Álgebra Moderna Ejercicios Clase 1

Tomás Ricardo Basile Álvarez
316617194

21 de septiembre de 2020

Ejercicio 1.9: Sea n un entero positivo.
a) Escribe las clases de congruencia módulo 12:

Como dice en el texto y se prueba en la parte b), las clases de congruencia son solamente $\overline{0}, \overline{1}, \overline{2}, ...\overline{12-1}$. Que en este caso son:

$$\begin{aligned}
\overline{0} &= \{0+12k \ : k \in \mathbb{Z}\} = \{..., -24, -12, 0, 12, 24\} \\
\overline{1} &= \{1+12k \ : k \in \mathbb{Z}\} = \{..., -23, -11, 1, 13, 25\} \\
\overline{2} &= \{2+12k \ : k \in \mathbb{Z}\} = \{..., -22, -10, 2, 14, 26\} \\
\overline{3} &= \{3+12k \ : k \in \mathbb{Z}\} = \{..., -21, -9, 3, 15, 27\} \\
\overline{4} &= \{4+12k \ : k \in \mathbb{Z}\} = \{..., -20, -8, 4, 16, 28\} \\
\overline{5} &= \{5+12k \ : k \in \mathbb{Z}\} = \{..., -19, -7, 5, 17, 29\} \\
\overline{6} &= \{6+12k \ : k \in \mathbb{Z}\} = \{..., -18, -6, 6, 18, 30\} \\
\overline{7} &= \{7+12k \ : k \in \mathbb{Z}\} = \{..., -17, -5, 7, 19, 31\} \\
\overline{8} &= \{8+12k \ : k \in \mathbb{Z}\} = \{..., -16, -4, 8, 20, 32\} \\
\overline{9} &= \{9+12k \ : k \in \mathbb{Z}\} = \{..., -15, -3, 9, 21, 33\} \\
\overline{10} &= \{10+12k \ : k \in \mathbb{Z}\} = \{..., -14, -2, 10, 22, 34\} \\
\overline{11} &= \{11+12k \ : k \in \mathbb{Z}\} = \{..., -13, -1, 11, 23, 35\}
\end{aligned}$$

.
b) Prueba que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ...\overline{n-1}\}$

$\subset$) : Sea $\overline{a} \in \mathbb{Z}_n$ con $a \in \mathbb{Z}$. Entonces, por definición de la clase de equivalencia tenemos que:

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} \ : a \equiv b\} \\
&= \{b \in \mathbb{Z} : n|(a-b)\} \ \text{ Por la definición de } \ a \equiv b
\end{aligned}$$

Luego, $n|(a-b)$ sii $\exists k \in \mathbb{Z}$ tal que $kn = a - b$ sii $\mathbf{b = a + kn}$
Y así, el conjunto $\overline{a}$ se ve como: $\overline{a} = \{a + kn : k \in \mathbb{Z}\}$ (1)
Luego, usamos el algoritmo de la división para a entre n y nos asegura que existen $r, q \in \mathbb{Z}$

tales que $a = qn + r$ y $\quad 0 \leq r < n$.
Entonces, $r = a - qn$ y por tanto:

$$\begin{aligned}
\overline{r} &= \{r + k'n : k' \in \mathbb{Z}\} \text{ por el mismo argumento con el se llega a (1)} \\
&= \{a - qn + k'n : k' \in \mathbb{Z}\} \\
&= \{a + (k' - q)n : k' \in \mathbb{Z}\} \\
&= \{a + kn : k \in \mathbb{Z}\} = \overline{a} \text{ por (1)}
\end{aligned}$$

El anteúltimo paso se justifica porque $k' - q$ varía sobre los enteros porque $k', q \in \mathbb{Z}$ y entonces se puede reemplazar por simplemente k que varíe sobre los enteros.
Así, $\overline{a} = \overline{r}$ para una r con $0 \leq r < n$ (por el algoritmo de la división) lo que prueba que $\overline{a}$ es uno de los elementos en $\{\overline{0}, \overline{1}, \overline{2}, ...\overline{n-1}\}$ y entonces $\mathbb{Z}_n \subset \{\overline{0}, \overline{1}, \overline{2}, ...\overline{n-1}\}$.

Por otro lado, si $\overline{r} \in \{\overline{0}, \overline{1}, \overline{2}, ...\overline{n-1}\}$, entonces es $\overline{r}$ es una clase de equivalencia módulo n y entonces pertenece a $\mathbb{Z}_n$. Por lo que $\{\overline{0}, \overline{1}, \overline{2}, ...\overline{n-1}\} \subset \mathbb{Z}_n$.
Y finalmente concluimos que estos dos conjuntos son iguales.

c) ¿Cuál es la clase de congruencia de 10^k módulo 3?

