Tema 1.- Anillos: ideales primos y maximales. Cuerpos: característica

1.1 Ideales primos e ideales maximales

`Las nociones de anillo, ideal, dominio de integridad, cuerpo, homomorfismo de anillos, anillo cociente, DIP, DFU, etc. se han estudiado en el tema 1 de la asignatura Algebra.`

En lo que sigue, A designará un anillo, que siempre consideraremos conmutativo (y unitario, i.e. con elemento unidad = elemento neutro para la multiplicación).

DEFINICIÓN 1.1.1.– Diremos que un ideal $I \subset A$ de A es un ideal *primo* si $I \neq A$ y se verifica la siguiente condición: el producto de dos elementos del anillo pertenece al ideal si y sólo si alguno de los elementos pertenece al ideal, es decir, si

$$x, y \in A, xy \in I \Rightarrow x \in I \quad \text{ó} \quad y \in I.$$

EJEMPLO 1.1.2.– Si I es el ideal de A generado por un elemento $p \in A$, se tiene que I es un ideal primo si y sólo si p es un elemento primo.
Por ejemplo, si $A = \mathbb{Z}$, los ideales primos de A son los ideales de la forma $\mathbb{Z}p$, donde p es un número primo.

PROPOSICIÓN 1.1.3.– Sea $I \subset A$ un ideal. Las propiedades siguientes son equivalentes:

1. I es un ideal primo.
2. El anillo cociente A/I es un dominio de integridad.

DEFINICIÓN 1.1.4.– Diremos que un ideal $I \subset A$ de A es un ideal *maximal* si $I \neq A$ y el único ideal de A que contiene a I es el propio A.

PROPOSICIÓN 1.1.5.– Todo ideal maximal es primo.

PROPOSICIÓN 1.1.6.– Todo ideal propio I de A está contenido en algún ideal maximal.

La prueba de esta proposición usa el *lema de Zorn*.

EJEMPLO 1.1.7.– En $\mathbb{Z}$ todo ideal primo es maximal. Más generalmente, todo ideal primo de un DIP es maximal.
En $\mathbb{Z}[X]$ el ideal $I = (X)$ es primo pero no es maximal.

PROPOSICIÓN 1.1.8.– Sea $I \subset A$ un ideal. Las propiedades siguientes son equivalentes:

1. I es un ideal maximal.
2. El anillo cociente A/I es un cuerpo.

EJEMPLO 1.1.9.– En $\mathbb{Z}[X]$ el ideal $I = (X, p)$, donde $p \in \mathbb{Z}$ es un número primo, es maximal,

1.2 Característica de un cuerpo

En lo que sigue k denotará un cuerpo.

Sabemos que existe un único homomorfismo de anillos $\varphi : \mathbb{Z} \to k$, que viene dado por $\varphi(n) = n \cdot 1_k$.

DEFINICIÓN 1.2.1.– Definimos la *característica* de k como el entero $p \geq 0$ que engendra al ideal $\ker \varphi$.

Un cuerpo k es de característica cero si y sólo si no existe ningún entero $m > 0$ tal que $m \cdot 1_k = 0_k$. Si k no es de característica cero, su característica es el menor entero positivo p tal que $p \cdot 1_k = 0_k$.

Nótese que todo cuerpo finito ha de ser de característica positiva.

PROPOSICIÓN 1.2.2.– La característica de un cuerpo es o bien 0 o bien un número primo $p > 0$.

EJEMPLO 1.2.3.– El cuerpo $\mathbb{Q}$ de los racionales es de característica cero.
Si $p > 0$ es un número primo, el cuerpo $\mathbb{F}_p = \mathbb{Z}/(p)$ es un cuerpo de característica p, que además es un cuerpo primo.

Si un cuerpo es subcuerpo de otro, entonces los dos tienen la misma característica.

DEFINICIÓN 1.2.4.– El *subcuerpo primo* de k es la intersección de todos los subcuerpos de k.
Diremos que k es un *cuerpo primo* si coincide con su subcuerpo primo.

EJEMPLO 1.2.5.– El cuerpo $\mathbb{Q}$ de los racionales es un cuerpo primo.
Si $p > 0$ es un número primo, el cuerpo $\mathbb{F}_p$ es un cuerpo primo.

PROPOSICIÓN 1.2.6.– Sea k un cuerpo primo. Entonces se verifica una y sólo una de las siguientes propiedades:

1. o bien k es de característica 0, y entonces k es isomorfo a $\mathbb{Q}$,
2. o bien k es de característica $p > 0$, y entonces el homomorfismo $\varphi : \mathbb{Z} \to k$ es sobreyectivo y k es isomorfo a $\mathbb{F}_p$.

COROLARIO 1.2.7.– Dado un número primo $p > 0$, existe un único cuerpo finito con p elementos, salvo isomorfismo.

En el tema 6 estudiaremos con más detalle los cuerpos finitos.