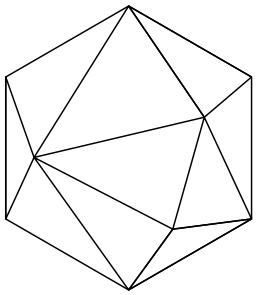

Universidad Nacional de Educación a Distancia

Facultad de Ciencias

Álgebra: Anillos y cuerpos

César Rellán Vega

16 de mayo de 2021

Índice

Tema 1

Anillos

1.1. Generalidades

Definición 1.1 Se llama **anillo** a un conjunto A dotado de dos operaciones que convenimos en denominar suma y producto, y en denotar por $+$ y $\cdot$, respectivamente, que cumplen las siguientes condiciones:

(I) Dotado de la suma, A es un grupo conmutativo.

(II) Asociatividad del producto: para cualesquiera x, y, z de A, se verifica: $x(yz) = (xy)z$.

(III) Distributividad: para cualesquiera x, y, z de A se verifica:

$$(x+y)z = xz + yz, \qquad z(x+y) = zx + zy.$$

En un anillo A, el elemento neutro para la suma se denomina *cero* y se representa por 0_A ó simplemente 0. Denotaremos A^* al conjunto $A \setminus \{0\}$.

Algunas propiedades:

- $(x-y)z = xz - yz, \qquad z(x-y) = zx - zy, \qquad (x, y, z \in A).$
- $0 \cdot z = z \cdot 0 = 0, \qquad (z \in A).$
- $(-y)z = -yz, \qquad z(-y) = -zy.$
- $(-y)(-x) = -(y(-x)) = -(-yx) = yx.$

Definición 1.6 Se llama **anillo unitario** a un anillo A cuyo producto tiene elemento neutro en A^*. Dicho elemento se denomina *uno* y se representa por 1_A ó simplemente 1, si no hay riesgo de confusión.

Definición 1.7 Sea A un anillo unitario. Una **unidad** de A es un elemento $x \in A$ que tiene inverso $y \in A$ respecto del producto:

$$xy = yx = 1.$$

El inverso de x, si existe, es único y se denota por x^{-1}. El conjunto de todas las unidades de A se representa por $U(A)$, y es un grupo para el producto.

Definición 1.8 Se llama **cuerpo** a un anillo K tal que $K^* = K \setminus \{0\}$ dotado del producto, es un grupo.

Ejemplo 1.9

(I) El conjunto $\mathbb{Z}$ de los números enteros (con la suma y producto habituales) es un anillo unitario conmutativo; -1 y 1 son las únicas unidades de $\mathbb{Z}$, que, por tanto, no es un cuerpo.

(II) Los conjuntos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ de los números racionales, reales y complejos son cuerpos conmutativos.

(III) *Enteros de Gauss* — $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$. Este conjunto es un anillo con las operaciones heredadas de $\mathbb{C}$.

(IV) Sean A un anillo y $M_2 = M_2(A)$ el conjunto de las matrices cuadradas de orden 2 de elementos de A. Este conjunto es un anillo con:

$$\text{Suma:} \qquad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\text{Producto:} \quad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

Se tiene que $a \in U(M_2)$ si y sólo si $\det(a) \in U(A)$.

(V) Un anillo de matrices no es conmutativo.

(VI) Sea $A = \mathcal{C}(\mathbb{R}, \mathbb{R})$ el conjunto de las funciones continuas de variable real. Se trata de un anillo con las operaciones:

$$(f + g)(t) = f(t) + g(t),$$

$$(f \cdot g)(t) = f(t) \cdot g(t), \quad t \in \mathbb{R}, \quad f, g \in A.$$

Es conmutativo y unitario.

Definición 1.10 Sea A un anillo. Se llama **divisor de cero** a un elemento $x \in A^*$ tal que $xy = 0_A$ para algún $y \in A^*$.

Definición 1.11 Se llama **dominio de integridad** a un anillo unitario y conmutativo sin divisores de cero.

(1.12) Cuerpo de fracciones de un dominio de integridad — Sean A un dominio de integridad y $T = A \times A^*$. En T se define una relación de equivalencia dada por

$$(x, y) \text{ está relacionado con } (x', y') \text{ si } xy' = yx'.$$

La clase de (x, y) se denotará $[x, y]$.

Es fácil comprobar que el conjunto cociente de T para esta relación, que denotamos K, es un anillo con las operaciones:

$$[x, y] + [x', y'] = [xy' + yx', yy'],$$

$$[x, y] \cdot [x', y'] = [xx', yy'].$$

Además, K es un cuerpo.

Ejemplo 1.13

(I) Un anillo de matrices M_2 nunca es dominio de integridad.

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad (x \in A).$$

(II) La construcción 1.12 con $A = \mathbb{Z}$ produce el cuerpo $\mathbb{Q}$ de los números racionales. Para $\mathbb{Z}[i]$ obtenemos $K = \mathbb{Q}[i]$, esto es, el cuerpo de fracciones de $\mathbb{Z}[i]$ consiste en los números complejos $a + bi$, con $a, b \in \mathbb{Q}$.

(III) Pudiera ocurrir que la construcción 1.12 no produjera nada esencialmente nuevo, en el sentido de que el subconjunto

$$\tilde{A} = \{x/1 : x \in A\}$$

fuera todo K. Este hecho se corresponde con que A ya sea un cuerpo.

(IV) Una propiedad esencial de los dominios de integridad (y de los cuerpos), es que se pueden simplificar factores comunes en las igualdades.

(V) Una construcción que da lugar siempre a que haya divisores de cero es el **producto de anillos**. Sean A y B dos anillos unitarios conmutativos. Entonces $C = A \times B$ es un anillo unitario conmutativo con las operaciones

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

En un anillo como C *siempre* encontramos divisores de cero: todos los elementos de la forma $(0, b)$ ó $(a, 0)$ con $b \neq 0$ y $a \neq 0$. Esto es así aunque A y B sean dominios de integridad.

Una propiedad del producto de anillos importante es que se verifica:

$$U(A \times B) = U(A) \times U(B).$$

Definición 1.14 Sea A un anillo unitario conmutativo. Se llama **ideal** a un subconjunto $I \subset A$ tal que:

(I) I es un subgrupo de A para la suma (en particular, $0 \in I$).

(II) Para cualesquiera $x \in I$, $a \in A$, el producto ax está en I.

Observación 1.15

- En presencia de (II) la condición (I) es equivalente a:

  (I') Para cualesquiera $x, y \in I$ la suma $x + y$ está en I.

- Se habla de un *ideal propio* I cuando $I \neq A$. I es propio si y sólo si $1 \notin I$. También se distingue el ideal $\{0\} \subset A$; éste se denota *ideal trivial*.

(1.16) Anillos cociente — La importancia de la noción de ideal radica en que es la adecuada para definir relaciones de equivalencia en un anillo de tal manera que el conjunto cociente pueda ser dotado de estructura de anillo a su vez.

(I) Sean A un anillo unitario conmutativo e $I \subset A$ un ideal propio. Se define en A la siguiente relación de equivalencia:

$$x \text{ está relacionado con } y \text{ si } x - y \in I, \qquad (x, y \in A).$$

El conjunto cociente de A para esta relación se denota A/I y la clase de equivalencia de un elemento $x \in A$ es:

$$x + I = \{x + a : a \in I\}.$$

La condición $x + I = y + I$ se expresa también:

$$x \equiv y \mod I.$$

Se definen las operaciones en A/I:

$$\text{Suma:} \qquad (x + I) + (y + I) = (x + y) + I, \qquad (x, y \in A),$$

$$\text{Producto:} \qquad (x + I) \cdot (y + I) = xy + I, \qquad (x, y \in A).$$

El elemento $1 + I$ es el uno de A/I. Este conjunto A/I es un anillo unitario conmutativo; se le llama **anillo de clases de restos módulo** I.

(II) Sean A e I como en (I). Sea $\widetilde{J}$ un ideal del anillo cociente. Consideramos el conjunto

$$J = \left\{ x \in A : x + I \in \widetilde{J} \right\}.$$

Evidentemente J es un ideal de A, que contiene a I. La correspondencia

$$\widetilde{J} \mapsto J$$

es una biyección entre el conjunto de los ideales de A/I y el de los ideales de A que contienen a I. Su inversa es:

$$J \mapsto \widetilde{J} = \{ x + I : x \in J \}.$$

(1.17) Ideales generados por un subconjunto — Sean A un anillo unitario conmutativo y L un subconjunto de A, sin estructura algebraica alguna. Se considera el conjunto $I \subset A$ de todas las sumas *finitas* de la forma:

$$a_1 x_1 + \cdots + a_r x_r, \qquad a_1, \ldots, a_r \in A, \quad x_1, \ldots x_r \in L, \quad r \geq 1.$$

Entonces:

(I) I es un ideal.

