TEMA 2.

1. INTRODUCCIÓN

En este tema vamos a estudiar más en profundidad los anillos de integridad: recordamos que dado un anillo R, un elemento no nulo $a \in R$ se dice que es un **divisor de cero por la izquierda** si existe un elemento no nulo $b \in R$ tal que $a.b = 0$. De manera análoga se define **divisor de cero por la derecha**. Un **dominio de integridad** es un anillo conmutativo y unitario sin divisores de cero.

Como primer resultado obtendremos que los dominios de integridad son precisamente los anillo R en los que las ecuaciones $aX + b = 0$ y $Xa + b = 0$, con $a, b \in R$, caso de tener solución, está es única (esto no es más que otra forma de expresar las leyes de cancelación).

Observamos que los anillos de división son precisamente los anillos en los que estas ecuaciones tienen solución única.

Como último resultado de la sección demostraremos que todo dominio de integridad finito es cuerpo. Para finalizar el tema, demostraremos el Teorema (pequeño) de Fermat y una generalización de este, el teorema de Euler.

Nos harán falta los siguientes resultados (todos ellos visto en el primer cuatrimestre):

- ⋆ Toda aplicación inyectiva de un conjunto finito en si mismo es biyectiva.
- ⋆ Algoritmo de la división.
- ⋆ Nociones de divisibilidad. Los números primos.
- ⋆ Factorización de números enteros.
- ⋆ El máximo común divisor. El teorema de Bezout.
- ⋆ El mínimo común múltiplo.

2. PRIMERAS PROPIEDADES

2.1 Def. Diremos que un anillo R verifica la ley de cancelación por la izquierda si dados $a, b, c \in R$ con $c \neq 0$, $ca = cb$ entonces $a = b$. Diremos que un

anillo R verifica la ley de cancelación por la derecha si dados $a, b, c \in R$ con $c \neq 0$, $ac = bc$ entonces $a = b$.

2.2 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R verifica la ley de cancelación por la izquierda.

(ii) R no tiene divisores de cero por la derecha.

(iii) R no tiene divisores de cero por la izquierda.

(iv) R verifica la ley de cancelación por la derecha.

Nota: A partir de ahora hablaremos de anillos que verifican la ley de cancelación y anillos sin divisores de cero.

Nota: Todo dominio de integridad y todo anillo de división (en particular todo cuerpo) verifica la ley de cancelación.

2.3 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero.

(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, las ecuaciones $aX + b = 0$ y $Xa + b = 0$, si poseen solución, ésta es única.

2.4 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R es un anillo de división.

(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, las ecuaciones $aX + b = 0$ y $Xa + b = 0$, poseen solución única.

2.5 Teorema. Todo dominio de integridad finito es cuerpo.

Demo: Sea D un dominio de integridad finito y $0 \neq a \in D$. Veamos que a es un elemento inversible de D. Consideremos la aplicación

$$\phi_a : D \to D \quad \text{definida por} \quad \phi_a(x) = ax.$$

Como D verifica la ley de cancelación por la izquierda, ϕ_a es una aplicación inyectiva y como D es finito, ϕ_a es sobreyectiva. Por tanto, existe $b \in D$ con $ab = 1$. Por último, como D es conmutativo $ab = ba = 1$ y a es inversible con inverso b. ■

Nota: Hemos demostrado un poco más:

⋆ Un anillo unitario y finito sin divisores de cero por la derecha (o por la izquierda) es un cuerpo: por la demostración anterior dado $a \in R$ existe $b \in R$ con $ab = 1$. Si repetimos el proceso para b, existe $c \in R$ con $bc = 1$. Pero entonces $a = a(bc) = (ab)c = c$ lo que demuestra que $a = c$ es un inverso para b en D, o lo que es lo mismo, que a es inversible con inverso b.

⋆ Si R es un anillo finito y unitario y $a \in R$ es un elemento que no es divisor de cero por la izquierda, entonces existe $b \in R$ con $ab = 1$. Si además a no es divisor de cero por la derecha, a es inversible (tomamos la aplicación $\rho_a(b) = ba$ y repetimos el argumento.

3. RECUERDO DEL PRIMER CUATRIMESTRE

Vamos a trabajar con $\mathbb{Z}$, el anillo de los enteros y su orden usual (recordamos que $(\mathbb{N}, \leq)$ es un conjunto bien ordenado: todo subconjunto no vacio de $\mathbb{N}$ posee un mínimo).

3.1 Algoritmo de la división. Dados $m, d \in \mathbb{Z}$, con $d > 0$, existen dos únicos elementos $c, r \in \mathbb{Z}$, con $0 \leq r < d$, tales que $m = cd + r$.

Nota: Se considera el conjunto $\{m - td \mid t \in \mathbb{Z} \text{ y } m - td > 0\}$. Se demuestra que es no vacio y se toma como r es mínimo en este conjunto. Posteriormente se demuestra la unicidad. ■

3.2 Def. Sean $n, m \in \mathbb{Z}$. Diremos que n divide a m (o que m es múltiplo de n) si existe $r \in \mathbb{Z}$ tal que $m = nr$.

