Universidad Nacional Autónoma de México

Facultad de Ciencias

CAMPOS FINITOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
SANTIAGO HERNÁNDEZ OROZCO

DIRECTOR DE TESIS:
DRA. EUGENIA O'REILLY REGUEIRO

2011

Hoja de Datos del Jurado

1. Datos del alumno
Hernández Orozco Santiago
56-59-80-28
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas 099146764

2. Datos del tutor
Dra. Eugenia O'Reilly Regueiro

3. Datos del sinodal 1
Dr. José Ríos Montes

4. Datos del sinodal 2
Dr. Emilio Esteben Lluis Puebla

5. Datos del sinodal 3
Dr. Alejandro Alvarado García

6. Datos del sinodal 4
Dr. Francisco Marmolejo Rivas

7. Datos del trabajo escrito
Campos Finitos
89p
2011

Índice general

Capítulo 1

Introducción.

El uso de los objetos matemáticos a los cuales llamamos números empezó probablemente hace varias docenas de miles de años, se han encontrado marcas en hueso y piedra en notación unaria que datan de tiempos anteriores al año 36,000 A. C. Basados en estos primeros sistemas de numeración, el ser humano dio inicio al estudio del primer conjunto infinito de números, los números naturales, conjunto denotado por $\mathbb{N} = \{1, 2, 3, ...\}$, y la primera operación binaria, la suma.

Conforme nuestro entendimiento sobre estos objetos abstractos, y del mundo en general, fue avanzando, se presentó la necesidad de nuevas clases de números. El siguiente conjunto a presentar es el conjunto de los números enteros $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$. Aunque posterior en su desarrollo histórico a los números fraccionarios, es la primera *extensión natural* de $\mathbb{N}$, resultado de la necesidad de resolver ecuaciones simples, problemas de la forma $a+b = c$. Así, con la introducción de nuevas operaciones aritméticas, surgen nuevas ecuaciones cuya solución requiere de nuevas clases de números. Ecuaciones de la forma $a * b = c$ dieron origen al conjunto de los números fraccionarios, $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ con } q \neq 0\}$. Límites de sucesiones, necesarias para determinar números trascendentes como π, dieron origen al conjunto de los números reales $\mathbb{R}$; y ecuaciones exponenciales, $a^b = c$, a los números complejos $\mathbb{C}$, objetos principales de estudio del Análisis Matemático.

Las tres operaciones binarias descritas generan en su conjunto los problemas conocidos como ecuaciones polinomiales. La solución de ecuaciones de segundo grado se remonta a los tiempos de la antigua Babilonia (1600

A. C.), evidenciado por la presencia de grabados de arcilla que presentan soluciones generales que sugieren construcciones algebraicas. Para mediados del siglo XVI, gracias al desarrollo del álgebra y los trabajos de Tartaglia y Cardano, entre otros, soluciones generales a los problemas polinomiales de tercer y cuarto grado eran conocidas. Sin embargo, las ecuaciones de quinto y mayor grado mostraron ser un desafío cuya solución evadió incluso a algunos de los más reconocidos matemáticos como Euler y Lagrange. Finalmente se demostró la inexistencia de una solución general gracias al teorema de Ruffini-Abel. Sin embargo, casos especiales de ecuaciones de grado mayor a 4 todavía podían presentar soluciones.

Motivado a encontrar condiciones generales para la existencia de soluciones de los ecuaciones polinomiales de grado mayor 4, el joven matemático Évariste Galois (25 de Octubre, 1811 – 31 de Mayo, 1832) desarrolló el concepto de Grupo, una asociación entre estas nuevas estructures algebraicas y los polinomios y, con estos resultados, dio condiciones suficientes y necesarias para la existencia de soluciones por radicales. Sus resultados, de gran importancia para este texto, dieron origen al marco de la Teoría de Galois, que provee una importante asociación entre la Teoría de Grupos y la Teoría de Campos.

Los conceptos modernos de anillo y campo como estructuras algebraicas se deben al trabajo realizado por el matemático alemán Julius Wilhelm Richard Dedekind (6 de Octubre, 1831 – 12 de Febrero, 1916), basado en la recurrencia de propiedades algebraicas presentes en los sistemas clásicos de números, los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Las ideas de Dedekind se asentaron con el posterior desarrollo del álgebra abstracta influenciado por Weber, Hilbert, Noether y van der Waerden, entre otros. Gracias a esta nueva visión abstracta de los sistemas algebraicos, podemos definir y estudiar nuevas clases de estructuras algebraicas. Entre ellas, los campos y una de sus subclases, los campos finitos.

Capítulo 2

Anillos y Campos.