10^k se puede escribir como $9 \times 10^{k-1} + 9 \times 10^{k-2} + ... + 9 \times 10^1 + 9 + 1 = 3 \times (3 \times 10^{k-1} + 3 \times 10^{k-2} + ... + 3 \times 10^1 + 3) + 1$
Es decir, se puede escribir como un entero multiplicado por 3 más 1. Entonces, 10^k tiene un residuo de 1 al dividirlo por 3 y por tanto es congruente a 1 módulo 3. Entonces, la clase de equivalencia de 10^k es igual a la clase de equivalencia de 1.

d) Pruebe que si $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_k \cdot 10^k$, entonces la clase de congruencia de a módulo 9 es $\overline{a_0 + a_1 + ... + a_k}$

Tenemos que probar que a y $a_0 + a_1 + a_2 + ... + a_k$ son congruentes módulo 9 para probar que entonces pertenecen a la misma clase de congruencia que se puede representar como $\overline{a_0 + a_1 + a_2 + ... + a_k}$.
Entonces, debemos de demostrar que $a \equiv (a_0 + a_1 + a_2 + ... + a_k)$ módulo 9, o lo que es lo mismo, probar que $9|a - (a_0 + a_1 + a_2 + ... + a_k)$
Pero $a - (a_0 + a_1 + a_2 + ... + a_k) = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_k \cdot 10^k - (a_0 + a_1 + a_2 + ... + a_k) = 9a_1 + 99a_2 + 999a_3 + ... + 99...99a_k = 9(a_1 + 11a_2 + 111a_3 + ... + 11...11a_k)$
Este último número es claramente un múltiplo de 9, por lo que $a - (a_0 + a_1 + a_2 + ... + a_k)$ es un múltiplo de 9 y queda probado que $9|a - (a_0 + a_1 + a_2 + ... + a_k)$.

e) Sea $n = mk$. Prueba que $\overline{m} \cdot \overline{k} = \overline{0}$ en $\mathbb{Z}_n$

Por como se define el producto en $\mathbb{Z}_n$, tenemos que:

$$\begin{aligned}
\overline{m} \cdot \overline{k} &= \overline{mk} \\
&= \overline{n} \\
&= \overline{0}
\end{aligned}$$

En el último paso, probar que $\overline{n} = \overline{0}$ es fácil, pues $n \equiv 0$ módulo n ya que claramente $n|(n-0)$. Luego, como n es congruente con 0 entonces $n \in \overline{0}$ pero por reflexividad de la relación de congruencia, se tiene también que $n \in \overline{n}$. Y como dos clases de equivalencia o son disjuntas o son iguales, concluimos que éstas son iguales y entonces $\overline{0} = \overline{n}$.

f) Pruebe que $\mathbb{Z}_n$ es un anillo:

Primero probamos un resultado preliminar: para $x, x' \in \mathbb{Z}$, se cumple que $\overline{x} = \overline{x'}$ sii $x' = x + kn$ para k entero.
Pues si $\bar{x} = \bar{x'}$ entonces como $x \in \{x + qn : q \in \mathbb{Z}\} = \overline{x} = \bar{x'} = \{x' + kn : k \in \mathbb{Z}\}$ entonces $x = x' + kn$ para algún k entero.
Por otro lado, si $x' = x + kn$, entonces como $n|kn \Rightarrow \ n|(x' - x) \ \Rightarrow \ x' \equiv x$. Pero entonces, x pertenece a la clase de equivalencia $\bar{x'}$ pero también pertenece a su propia clase de equivalencia por reflexividad. Como dos clases de equivalencia o son disjuntas o son iguales, concluimos que son iguales concluimos que $\bar{x} = \bar{x'}$

Suma (como se define en el texto):
1) Probar que está bien definida: Sea $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$, para $a, a', b, b' \in \mathbb{Z}$ entonces, por el resultado preliminar, existen k, q enteros tales que: $a = nk + a'$ y $b = nq + b'$ y luego:

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{(nk + a') + (nq + b')} = \overline{n(k + q) + (a' + b')} = \overline{a' + b'} = \overline{a'} + \overline{b'}$$

Donde en el penúltimo paso se usó también el resultado preliminar.
2) Asociativa:

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

3) Conmutatividad:

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

4) Neutro: El neutro aditivo es $\overline{0}$ pues:

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$$

5) Inverso: Para $\overline{a} \in \mathbb{Z}_n$, su inverso es $\overline{-a} \in \mathbb{Z}_n$ pues:

$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$$

.
Producto:
1) Probar que está bien definida: Sea $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$, para $a, a', b, b' \in \mathbb{Z}$ entonces, existen k, q tales que:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{(nk + a')(nq + b')} = \overline{n(nkq + kb' + qa') + a'b'} = \overline{a'b'} = \overline{a'} \cdot overline b'$$

Donde se usó múltiples veces el resultado preliminar de la misma forma que en la suma.
2) Asociativa:

$$(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{a\cdot b}\cdot\overline{c}=\overline{(a\cdot b)\cdot c}=\overline{a(bc)}=\overline{a}\cdot\overline{bc}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$$

3. Neutro: El neutro multiplicativo es $\overline{1}$ pues:

$$\overline{a}\cdot\overline{1}=\overline{a\cdot 1}=\overline{a}=$$
$$\overline{1}\cdot\overline{a}=\overline{1\cdot a}=\overline{a}$$

4. Conmutatividad (si se quiere probar que es un anillo conmutativo):

$$\overline{a}\cdot\overline{b}=\overline{ab}=\overline{ba}=\overline{b}\cdot\overline{a}$$

Distributividad:

$$\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{(b+c)}=\overline{a(b+c)}=\overline{ab+ac}=\overline{ab}+\overline{ac}=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$$
$$(\overline{b}+\overline{c})\cdot\overline{a}=\overline{(b+c)}\cdot\overline{a}=\overline{(b+c)a}=\overline{ba+ca}=\overline{ba}+\overline{ca}=\overline{b}\cdot\overline{a}+\overline{c}\cdot\overline{a}$$

.

g) Muestra un ejemplo donde $\mathbb{Z}_n$ no es un campo:

El ejemplo que daré es $\mathbb{Z}_4$. Para ser un campo, todos los elementos tienen que tener un inverso multiplicativo. Pero $\overline{2}\in\mathbb{Z}_4$ no lo tiene. Podemos ver esto al ir probando con todos los elementos de $\mathbb{Z}_4$:
a) $\overline{0}$ no es el inverso de $\overline{2}$ pues: $\overline{0}\cdot\overline{2}=\overline{0\cdot 2}=\overline{0}\neq\overline{1}$
b) $\overline{1}$ no es el inverso de $\overline{2}$ pues: $\overline{1}\cdot\overline{2}=\overline{1\cdot 2}=\overline{2}\neq\overline{1}$
c) $\overline{2}$ no es el inverso de $\overline{2}$ pues: $\overline{2}\cdot\overline{2}=\overline{2\cdot 2}=\overline{4}=\overline{0}\neq\overline{1}$
d)$\overline{3}$ no es el inverso de $\overline{2}$ pues: $\overline{3}\cdot\overline{2}=\overline{3\cdot 2}=\overline{6}=\overline{2}\neq\overline{1}$

h) Muestra un ejemplo donde $\mathbb{Z}_n$ es un campo

Lo probaré para $\mathbb{Z}_2$. En la parte f) ya se probó que en $\mathbb{Z}_n$ la suma es conmutativa, asociativa, con neutro y con inverso, que el producto es conmutativo, asociativo, y con neutro y que las operaciones son distributivas.
Ya solo falta probar que los elementos distintos al cero (que en este caso es $\overline{0}$) tienen inverso multiplicativo. El único elemento de $\mathbb{Z}_n$ distinto de $\overline{0}$ es $\overline{1}$ y su inverso es $\overline{1}$ pues: $\overline{1}\cdot\overline{1}=\overline{1\cdot 1}=\overline{1}$

i) Un entero m es primo relativo de n si $(n,m)=1$. Muestra que m es primo relativo a n si y sólo si $\overline{m}$ es invertible en Z_n:

Ida) Por la identidad de Bezout, existen enteros x,y tales que:

$$nx+my=(m,n)$$

Luego, por hipótesis tenemos que $nx+my=1$.
Por lo tanto:

$$\overline{nx+my}=\overline{1}$$
$$\Rightarrow\quad\overline{my}=\overline{1}$$

Esto es porque $\overline{nx+my} = \overline{my}$. Pues $\overline{my} = \{my + kn \ : k \in \mathbb{Z}\} = \{my + nx + (k-x)n \ : k \in \mathbb{Z}\} = \{my + nx + k'n : \ k' \in \mathbb{Z}\}$.
Donde definimos $k' = k - x$ y notamos que si k varía en $\mathbb{Z}$ entonces $k - x = k'$ también varía en $\mathbb{Z}$ porque $x \in \mathbb{Z}$.
Luego, este último conjunto es $\{my + nx + k'n : \ k' \in \mathbb{Z}\} = \overline{my + nx}$.