(II) I es el mínimo ideal que contiene a L, es decir, si $\mathscr{L}$ es la colección de todos los ideales $J \subset A$ tales que $L \subset J$, se verifica:

$$I = \bigcap_{J \in \mathscr{L}} J.$$

Es el *ideal generado por* L.

Definición 1.18 Sea A un anillo unitario conmutativo. Un ideal $I \subset A$ se llama **finitamente generado** si es el ideal generado por un subconjunto finito $L = \{x_1, \ldots, x_r\} \subset A$. En este caso:

$$I = Ax_1 + \cdots + Ax_r = \left\{ \sum_{k=1}^{r} a_k x_k : a_1, \ldots, a_r \in A \right\},$$

y se denota $I = (x_1, \ldots, x_r)$. Si $r = 1$, esto es, el ideal está generado por *un solo elemento*, I se llama *principal*.

(1.19) Operaciones con ideales — Sean I, J ideales de un anillo unitario conmutativo A.

- Suma: Se denota $I + J$, y consiste en todos los elementos de la forma $x + y$, con $x \in I$, $y \in J$. Coincide con el ideal generado por $I \cup J$.
- Producto: Se denota por $I \cdot J$, o simplemente IJ, y es el ideal generado por todos los productos xy, con $x \in I$, $y \in J$. consiste en el conjunto de todos los elementos de la forma
$$x_1 y_1 + \cdots + x_r y_r, \qquad x_1, \ldots, x_r \in I, \quad y_1, \ldots, y_r \in J, \quad r \geq 1.$$
- Intersección: La intersección conjuntista $I \cap J$ es un ideal de A. También es un ideal la intersección *infinita* de ideales.

Ejemplo 1.20

(I) En el anillo $\mathbb{Z}$ de los números enteros todos los ideales son principales. Así, para cada número entero k se tiene el ideal

$$J_k = (k) = \{ pk : p \in \mathbb{Z} \}.$$

(II) En un cuerpo K no hay más ideales que $\{0\}$ y K. Recíprocamente, si un anillo unitario conmutativo K no tiene otros ideales más que $\{0\}$ y K, entonces es un cuerpo.

(III) Consideremos el anillo $A = \mathcal{C}(\mathbb{R}, \mathbb{R})$ del ejemplo 1.9.6, y el ideal $I \subset A$ de todas las funciones continuas $f : \mathbb{R} \to \mathbb{R}$ tales que

$$\text{«Existe } t_f \in \mathbb{R}, \text{ tal que para todo } t \geq t_f \text{ se verifica } f(t) = 0\text{»}.$$

Es un ideal, pues si $f, g \in I$, $h \in A$, se tiene que $t_{f+g} \leq \text{máx}\,\{t_f, t_g\}$, y $t_{hf} \leq t_f$. No es finitamente generado.

Proposición y Definición 1.21 Sean A un anillo unitario conmutativo e I un ideal de A. Se dice que I es **maximal** si verifica una (y, por tanto, ambas) de las dos condiciones equivalentes siguientes:

(I) El anillo cociente A/I es un cuerpo.

(II) I es un ideal propio y ningún otro ideal propio lo contiene estrictamente.

Proposición y Definición 1.22 Sean A un anillo unitario conmutativo e I un ideal de A. Se dice que I es **primo** si verifica una (y, por tanto, ambas) de las dos condiciones equivalentes siguientes:

(I) El anillo cociente A/I es un dominio de integridad.

(II) I es un ideal propio y para cualesquiera $x, y \in A$, si $xy \in I$, entonces $x \in I$ ó $y \in I$.

Ejemplo 1.23

(I) Todo ideal maximal es primo, pues todo cuerpo es dominio de integridad.

(II) El ideal generado por 4 en el anillo $\mathbb{Z}$ no es primo, pues contiene a $4 = 2 \cdot 2$, pero no a 2.

(III) La razón del término ideal *primo* está en que los ideales primos no nulos del anillo $\mathbb{Z}$ son precisamente los generados por los números primos.

(IV) Si I es un ideal primo de un anillo unitario conmutativo A tal que el anillo cociente A/I es finito, entonces I es un ideal maximal.

Definición 1.24 Sean A y B dos anillos unitarios conmutativos. Un **homomorfismo (de anillos unitarios)** de A en B es una aplicación $f : A \to B$ tal que:

(I) $f(x + y) = f(x) + f(y), \quad (x, y \in A).$

(II) $f(x \cdot y) = f(x)f(y), \quad (x, y \in A).$

(III) $f(1_A) = 1_B.$

Ejemplo 1.25 Veamos dos ejemplos de homomorfismos:

- La *conjugación*

$$\begin{aligned} f : \mathbb{Z}[i] &\to \mathbb{Z}[i] \\ x = a + bi &\mapsto \overline{x} = a - bi \end{aligned}$$

es un homomorfismo.

- Sea $A = \mathcal{C}(\mathbb{R}, \mathbb{R})$ el anillo definido en 1.9.6. La *composición* es un homomorfismo. Sea $f \in A$ una función fija y

$$\begin{aligned} \phi : A &\to A \\ g &\mapsto g \circ f. \end{aligned}$$

(1.26) Núcleo de un homomorfismo — Sea $f : A \to B$ un homomorfismo de anillos unitarios conmutativos.

(I) Se llama **núcleo** de f y se denota $\ker f$ el ideal

$$\ker f = \{x \in A : f(x) = 0\}.$$

(II) Se llama **imagen** de f y se denota $\operatorname{im} f$ el anillo

$$\operatorname{im} f = \{y \in B : \text{existe } x \in A \text{ con } y = f(x)\}.$$

Es en efecto un anillo unitario conmutativo con las operaciones heredadas de B.

Proposición 1.27 Teorema de isomorfía Sea $f : A \to B$ un homomorfismo de anillos unitarios conmutativos. Se considera el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle j} \\ A/\ker f & \xrightarrow{\quad \overline{f} \quad} & \operatorname{im} f \end{array}$$

donde $A/\ker f$ es el anillo de clases módulo $\ker f$ y

$$\begin{aligned} p : A &\to A/\ker f \\ x &\mapsto x + \ker f, \end{aligned}$$

$$\begin{aligned} \overline{f} : A/\ker f &\to \operatorname{im} f \\ x + \ker f &\mapsto f(x), \end{aligned}$$

$$\begin{aligned} j : \operatorname{im} f &\to B \\ y &\mapsto y. \end{aligned}$$

En estas condiciones, todas estas aplicaciones son homomorfismos, el diagrama es conmutativo, y

- p es suprayectiva.
- $\overline{f}$ es biyectiva.
- j es inyectiva.

Definición 1.28 Sea $f : A \to B$ un homomorfismo de anillos unitarios conmutativos. Se dice que:

- f es un **epimorfismo**, si es una aplicación suprayectiva.

- f es un **monomorfismo**, si es una aplicación inyectiva.
- f es un **isomorfismo**, si es una aplicación biyectiva.

Ejemplo 1.29

(I) Sean A un anillo unitario conmutativo e I un ideal propio de A. Como en 1.27 podemos definir una aplicación

$$\begin{aligned} p : A &\to A/I \\ x &\mapsto x + I, \end{aligned}$$

que es un epimorfismo.

(II) *Subanillos* — Sea B un anillo unitario conmutativo y $A \subset B$ un subconjunto que, con las operaciones inducidas por B, es a su vez anillo unitario, y tal que $1_A = 1_B$. Entonces se dice que A es un *subanillo* de B, y resulta que la aplicación canónica $A \to B : x \mapsto x$ es un monomorfismo. Análogamente para cuerpos.

Si $\{A_i : i \in I\}$ es una familia de subanillos (subcuerpos) de un mismo anillo B, entonces su intersección

$$A = \bigcap_{i \in I} A_i$$

es a su vez subanillo (subcuerpo) de B.

(III) La conjugación del anillo de enteros de Gauss es un isomorfismo. La aplicación inversa es ella misma.

