TEMA 6.

1. INTRODUCCIÓN

Hemos estudiado a lo largo del curso dos anillos de integridad: $\mathbb{Z}$, el anillo de los enteros, y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo, el anillo de polinomios con coeficientes en un cuerpo, que además de ser dominios de integridad tienen una propiedad muy curiosa: todo elemento se escribe "de forma única" como producto de "primos". En este tema vamos a estudiar dominios de integridad con esta propiedad, los dominios de factorización única.

2. DEFINICIONES

2.1 DEF. Sea D un dominio de integridad. Se dice que $u \in D$ es una unidad si u es un elemento inversible de D. Dados $a, b \in D$. Se dice que a divide a b y se representa $a|b$ si existe $c \in D$ tal que $b = ac$.

2.2 PROPIEDADES. Sea D un dominio de integridad y sean $a, b, c \in D$. Entonces:

(i) $a|a$.

(ii) Si $a|b$ y $b|c$, entonces $a|c$.

(iii) Si $a|b$ y $a|c$, entonces $a|xb + yc$ para todo $x, y \in \mathbb{Z}$.

2.3 PROPOSICIÓN. Sea D un dominio de integridad y sean $a, b \in D$. Las siguientes condiciones son equivalentes:

(i) $a|b$ y $b|a$.

(ii) Existe $u \in D$ una unidad tal que $a = ub$.

(iii) $Da = Db$ (El ideal generado por a coincide con el ideal generado por b).

Si a, b verifican las condiciones anteriores, se dice que a y b son asociados y se representa por $a \sim b$.

2.4 COROLARIO. Sea D un dominio de integridad. Entonces la relación $\sim$ es de equivalencia.

2.5 Def. Sea D un dominio de integridad. Se dice que un elemento $p \in D$ es irreducible si:

(i) p no es una unidad ni es cero.

(ii) Si $p = ab$ con $a, b \in D$, entonces a o b es una unidad de D.

2.6 Ejemplo. Los números primos de $\mathbb{Z}$ o los polinomios irreducibles de $\mathbb{F}[\mathbb{X}]$, con $\mathbb{F}$ un cuerpo, son irreducibles.

2.7 Teorema. Sea D un dominio de integridad y sea $0 \neq p \in D$ que no es unidad. las siguientes condiciones son equivalentes:

(i) p es irreducible.

(ii) Si $d|p$, entonces d es inversible o $d \sim p$.

(iii) Si $p = ab$ entonces $p \sim a$ o $p \sim b$.

2.8 Corolario. Sea D un dominio de integridad y sean $a, b \in D$ con a irreducible. Entonces si $b \sim a$, b es irreducible.

2.9 Def. Se dice que un dominio de integridad verifica la condición de cadena ascendente (C.C.A.) para sus ideales principales si toda cadena de ideales principales,

$$Da_1 \subset Da_2 \subset \cdots \subset Da_n \subset \cdots$$

es estacionaria. Es decir, existe $k \in \mathbb{N}$ tal que $Da_k = Da_{k+s}$ para todo $s \in \mathbb{N}$.

2.10 Teorema. Sea D un dominio de integridad que satisface C.C.A. para sus ideales principales. Entonces todo elemento de D se puede escribir como producto de elementos irreducibles.

3. DOMINIOS DE FACTORIZACIÓN ÚNICA (DFU)

3.1 Def. Se dice que un dominio de integridad D es un dominio de factorización única si para todo elemento no nulo $a \in D$, con a no inversible se tiene:

(i) a se factoriza como producto de irreducibles.

(ii) Si $a = p_1 \cdots p_r = q_1, \cdots q_s$ con p_i, q_i irreducibles, entonces $r = s$ y existe $\sigma \in S_r$ (el grupo de permutaciones con r elementos) tal que p_i es asociado a $q_{\sigma(i)}$ para $i = 1, 2, \ldots, r$.

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ son DFU.

3.2 Def. Sea D un dominio de integridad. Se dice que un elemento $p \in D$ es primo si para todo par de elementos $a, b \in D$, si $p|ab$ entonces $p|a$ o $p|b$.

3.3 Lema. Sea D un dominio de integridad y sean $p, a_1, \ldots, a_n \in D$. Supongamos que p es primo y divide a $a_1 a_2 \cdots a_n$. Entonces existe $k \in \{1, 2, \ldots, n\}$ tal que $p|a_k$.

3.4 Teorema. En un dominio de integridad D los elementos primos son irreducibles. Es más, si D es un DFU, se tiene el recíproco.

