Álgebra

Anillos

Generalidades

Definición 1.1 (Anillo) Un **anillo** es una estructura $(A, +, \cdot)$ con las propiedades:

- $(A, +)$ es un grupo conmutativo
- Asociatividad: $(xy)z = x(yz)$
- Distributividad: $(x+y)z = xz+yz, x(y+z) = xy + xz$

Se denota al elemento unitario de $(A, +)$ por 0_A y al unitario de $(A, +, \cdot)$, si existe, por 1_A. $A^* = A/\{0\}$. $0_A = 1_A \iff A = \{0\}$.

Definición 1.6 Si $1_A \in A$, entonces A es un **anillo unitario**. Una **unidad** de A es un elemento x que tiene su inverso y: $xy = 1$. El conjunto de unidades es $U(A)$. El inverso, si existe, se puede denotar por x^{-1} y $x/y = xy^{-1}$.

Definición 1.8 Un **cuerpo** es un anillo K tal que K^* es un grupo. O, un anillo unitario con inverso.

Definición 1.10 Un **divisor de cero** es un elemento $x \in A^*$ tal que, para algún $y \in A^*$, $xy = 0_A$. Un cuerpo nunca tiene divisores de cero: $x = x(yy^{-1}) = (xy)y^{-1} = 0y^{-1} = 0$

Definición 1.11 Se denomina **dominio de integridad** a un anillo unitario sin divisores de cero. El producto de dos anillos conmutativos $C = A \times B$ nunca es un dominio de integridad, pues $(a, 0) \neq 1_A, (0, b) \neq 1_B$ y $(a, 0) \times (0, b) = (0, 0) = 0_C$.

A un dominio de integridad se le puede asociar un cuerpo mediante el **cuerpo de fracciones de un dominio**. Dada la relación $(x, y)R(x', y') \iff xy' = x'y$, para el producto de dominios $A \times A^*$ entonces para la clase de equivalencia $[x, y]$, las operaciones $[x, y]+[x', y'] = [xy'+y'x, yy'], [x, y] \cdot [x', y'] = [xx', yy']$ forman un cuerpo, K, con $0_K = [0, 1]$, $1_K = [1, 1]$, y $[x, y]^{-1} = [y, x]$.

Definición 1.14 (Ideal) Un **ideal** es un subconjunto $I \subset A$ tal que

- I es subgrupo de A
- $\forall i \in I, a \in A, ia \in I$.

$A, \{0\}$ son los **ideales triviales**, y si $I \neq A$, I es un **ideal propio**. Si $1_A \in I$, $I = A$: $\forall a \in A$, $a = a \cdot 1$, y como $1 \in I, a \in I$.

Definición 1.16 Dado un ideal I de A, dada la relación $xRy \iff x - y \in I$, se forma el **anillo cociente** A/I con las clases de equivalencia $[x] = x + I = \{x + a \mid a \in I\}$. Las operaciones suma y producto definidas por $(x + I) + (y + I) = (x + y) + I$, $(x + I)(y + I) = xy + I$, son inyectivas.

Definición 1.17 - 1.19 Sea A un anillo conmutativo y L un subconjunto de A. El conjunto I de sumas finitas $a_1x_1 + ... + a_lx_l$, $a_i \in A, l_i \in L$ es un **ideal generado por** L. Además, I es el mínimo ideal que contiene a L. Si L es finito, I es **finitamente generado**; y si L tiene un solo elemento, es decir, $I = Al$, el ideal es **principal**.

En los ideales se definen la (1) suma: $I + J$ está dado por $a_1, \cdots, a_r, b_1, \cdots, b_s \in A, x_1, \cdots, x_r \in I, y_1, \cdots, y_s \in J, a_1x_1 + \cdots + a_rx_r + b_1y_1 + \cdots + b_sy_s = x + y$; (2) producto: IJ $= x_1y_1 + \cdots + x_ry_r, x_1, \cdots, x_r \in I, y_1, \cdots, y_r \in J$, (3) intersección $I \cap J$.

