, y \in A\}$. Considere el ideal generado por S, definido en el ejercicio 17.5. de la ayudantía 17. Demostrar que $A/[S]$ es un anillo conmutativo.
Hint: Usar definiciones.

Ejercicio 20.11. Sea $n \in \mathbb{N}$. Consideremos $R = \mathbb{Z} + \sqrt{-n}\mathbb{Z} := \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$. Definimos la función $N : R \setminus \{0\} \longrightarrow \mathbb{N}$, $a + b\sqrt{-n} \mapsto a^2 + nb^2 = (a + b\sqrt{-n})(a - b\sqrt{-n})$. Demostrar que $N(xy) = N(x)N(y)$ para todo $x, y \in R \setminus \{0\}$.
Nota: No hemos demostrado que R es un anillo. Pero se puede demostrar que es el subanillo de $\mathbb{C}$ generado por $S = \mathbb{Z} \cup \{\sqrt{-n}\}$.