3.5 Teorema. Sea D un dominio de integridad. Las siguientes condiciones son equivalentes:

(i) D verifica CCA y todo elemento irreducible de D es primo.

(ii) D es un DFU.

3.6 Proposición. Sea D un dominio de factorización única. Sea $a \in D$ que factoriza como producto de primos $a = p_1^{n_1} \cdots p_k^{n_k}$, con $n_i \in \mathbb{N}$. Entonces los divisores de a, salvo asociados, son de la forma $p_1^{m_1} \cdots p_k^{m_k}$, con $m_i \leq n_i$.

3.7 Def. Sea D un DFU. y sean $a_1, a_2, \ldots, a_n \in D$.

$\star$ Se define el máximo común divisor de $a_1, \ldots, a_n$ y se representa por

$$m.c.d(a_1, a_2, \ldots, a_n)$$

a cualquier $d \in D$ con las siguientes propiedades:

(i) $d|a_i$ para $i = 1, 2, \ldots, n$.

(ii) Si $r|a_i$ para $i = 1, 2, \ldots, n$, entonces $r|d$.

$\star$ Se define el mínimo común múltiplo $a_1, \ldots, a_n$ y se representa por

$$M.C.M(a_1, a_2, \ldots, a_n)$$

a cualquier $d' \in D$ con las siguientes propiedades:

(i) $a_i|d$ para $i = 1, 2, \ldots, n$.

(ii) Si $a_i|r$ para $i = 1, 2, \ldots, n$, entonces $d|r$.

$\star$ Es fácil de demostrar que el máximo común divisor y el mínimo común múltiplo, si existe, son únicos salvo asociados.

3.8 Teorema. Sea D un dominio de factorización única y sean $a_1, \ldots, a_n \in D$ no nulos ni unidades. Sean $p_1, \ldots, p_k$ elementos primos de D tales que para cada $i \in \{1, \ldots, n\}$, $a_i = p_1^{n_1^i} \cdots p_k^{n_k^i}$. Entonces:

(i) $m.c.d(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes con el menor exponente.

(ii) $M.C.M(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes y no comunes con el mayor exponente.

Por tanto, dados $a, b \in D$ no nulos ni unidades,

$$a\ b = m.c.d(a, b)\ M.C.M(a, b).$$

Nota: El teorema de Bezout no se tiene que verificar para DFU.

3.9 Teorema. Si D es un DFU, entonces $D[X]$ es un DFU.

4. DOMINIOS DE IDEALES PRINCIPALES (DIP)

Sea D un dominio de integridad, o más generalmente, sea D un anillo conmutativo y unitario. Sabemos entonces que dado $a \in D$ el ideal generado por a es Da. (en un anillo arbitrario R es $< a >= RaR + Ra + aR + \mathbb{Z}a$).

Nota: Durante esta sección denotaremos indistintamente al ideal generado por a como Da o $< a >$.

4.1 Def. Se dice que un dominio de integridad D es un dominio de ideales principales (DIP) si todo ideal de D es principal, es decir, si I es un ideal de D, existe $a \in I$ tal que $I = Da$.

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo son dominios de ideales principales: Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para $n \in \mathbb{N}$ y si I es un ideal de $\mathbb{F}[X]$ y $p(x)$ es un polinomio de I con grado mínimo, entonces $I =< p(x) >$.

4.2 Proposición. Todo DIP verifica CCA para sus ideales.

4.3 Proposición. En un DIP los elementos irreducibles son primos.

4.4 Teorema. Todo DIP es un DFU.

4.5 Proposición. Sea D un DIP y sean $a_1, \ldots, a_n \in D$ no nulos ni inversibles. Entonces:

(i) $d = m.c.d(a_1, \ldots, a_n)$ si y sólo si $Da_1 + Da_2 + \cdots + Da_n = Dd$.

(i) $d = M.C.M(a_1, \ldots, a_n)$ si y sólo si $Da_1 \cap Da_2 \cap \cdots \cap Da_n = Dd$.

Nota: Como corolario de (i) se obtiene el teorema de Bezout para DIP (recordamos que no era cierto para DFU).

4.6 Teorema. Sea D un DIP y sea $0 \neq p \in D$. Las siguientes condiciones son equivalentes:

(i) p es primo (que es lo mismo que irreducible).

(ii) Dp es un ideal maximal de D.

(iii) D/Dp es un cuerpo.

(iv) D/Dp es un dominio de integridad.