Definición 2.1. Un *anillo* es una estructura algebraica $(R, +, *)$ donde R es un conjunto con dos operaciones binarias $+ : R \times R \to R$ y $* : R \times R \to R$ que cumplen los siguientes axiomas:

Para todos a, b y c *elementos de* R:

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$.
3. *Existe* $0 \in R$ *tal que para toda* $a \in R$, $a + 0 = 0 + a = a$.
4. *Dada* $a \in R$, *existe* $-a \in R$ *tal que* $a + (-a) = 0$, $-a$ es llamado el *inverso aditivo* de a.
5. $(a * b) * c = a * (b * c)$.
6. $c * (a + b) = (c * a) + (c * b)$ y $a * (b + c) = (a * b) + (a * c)$.

   Si también cumple con:
7. $a * b = b * a$.
8. *Existe* $1_R \in R$, *tal que* $1_R * a = a$ *para toda* $a \in R$.

entonces R es un *anillo conmutativo con* 1. Para efectos de esta tesis todo anillo será un anillo conmutativo con 1. A los elementos 0_R y 1_R se les llama el 0 y el 1 del anillo respectivamente. Si R cumple con 2, 3 y 4 entonces

$(R, +)$ es un *grupo*; es un *grupo abeliano* si además cumple con 1. Un subconjunto no vacío H de un grupo $(G, +)$ es un *subgrupo* si es cerrado bajo $+$ y, si $a \in H$ entonces $-a \in H$.

Definición 2.2. Un *campo* es un anillo F tal que

9. Para todo $a \in F$, $a \neq 0$, existe $b \in F$ tal que $a * b = 1$.

Sean $a * b = 1$ y $a * b' = 1$. Entonces tenemos que $a * b = a * b'$, multiplicando ambos lados por b, tenemos que $(a * b) * b = (a * b) * b'$ de donde $b = b'$. Entonces el *inverso múltiplicativo* de a es único y se denota por a^{-1}

Si F es un campo definimos la *división* de la siguiente forma:

$$a/b = a * b^{-1} \quad a, b \in F, b \neq 0 \tag{2.3}$$

Definición 2.4. Un elemento $u \in R$ es una unidad si existe $v \in R$ tal que $u * v = 1$. En un campo, todo elemento distinto de cero es una unidad.

Teorema 2.5. *Sea R un anillo. Entonces:*

(*i*) *Si $e * r = r$ y $1 * r = r$ para toda $r \in R$, entonces $e = 1$. El neutro multiplicativo es único.*

(*ii*) $0 * r = 0$ *para toda* $r \in R$.

(*iii*) *Si $-r$ es el inverso aditivo de $r \in R$ entonces $-r = (-1) * r$.*

(*iv*) $(-r)*(-s) = -(r*s)$ *para toda* $r, s \in R$. *En particular* $(-1) * (-1) = 1$.

Demostración.

(*i*) Sea $e \in R$ tal que $e * r = r$ para toda $r \in R$. En particular, cuando $r = 1$, tenemos que $e * r = 1$. Pero $e * 1 = e$, por lo tanto $e = 1$.

(*ii*) Como $0 = 0 + 0$, podemos distribuir $0 * r = (0 + 0) * r$ como $(0 + 0) * r = 0 * r + 0 * r$, de donde $0 * r = 0 * r + 0 * r$ restando $0 * r$ en ambos lados tenemos que $0 * r = 0$.

(*iii*) Ya que $-1 + 1 = 0$, $0 = 0 * r = (-1 + 1) * r$, por distributividad $(-1 + 1) * r = (-1) * r + r$; de donde $0 = (-1) * r + r$. Por lo tanto, sumando $-r$ en ambos lados, $-r = (-1) * r$.

(iv) Por el iii tenemos que $0 = 0 * (-r) = (-s + s) * (-r) = (-r) * (-s) + (-r) * (s) = (-r) * (-s) + (-r * s)$, sumando $r * s$ en ambos lados tenemos $-(r * s) = (-r) * (-s)$.

□

Consideremos un anillo R tal que $1 = 0$, si $r \in R$, entonces $r = 1 * r = 0 * r = 0$; por lo tanto, R solo cuenta un elemento, el 0. Llamamos a este anillo el anillo trivial. *De aquí en adelante, en todo anillo, $1 \neq 0$.*

Definición 2.6. Sea R un anillo. Si $r, s \in R$ decimos que r *divide a* s, ó s *es múltiplo de* r, si existe $r' \in R$ tal que $r * r' = s$. Se denota por $r|s$.