Ejemplo 1.20.2 En un cuerpo K sólo son ideales $\{0\}$ y K. Si I es ideal no trivial de K, para $x \in I \ \{0\} existe x^{-1} \in$ K y $1 = xx^{-1} \in I$, y I es ideal impropio. \)

Definición 1.21 Un ideal es **maximal** si (1) A/I es un cuerpo y (2) I es propio y ningún otro ideal propio lo contiene. (1) $\iff$ (2). Si A/I es un cuerpo, luego contiene una unidad. Ninguna unidad i de A/I puede estar en $I^* = I + i$ porque entonces $I^* = A$.

Definición 1.22 Sean A unitario e I un ideal. Se dice que I es **primo** si (1) A/I es un dominio de integridad y (2) I es propio, y $\forall x, y \in A$, si $xy \in I$, $x \in I$ o $y \in I$. (1) $\iff$ (2). Demostración. Si $xy \in I$, $0 + I = xy + I = (x + I)(y + I)$. Como A/I es dominio, $x + I = 0 + I \to x \in I$ o $y + I = 0 + I \to y \in I$.

Definición 1.24 Un **homomorfismo** de los anillos A, B es una aplicación $f : A \to B$ definida por:

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_A) = 1_B$

$f(x)(f(1_A) - 1_B) = f(x)f(1_A) - f(x)1_B = f(x \cdot 1_A) - f(x) = 0$. Si $f(1_A) \neq 1_B$, f(A) son divisores de 0. La aplicación composición $\phi : A \to A : g \mapsto g \circ f$ es homeomorfismo.

Definición 1.26 (Núcleo e imagen) Se define el **núcleo** de f al ideal: $\ker f = \{x \in A \mid f(x) = 0\}$, y se define la **imagen** de f al anillo $\operatorname{im} f = \{y \in B \mid \exists x \in A, f(x) = y\}$.

Proposición 1.27 / 1.30 Teorema de isomorfía. Dado un homomorfismo f, el diagrama

Ejemplo 1.31 Si $f : K \to B$ es homomorfismo de anillos unitarios conmutativos y K es un cuerpo, entonces f es monomorfismo, pues $\ker f = \{0\}$ es ideal propio.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"] & B \\ A/\ker f \arrow[r, "\bar{f}"] & \operatorname{im} f \arrow[u, "j"] \end{tikzcd}$$

Con $p : x \mapsto x + \ker f$ sobreyectiva / **epimorfismo**, $\bar{f} : x + \ker f \mapsto f(x)$ biyectiva / **isomorfismo**, $j : y \mapsto y$ inyectiva / **monomorfismo**; es conmutativo. Si f es monomorfismo entonces $\ker f = \{0\}$. Dos anillos conmutativos son **isomorfos** ($A \simeq B$) si existe un isomorfismo entre ellos.

Divisibilidad

Definición 2.1 x es un divisor de y o y es un múltiplo de x, $x|y$ si existe $a \in A, y = ax$. Si $(x) = \{kx \mid k \in \mathbb{Z}\}$, entonces $x|y \iff (y) \subset (x)$. x **está relacionado con** y si $(x) = (y) \iff x|y, y|x$. En ese caso, existe una unidad $a \in U(A)$ tal que $y = ax$. Si $(y) = (x), y \in (x), x \in (y); y = ax, x = by. y = aby \iff 1 = ab.$

Denotamos $\operatorname{div}(y)$ al conjunto de divisores de y. Si y genera un ideal primo, entonces decimos que y **es primo**. y es **irreducible** si sus divisores son las unidades y productos de y por unidades. **Todo primo es irreducible**, pero **NO TODO irreducible es primo** (hay irreducibles que no generan ideales primos).

Definición 2.6 Se dice que A es un **dominio euclídeo DE** si existe una aplicación $\|\cdot\| : A \to \mathbb{N}$ tal que

- $\|x\| = 0 \iff x = 0$
- $\|xy\| = \|x\| \cdot \|y\|$
- Si $x, y \in A^*$ existe $r \in A$ tal que $y|(x - r)$ y $\|r\| < \|y\|$

$\mathbb{Z}$ es DE porque el valor absoluto cumple la función. En $\mathbb{Z}[i]$ la función $\|a + bi\| = a^2 + b^2$ cumple las propiedades y $\mathbb{Z}[i]$ es DE.

