Notas del curso de Algebra Moderna II

Luis Valero Elizondo

15 de Enero del 2004

Índice general

1. Anillos. **5**
- 1.1. Monoides. . . . 5
- 1.2. Anillos. . . . 5
- 1.3. Ejemplos de anillos. . . . 7
- 1.4. Propiedades básicas de los anillos. . . . 9
- 1.5. Unidades. . . . 10
- 1.6. Operaciones con subconjuntos. . . . 10
- 1.7. Subanillos 11

2. Ideales. **12**
- 2.1. Ideales. . . . 12
- 2.2. Anillos cocientes. . . . 14
- 2.3. Ideales primos. . . . 14
- 2.4. Ideales maximales. . . . 15

3. Homomorfismos. **16**
- 3.1. Homomorfismos. . . . 16
- 3.2. Algunas propiedades de los homomorfismos. . . . 17
- 3.3. Isomorfismos. . . . 17
- 3.4. Núcleos e imágenes. . . . 18
- 3.5. Teoremas de isomorfismo. . . . 18
- 3.6. Teorema de la correspondencia. . . . 19

4. Dominios enteros. **20**
- 4.1. Ejemplos. . . . 20
- 4.2. Campo de cocientes de un dominio entero. . . . 20
- 4.3. Divisibilidad. . . . 21
- 4.4. Máximo común divisor. . . . 22

4.5. Elementos irreducibles y elementos primos. 22
4.6. Dominios de factorización única. 23
4.7. Dominios de ideales principales. 23
4.8. Dominios euclidianos. 24

5. Anillos de polinomios. 25
5.1. Definición de los polinomios con coeficientes en un anillo conmutativo. 25
5.2. Anillos de polinomios sobre dominios enteros. 26
5.3. Anillos de polinomios con coeficientes en un campo. 27
5.4. Derivadas y raíces múltiples. 28
5.5. Polinomios irreducibles. 29

6. Campos. 31
6.1. Extensiones algebraicas. 31
6.2. Generadores de una extensión. 32
6.3. Campos de descomposición. 32
6.4. Cerradura algebraica. 33
6.5. Extensiones separables. 34

7. Teoría de Galois. 36
7.1. Grupo de Galois. 36
7.2. Extensiones normales. 37
7.3. Teorema fundamental de la teoría de Galois. 38
7.4. Extensiones cíclicas y abelianas. 38
7.5. Campos finitos. 39
7.6. Teorema del elemento primitivo. 39
7.7. Construcciones con regla y compás. 40
7.8. Solubilidad por radicales. 41

Introducción

Estas son notas para el curso de Algebra Moderna II que se imparte en la Facultad de Ciencias Físico-Matemáticas de la Universidad Michoacana de San Nicolás de Hidalgo. En este curso se cubren los temas de teoría de anillos, teoría de campos y teoría de Galois. Este último tema es el corazón del curso.

La teoría de Galois es una de las ramas más elegantes del álgebra, o quizás incluso de la matemática misma. Para poder entenderla, es necesario manejar con cierta soltura anillos (principalmente los anillos de polinomios) y la teoría de grupos. Así pues el curso comienza con una introducción rápida a la teoría de anillos (anillos conmutativos, ideales, homorfismos, anillos cociente, ideales maximales, ideales primos, dominios enteros y anillos de polinomios), y sigue con otra introducción sencilla a la teoría de campos (extensiones, extensiones algebraicas, campos de descomposición, extensiones separables). Una vez cubiertos estos requisitos, abordamos la teoría de Galois (grupo de Galois, extensiones normales, teorema fundamental de la teoría de Galois, aplicaciones a campos finitos, a extensiones primitivas, construcciones con regla y compás y solubilidad por radicales).

Las notas están escritas como una lista (bastante larga) de ejercicios y definiciones. Muchos de los ejercicios los haremos en clase, y los demás quedarán como tarea para que los hagan ustedes. La secuencia de los ejercicios es muy importante, pues problemas anteriores suelen simplificar enormemente ejercicios posteriores (por lo que si se atoran en un problema, les conviene ver los enunciados de los problemas anteriores). No se dejen engañar por el nombre "ejercicios"; de hecho, muchos de ellos son teoremas clásicos de la teoría. Todas las definiciones son importantes y deberán aprenderlas de memoria. Es posible que en los exámenes les pregunte una que otra definición.

Al final de las notas hay un índice analítico – para que puedan localizar fácilmente la definición de cualquier concepto – y una bibliografía con algunos

libros clásicos en el tema.

Espero que este curso sea una experiencia educativa agradable para todos nosotros.

Capítulo 1

Anillos.

1.1. Monoides.

Definición 1. Un **monoide** es un semigrupo $(M,*)$ en el que existe un elemento 1 tal que $1m = m = m1$ para todo $m \in M$. Usualmente denotamos al monoide $(M,*)$ por M, y escrimos mn en lugar de $m * n$.

Ejercicio 2. Mencione cinco monoides que no sean grupos.

Ejercicio 3. Sea M un monoide. Demuestre que existe un único elemento 1 tal que $1\ m = m$ para todo $m \in M$. Al elemento 1 se le llama el **elemento identidad** del monoide M.

1.2. Anillos.

Definición 4. Un **anillo** es una tercia ordenada $(A, +, \cdot)$, donde A es un conjunto no vacío y $+$, $\cdot$ son operaciones binarias asociativas en A que cumplen lo siguiente:

(1) $(A, +)$ es un grupo abeliano, cuyo elemento identidad se suele denotar 0, y comúnmente se llama el **cero** del anillo A. A veces lo escribiremos como 0_A para enfatizar el hecho de que es el cero del anillo A.

(2) $(A, \cdot)$ es un monoide, cuyo elemento identidad se suele denotar 1, y comúnmente se llama el **uno** del anillo A. A veces lo escribiremos como 1_A para enfatizar el hecho de que es el uno del anillo A.

(3) (Leyes distributivas) Para cualesquiera a, b, $c \in A$ se tiene que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Usualmente denotamos un anillo $(A, +, \cdot)$ simplemente por A. La operación $+$ se llama **suma**, y la operación $\cdot$ el **producto** del anillo A. Siguiendo la convención para grupos abelianos, el inverso aditivo de a se denota $-a$. Usualmente escribimos ab en lugar de $a \cdot b$. Para algunos autores, nuestra definición de anillo es lo que ellos llaman un **anillo con uno**.

Notación 5. Al interpretar una expresión que involucre sumas y productos en un anillo, el producto lleva prioridad sobre la suma. Es decir, la expresión $a + bc$ se debe interpretar como $a + (bc)$.

Ejercicio 6. Mencione diez anillos.

Ejercicio 7. Explique por qué $\mathbb{N}$ con las operaciones usuales de suma y producto no es un anillo.

Definición 8. Un anillo A es **conmutativo** si el producto de A es conmutativo, es decir, si para cualesquiera $a, b \in A$ se tiene que $ab = ba$.

Observación 9. En estas notas nos vamos a interesar principalmente en los anillos conmutativos. Sin embargo, muchos resultados valen en general para anillos no conmutativos también, así que el lector encontrará muchos ejercicios enunciados para anillos en general.

Ejercicio 10. Sea D un anillo conmutativo no cero. Demuestre que son equivalentes las siguientes condiciones:

(1) Para cualesquiera $a, b \in D$, si $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$.

(2) Para cualesquiera $a, b \in D$, si $ab = 0$, entonces $a = 0$ o $b = 0$.

(3) (Ley de la cancelación izquierda) Para cualesquiera $a, b, c \in D$, si $ab = ac$, entonces $b = c$.

(4) (Ley de la cancelación derecha) Para cualesquiera $a, b, c \in D$, si $ba = ca$, entonces $b = c$.

Un anillo conmutativo que satisfaga cualquiera de estas condiciones se llama un **dominio**, o también un **dominio entero**.

Ejercicio 11. Mencione cuáles de los siguientes anillos son dominios enteros: $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $M_2(\mathbb{Q})$.

Ejercicio 12. Sea A un anillo no cero. Demuestre que son equivalentes las siguientes condiciones:

(1) Para cualquier $a \in A$, si $a \neq 0$, entonces existe $b \in A$ tal que $ab = 1$.

(2) Para cualquier $a \in A$, si $a \neq 0$, entonces existe $b \in A$ tal que $ba = 1$.

(3) Para cualquier $a \in A$, si $a \neq 0$, entonces existe $b \in A$ tal que $ab = 1 = ba$.

(4) El conjunto $\{a \in A \mid a \neq 0\}$ forma un grupo con el producto de A.

Un anillo que cumpla cualquiera de las condiciones anteriores se llama un **anillo con división**.

Ejercicio 13. Sea A un anillo. Demuestre que son equivalentes las siguientes condiciones:

(1) A es un anillo conmutativo con división.

(2) A es un anillo conmutativo en donde todo elemento distinto de cero tiene un inverso multiplicativo.

(3) El conjunto $\{a \in A \mid a \neq 0\}$ forma un grupo abeliano con el producto de A.

Un anillo que cumpla cualquiera de las condiciones anteriores se llama un **campo**. Algunos autores usan la palabra **cuerpo** en lugar de campo.

Ejercicio 14. Mencione cuáles de los siguientes anillos son campos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

Ejercicio 15. Demuestre que todo campo es un dominio entero.

Ejercicio 16. Exhiba un dominio entero que no sea campo.

1.3. Ejemplos de anillos.

Ejercicio 17. Sea A un conjunto con un sólo elemento. Demuestre que existe una única operación binaria en A, y que A con esa operación binaria como suma y producto a la vez es un anillo conmutativo. A este tipo de anillo se le llama **anillo cero**.

Ejercicio 18. Sea A un anillo. Demuestre que A es el anillo cero si y sólo si $0 = 1$.

Ejercicio 19. Sea $\mathbb{G} = \{n + mi \mid n, m \in \mathbb{Z}\}$, donde i denota una de las raíces cuadradas complejas de -1. Demuestre que $\mathbb{G}$ es un anillo conmutativo con las operaciones usuales de suma y producto de números complejos. A este anillo se le conoce como el anillo de los **enteros Gaussianos**.

Ejercicio 20. Sea $A = \{n + m\sqrt{5} \mid n, m \in \mathbb{Z}\}$, donde $\sqrt{5}$ denota una de las raíces cuadradas reales de 5. Demuestre que A es un anillo conmutativo con las operaciones usuales de suma y producto de números reales.

Ejercicio 21. Sean A y B anillos. Demuestre que el producto cartesiano $A \times B$ es un anillo con suma y producto **coordenada a coordenada**, es decir, $(a, b) + (c, d) = (a + c, b + d)$ y $(a, b) \cdot (c, d) = (ac, bd)$. A este anillo se le llama el **producto directo externo** de A y B.