Ejemplo 2.7. Si R es un anillo, definimos un *polinomio $f(x)$ con coeficientes en R*, un *polinomio sobre R*, como una sucesión de la forma

$$f(x) = (c_0, c_1, ..., c_n, 0, 0, ...)$$

donde $c_0, ..., c_n \in R$ y $c_j = 0$ para toda $j > n$. Si $g(x) = (b_0, b_1, ...,)$ entonces $g(x) = f(x)$ si, y sólo si, $b_i = c_i$ para toda i. Denotamos como $R[x]$ al conjunto de todos los polinomios $f(x)$ sobre R, y definimos las operaciones *suma* $(+ : R[x] \times R[x] \to R[x])$ y *multiplicación* $(* : R[x] \times R[x] \to R[x])$ de la siguiente forma:

$$+((c_0, c_1, ...), (b_0, b_1, ...)) = (c_0 + b_0, c_1 + b_1, ..., c_i + b_i, ...)$$
$$\text{y}$$
$$*((c_0, c_1, ...), (b_0, b_1, ...)) = (e_0, e_1, ..., e_i, ...),$$

donde $e_k = \sum_{k=i+j} c_i * b_j$. La estructura algebraica dada por $(R[x], +, *)$ es un anillo con $0_{R[x]} = (0, 0, ...)$ y $1_{R[x]} = (1, 0, 0, ...)$.

Definimos el *grado de un polinomio $f(x)$*, $\partial(f)$, como el número natural n tal que $c_j = 0$ para toda $j > n$, y $c_n \neq 0$. Si $f = 0$ entonces $\partial(f) = -\infty$. Si $\partial(f) = n$ entonces podemos describir a $f(x)$ como $f(x) = (c_0, ..., c_n)$. Llamamos a c_n el *coeficiente líder*.

Ejemplo 2.8. Sean n un número entero positivo y $a \in \mathbb{Z}$, definimos la clase de equivalencia de a módulo n como

$$\begin{aligned}[a] &= \{m \in \mathbb{Z} : m = a + k * n \text{ para alguna } k \in \mathbb{Z}\} \\ &= \{m \in \mathbb{Z} : m \equiv a \text{ módulo } n\}.\end{aligned}$$

Si definimos el conjunto $n * \mathbb{Z} = n\mathbb{Z}$ como

$$n\mathbb{Z} = \{n * m : m \in \mathbb{Z}\}$$

entonces, tenemos que $[a] = [b]$ si, y sólo si, $a - b \in n * \mathbb{Z}$.

Dado lo anterior, podemos definir al conjunto $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$ y en él dos operaciones binarias:

$$\begin{aligned} + :&\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ &([a], [b]) \mapsto [a + b] \end{aligned}$$

$$\begin{aligned} * :&\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ &([a], [b]) \mapsto [a * b]. \end{aligned}$$

Sean $[a] = [a']$ y $[b] = [b']$, entonces $a' = a + k_1 * n$ y $b' = b + k_2 * n$, de donde $a' + b' = (a + k_1 * n) + (b + k_2 * n) = (a + b) + (k_1 + k_2) * n$. De forma análoga, $a * b = (a + k_1 * n) * (b + k_2 * n) = a * b + (a * k_2 + b * k_1 + k_1 * k_2 * n) * n$. Por lo tanto, las operaciones $+, *$ están bien definidas y $(\mathbb{Z}_n, +, *)$ es un anillo. Llamamos a $(\mathbb{Z}_n, +, *)$ el *anillo de los números enteros módulo n*.

En general, si R es un grupo abeliano e I es un subgrupo de R, definimos una *clase de equivalencia* de I como

$$I + s = \{m \in R : m - s \in I\}, \tag{2.9}$$

y al conjunto R/I, como el conjunto de todas las clases de equivalencia de I. Si definimos $+_{R/I}$ como $(I + s) + (I + s') = I + (s + s')$, $(R/I, +)$ es un grupo llamado *grupo cociente*. El conjunto $I + s = s + I$ es llamado la *clase lateral que contiene a s* y se denota por $[s]$.

Definición 2.10. Un *ideal* en un anillo R es un subconjunto I tal que

(*i*) $0 \in I$

(*ii*) $a, b \in I$ implica que $a - b \in I$

(*iii*) $a \in I$ y $r \in R$ implica que $r * a \in I$

Un ideal I se dice que es un *ideal propio* si $I \neq R$.

Todo anillo R contiene a los ideales R y $\{0\}$. Si el ideal I del anillo R contiene a una unidad u, entonces, para toda $r \in R$, tenemos que $r * u \in I$, de donde $r = (u * u^{-1}) * r = u^{-1} * (u * r) \in I$, por lo tanto, $I = R$. Esto es, un ideal no es propio si contiene una unidad, en particular, si contiene al 1_R.

