Álgebra Moderna 2: Teoría de Anillos

Rafael Dubois
Universidad del Valle de Guatemala
dub19093@uvg.edu.gt

19 de agosto de 2021

1. Anillos: Definiciones preliminares

Un conjunto no vacío R es un anillo si en él se definen dos operaciones binarias (a menudo llamadas suma ($+$) la primera, y producto ($\cdot$) la segunda), las cuales cumplen con las siguientes propiedades:

1. **Cerradura de la suma.**
2. **Asociatividad de la suma.**
3. **Neutro de la suma.**
4. **Inversos de la suma.**
5. **Conmutatividad de la suma.**
6. **Cerradura del producto.**
7. **Asociatividad del producto.**
8. **Distributividades del producto sobre la suma.**

Es decir, $(R, +)$ es un grupo abeliano, mientras $(R, \cdot)$ no necesariamente es conmutativo, posee inversos, y ni siquiera necesita un elemento neutro.

Anillo con elemento neutro multiplicativo

Si $(R, +, \cdot)$ es un anillo en el cual existe $1 \in R$ tal que $r \cdot 1 = 1 \cdot r = r$ para todo $r \in R$, entonces R es un anillo con elemento neutro multiplicativo.

Anillo conmutativo

Si $(R, +, \cdot)$ es un anillo en el cual todos sus elementos conmutan, entonces R es un anillo conmutativo.

Anillo de división

Si $(R, +, \cdot)$ es un anillo tal que $(R - \{0\}, \cdot)$ forma un grupo no necesariamente abeliano, entonces R es un anillo de división.

Campo

Si $(R, +, \cdot)$ es un anillo para el cual $(R - \{0\}, \cdot)$ forma un grupo abeliano, entonces R es un campo.

En este documento, los códigos de color van de la siguiente manera: Negro, Títulos; Azul, Lemas; Rojo, Teoremas; Violeta, Definiciones; Morado, Propiedades; Aqua, Otros subtítulos.

2. Anillos: Casos especiales

Divisores de cero

En un anillo R, si $a, b \in R - \{0\}$ cumplen $ab = 0$, entonces a y b son divisores de cero.

Dominio entero

Si R es un anillo conmutativo y no tiene divisores de cero, entonces R es un dominio entero.

Lema 3.1:

Si R es un anillo con elementos a y b arbitrarios,

- $a \cdot 0 = 0 \cdot a = 0$;
- $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;
- $(-a) \cdot (-b) = a \cdot b$.

Si $1 \in R$, se cumple también

- $(-1) \cdot a = -a$;
- $(-1) \cdot (-1) = 1$.

Lema 3.2:

Todo dominio entero finito es un campo.

Corolario del lema 3.2:

Si p es un número primo, entonces $(\mathbb{Z}_p, +, \cdot)$ es un campo.

Notación de producto por un entero

Para $a \in R$ con R un anillo y $n \in \mathbb{Z}^+$, la notación na se refiere a

$$na = \underbrace{a + a + \cdots + a}_{n \text{ veces}}.$$

Característica de un dominio entero

La característica de un dominio entero es el menor entero no negativo que anula a todos sus elementos.

Característica cero

Un dominio entero D es de característica 0 si la relación $ma = 0$ para $a \neq 0$ en D y $m \in \mathbb{Z}$ solo puede ocurrir si $m = 0$.

Característica finita

Un dominio entero D es de característica finita si existe $p \in \mathbb{Z}^+$ tal que $pa = 0$ para todo $a \in D$. En este caso, p debe ser un número primo.

3. Homomorfismos de anillos

Si $(R, +, \cdot)$ y $(R', +', \cdot')$ son anillos y $\varphi : R \to R'$ es una función, se dice que φ es un homomorfismo si

$$\phi(r_1 + r_2) = \phi(r_1) +' \phi(r_2), \qquad \phi(r_1 \cdot r_2) = \phi(r_1) \cdot' \phi(r_2).$$

Lema 3.3:

Si R y R' son anillos y $\varphi : R \to R'$ es un homomorfismo, entonces

- $\phi(0) = 0$;
- $\phi(-a) = -\phi(a)$.