Definición 22. Sea A un anillo y sea $\sim$ una relación de equivalencia en A. Decimos que $\sim$ **preserva las operaciones** del anillo A si para todos $a, b, c, d \in A$ se tiene que si $a \sim b$ y $c \sim d$ entonces $a + c \sim b + d$ y $ac \sim bd$.

Ejercicio 23. Sea A un anillo y sea $\sim$ una relación de equivalencia en A que preserva las operaciones del anillo. Sea $A/\sim$ el conjunto de clases de equivalencia de A. Definamos una suma y un producto en $A/\sim$ como sigue: Dados $C, D \in A/\sim$, escojamos representantes $a \in C$ y $b \in D$; la suma $C + D$ de las clases de equivalencia es la clase que contiene a $a + b$; el producto CD de las clases de equivalencia es la clase que contiene a ab. Demuestre que estas operaciones en $A/\sim$ están bien definidas, y que dan a $A/\sim$ estructura de anillo, llamado el **anillo cociente** de A módulo la relación de equivalencia $\sim$. Un elemento C de $A/\sim$ se suele denotar $\bar{a}$, donde a es un elemento de C, llamado un **representante** de C.

Ejercicio 24. Sea n un entero positivo. Demuestre que la relación de congruencia módulo n en $\mathbb{Z}$, (denotada $\equiv_n$), preserva la suma y el producto de $\mathbb{Z}$. Concluya que $\mathbb{Z}/\equiv_n$ es un anillo. Demuestre que este anillo tiene exactamente n elementos. Este anillo se llama el **anillo de los enteros módulo n** , y se denota $\mathbb{Z}/n\mathbb{Z}$.

Ejercicio 25. Sea A un anillo, y sea n un entero positivo. Sea $M_n(A)$ el conjunto de las matrices de tamaño n por n con coeficientes en el anillo A. Demuestre que $M_n(A)$ es un anillo con la suma y el producto usual de matrices. Demuestre que si $n \geq 2$, entonces $M_n(A)$ no es conmutativo.

Ejercicio 26. Sean A un anillo y C un conjunto cualquiera. Sea A^C el conjunto de funciones de C en A. Definimos una suma y un producto en A^C **puntualmente**, es decir, para $f, g \in A^C$ definimos $f + g$ como la función dada por $(f + g)(a) = f(a) + g(a)$. Análogamente definimos el producto $f \cdot g$ como la función dada por $(f \cdot g)(a) = f(a)g(a)$. Demuestre que estas operaciones convierten a A^C en un anillo, llamado el **anillo de funciones** de C en A.

Ejercicio 27. Sea A un anillo. Demuestre que $A^\emptyset$ es el anillo cero.

Ejercicio 28. Sea A un anillo y C un conjunto no vacío. Demuestre que A es conmutativo si y sólo si A^C es conmutativo.

Ejercicio 29. Sea k un campo y V un k-espacio vectorial. Sea $End_k(V)$ el conjunto de transformaciones lineales de V en sí mismo. Defina en V una suma puntualmente (vea el Ejercicio 26), y defina el producto en $End_k(V)$ como la composición de funciones. Demuestre que $End_k(V)$ es un anillo, llamado el **anillo de endomorfismos** del espacio vectorial V.

1.4. Propiedades básicas de los anillos.

Ejercicio 30. Sea A un anillo. Demuestre que para cualquier $a \in A$ se tiene que $-(-a) = a$, es decir, el inverso aditivo del inverso aditivo de a es a.

Definición 31. Sean A un anillo, $a \in A$ y n un entero positivo. Definimos $0a = 0$ (donde el 0 de la izquierda está en $\mathbb{Z}$, y el 0 de la derecha está en A), $1a = a$, y $a^1 = a$ (donde ambos 1's están en $\mathbb{Z}$). Inductivamente también definimos $(n+1)a = na + a$ y $a^{n+1} = a^n a$. Además, definimos $(-n)a = -(na)$, donde -b denota al inverso aditivo de b en $(A, +)$. Los elementos de la forma na y (-n)a se llaman **múltiplos enteros** de a, y los elementos de la forma a^n se llaman **potencias** de a.

Ejercicio 32. Sean A un anillo y $a \in A$. Demuestre que $(-1)a = -a$, donde -1 denota un elemento de $\mathbb{Z}$, y $-a$ denota el inverso aditivo de a en A.

Ejercicio 33. Sean A un anillo, $a \in A$, n, m enteros. Demuestre que $(nm)a = n(ma)$, y que $(n + m)a = na + ma$.

Ejercicio 34. Sean A un anillo, $a \in A$, n, m enteros positivos. Demuestre que $(a^n)^m = a^{nm} = (a^m)^n$.

Ejercicio 35. Sea A un anillo. Demuestre que para cualquier $a \in A$ se tiene que $0a = 0a + 0a$. Concluya que $0a = 0$. Demuestre análogamente que $a0 = 0$.

Ejercicio 36. Sea A un anillo. Demuestre que para cualquier $a \in A$ se tiene que $(-1)a = -a$, donde -1 denota al inverso aditivo de 1 en A, y $-a$ denota al inverso aditivo de a. Demuestre también que $a(-1) = -a$. Compare este ejercicio con el Ejercicio 32.

Ejercicio 37. Sea A un anillo. Demuestre que $(-1)(-1) = 1$.

Ejercicio 38. Sea A un anillo. Demuestre que para cualesquiera $a, b \in A$ se tiene que $(-a)b = -(ab) = a(-b)$.

Ejercicio 39. Sea A un anillo. Demuestre que para cualesquiera $a, b \in A$ se tiene que $(-a)(-b) = ab$.

1.5. Unidades.

Definición 40. Sea A un anillo, y sea $a \in A$. Decimos que a es una **unidad** de A si existe un elemento $b \in A$ tal que $ab = 1 = ba$. Al conjunto de todas las unidades del anillo A lo denotamos A^*.

Ejercicio 41. Sea A un anillo. Demuestre que el producto de dos unidades es una unidad. Concluya que A^* es un grupo con el producto de A. A este grupo se le llama el **grupo de unidades** del anillo A.

Ejercicio 42. Calcule el grupo de unidades de $\mathbb{Z}$ y de $\mathbb{Z} \times \mathbb{Z}$.

Ejercicio 43. Sean k un campo y V un k-espacio vectorial de dimensión infinita numerable. Demuestre que un elemento en $End_k(V)$ tiene inverso izquierdo si y sólo si es una función inyectiva. Demuestre que existe un elemento en $End_k(V)$ que tiene inverso izquierdo pero que no es unidad. Demuestre que el conjunto de todos los elementos de $End_k(V)$ que tienen inverso izquierdo es cerrado bajo productos pero no bajo inversos multiplicativos. Compare este ejercicio con el Ejercicio 12.

Ejercicio 44. Sea A un anillo y sea $a \in A$ tal que existen $b, c \in A$ con $ab = 1 = ca$. Simplifique la expresión cab de dos maneras para demostrar que $b = c$. Concluya que a es una unidad. Al elemento b se le denota a^{-1}, y se le llama el **inverso multiplicativo** de la unidad a, o simplemente el **inverso** de la unidad a. Note que solamente las unidades tienen inversos multiplicativos.

1.6. Operaciones con subconjuntos.

Definición 45. Sea A un anillo, y sean C y D subconjuntos de A. Definimos su **suma**, denotada $C+D$, como el conjunto $\{a+b \mid a \in C, b \in D\}$. Si $C = \{a\}$, usualmente escribimos $a + D$ en lugar de $\{a\} + D$.

Ejercicio 46. Sean A un anillo y C, D, E subconjuntos de A. Demuestre que $(C + D) + E = C + (D + E)$. Por esta razón, este conjunto se denota $C + D + E$.

Ejercicio 47. Demuestre que $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Ejercicio 48. Sean A un anillo, C un subconjunto de A y a un elemento de A. Definimos aC como el conjunto $\{ab \mid b \in C\}$. Análogamente se define Ca como el conjunto $\{ba \mid b \in C\}$.

Observación 49. Más adelante definiremos un producto para algunos subconjuntos de A, pero la definición no es la "obvia".

1.7. Subanillos

Definición 50. Sea A un anillo. Un **subanillo** de A es un subconjunto no vacío S que es cerrado bajo sumas, inversos aditivos y productos, y tal que existe un elemento $e \in S$ con la propiedad de que $ea = a = ae$ para todo $a \in S$. Note que e no necesariamente es igual al uno de A.

Ejercicio 51. Sea $A = \mathbb{Z} \times \mathbb{Z}$. Demuestre que $S = \{(n, 0) \mid n \in \mathbb{Z}\}$ es un subanillo de A, y que el uno de A no pertenece a S.

Ejercicio 52. Sea A un anillo, y sea $e \in A$ tal que $e^2 = e \neq 0$. Demuestre que el conjunto $eAe = \{eae \mid a \in A\}$ es un subanillo de A cuyo uno es e.

Ejercicio 53. Muestre con un ejemplo que no todo subanillo es de la forma descrita en el Ejercicio 52, es decir, exhiba un anillo A y un subanillo S tal que no existe $e \in A$ con $e^2 = e$ y $S = eAe$.

Capítulo 2

Ideales.

2.1. Ideales.

Definición 54. Sea A un anillo. Un **ideal izquierdo** de A es un subconjunto no vacío I que es cerrado bajo sumas e inversos aditivos, y tal que para todo $a \in A$ se tiene $aI \subseteq I$, es decir, para todo $i \in I$ tenemos que $ai \in I$.

Ejercicio 55. Defina **ideal derecho**.

Definición 56. Sea A un anillo. Un **ideal bilateral** de A (también llamado simplemente **ideal** de A) es un subconjunto no vacío I que es cerrado bajo sumas e inversos aditivos, y tal que para todo $a \in A$ se tiene $aI \subseteq I$ y $Ia \subseteq I$, es decir, para todo $i \in I$ tenemos que $ai \in I$ y $ia \in I$.

Ejercicio 57. Sea A un anillo. Demuestre que A es un ideal bilateral de A, llamado el **ideal total** de A.

Definición 58. Sea A un anillo y sea I un ideal de A. Decimos que I es un ideal **propio** de A si $I \neq A$.

Ejercicio 59. Sea A un anillo. Demuestre que el conjunto $\{0\}$ es un ideal bilateral de A, llamado el **ideal cero** de A, y denotado usualmente 0.