Definición 2.11. Sea $a \in R$, consideremos el conjunto $\langle a \rangle = \{r * a : r \in R\}$. Entonces:

(*i*) $0 * a = 0$, por lo cual, $0 \in \langle a \rangle$

(*ii*) Si $r, s \in \langle a \rangle$ existen $r', s' \in R$ tales que $r = r' * a$ y $s = s' * a$. De donde $r - s = r' * a - s' * a = (r' - s') * a$, por lo cual, $r - s \in \langle a \rangle$.

(*iii*) Si $s \in \langle a \rangle$ y $r \in R$, $r * s = r * (s' * a) = (r * s') * a$, por lo cual, $r * s \in \langle a \rangle$.

Por lo tanto $\langle a \rangle$ es un ideal, llamado el *ideal principal generado por a*. Un anillo R es llamado un *dominio de ideales principales* si todo ideal es un ideal principal.

Ejemplo: Lema 2.12. Si R es un anillo cuyos únicos ideales son $\{0\}$ y R, entonces R es un campo.

Demostración. Sea $a \in R$, $a \neq 0$. Consideremos al ideal $\langle a \rangle$, por hipótesis $\langle a \rangle = \{0\}$ o $\langle a \rangle = R$. Ya que $a \neq 0$ y $a \in \langle a \rangle$, tenemos que $\langle a \rangle \neq \{0\}$. Por lo cual, $\langle a \rangle = R$ y $1 \in R$, de donde existe $a^{-1} \in R$ tal que $1 = a * a^{-1}$. Por lo tanto, R es un campo. □

Ejemplo 2.13. Sean R un anillo y $a_1, ..., a_n \in R$; definimos el conjunto

$$\langle a_1, ..., a_n \rangle = \{r_1 * a_1 + ... + r_n * a_n : r_i \in R, 1 \leq i \leq n\} = I.$$

Notemos que si $r_i = 0$ para todo i tenemos que $r_1 * a_1 + ... + r_n * a_n = 0$ y $0 \in I$. Además, si $r_1 * a_1 + ... + r_n * a_n, r'_1 * a_1 + ... + r'_n * a_n \in I$, entonces

(*i*) $r_1 * a_1 + ... + r_n * a_n - (r'_1 * a_1 + ... + r'_n * a_n) = (r_1 - r'_1) * a_1 + ... + (r_n - r'_n) * a_n \in I$,

y que, para toda $r \in R$,

(*ii*) $r * (r'_1 * a_1 + ... + r'_n * a_n) = (r * r'_1) * a_1 + ... + (r * r'_n) * a_n \in I$.

Por lo tanto, $\langle a_1, ..., a_n \rangle$ es un ideal llamado el *ideal generado por el conjunto* $\{a_1, ..., a_n\}$.

Teorema 2.14. *Si F es un campo, entonces $F[x]$ es un dominio de ideales principales.*

Demostración. Sea I un ideal en $F[x]$. Si $I = \{0\}$, entonces $I = \langle 0\rangle$. Supongamos que $I \neq \{0\}$, sea $m(x) \in I$ un polinomio de grado mínimo distinto de 0, es decir, si $n(x) \in I$, $n(x) \neq 0$, entonces $\partial(m) \leq \partial(n)$. Notemos que $m(x)$ existe, al ser $I \neq \{0\}$ existe al menos un polinomio de grado no negativo; además el conjunto de grados no negativos es un subconjunto de los naturales, por lo que tiene un primer elemento.

Consideremos a $\langle m(x)\rangle$. Sea $f(x) \in \langle m(x)\rangle$, existe $g(x) \in F[x]$ tal que $f(x) = m(x) * g(x)$. Ya que $m(x) \in I$ tenemos que $f(x) \in I$, por lo cual $\langle m(x)\rangle \subset I$.

Sea $f(x) \in I$. Usando el algoritmo de la división (8.11), existen polinomios $q(x)$ y $r(x)$, con $\partial(r) < \partial(m)$ en $F[x]$ tales que $f(x) = q(x) * m(x) + r(x)$, de donde $r(x) = f(x) - q(x) * m(x) \in I$. Pero como $m(x)$ es un polinomio de grado mínimo, $r(x) = 0$. Por lo tanto, $f(x) = q(x) * m(x) \in \langle m(x)\rangle$, $I \subset \langle m(x)\rangle$ e $I = \langle m(x)\rangle$. □

Sean R un anillo, $a \in R$ y u una unidad en R. Claramente $\langle u * a\rangle \subset \langle a\rangle$. Sea $u' \in R$ tal que $u * u' = 1$. Si $s \in \langle a\rangle$ entonces existe $r \in R$ tal que $s = r * a$, de donde $s = (r * a) * (u * u') = (r * u') * (u * a)$; por lo cual, $s \in R\langle u * a\rangle$, $\langle a\rangle \subset \langle u * a\rangle$ y $\langle a\rangle = \langle u * a\rangle$.