Proposición 2.8 Si A es DE, entonces $U(A) = \{x \in A \mid \|x\| = 1\}$. $\to$) $\|1_A\| = 1$ porque $\|1_A\| = \|1_A \cdot 1_A\| = \|1_A\| \|1_A\|$, y como $\|1_A\| \neq 0$, $\|1_A\| = 1$. Si $x \in A$, existe x^{-1} y $\|x\| \left\|x^{-1}\right\| = \left\|xx^{-1}\right\| = 1$ y como $\|x\| \in \mathbb{N}$, $\|x\| = \left\|x^{-1}\right\| = 1$

Proposición 2.10/Definición 2.11 En un **dominio de ideales principales DPI** todos los ideales son principales. Un DE es un DIP. Elegimos x tal que $\|x\| = \min\{\|y\| \mid 0 \neq y \in I\}$. Entonces $x > 0$ y I está generado por x, ya que si $y \neq 0, y \in I$, existe $r \in A$ tal que $x|(y - r), \|r\| < \|x\|$. Entonces $y - r \in I$ y como $y \in I, r \in I$, pero como $\|r\| < \|x\|$, y $\|x\|$ es el mínimo en I, r = 0 y $y \in (x)$.

Proposición 2.12 Si A es un DIP, todo elemento irreducible $a \in A^*$ genera un ideal maximal. Sea I, $(a) \subset I$. Entonces $I = (a)$ o $I = A$. Sea $b \in A$ tal que $I = (b)$. Entonces $(a) \subset I = (b), b|a$. Como a es irreducible, o bien $b = ua, u \in U(A)$, y (a) = (b) = I o $b \in U(A)$, y I = (b) = A.

Definición 2.13 (Característica de un dominio de integridad) Definimos $\phi = \phi_A : \mathbb{Z} \to A : k \mapsto k \cdot 1_A = 1_A + \cdots + 1_A$ $(k > 0), 0$ $(k = 0), -((-k) \cdot 1_A)$ $(k < 0)$. ϕ es un homomorfismo. Si $\ker \phi = \{0\}$, $\mathbb{Z} \subset A$, y tiene característica 0; y si $\ker \phi \neq \{0\}$, A tiene característica positiva. En este caso, como A es dominio de integridad y $Z/\ker \phi \simeq \operatorname{im} A \subset A$, $Z/\ker \phi$ también es dominio y $\ker \phi = (p)$ es un ideal primo.

Definición 2.14 Sean $x, y \in A^*, z \in A$. z es un **máximo común divisor** si $z|x$, $z|y$, y z divide cualquier otro divisor de ambos. z es un **mínimo**

común múltiplo si $x|z$, $y|z$ y z divide a cualquier otro múltiplo de ambos. Estos elementos son únicos.

Proposición 2.17 / 2.18 / 2.19. Para un dominio de integridad A^*:

- $\forall x, y \in A^*$ tiene mcd: $(x) + (y) \subset (mcd)$.
- $\forall x, y \in A^*$ tiene mcm: $(x) \cap (y) = (mcm)$.
- xy = mcm· mcd.

Si se cumple cualquiera de los dos primeros puntos MC , todo elemento irreducible es primo P .

Proposición 2.20 (**Identidad de Bezout B**). Si $x, y \in A^*$ generan un ideal principal, existe $z = mcd(x, y)$ y existen $a, b \in A$ tales que $z = ax + by$.

Definición 2.21 Dos elementos $x, y \in A^*$ son primos entre sí si no comparten más divisores que las unidades, es decir, $mcd(x, y) = 1_A$.