Proposición 1.30 Sea $f : A \to B$ un homomorfismo de anillos unitarios conmutativos. Como $f(1_A) = 1_B \neq 0$, $\ker f$ es un ideal propio de A, y se verifica:

$$f \text{ es un monomorfismo si y sólo si } \ker f = \{0\}.$$

(1.31) Aplicación — Si $f : K \to B$ es un homomorfismo de anillos unitarios conmutativos y K es un cuerpo, entonces f es necesariamente un monomorfismo, pues al ser $\ker f$ un ideal propio de K, necesariamente es trivial 1.20.(II).

(1.32) Isomorfía — Dos anillos unitarios conmutativos A y B son *isomorfos* cuando existe un isomorfismo $f : A \to B$.

1.2. Divisibilidad

En toda esta sección A es un *dominio de integridad*.

Definición 2.1 Sean x, y elementos de A tales que $x \neq 0$. Se dice que x *divide a* y, que x *es un divisor de* y, que y *es divisible por* x o que y *es múltiplo de* x, si existe $a \in A$ tal que $y = ax$. Se escribe entonces: $x|y$. Si x no divide a y, escribiremos $x \not| y$.

En otras palabras, $x|y$ si y sólo si $y \in (x)$ o, equivalentemente:

$$(y) \subset (x).$$

- Si $y \in A^*$ no es unidad, denotaremos $\mathrm{div}(y)$ el conjunto de todos los divisores de y. Obviamente, los conjuntos $y \cdot U(A)$ y $U(A)$ están contenidos en $\mathrm{div}(y)$. Si y no tiene otros divisores que los anteriores, o sea, que las unidades y los productos del propio y por unidades, se dice que y es *irreducible*.
- Si $y \in A^*$ genera un ideal primo, diremos que y es *primo*. Todo elemento primo es irreducible.

Definición 2.6 Se dice que A es un **dominio euclídeo** (DE) si existe una aplicación

$$\|\cdot\| : A \to \mathbb{N}$$

siendo $\mathbb{N}$ el conjunto de los números enteros no negativos, tal que:

(I) $\|x\| = 0$ si y sólo si $x = 0$.

(II) $\|xy\| = \|x\| \cdot \|y\|$.

(III) Si $x, y \in A^*$, existe $r \in A$, tal que $y|(x - r)$ y $\|r\| < \|y\|$.

Se suele denominar a r el *resto*, y el elemento $q \in A$ tal que $x - r = qy$, *cociente*.

Proposición 2.8 Sea A un dominio euclídeo. Se verifica:

$$U(A) = \{x \in A : \|x\| = 1\}.$$

Proposición 2.10 En un dominio euclídeo todos los ideales son principales.

Definición 2.11 Se llama **dominio de ideales principales** (DIP) a un dominio de integridad en el que todos sus ideales son principales.

Proposición 2.12 Supongamos que A es un dominio de ideales principales. Entonces todo elemento irreducible $a \in A^*$ genera un ideal maximal.

(2.13) Característica de un dominio de integridad — Consideremos de nuevo un dominio A. Si $k \in \mathbb{Z}$, definimos un elemento $k \cdot 1_A \in A$ como sigue:

$$\begin{aligned} k \cdot 1_A &= 1_A + \overbrace{\cdots}^{k} + 1_A && \text{si } k > 0, \\ k \cdot 1_A &= 0 && \text{si } k = 0, \\ k \cdot 1_A &= -((-k) \cdot 1_A) && \text{si } k < 0. \end{aligned}$$

Sea el homomorfismo de anillos:

$$\begin{aligned} \phi = \phi_A : \mathbb{Z} &\to A \\ k &\mapsto k \cdot 1_A. \end{aligned}$$

Consideremos su núcleo $\ker \phi$. Pueden presentarse dos casos:

- $\ker \phi = \{0\}$. Entonces $\mathbb{Z} \subset A$ vía ϕ, y se dice que A tiene *característica 0*. Es así, por ejemplo, para $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i], \ldots$.
- $\ker \phi \neq \{0\}$. Como $\mathbb{Z}/\ker \phi \simeq \operatorname{im} \phi \subset A$ y A es dominio de integridad, $\mathbb{Z}/\ker \phi$ también lo es, y en consecuencia $\ker \phi$ es un ideal primo. Como $\mathbb{Z}$ es un dominio de ideales principales, $\ker \phi = (p)$, y p será un número primo que podemos tomar positivo. En este caso se dice que A tiene *característica (positiva) p*. Obsérvese además que $\mathbb{Z}/(p)$ es de hecho un cuerpo, que se puede considerar contenido en A vía $\overline{\phi}$. (1.27)
  Por ejemplo, todo anillo finito tiene característica positiva: si A es finito, también tiene que serlo $\mathbb{Z}/\ker \phi$, luego su núcleo no es $\{0\}$.
  Si A es subanillo de otro dominio B, $\ker \phi_A = \ker \phi_B$. En consecuencia, A y B tienen igual característica.

Definición 2.14 Sean $x, y \in A^*$. Se dice que $z \in A$ es:

- Un **máximo común divisor** (mcd) de x, y si z divide tanto a x como a y, y es múltiplo de cualquier otro divisor de ambos.
- Un **mínimo común múltiplo** (mcm) de x, y si z es múltiplo de x y de y, y divide a cualquier otro múltiplo de ambos.

Observación 2.15

(I) Hay unicidad del mcd y del mcm.

(II) La descripción del mcd mediante ideales es como sigue:

$$(x)+(y) \subset (z) \subset \bigcap \{I : I \supset (x)+(y) \text{ e } I \text{ es principal}\}.$$

(III) La descripción del mcm mediante ideales es: z es mcm de x, y si y sólo si $(x) \cap (y) = (z)$.

(IV) En general, el mcd puede no existir.

Lema 2.16 Sean $x, y \in A^*$, y supongamos que tienen un mcm z. Entonces $t = xy/z \in A$ y es un mcd de x, y.

Proposición 2.17 Para un dominio de integridad A, son equivalentes:

- Todo par de elementos de A^* tiene mcm.
- Todo par de elementos de A^* tiene mcd.

En ese caso, si $x, y \in A^*$, se verifica:

$$\text{mcm}(x,y) \cdot \text{mcd}(x,y) = xy.$$

Corolario 2.18 Sea A un dominio de ideales principales. Entonces el mcd y el mcm de dos elementos cualesquiera de A^* siempre existe, y se verifica:

(I) $(x)+(y) = (\text{mcd})$.

(II) $(x) \cap (y) = (\text{mcm})$.

(III) $xy = \text{mcd} \cdot \text{mcm}$.

Proposición 2.19 Supóngase que en A se verifica (I) ó (II) de 2.17 (por ejemplo, si A es un *DIP*). Entonces todo elemento irreducible de A es primo.

Proposición 2.20 Identidad de Bezout Supóngase que $x, y \in A^*$ generan un ideal principal (por ejemplo, si A es un *DIP*). Entonces existe $z = \text{mcd}(x,y)$ y

$$z = ax + by$$

con $a, b \in A$.

Definición 2.21 Dos elementos $x, y \in A^*$ se denominan **primos entre sí** cuando no comparten más divisores comunes que las unidades, es decir, cuando $1 = \text{mcd}(x,y)$.

En un *DIP* se verifica:
(P) Todo elemento irreducible es primo.
(MC) Siempre existen mcd y mcm.
(B) La identidad de Bezout.

Proposición 2.22 Sea A un dominio de ideales principales. Para cada elemento $x \in A^*$ que no es unidad se verifica:

(I) Existen elementos irreducibles $a_1, \ldots, a_r$ dos a dos primos entre sí, enteros $\alpha_1, \ldots, \alpha_r > 0$ y $u \in U(A)$ tales que:
$$x = u a_1^{\alpha_1} \cdots a_r^{\alpha_r}$$
Estos a_i se llaman *factores irreducibles* de x.

(II) Los elementos $a_1, \ldots, a_r$ son únicos, salvo producto por unidades de A, así como los elementos $\alpha_1, \ldots, \alpha_r$.

Definición 2.23 Un **dominio de factorización única** (DFU) es un dominio de integridad en el que se cumple:

(P) Todo elemento irreducible es primo.

(F) Todo elemento no nulo que no sea unidad es producto de elementos irreducibles.

Observación 2.24

(I) La condición ***(F)*** por sí sola no garantiza la unicidad de la factorización.