Decimos que un polinomio es *mónico* si su coeficiente líder (el de mayor grado) es 1. Entonces, si $I = \langle p(x)\rangle$ con $p(x) = (a_0, a_1, ..., a_n)$, para la unidad $u(x) \in F[x]$ dada por $u(x) = (u_0 = a_n^{-1}, 0, ..., 0, ...)$, tenemos que $\langle p(x)\rangle = \langle u(x) * f(x)\rangle = \langle f(x)\rangle$ donde $f(x)$ es el polinomio mónico $f(x) = (a_0 * a_n^{-1}, a_1 * a_n^{-1}, ..., a_{n-1} * a_n^{-1}, 1)$. Es decir, para un campo F, *todo ideal I de $F[x]$ está generado por un polinomio mónico $f(x)$ único para cada ideal, $I = \langle f(x)\rangle$.*

Definición 2.15. Un anillo R es un *dominio entero* si para todo $a, b \in R$ tales que $a \neq 0$ y $b \neq 0$ entonces $a * b \neq 0$. Si para $a \neq 0$ existe $b \neq 0$ tal que $a * b = 0$, entonces a es un *divisor de cero*. Un anillo es un dominio entero si no contiene divisores de cero. A estos anillos se les puede llamar simplemente *dominio*.

Proposición 2.16. *Todo campo es un dominio entero.*

Demostración. Supongamos que R es un campo y $r, s \in R$ tales que $r*s = 0$ con $r \neq 0$. Como $r^{-1} * r = 1$, entonces $0 = r^{-1} * 0 = r^{-1} * (r * s) = (r^{-1} * r) * s = 1 * s = s$, por lo tanto $s = 0$. □

Teorema 2.17. *Un anillo R es un dominio si, y sólo si satisface la* regla de la cancelación*: si $r * a = r * b$ y $r \neq 0$, entonces $a = b$.*

Demostración. Sean R un dominio y $r \in R$ con $r \neq 0$. Si $r * a = r * b$ entonces $r*(a-b) = 0$. Como R es un dominio, $a-b = 0$ y, por lo tanto, $a = b$.

Ahora supongamos que la regla de cancelación es cierta en R. Sean $r, a \neq 0$ tales que $r * a = 0$. Entonces, por el teorema 2.5, $r * a = 0 = r * 0$ implica que $a = 0$, que es una contradicción.

□

Definición 2.18. Sean R un dominio y $f(x), g(x) \in R[x]$. Un *máximo común divisor (mcm)* de $f(x)$ y $g(x)$ es un polinomio $d(x)$ tal que:

(*i*) $d(x)|f(x)$ y $d(x)|g(x)$. Se dice que $d(x)$ es un *común divisor* de $f(x)$ y $g(x)$.

(*ii*) Si $c(x)$ es un común divisor de $f(x)$ y $g(x)$, entonces $c(x)|d(x)$.

(*iii*) $d(x)$ es un polinomio mónico.

Notemos que podemos extender esta definición a cualquier anillo omitiendo el axioma (*iii*). Para el anillo de polinomios sobre un campo, el máximo común divisor es único y se denota por $d(x) = (f(x), g(x))$.

Si $(f(x), g(x)) = 1$, decimos que $f(x)$ y $g(x)$ son *primos relativos.*

Teorema 2.19. *Sean F un campo y $f(x), g(x) \in F[x]$ dos polinomios distintos de cero. Entonces, $d(x) = (f(x), g(x))$ existe y es una* combinación lineal *de $f(x)$ y $g(x)$. Es decir, existen elementos $a(x), b(x)$ en el anillo $F[x]$ tales que*

$$d(x) = a(x) * f(x) + b(x) * g(x). \tag{2.20}$$

Demostración. Por el ejemplo 2.13, el conjunto

$$I = \{a(x) * f(x) + b(x) * g(x) : a(x), b(x) \in F[x]\}$$

es un ideal. Como F es un campo, por el teorema 2.14, $F[x]$ es un dominio de ideales principales e I es un ideal principal, es decir, existe un polinomio

mónico $d(x) \in I$ tal que $\langle d(x) \rangle = I$.

Ya que $d(x) \in I$, existen $a(x), b(x) \in F[x]$ tales que $d(x) = a(x) * f(x) + b(x) * g(x)$. Como $f(x), g(x) \in I$, $d(x)|f(x)$ y $d(x)|g(x)$. Finalmente, si $c(x)$ es un divisor común de $f(x)$ y $g(x)$, para algunos polinomios $c'(x), c''(x)$ tenemos que $f(x) = c(x) * c'(x)$ y $g(x) = c(x) * c''(x)$, de donde

$$\begin{aligned} d(x) &= a(x) * f(x) + b(x) * g(x) \\ &= a(x) * (c(x) * c'(x)) + b(x) * (c(x) * c''(x)) \\ &= c(x) * (a(x) * c'(x) + b(x) * c''(x)) \text{ y } c(x)|d(x). \end{aligned}$$

Por lo tanto, $d(x) = (f(x), g(x))$.