Definición 2.23 Un dominio de factorización única, **DFU**, es un dominio de integridad donde todo elemento irreducible es primo (**P**) y todo elemento no unitario es producto de elementos irreducibles (**F**).

$$\begin{tikzcd}
DE \arrow[r] & DIP \arrow[r] \arrow[d] & DFU \arrow[r] \arrow[d] & F \\
 & B \arrow[r] & MC \arrow[r] & P
\end{tikzcd}$$

Proposición 2.26 Ecuaciones diofánticas lineales con dos incógnitas. Las ecuaciones son de la forma $c = aX + bY$, de un dominio. Si se cumple la identidad de Bezout, y $d = \text{mcd}(a, b)$, entonces se cumple que $d = \alpha a + \beta b$. Por tanto, existen $a_0, b_0, c_0 \in A$ tales que $c = c_0 d, a = a_0 d, b = b_0 d$, y $1 = \alpha a_0 + \beta b_0$, de modo que la nueva ecuación a resolver es

Multiplicando por α y sustituyendo $\alpha a_0 = 1 - \beta b_0$ tenemos $X = \alpha c_0 + b_0(\beta X - \alpha Y)$. Igualmente, multiplicando por β y sustituyendo $\alpha a_0 = 1 - \beta b_0$ tenemos $Y = \beta c_0 - a_0(\beta X - \alpha Y)$. Así, si $t = \beta x - \alpha y$, para algunos x, y, tenemos las ecuaciones $x = \alpha c_0 + b_0 t; y = \beta c_0 - a_0 t$.

Así, primero hallamos $d = \alpha a + \beta b$, con lo cual obtenemos α, β, a, b, y de ahí sacamos $a_0 = a/\text{mcd}$, $b_0 = b/\text{mcd}$, $c_0 = c/\text{mcd}$. Para obtener $d = \alpha a + \beta b$ empleamos el algoritmo de Euclides.

Proposición 2.27 Algoritmo de Euclides. Este algoritmo sólo es válido en DIPs, ya que en ellos se da B y MC. Ponemos un ejemplo práctico con 4329/132:

$4329 = 132 \cdot 32 + 105$, $132 = 105 \cdot 1 + 27$, $105 = 27 \cdot 3 + 24$, $27 = 24 \cdot 1 + 8$, $24 = 8 \cdot 3$

Si tenemos la ecuación diofántica $4329X + 132Y = 33$, vemos que tiene solución pues $\text{mcd}(4329, 132) = 3$ y $3|33$. Para encontrar las soluciones primero necesitamos reconstruir la ecuación $d = \alpha a + \beta b$, con $a = 4329, b = 132$. Para ello vamos sustituyendo el cociente de cada una de las ecuaciones por la siguiente.

$a = 32b + x_2 \iff x_2 = a - 32b$ || $b = x_2 + x_3 \iff x_3 = b - x_2$ || $x_2 = 3x_3 + x_4 \iff x_4 = x_2 - 3x_3$

Finalmente, $3 = x_3 - x_4$. De aquí empezamos a sustituir todas las secuencias, al reves, hasta llegar con a, b. $3 = x_3 - x_4 = 4x_3 - x_2 = 4b - 5x_2 = 164b - 5a$. Luego $3 = 164b - 5a = \beta b + \alpha a$. Así, $\beta = 164, \alpha = -5$. Si, además, $a_0 = a/\text{mcd} = 4329/3 = 1443$, $b_0 = b/\text{mcd} = 132/3 = 44$, $c_0 = c/\text{mcd} = 33/3 = 11$, tenemos las ecuaciones $x = -5 \cdot 11 + 44t; y = 164 \cdot 11 - 1443t$.

Proposición 3.7 (Teoreama chino del resto) Si (a, b) son enteros primos entre sí, $\mathbb{Z}/ab\mathbb{Z} = \mathbb{Z}/(ab) \simeq \mathbb{Z}/(a) \times \mathbb{Z}/(b)$. Así, el sistema de congruencias $X \equiv m \text{ mod } a$; $X \equiv n \text{ mod } b$.

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

- $[k] \in U(\mathbb{Z}/(n))$
- $\text{mcd}(k, n) = 1$
- $[k] \neq 0$ y k no es divisor de cero en $\mathbb{Z}/(n)$.

Definición 3.9 (Identidad de Euler) Sea m positivo. Definimos $\phi(m)$ como el número de enteros coprimos con m.