Lema 3.4:

Si R y R' son anillos y $\varphi : R \to R'$ es un homomorfismo, entonces

- $(K_\varphi, +)$ es un subgrupo de $(R, +)$;
- Si $k \in K_\varphi$ y $r \in R$, entonces kr y rk están en K_φ (K_φ atrapa productos).

Epimorfismos de anillos

Si R y R' son anillos y $\varphi : R \to R'$ es un homomorfismo sobreyectivo, entonces φ es un epimorfismo.

Isomorfismos de anillos

Si R y R' son anillos y $\varphi : R \to R'$ es un homomorfismo biyectivo, entonces φ es un isomorfismo.

Lema 3.5:

Si R y R' son anillos y $\varphi : R \to R'$ es un homomorfismo sobreyectivo (epimorfismo) es un isomorfismo si y solo si $K_\varphi = \{0\}$.

4. Ideales y anillos cociente

Si R es un anillo y U es un subconjunto no vacío de R tal que

- $(U, +)$ es un subgrupo de $(R, +)$;
- Si $u \in U$ y $r \in R$, entonces u y ru están en U (U atrapa productos);

se dice que U es un ideal de R.

Lema 3.6:

Si R es un anillo y U es un ideal de R, entonces R/U es un anillo y es una imagen homomórfica de R.

Anillo cociente

Si R es un anillo y U es un ideal de R, entonces R/U es el anillo cociente de R sobre U.

Teorema 3A:

Si R y R' son anillos y $\varphi : R \to R'$ es un epimorfismo, entonces $R' \approx R/K_\varphi$. Además, existe una biyección entre la colección de ideales de R' y la colección de ideales que contienen a K_φ, la cual se obtiene asociando cada ideal I' de R' con el ideal $\varphi^{-1}(I')$ de R, con lo cual $R/\varphi^{-1}(I') \approx R'/I'$.

5. Más sobre ideales y anillos cociente

Lema 3.7:

Si R es un anillo conmutativo con elemento neutro multiplicativo, cuyos únicos ideales son (0) y R mismo, entonces R es un campo.

Ideales maximales

Si R es un anillo y M es un ideal de R tal que $M \neq R$, y si U es un ideal de R tal que $M \subseteq U \subseteq R$ implica $U = M$ o $U = R$, se dice que M es un ideal maximal de R. En otras palabras, M es un ideal maximal de R si no hay ideales distintos de M o R entre M y R.

La importancia de los elementos primos

Un ideal de $(\mathbb{Z}, +, \cdot)$ es maximal si y solo si es generado por un número primo p.

Teorema 3B:

Si R es un anillo conmutativo con elemento neutro multiplicativo y M es un ideal de R, entonces M es un ideal maximal de R si y solo si R/M es un campo.

Ideales principales

Un ideal A de R es un ideal principal si es generado de un elemento $a \in R$. Es decir, si $A = (a)$.

6. El anillo de cocientes de un dominio entero

Inmersión

Para R y R' anillos, y $\varphi : R \to R'$ es un homomorfismo inyectivo, se dice que R está sumergido o inmerso en R', y que φ es una inmersión de R en R'.

Teorema 3C:

Todo dominio entero puede sumergirse en un campo. La construcción de este campo es casi completamente análoga a la construcción de los racionales a partir de los enteros.

Campo de cocientes

Si D es un dominio entero, el campo de cocientes $(F, +, \cdot)$ (cuya existencia se prueba para demostrar el teorema 3C) se construye de tal manera que $a/b = c/d$ si y solo si $ad = bc$, y

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

La inmersión $\varphi : D \to F$ es tal que $\varphi(a) = ab/b$, para $b \in D - \{0\}$.

7. Anillos euclideanos

Un dominio entero R es un anillo euclideano si existe una función $d : R \to \mathbb{Z}^+$ llamada d-valor, la cual cumple las siguientes propiedades:

- Si $a, b \in R - \{0\}$, entonces $d(a) \leq d(ab)$;
- Si $a, b \in R - \{0\}$, entonces existen $q, r \in R$ tales que $a = qb + r$, donde $r = 0$ o $d(r) < d(b)$.