Ejercicio 60. Sea A un anillo, y sea $a \in A$. Demuestre que el conjunto $Aa = \{ba \mid b \in A\}$ es un ideal izquierdo de A.

Ejercicio 61. Enuncie y demuestre un resultado análogo al Ejercicio 60 para ideales derechos.

Ejercicio 62. Sea A un anillo no cero. Demuestre que son equivalentes las siguientes condiciones:

(1) A es un anillo con división.
(2) Los únicos ideales izquierdos de A son el cero y el total.
(3) Los únicos ideales derechos de A son el cero y el total.

Ejercicio 63. Sea A un anillo, y sea I un subconjunto de A. Demuestre que I es un ideal bilateral de A si y sólo si I es simultáneamente un ideal izquierdo y un ideal derecho de A.

Ejercicio 64. Sea A un anillo conmutativo, y sea I un ideal de A. Demuestre que I es un ideal izquierdo de A si y sólo si I es un ideal derecho de A si y sólo si I es un ideal bilateral de A.

Ejercicio 65. Sea A un anillo conmutativo no cero. Demuestre que A es un campo si y sólo si los únicos ideales de A son el cero y el total.

Ejercicio 66. Sea n un entero positivo. Demuestre que el conjunto $n\mathbb{Z}$ que consta de los múltiplos enteros de n es un ideal de $\mathbb{Z}$.

Ejercicio 67. Demuestre que todos los ideales no cero de $\mathbb{Z}$ son de la forma descrita en el ejercicio 66, es decir, de la forma $n\mathbb{Z}$ para algún entero positivo n.

Ejercicio 68. Demuestre que la intersección arbitraria de ideales de un anillo es un ideal. Muestre con un ejemplo que la unión de dos ideales no necesariamente es un ideal.

Ejercicio 69. Sea A un anillo y sea C un subconjunto de A. Demuestre que existe un único ideal I con las siguientes propiedades:

(1) $C \subseteq I$;
(2) Para todo ideal J de A, si $C \subseteq J$ entonces $I \subseteq J$.

Al ideal I se le llama el **ideal generado** por el conjunto C, y se le denota $< C >$. Si $C = \{a_1, \ldots, a_n\}$, uno escribe $<a_1, \ldots, a_n>$ en lugar de $< C >$.

Ejercicio 70. Sea A un anillo conmutativo, y sea $a \in A$. Demuestre que $< a >= aA$. Muestre con un ejemplo que este resultado no es válido para anillos no conmutativos.

Ejercicio 71. Sean A un anillo, I y J ideales de A. Demuestre que $I + J$ es un ideal de A. Más aún, demuestre que $I + J$ está contenido en cualquier ideal que contenga tanto a I como a J. En otras palabras, $I + J$ es el ideal generado por $I \cup J$.

Definición 72. Sea A un anillo, y sean I y J ideales de A. Definimos el **ideal producto** de I y J, denotado IJ, como el ideal generado por el conjunto $\{ab \mid a \in I,\ b \in J\}$.

Ejercicio 73. Sea A un anillo conmutativo, y sean $a, b \in A$. Demuestre que $(aA)(bA) = abA$.

Ejercicio 74. Muestre con un ejemplo que dado un anillo A y dos ideales I y J, el conjunto $\{ab \mid a \in I,\ b \in J\}$ no es en general un ideal de A. (Si necesita ayuda, consulte la sección sobre anillos de polinomios.)

2.2. Anillos cocientes.

Ejercicio 75. Sea A un anillo y sea I un ideal bilateral de A. Defina una relación $\sim_I$ por $a \sim_I b$ si y sólo si $a - b \in I$. Demuestre que $\sim_I$ es una relación de equivalencia en A que preserva la suma y el producto de A. Al anillo $A/\sim_I$ se le llama **anillo cociente** de A módulo el ideal I, y se denota A/I.

Ejercicio 76. Sea n un entero positivo. Demuestre que el anillo $\mathbb{Z}/n\mathbb{Z}$ es un anillo cociente de $\mathbb{Z}$ módulo un ideal.

2.3. Ideales primos.

Definición 77. Sea A un anillo conmutativo. Un ideal propio P de A es un **ideal primo** de A si para cualesquiera $a, b \in A$ se tiene que si $ab \in P$, entonces $a \in P$ o $b \in P$.

Ejercicio 78. Sea A un anillo conmutativo no cero. Demuestre que A es un dominio entero si y sólo si el ideal cero es primo.

Ejercicio 79. Sea n un entero positivo. Demuestre que el ideal $n\mathbb{Z}$ de $\mathbb{Z}$ es primo si y sólo si n es un número primo.

Ejercicio 80. Sean A un anillo conmutativo, P un ideal propio de A. Demuestre que P es un ideal primo si y sólo si A/P es un dominio entero.

2.4. Ideales maximales.

Definición 81. Sea A un anillo. Un ideal M de A es un ideal **maximal** de A si M es un ideal propio de A (es decir, $M \neq A$), y M no está contenido propiamente en ningún ideal intermedio entre M y A, es decir, no existe un ideal I tal que $M \subset I \subset A$ con inclusiones propias.

Ejercicio 82. Sea A un anillo, y M un ideal propio de A. Demuestre que M es un ideal maximal de A si y sólo si para todo ideal I de A, o bien $I \subseteq M$, o bien $M + I = A$.

Ejercicio 83. Sea A un anillo conmutativo no cero. Demuestre que A es un campo si y sólo si el ideal cero es maximal.

Ejercicio 84. Sean A un anillo conmutativo no cero, M un ideal propio de A. Demuestre que M es un ideal maximal si y sólo si A/M es un campo.

Ejercicio 85. Sea A un anillo conmutativo, y sea M un ideal maximal de A. Demuestre que M es un ideal primo de A.

Ejercicio 86. Sea n un entero positivo. Demuestre que el ideal $n\mathbb{Z}$ de $\mathbb{Z}$ es maximal si y sólo si n es un número primo.

Ejercicio 87. Encuentre un ideal de $\mathbb{Z}$ que sea primo pero que no sea maximal.

Capítulo 3

Homomorfismos.

3.1. Homomorfismos.

Definición 88. Sean A y B anillos, y sea $\varphi : A \longrightarrow B$ una función. Decimos que φ es un **homomorfismo de anillos** si cumple lo siguiente:

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ para cualesquiera $a, b \in A$;
(2) $\varphi(ab) = \varphi(a)\varphi(b)$ para cualesquiera $a, b \in A$;
(3) $\varphi(1_A) = 1_B$.

Algunos autores le llaman a esto un **homomorfismo de anillos con uno**, y reservan el nombre de homomorfismo de anillos a algo que cumpla (1) y (2), aunque no mande al uno de A en el uno de B. Un **isomorfismo** es un homomorfismo biyectivo. Un **endomorfismo** es un homomorfismo de un anillo en sí mismo. Un **automorfismo** es un isomorfismo de un anillo en sí mismo. Dos anillos A y B son **isomorfos**, denotado $A \cong B$, si existe un isomorfismo de A en B.

Ejercicio 89. Mencione diez ejemplos de homomorfismos de anillos.

Ejercicio 90. Sea A un anillo y sea I un ideal de A. Demuestre que la función $\pi : A \longrightarrow A/I$ dada por $\pi(a) = aI$ es un homomorfismo suprayectivo de anillos. A esta función se le llama el **mapeo natural** de A en A/I. También se le conoce como **aplicación cociente**.

Ejercicio 91. Demuestre que no existen homomorfismos de anillos de $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/3\mathbb{Z}$, ni tampoco de $\mathbb{Z}/3\mathbb{Z}$ en $\mathbb{Z}/2\mathbb{Z}$.

Ejercicio 92. Sea A un anillo arbitrario. Demuestre que existe un único homomorfismo de $\mathbb{Z}$ en A, el cuál está dado por la fórmula $\varphi(n) = n1_A$.

Ejercicio 93. Demuestre que la composición de dos homomorfismos es un homomorfismo.

3.2. Algunas propiedades de los homomorfismos.

Ejercicio 94. Sea $\varphi : A \longrightarrow B$ un homomorfismo de anillos. Demuestre que φ es un homomorfismo entre sus grupos aditivos. Concluya que $\varphi(0_A) = 0_B$.

Ejercicio 95. Sean A y B anillos, $\varphi : A \longrightarrow B$ un homomorfismo, y sea $a \in A$ una unidad. Demuestre que $\varphi(a)$ es una unidad, y que de hecho φ se restringe a un homomorfismo de grupos de A^* a B^*. Concluya que $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Ejercicio 96. Sean A y B anillos, $\varphi : A \longrightarrow B$ un homomorfismo, y sea $a \in A$. Demuestre que φ preserva múltiplos enteros y potencias, es decir, para cualquier entero n se tiene que $\varphi(na) = n\varphi(a)$, y si n es positivo, también se tiene $\varphi(a^n) = \varphi(a)^n$.

3.3. Isomorfismos.

Ejercicio 97. Sea A un anillo. Demuestre que la **función identidad** de A, es decir, $id_A : A \longrightarrow A$ dada por $id_A(a) = a$ para toda a en A, es un automorfismo del anillo A.

Ejercicio 98. Sean A un anillo y $a \in A$. Defina la función $\varsigma_a : A \longrightarrow A$ por $\varsigma_a(b) = aba^{-1}$ para todo $b \in A$. Demuestre que ς_a es un automorfismo de A, llamado un automorfismo **interno**.

Ejercicio 99. Demuestre que la composición de dos isomorfismos es un isomorfismo.

Ejercicio 100. Demuestre que el inverso de un isomorfismo es un isomorfismo.

Ejercicio 101. Sea A un anillo. Demuestre que el conjunto de los automorfismos de A es un grupo con la composición de funciones. Este grupo se llama el **grupo de automorfismos** de A.

Ejercicio 102. Sean A, B, C anillos.
(i) Demuestre que $A \cong A$.
(ii) Demuestre que si $A \cong B$, entonces $B \cong A$.
(iii) Demuestre que si $A \cong B$ y $B \cong C$, entonces $A \cong C$.

3.4. Núcleos e imágenes.

Definición 103. Sean A y B anillos, y $\varphi : A \longrightarrow B$ un homomorfismo. El **núcleo** de φ, denotado $\mathrm{Ker}(\varphi)$, es el conjunto $\{a \in A \mid \varphi(a) = 0_B\}$. La **imagen** de φ, denotada $\mathrm{Im}(\varphi)$, es el conjunto $\{\varphi(a) \mid a \in A\}$.

Ejercicio 104. Sean A y B anillos, y $\varphi : A \longrightarrow B$ un homomorfismo. Demuestre que $\mathrm{Ker}(\varphi)$ es un ideal de A.