(II) En un DFU siempre existen mcd y mcm.

(III) Las relaciones entre las diversas propiedades estudiadas puede resumirse en el diagrama:

$$\begin{array}{ccccccc} (DE) & \Rightarrow & (DIP) & \Rightarrow & (DFU) & \Rightarrow & \boldsymbol{(F)} \\ & & \Downarrow & & \Downarrow & & \\ & & \boldsymbol{(B)} & \Rightarrow & \boldsymbol{(MC)} & \Rightarrow & \boldsymbol{(P)} \end{array}$$

(V) Los anillos $\mathbb{Z}$ y $\mathbb{Z}[i]$ son DE, luego son DFU. Para $\mathbb{Z}$ reencontramos el *Teorema Fundamental de la Aritmética*.

(VI) El estudio de la divisibilidad es más fácil en un anillo A que es DFU, utilizando las factorizaciones precisamente. Un par de ejemplos:

- Si $x^4 | y^2$, entonces $x^2 | y$.
- Si x e y son primos entre sí y su producto es un cuadrado en A, entonces ambos son cuadrados en A.

(2.26) Ecuaciones diofánticas lineales con dos incógnitas — Se denomina así a una ecuación de la forma:
$$aX + bY = c,$$
donde los coeficientes a, b, c son elementos de un dominio A fijado, y las soluciones $X = x$ e $Y = y$ deben ser elementos de ese dominio.

(I) Se podrá resolver la ecuación si y sólo si existe $d = \text{mcd}(a, b)$ y es de la forma
$$d = \alpha a + \beta b, \qquad \text{con } \alpha, \beta \in A,$$
tal que $d | c$. Tendremos:
$$a = a_0 d, \quad b = b_0 d, \quad c = c_0 d,$$
$$1 = \alpha a_0 + \beta b_0.$$
Así la ecuación es equivalente a $a_0 X + b_0 Y = c_0$ y si x, y son soluciones entonces existe $t = \beta x - \alpha y$ tal que:
$$\begin{cases} x = \alpha c_0 + b_0 t \\ y = \beta c_0 - a_0 t \end{cases} \quad (t \in A).$$

(II) Si A es subanillo de otro anillo unitario B, y $a, b \in A$ cumplen una identidad de Bezout como en (I), las soluciones en B se expresan de igual manera (con soluciones adicionales) pero con $t \in B$.

(2.27) Algoritmo de Euclides — Se cumplirá una identidad de Bezout *siempre* si A es un *DIP*. Veamos cómo es posible dar un algoritmo para el mcd cuando A es un *DE*, utilizando la aplicación $\|\cdot\| : A \to \mathbb{N}$.

(I) **Cálculo del mcd mediante el algoritmo de Euclides:**
Sean $a, b \in A^*$ con, por ejemplo, $\|b\| \leq \|a\|$. Ponemos $x_0 = a$, $x_1 = b$, y por tanto existe un número finito de igualdades

$$(*) \begin{cases} x_0 &= y_1 x_1 + x_2 \\ x_1 &= y_2 x_2 + x_3 \\ x_2 &= y_3 x_3 + x_4 \\ &\vdots \\ x_{r-2} &= y_{r-1} x_{r-1} + x_r \\ x_{r-1} &= y_r x_r \end{cases}$$

con $\|x_0\| \geq \|x_1\| > \cdots > \|x_r\| > 0$. Así, $d = x_r = \mathrm{mcd}(x_0, x_1) = \mathrm{mcd}(a, b)$, «el máximo común divisor es el último resto no nulo».

(II) **Identidad de Bezout:**
Las ecuaciones $(*)$ permiten calcular $\alpha, \beta \in A$ tales que

$$d = \alpha a + \beta b.$$

Para ello obsérvese que podemos ir calculando sucesivamente $x_2, \ldots, x_r$ en función de $a = x_0$ y $b = x_1$. Al final, obtenemos α y β en función de $y_1, \ldots, y_{r-1}$, y la expresión buscada es:

$$d = x_r = \alpha a + \beta b.$$

1.3. Congruencias

Algunas propiedades de $\mathbb{Z}$ son:

(3.1) Un número entero p es irreducible si y sólo si es primo, si y sólo si genera un ideal maximal, si y sólo si $\mathbb{Z}/(p)$ es cuerpo.

(3.2) El anillo $\mathbb{Z}$ es un *DFU*.

(3.3) El conjunto de los números primos es infinito.

(3.4) Anillo de restos — Sea n un número entero. Se llama **anillo de restos módulo** n al anillo cociente $\mathbb{Z}/(n)$. Sea $k \in \mathbb{Z}$, denotaremos $[k]_n$, e incluso $[k]$, la clase de k, $k + (n) = \{k + qn : q \in \mathbb{Z}\}$. Se tiene:

$$\mathbb{Z}/(n) = \{[0], [1], \ldots, [n-1]\}.$$

(3.5) Ideales de un anillo de restos — Sea $n > 1$. Por 1.16.2 los ideales de $\mathbb{Z}/(n)$ están en biyección con los ideales $I \subset \mathbb{Z}$ que contienen a (n). Luego resulta que los ideales de $\mathbb{Z}/(n)$ están en biyección con los divisores positivos de n.

(3.6) Homomorfismos entre anillos de restos —

(I) No existe ningún homomorfismo de anillos unitarios $f : \mathbb{Z}/(n) \to \mathbb{Z}$ con $n > 0$.

(II) La identidad es el único homomorfismo de anillos unitarios $f : \mathbb{Z} \to \mathbb{Z}$.

(III) El *homomorfismo canónico* es el único homomorfismo de anillos unitarios $f : \mathbb{Z} \to \mathbb{Z}/(n)$ con $n > 1$.

$$f(k) = [k].$$

(IV) Sea $n > 1$. Si n no divide a m, no existe ningún homomorfismo de anillos unitarios $f : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$.

(V) Sea $n > 1$ y $n|m$. Existe un único homomorfismo de anillos unitarios $f : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$, que es epimorfismo. Se trata por el definido por $f([k]_m) = [k]_n$.

Proposición 3.7 Teorema chino del resto Si a, b son enteros primos entre sí, se tiene un isomorfismo de anillos unitarios

$$\mathbb{Z}/(ab) \simeq \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

El teorema anterior proporciona una condición *suficiente* para resolver un sistema de congruencias

$$\begin{cases} X \equiv m \mod a \\ X \equiv n \mod b \end{cases}$$

donde a, b, m, n son números dados: si a y b son primos entre sí, por el teorema anterior existe un entero x tal que

$$f([x]_{ab}) = ([m]_a, [n]_b),$$

siendo

$$f([x]_{ab}) = ([x]_a, [x]_b).$$

Proposición 3.8 Sean $n > 1$ y $k \in \mathbb{Z}$. Son equivalentes:

(I) $[k] \in U(\mathbb{Z}/(n))$.

(II) $\text{mcd}(k, n) = 1$.

(III) $[k] \neq 0$ y no es divisor de cero en $\mathbb{Z}/(n)$.

Definición 3.9 Sea m un entero positivo. Se denota por $\phi(m)$ el número de enteros k tales que

$$0 < k \leq m \quad y \quad \text{mcd}(k, m) = 1.$$

La aplicación: $m \mapsto \phi(m)$ se denomina **indicador de Euler**.

Observación 3.10

(I) Los primeros valores de ϕ son:

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \ldots$$

(II) Si $n > 1$, entonces $\phi(n)$ es el número de unidades de $\mathbb{Z}/(n)$.

(III) Si $p > 1$ es primo, entonces $\mathrm{mcd}(k, p) = 1$ para todo $0 < k < p$, y por tanto, $\phi(p) = p - 1$.

(IV) Si $\phi(p) = p - 1$, entonces p es primo.

(3.11) Cálculo del indicador de Euler — Sea

$$m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

la factorización de m. Entonces

$$\phi(m) = m \cdot \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Proposición 3.12 (Gauss) Para cada entero positivo n se verifica:

$$n = \sum_{d|n,\, d>1} \phi(d).$$

Proposición 3.13 (Euler) Si $n > 1$ y k son enteros primos entre sí, entonces:

$$k^{\phi(n)} \equiv 1 \mod n.$$

Corolario 3.14 (Pequeño Teorema de Fermat) Sea p un número primo y k un entero. Entonces:

$$k^p \equiv k \mod p.$$

Proposición 3.15 (Teorema de Wilson) Sea p un número primo. Entonces:

$$(p-1)! \equiv -1 \mod p.$$

Corolario 3.16 Sea p un número primo impar. Entonces $\frac{1}{2}(p-1) \in \mathbb{Z}$ y

$$\left(\left(\tfrac{1}{2}(p-1)\right)!\right)^2 \equiv (-1)^{\frac{1}{2}(p+1)} \mod p.$$

Tema 2

Polinomios

2.1. Generalidades

Sean A un anillo conmutativo y unitario y n un entero ≥ 1.