La segunda es una formulación análoga al algoritmo de la división. Nótese que, por ejemplo, $(\mathbb{Z}, +, \cdot)$ es un anillo euclideano con d-valor dado por el valor absoluto.

Anillo de ideales principales

Un dominio entero R con elemento neutro multiplicativo es un anillo de ideales principales si para todo ideal A de R existe $a \in R$ tal que $A = (a)$.

Teorema 3D:

Si R es un anillo euclideano y A es un ideal de R, entonces existe $a \in R$ tal que $A = (a)$. Es decir, todo ideal de R es generado de algún elemento de R.

Corolario 1 del teorema 3D:

Todo anillo euclideano tiene elemento neutro multiplicativo.

Corolario 2 del teorema 3D:

Todo anillo euclideano es un anillo de ideales principales.

Divisibilidad

Si R es un anillo conmutativo y $a, b \in R$ con $a \neq 0$, entonces se dice que a divide a b si existe $c \in R$ tal que $ac = b$. Esto se denota por $a \mid b$.

Propiedades de la divisibilidad

Si R es un anillo conmutativo, entonces

- $\forall a, b \in R - \{0\}$ y $\forall c \in R$: Si $a \mid b$ y $b \mid c$, entonces $a \mid c$;
- $\forall a \in R - \{0\}$ y $\forall b, c \in R$: Si $a \mid b$ y $a \mid c$, entonces $a \mid (b \pm c)$;
- $\forall a \in R - \{0\}$ y $\forall b, c \in R$: Si $a \mid b$, entonces $a \mid bc$.

Máximo común divisor

Si R es un anillo conmutativo y $a, b \in R$, entonces $d \in R - \{0\}$ es un máximo común divisor de a y b en R si se cumplen

- $d \mid a$ y $d \mid b$;
- Si $c \in R - \{0\}$ es tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Lema 3.8 (propiedad de Bézout):

Si R es un anillo euclideano y $a, b \in R$ con máximo común divisor $d \in R - \{0\}$, entonces existen elementos $\lambda, \mu \in R$ tales que $d = \lambda a + \mu b$.

Unidad

Si R es un anillo conmutativo con elemento neutro multiplicativo, entonces u es una unidad de R si $u^{-1} \in R$ existe y es tal que $u \cdot u^{-1} = 1$. Esto es, un elemento de un anillo conmutativo con elemento neutro multiplicativo es unidad del mismo si y solo si su inverso multiplicativo está también en el anillo conmutativo.

Lema 3.9:

Si R es un dominio entero con elemento neutro multiplicativo y $a, b \in R$ tales que $a \mid b$ y $b \mid a$, entonces existe una unidad $u \in R$ tal que $a = ub$.

Asociación de elementos

Si R es un anillo conmutativo con elemento neutro multiplicativo con $a, b, u \in R$ donde u es una unidad de R y $a = ub$, entonces se dice que a y b están asociados.

Propiedad de la relación de asociación de elementos

La relación de asociación de elementos en un anillo conmutativo con elemento neutro multiplicativo es una relación de equivalencia.

Propiedad: Unicidad salvo asociación del máximo común divisor

Si R es un anillo euclideano con $a, b \in R$ tal que $d_1, d_2 \in R$ son máximos comunes divisores de a y b, entonces d_1 y d_2 son asociados.

Nota sobre el máximo común divisor

En rigor, en un anillo euclideano el máximo común divisor de un elemento no es único. Sin embargo, por la propiedad anterior, todos los máximos comunes divisores de un par de elementos son asociados. Entonces, en adelante, el símbolo (a, b) denotará a cualquier representante de la clase de equivalencia respecto a la asociación de los máximos comunes divisores de a y b. En este sentido es que en los anillos euclideanos se habla de unicidad salvo asociación del máximo común divisor.

Lema 3.10:

Si R es un anillo euclideano con $a, b \in R - \{0\}$ y b no es una unidad de R, entonces $d(a) < d(ab)$.

Elemento primo de un anillo euclideano

Si R es un anillo euclideano y $\pi \in R$ tal que π no es una unidad de R, se dice que π es un elemento primo de R si $\pi = ab$ implica que uno de a o b es unidad de R.