□

Corolario: Lema de Euclides 2.21. *Sea F un campo, y sea $p(x)$ un polinomio en $F[x]$ tal que no existen polinomios $f(x), g(x) \in F[x]$ con $\partial(f), \partial(g) < \partial(p)$ tales que $p(x) = f(x) * g(x)$. Si $p(x)|q_1(x) * ... * q_n(x)$ entonces existe $q_j(x)$, $1 \leq j \leq n$, tal que $p(x)|q_j(x)$.*

Demostración. Supongamos que $p(x)|q_1(x)*q_2(x)$, si $p(x)$ no divide a $q_1(x)$, entonces, por el teorema 2.19, existen $a(x), g(x) \in F[x]$ tales que $1 = a(x)*p(x)+b(x)*q_1(x)$. Por lo cual, $q_2(x) = q_2(x)*1 = q_2(x)*(a(x)*p(x)+b(x)*q_1(x))$. Ya que $p(x)|q_1(x)*q_2(x)$. y $p(x)$ no puede ser de la forma $p(x) = f(x) * g(x)$, existe $k(x) \in F[x]$ tal que $p(x) * k(x) = q_1(x) * q_2(x)$, de donde $q_2(x) = q_2(x)*a(x)*p(x)+b(x)*k(x)*p(x) = p(x)*(q_2(x)*a(x)+b(x)*k(x))$. Por lo tanto, $p(x)|q_2(x)$.

Por inducción sobre $n \geq 2$, terminamos. □

Corolario 2.22. *Sean F un campo, $f(x)$,$g(x) \in F[x]$, y sea $I = \langle f(x), g(x) \rangle$ el ideal generado por $f(x)$ y $g(x)$. Entonces $I = \langle d(x) \rangle$ donde $d(x) = (f(x), g(x))$ ($d(x)$ es el máximo común divisor).*

Demostración. Por la demostración del teorema 2.19 tenemos que $I = \langle d(x) \rangle$. □

Definición 2.23. Sea I un ideal del anillo R, el *anillo cociente* R/I consiste en $(R/I, +, *)$, donde $+$ y $*$ están dados por:

$$(I + s) + (I + s') = I + (s + s')$$
$$(I + s) * (I + s') = I + (s * s')$$

Ejemplo 2.24. Sean F un campo, $I = \langle p(x) \rangle$ el ideal principal generado por $p(x)$ y R el anillo $R = F[x]/I$. Si $f(x)$ y $p(x)$ son primos relativos, entonces existen $a(x), b(x) \in F(x)$ tales que $a(x) * f(x) + b(x) * p(x) = 1$.

Notemos que $I + 1 = I + a(x) * f(x) + b(x) * p(x) = I + a(x) * f(x)$, ya que $b(x) * p(x) \in I$, de donde $I + f(x)$ es una unidad con $I + a(x)$ como inverso.

Definición 2.25. Un *subanillo* de un anillo R es un subgrupo S de R bajo $+$ que contiene a 1 y es cerrado bajo $*$. Un *subcampo* es un subanillo de un anillo que es un campo.

Definición 2.26. El *subcampo primario* de un campo F es la intersección de todos los subcampos de F.

Teorema 2.27. *El anillo $\mathbb{Z}_n$ es un campo si, y solo si n es un número primo.*

Demostración. Supongamos que n no es un número primo. Si $n = 1$, entonces $\mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}$ que solo contiene un elemento, por lo cual no puede ser un campo. Si $n > 1$, entonces existen r y s enteros positivos menores a n tales que $n = r * s$. Sea $I = n\mathbb{Z}$,

$$(I + r) * (I + s) = I + (r * s) = I \tag{2.28}$$

Pero I es el elemento cero de $\mathbb{Z}/I$, mientras que $I + r$ e $I + s$ son diferentes de cero. Ya que el producto de dos elementos diferentes de cero es cero, $\mathbb{Z}/I$ no puede ser un campo.

