Tema 2.- Dominios euclídeos. Factorización.

2.1 Dominios euclídeos.

En este punto ya hemos utilizado propiedades elementales de la división euclídea en $\mathbb{Z}$:"Dados $D, d \in \mathbb{Z}$, $d \neq 0$, existen unos únicos $c, r \in \mathbb{Z}$ (cociente y resto) tales que: $D = dc + r$ y $0 \leq r < |d|$".

De una manera análoga en $k[X]$, anillo de polinomios en la variable X sobre un cuerpo k, hay una división euclídea de polinomios: "Dados $D(X), d(X) \in k[X]$, $d \neq 0$, existen unos únicos $c(X), r(X) \in k[X]$ (cociente y resto) tales que: $D(X) = d(X)c(X) + r(X)$ y $r = 0$ ó bien $\mathrm{gr}(r) < \mathrm{gr}(d)$". La demostración informal de lo anterior se conoce desde la secundaria. Una demostración formal se puede hacer por inducción en $n = \mathrm{gr}(D) - \mathrm{gr}(d)$.

Vamos a definir los dominios euclídeos como los anillos en donde se da una propiedad análoga a las anteriores.

Definición 2.1.1.– Sea A un dominio de integridad. Diremos que A es un *dominio euclídeo* si existe una aplicación $\delta : A \setminus \{0\} \to \mathbb{N}$ tal que:

1. Si $a, b \in A \setminus \{0\}$ y $a|b$, entonces $\delta(a) \leq \delta(b)$.
2. (*División entera con resto respecto de δ*) Dados $D, d \in A$, $d \neq 0$, existen $c, r \in A$ tales que: $D = dc + r$ y $\delta(r) < \delta(d)$ si $r \neq 0$.

Por el comentario anterior es obvio que $\mathbb{Z}$ y $k[X]$ son dominios euclídeos, para $\delta(a) = |a|$ en el primer caso, y $\delta(f) = \mathrm{gr}(f)$ en el segundo.

En la segunda propiedad de la definición no se exige que el "cociente" c y el "resto" r sean únicos. De hecho después veremos ejemplos en los que no se da esta unicidad.

Proposición 2.1.2.– Sea (A, δ) un dominio euclídeo.

1. Si u es una unidad de A, $\delta(u)$ es el valor mínimo de δ.
2. Si $a, b \in A \setminus \{0\}$ son asociados, entonces $\delta(a) = \delta(b)$.
3. Si $a, b \in A \setminus \{0\}$, $a|b$ y $\delta(a) = \delta(b)$, entonces a y b son asociados.
4. Un elemento $a \in A \setminus \{0\}$ es una unidad, si y sólo si $\delta(a) = \delta(1)$.

DEMOSTRACIÓN: La primera afirmación es consecuencia inmediata de que una unidad divide a todo elemento, y de la primera condición de dominio euclídeo. La segunda afirmación es trivial. Para la tercera afirmación, dividimos a por b: $a = cb + r$. Si $r \neq 0$, entonces $\delta(r) < \delta(b)$. Como $a|b$, existe $a' \in A$ tal que $b = a'a$. Por tanto $r = a - cb = (1 - ca')a$, por lo que $\delta(a) \leq \delta(r)$, que contradice la hipótesis. Por ello $r = 0$, y $b|a$ como queríamos. La última afirmación es consecuencia fácil de las anteriores. $\square$

Un ejemplo de dominios que hemos manejado en el tema anterior es $A = \mathbb{Z}[\sqrt{m}] \subset \mathbb{C}$, con m entero libre de cuadrados. En ellos podemos definir una aplicación "norma", que verifica siempre la primera condición de dominio euclídeo, y en algunos casos también la segunda:

$$N : A \to \mathbb{N}, \quad \text{con} \quad N(a + b\sqrt{m}) = |(a + b\sqrt{m})(a - b\sqrt{m})| = |a^2 - mb^2|.$$

Proposición 2.1.3.– N verifica las siguientes propiedades:

1. $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{m}]$.
2. Si $u \in \mathbb{Z}[\sqrt{m}]$, $N(u) = 1$ si y sólo si u es una unidad.
3. Si $x, y \in \mathbb{Z}[\sqrt{m}]$, $x|y$ y $N(x) = N(y)$, si y sólo si x e y son asociados.
4. Si $x \in \mathbb{Z}[\sqrt{m}]$ y $N(x)$ es un número primo, entonces x es irreducible.