Propiedad: Caracterización de una unidad

Si R es un anillo euclideano y $a \in R - \{0\}$, entonces a es una unidad de R si y solo si $d(a) = d(1)$.

Lema 3.11 (existencia de factorizaciones primas):

Si R es un anillo euclideano, entonces todo elemento de $R - \{0\}$ puede factorizarse como el producto de un número finito de elementos primos de R.

Primos relativos

Si R es un anillo euclideano, se dice que $a, b \in R - \{0\}$ son primos relativos si su máximo común divisor es una unidad de R. Esta definición es equivalente a decir que a y b son primos relativos en R si y solo si $(a, b) = 1$.

Lema 3.12:

Si R es un anillo euclideano con $a, b, c \in R - \{0\}$ tales que $a \mid bc$ y $(a, b) = 1$, entonces $a \mid c$.

Propiedad: Comportamiento de los elementos primos

Si R es un anillo euclideano con elemento primo π y $a \in R$ es arbitrario, entonces $(\pi, a) = 1$ o $\pi \mid a$.

Lema 3.13:

Si R es un anillo euclideano con un elemento primo π y $a, b \in R - \{0\}$ tales que $\pi \mid ab$, entonces se cumple que $\pi \mid a$ o $\pi \mid b$.

Corolario del lema 3.13:

Si R es un anillo euclideano con elemento primo π y $r_1, \ldots, r_n \in R - \{0\}$ tal que $\pi \mid \prod_{i=1}^{n} r_i$, entonces existe un índice entero i con $1 \leq i \leq n$ tal que $\pi \mid r_i$

Teorema 3E (factorización prima única salvo asociación):

Si R es un anillo euclideano y $r \in R - \{0\}$ no es unidad de R, entonces si $r = \prod_{i=1}^{m} \pi_i = \prod_{j=1}^{n} \pi'_j$, donde todos los $\pi_1, \ldots, \pi_m$ y $\pi'_1, \ldots, \pi'_n$ son elementos primos de R, entonces $m = n$ y cada π_i es asociado con algún π'_j (y viceversa).

Lema 3.14:

Si R es un anillo euclideano y $a_0 \in R$, entonces (a_0) es un ideal maximal de R si y solo si a_0 es un elemento primo de R.

Las propiedades críticas de los anillos euclideanos

Nótese que los anillos euclideanos son una generalización que toma las siguientes propiedades de $\mathbb{Z}$:

1. **Dominio entero: Conmutativo, sin divisores de cero. Produce un campo de cocientes.**
2. **Tiene un d-valor.**
3. **Posee neutro multiplicativo y es anillo de ideales principales.**
4. **Algoritmo de la división.**
5. **Propiedad de Bézout.**
6. **Máximo común divisor único (salvo asociación).**
7. **Factorización prima única (salvo asociación).**
8. **π es elemento primo $\iff$ (π) es un ideal maximal $\iff$ $R/(\pi)$ es un campo.**

8. Un anillo euclideano particular

Además de los enteros, no es fácil encontrar anillos euclideanos (que no sean campos) particulares. Se platicó acerca de un caso particular: los enteros gaussianos.

El conjunto de los enteros de Gauss

El conjunto $\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$ (donde $i^2 = -1$) se llama conjunto de los enteros de Gauss o enteros gaussianos.

Los enteros de Gauss forman un dominio entero

El anillo $(\mathbb{Z}(i), +, \cdot)$ (donde $+$ y $\cdot$ representan la suma y producto usuales en los números complejos) es un dominio entero.

Teorema 3F:

El conjunto de los enteros de Gauss $(\mathbb{Z}(i), +, \cdot)$ es un anillo euclideano.

Lema 3.15:

Si $p \in \mathbb{Z}$ es un número primo tal que para $c \in \mathbb{Z}$ se cumple $(c, p) = 1$ y $cp = x^2 + y^2$ para $x, y \in \mathbb{Z}$, entonces también existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.

Lema 3.16:

Si $p \in \mathbb{Z}$ es un número primo de la forma $4n + 1$, entonces la congruencia $x^2 \equiv -1 \mod p$ tiene solución, con $x = [(p - 1)/2]!$.