(1.1) Dado A como anteriormente, existe, y es único salvo isomorfismo, un anillo conmutativo y unitario B, y n elementos $X_1, \ldots, X_n \in B$ tales que

(I) A es subanillo de B.

(II) Cada elemento $f \in B$ se escribe de una única manera como una suma:

$$f = \sum_{v=(v_1,\ldots,v_n)} a_v X_1^{v_1} \cdots X_n^{v_n},$$

donde los a_v son elementos de A, todos nulos salvo para una cantidad finita de índices.

Definición 1.2 El anillo que cumple las propiedades anteriores se denomina **anillo de polinomios en n indeterminadas con coeficientes en A**, y se denota por $A[X_1, \ldots, X_n]$.

(1.5) Evaluación de polinomios — Sean A un anillo conmutativo unitario, $X_1, \ldots, X_n$ indeterminadas. Sea B un anillo que contiene a A como subanillo, y fijemos n elementos $x_1, \ldots, x_n \in B$. Definimos la **evaluación** en $x_1, \ldots, x_n$ por

$$\begin{aligned} ev : A[X_1, \ldots, X_n] &\longrightarrow B \\ f = \sum_v a_v X_1^{v_1} \cdots X_n^{v_n} &\longmapsto f(x_1, \ldots, x_n) = \sum_v a_v x_1^{v_1} \cdots x_n^{v_n}. \end{aligned}$$

Es claro que ev es un homomorfismo.

(1.6) Funciones polinomiales — Sean A un anillo conmutativo unitario, $X_1, \ldots, X_n$ indeterminadas, y f un polinomio de $A[X_1, \ldots, X_n]$. Sea B un anillo conmutativo y unitario que contenga a A como subanillo. Definimos una aplicación asociada a f como sigue:

$$\begin{aligned} F : B \times \overset{(n)}{\cdots} \times B &\longrightarrow B \\ (x_1, \ldots, x_n) &\longmapsto f(x_1, \ldots, x_n). \end{aligned}$$

Una aplicación tal como F, definida a través de un polinomio se llama **función polinomial**, y debe distinguirse siempre del polinomio que la define.

(1.7) Grado — Dado un polinomio *no nulo* $f = \sum_v a_v X_1^{v_1} \cdots X_n^{v_n}$ de $A[X_1, \ldots, X_n]$, la condición de que sólo una cantidad finita de los coeficientes a_v sean no nulos, garantiza que los números siguientes existen:

- $\operatorname{gr} f = \partial f = \operatorname{máx} d \geq 0$ tal que existe $a_v \neq 0$ con $v_1 + \cdots + v_n = d$.
- $\operatorname{gr}_i f = \partial_i f = \operatorname{máx} d \geq 0$ tal que existe $a_v \neq 0$ con $v_i = d$, $(i = 1, \ldots, n)$.

Estos números se llaman, respectivamente, **grado total** y **grado parcial** (en X_i para $i = 1, \ldots, n$) de f.

Por convenio pondremos

$$\partial 0 = \partial_1 0 = \cdots = \partial_n 0 = -\infty.$$

Si sólo se considera una variable, se habla simplemente de *grado*, pues sólo hay uno posible. En este caso escribimos $f = a_0 T^n + a_1 T^{n-1} + \cdots + a_n$, se dice que a_0 es el **coeficiente director** de f. Cuando $a_0 = 1$, diremos que f es **mónico**.
Se verifican las siguientes fórmulas: Sean $f, g \in A[X_1, \ldots, X_n]$, entonces:

(I) $\partial(f + g) \leq \operatorname{máx}\{\partial f, \partial g\}$.

(II) $\partial(f \cdot g) \leq \partial f + \partial g$.

Y lo mismo para los grados parciales.

(1.8) Componentes homogéneas — Sea $f \in A[X_1, \ldots, X_n]$, $p = \partial f$. Agrupando sumandos de igual grado (total), podemos escribir

$$f = \sum_v a_v X_1^{v_1} \cdots X_n^{v_n} = f_0 + f_1 + \cdots + f_p,$$

donde

$$f_r = \sum_{v_1 + \cdots + v_n = r} a_v X_1^{v_1} \cdots X_n^{v_n} \quad \text{para } 0 \leq r \leq p, \quad f_p \neq 0.$$

Los polinomios $f_0, \ldots, f_p$ se denominan **componentes homogéneas** de f.

- El polinomio no nulo f se denomina *homogéneo* si tiene una única componente homogénea.
- El polinomio nulo se considera homogéneo.
- Habitualmente un polinomio homogéneo se denomina **forma homogénea**.
- Un tipo particular de formas son los **monomios**: aquellas que sólo tienen un sumando, esto es, son del tipo
$$a_v X_1^{v_1} \cdots X_n^{v_n}.$$
- El producto de formas homogéneas es de nuevo una forma homogénea (eventualmente nula).

Proposición 1.9 Un anillo de polinomios $A[X_1, \ldots, X_n]$ es dominio de integridad si y sólo si lo es A.

Corolario 1.10 Si A es un dominio de integridad,

$$\partial(fg) = \partial f + \partial g$$

para cualesquiera $f, g \in A[X_1, \ldots, X_n]$ (lo mismo vale para los grados parciales).

Corolario 1.11 Si A es un dominio de integridad,

$$U(A) = U(A[X_1, \ldots, X_n]).$$

(1.12) Cuerpos de funciones racionales — Sean A un dominio de integridad y K su cuerpo de fracciones. Como A es dominio, $A[X_1, \ldots, X_n]$ también lo es, y tiene cuerpo de fracciones F. Resulta que los elementos de F son «fracciones» f/g con

$$f, g \in A[X_1, \ldots, X_n], \quad g \neq 0.$$

Podemos definir una aplicación

$$\phi : f/g \longmapsto (cdf)/(cdg) \in F,$$

siendo c el producto de los denominadores de los coeficientes de f y d el producto de los denominadores de los coeficientes de g.
(1.12.1) Los cuerpos de fracciones de $A[X_1, \ldots, X_n]$ y $K[X_1, \ldots, X_n]$ se identifican mediante el isomorfismo anterior, y se denotan por

$$K(X_1, \ldots, X_n).$$

Definición 1.12.2 El cuerpo $K(X_1, \ldots, X_n)$ se denomina **cuerpo de funciones racionales con coeficientes en K en n indeterminadas**.

(1.13) Derivación — Consideramos un anillo de polinomios $A[T]$ con coeficientes en un anillo A, en la indeterminada T. La **derivada** de un polinomio

$$f = a_0 + a_1 T + \cdots + a_p T^p$$

es, por definición, el polinomio

$$\frac{\partial f}{\partial T} = a_1 + 2a_2 T + \cdots + p a_p T^{p-1}.$$

Se deduce:

(I) $\dfrac{\partial}{\partial T}(f+g) = \dfrac{\partial f}{\partial T} + \dfrac{\partial g}{\partial T}$; $\quad \dfrac{\partial}{\partial T}(fg) = f \cdot \dfrac{\partial g}{\partial T} + \dfrac{\partial f}{\partial T} \cdot g$ *(Leibniz)*.

(II) Las derivadas de orden superior se definen por inducción:

$$\frac{\partial^s f}{\partial T^s} = \frac{\partial}{\partial T}\left(\frac{\partial^{s-1} f}{\partial T^{s-1}}\right), \quad s \geq 2.$$

(III) Es claro que:

$$\frac{\partial^p f}{\partial T^p} = p! a_p, \quad \frac{\partial^s f}{\partial T^s} = 0 \quad \text{para } s > p.$$

Fórmula de Leibniz generalizada: $\dfrac{\partial^s}{\partial T^s}(f \cdot g) = \displaystyle\sum_{k=0}^{s} \binom{s}{k} \frac{\partial^{s-k} f}{\partial T^{s-k}} \cdot \frac{\partial^k g}{\partial T^k}$.