Entonces, la igualdad a la que llegamos $\overline{my} = \overline{1}$ nos dice que $\overline{m} \cdot \overline{y} = \overline{1}$ y así, el inverso de $\overline{m}$ es $\overline{y}$.

Regreso) Digamos que $\overline{m}$ es invertible en $\mathbb{Z}_n$ y esperando una contradicción, supongamos que n, m no son coprimos. Entonces, existe un $d > 1$ que es factor de tanto m como n. Es decir, existen a, b enteros tales que $m = da$ (1) y $n = db$ (2).

Pero como $\overline{m}$ es invertible, existe su inverso $\overline{p}$ tal que $\overline{mp} = \overline{1}$
Entonces, en particular $pm \equiv 1$ módulo n, lo que implica que $n|(pm-1)$ y por tanto existe una $k \in \mathbb{Z}$ tal que $kn = (pm - 1) \ \Rightarrow \ pm = kn + 1$
Entonces, usando (1) y (2) para reemplazar m y n tenemos que $pda = kdb + 1$
Por tanto, $d(pa - kb) = 1$.
Como todas las cantidades aquí son enteras, esto implica que $d = \pm 1$ lo cual contradice la suposición inicial de que d era un factor mayor que 1 compartido por m y n.

Ejercicio 1.10: Sea n un entero positivo.
a) Prueba que la suma y el producto en $\mathbb{Z}_n$ están bien definidos:

Ya lo probé en el inciso f de la pregunta anterior antes de probar que $\mathbb{Z}_n$ es un anillo.

Prueba que $\mathbb{Z}_n$ es un grupo abeliano con la suma:

En la pregunta anterior inciso f) ya probé que la suma es cerrada, asociativa, tiene neutro, inverso y es conmutativa, con lo que se prueba que $(\mathbb{Z}_n, +)$ es un grupo.

c) Prueba que $\mathbb{Z}_n - \{0\}$ es un grupo abeliano con el producto si n es primo.

En el inciso f de la pregunta anterior ya probé que el producto es cerrado, asociativo, tiene neutro y es conmutativo.
Solo falta probar que los elementos tienen inverso. Para esto, sea $\overline{m} \in \mathbb{Z}_n$.
Luego, como n es primo, se cumple uno de los siguientes casos:

1) m y n son coprimos: En este caso, se probó en el inciso i del ejercicio pasado que $\overline{m}$ tiene inverso.
2) m es múltiplo de n: Es decir, $m = kn$ para algún $k \in \mathbb{Z}$ en este caso, $\overline{m} = \overline{n}$, pero $\overline{n} = \overline{0}$. Entonces $\overline{m} = \overline{0}$. Pero entonces, esta $\overline{m}$ no pertenece al conjunto, ya que el conjunto en cuestión es $\mathbb{Z}_n - \{0\}$. Por lo que no hace falta buscarle un inverso multiplicativo (que no tiene) porque ni está en el conjunto.

d) Sea $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n | (a,n) = 1\}$. Prueba que $\mathbb{Z}_n^*$ es un grupo abeliano con el producto.

Probamos primero que el producto es cerrado: Sea $\overline{a}, \overline{b} \in \mathbb{Z}_n^*$. Entonces, queremos probar que $\overline{a}\overline{b} = \overline{ab}$ está también en $\mathbb{Z}_n^*$.
Para esto, tiene que cumplir la condición que $(ab, n) = 1$. Lo cual es una consecuencia directa de que $(a, n) = 1$ y $(b, n) = 1$.
Pues si $(a, n) = 1$ entonces a no comparte factores primos con los factores primos de n. Y similarmente como $(b, n) = 1$, b no comparte factores primos con los de n. Por tanto, como el producto ab tiene los factores primos de a y los de b, ninguno de estos está compartido con los de n y entonces ab no comparte factores primos con n y por tanto $(ab, n) = 1$.

e) Muestra que $\mathbb{Z}_n$ no es un grupo con el producto si $n > 1$.

Consideremos $\overline{0} \in \mathbb{Z}_n$. Probamos que este elemento no tiene un inverso multiplicativo en $\mathbb{Z}_n$. Pues para todo $\overline{a} \in \mathbb{Z}_n$ se cumple que:

$$\overline{0}\overline{a} = \overline{0 \cdot a} = \overline{0} \neq \overline{1}$$

Usamos que $n > 1$ al indicar que $\overline{0} \neq \overline{1}$ pues el conjunto tiene por lo menos estos dos elementos y son distintos entre sí.