Teorema 3G (por Fermat):

Si $p \in \mathbb{Z}$ es un número primo de la forma $4n + 1$, entonces existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.

9. Anillos de polinomios

Sea $\mathbb{F}$ un campo, entonces

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{F}, a_n \neq 0, n \in \mathbb{N} \right\}$$

es el conjunto de los polinomios en la variable x y coeficientes en $\mathbb{F}$ o sobre $\mathbb{F}$.

Igualdad entre polinomios

Si $\mathbb{F}$ es un campo, con $p(x) = \sum_{i=0}^{m} a_i x^i$ y $q(x) = \sum_{j=0}^{n} b_j x^j$ en $\mathbb{F}[x]$, entonces se da la igualdad $p(x) = q(x)$ si y solo si $m = n$ y $a_k = b_k$ para todo índice k.

Operaciones entre polinomios

Si $\mathbb{F}$ es un campo, con $p(x) = \sum_{i=0}^{m} a_i x^i$ y $q(x) = \sum_{j=0}^{n} b_j x^j$ en $\mathbb{F}[x]$, entonces

$$p(x) + q(x) = \sum_{k=0}^{\text{máx}\{m,n\}} (a_k + b_k) x^k,$$

$$p(x) \cdot q(x) = \sum_{l=0}^{m+n} \left(\sum_{k=0}^{l} a_{l-k} b_k \right) x^l,$$

con $a_i = 0$ cuando $i > m$ y $b_j = 0$ cuando $j > n$.

Estructura de los anillos de polinomios

Si $\mathbb{F}$ es un campo, entonces $(\mathbb{F}[x], +, \cdot)$ donde $+$ y $\cdot$ representan la suma y producto definidos anteriormente, forma un anillo conmutativo con elemento neutro multiplicativo.

Grado de un polinomio

Si $\mathbb{F}$ es un campo, entonces la función $\text{gr} : \mathbb{F}[x] - \{0\} \to \mathbb{N}$ tal que si

$$p(x) = \sum_{i=0}^{m} a_i x^i,$$

entonces $\text{gr}[p(x)] = m$ es el grado del polinomio $p(x)$. Por otro lado, el grado del polinomio 0 no está definido, y si $\text{gr}[q(x)] = 0$, entonces $q(x)$ es un polinomio constante.

Lema 3.17:

Si $\mathbb{F}$ es un campo con $f(x), g(x) \in \mathbb{F}[x] - \{0\}$, entonces $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.

Corolario 1 del lema 3.17:

Si $\mathbb{F}$ es un campo con $f(x), g(x) \in \mathbb{F}[x] - \{0\}$, entonces $\text{gr}(f) \leq \text{gr}(fg)$.

Corolario 2 del lema 3.17:

Si $\mathbb{F}$ es un campo entonces $(\mathbb{F}[x], +, \cdot)$ es un dominio entero.

Campo de las funciones racionales

Si $\mathbb{F}$ es un campo, el campo de cocientes de $\mathbb{F}[x]$ se denota por $\mathbb{F}(x)$ y se llama campo de funciones racionales en la variable x y con coeficientes en $\mathbb{F}$.

Lema 3.18 (Algoritmo de la división):

Si $\mathbb{F}$ es un campo con $f(x), g(x) \in \mathbb{F}[x] - \{0\}$, entonces existen polinomios $q(x), r(x) \in \mathbb{F}[x]$ tales que se cumple $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ o $\text{gr}(r) < \text{gr}(g)$.

Teorema 3H:

Si $\mathbb{F}$ es un campo, entonces $(\mathbb{F}[x], +, \cdot)$ es un anillo euclideano.

Lema 3.19:

Si $\mathbb{F}$ es un campo, entonces $\mathbb{F}[x]$ es un anillo de ideales principales.

Lema 3.20:

Si $\mathbb{F}$ es un campo, entonces $f(x), g(x) \in \mathbb{F}[x]$ tienen un único máximo común divisor (salvo asociación) llamado $d(x)$, para el cual existen polinomios $\lambda(x), \mu(x) \in \mathbb{F}[x]$ tales que $d(x) = \lambda(x)f(x) + \mu(x)g(x)$.