- $\phi(ab) = \phi(a)\phi(b) \iff \text{mcd}(a, b) = 1$

- $\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$ si p primo
- $\phi(m) = m \prod_{i=1}^{s}(1 - 1/p_i)$

Proposición 3.12 Para cada entero n, $n = \sum_{d|n, d\geq 1} \phi(d)$. Consideramos el grupo aditivo $H = \mathbb{Z}/(n)$, que es cíclico de orden n. Para $1 \leq d \leq n$, H_d es el cjto de elementos de H con orden d. Por el Tma de Lagrange, para ser H_d subgrupo, $d|n$. Además, para cada d H_d es disjunto (dos elementos diferentes no pueden tener el mismo orden), luego $H = \cup_{d|n} H_d$. Finalmente, se puede demostrar que $o(H_d) = \phi(d)$.

Proposición 3.13, 3.14 (Euler, p. t. de Fermat) Si $\mathrm{mcd}(k, n) = 1$, $k^{\phi(n)} \equiv 1 \bmod n$. Si p es primo, $k^{p-1} \equiv 1 \bmod p$. Basta ver que $Z_n^* tiene \phi(n)$ elementos, luego si $\mathrm{mcd}(k, n) = 1$, o(k) = o(Z_n^*) = $\phi(n) y k^{\phi(n)}$ = 1.

Proposición 3.15 (Teorema de Wilson) Sea p primo. Entonces $(p-1)! \equiv -1 \bmod p$. Demo basada en el libro de EA, que me gusta más. (Z/p Z, $\cdot$) es grupo. Quitando $[1], [-1]$, $o([a]) > 2$, ya que [a][b] $\equiv -1$ o 1 $\iff$ $a = (p+1), b = (p-1) o (p+1)$. Como $o(x) = o(-x)$, para cada $[a]$ existe un $[b]$ tal que $[a][b] = [1]$, y denotamos a ese cjto M. Entonces, $M = \{[2], [p-2], [3], [p-3], \cdots, [(p-1)/2], [(p+1)/2]\}$ y $[p-1]! = [p-1]([p-2]!) = [p-1][1] = [-1][1] = [-1]$ y $(p-1)! \equiv -1 \bmod p$.

Corolario 3.16 Sea $p \neq 2$ primo. Entonces si $q = (p-1)/2$, $(q!)^2 \equiv (-1)^{q+1} \bmod p$.

Polinomios

Generalidades

Definición 1.1 Un polinomio es una construcción que necesita un anillo conmutativo unitario B y un subanillo A. Cada elemento f de B se escribe como la suma $f = \sum_{v=(v_1,\cdots,v_n)} a_v X_1^{v_1} \cdots X_n^{v_n}$ donde cada $X_i \in B$ y $a \in A$. $v = (v_1, \cdots, v_n)$ son las posibles combinaciones distintas de cero de los exponentes para las variables X_i. Este anillo se denomina **anillo de polinomios en n indeterminadas con coeficientes en** A y se representa por $A[X_1, \cdots, X_n]$.

Los polinomios cumplen la unicidad, y pueden sumarse y multiplicarse de la siguiente manera:

$$f + g = \sum_v (a_v + b_v) X_1^{v_1} \cdots X_n^{v_n}$$

$$fg = \sum_v \left(\sum_{v=\lambda+\mu} a_\lambda b_\mu \right) X_1^{v_1} \cdots X_n^{v_n}$$

Definición 1.4 Si $\phi : A \longrightarrow A'$ es un homomorfismo entre anillos, entonces ϕ induce un anillo entre polinomios: $\Phi : A[X_1, \cdots, X_n] \rightarrow A'[X_1, \cdots, X_n]$ tal que $\sum_v a_v X_1^{v_1} \cdots X_n^{v_n} \rightarrow \sum_v \phi(a_v) X_1^{v_1} \cdots X_n^{v_n}$. Además, Φ es epi/-monomorfismo ssi lo es ϕ.

Definición 1.5 Evaluación de polinomios. Dado un polinomio f, y dados $x_1, \cdots, x_n \in B$, definimos la evaluación de un polinomio como $ev : A[X_1, \cdots, X_n] \rightarrow B; f(x_1, \cdots, x_n) = \sum_v a_v x_1^{v_1} \cdots x_n^{v_n}$.

El teorema de isomorfía garantiza que $A[X_1, \cdots, X_n]/\ker(ev) \simeq A[x_1, \cdots, x_n]$. Los **ceros** de f son los elementos del núcleo ($f(x_1, \cdots, x_n) = 1_B$), y en polinomios de una variable ($A[T]$) se llaman **raíces**.