(v) Dp es un ideal primo de D.

4.7 Corolario. Si D es un DIP y I es un ideal no nulo de D, I es un ideal primo si y sólo si es maximal.

Nota: en un dominio de integridad D, el ideal nulo es siempre primo y no tiene que ser maximal (sólo es maximal si D es un cuerpo).

5. DOMINIOS EUCLíDEOS

Cuando trabajamos con $\mathbb{Z}$ o con $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$, demostramos que verificaban el "algoritmo de la division". En esta sección vamos a estudiar dominios de integridad en los que existe, en cierta forma, un algoritmo de la división.

5.1 Def. Sea D un dominio de integridad. Se dice que D es un dominio euclídeo (DE) si existe una función $\delta : D^* \to \mathbb{N}^*$ tal que:

(i) dados $a, b \in D$ con $b \neq 0$ existe $c, r \in D$ tales que $a = cb + r$ en donde $r = 0$ o $\delta(r) < \delta(b)$.

(ii) para todo par de elementos no nulos $a, b \in D$, $\delta(a) \leq \delta(ab)$.

Nota: $\mathbb{Z}$ es un dominio euclídeo en donde δ es el valor absoluto y $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$ es dominio euclídeo en donde δ es la función grado.

5.2 Teorema. Todo DE es un DIP.

5.3 Teorema. En DE se verifica el algoritmo euclídeo. Es decir,

$\star$ dados $a, b \in D$ no nulos, si $a = cb + r$, entonces $m.c.d(a, b) = m.c.d(b, r)$

Por tanto, la función Euclídea permite un método recursivo para calcular el máximo común divisor de dos elementos no nulos:

Sean a, b dos elementos no nulos de un dominio Euclídeo D. Aplicacos el algoritmo de la división a a, b

$$\begin{aligned}
a = c_1 b + r_1 \qquad & \text{Si} \quad r_1 \neq 0, \quad \delta(r_1) < \delta(b) \\
b = c_2 r_1 + r_2 \qquad & \text{Si} \quad r_2 \neq 0, \quad \delta(r_2) < \delta(r_1) \\
r_1 = c_3 r_2 + r_3 \qquad & \text{Si} \quad r_3 \neq 0, \quad \delta(r_3) < \delta(r_2) \\
& \vdots \\
r_n = c_3 r_{n+1} + r_{n+2} \qquad & \text{Si} \quad r_{n+2} \neq 0, \quad \delta(r_{n+2}) < \delta(r_{n+1})
\end{aligned}$$

Como $\delta(b) > \delta(r_1) > \cdots > \delta(r_n) > \cdots$, existe un k tal que $r_k = 0$. Para este k se tiene que $r_{k-2} = c_k r_{k-1}$ y por la propiedad $\star$

$$m.c.d(a, b) = m.c.d(b, r_1) = \cdots = m.c.d(r_{k-2}, r_{k_1}) = m.c.d(c_k r_{k-1}, r_{k_1}) = r_{k-1}.$$

6. EL ANILLO DE LOS ENTEROS DE GAUSS

En esta última sección vamos a estudiar una familia de anillos que aparecen al adjuntar a $\mathbb{Z}$ un elemento $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ (es decir, ω es solución del polinomio $X^2 - \omega^2 \in \mathbb{Z}[X]$).

6.1 Def. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos el subanillo de $\mathbb{C}$ generado por $\mathbb{Z}$ y ω, denotado por $\mathbb{Z}[\omega]$. Es claro que tienes que contener a $\mathbb{Z}$, y a $\mathbb{Z}\omega$ y a sumas de estos elementos. Es fácil ver que no contiene elementos nuevos:

$$\mathbb{Z}[\omega] = \{n + m\omega \quad | \quad n, m \in \mathbb{Z}\}$$

Nota: Dado $\xi \in \mathbb{C}$ consideremos el homomorfismo evaluación $\Phi_\xi : \mathbb{Z}[X] \to \mathbb{C}$ que a cada $p(x) \in \mathbb{Z}[X]$ le hace corresponder $p(\xi)$. Entonces $\operatorname{Im} \Phi_\xi \cong \mathbb{Z}[\xi] \cong \mathbb{Z}[X]/(\operatorname{Ker}(\Phi_\xi))$.

6.2 Lema. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces:

(i) $w \notin \mathbb{Q}$.

(ii) Si $n + m\omega = n' + m'\omega \in \mathbb{Z}[\omega]$, entonces $n = n'$ y $m = m'$.