Polinomios irreducibles

Si $\mathbb{F}$ es un campo, $p(x) \in \mathbb{F}[x] - \{0\}$ es irreducible sobre $\mathbb{F}$ o irreducible en $\mathbb{F}[x]$ si siempre que existan $a(x), b(x) \in \mathbb{F}[x] - \{0\}$ tales que $p(x) = a(x)b(x)$, se tiene que solo uno de $\text{gr}(a)$ y $\text{gr}(b)$ es 0. Nótese que esta definición es equivalente a la de los elementos primos en un anillo euclideano.

Lema 3.21:

Si $\mathbb{F}$ es un campo, entonces todo polinomio en $\mathbb{F}[x] - \{0\}$ puede factorizarse de manera única (salvo asociación) como producto de polinomios irreducibles en $\mathbb{F}[x]$, o bien, es una unidad del anillo.

Lema 3.22:

Si $\mathbb{F}$ es un campo y $p(x) \in \mathbb{F} - \{0\}$, entonces $\big(p(x)\big)$ es un ideal maximal del anillo de polinomios si y solo si $p(x)$ es irreducible sobre $\mathbb{F}$.

10. Polinomios sobre el campo de racionales

Polinomios primitivos

Un polinomio con coeficientes enteros es primitivo si sus coeficientes son primos relativos.

Lema 3.23:

Si $f(x), g(x) \in \mathbb{Z}[x]$, ambos primitivos, entonces $f(x)g(x)$ es primitivo.

Contenido de un polinomio

El contenido de un polinomio con coeficientes enteros es el máximo común divisor de sus coeficientes. Si $f(x) \in \mathbb{Z}[x]$, su contenido se denota por $c(f)$.

Polinomio general como un primitivo por el contenido

Todo polinomio con coeficientes enteros puede escribirse como su contenido por un polinomio primitivo.

Teorema 3I (Lema de Gauss):

Si $f(x) \in \mathbb{Z}[x]$ es primitivo y puede factorizarse como el producto de dos polinomios con coeficientes en $\mathbb{Q}$, entonces puede factorizarse como el producto de dos polinomios $\lambda(x), \mu(x) \in \mathbb{Z}[x]$.

Polinomio mónico

Un polinomio es mónico si su coeficiente principal es 1.

Primitividad de los polinomios mónicos

Todo polinomio mónico es primitivo. Como corolario de esta propiedad, si un polinomio entero mónico se factoriza como el producto de dos polinomios con coeficientes racionales, entonces es posible factorizarlo como el producto de dos polinomios enteros mónicos.

Teorema 3J (Criterio de Einsenstein):

Si $f(x) \in \mathbb{Z}[x]$ tiene $\text{gr}(f) = n$ y coeficientes a_k para $0 \leq k \leq n$ con $k \in \mathbb{Z}$, y si p es un número primo tal que $p \nmid a_n$, pero $p \mid a_k$ para cada $0 \leq k \leq n-1$ y $p^2 \nmid a_0$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

11. Anillos de polinomios sobre anillos conmutativos

Polinomios en varias variables

Sea R un anillo conmutativo con elemento neutro multiplicativo, y sean $R_1 = R[x_1]$; $R_2 = R_1[x_2]$; $R_3 = R_2[x_3]$; y en general, se repite el proceso hasta llegar a

$$R_n = R_{n-1}[x_n] = R[x_1, \ldots, x_n] = \left\{ \sum a_{i_1,\ldots,i_n} \prod_{j=1}^{n} x_j^{i_j} : \ a_{i_1,\ldots,i_n} \in R, \ \ i_j \in \mathbb{N} \right\}.$$

Este es el conjunto de polinomios en las variables $x_1, \ldots, x_n$ con coeficientes en R. La igualdad y la suma en $R[x_1, \ldots, x_n]$ se define coeficiente por coeficiente y la multiplicación se define a través de la ley distributiva en R y las reglas de exponentes habituales:

$$\left(\prod_{j=1}^{n} x_j^{i_j} \right) \cdot \left(\prod_{j=1}^{n} x_j^{k_j} \right) = \left(\prod_{j=1}^{n} x_j^{i_j + k_j} \right).$$

Los anillos de polinomios en varias variables son anillos conmutativos

Si R es un anillo conmutativo con elemento neutro multiplicativo, $R[x_1, \ldots, x_n]$ también lo es.