2.2. División de polinomios

En esta sección A denotará a un dominio de integridad.

Lema 2.1 Sean $g \in A[T]$ un polinomio de grado positivo, y $a \neq 0$ su coeficiente director. Entonces para cualquier $f \in A[T]$ existen $Q, R \in A[T]$ tales que

$$a^r f = Q \cdot g + R, \quad \partial R < \partial g,$$

siendo $r = \text{máx}\{\partial f - \partial g + 1, 0\}$. Además, Q y R son únicos con estas condiciones.

Corolario 2.2 (Regla de Ruffini) Sea $c \in A$ fijo. Para cada $f \in A[T]$ existe $Q \in A[T]$ tal que $f = Q \cdot (T - c) + f(c)$.
En particular, $(T - c) | f$ si y sólo si $f(c) = 0$.

Corolario 2.3 Un polinomio *no nulo* $f \in A[T]$ tiene a lo más $p = \partial f$ ceros distintos en A.

Corolario 2.4 (Principio de prolongación de identidades polinomiales) Supongamos que A es un dominio de integridad *infinito*. Sean $f, g \in A[X_1, \ldots, X_n]$ dos polinomios tales que:

Existe otro $\ell \in A[X_1, \ldots, X_n]$ no nulo de modo que para cualesquiera $x_1, \ldots, x_n \in A$ con $\ell(x_1, \ldots, x_n) \neq 0$ se tiene $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$. Entonces $f = g$.

(2.5) Puede utilizarse el grado para introducir una aplicación

$$\|\cdot\| : A[T] \to \mathbb{N}$$

y estudiar si hace de $A[T]$ un dominio euclídeo:

$$\|f\| = 2^{\partial f} \quad (\text{convenimos } 2^{-\infty} = 1/2^{\infty} = 1/\infty = 0).$$

Proposición 2.6 Las siguientes afirmaciones son equivalentes:

(I) A es cuerpo.

(II) $A[T]$ es dominio euclídeo *(DE)*.

(III) $A[T]$ es dominio de ideales principales *(DIP)*.

Proposición 2.7 (Teorema de Gauss) Las siguientes afirmaciones son equivalentes:

(I) A es un dominio de factorización única *(DFU)*.

(II) $A[T]$ es un dominio de factorización única *(DFU)*.

(III) $A[X_1, \ldots, X_n]$ es un dominio de factorización única *(DFU)*.

Corolario 2.7.1 $K[X_1, \ldots, X_n]$ es un dominio de factorización única *(DFU)*.

(2.9.1) Un elemento $a \in A$ es irreducible en A si y sólo si lo es en $A[T]$.

(2.10.1) Se llama **contenido** de un polinomio $f \in A[T]$ y se denota $\mathbf{c}(f)$ al máximo común divisor (en A) de sus coeficientes.

(2.10.2) Si $f \in A[T]$, entonces $\mathbf{c}(f)|f$ y $f = \mathbf{c}(f)f_1$, siendo $\mathbf{c}(f_1) = 1$.

(2.10.3) Si $f, g \in A[T]$, entonces $\mathbf{c}(fg) = \mathbf{c}(f)\mathbf{c}(g)$.

(2.10.4) Si $f \in A[T]$ es irreducible en $A[T]$ y tiene grado positivo, entonces $\mathbf{c}(f) = 1$ y f es irreducible en $K[T]$.

(2.10.5) Si $f \in A[T]$ es irreducible en $A[T]$, entonces genera un ideal primo en $A[T]$.

(2.10.6) Todo polinomio $f \in A[T]$ no nulo y no unidad es producto de polinomios irreducibles de $A[T]$.

Observación 2.11.2 Suponemos que A es *DFU*. Un polinomio $f \in A[T]$ con contenido 1 es irreducible en $A[T]$ si y sólo si lo es en $K[T]$.

Proposición 2.13 Sean A un dominio de integridad y $f_1, \ldots, f_s \in A[T]$ polinomios de grados $n_1 \geq 1, \ldots, n_s \geq 1$. Entonces existen un cuerpo $L \supset A$, entendiéndose que A es subanillo de L, y elementos

$$a_{i0}, x_{i1}, \ldots, x_{in_i} \in L, \quad i = 1, \ldots, s,$$

tales que

$$f_i = a_{i0}(T - x_{i1}) \cdots (T - x_{in_i}), \quad i = 1, \ldots, s.$$

2.3. Factorización

(3.2) Factorización de Kronecker — Supondremos que A tiene característica cero y que $U(A)$ es finito.

Sea $f \in A[T]$, $\mathbf{c}(f) = 1$, $\partial f = d > 0$, y sea s el mayor entero $\leq d/2$. Podemos elegir $s+1$ elementos distintos $n_0, n_1, \ldots, n_s \in \mathbb{Z} \subset A$ tales que

$$f(n_0) \neq 0, \ldots, f(n_s) \neq 0.$$

Para cada $i = 0, 1, \ldots, s$, consideramos el conjunto D_i de todos los divisores en A de $f(n_i) = p_{i1}^{\alpha_1} \cdots p_{ir}^{\alpha_r}$:

$$D_i = \left\{ u \cdot p_{i1}^{\gamma_1} \cdots p_{ir}^{\gamma_r} : u \in U(A),\ 0 \leq \gamma_i \leq \alpha_i,\ i = 1, \ldots, r \right\}.$$

Finalmente ponemos $D = D_0 \times \cdots \times D_s$, y para cada $M = (m_0, \ldots, m_s) \in D$ introducimos el polinomio

$$f_M = \sum_{k=0}^{s} m_k \prod_{\substack{l=0 \\ l \neq k}}^{s} \frac{T - n_l}{n_k - n_l} \in K[T], \quad \partial f_M \leq s.$$

Se tiene:

$$f_M(n_j) = m_j, \quad j = 0, 1, \ldots, s.$$

(3.2.3) Si f es reducible en $K[T]$, algún $f_M \in A[T]$ tiene grado ≥ 1 y divide a f. Esta observación significa que dividiendo f por todos los f_M concluiremos: o bien que f es irreducible (ninguno lo divide), o bien lo contrario. En este último caso, además, encontramos una factorización $f = f_M \cdot h$.

Proposición 3.4 Sea $f \in K[T]$, $2 \leq \partial f \leq 3$. Son equivalentes.

(I) f es reducible.

(II) f tiene alguna raíz en K.

Proposición 3.5 Sea $f = a_0 + a_1T + \cdots + a_pT^p \in A[T]$, $a_p \in U(A)$. Entonces toda raíz de f en K está de hecho en A, y es un divisor de $a_0 = f(0)$ en A. Por tanto, las raíces de f en K se obtienen comprobando qué divisores de $f(0)$ en A lo son.

Proposición 3.7 Criterio de Eisenstein Sea $f = a_0 + a_1T + \cdots + a_pT^p \in A[T]$ con contenido 1, y $d \in A$ un elemento irreducible. Supongamos que

$$d|a_0, \ldots, d|a_{p-1},\ d^2 \not| a_0.$$

Entonces f es irreducible.

Proposición 3.8 Criterio de traslación Sea $f \in A[T]$. Son equivalentes:

(I) f es irreducible en $A[T]$.

(II) Para cada $a \in A$, $f(a+T)$ es irreducible.

(III) Existe $a \in A$ tal que $f(a+T)$ es irreducible.

El mismo enunciado es válido cambiando A por K.

Proposición 3.10 Criterio del módulo finito Sea

$$f = a_0 + a_1T + \cdots + a_pT^p \in A[T], \quad a_p \in U(A).$$

Supongamos que existe un elemento irreducible $d \in A$, tal que en $A/(d)[T]$ el polinomio siguiente es irreducible:

$$\overline{f} = \overline{a}_0 + \overline{a}_1T + \cdots + \overline{a}_pT^p, \quad \overline{a}_i = a_i + (d).$$

Entonces f es irreducible.

Ejercicio 23 Criterio de irreducibilidad de Netto Sea

$$f = a_0 + a_1T + \cdots + a_{2m+1}T^{2m+1}$$

un polinomio con coeficientes enteros. Supóngase que existe un primo p tal que:

(I) $p \not| a_{2m+1}$.

(II) $p|a_k$ si $m < k \leq 2m$.

(III) $p^2|a_k$ si $k \leq m$.

(IV) $p^3 \not| a_0$.

Entonces f es irreducible en $\mathbb{Q}[T]$.