Ejercicio 105. Sean A y B anillos, y $\varphi : A \longrightarrow B$ un homomorfismo. Demuestre que φ es inyectivo si y sólo si $\mathrm{Ker}(\varphi)$ es el ideal cero.

Ejercicio 106. Sean A y B anillos, y $\varphi : A \longrightarrow B$ un homomorfismo. Demuestre que $\mathrm{Im}(\varphi)$ es un subanillo de B. Dé un ejemplo en el que $\mathrm{Im}(\varphi)$ no sea un ideal de H.

3.5. Teoremas de isomorfismo.

Ejercicio 107. Sean A y B anillos, y sea $\varphi : A \longrightarrow B$ un homomorfismo con núcleo I. Demuestre que la función $\bar{\varphi} : A/I \longrightarrow B$ dada por $\bar{\varphi}(aI) = \varphi(a)$ está bien definida y es un homomorfismo inyectivo.

Ejercicio 108. Sean A y B anillos, sea I un ideal de A y sea $\varphi : A \longrightarrow B$ un homomorfismo. Demuestre que la función $\bar{\varphi} : A/I \longrightarrow B$ dada por $\bar{\varphi}(aI) = \varphi(a)$ está bien definida si y sólo si $\mathrm{Ker}(\varphi)$ contiene a I. Demuestre que si $\bar{\varphi}$ está bien definida, entonces es un homomorfismo, y que $\bar{\varphi}$ es inyectiva si y sólo si $\mathrm{Ker}(\varphi) = I$.

Ejercicio 109. (Primer teorema de isomorfismo) Sean A y B anillos, y sea $\varphi : A \longrightarrow B$ un homomorfismo con núcleo I. Demuestre que I es un ideal de A y que A/I es isomorfo a la imagen de φ. Demuestre que la función $\bar{\varphi} : A/I \longrightarrow \mathrm{Im}(\varphi)$ dada por $\bar{\varphi}(aI) = \varphi(a)$ es un isomorfismo.

Ejercicio 110. (Segundo teorema de isomorfismo) Sean A un anillo, S un subanillo cualquiera de A y sea I un ideal de A. Demuestre que $S+I$ es un subanillo de A que contiene a I como ideal, $S \cap I$ es un ideal de S, y $(S+I)/I$ es isomorfo a $S/(S \cap I)$, con un isomorfismo que manda a $a+I$ en $a+(S \cap I)$, con $a \in S$.

Ejercicio 111. Explique las complicaciones para poder enunciar un "Tercer teorema de isomorfismo para anillos".

3.6. Teorema de la correspondencia.

Ejercicio 112. (Teorema de la correspondencia) Sean A un anillo, I un ideal de A y $\pi : A \longrightarrow A/I$ el mapeo natural. Considere a A como grupo abeliano con la suma y a I como un subgrupo normal, y considere la correspondencia usual a nivel de grupos. Para cada S subgrupo aditivo de A con $I \leq S$, denote su correspondiente por $S^\bullet = S/I = \pi(S) = \{sI \mid s \in S\}$. Demuestre lo siguiente:

(1) Para todo S subgrupo aditivo de A con $I \leq S$, se tiene que S es un subanillo de A si y sólo si $S^\bullet$ es un subanillo de A/I.

(2) Para todo J subgrupo aditivo de A con $I \leq J$, se tiene que J es un ideal de A si y sólo si $J^\bullet$ es un ideal de A/I. En este caso, demuestre que la asignación $\varphi : A/J \longrightarrow A^\bullet/J^\bullet$ que manda a $a+J$ en $\pi(a)+J^\bullet$ es un isomorfismo.

Capítulo 4

Dominios enteros.

4.1. Ejemplos.

Ejercicio 113. Sea A un anillo conmutativo. Demuestre que son equivalentes las siguientes propiedades:

(a) Para todos $a, b \in A$, si $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$.

(b) Para todos $a, b, b \in A$, si $ab = ac$ y $a \neq 0$, entonces $b = c$.

Un anillo conmutativo que satisfaga estas propiedades se llama un **dominio entero** (o simplemente un **dominio**).

Ejercicio 114. Para cada uno de los siguientes anillo, diga si se trata de un dominio entero o no (con las operaciones usuales de suma y producto):

(a) Los enteros

(b) Los racionales

(c) Los enteros módulo 2

(d) Los enteros módulo 4

Ejercicio 115. Sea D un dominio entero y sea §un subanillo de D. Demuestre que §es un dominio entero.

4.2. Campo de cocientes de un dominio entero.

Ejercicio 116. Sea D un domino entero. Sea $X = \{(d, c) \mid d, c \in D, c \neq 0\}$. Definimos una relación en X por medio de $(d, c)\tilde{(}b, a)$ si y sólo si $da = cb$.

Demuestre que ésta es una relación de equivalencia en X. Denotamos a la clase de (d,c) por d/c, y al conjunto de todas estas clases de equivalencia por *CC(D)*. Definimos una suma y un producto en *CC(D)* por

$$d/c + b/a = (da + bc)/ca, \qquad d/c \cdot b/a = db/ca$$

Demuestre que estas operaciones están bien definidas, y que hacen de *CC(D)* un campo, llamado el **campo de cocientes** del dominio entero D. Demuestre que existe un homomorfismo inyectivo de anillos de D en *CC(D)* que manda a d en la clase de $(d,1)$. Concluya que *CC(D)* contiene un subanillo isomorfo a D.

4.3. Divisibilidad.

Definición 117. Sea A un anillo conmutativo, y sean $a, b \in A$. Decimos que a **divide** a b, denotado $a, b \mid$, si existe $c \in A$ tal que $ac = b$. También decimos que a es un **divisor** de b, o que b es un **múltiplo** de a.

Ejercicio 118. Sea A un anillo conmutativo. Demuestre que $a, 0 \mid y\ a, a \mid p$ara cualquier $a \in A$. Demuestre que $0, a \mid s$i y sólo si $a = 0$. Demuestre que a es una unidad de A si y sólo si $ru, 1 \mid$.

Ejercicio 119. Sea A un anillo conmutativo, y sean $a, b, c \in A$. Demuestre que si a divide a b y c, entonces a divide a $bd + ce$ para cualesquiera $d, e \in A$.

Ejercicio 120. Sea A un anillo conmutativo, y sean $a, b \in A$. Decimos que a es **asociado** a b en A si existe una unidad u de A tal que $a = u\ b$. Demuestre que la relación "ser asociado a" es una relación de equivalencia en A. Si a es asociado a b en A, también decimos que a y b son **asociados** en A. Si no hay riesgo de confusión, decimos simplemente que a y b son asociados.

Ejercicio 121. Demuestre que 2 y 3 no son asociados en los enteros, pero que sí son asociados en los racionales.

Ejercicio 122. Sea D un dominio entero y sean $d, c \in D$. Demuestre que $d, c \mid y\ c, d \mid s$i y sólo si d y c son asociados en D.

4.4. Máximo común divisor.

Definición 123. Sea D un dominio entero, y sean $d, c, b \in D$. Decimos que b es un **máximo común divisor** de d y c si se cumple lo siguiente:

(a) b es un divisor de d y de c

(b) para cualquier $a \in D$, si a es un divisor de d y de c, se tiene que a es un divisor de b.

Si los elementos d, c y b pertenecen a varios dominios enteros y hay riesgo de confusión, nos referiremos a b como a un máximo común divisor de d y c en D.

Ejercicio 124. Demuestre que 2 no es un máximo común divisor de 2 y 3 en los enteros, pero que 2 sí es un máximo común divisor de 2 y 3 en los racionales.

Ejercicio 125. Sea D un dominio entero, y sean $d, c \in D$. Demuestre que cualesquiera dos máximos comunes divisores de d y c son asociados. Demuestre que cualquier asociado a un máximo común divisor de d y c es un máximo común divisor de d y c.

Ejercicio 126. Sea D un dominio entero, y sean $d, c, b, a \in D$ tales que $d = cb + a$. Demuestre que el conjunto de los máximos comunes divisores de d y c coincide con el conjunto de los máximos comunes divisores de c y a.

4.5. Elementos irreducibles y elementos primos.

Definición 127. Sea D un dominio entero, y sea d un elemento en D. Decimos que d es un elemento **irreducible** en D si cumple lo siguiente:

(a) d es diferente de 0

(b) d no es una unidad de D

(c) los únicos divisores de d son las unidades de D y los asociados de d

Definición 128. Sea D un dominio entero, y sea d un elemento de D. Decimos que d es un elemento **primo** de D si cumple lo siguiente:

(a) d es diferente de 0

(b) d no es una unidad de D

(c) para cualesquiera c, b en D, si d divide a c b, entonces d divide a c o d divide a b.

Ejercicio 129. Demuestre que todo elemento primo es irreducible.

4.6. Dominios de factorización única.

Definición 130. Sea D un dominio entero. Decimos que D es un **dominio de factorización única** si ocurre lo siguiente:

(1) Para todo elemento distinto de 0 y que no sea unidad de D, existe una factorización en elementos irreducibles.

(2) Cualesquiera dos factorizaciones del mismo elemento en irreducibles son iguales salvo asociados, es decir, existe una biyección entre el conjunto de irreducibles de una factorización y el conjunto de irreducibles de la otra factorización de tal manera que elementos correspondientes son asociados.

Ejercicio 131. Demuestre que todo campo es un dominio de factorización única.

Ejercicio 132. Demuestre que en un dominio de factorización única, un elemento es irreducible si y sólo si es primo.

Ejercicio 133. Demuestre que en un dominio de factorización única, cualesquiera dos elementos diferentes de cero tienen al menos un máximo común divisor.

4.7. Dominios de ideales principales.

Definición 134. Sea D un dominio entero. Decimos que D es un **dominio de ideales principales** si todo ideal de D es principal (es decir, está generado por un elemento).

Ejercicio 135. Demuestre que los enteros son un dominio de ideales principales.

Ejercicio 136. Demuestre que todo domino de ideales principales es un dominio de factorización única.

Definición 137. Sea A un anillo conmutativo, y sean a y b elementos de A. Decimos que un elemento c de A es **combinación lineal** de a y b si existen d y e en A tales que $c = ad + be$.

Ejercicio 138. Sea D un dominio de factorización única, y sean d y c elementos diferentes de cero en D. Demuestre que existe un máximo común divisor de d y c. Demuestre que cualquier máximo común divisor de d y c se puede escribir como combinación lineal de d y c.