La demostración es un fácil ejercicio.

Nota 2.1.4.–

1. Con las propiedades anteriores, es un ejercicio elemental probar que $\mathbb{Z}[\sqrt{-3}]$ no es DFU, puesto que 2 es un elemento irreducible, pero no primo, ya que divide a $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, pero no divide a ningún factor.
2. El caso $m = -1$ es el del anillo de los enteros de Gauss, $\mathbb{Z}[i]$, que es dominio euclídeo, cuando definimos una división entera en él.

   Sean $x, y \in \mathbb{Z}[i]$, $b \neq 0$. Entonces el cociente complejo de x y y es $u + vi \in \mathbb{C}$, con $u, v \in \mathbb{Q}$. Sean $m, n \in \mathbb{Z}$ unas aproximaciones enteras que redondean u, v, es decir tales que

   $$|m - u| \leq \frac{1}{2} \qquad \text{y} \qquad |n - v| \leq \frac{1}{2}.$$

   Entonces $r = x - (m + ni)y \in \mathbb{Z}[i]$. Por la elección anterior, se tiene que $r = y[(u - m) + i(v - n)]$, por lo que $N(r) \leq \frac{1}{2}N(y) < N(y)$. Se tiene así que

   $$x = (m + ni)y + r, \quad \text{con} \quad N(r) < N(y),$$

   por lo que $\mathbb{Z}[i]$ queda dotado de estructura de dominio euclídeo, con la norma N como aplicación δ.
3. De un modo análogo se podría dotar a $\mathbb{Z}[\sqrt{2}]$ de una estructura de dominio euclídeo.

Definición 2.1.5.– Un dominio A se dice de *ideales principales*, (DIP), cuando todos sus ideales lo son.

El resultado siguiente nos da una gran cantidad de ejemplos.

Proposición 2.1.6.– Todo dominio euclídeo es un dominio de ideales principales.

DEMOSTRACIÓN: Sea (A, δ) un dominio euclídeo, e I un ideal no nulo de A. Sea $a \in I \setminus \{0\}$ un elemento con $\delta(a)$ mínimo. Vamos a probar que $I = (a)$. Una inclusión es clara. Recíprocamente, sea $b \in I$, que dividimos por a, obteniendo

$b = ca+r$. Si r no es cero, como está en I y $\delta(r) < \delta(a)$, llegamos a contradicción con la elección de a. Por tanto $r = 0$, y se tiene lo deseado. $\square$

No es cierto el recíproco. Hay dominios de ideales principales que no son euclídeos, como $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, pero esta comprobación es bastante difícil.

$\mathbb{Z}[X]$, con X una variable, es un ejemplo de un dominio que no es DIP. Para ello verifíquese que $(2, X)$ no es un ideal principal en $\mathbb{Z}[X]$.

2.2 Factorización.

El resultado fundamental de esta sección es el siguiente:
Teorema 2.2.1.– Todo DIP es un DFU.

Definición 2.2.2.– Se dice que un anillo A verifica la *condición de cadena ascendente para ideales* (o, brevemente, la CCA) si toda cadena estrictamente creciente de ideales de A

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

es finita. Equivalentemente, toda cadena ascendente infinita de ideales

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

es estacionaria, es decir, existe un entero $n > 0$ tal que $I_j = I_n$, para todo $j \geq n$.

Proposición 2.2.3.– Sea A un DIP; entonces verifica la CCA.

Demostración: Sea

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

una cadena ascendente de ideales, y sea

$$I = \bigcup_{j \geq 1} I_j$$

la unión de todos ellos; entonces I es un ideal. En efecto, sean $a, b \in I$, digamos $a \in I_j$ y $b \in I_k$. Si, por ejemplo, $k \geq j$, entonces $a, b \in I_k$, luego $a - b \in I_k \subseteq I$. Si $a \in I$, digamos $a \in I_j$, y $x \in A$, entonces $ax \in I_j \subseteq I$. Ahora bien, el ideal I es principal; escribamos $I = Ad$. Entonces $d \in I_n$ para un cierto n, luego $I_n = I$. Así, para todo $j \geq n$ es $I_j = I = I_n$. Esto prueba la proposición. $\square$

Proposición 2.2.4.– Sea A un DIP; entonces A verifica la condición *(DFU1)*.

