Ayudantia 15

Profesor: Cristóbal Rivas
Ayudantes: Benajamin Martinez, Javier Pavez

Viernes 21 de Octubre 2022

De ahora en adelante asumiremos los siguientes lemas.

Lema 15.1. Sea A un anillo y 0 su neutro aditivo. Entonces $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in A$.

Lema 15.2. Sea A un anillo y denotemos por $-x$ al inverso aditivo de x, para todo $x \in A$. Entonces $(-c) \cdot a = c \cdot (-a) = -(c \cdot a)$ para todo c, $a \in A$.

Lema 15.3. Sea A un anillo conmutativo y unitario y sea 0 su neutro aditivo. Entonces las siguientes condiciones son equivalentes.

a) $ca = cb \Longrightarrow a = b, \ \forall a, \, b \in A$ y $\forall c \in A \setminus \{0\}$.

b) $ab = 0 \Longrightarrow a = 0 \vee b = 0, \ \forall a, \, b \in A$.

Las demostraciones de los lemas precedentes es análoga a las demostraciones del Lema 1, Lema 2 y Ejercicio 13.3. de la ayudantía 13, respectivamente. Su demostración se deja como ejercicio para quien esté leyendo.

Antes de demostrar los ejercicio, demostraremos un lema.

Lema 15.4. Sea A un dominio de integridad, 0 su neutro aditivo y $n \in \mathbb{N}$. Sean $a_1, \, a_2, \, ..., \, a_n \in A \setminus \{0\}$. Entonces $\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdots a_n \neq 0$.

Demostración. Demostraremos el enunciado por inducción en n. Fijemos $n \in \mathbb{N}_{>1}$

1° Caso base.
Queremos verificar que $ab \neq 0$ para todo a, $b \in A \setminus \{0\}$.
Sean a, $b \in A \setminus \{0\}$, supongamos que $ab = 0$. Como A es un dominio de integridad, el que $ab = 0$ implica que $a = 0$ o $b = 0$, lo que genera una contradicción con la elección de los elementos. Concluimos lo querido, y por lo tanto está verificado. ✓

2° Hipótesis de inducción.
Supondremos que $\prod_{i=1}^{n-1} a_i \neq 0$ para todo $a_1, ..., \, a_{n-1} \in A \setminus \{0\}$.

3° Tesis: $\prod_{i=1}^{n} a_i \neq 0$ para todo $a_1, ..., \, a_n \in A \setminus \{0\}$.
Demostración. Sean $a_1, ..., \, a_n \in A \setminus \{0\}$. Por hipótesis de inducción tenemos que $\prod_{i=1}^{n-1} a_i \neq 0$. Denotemos $b := \prod_{i=1}^{n-1} a_i \in A \setminus \{0\}$. El caso base nos dice que $ba_n \neq 0$. Lo que concluye la demostración.

Luego, por inducción, el enunciado es verdadero para todo $n \in \mathbb{N}$. □

Ejercicio 15.1. Demostrar que todo dominio de integridad finito es un cuerpo.

Demostración. (Solución de Fernando Riveros P.) Sea R un dominio de integridad finito.

Los casos cuando $\#R = 1$ o $\#R = 2$ quedan como ejercicio para quien esté leyendo. Trabajaremos con $\#R \geq 3$.

Dado que es finito, podemos renombrarlo como $R = \{a_1,\, a_2, ..., \, a_n\}$ con $n = \#R \geq 3$ y $a_1 = 0$ el neutro aditivo. Denotaremos por $1 \neq 0$ al neutro multiplicativo, esté será alguno de los a_i.

Consideramos $\prod_{i=2}^{n} a_i$. Dado que $a_i \neq 0$ para todo $i \in [2,\, n]$, tendremos por el Lema 15.4. que $\prod_{i=2}^{n} a_i \in R \setminus \{0\}$. Dado que a los elementos le pusimos los nombres de manera arbitraria y la multiplicación es conmutativa, podemos suponer sin pérdida de generalidad que $\prod_{i=2}^{n} a_i = a_2$.

Como la multiplicación es asociativa, tendremos que $a_2 \cdot 1 = a_2 = \prod_{i=2}^{n} a_i = a_2 \left(\prod_{i=3}^{n} a_i\right)$. Como R es D.I. y $a_2 \neq 0$, el Lema 15.3. nos dice que se cumple que $1 = \prod_{i=3}^{n} a_i$. Luego, $1 = a_j \left(\prod_{i=3,\, i\neq j}^{n} a_i\right)$, y por lo tanto a_j es una unidad para todo $j \in [3, n]$.

Nota: Si $n = 3$, tendremos que $a_3 = 1$, obteniendo el mismo resultado.

Nos falta ver que a_2 sea una unidad. Para eso consideramos $a_2 \cdot a_2$. Como $a_2 \neq 0$, el Lema 15.4. nos dice que $a_2 \cdot a_2 \neq 0$.