Ahora supongamos que n es primo. Sea $I + r$ un elemento diferente de cero en $\mathbb{Z}/I$, de donde n no divide a r. Ya que n es primo, r y n son primos relativos, por lo cual existen enteros s y t tales que $s * r + t * n = 1$. De donde,

$$(I + s) * (I + r) = (I + 1) - (I + n) * (I + t) = (I + 1) - (I + n * t) = I + 1.$$

Ya que $I + 1$ es el elemento identidad de $\mathbb{Z}/I$, hemos encontrado un inverso multiplicativo dado cualquier elemento $I + r$. Por lo tanto, todo elemento no cero de $\mathbb{Z}/I$ es una unidad. Entonces $\mathbb{Z}_n = \mathbb{Z}/I$ es un campo. □

Teorema 2.29. *Para cada dominio R existe un campo $Frac(R)$ que contiene a R como subanillo. Además, cada elemento $r \in Frac(R)$ tiene una factorización $r = p * q^{-1}$ con $p, q \in R$ y $q \neq 0$.*

Demostración. Sean R un dominio, y S el conjunto de todas las parejas ordenadas (r, s) donde $r, s \in R$ con $s \neq 0$. Definimos una relación de equivalencia $\sim$ en S dada por

$$(r, s) \sim (t, u) \text{ si, y sólo si } r * u = s * t$$

Denotamos la clase lateral de (r, s) por $[r, s]$. Sea $Frac(R)$ el conjunto de todas las clases laterales. Definimos dos operaciones binarias $+, * : Frac(R) \times Frac(R) \to Frac(R)$ por

$$[r, s] + [t, u] = [r * u + t * s, s * u]$$
$$[r, s] * [t, u] = [r * t, s * u]$$

Como R es un dominio, $s * u \neq 0$. Sean $[r, s] = [a, b]$ y $[t, u] = [c, d]$,

$$[r, s] + [t, u] = [r * u + t * s, s * u] \quad \& \quad [a, b] + [c, d] = [a * d + c * b, b * d]$$

ya que $r * b = s * a$ y $t * d = u * c$,

$$\begin{aligned}(r * u + t * s) * (b * d) &= (r * b) * (d * u) + (t * d) * (b * s) \\ &= (s * a) * (d * u) + (u * c) * (b * s) \\ &= (s * u)(a * d + c * b)\end{aligned}$$

por lo cual $[r * u + t * s, s * u] = [a * d + c * b, b * d]$. Además,

$$[r, s] * [t, u] = [r * t, s * u] \quad \& \quad [a, b] * [c, d] = [a * c, b * d]$$

tenemos que,

$$\begin{aligned}(r * t) * (b * d) &= (r * b) * (t * d) \\ &= (s * a) * (u * c)\end{aligned}$$

Por lo cual $[r, s] * [t, u] = [a, b] * [c, d]$. Por lo tanto, $+$ y $*$ *están bien definidas.*

Sean $[r, s], [t, u], [p, q] \in R$, como R es un anillo y r, s, t, u, p y $q \in R$, $r, s \neq 0$:

1. $[r,s]+[t,u]=[r*u+s*t,s*u]=[t*s+u*r,u*s]=[t,u]+[r,s]$.

2.
$$\begin{aligned}[r,s]+([t,u]+[p,q]) &= [r,s]+[t*q+u*p,u*q]\\ &= [r*u*q+s(t*q+u*p),u*q*s]\\ &= [r*u*q+s(t*q+u*p),u*q*s]\\ &= [r*u*q*s+s*t*q+s*u*p,u*q*s]\\ &= [(r*u+s*t)*q+s*u*p,s*u*q]\\ &= [r*u+s*t,s*u]+[p,q]\\ &= ([r,s]+[t,u])+[p,q]\end{aligned}$$

3. $[r,s]+[0,1]=[r*1+s*0,s*1]=[r,s]$

4. $[r,s]+[-r,s]=[r*s-s*r,s*s]=[0,s*s]$. Notemos que $0*1=0=(s*s)*0$ implica que $[0,s*s]=[0,1]=0_{Frac(R)}$.

5.
$$\begin{aligned}[r,s]*([t,u]+[p,q]) &= [r,s]*[t*q+u*p,u*q]\\ &= [r*t*q+r*u*p,s*u*q]\end{aligned}$$
y
$$\begin{aligned}[r,s]*[t,u]+[r,s]*[p,q] &= [r*t,s*u]+[r*p,s*q]\\ &= [(r*t)*(s*q)+(s*u)*(r*p),\\ &\quad (s*u)*(s*q)].\end{aligned}$$

Tenemos que

$$\begin{aligned}&((s*u)*(s*q))*(r*t*q+r*u*p)\\ &\quad = s*u*s*q*r*t*q+s*u*s*q*r*u*p\\ &\quad = (s*u*q)*((r*t*s*q)+(s*u*r*p)\\ &\quad = (s*u*q)*((r*t)*(s*q)+(s*u)*(r*p)),\end{aligned}$$

por lo tanto, $[r,s]*([t,u]+[p,q])=[r,s]*[t,u]+[r,s]*[p,q]$.

