Tema 1.- Nociones preliminares: grupos, anillos, cuerpos. Divisibilidad

1.1 Grupos

`Al haber alterado el orden de los temas, este apartado ya se ha visto en el tema 9`

1.2 Anillos y cuerpos

Definición 1.2.1.– Un *anillo* es una terna $(A, +, \cdot)$ formada por un conjunto A y dos operaciones binarias $+, \cdot$ verificando:

1. El par $(A, +)$ es un grupo abeliano, cuyo elemento neutro llamaremos normalmente "cero (0)".
2. La operación binaria $\cdot$ es asociativa y tiene elemento neutro, que llamaremos normalmente "uno (1)".
3. La operación $\cdot$ es *distributiva* a la derecha y a la izquierda respecto de la operación $+$, i.e. para todos $x, y, z \in A$, se tiene $(x + y) \cdot z = x \cdot z + y \cdot z$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Si además la operación $\cdot$ es conmutativa, diremos que el anillo es conmutativo.

Nota 1.2.2.–

1. En general se usará la expresión "sea A un anillo", sobreentendiendo las operaciones. La operación $\cdot$ se notará normalmente por simple yuxtaposición.
2. En un anillo A se tiene $0 \cdot x = x \cdot 0 = 0$ para todo $x \in A$.
3. Si en un anillo A se tiene $1 = 0$, entonces $A = \{0\}$.
4. Para todo $x, y \in A$, ese tiene $x(-y) = (-x)y = -(xy)$.
5. Si $A_1, \ldots, A_n$ son anillos, el producto cartesiano $A_1 \times \cdots \times A_n$ posee una estructura natural de anillo, donde las operaciones están definidas componente a componente.

Ejemplo 1.2.3.–

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son anillos conmutativos. La estructura de anillo de $\mathbb{Z}$ viene determinada por la de grupo aditivo: el producto de dos enteros xy coincide con el múltiplo de y con coeficiente x. Así pues, la estructura de anillo de $\mathbb{Z}$ no añade nada nuevo a la de grupo. Esto es falso para $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ en los que, obviamente, la estructura multiplicativa no viene determinada por la aditiva.

2. El conjunto $\mathcal{M}(n)$ de las matrices $n \times n$ sobre $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es un anillo, con respecto a la adición y la multiplicación ordinaria de matrices. No es conmutativo.

3. En el grupo $(\mathbb{Z}_n, +)$ (ver ejemplo 9.1.3, 5) podemos definir un producto de la siguiente manera:

$$(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n \mapsto a \cdot b := \text{resto de la división de } ab \text{ entre } n.$$

   De esta forma $\mathbb{Z}_n$ es un anillo.

DEFINICIÓN 1.2.4.– Sea A un anillo. Una *unidad* es un elemento que posee un simétrico multiplicativo (a la izquierda y a la derecha), que llamaremos *inverso*. El conjunto de las unidades de A es un grupo para el producto y se notará A^*. Un *cuerpo* es un anillo conmutativo tal que todo elemento distinto de cero es una unidad, i.e. $A^* = A - \{0\}$. (En algunos textos también se llaman cuerpos aquellos anillos no necesariamente conmutativos tales que todos sus elementos no nulos son unidades. En otros textos a estos anillos se les llama *anillos de división*).

EJEMPLO 1.2.5.–

1. Las unidades de $\mathbb{Z}$ son $1, -1$. Los anillos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.

2. El grupo de las unidades del anillo $\mathcal{M}(n, k)$ con $k = \mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$ es $\mathbf{GL}(n, k)$.

DEFINICIÓN 1.2.6.– Sea A un anillo. Un *subanillo* de A es un subconjunto $B \subset A$ que es un subgrupo de $(A, +)$, que es estable para la operación $\cdot$ y tal que $1 \in B$.
Si A es un cuerpo, diremos que B es un *subcuerpo* de A si es un subanillo y además $x^1 \in B$ para todo $x \in B - \{0\}$.

A partir de ahora sólo trabajaremos con anillos conmutativos. Así pues, la palabra '*anillo*' significará siempre anillo conmutativo.

DEFINICIÓN 1.2.7.– Sea A un anillo. Un elemento $x \in A$ se llamará un *divisor de cero* si y sólo si es distinto de cero y existe $y \in A$, $y \neq 0$, tal que $xy = 0$. Un anillo sin divisores de cero se llama un *dominio de integridad*. Un elemento $x \in A$ se llamará *nilpotente* si es distinto de cero y existe un entero $n > 0$ tal que $x^n = 0$. En un dominio de integridad se da la propiedad cancelativa por el producto de elementos no nulos:

$$a \neq 0, ab = ac \Rightarrow b = c.$$

EJEMPLO 1.2.8.–

1. Las unidades no son divisores de cero. Así, todo cuerpo es un dominio de integridad.

2. $\mathbb{Z}$ es un dominio de integridad.