Si $a_2 a_2 = a_2$, de nuevo ocupamos el Lema 15.3. y obtenemos que $a_2 = 1$ y por lo tanto es una unidad.

Si $a_2 a_2 = a_j$ para algún $j \in [3,\, n]$. De partida tenemos que existe $b \in R$ tal que $a_j b = 1$. Luego, $1 = a_j b = (a_2 a_2) b = a_2(a_2 b)$ y por lo tanto a_2 es una unidad.

Conlcuimos que todo elemento en $R \setminus \{0\}$ es una unidad, y como A ya era un D.I. tenemos que además es un cuerpo.

Dado que R es cualquier dominio de integridad finito, se deduce lo pedido. □

Para este ejercicio se escribirán las respuestas correspondientes al final de la guía, queda como ejercicio para quien esté leyendo.

Ejercicio 15.2. Verificar si los siguientes tríos de un conjunto y dos operaciones son anillos. De ser un anillo hay que ponerle apellido (conmutativo, unitario, etc).

a) $(\mathbb{Z},\, +,\, \cdot)$, donde las operaciones son las usuales en los enteros.

b) $(\mathbb{R},\, +,\, \cdot)$, donde las operaciones son las usuales en los reales.

c) $(\mathbb{Q},\, +,\, \cdot)$, donde las operaciones son las usuales en los racionales.

d) $(n\mathbb{Z},\, +,\, \cdot)$, donde $n \in \mathbb{N}_0$ las operaciones son las usuales en los enteros.

e) $(\mathbb{Z}/n\mathbb{Z},\, +,\, \cdot)$, donde $n \in \mathbb{N}_0$ y las operaciones son las usuales en los enteros módulo.

f) $(M_{2\times 2}(\mathbb{R}),\, +,\, \cdot)$, donde las operaciones son las usuales en las matrices con coeficientes en los reales.

g) $(M_{2\times 2}(A),\, +_M,\, \cdot_M)$, donde $(A,\, +,\, \cdot)$ es un anillo y $M_{2\times 2}(A)$ es el conjunto de matrices con coeficientes en A. Sean $a,\, b,\, c,\, d,\, x,\, y,\, z,\, w \in A$, Las operaciones están definidas mediante:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} +_M \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot_M \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}$$

h) $(S_{10}, \circ, *)$, donde la operación $\circ$ es la composición usual en las biyecciones. Y $*$ es una operación asociativa en S_{10} que se distribuye en $\circ$.

i) $(\mathbb{Z}, \cdot, \wedge)$, donde la multiplicación es la usual en los enteros. Y $\wedge$ es elevar un número a otro.

j) $(\mathbb{R}_0^+, \cdot, \wedge)$, donde la multiplicación es la usual en los reales. Y $\wedge$ es elevar un número a otro.

k) $(\mathbb{R}[x], +, \cdot)$, donde las operaciones son las usuales en los polinomios con coeficientes en los reales.

l) $(\mathbb{Z}[x], +, \cdot)$, donde las operaciones son las usuales en los polinomios con coeficientes en los enteros.

m) $(\mathbb{Z}[i], +, \cdot)$, donde $\mathbb{Z}[i] := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ y las operaciones son las usuales en los complejos.

n) $(\mathbb{Q}(i), +, \cdot)$, donde $\mathbb{Q}(i) := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ y las operaciones son las usuales en los complejos.

ñ) $(\mathbb{F}_4, +, \cdot)$, donde $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ y se cumple que:

   a) $+$ y $\cdot$ son dos operaciones bien definidas.
   b) $\cdot$ se distribuye en $+$.
   c) 0 es un neutro de $+$.
   d) 1 es un neutro de $\cdot$.
   e) $\beta = \alpha + 1 = 1 + \alpha$.
   f) $x + x = 0$ para todo $x \in \mathbb{F}_4$.
   g) $+$ es asociativa.
   h) $\cdot$ es asociativa.

o) $(\mathbb{Z}, +, *)$, donde $+$ es la suma usual en los enteros y $x * y = 0$ para todo $x, y \in \mathbb{Z}$.

p) $(\mathbb{Z}_{f=2}, +, \cdot)$, donde $\mathbb{Z}_{f=2} := \left\{\frac{a}{2^n} \in \mathbb{Q} \mid a \in \mathbb{Z}, n \in \mathbb{Z}\right\}$ y las operaciones son las usuales en los racionales.

q) $(\mathbb{Z}_{3\mathbb{Z}}, +, \cdot)$, donde $\mathbb{Z}_{3\mathbb{Z}} := \left\{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b \notin 3\mathbb{Z}\right\}$ y las operaciones son las usuales en los racionales.

r) $(\mathbb{C}, +, \cdot)$, donde las operaciones son las usuales en los complejos.

Ejercicio 15.3. Verificar en el ejercicio anterior si algún anillo es un subanillo de algún otro anillo. En general, ¿que propiedades de los anillos se heredan a los subanillos?