Ejercicio 59 Sea K un cuerpo, $a, c \in K - \{0\}$, $b \in K$. Entonces

$$aT^2 + bT + c \text{ irreducible en } K[T] \iff aX^2 + bXY + cY^2 \text{ irreducible en } K[X,Y].$$

Tema 3

Extensiones de cuerpos

3.1. Generalidades

Definición 1.1

(I) Sean K, E cuerpos. Se dice que E es una **extensión** de K y se escribe E/K cuando existe un homomorfismo de cuerpos $j : K \to E$. Como K es cuerpo, j es un monomorfismo, y, por tanto, K es isomorfo a su imagen $j(K)$. Podemos entonces identificar K con $j(K)$, un subcuerpo de E.

(II) Un **homomorfismo** (respectivamente *isomorfismo*) **de una extensión** E_1/K en otra E_2/K es un homomorfismo de cuerpos (respectivamente isomorfismo) $\phi : E_1 \to E_2$ que induce la identidad en K (aquí ya estamos suponiendo $K \subset E_1$, $K \subset E_2$). Se denotará $\phi : E_1/K \to E_2/K$.

Proposición 1.3 Sea E/K una extensión de cuerpos. Entonces E tiene una estructura canónica de espacio vectorial sobre K.

Definición 1.4 Sea E/K una extensión de cuerpos. Se llama **grado de la extensión**, y se denota $[E : K]$, la dimensión $\dim_K E$ de E como espacio vectorial sobre K.

Definición 1.5 Una extensión de cuerpos cuyo grado es finito se denomina **extensión finita**.

Proposición 1.6 Sean L/K y E/L dos extensiones de cuerpos. Son equivalentes:

(I) L/K y E/L son finitas.

(II) E/K es finita.

Además en ese caso:

$$[E : K] = [E : L][L : K].$$

Corolario 1.7 Sean E/L y L/L' dos extensiones finitas de cuerpos. Si

$$[E : L] = [E : L']$$

entonces $L = L'$.

Observación 1.8 Sea K un subcuerpo de E (y, por tanto, tenemos una extensión E/K). Si $[E : K] = 1$, entonces $E = K$.

(1.9) Si $[E : K]$ es un número primo, no existen **subextensiones propias** (es decir, distintas de E/K y K/K).

(1.10) Subextensión generada por un subconjunto — Sea E/K una extensión de cuerpos, no necesariamente finita, que supondremos corresponde a una inclusión $K \subset E$. Sea

$$A = \{a_i : i \in I\} \subset E$$

un subconjunto arbitrario (eventualmente infinito) no vacío.

Denotaremos $K(A)$ la intersección de todos los subcuerpos $L \subset E$ que contengan a K y A. En virtud de (I.1.29.2) esta intersección es un cuerpo. De esta manera, $K(A)$ es el *menor subcuerpo de E que contiene a K y A.*

El cuerpo $K(A)$ se denomina **cuerpo generado por A sobre K**. La igualdad $L = K(A)$ se expresa diciendo que **L está generado por A sobre K**.

Un elemento $x \in E$ está en $K(A)$ si y sólo si existen $r \geq 1$, elementos $a_1, \ldots, a_r \in A$ y polinomios $f, g \in K[X_1, \ldots, X_r]$ en r indeterminadas $X_1, \ldots, X_r$ tales que

$$g(a) \neq 0 \quad \text{y} \quad x = f(a)/g(a),$$

donde $a = (a_1, \ldots, a_r)$.

Definición 1.11 Se dice que una extensión de cuerpos L/K es **finitamente generada** cuando L está generado sobre K por un conjunto finito. Si ese conjunto consta de un solo elemento, se dice que la extensión es **simple**.

Si L está generado sobre K por $A = \{a_1, \ldots, a_n\}$, se denota

$$L = K(a_1, \ldots, a_n).$$

Definición 1.13 Sean E/K una extensión de cuerpos y $a_1, \ldots, a_n$, elementos de E. Se tiene un homomorfismo (de evaluación)

$$\begin{aligned} K[X_1, \ldots, X_n] &\longrightarrow E \\ f &\longmapsto f(a_1, \ldots, a_n) \end{aligned}$$

cuyo núcleo denotaremos I.

(I) Se dice que $a_1, \ldots, a_n$ son **algebraicamente independientes** sobre K si $I = \{0\}$, esto es, $f(a_1, \ldots, a_n) \neq 0$ para todo polinomio no nulo $f \in K[X_1, \ldots, X_n]$.

(II) Se dice que $a_1, \ldots, a_n$ son **algebraicamente dependientes** sobre K si $I \neq \{0\}$, esto es, $f(a_1, \ldots, a_n) = 0$ para algún polinomio no nulo $f \in K[X_1, \ldots, X_n]$.

(1.14) Observaciones y Ejemplos

(I) Si $a_1, \ldots, a_n \in E$ son algebraicamente independientes sobre K, se tiene un isomorfismo de anillos

$$K[X_1, \ldots, X_n] \simeq K[a_1, \ldots, a_n] \subset E,$$

que induce otro de cuerpos

$$K(X_1, \ldots, X_n) \simeq K(a_1, \ldots, a_n) \subset E.$$

Es claro que cualesquiera indeterminadas distintas $X_1, \ldots, X_n$ son algebraicamente independientes sobre K.

(II) Si $a_1, \ldots, a_n \in E$ son algebraicamente independientes sobre K también lo son $a_{i_1}, \ldots, a_{i_r}$ para cualesquiera $1 \leq i_1 < \cdots < i_r \leq n$.

(III) Si $n = 1$ y a_1 es algebraicamente independiente sobre K se dice que a_1 es **trascendente sobre K**.

(IV) Supongamos $n = 1$ y que a_1 es algebraicamente dependiente sobre K. En este caso se dice simplemente que a_1 es **algebraico sobre K**. Entonces se tiene un isomorfismo

$$K[X_1]/I \simeq K[a_1] \subset E.$$

Se deduce que $K[X_1]/I$ es un cuerpo. También lo es $K[a_1]$, y concluimos

$$K[a_1] = K(a_1).$$

(V) En $K(T)$, T indeterminada, los elementos $a_1 = T$, $a_2 = T^2$, son algebraicamente dependientes: tómese $f = X_1^2 - X_2$ y queda

$$f(a_1, a_2) = a_1^2 - a_2 = T^2 - T^2 = 0.$$

(1.15) Existencia de números trascendentes: El teorema de Cantor — El conjunto de números complejos algebraicos sobre $\mathbb{Q}$ es numerable.

3.2. Extensiones simples

En toda esta sección E/K denota una extensión simple, esto es, E está generado sobre K por cierto elemento $\alpha \in E$.

(2.1) Caso en que α es trascendente — Entonces $T \mapsto \alpha$ define un isomorfismo $K(T) \simeq K(\alpha) = E$ y E es un *cuerpo de funciones racionales en* α. Diremos que E/K es una **extensión simple trascendente**.

(2.2) Caso en que α es algebraico — Entonces $T \mapsto \alpha$ define un epimorfismo $K[T] \to K[\alpha] = E$ y E es un *anillo de polinomios en* α. Diremos que E/K es una **extensión simple algebraica**.

Supongamos que α es algebraico sobre K. Entonces tenemos un epimorfismo canónico

$$K[T] \to E,$$

cuyo núcleo está generado por un *polinomio irreducible* f. Sabemos que f está determinado salvo unidades de $K[T]$, esto es, salvo elementos de K^*. Para definir f sin ambigüedad basta elegirlo *mónico*. El polinomio f se denomina **polinomio mínimo de α sobre K**, y se denota

$$f = P(\alpha, K) \in K[T].$$

Así pues, $P(\alpha, K)$ es el único polinomio mónico irreducible de $K[T]$ que tiene α por raíz. Cualquier otro polinomio de $K[T]$ del que α sea raíz es múltiplo de $P(\alpha, K)$.

Proposición 2.3 Supongamos que el polinomio mínimo de α sobre K tiene grado n. Entonces $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de E sobre K, y en consecuencia,

$$[E : K] = n,$$

con lo que la extensión E/K es finita.

Proposición 2.5 (Lüroth) Sea E/K una extensión simple trascendente. Entonces toda subextensión no trivial L/K es también simple trascendente.

Proposición 2.6 Sea E/K una extensión simple algebraica. Entonces toda subextensión no trivial L/K es también simple algebraica.
En este caso, además, hay una cantidad finita de subextensiones.