Nota: Recordamos el anillo de los enteros de Gauss que corresponde a $\mathbb{Z}[i]$ con i la raíz imaginaria ($i^2 = -1$).

6.3 DEF. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos $\mathbb{Z}[\omega]$:

$\star$ Se define el conjugado de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $(n + m\omega)^*$ como

$$(n + m\omega)^* := n - m\omega.$$

$\star$ Se define la norma de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $N(n + m\omega)$ como

$$N(n + m\omega) := n^2 - \omega^2 m^2.$$

6.4 PROPOSICIÓN. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Sean $a, b \in \mathbb{Z}[\omega]$, entonces:

(i) $aa^* = a^*a = N(a) = N(a^*)$.

(ii) $(ab)^* = a^*b^*$ y $a^{**} = a$.

(iii) $N(ab) = N(a)N(b)$.

(iv) a es una unidad de $\mathbb{Z}[\omega]$ si y sólo si $N(a) = \pm 1$. Además, $a^{-1} = N(a)\ a^*$.

(v) $N(a) = 0$ si y sólo si $a = 0$.

(vi) Si $N(a)$ es un primo de $\mathbb{Z}$, entonces a es irreducible en $\mathbb{Z}[\omega]$.

6.5 TEOREMA. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces $\mathbb{Z}[\omega]$ verifica la C.C.A para sus ideales principales. En particular todo elemento de $\mathbb{Z}[\omega]$ factoriza como producto de irreducibles.

6.6 TEOREMA. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Supongamos que para cada $r, s \in \mathbb{Q}$ existen $n, m \in \mathbb{Z}$ tales que

$$|(r - m) - \omega^2(s - n)| < 1$$

Entonces $\mathbb{Z}[\omega]$ es un dominio euclídeo, con función Euclídea $\delta(a) = |N(a)|$.

6.7 COROLARIO. EL anillo de los enteros de Gauss es un dominio euclídeo.

Nota: Las unidades de $\mathbb{Z}[i]$ son $\pm 1, \pm i$.

Estudiemos ahora cuales son los elementos irreducibles de $\mathbb{Z}[i]$. Ya sabemos que dado $a = n + mi \in \mathbb{Z}[i]$, si $N(a)$ es un número primo, a es irreducible.

En primer lugar podríamos pensar que todo primo de $\mathbb{Z}$ es primo en $\mathbb{Z}[i]$, pero es falso: $5 = (2+i)(2-i)$ (esta es la factorización de 5 como producto de primos).

6.8 Proposición. Un número primo $p \in \mathbb{Z}$ es primo en $\mathbb{Z}[i]$ si y sólo si no se puede escribir como suma de dos cuadrados.

Demo: Supongamos que p se puede escribir como suma de dos cuadrados, $p = n^2 + m^2$. Entonces

$$p = (n + mi)(n - mi)$$

en donde $n + mi, n - mi$ si son primos de $\mathbb{Z}[i]$ (ya que su norma es un número primo).

Supongamos que $p = (n + mi)(n' + m'i)$, en donde $n + mi$, $n' + m'i$ no son unidades. Podemos suponer n, m son primos entre si, entonces:

$$nn' - mm' = p \qquad (*)$$
$$nm' + mn' = 0 \qquad (**)$$

veamos varios casos:

$\star$ Si $n = 0$, entonces $p = mi\ (n' + m'i) = -mm' + mn'i$, por tanto $n' = 0$ y $p = -mm'$ implica que m o m' es ± 1 (al ser p primo) y $n+mi = \pm i$ o $n'+m'i = \pm i$ es inversible.

$\star$ Si $m = 0$ llegamos al mismo resultado.

$\star$ So n, m son no nulos, entonces $nm' = -mn'$, como $m.c.d(n, m) = 1$, n divide a n', por lo que $n' = \alpha n$, Así, por $(*)$, $nm' = -n'm = -\alpha nm$, por lo que $m' = -\alpha m$. Ahora por $(**)$, $p = nn' - mm' = \alpha n^2 + \alpha m^2 = \alpha(n^2 + m^2)$ y así, como p es un primo de $\mathbb{Z}$, o $n^2 + m^2 = 1$ con lo que $n + mi$ sería inversible, o $\alpha = \pm 1$ y $p = (n + mi)(n - mi) = n^2 + m^2$, una suma de cuadrados. ■

6.9 Lema. Sea $p \in \mathbb{Z}$ un número primo tal que $p \equiv 1$ (Mod 4). Entonces la ecuación $x^2 + 1 = 0$ tiene solución en $\mathbb{Z}_p$.