Definición 1.5.3 Sustitución. Los polinomio permiten el cambio de unas variables $x_1, \cdots, x_n$ a unas nuevas $h_1, \cdots, h_n$. Por ejemplo, si denotamos $t = a + T$ en $A[T]$, entonces podemos definir la sustitución $\phi_a : A[T] \longrightarrow A[T] ; f \mapsto f(a+T)$.

Definición 1.5.4 Los ideales de un polinomio son de la forma $(X_i) : A[X_1, \cdots, X_n]; x_j = X_j$ si $j \neq i$, 0 si $j = i$, es decir, cuando eliminamos una de las variables. Así, $A[X_1, \cdots, X_n]/(X_i) \simeq A[X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n]$.

Definición 1.6 Funciones polinomiales. Sea $f = A[X_1, \cdots, X_n]$. Se define una **función polinomial**, $F : B \times \cdots \times B \longrightarrow B; (x_1, \cdots, x_n) \mapsto f(x_1, ..., x_n)$.

Definición 1.7 Dado un polinomio no nulo $f = \sum_{v=(v_1,\cdots,v_n)} a_v X_1^{v_1} \cdots X_n^{v_n}$ se define el **grado** del polinomio, ∂f, a la máxima suma de exponentes de variables, es decir, $\text{máx}(d) | v_1 + \cdots + v_n = d, a_v \neq 0$. El **grado parcial** es $\partial_i f : \text{máx}(d) | v_i = d$, es decir, el exponente más alto de la variable X_i. Por convenio, $\partial 0 = \partial_i 0 = -\infty$. Se verifica que $\partial(f+g) \leq \text{máx}(\partial f, \partial g)$ y $\partial(fg) \leq \partial f + \partial g$. Ídem para grados parciales.

En polinomios de una variable $f = a_0 + a_1 T + \cdots + a_n T^n$, el **coeficiente director** es a_n. Si $a_n = 1$, decimos que f es **mónico**.

Definición 1.8 Dado un polinomio f de grado p, las **componentes homogéneas**, $f_0, f_1, \cdots, f_p$ son los sumandos de igual grado total. Los **monomios** son las componentes homogéneas de un solo sumando, $a_v X_1^{v_1} \cdots X_n^{v_n}$. Dadas dos formas homogéneas de grados p y q, su producto tiene grado $p + q$.

Proposición 1.9/**Corolario 1.10** $A[X_1, \cdots, X_n]$ es dominio de integridad ssi lo es A. Entonces $\partial(fg) = \partial f + \partial g$.

Corolario 1.11 Si A es dominio, $U(A) = U(A[X_1, \cdots, X_n])$. Si $a \in U(A)$, existe a^{-1} en $U(A)$, y es inverso en $A[X_1, \cdots, X_n]$, luego $a \in U(A[X_1, \cdots, X_n])$. Por otra parte, si $f \in U(A[X_1, \cdots, X_n])$, existe g tal que $1 = fg$, y $0 = \partial 1 = \partial(fg) = \partial f + \partial g \iff \partial f = \partial g = 0$, luego $f \in U(A)$.

Definición 1.12.2 El cuerpo $K(X_1, \cdots, X_n)$ es el **cuerpo de funciones racionales** con coeficientes en K en n indeterminadas, y sus elementos vienen dados como $f/g; f, g \in K[X_1, \cdots, X_n]$, donde K es el cuerpo de fracciones de A. Así, cada elemento f/g es de la forma $\sum_\lambda a_\lambda X_1^{\lambda_1}\cdots X_n^{\lambda_n}/\sum_\mu b_\mu X_1^{\mu_1}\cdots X_n^{\mu_n}$.

Definición 1.13 Derivación. Dado un anillo $A[T]$, la derivada de un polinomio $f = a_0 + a_1T + \cdots + a_pT^p$ es el polinomio $\frac{\partial f}{\partial T} = a_1 + \cdots + pa_pT^{p-1}$. Se comprueba que $\frac{\partial(f+g)}{\partial T} = \frac{\partial f}{\partial T} + \frac{\partial g}{\partial T}$ y $\frac{\partial fg}{\partial T} = f\frac{\partial g}{\partial T} + g\frac{\partial f}{\partial T}$.