4.8. Dominios euclidianos.

Definición 139. Sea D un dominio entero. Una **norma euclidiana** en D es una función $\partial : D - \{0\} \longrightarrow \mathbb{Z}$ con las siguientes propiedades:

(1) La función ∂ nunca toma valores negativos.

(2) Para cualesquiera elementos d, c de D diferentes de 0, existen q y r en D tales que $d = cq + r$, donde $r = 0$ o $\partial(r) < \partial(c)$.

Si D es un dominio entero en el que se puede definir una norma euclidiana, decimos que D es un **dominio euclidiano**.

Ejercicio 140. Demuestre que los enteros son un dominio euclidiano.

Ejercicio 141. Demuestre que todo campo es un dominio euclidiano.

Ejercicio 142. Demuestre que todo dominio euclidiano es un dominio de ideales principales (y por lo tanto también es un dominio de factorización única).

Ejercicio 143. *(Algoritmo euclidiano)* Sea D un dominio euclidiano con norma euclidiana ∂, y sean d, c elementos diferentes de cero en D. Demuestre que si c divide a d, entonces c es un máximo común divisor de d y c. Demuestre que si c no divide a d, y $d = cq + r$ con $r \neq 0$ y $\partial(r) < \partial(c)$, entonces el conjunto de máximos comunes divisores de d y c coincide con el conjunto de máximos comunes divisores de c y r. Utilice este argumento para construir un algoritmo que calcule un máximo común divisor de d y c.

Ejercicio 144. Calcule un máximo común divisor de 314880 y 97102350 en los enteros.

Capítulo 5

Anillos de polinomios.

5.1. Definición de los polinomios con coeficientes en un anillo conmutativo.

Definición 145. Sea A un anillo conmutativo. Un **polinomio** con coeficientes en A es una sucesión infinita $p = (p_0, p_1, p_2, \dots)$ que cumple lo siguiente:

(1) $p_i \in A$ para toda $i = 0, 1, 2, \dots$

(2) Existe un entero N tal que $p_n = 0$ para toda $n \geq N$.

Notación 146. Sea A un anillo conmutativo y sea $p = (p_i)_{i=0}^{\infty}$ un polinomio con coeficientes en A. Usualmente denotamos al polinomio p como $p(x)$, y llamamos a la "x" una "indeterminada". Además, si $p_i = 0$ para toda $i = 0, 1, \dots,$ llamamos a p el **polinomio cero**, y lo denotamos 0. Si $p \neq 0$, entonces existe un único entero no negativo n tal que $p_n \neq 0$ y $p_i = 0$ para toda $i > n$. A tal n la llamamos el **grado** del polinomio $p(x)$, y usualmente en lugar de escribir $p = (p_i)_{i=0}^{\infty}$ escribimos $p(x) = p_0 + p_1 x + p_2 x^2 + p_3 x^3 + \cdots + p_n x^n$. A los elementos p_i los llamamos los **coeficientes** del polinomio $p(x)$. A las expresiones $p_i x^i$ las llamamos los **términos** del polinomio p (x). Si algún p_i es igual a 1, usualmente escribimos x^i en lugar de $1x^i$. Si algún p_i es igual a 0, usualmente omitimos el término $0x^i$ en la descripción del polinomio $p(x)$. Al elemento p_n lo llamamos el **coeficiente principal** del polinomio $p(x)$, y al elemento p_0 lo llamamos el **término constante** del polinomio $p(x)$. Si el coeficiente principal de $p(x)$ es 1, decimos que $p(x)$ es un polinomio **mónico**. Si el grado de $p(x)$ es cero, decimos que $p(x)$ es un polinomio **constante**. El polinomio cero también es un polinomio constante, pero no se le asigna un

grado. Los polinomios constantes usualmente se identifican con los elementos del anillo conmutativo A. Al anillo de polinomios con coeficientes en A se le denota como $A[x]$.

Definición 147. Sean $p_0+p_1x+\cdots+p_nx^n$y $q_0+q_1x+\cdots+q_mx^m$polinomios con coeficientes en un anillo conmutativo A. Definimos su suma $p_0+p_1x+\cdots+p_nx^n+q_0+q_1x+\cdots+q_mx^m$como el polinomio $(p_i+q_i)_{i=0}^{\infty}$, y su producto como el polinomio cuya entrada i-ésima es $\sum_{j=0}^{i} p_j q_{i-j}$.

Ejercicio 148. Sume los polinomios $1-2x+3x$ y $2-x$ en $\mathbb{Z}[x]$. Ahora súmelos como si fueran elementos de $\mathbb{F}_2[x]$. Multiplique los polinomios $1-2x+3x$ y $2-x$ en $\mathbb{Z}[x]$. Ahora multiplíquelos como si fueran elementos de $\mathbb{F}_2[x]$.

Ejercicio 149. Demuestre la suma de polinomios es asociativa, conmutativa, y que tiene al polinomio constante 0 como elemento neutro. Demuestre además que tiene inversos.

Ejercicio 150. Demuestre el producto de polinomios es asociativo, conmutativo, y que tiene al polinomio constante 1 como elemento neutro. Demuestre además que los únicos polinomios que tienen inverso multiplicativo son los polinomios constantes representados por unidades en el anillo A.

Ejercicio 151. (Propiedad universal de los anillos de polinomios.) Sean A y B anillos conmutativos, sea $\varphi : A \longrightarrow B$ un homomorfismo de anillos, y sea $a \in B$. Demuestre que existe un único homomorfismo de anillos de $A[x]$ en B que manda a los polinomios constantes segun f, y que manda al polinomio x en a.

Ejercicio 152. Sea D un anillo conmutativo, sea A un anillo conmutativo que contiene a D, y sea $a \in A$. La **función evaluación** en a de $D[x]$ a A es el homomorfismo de anillos $\varphi_a : D[x] \longrightarrow A$ definido en los escalares como la inclusión de D en A, y que manda a x en a. Denotamos usualmente a la imagen del polinomio p bajo la función evaluación en a por $p\ (a)$. Si $p\ (a)=0$ decimos que a es una **raíz** del polinomio p.

5.2. Anillos de polinomios sobre dominios enteros.

Ejercicio 153. Sea D un anillo conmutativo. Demuestre que D es un dominio entero si y sólo si D [x] es un dominio entero.

Ejercicio 154. Sean $p_0 + p_1x + \cdots + p_nx^n$y $q_0 + q_1x + \cdots + q_mx^m$polinomios distintos de cero con coeficientes en un dominio entero D. Demuestre que el grado del producto p q es la suma de sus grados. Muestre con un ejemplo que este resultado no es cierto si se reemplaza el dominio entero D con un anillo conmutativo.

Ejercicio 155. Demuestre que el ideal de $\mathbb{Z}[x]$ generado por x y 2 no es un ideal principal. Concluya que aunque D sea un dominio de ideales principales, D [x] no necesariamente es dominio de ideales principales.

Ejercicio 156. Sea D un dominio entero y sea p un polinomio con coeficientes en D. Demuestre que el número de factores en cualquier descomposición de p como producto de polinomios irreducibles (no necesariamente distintos) es menor o igual al grado de p. Concluya que el número de raíces de p (contando raíces múltiples tantas veces como su multiplicidad) es menor o igual a su grado.

5.3. Anillos de polinomios con coeficientes en un campo.

Ejercicio 157. Sea k un campo y sea I un ideal no cero en $k[x]$. Sea p un polinomio en I de grado mínimo. Demuestre que el ideal generado por p es I. Concluya que $k[x]$ es un dominio de ideales principales, y por lo tanto $k[x]$ también es un dominio de factorización única. Concluya que los elementos irreducibles de $k[x]$ coinciden con los elementos primos en $k[x]$, y que dos elementos no cero cualesquiera siempre tienen máximos comunes divisores en $k[x]$.

Notación 158. Por convención, en $k[x]$ se pide que el máximo común divisor de dos polinomios sea un polinomio mónico, y por lo tanto, es único.

Ejercicio 159. Demuestre que si k es un campo, entonces $k[x]$ es un dominio euclidiano con norma euclidiana dada por el grado.

Ejercicio 160. Sea k un campo, y sea $p(x)$ un polinomio en $k[x]$. Demuestre que el ideal principal $< p(x) >$ es maximal en $k[x]$ si y sólo si $p(x)$ es un polinomio irreducible en $k[x]$.

Ejercicio 161. Sea k un campo, y sean $f(x)$, $g(x)$ y $h(x)$ polinomios en $k[x]$ tales que el máximo común divisor de $f(x)$ y $g(x)$ en $k[x]$ es 1. Demuestre que si $f(x)$ divide a $g(x)h(x)$, entonces $f(x)$ divide a $h(x)$.

Ejercicio 162. Sea k un campo, y sean $f(x)$ y $g(x)$ polinomios en $k[x]$. Sea F un campo que contiene a k. Demuestre que el máximo común divisor de $f(x)$ y $g(x)$ en $k[x]$ es también el máximo común divisor de $f(x)$ y $g(x)$ en $F[x]$.

5.4. Derivadas y raíces múltiples.

Definición 163. Sea $a_0 + a_1x + \cdots + a_nx^n$ un polinomio. Su **derivada** es el polinomio $a_1 + 2a_2x + 3a_3x^2 \cdots + na_nx^{n-1}$. La derivada del polinomio $p(x)$ se denota $p'(x)$.

Ejercicio 164. Encuentre un polinomio no constante en $F_2[x]$ cuya derivada sea cero.

Ejercicio 165. Sean p y q polinomios. Demuestre que $(p+q)' = p'+q'$, y que $(pq)' = p'q+pq'$. Demuestre que para todo natural n se tiene $(p^n)' = np^{n-1}p'$.

Ejercicio 166. Sean k un campo de característica $p > 0$, y $f \in k[x]$. Demuestre que $f' = 0$ si y sólo si todos los términos en f involucran potencias de x^p.

Ejercicio 167. Sean k un campo de característica 0, y $f \in k[x]$. Demuestre que $f' = 0$ si y sólo f es un polinomio constante.

Definición 168. Sean k un campo, $f \in k[x]$ y $a \in k$. Decimos que a es una **raíz múltiple** de f si existe un entero $n > 1$ tal que $(x - a)^n$ divide a f.

Ejercicio 169. Sean k un campo, $f \in k[x]$ y $a \in k$. Demuestre que a es una raíz múltiple de f si y sólo si $f(a) = 0 = f'(a)$.

Ejercicio 170. Sean k un campo de característica $p > 0$, $a, b \in k$. Demuestre que $(a + b)^p = a^p + b^p$. Demuestre también que $(x - a)^p = x^p - a^p$.