3.3 Def. Sean $n, m \in \mathbb{Z}$ no nulos. Se define el máximo común divisor de m y n y se representa por $mcd(n, m)$ como un $d \in \mathbb{Z}$ tal que:

(i) $d > 0$.

(ii) d divide a n y a m.

(iii) Si a divide a n y a m, entonces a divide a d.

Nota: No hay que ser crédulo, hay que demostrar que este número siempre existe.

3.4 Def:. Sean $n, m \in \mathbb{Z}$ no nulos. Se define el mínimo común múltiplo de m y n y se representa por $MCM(n, m)$ como un $D \in \mathbb{Z}$ tal que:

(i) $D > 0$.

(ii) n y m dividen a D.

(iii) Si n y m dividen a a, entonces D divide a a.

Nota: Lo mismo de antes.

3.5 Teorema de Bezout. Sean $n, m \in \mathbb{Z}$ no nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que $mcd(n, m) = xn + ym$.

3.6 Def:. Se dice que $p \in \mathbb{Z}$ es un número primo si $p \geq 2$ y los únicos divisores de p son $\pm 1, \pm p$.

3.7 Teorema. Sea p un número primo de $\mathbb{Z}$ y sean $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, con $k \in \mathbb{N}$. Entonces, si p divide a $\Pi_{i=1}^{k} n_i$, existe $s \in \{1, \ldots, n\}$ tal que p divide a n_s.

3.8 Teorema de factorización. Sea $n \in \mathbb{Z}$ con $n > 1$. Entonces n se puede escribir de forma única (salvo permutación) como producto de primos.

3.9 Teorema. Sean $n, m \in \mathbb{Z}$ no nulos. Entonces

$$mcd(n, m)MCM(n, m) = nm$$

4. ALGUNOS RESULTADOS EN TEORíA DE NÚMEROS

4.1 Proposición. Sea $n \in \mathbb{N}$. Entonces $\bar{a} \in \mathbb{Z}_n$ es divisor de cero si y sólo si $m.c.d(a, n) \neq 1$ si y solo si $\bar{a}$ no es inversible. Por tanto, $\mathbb{Z}_n$ es un cuerpo si y sólo si n es un número primo.

Demo: Sea $a \in \mathbb{Z}$. Supongamos en primer lugar que $mcd(n, a) = 1$. Entonces, por la igualdad de Bezout existen $x, y \in \mathbb{Z}$ tales que $xa + yn = 1$. Si miramos esta igualdad en $\mathbb{Z}_n$ lo que obtenemos es: $\bar{1} = \overline{xa + yn} = \bar{x}\bar{a} + \bar{y}\bar{n} = \bar{x}\bar{a}$ y por tanto $\bar{a}$ es un elemento inversible de $\mathbb{Z}_n$, por lo que no es divisor de cero. Si $mcd(a, n) = d \neq 1$, entonces $a = da'$, $n = dn'$ con $n' < n$. Por tanto $\bar{0} \neq \bar{n}' \in \mathbb{Z}_n$ y $\bar{a}\bar{n}' = \overline{da'n'} = \overline{a'n} = 0$, con lo que a es divisor de cero y no es inversible. ■

4.2 Teorema de Fermat. Sea p un número primo y $a \in \mathbb{Z}$ tal que p no divide a a. Entonces $a^{p-1} \equiv 1$ (mod p).

Demo: Consideremos $(\mathcal{U}(\mathbb{Z}_n), \ )$ el grupo de los elementos inversibles de $\mathbb{Z}_n$. Tenemos entonces, por un lado, que $\#U = p - 1$ y por otro que si p no divide a

a, $mcd(p,a) = 1$ y $a \in \mathcal{U}(\mathbb{Z}_n)$. luego por el Teorema de Lagrange, $\bar{a}^{p-1} = \bar{1}$ en $\mathcal{U}(\mathbb{Z}_n)$, o lo que es lo mismo, $a^{p-1} \equiv 1(mod(p))$. ■

4.3 Corolario. Sea $p \in \mathbb{Z}$ primo y $a \in \mathbb{Z}$. Entonces $a^p \equiv a$ (mod p).

4.4 Def. Se define la función de Euler como la aplicación $\phi : \mathbb{N} \to \mathbb{N}$ definida por

$$\phi(n) := \#\{a \in \mathbb{N} \mid a < n \text{ y } m.c.d(a,n) = 1\}$$

4.5 Teorema de Euler. Sea $a, n \in \mathbb{N}$ tales que $m.c.d(a,n) = 1$. Entonces $a^{\phi(n)} \equiv 1$ (mod n).

Demo: Análoga al teorema de Fermat. ■

5. BIBLIOGRAFíA

⋆ **J. B. Fraleigh**, "A First Course in Abstract Algebra". Addison-Wesley Publishing Company (1982).

⋆ **W. Keith Nicholson**, "Introduction to Abstract Algebra". J. Wesley & Sons Publishing Company (1999).