3. El anillo $\mathbb{Z}_4$ no es un dominio de integridad. El anillo $\mathbb{Z}_3$ es un cuerpo.

4. El elemento 2 es nilpotente en $\mathbb{Z}_4$.

DEFINICIÓN 1.2.9.– Sea A un anillo. Un *ideal* de A es un subconjunto I de A que verifica:

1. I es un subgrupo del grupo aditivo de A.

2. Para todo $a \in I$, $x \in A$ se tiene $xa \in I$.

NOTA 1.2.10.– Sea $I \subset A$ un ideal de A. Se tiene:

1. Si I contiene una unidad, entonces $I = A$.

2. Si A es un cuerpo, sus únicos ideales son $\{0\}$ y A.

3. El grupo cociente A/I admite una estructura canónica de anillo. En efecto, basta ver que la fórmula

$$(a + I)(b + I) = ab + I$$

define una operación en A/I. Si $a+I = a'+I$ y $b+I = b'+I$ es $a-a' \in I$, y $b - b' \in I$. Así

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I,$$

lo que prueba nuestro aserto.

4. Los ideales de $\mathbb{Z}$ y los subgrupos son la misma cosa, pues la estructura multiplicativa viene determinada por la aditiva.

DEFINICIÓN 1.2.11.– Si A es un anillo y $a_1, \dots, a_n \in A$, el conjunto

$$(a_1, \dots, a_n) := \{x_1a_1 + \cdots + x_na_n \mid x_1, \dots, x_n \in A\}$$

es un ideal de A, que se llama *engendrado* por el conjunto de las a_i. Si $n = 1$, el ideal de llama *principal*. Todo ideal de $\mathbb{Z}$ es principal.

DEFINICIÓN 1.2.12.– Sean A, B anillos, $f : A \to B$ una aplicación. Se dirá que f es un *homomorfismo* de anillos si verifica:

1. Para todos $x, y \in A$, es $f(x + y) = f(x) + f(y)$.

2. Para todos $x, y \in A$, es $f(xy) = f(x)f(y)$.

3. $f(1) = 1$.

Un homomorfismo biyectivo se llama un *isomorfismo*.

PROPOSICIÓN 1.2.13.– Sea $f : A \to B$ un homomorfismo de anillos. Se tienen las siguientes propiedades:

1. $\ker(f) := \{a \in A \mid f(a) = 0\}$ es un ideal de A, y f es inyectivo si y sólo si $\ker(f) = \{0\}$.

2. Si $u \in A$ es una unidad, entonces $f(u)$ es una unidad en B. En particular cualquier homomorfismo (de anillos) entre cuerpos es inyectivo.

3. $\mathrm{Im}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$ es un subanillo de B.

1.3 Divisibilidad

DEFINICIÓN 1.3.1.– Sea A un dominio de integridad.

1. Sean $a, b \in A$, con $a \neq 0$. Se dirá que a divide a b, o que a es un *divisor* de b si existe $c \in A$ tal que $b = ac$. Este elemento c es único por ser A un dominio de integridad, y se le designará por b/a. También se dirá, en este caso, que b *es divisible por* a. Se escribirá $a|b$ para designar esta relación. Es evidente que una unidad divide a cualquier otro elemento de A.

2. Se dirá que a y b, con $a, b \neq 0$, son *asociados* si y sólo si $a|b$ y $b|a$. En este caso se puede escribir $b = ac$ y $a = bc'$, luego $a = acc'$, de donde $a(1 - cc') = 0$, y así $cc' = 1$. De aquí se ve ya fácilmente que a, b son asociados si y sólo si uno de ellos es igual al otro multiplicado por una unidad.

3. Sean $a, b \in A$ distintos de cero. Un *máximo común divisor* de a y b es un elemento $d \in A$ que verifica:

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

   (b) Si $d' \in A$ es tal que $d'|a$ y $d'|b$, entonces $d'|d$.

   De lo anterior se deduce que, si d, d' son dos máximos comunes divisores de a, b, entonces $d|d'$ y $d'|d$, luego son asociados. Así pues, el máximo común divisor de a, b está unívocamente determinado, salvo producto por unidades, y se escribe m.c.d.(a, b).

4. Sean $a, b \in A$, distintos de cero. Un mínimo común múltiplo de a y b es un elemento $m \in A$ que verifica:

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

   (b) Si $m' \in A$ es tal que $a|m'$ y $b|m'$, entonces $m|m'$.

   De lo anterior se deduce que, si m, m' son dos mínimos comunes múltiplos de a, b, entonces $m|m'$ y $m'|m$, luego son asociados. Así pues, el mínimo común múltiplo de a, b está unívocamente determinado, salvo producto por unidades, y se escribe m.c.m.(a, b).

5. Un elemento $p \in A$ se llama *irreducible* si sólo es una no unidad distinta de cero, divisible únicamente por sus asociados y por las unidades.

6. Un elemento $p \in A$ se llama *primo* si $p|(ab) \Rightarrow p|a$ ó $p|b$.

PROPOSICIÓN 1.3.2.– Todo elemento primo de un dominio de integridad es irreducible.

EJEMPLO 1.3.3.– El recíproco de la proposición anterior no es cierto. Si consideramos el domino de integridad

$$A = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

se tiene la igualdad $2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ y $2 \in A$ es irreducible pero no divide a $1 + \sqrt{-3}$ (los detalles se verán más adelante).