5.5. Polinomios irreducibles.

Ejercicio 171. Sea $f \in k[x]$ un polinomio de grado 2 o 3. Demuestre que f es irreducible en $k[x]$ si y sólo si f no tiene raíces en k. Muestre con un ejemplo que este criterio falla en grado 4.

Ejercicio 172. Demuestre que el polinomio $a_0 + a_1x + a_2x^2 + \cdots + a_nx$ es irreducible en $k[x]$ si y sólo si el polinomio $a_n + a_{n-1}x + a_{n-2}x^2 + \cdots + a_ox^n$ es irreducible en $k[x]$, donde $a_0 \neq 0 \neq a_n$.

Ejercicio 173. Sea $f : R \longrightarrow S$ un mapeo de anillos conmutativos, y sea $\varphi : R[x] \longrightarrow S[x]$ el mapeo inducido por f que manda a x en x. Demuestre que si R y S son dominios enteros y $p(x) \in R[x]$ es tal que $\varphi(p(x))$ es irreducible en $S[x]$ y del mismo grado que $p(x)$, entonces $p(x)$ es irreducible en $R[x]$.

Ejercicio 174. Demuestre que el polinomio x^3+2x+1 es irreducible en $F_3[3]$, donde F_3 es el campo $Z/3Z$. Concluya que el polinomio $x^3 + 6x^2 + 5x + 25$ es irreducible en $Z[x]$

Definición 175. Un polinomio $a_0 + a_1x + \cdots + a_nx^n$ en $Z[x]$ se llama **primitivo** si el máximo común divisor de sus coeficientes es 1.

Ejercicio 176. (Lema de Gauss) Demuestre que el producto de dos polinomios primitivos es primitivo.

Teorema y definición 177. *Demuestre que todo polinomio $f(x) \in Q[x]$ distinto de cero tiene una factorización única $f(x) = c(x)f^*(x)$ donde $c(f)$ es un racional positivo y $f^*(x) \in Z[x]$ es un polinomio primitivo. A $c(f)$ se le llama el* ***contenido*** *del polinomio $f(x)$.*

Ejercicio 178. Sean $f, g, h \in Q[x]$ tales que $f(x) = g(x)h(x)$. Demuestre que $c(f) = c(g)c(h)$ y $f^*(x) = g^*(x)h^*(x)$. Concluya que si $f(x) \in Z[x]$, entonces f es irreducible en $Z[x]$ si y sólo si $f(x)$ es irreducible en $Q[x]$.

Ejercicio 179. (Criterio de Eisenstein)Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$. Si existe un primo p que divide a a_i para toda $i < n$, pero tal que p no divide a a_n y p^2 no divide a a_0, entonces $f(x)$ es irreducible sobre Q.

Ejercicio 180. Demuestre que $x^5 - 4x + 2$ es irreducible sobre Q.

Ejercicio 181. Sea a un entero libre de cuadrados que no sea unidad. Demuestre que el polinomio $x^n - a$ es irreducible en $Q[x]$ para toda $n > 1$.

Definición 182. Sea p un número primo. El p-ésimo polinomio **ciclotómico** es

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Ejercicio 183. Demuestre que $\Phi_p(x)$ es irreducible en $Q[x]$ para todo primo p.

Capítulo 6

Campos.

6.1. Extensiones algebraicas.

Definición 184. Sean K y F campos. Decimos que F es una **extensión** de K (o equivalentemente, que K es un **subcampo** de F) si K está contenido en F y K hereda la suma y multiplicación de F.

Teorema y definición 185. *Sea F una extensión del campo k. Demuestre que F es un espacio vectorial sobre K. A la dimensión de F sobre K se le llama el **grado** de F sobre K, y se denota $[F : K]$. Decimos que F es una **extensión finita** de K si el grado de F sobre K es finito.*

Ejercicio 186. Demuestre que $\mathbb{C}$ tiene grado 2 sobre $\mathbb{R}$, y que $\mathbb{R}$ tiene grado infinito sobre $\mathbb{Q}$.

Ejercicio 187. Sea F una extensión del campo ky sea H una extensión de F. Demuestre que H es una extensión de K y que $[H : K] = [H.F][F : K]$.

Definición 188. Sea F una extensión del campo k, y sea $a \in F$. Decimos que a es **algebraico** sobre K si existe $0 \neq f(x) \in K[x]$ tal que $f(a) = 0$. Si a no es algebraico sobre K, decimos que a es **trascendente** sobre K. Si todo elemento de F es algebraico sobre K, decimos que F es una **extensión algebraica** de K.

Ejercicio 189. Sea F una extensión del campo k. Demuestre que si F es una extensión finita de K, entonces F es una extensión algebraica de K.

Teorema y definición 190. *Sea F una extensión del campo k y sea $a \in F$ tal que a es algebraico sobre K. Demuestre que existe un único polinomio mónico en $K[x]$ de grado mínimo que tiene a a como raíz. Dicho polinomio se llama el* ***polinomio mínimo*** *de a sobre K, y se denota $irr_K(a)$. Demuestre que para todo $f(x) \in K[x]$ se tiene que $f(a) = 0$ si y sólo si el polinomio mínimo de a sobre K divide a $f(x)$ en $K[x]$.*

6.2. Generadores de una extensión.

Teorema y definición 191. *Sea F una extensión del campo k, y sea $a \in F$. Demuestre que existe un único subcampo H de F que contiene a K y a a y que está contenido en cualquier otro subcampo de F que contenga a K y a a. A dicho subcampo se le llama el subcampo de F generado por K y a, o la extensión de K adjuntando a, y se denota $K(a)$. Decimos que F es una* ***extensión simple*** *de K si existe $a \in F$ tal que $F = K(a)$.*

Ejercicio 192. Sea F una extensión del campo k y sea $a \in F$ algebraico sobre K. Demuestre que $K(a)$ es isomorfo al anillo cociente $K[x]/ < irr_K(a) >$. Concluya que si a y b son elementos en sendas extensiones de K tales que a y b tienen el mismo polinomio irreducible sobre K, entonces $K(a)$ es isomorfo a $K(b)$.

Ejercicio 193. Sea K un campo y sea $p(x) \in K[x]$ un polinomio irreducible. Demuestre que $K[x]/ < p(x) >$ es una extensión de K, y que la clase del polinomio x en dicha extensión es una raíz de $p(x)$. Concluya que dado cualquier polinomio no constante $f(x) \in K[x]$, existe una extensión de K en donde $f(x)$ tiene al menos una raíz.

Teorema y definición 194. *Sea F una extensión del campo k, y sean $a_1, \ldots, a_n \in F$. Demuestre que existe un único subcampo H de F que contiene a K y a $a_1, \ldots, a_n$ y que está contenido en cualquier otro subcampo de F que contenga a K y a $a_1, \ldots, a_n$. A dicho subcampo se le llama el subcampo de F generado por K y $a_1, \ldots, a_n$, o la extensión de K adjuntando $a_1, \ldots, a_n$, y se denota $K(a_1, \ldots, a_n)$*

6.3. Campos de descomposición.

Definición 195. Sea F una extensión del campo k y sea $f(x) \in K[x]$ un polinomio no constante. Decimos que $f(x)$ **tiene todas sus raíces** en F,

o que $f(x)$ se **descompone** en F, o que $f(x)$ se **factoriza totalmente** en F, si $f(x)$ se factoriza como producto de polinomios de grado uno en $F(x)$. Decimos que F es un **campo de descomposición** de $f(x)$ si se cumple lo siguiente:

(1) $f(x)$ se descompone en F;
(2) $f(x)$ no se descompone en ningún subcampo propio de F.

Ejercicio 196. Sea K un campo y sea $f(x) \in K[x]$ un polinomio no constante. Demuestre que existe un campo de descomposición de $f(x)$. Demuestre que dos campos de descomposición de $f(x)$ son isomorfos.

Ejercicio 197. Sea $\mathbb{F}_p$ el campo con p elementos, y sea n un entero positivo. Demuestre que el campo de descomposición del polinomio $x^{p^n} - x \in k[x]$ es un campo con p^n elementos. Inversamente, demuestre que si F es un campo con p^n elementos, entonces F es campo de descomposición de dicho polinomio. Concluya que dos campos con p^n elementos son isomorfos.

Ejercicio 198. Sea k un campo finito de característica p. Demuestre que k tiene un subcamp isomorfo a $\mathbb{F}_p$, y que k tiene p^n elementos para algún entero positivo n. Concluya que dos campos finitos son isomorfos si y sólo si tienen el mismo número de elementos.

6.4. Cerradura algebraica.

Definición 199. Sea k un campo. Decimos que k es **algebraicamente cerrado** si todo polinomio no constante en $k[x]$ tiene todas sus raíces en k.

Ejercicio 200. Sea k un campo. Demuestre que k es algebraicamente cerrado si y sólo si todo polinomio no constante en $k[x]$ tiene al menos una raíz en k.

Ejercicio 201. Demuestre que todo campo algebraicamente cerrado es infinito.

Definición 202. Sea k un campo, y sea F una extensión algebraica de k. Decimos que F es una **cerradura algebraica** de k si F es algebraicamente cerrado.

Ejercicio 203. Sea k un campo y F una extensión algebraica de k. Sea $W = k[x] \times \mathbb{Z}$. Demuestre que la cardinalidad de F es menor o igual a la cardinalidad de W. Sea C la familia de extensiones algebraicas de k cuyos

conjuntos subyacentes son subconjuntos de W. Demuestre que la extensión de campos es un orden parcial en C. Demuestre que C es una familia inductiva, y que cualquier elemento maximal de C es una cerradura algebraica de k.

Ejercicio 204. Sea k un campo y sea F una cerradura algebraica de k. Demuestre que si E es un campo intermedio $k \leq E \leq F$, entonces E es algebraicamente cerrado si y sólo si $E = F$.

Ejercicio 205. Sea k un campo, y sean F y H dos cerraduras algebraicas de k. Sea C la familia de (E, f) tales que E es un subcampo de F y $f : E \longrightarrow H$ es un homomorfismo inyectivo de anillos. Defina un orden parcial en C por $(E, f) \leq (E', f')$ si y sólo si $E \leq E'$ y f' es una extensión de f. Demuestre que C es una familia inductiva, y que si (E, f) es un elemento maximal en C entonces $E = F$. Concluya que F y H son isomorfos, y que por tanto la cerradura algebraica de un campo k es única hasta isomorfismo. Dicha cerradura algebraica se denota $\bar{k}$.

6.5. Extensiones separables.

Definición 206. Sea k un campo y sea $f(x) \in k[x]$. Decimos que $f(x)$ es un polinomio **separable** sobre k si ninguno de sus factores irreducibles en $k[x]$ tiene raíces múltiples.