Demostración. Tenemos las siguientes contenciones.
d) $\subset$ a) $\subset$ p) $\subset$ q) $\subset$ c) $\subset$ b) $\subset$ r).
m) $\subset$ n) $\subset$ r).
$\mathbb{Z}/2\mathbb{Z} \subset$ ñ).
l) $\subset$ k).
Abusando un poco de la notación podemos decir que a) $\subset$ l) y que b) $\subset$ k).

Además tenemos que b) $\cong \left(\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}\right\}, +, \cdot\right) \subset$ f), donde las operaciones son las usuales en las matrices.

Después de todos esos ejemplos, las únicas propiedades que podemos afirmar que los subanillos heredan de los anillos son la conmutatividad y el no tener divisores de cero. Sean A un anillo y B un subanillo de A.
1° Si A es conmutativo, entonces $xy = yx$ para todo $x, y \in A$. Como $B \subset A$, en particular tenemos que $xy = yx$ para todo $x, y \in B$, y por lo tanto B es conmutativo.
2° Si A no tiene divisores de cero, entonces $xy \neq 0$ para todo $x, y \in A \setminus \{0\}$. Como $B \subset A$, en particular tenemos que $xy \neq 0$ para todo $x, y \in B$, y por lo tanto B no tiene divisores de cero.

Queda como ejercicio para quien esté leyendo la pregunta ¿Alguna propiedad de un subanillo puede trascender al anillo?
Ayuda: Estudiar los ejemplos del ejercicio 15.2. teniendo en cuenta las contenciones vistas en este ejercicio. □

Ejercicio 15.4. ¿Como se ven los ideales del anillo $\mathbb{Z}$ con las operaciones usuales?

Demostración. Para comenzar, sabemos que los ideales deben ser subgrupos con la suma. Luego, los ideales tendrán la forma $n\mathbb{Z}$ con $n \in \mathbb{N}_0$ debido a la ayudantía 1. La pregunta que uno se puede generar ahora es ¿Todos los conjuntos de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}_0$ son ideales? La respuesta es si, pero hay que demostrarlo.

Sea $n \in \mathbb{N}_0$ fijo. Estamos considerando el subconjunto $n\mathbb{Z}$ del anillo $\mathbb{Z}$ con las operaciones usuales.
Como $\mathbb{Z}$ es un anillo conmutativo, solo debemos verificar que $r(n\mathbb{Z}) \subset n\mathbb{Z}$ para todo $r \in \mathbb{Z}$.
Sea $r \in \mathbb{Z}$ fijo, procedamos a anotar nuestros conjuntos.

$$n\mathbb{Z} = \{x \in \mathbb{Z} \mid n \text{ divide a } x\} \tag{1}$$
$$r(n\mathbb{Z}) = \{rx \in \mathbb{Z} \mid x \in n\mathbb{Z}\} \tag{2}$$

Sea $a \in r(n\mathbb{Z})$. Por (2), $a = rx$ con $x \in n\mathbb{Z}$. Por (1), $a = rx$ tal que n divide a x. Luego, n divide a a. De (1), tenemos que $a \in n\mathbb{Z}$. Dado que a era cualquier elemento de $r(n\mathbb{Z})$, deducimos la inclusión querida.
Dado que r era cualquier entero, deducimos lo que queríamos verificar.
Dado que n era cualquier entero no negativo, concluimos que $n\mathbb{Z}$ es un ideal para todo $n \in \mathbb{N}_0$. □

Respuestas Ejercicio 15.2.

a) Dominio de integridad. Solo 1 y -1 son unidades.

b) Cuerpo.

c) Cuerpo.

d) Si $n = 0$, cuerpo. Si $n = 1$, dominio de integridad (es $\mathbb{Z}$). Si $n > 1$, es un anillo conmutativo, nada más.

e) Si n es primo, es un cuerpo. Si n no es primo, es un anillo conmutativo y unitario, nada más.

f) Solo es un anillo unitario.

g) Depende de A, mostraremos ejemplos. Si $A = \{0\} \subset \mathbb{R}$, es un cuerpo. Si $A = 2\mathbb{Z}$ es solo un anillo, no tienen ningún apellido. Si A tiene al menos dos elementos, entonces tiene divisores de cero. Si existen $a, b \in A$ tal que $a \cdot b \neq 0$ (el neutro aditivo de A), entonces no es conmutativo. Es un anillo unitario si y solo si A es un anillo unitario.

h) No es un anillo.

i) No es un anillo.

j) No es un anillo.

k) Dominio de integridad. Sus unidades son los polinomios de grado cero.

l) Dominio de integridad. Sus unidades son 1 y -1.

m) Dominio de integridad. Sus unidades son 1, -1, i y $-i$.

n) Cuerpo.

ñ) Cuerpo.

o) Anillo conmutativo, nada más.

p) Dominio de integridad.

q) Dominio de integridad.

r) Cuerpo.