Demo: En caso contrario, no habría elementos en $\mathbb{Z}_p$ tales que $x^2 = -1$ y como $\mathbb{Z}_p$ es un cuerpo para cada $r \in \mathbb{Z}_p$ existiría $s \in \mathbb{Z}_p$ con $rs = -1$ (los podré reordenar a pares), luego si multiplico todos los elementos de $\mathbb{Z}_p^*$,

$$(p-1)! \equiv (-1)^{(p-1)/2} \text{ (Mod } p)$$

y como $p \equiv 1 \pmod 4$, $(p-1)/2$ es par por lo que

$$(p-1)! \equiv 1 \pmod p$$

que contradice el teorema de Wilson $(p-1)! \equiv -1 \pmod p$. ■

6.10 Teorema. Sea $p \in \mathbb{Z}$ un número primo. Entonces p es irreducible en $\mathbb{Z}[i]$ si y sólo si $p \equiv 3 \pmod 4$.

Demo: Supongamos que p es reducible. Entonces por el teorema anterior $p = n^2 + m^2$ con $n, m \in \mathbb{N}$. Si $p = 2$, $p \equiv 2 \pmod 4$ y si p es impar, n es par y m es impar o viceversa, podemos suponer n par, por lo que

$$p \equiv n^2 + m^2 \equiv 0 + 1^1 \equiv 1 \pmod 4 \qquad \text{ó},$$
$$p \equiv n^2 + m^2 \equiv 0 + 3^3 \equiv 1 \pmod 4$$

Supongamos ahora que p es irreducible y no es congruente con 3 módulo 4. Entonces,

⋆ p no puede ser congruente con cero módulo 4 (ya que es primo).

⋆ Si $p \equiv 2 \pmod 4$, $p = 2$ que es reducible, contradicción.

⋆ Luego $p \equiv 1 \pmod 4$. Tenemos entonces que la ecuación $x^2 + 1 \equiv 0 \pmod p$ tiene solución por lo que existe $u \in \mathbb{Z}$ tal que $u^2 + 1$ es divisible por p, pero en $\mathbb{Z}[i]$, $u^2 + 1 = (u+i)(u-i)$ y como es primo, p dividiría a $u - i$ o a $u + i$, una contradicción. ■

6.11 Teorema. Sea $z = n + mi \in \mathbb{Z}[i]$, el anillo de los enteros de Gauss. Entonces z es irreducible (y por tanto primo) si y sólo si se verifica una de las siguientes condiciones:

(i) $N(z)$ es un número primo.

(ii) $z \in \mathbb{Z}$ es un número primo con $z \equiv 3 \pmod 4$ o asociado a éste.

Demo: Por los teoremas anteriores, los elementos que verifican (i) y (ii) son irreducibles. Supongamos ahora que $z \in \mathbb{Z}[i]$ es irreducible y consideremos $N(z)$. Factorizamos $N(z)$ como producto de primos de $\mathbb{Z}$ y si p es uno de estos primos y es reducible sobre $\mathbb{Z}[i]$ lo escribimos como $p = (n + mi)(n - mi)$ producto de primos por (i),(con $n^2 + m^2 = p$) luego como z divide a $N(z)$, y es primo tiene que dividir a alguno de estos y por tanto es (salvo equivalencia) uno de estos. ■

6.12 Veamos un proceso para factorizar un número de Gauss: Consideremos $n + mi \in \mathbb{Z}[i]$.

⋆ Paso primero: calculamos la norma de z.

$$N(z) = n^2 + m^2$$

⋆ Paso segundo: factorizamos en $\mathbb{Z}$ el número entero $N(z)$.

$$N(z) = p_1^{n_1} \cdots p_k^{n_k}$$

⋆ Paso tercero: Factorizamos cada uno de los primos que aparecen.

⋆ Paso final: Como $N(z) = zz^*$, y $\mathbb{Z}[i]$ es un dominio de factorización única, al ser un dominio euclídeo, de la factorización en primos de $N(z)$ sólo nos tenemos que quedar con los que corresponden a z (que son justamente la mitad).

Nota: Si p_i está en la factorización de $N(z)$ y es primo de $\mathbb{Z}[i]$, por tanto $p_i \equiv 3$ (Mod 4), entonces debe de aparecer elevado a un número par.

7. 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).

⋆ **J. Dorronsoro y E. Hernández** , "Números, Grupos y Anillos". Addison-Wesley (1996).