Ejercicio 207. Sea k un campo y sea $f(x) \in k[x]$ un polinomio irreducible. Demuestre que $f(x)$ es separable sobre k si y sólo si $f(x)$ no tiene raíces múltiples.

Ejercicio 208. Sea k un campo y sea $f(x) \in k[x]$ un polinomio. Demuestre que si $f(x)$ no tiene raíces múltiples entonces $f(x)$ es separable sobre k. Muestre con un ejemplo que el inverso no es cierto.

Ejercicio 209. Sea k un campo y sea $f(x) \in k[x]$ un polinomio. Demuestre que $f(x)$ es separable sobre k si y sólo si para cualesquiera polinomios irreducibles $p(x)$ y $q(x)$ no asociados que dividan a $f(x)$ en $k[x]$ se tiene que p y q son primos relativos en $k[x]$.

Ejercicio 210. Sea k un campo y F una extensión de k. Sea $f(x) \in k[x]$. Demuestre que $f(x)$ es separable sobre k si y sólo si $f(x)$ es separable sobre F.

Definición 211. Sea k un campo y sea F una extensión de k. Sea $a \in F$. Decimos que a es un **elemento separable** sobre k si a es trascendente sobre k o si su polinomio mínimo sobre k es separable sobre k. Decimos que F es una **extensión separable** de k si todo elemento en F es separable sobre k.

Ejercicio 212. Sea k un campo de característica p, y sea $f(x) = x^p - a$ para algún $a \in k$. Demuestre que $f(x)$ tiene una única raíz de multiplicidad p en su campo de descomposición. Concluya que dos factores irreducibles cualesquiera de $f(x)$ tienen que ser asociados. Demuestre que o bien $f(x)$ es irreducible en $k[x]$, o se factoriza como $(x - b)^p$ para algún $b \in k$.

Ejercicio 213. Sea $k = \mathbb{F}_p(t)$, y sea $f(x) \in k[x]$ el polinomio $f(x) = x^p - t$. Demuestre que $f(x)$ es irreducible sobre k, y que el campo de descomposición de $f(x)$ es una extensión no separable de k.

Capítulo 7

Teoría de Galois.

7.1. Grupo de Galois.

Definición 214. Sea F una extensión del campo k, y sea σ un automorfismo del campo F. Decimos que σ **fija** al subcampo k, o que k queda fijo bajo la acción de σ, si $\sigma(a) = a$ para toda $a \in k$. Al conjunto de todos los automorfismos de F que fijan a k lo denotamos $Gal(F, k)$, y lo llamamos el **grupo de Galois** de F sobre k.

Ejercicio 215. Demuestre que $Gal(F, k)$ es un grupo con la composición de funciones.

Ejercicio 216. Calcule $Gal(\mathbb{C}, \mathbb{R})$.

Ejercicio 217. Calcule $Gal(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$, $Gal(\mathbb{Q}(\sqrt{3}), \mathbb{Q})$ y $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$.

Ejercicio 218. Calcule $Gal(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$,

Definición 219. Sea F una extensión del campo k, y sea H un subgrupo de $Gal(F, k)$. El **campo fijo** de H, (o también llamado el **subcampo de H-invariantes** de F) denotado F^H (o también denotado $Inv(H)$), es el conjunto $\{a \in F \mid \sigma(a) = a \forall \sigma \in H\}$.

Ejercicio 220. Sea F una extensión del campo k, y sea H un subgrupo de $Gal(F, k)$. Demuestre que F^H es un subcampo de F.

Ejercicio 221. Sean k y k' campos y sea $\sigma : k \longrightarrow k'$ un isomorfismo de campos. Sea $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$ un polinomio irreducible,

y sea $q(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$ el correspondiente polinomio irreducible en $k'[x]$. Sean β una raíz de $p(x)$ y β' una raíz de $q(x)$. Demuestre que existe un único isomorfismo $\tau : k(\beta) \longrightarrow k'(\beta')$ que extiende a σ y tal que $\tau(\beta) = \beta'$.

Ejercicio 222. Sea $k = \mathbb{Q}$, y sean $f(x) = x^3 - 5$, $g(x) = x^2 - 7$ y $h(x) = f(x)g(x)$ polinomios en $\mathbb{Q}[x]$. Sean F el campo de descomposición de $f(x)$ sobre $\mathbb{Q}$, y H el campo de descomposición de $g(x)$ sobre F. Demuestre que H es el campo de descomposición de $h(x)$ sobre $\mathbb{Q}$. Calcule el orden de $Gal(F, k)$, $Gal(H, F)$ y $Gal(H, k)$. Calcule el grado $[F : k]$, $[H : F]$ y $[H : k]$.

Ejercicio 223. (Actividad) Sean k un campo, $f(x) \in k[x]$ y F el campo de descomposición de $f(x)$. Demuestre que el orden de $Gal(F, k)$ es menor o igual al grado de F sobre k. Demuestre que se tiene igualdad si $f(x)$ es separable.

Ejercicio 224. (Actividad) Sea F un campo y G un subgrupo del grupo de automorfismos de F. Sea k el campo fijo de G. Demuestre que $[F : k] \leq |G|$.

7.2. Extensiones normales.

Definición 225. Sea F una extensión del campo k. Decimos que F es una extensión **normal** de k si todo polinomio irreducible en $k[x]$ que tenga una raíz en F se factoriza totalmente en F.

Ejercicio 226. Sea F una extensión algebraica de k. Demuestre que F es una extensión normal de k si y sólo si para todo $a \in F$, F tiene todas las raíces del polinomio mínimo de a sobre k.

Ejercicio 227. Demuestre que $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión normal de $\mathbb{Q}$.

Ejercicio 228. Sea F una extensión del campo k. Demuestre que las tres condiciones siguientes son equivalentes:

(a) F es el campo de descomposición de un polinomio separable $f(x) \in k[x]$.

(b) k es el campo invariante de un grupo finito de automorfismos G de F.

(c) F es de grado finito, normal y separable sobre k.

Más aún, si k y F son como en (a) y $G = Gal(F, k)$, entonces $k = Inv(G)$; si G y k son como en (b), entonces $G = Gal(F, k)$.

7.3. Teorema fundamental de la teoría de Galois.

Ejercicio 229. (Teorema Fundamental de la Teoría de Galois) Sea F una extensión normal, separable y de dimensión finita sobre k. Sea $G = Gal(F, k)$, y sea Λ la familia de los subgrupos de G. Sea Σ la familia de los campos intermedios entre k y F. Las funciones $H \mapsto Inv(H)$ y $E \mapsto Gal(F, E)$ con $H \in \Lambda$ y $E \in \Sigma$ son inversas, y por tanto son biyecciones entre Λ y Σ. Más aún, tenemos las siguientes propiedades:

(1) $H_2 \leq H_1$ si y sólo si $Inv(H_1) \leq Inv(H_2)$

(2) $|H| = [F : Inv(H)]$, $[G : H] = [Inv(H) : k]$

(3) H es normal en G si y sólo si $Inv(H)$ es normal sobre k. En este caso, $Gal(Inv(H), k) = G/H$.

Ejercicio 230. Calcule el grupo de Galois de $x^3 - 2$ sobre $\mathbb{Q}$. Calcule los subcampos del campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$, y diga cuáles son extensiones normales de $\mathbb{Q}$.

Ejercicio 231. Calcule el grupo de Galois de $(x^2-3)(x^2-5)$ sobre $\mathbb{Q}$. Calcule los subcampos del campo de descomposición de $(x^2 - 3)(x^2 - 5)$ sobre $\mathbb{Q}$, y diga cuáles son extensiones normales de $\mathbb{Q}$.

7.4. Extensiones cíclicas y abelianas.

Definición 232. Sea F una extensión del campo k. Decimos que F es una extensión **cíclica** de k si $Gal(F, k)$ es un grupo cíclico. Decimos que F es una extensión **abeliana** de k si $Gal(F, k)$ es un grupo abeliano.

Ejercicio 233. Sea F una extensión del campo k. Demuestre que si F es una extensión de grado p normal y separable de k entonces F es una extensión cíclica de k.

Definición 234. Sea n un entero positivo y k un campo arbitrario. El **campo ciclotómico** de orden n sobre k es el campo de descomposición de $x^n - 1$ sobre k.

Ejercicio 235. Sea F el campo ciclotómico de orden p sobre $\mathbb{Q}$ con p un primo. Demuestre que F es el campo de descomposición del polinomio ciclotómico $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Ejercicio 236. Sea F una extensión del campo $k$con k un campo de característica cero y F el campo ciclotómico de orden n sobre k. Demuestre que F es una extensión abeliana de k.

Ejercicio 237. Sea F una extensión del campo k. Demuestre que si k contiene n raíces n-ésimas distintas de la unidad, entonces el grupo de Galois de $x^n - a$ sobre k es cíclico y su orden divide a n.

Ejercicio 238. Sea p un primo y suponga que k contiene p raíces p-ésimas distintas de la unidad. Sea F una extensión cíclica de k de dimensión p. Demuestre que $F = k(d)$ donde $d^p \in k$.

7.5. Campos finitos.

Ejercicio 239. Sea k un campo finito y sea p la característica de k. Demuestre que existe un entero positivo n tal que k tiene p^n elementos. Demuestre que dos campos finitos son isomorfos si y sólo si tienen el mismo número de elementos.

Ejercicio 240. Sea k el campo con p elementos y sea F el campo con p^n elementos. Demuestre que F es una extensión cíclica de k, y que $Gal(F, k)$ está generado por el automorfismo $\tau : F \longrightarrow F$ dado por $\tau(a) = a^p$. (A τ se le conoce como el **automorfismo de Frobenius** de F)

Ejercicio 241. Sea k un campo con $q = p^n$ elementos (p primo), y sea F una extensión de k de grado n. Demuestre que F es una extensión cíclica de k y que su grupo de Galois está generado por el automorfismo τ dado por $\tau(a) = a^q$.

Ejercicio 242. Sean k un campo con $q = p^n$ elementos (p primo), y sea F una extensión de k de grado n. Demuestre que si E es un subcampo de F que contiene a k, entonces $|E| = q^m$ donde m divide a n. Inversamente, demuestre que si m es un entero positivo que divide a n, entonces existe un único campo intermedio E entre F y k con $|E| = q^m$.

7.6. Teorema del elemento primitivo.

Definición 243. Sea F un campo y sea E una extensión de F. Decimos que E es una **extensión simple** de F si existe $a \in E$ tal que $E = F(a)$. En este caso, decimos que a es un **elemento primitivo**.

Ejercicio 244. Sean F un campo finito y E una extensión finita de F. Demuestre que E es una extensión simple de F.