Ejemplo 2.7

(I) Si E/K, $E = K(\alpha)$, es trascendente, el número de subextensiones es infinito. Por ejemplo, tómese

$$L_n = K(\alpha^n) \supset K, \quad n \geq 1.$$

3.3. Extensiones finitamente generadas

En toda esta sección E/K es una extensión finitamente generada.

Definición 3.1 Se llama **grado de trascendencia** de E/K y se denota gr. trans. E/K, el mayor número posible de elementos de E algebraicamente independientes sobre K.

Proposición 3.2 La extensión E/K tiene grado de trascendencia cero si y sólo si es finita.
(3.2.1) Todos los elementos de una extensión finita E/K son algebraicos sobre K.

Lema 3.3 Sean $a_1, \ldots, a_n \in E$ y denotemos

$$\begin{aligned} K_0 &= K, \\ K_i &= K(a_1, \ldots, a_i), \quad i = 1, \ldots, n. \end{aligned}$$

Entonces son equivalentes:

(I) $a_1, \ldots, a_n$ son algebraicamente independientes sobre K.

(II) a_i es trascendente sobre K_{i-1}, para cada $i = 1, \ldots, n$.

Ejemplo 3.4 Supongamos que E/K es simple trascendente. Entonces

$$\text{gr. trans. } E/K = 1.$$

Proposición 3.5 (Steinitz) El grado de trascendencia de una extensión finitamente generada, no finita, E/K, es un entero $r \geq 1$, caracterizado por la propiedad siguiente:
Existen r elementos $\alpha_1, \ldots, \alpha_r \in R$ algebraicamente independientes sobre K, tales que $E/K(\alpha, \ldots, \alpha_r)$ es una extensión finita.

(3.5.1) Existen s elementos $\beta_1, \ldots, \beta_s \in E$ algebraicamente independientes sobre K, tales que $E/K(\beta_1, \ldots, \beta_s)$ es finita.

(3.5.2) Si $\alpha \in E$ es trascendente sobre K, entonces podemos sustituir algunos de los β_i por α, de modo que $\beta_1, \ldots, \alpha, \ldots, \beta_s$ también cumplen (3.5.1).

Corolario 3.7 Si E/K está generada por n elementos, entonces gr. trans. $E/K \leq n$.

Corolario 3.8 Sean E/K, L/K extensiones finitamente generadas. Entonces

$$\text{gr. trans. } E/K = \text{gr. trans. } E/L + \text{gr. trans. } L/K.$$

Proposición 3.9 (Teorema del elemento primitivo) Si E/L es una extensión finita de cuerpos de característica cero, entonces es simple algebraica: $E = L(\alpha)$ para algún $\alpha \in E$. Tal α se llama **elemento primitivo** de la extensión.

(3.9.1) Si $f \in L[T]$ es irreducible, y $c \in E'$ una raíz suya en una extensión E' de L, entonces $(T-c)^2 \not| f$ en $E'[T]$.

Tema 4

Teoría de Galois

4.1. Grupos de automorfismos

En toda esta sección K será un cuerpo de característica cero y E/K una extensión.

Un isomorfismo $E/K \simeq E/K$ es un isomorfismo de cuerpos $\phi : E \to E$ tal que $\phi|_K = \mathrm{id}_K$. Un tal isomorfismo se llama **automorfismo**, y el conjunto de todos ellos se denota $\mathrm{Aut}(E : K)$ ó $G(E : K)$. Es un grupo para la composición de aplicaciones, y se denomina **grupo de automorfismos** de E/K. El elemento neutro es $e = \mathrm{id}_E$.

Observación 1.1 Si denotamos $\mathrm{Aut}(E)$ ó $G(E)$ el conjunto de todos los isomorfismos de cuerpos $\phi : E \to E$, entonces $G(E)$ es un grupo que contiene a $G(E : K)$ como subgrupo. Estos dos grupos son, en general, distintos.

Proposición 1.2 Si E'/K es una extensión isomorfa a E/K, entonces $G(E' : K)$ y $G(E : K)$ son isomorfos.

(1.3) Grupo de automorfismos de una extensión simple trascendente — Sea E/K una extensión simple trascendente, esto es: $E = K(\alpha)$ con α trascendente sobre K. Al analizar el comportamiento de un automorfismo $\phi \in G(E : K)$ es útil observar:

(1.3.1) ϕ está completamente determinado por el elemento $\phi(\alpha) \in E$.

(1.3.2) Sea $M_2(K)$ el anillo de las matrices de orden 2 con coeficientes en K. Es sabido que el grupo de unidades $U = U(M_2(K))$ consiste en las matrices cuyo determinante no es nulo. Definimos el siguiente epimorfismo de grupos:

$$\begin{aligned} \Psi : U &\to G(E : K) \\ u &\mapsto \phi \end{aligned}$$

tal que si $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces $\phi(\alpha) = \dfrac{a\alpha + b}{c\alpha + d}$.

(1.3.3) Por el primer teorema de isomorfía de grupos se tiene

$$U/K^* \simeq G(E : K),$$

donde $K^* \simeq \ker \Psi$.

(1.4) Grupo de automorfismos de una extensión finita — Supondremos siempre que E/K es una extensión finita. El teorema del elemento primitivo asegura que la extensión dada E/K es simple algebraica: $E = K[\alpha]$. Así tenemos el polinomio mínimo

$$f = T^n + a_1 T^{n-1} + \cdots + a_n = P(\alpha, K) \in K[T].$$

Sean $\alpha = \alpha_1, \ldots, \alpha_r$ todas las raíces distintas de f en E. Entonces:

(1.4.1) Queda definida una aplicación biyectiva

$$\Psi : G(E:K) \to \{\alpha_1, \ldots, \alpha_r\}$$
$$\phi \mapsto \phi(\alpha)$$

(1.4.2) Orden $(G(E:K)) =$ número de raíces distintas de f en E.

(1.4.3) Orden $(G(E:K)) \leq [E:K]$.

4.2. Extensiones de Galois

Definición 2.1 La extensión finita E/K se denomina **extensión de Galois** si orden $G(E:K) = [E:K]$.

(2.2) Observaciones y Ejemplos

(I) Si $\alpha \in E$ es un elemento primitivo de E/K, esto es, $E = K(\alpha)$, E/K es de Galois si y sólo si el polinomio mínimo $P = P(\alpha, K)$ de α sobre K tiene $r = \partial P = [E:K]$ raíces (distintas) en E.

(II) Algunos ejemplos son:

- $\mathbb{C}/\mathbb{R}$ es de Galois, y en general toda extensión finita de grado 2 es de Galois.
- $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ no es de Galois.
- $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)/\mathbb{Q}$ es de Galois.

Proposición 2.3 Si E/K es de Galois y L/K es una subextensión de E/K, entonces E/L es de Galois.

(2.4) Cuerpo fijo de un grupo de automorfismos — Consideremos el cuerpo de característica cero E, y su grupo de automorfismos $G(E)$. Dado un subgrupo *finito* H de $G(E)$ definimos el conjunto

$$F = \{x \in E : \ \phi(x) = x \text{ para todo } \phi \in H\}.$$

Entonces F es un subcuerpo de E, denominado **cuerpo fijo de H**, y E/F es una extensión de Galois, cuyo grupo de automorfismos $G(E:F)$ es precisamente H.

Proposición 2.5 Sea E/K una extensión finita y $H = G(E:K)$ su grupo de automorfismos. Son equivalentes:

(I) E/K es de Galois.

(II) K es el cuerpo fijo de H.

Proposición 2.6 Teorema fundamental de la teoría de Galois, 1ª parte Sea E/K una extensión de Galois. Entonces la aplicación

$$L/K \mapsto G(E:L)$$

es una biyección del conjunto de las subextensiones de E/K sobre el conjunto de los subgrupos de $G(E:K)$. La aplicación inversa: $H \mapsto L/K$ queda definida por

$$L = \text{cuerpo fijo de } H.$$

Proposición 2.7 Teorema fundamental de la teoría de Galois, 2ª parte Sea E/K una extensión de Galois. Entonces son equivalentes:

(I) L/K es una subextensión de Galois de E/K.

(II) $G(E:L)$ es un subgrupo normal de $G(E:K)$.

Además, en ese caso:

$$G(L:K) \simeq G(E:K)/G(E:L).$$