División de polinomios

Lema 2.1 Sea $g \in A[T]$ y $a \neq 0$ su coeficiente director. Entonces para cualquier $f \in A[T]$ existen $Q, R \in A[T]$ únicos tales que $a^r f = Qg + R$ y $\partial R < \partial g$; siendo $r = \max(0, \partial f - \partial g + 1)$.

Corolario 2.2 Regla de Ruffini. Sea $c \in A$ fijo. Para cada $f \in A[T]$ existe un $Q \in A[T]$ tal que $f = Q(T-c) + f(c)$. En particular, $(T-c)|f \iff f(c) = 0$. Aplicando $g = T - c$ obtenemos $f = Q(T-c)+R$, y como $\partial R < \partial g = 1$, $\partial R = 0$ y $R \in A$. Evaluamos la expresión en c y tenemos $f(c) = Q(c)(c-c) + R(c) = R$ y resulta el lema.

Corolario 2.3 Un polinomio no nulo $f \in A[T]$ tiene a lo sumo ∂f ceros distintos en A.

Corolario 2.4 Sea A un dominio infinito. Sean $f, g \in A[X_1, \cdots, X_n]$ dos polinomio tal que existe otro $l \in A[X_1, \cdots, X_n]$ tal que para todo $(x_1, \cdots, x_n)$, $f(x_1, \cdots, x_n) \neq 0$, y $f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n)$, entonces $f = g$.

Lema 2.5 Para los polinomios $A[T]$ la aplicación $||\cdot|| : A[T] \longrightarrow \mathbb{N}$; $f \mapsto ||f|| = 2^{\partial f}$ define a $A[T]$, **si** A **es cuerpo**, como DE.

Proposición 2.6 A es cuerpo $\iff A[T]$ es DE $\iff A[T]$ es DIP.

Proposición 2.7 A es DFU $\iff A[T]$ es DFU $\iff A[X_1, \cdots, X_n]$ es DFU.

Definición 2.10.1 Se llama **contenido** de un polinomio $f \in A[T]$ y se denota por $\mathbf{c}f$, al máximo común divisor de sus coeficientes. Así, $\mathbf{c}(f)|f$ y $f = \mathbf{c}(f)f_1$.

Observación 2.11 Un polinomio $f \in A[T]$ con contenido 1 es irreducible en $A[T]$ ssi lo es en $K[T]$.

Proposición 2.13 (simplificada). Sea A dominio y $f \in A[T]$, con grado n. Entonces existe un cuerpo $L \supset A$ y elementos $a_0, x_1, \cdots, x_n \in L$ tales que $f = a_0(T-x_1)\cdots(T-x_n)$.

Factorización

Proposición 3.2 (Factorización de Kronecker) Sea $f \in A[T]$, A de característica 0 y $U(A)$ es finito, $\mathbf{c}(f) = 1$, $\partial f > 0$ y sea s el mayor entero $\leq \partial f/2$. Entonces la factorización, si existe, se da en los siguientes pasos:

- Elegir $s+1$ elementos distintos $n_0, ..., n_s$ tales que $f(n_0), f(n_1), \cdots, f(n_s) \neq 0$.
- Creamos, para cada n_i, el conjunto de divisores D_i en A de $f(n_i)$, y establecemos $D = D_0 \times \cdots \times D_s$.
- Para cada $M = (m_0, \cdots, m_s) \in D$ creamos el polinomio

$$f_M = \sum_k^s m_k \prod_{l\neq k}^s \frac{T - n_l}{n_k - n_l} \in K[T]c$$

- Si $f_M|f$, hemos encontrado un polinomio divisor. Si ningún f_M es divisor de f, f es irreducible.

Proposición 3.4 Sea $f \in K[T]$, $2 \leq \partial f \leq 3$. Entonces f es reducible ssi f tiene alguna raíz de 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 en K está en A y es divisor de $a_0 = f(0)$ en A.