NOTA 1.3.4.–

1. Sea $d = \text{m.c.d.}(a, b)$ y escribamos $a' = a/d$, $b' = b/d$; entonces

$$\text{m.c.d.}(a', b') = 1.$$

   En efecto, supongamos que existiese una no unidad $e \in A$, distinta de cero, tal que $e|a'$ y $e|b'$. Entonces $(ed)|a$ y $(ed)|b$, luego $(ed)|d$, lo que implicaría que ed, d son asociados. Esto no es posible, pues e no es una unidad.

2. Nótese que, hasta ahora, no hemos afirmado nada sobre la existencia del máximo común divisor de dos elementos. Nos hemos limitado a dar propiedades de él, caso de que exista.

EJEMPLO 1.3.5.– En $\mathbb{Z}$ sabemos que existe el máximo común divisor y el mínimo común múltiplo de cualquier par de enteros no nulos.

DEFINICIÓN 1.3.6.– Un *dominio de factorización única* (DFU) es un dominio de integridad A que verifica las siguientes condiciones:

(DFU1) Toda no unidad distinta de cero es producto finito de factores irreducibles.

(DFU2) La descomposición anterior es única salvo orden y producto por unidades. Se llama la *descomposición factorial* del elemento en cuestión.

EJEMPLO 1.3.7.– $\mathbb{Z}$ es un dominio de factorización única.

PROPOSICIÓN 1.3.8.– Sea A un dominio de integridad que satisface la condición (DFU1). Entonces A satisface (DFU2) si y sólo si satisface la siguiente:

(DFU3) Todo elemento irreducible de A es primo (esta propiedad se la conoce con el nombre de *teorema de Euclides*, por analogía con el caso de los números enteros).

PRUEBA: Supongamos que A satisface (DFU2), y sean p, a, b como en el enunciado. Supongamos que p no divide a a, y sea $ab = pq$. Sean

$$a = p_1 \cdots p_s \ , \ b = q_1 \cdots q_t \ , \ q = r_1 \cdots r_u$$

las descomposiciones factoriales de a, b, q. Como

$$(p_1 \cdots p_s)(q_1 \cdots q_t) = pr_1 \cdots r_u,$$

la unicidad indica que p (o un asociado) tiene que figurar entre los elementos irreducibles del miembro de la izquierda de la anterior igualdad. Como no puede figurar entre los p_i, porque no divide a a, debe figurar entre los q_j. Así $p|b$, lo que prueba (DFU3).

Recíprocamente, supongamos que A verifica (DFU3), y sean

$$a = p_1 \cdots p_s = q_1 \cdots q_t$$

dos descomposiciones de a en producto de irreducibles. Por (DFU3), p_1 (o un asociado suyo) debe coincidir con un q_i, digamos q_1. Cancelando ambos en la igualdad anterior, se tiene la igualdad

$$p_2 \cdots p_s = q_2 \cdots q_t,$$

con la que se procede como antes, y así sucesivamente. Esto prueba (DFU2). □

COROLARIO 1.3.9.– Sea A un dominio de factorización única; cualquier par de elementos $a, b \in A$ distintos de cero tienen un máximo común divisor $d \in A$.

PRUEBA: Considerando las descomposiciones factoriales de a, b basta tomar como d el producto de todos los factores irreducibles comunes a las dos. En efecto, sean

$$a = (p_1 \cdots p_r)(p'_1 \cdots p'_s)\ ,\ b = (p_1 \cdots p_r)(q'_1 \cdots q'_t)$$

las descomposiciones factoriales, donde

$$\{p'_1, \ldots, p'_s\} \cap \{q'_1, \ldots, q'_t\} = \emptyset,$$

y sea $d = p_1 \cdots p_r$. Claramente $d|a$ y $d|b$. Sea $d' \in A$ tal que $d'|a$ y $d'|b$. Si p es un elemento irreducible que divide a d', entonces p (o un asociado) debe coincidir con un p_i, digamos p_1. De aquí se deduce que $(d'/p_1)|(a/p_1)$ y $(d'/p_1)|(b/p_1)$. Repitiendo el razonamiento cuantas veces sea necesario se deduce que $d'|d$. Esto prueba el corolario. □

DEFINICIÓN 1.3.10.– Sean $a, b \in A$; entonces m.c.d.$(a, b) = 1$ si y sólo si ningún elemento irreducible divide a ambos. En este caso se dice que a, b *son primos entre sí.*

COROLARIO 1.3.11.– Sean $a, b, c \in A$ tales que $c|(ab)$ y a, c son primos entre sí. Entonces c divide a b.

La demostración se hace al estilo de la del corolario 1.3.9, considerando sucesivamente divisores irreducibles de c y viendo que dividen a b.

COROLARIO 1.3.12.– Sea A un dominio de factorización única, $a, b \in A$ distintos de cero, $d =$ m.c.d.(a, b). Entonces a, b tienen un mínimo común múltiplo, que es $m = ab/d$.