Lema 3.24:

Si R es un dominio entero, entonces $R[x]$ es un dominio entero.

Corolario del lema 3.24:

Si R es un dominio entero, entonces $R[x_1, \ldots, x_n]$ es un dominio entero.

Campos de cocientes de anillos de polinomios de varias variables

Si R es un dominio entero, el campo de cocientes del dominio entero $R[x_1, \ldots, x_n]$ se llama campo de las funciones racionales en las variables $x_1, \ldots, x_n$ con coeficientes en R, y se denota por $R(x_1, \ldots, x_n)$.

Campo de funciones racionales en varias variables

En específico, para un campo $\mathbb{F}$ se tiene que $\mathbb{F}(x_1, \ldots, x_n)$ es el campo de las funciones racionales en las variables $x_1, \ldots, x_n$ con coeficientes en $\mathbb{F}$. Este campo es importante en la geometría algebraica y en la teoría de Galois.

Los anillos de polinomios en varias variables no necesariamente son anillos euclideanos

En efecto, los anillos de polinomios en varias variables no necesariamente son anillos de ideales principales, por lo cual no necesariamente son anillos euclideanos.

Dominio de factorización única

Un dominio entero R con elemento neutro multiplicativo es un dominio de factorización única si:

- Todo elemento no nulo de R es una unidad de R o puede escribirse como el producto de un número finito de elementos primos de R.
- La factorización de cada elemento es única salvo el orden y salvo asociación.

Lema 3.25:

Si R es un dominio de factorización única y $a, b \in R$, entonces existe $(a, b) \in R$ máximo común divisor de a y b. Además, si a y b son primos relativos y $a \mid bc$, entonces $a \mid c$.

Corolario del lema 3.25:

Si R es un dominio de factorización única con a elemento primo de R, con $b, c \in R$, y con $a \mid bc$, entonces $a \mid b$ o $a \mid c$.

Lema 3.26:

Si R es un dominio de factorización única entonces el producto de dos polinomios primitivos en $R[x]$ es también un polinomio primitivo en $R[x]$.

Corolario 1 del lema 3.26:

Si R es un dominio de factorización única, $c(fg) = c(f)c(g)$ salvo asociación para $f(x), g(x) \in R[x]$.

Corolario 2 del lema 3.26:

Si R es un dominio de factorización única con $f_1(x), \ldots, f_n(x) \in R[x]$, entonces

$$c\left(\prod_{i=1}^{n} f_i\right) = \prod_{i=1}^{n} c(f_i).$$

Polinomios sobre el campo de cocientes

Sea R un dominio de factorización única y F su campo de cocientes. Viendo a $R[x]$ como un subanillo de $F[x]$, si $f(x) \in F[x]$ entonces existen $a \in R - \{0\}$ y $f_0(x) \in R[x]$ tales que $f(x) = f_0(x)/a$. Recordar que a no necesariamente es el contenido de f.

Lema 3.27:

Sea R un dominio de factorización única, F su campo de cocientes, y $f(x) \in R[x]$ un polinomio primitivo sobre R. Entonces, $f(x)$ es irreducible sobre R si y solo si $f(x)$ es irreducible sobre F.

Lema 3.28:

Si R es un dominio de factorización única, $f(x) \in R[x]$, y $f(x)$ es un polinomio primitivo sobre R, entonces puede factorizarse de manera única (salvo asociación) como producto de polinomios irreducibles en $R[x]$.

Teorema 3K:

Si R es un dominio de factorización única, entonces $R[x]$ es un dominio de factorización única.

Corolario 1 del teorema 3K:

Si R es un dominio de factorización única, entonces $R[x_1, \ldots, x_n]$ es un dominio de factorización única.

Corolario 2 del teorema 3K:

Si $\mathbb{F}$ es un campo, entonces $\mathbb{F}[x_1, \ldots, x_n]$ es un dominio de factorización única.