Demostración: Sea a una no unidad distinta de cero. Tenemos que probar que a se descompone en producto finito de elementos irreducibles. Si a es irreducible, no hay nada que probar. Si a no es irreducible, se puede escribir $a = bc$ donde b y c no son asociados de a, ni unidades. Así $Aa \subset Ab$ y $Aa \subset Ac$. Repitiendo el razonamiento con b, por ejemplo, y así sucesivamente, la CCA implica que este proceso es finito, lo que nos lleva a que a debe tener un divisor irreducible p_1. Entonces

$$Aa \subset A\frac{a}{p_1}.$$

Si $a_1 = a/p_1$ es irreducible, entonces $a = a_1p_1$ es una descomposición factorial de a, y nuestra demostración habrá concluido. Supongamos que a_1 no es irreducible. Aplicando a $a_1 = a/p_1$ el mismo razonamiento, llegamos a la existencia de un divisor irreducible p_2 de a_1, y a una terna

$$Aa \subset Aa_1 \subset Aa_2,$$

con $a_1 = p_2a_2$. Por CCA, este proceso debe tener un fin, es decir, debe existir un entero positivo n tal que $a/(p_1 \cdots p_{n-1}) = p_n$ sea irreducible. Así $a = p_1 \cdots p_{n-1}p_n$, lo que prueba la proposición. $\square$

Proposición 2.2.5.– (*Identidad de Bezout*) Sea A un DIP, y sean $a, b \in A$ dos elementos no nulos. Entonces existe un elemento $d = \alpha a + \beta b$ con $\alpha, \beta \in A$, tal que $d = \mathrm{mcd}(a, b)$.

DEMOSTRACIÓN: Sea (a, b) el ideal engendrado por a, b; entonces existe $d \in A$ tal que $(a, b) = Ad$. Como $Aa \subseteq Ad$ y $Ab \subseteq Ad$, es $d|a$ y $d|b$. El hecho de que $d = \mathrm{mcd}(a, b)$ viene, ahora, de que d es de la forma $d = \alpha a + \beta b$. $\square$

La demostración del teorema 2.2.1 termina con la siguiente
Proposición 2.2.6.– Sea A un DIP; entonces A verifica *(DFU3)*.

DEMOSTRACIÓN: Sea $p \in A$, irreducible, con $p|ab$, y supongamos que p no divide a a. Entonces $1 = \mathrm{mcd}(a, p)$ y, por la proposición anterior, $1 = \alpha a + \beta p$. Así, $b = \alpha ab + \beta bp$, de donde se deduce que $p|b$. Esto prueba la proposición. $\square$

Nota 2.2.7.–

1. Hay un procedimiento simple de construir un DFU: si A es un DFU, también lo es $A[X]$. La demostración de este resultado no la damos, puesto que alargaría demasiado este tema (cf. Delgado-Fuertes-Xambó: "Introducción al Álgebra" pp. 96-100).

2. En el caso de un dominio euclídeo A, se puede generalizar el algoritmo de Euclides para $\mathbb{Z}$, de cálculo del máximo común divisor de dos elementos $a, b \in A \setminus \{0\}$:

   Se construye la sucesión $r_0, r_1, r_2, \ldots, r_n$, poniendo $r_0 = a$, $r_1 = b$, y para cada $j \geq 2$, r_j es el resto de dividir r_{j-2} por r_{j-1}. El proceso acaba alcanzando el cero en cierto r_n. Entonces $r_{n-1} = \mathrm{mcd}(a, b)$. La validez del algoritmo se basa en dos cuestiones. Por una parte $\mathrm{mcd}(r_i, r_{i+1}) = \mathrm{mcd}(r_{i+1}, r_{i+2})$, para cada $i = 0, \ldots, n-3$, y por otra que el algoritmo debe acabar puesto que δ va decreciendo en la sucesión creada.