Ejercicio 245. (Teorema de Steinitz)Sea E una extensión finita de un campo F. Entonces E tiene un elemento primitivo sobre F si y sólo si hay únicamente un número finito de campos intermedios entre E y F.

Ejercicio 246. (Teorema del elemento primitivo) Toda extensión separable de dimensión finita contiene un elemento primitivo.

7.7. Construcciones con regla y compás.

Definición 247. Sean $z_1, \ldots, z_n \in \mathbb{C}$ y sea $k = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$. Sea $z \in \mathbb{C}$. Decimos que z es **construible con regla y compás** a partir de $z_1, \ldots, z_n$ si z está contenido en un subcampo de $\mathbb{C}$ de la forma $k(u_1, \ldots, u_r)$ donde $u_1^2 \in k$ y para toda $i = 2, \ldots, r$ se tiene que $u_i^2 \in k(u_1, \ldots, u_{i-1})$. En este caso, si $k = \mathbb{Q}$, decimos simplemente que z es construible con regla y compás.

Ejercicio 248. Sea $k = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$. Demuestre que si z es construible con regla y compás a partir de $z_1, \ldots . z_n$, entonces z es algebraico sobre k y de grado 2^m para algún entero positivo m. Concluya que todo número complejo construible con regla y compás es algebraico sobre $\mathbb{Q}$ de orden una potencia de 2.

Ejercicio 249. (Duplicación del cubo.) Demuestre que no se puede construir el lado de un cubo de volumen 2.

Ejercicio 250. Usando la identidad $\cos(3t) = 4\cos^3(t) - 3\cos(t)$, demuestre que $\cos(20^\circ)$ es raíz del polinomio $4x^3 - 3x - 1/2$. Demuestre que dicho polinomio es irreducible en $\mathbb{Q}[x]$ demostrando primero que $x^3 - 3x - 1$ es irreducible sobre $\mathbb{Q}$.

Ejercicio 251. (Trisección del ángulo.)Demuestre que el ángulo de 60° no se puede trisectar.

Ejercicio 252. (Cuadratura del círculo.) Usando que π es trascendente sobre $\mathbb{Q}$, demuestre que no es posible construir un cuadrado cuya área sea igual al área de un círculo de radio 1 (es decir, área π).

7.8. Solubilidad por radicales.

Definición 253. Sea F un campo. Una **torre de campos** sobre F es una cadena de campos

$$F = F_1 < F_2 < \ldots < F_{r+1}.$$

Si además se cumple que $F_{i+1} = F_i(d_i)$ con $d_i^{n_i} \in F_i$ (n_i enteros positivos) para toda $i = 1, \ldots, r$, decimos que ésta es una **torre de raíces** sobre F. Sea $f(x) \in F[x]$ un polinomio mónico de grado positivo. Decimos que la ecuación $f(x) = 0$ es **soluble por radicales** sobre F si existe una torre de raíces como la de arriba en la que F_{r+1} contiene un campo de descomposición de $f(x)$ sobre F.

Definición 254. Sea k un campo y sea $f(x) \in k[x]$ un polinomio no constante. El grupo de Galois de $f(x)$ sobre k es el grupo de Galois de un campo de descomposición de $f(x)$ sobre k.

Ejercicio 255. Sea k un campo y sea $f(x) \in k[x]$ un polinomio de grado positivo n. Demuestre que el grupo de Galois de $f(x)$ es isomorfo a un subgrupo de S_n.

Ejercicio 256. Sea F una extensión del campo k, y sea $f(x) \in k[x]$. Entonces el grupo de Galois de $f(x)$ sobre F es isomorfo a un subgrupo del grupo de Galois de $f(x)$ sobre F.

Ejercicio 257. Sea $E = F(a_1, \ldots, a_n)$ una extensión finita de F. Sea $f_i(x)$ el polinomio mínimo de a_i sobre F y sea $f(x)$ el producto de los $f_i(x)$. Sea K un campo de descomposición de $f(x)$ sobre E. Demuestre que K también es campo de descomposición de $f(x)$ sobre F. Suponga que $f(x)$ es separable sobre F. Demuestre que cualquier extensión normal de E contiene un subcampo isomorfo a K. El campo K se llama la **cerradura normal** de E sobre F. Sea $\eta \in Gal(K, F)$. Un subcampo de K se la forma $\eta(E)$ se llama un **conjugado** del campo E sobre F. Sea K' el subcampo de K generado por todos los conjugados de E. Demuestre que $Gal(K, F)$ manda a K' en sí mismo, y por lo tanto determina un grupo finito de automorfismos G' de K' cuyo campo fijo es F. Concluya que K' es normal sobre F, y que $K' = K$.

Ejercicio 258. Sea E una extensión de F, y suponga que existe una torre de raíces $F = F_1 < \ldots < F_{r+1} = E$ con $F_{i+1} = F_i(d_i)$, $d_i^{n_i} \in F_i$, y suponga además que E está generado sobre F por un conjunto finito de elementos

cuyos polinomios mínimos son separables. Entonces la cerradura normal K de E sobre F tiene una torre de raíces sobre F cuyos enteros coinciden con los n_i.

Ejercicio 259. (Criterio de Galois para solubilidad de una ecuación por radicales)(ACTIVIDAD) Sea k un campo de característica 0, y sea $f(x) \in k[x]$ un polinomio no constante. Demuestre que la ecuación polinomial $f(x) = 0$ es soluble por radicales sobre k si y sólo si el grupo de Galois de $f(x)$ sobre k es soluble.

Ejercicio 260. Sea $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Demuestre que $f(x)$ es irreducible en $\mathbb{Q}[x]$, y que $f(x)$ tiene tres raíces reales y dos raíces complejas. Sea G el grupo de Galois de $f(x)$. Demuestre que G es (isomorfo a) un subgrupo de S_5. Demuestre que G contiene un ciclo de longitud 5 y una transposición. Concluya que G es isomorfo a S_5.

Ejercicio 261. (Teorema de Abel-Ruffini) Existe un polinomio de grado 5 en $\mathbb{Q}[x]$ que no es soluble por radicales.

Índice alfabético

raíz múltiple, **168**

abeliana, **232**
algebraicamente cerrado, **199**
algebraico, **188**
anillo, **4**
anillo cero, **17**
anillo cociente, **23**, **75**
anillo con división, **12**
anillo con uno, **4**
anillo de endomorfismos, **29**
anillo de funciones, **26**
anillo de los enteros módulo n, **24**
aplicación cociente, **90**
asociado, **120**
asociados, **120**
automorfismo, **88**
automorfismo de Frobenius, **240**

cíclica, **232**
campo, **13**
campo ciclotómico, **234**
campo de cocientes, **116**
campo de descomposición, **195**
campo fijo, **219**
cero, **4**
cerradura algebraica, **202**
cerradura normal, **257**
ciclotómico, **182**
coeficiente principal, **146**
coeficientes, **146**
combinación lineal, **137**
conjugado, **257**
conmutativo, **8**
constante, **146**
construible con regla y comp
contenido, **177**
coordenada a coordenada, **21**
cuerpo, **13**

derivada, **163**
descompone, **195**
divide, **117**
divisor, **117**
dominio, **10**, **113**
dominio de factorización únic
dominio de ideales principale
dominio entero, **10**, **113**
dominio euclidiano, **139**

elemento identidad, **3**
elemento primitivo, **243**
elemento separable, **211**
endomorfismo, **88**
enteros Gaussianos, **19**
extensión, **184**
extensión algebraica, **188**
extensión finita, **185**
extensión separable, **211**
extensión simple, **191**, **243**

factoriza totalmente, **195**
fija, **214**
función evaluación, **152**
función identidad, **97**

grado, **146**, **185**
grupo de automorfismos, **101**
grupo de Galois, **214**
grupo de unidades, **41**

homomorfismo de anillos, **88**
homomorfismo de anillos con uno, **88**

ideal, **56**
ideal bilateral, **56**
ideal cero, **59**
ideal derecho, **55**
ideal generado, **69**
ideal izquierdo, **54**
ideal primo, **77**
ideal producto, **72**
ideal total, **57**
imagen, **103**
interno, **98**
inverso, **44**
inverso multiplicativo, **44**
irreducible, **127**
isomorfismo, **88**
isomorfos, **88**

máximo común divisor, **123**
mónico, **146**
múltiplo, **117**
múltiplos enteros, **31**
mapeo natural, **90**
maximal, **81**
monoide, **1**

núcleo, **103**

norma euclidiana, **139**
normal, **225**

polinomio, **145**
polinomio cero, **146**
polinomio mínimo, **190**
potencias, **31**
preserva las operaciones, **22**
primitivo, **175**
primo, **128**
producto, **4**
producto directo externo, **21**
propio, **58**
puntualmente, **26**

raíz, **152**
representante, **23**

separable, **206**
soluble por radicales, **253**
subanillo, **50**
subcampo, **184**
subcampo de H-invariantes,
suma, **4**, **45**

término constante, **146**
términos, **146**
tiene todas sus raíces, **195**
torre de campos, **253**
torre de raíces, **253**
trascendente, **188**

unidad, **40**
uno, **4**

Bibliografía

[1] John B. Fraleigh. 1 A first course in abstract algebra. Addison Wesley, 2002.

[2] The GAP Group. GAP – Groups, Algorithms and Programming. Version 4.3; 2002 (http://www.gap-system.org).

[3] I. N. Herstein. 1 Álgebra moderna: grupos, anillos, campos, teoría de Galois. Editorial Trillas, 1970.

[4] Nathan Jacobson. 1 Basic Algebra I. W H Freeman and Co., 2nd edition, 1985.

Aquí damos una pequeña bibliografía con los libros más importantes que les pueden servir en este curso.

Los dos libros más usados como textos son [3] y [1]. Yo en lo personal prefiero el Fraleigh, pues me parece más didáctico. En particular me gustan mucho sus capítulos cortos, porque uno puede avanzar gradualmente con la seguridad de haber entendido todo lo cubierto anteriormente; además, este libro tiene muchos ejercicios de diversos grados de dificultad. Por otro lado, el Herstein fue por muchos años el texto clásico en el tema.

Otro libro muy bueno pero quizás algo avanzado es [4]. Usualmente recomiendo el Jacobson como referencia más que como texto.

Yo exhorto a mis alumnos a usar la computadora para generar con facilidad ejemplos de lo que aprendemos en el curso. Uno de los mejores programas de álgebra que hay disponibles sin costo es GAP [2]. Pueden ir a la página de internet indicada y seguir las instrucciones para bajar GAP a su computadora personal.