Proposición 3.7 (Eisenstein) Sea $f = a_0 + a_1T + \cdots + a_pT^p \in A[T]$ con contenido 1 y $d \in A$ irreducible. Si $d|a_0, \cdots, d|a_{p-1}, d \nmid a_p, d^2 \nmid a_0$ entonces f es irreducible.

Proposición 3.8 Sea $f \in A[T]$. f es irreducible en $A[T]$ ssi para cada $a \in A$, $f(a+T)$ es irreducible ssi existe a tal que $f(a+T)$ es irreducible.

Proposición 3.10 (criterio del módulo finito) Sea $f = a_0 + \cdots + a_pT^p \in A[T]$, $a_p \in U(A)$. Supongamos que existe $d \in A$ irreducible tal que en $A/(d)[T]$ el polinomio $\overline{f} = \overline{a_0} + \cdots + \overline{a_p}T^p, \overline{a} = a + (d)$ es irreducible. Entonces f es irreducible.

Extensiones de cuerpos

Generalidades

Definición 1.1 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, $\ker f = \{0\}$ y f es monomorfismo, isomorfo a $j(K)$, subcuerpo de E.

Definición 1.1.1 Un homomorfismo / isomorfismo de una extensión E_1/K en otra E_2/K es un homomorfismo/isomorfismo de cuerpos $\phi : E_1 \to E_2$ que induce identidad en K, y se denota por $\phi : E_1/K \to E_2/K$.

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

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

Definición 1.5 Una extensión de cuerpos con grado finito es una **extensión finita**.

Proposición 1.6 (Transitividad) Sean L/K y E/L dos extensiones de cuerpos. Entonces L/K y E/L son finitas sii E/K es finita. En ese caso, $[E : K] = [E : L][L : K]$.

Corolario 1.7/Observación 1.8 Si $[E : L] = [E : L']$, L = L'. Si $[E : K] = 1$, $E = K$.

Observación 1.9 Si $[E : K]$ es primo, no existen subsextensiones propias (distintas de E/K y K/K.

Definición 1.10 **Subextensión generada por un subconjunto**. Sea E/K extensión de cuerpos, no necesaramente finita que suponemos es inclusion $K \subset E$. Sea $A = \{a_i \mid i \in I\} \subset E$ un subconjunto arbitratrio no vacío. Denotamos $K(A)$ la intersección de todos los subcuerpos $L \subset E$ que contengan K y A. Así $K(A)$ es el menor subcuerpo de E que contiene a K y A. Este cuerpo se llama **cuerpo generado por** A **sobre** K. La igualdad $L = K(A)$ se dice que L **está generado por** A **sobre** K.

Definición 1.10.1 $x \in E$ está en $K(A)$ sii existen elementos $a_1, \cdots, a_r \in A$ y polinomios $f, g \in K[X_1, \cdots, X_r]$ tales que $g(a_1, \cdots, a_r) \neq 0$ y $x = f(a_1, \cdots, a_r)/g(a_1, \cdots, a_r)$

Definición 1.11 Una extensión L/K es **finitamente generada** si L está generado sobre K por un conjunto finito. Si ese conjunto tiene un solo elemento, decimos que la extensión es *simple*. $L = K(A) = K(a_1, \cdots, a_n)$. x **Ejemplo 1.12.6** Sea E/K. Si $A, B \subset E$ entonces $K(A)(B) \subset K(A \cup B)$.

Ejemplo 1.12.7 Si $K(A) = K(B)$ no siempre $A = B$. P. ej. $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(2i)$. $K(A) = K(B) \iff A \subset K(B), B \subset K(A)$.

Definición 1.13 Sea E/K extensión de cuerpos y $a_1, \cdots, a_n$ elementos de E. Se tiene un homomorfismo evaluación $K[X_1, \cdots, X_n] \to E : f \mapsto (a_1, \cdots, a_n)$ con nucleo I. $a_1, \cdots, a_n$ son **alegráicamente independientes** sobre K si $I = \{0\}$, es decir, $f(a_1, \cdots, a_n) \neq 0$ para todo polinomioi no nulo; y **âlgebráicamente dependientes** si $I \neq \{0\}$.

Observación 1.14.3 Si $n = 1$ y a_1 es algebráicamente independiente, a_1 es **trascendente** sobre K.