6. $[r,s]*[t,u]=[r*t,s*u]=[t*r,u*s]=[t,u]*[r,s]$.

7. $([r,s]*[t,u])*[p,q]=[r*(t*p),s*(u*q)]=[r,s]*([t,u]*[p,q])$.

8. $[r,s]*[1,1]=[r*1,s*1]=[r,s]$.

9. $[r,s]*[s,r] = [r*s, s*r]$, como $(r*s)*1 = (s*r)*1$, $[r*s, s*r] = [1,1]$.

10. Por último $[r,s] = [r,1]*[1,s]$, donde $[1,s] = [s,1]^{-1}$.

Por lo tanto, $Frac(R)$ es un campo y existen $p, q \in R$ tales que $r = p*q^{-1}$ para cada $r \in Frac(R)$. Notemos que, podemos ver a los elementos en $Frac(R)$ de la forma a/b, con $b \neq 0$, donde $a, b \in R$. □

Definición 2.30. Si R es un dominio, entonces $Frac(R)$ es llamado el *campo de cocientes* de R.

Capítulo 3

Ideales y Homomorfismos

Definición 3.1. Sean R y S anillos, una función $\varphi : R \to S$ es un *homomorfismo de anillos* si, para toda $r, r' \in R$:

(i) $\varphi(r + r') = \varphi(r) + \varphi(r')$.

(ii) $\varphi(r * r') = \varphi(r) * \varphi(r')$.

(iii) $\varphi(1_R) = 1_S$.

Un homomorfismo $\varphi : R \to S$ es un *isomorfismo* si φ es una biyección. Si para R y S anillos existe dicho isomorfismo, entonces se dice que R y S son anillos *isomorfos* y se denota por $R \cong S$. Un homomorfismo φ de un anillo en sí mismo, es decir $\varphi : R \to R$, que además es un isomorfismo, es llamado un *automorfismo*.

Sean R un grupo y H un subgrupo de R. Decimos que un automorfismo σ de R *deja fijo a* H si $\sigma : h \mapsto h$ para todo $h \in H$.

Ejemplo 3.2. Sean R y S anillos. Definimos el conjunto $Hom(R, S)$ como

$$Hom(R, S) = \{\sigma : R \to S : \sigma \text{ es un homomorfismo } \}$$

y a las operaciones

$$\begin{aligned} + :& Hom(R,S) \times Hom(R,S) \to Hom(R,S) \\ & (\sigma, \tau) \mapsto (\sigma + \tau) \end{aligned}$$

y

$$\begin{aligned} * :& S \times Hom(R,S) \to Hom(R,S) \\ & (c, \sigma) \mapsto (c * \sigma) \end{aligned}$$

donde $(c * \sigma)(x) = c * \sigma(x)$ y $(\sigma + \tau)(x) = \sigma(x) + \tau(x)$. Entonces, las operaciones $+$ y $*$ definen en $Hom(R, S)$ la estructura de un S-módulo izquierdo. Si además S es un campo, entonces tenemos la estructura de un espacio vectorial sobre S.

Proposición 3.3. *Si $\varphi : R \to S$ es un mapeo suprayectivo de anillos tal que cumple con $\varphi(r * r') = \varphi(r) * \varphi(r')$, entonces $\varphi(1_R) = 1_S$. Además, si cumple con $\varphi(r + r') = \varphi(r) + \varphi(r')$ entonces $\varphi(0) = 0$ y $\varphi(-r) = -\varphi(r)$.*

Demostración. Sea $s \in S$ tal que $s \neq 0$. Entonces existe $r \in R$ tal que $\varphi(r) = s$ y $s = \varphi(r) = \varphi(r * 1_r) = \varphi(r) * \varphi(1_R)$. Luego, por el teorema 2.5, $\varphi(1_R) = 1_S$.

Ahora, si $\varphi(r) \in S$ entonces $\varphi(r) = \varphi(r+0) = \varphi(r)+\varphi(0)$; por lo tanto, $\varphi(0) = 0$. Luego, $0 = \varphi(r-r) = \varphi(r)+\varphi(-r)$. De donde, al ser S un anillo, $\varphi(-r) = -\varphi(r)$. □

Ejemplo 3.4. Definimos el conjunto *imagen* del homomorfismo de anillos $\varphi : R \to S$ como $img\varphi = \{\varphi(r) : r \in R\}$.

Sean $s, s' \in img\varphi$, entonces existen $r, r' \in R$ tales que $\varphi(r) = s$ y $\varphi(r') = s'$. Luego:

(i) $s + s' = \varphi(r) + \varphi(r') = \varphi(r + r') \in img\varphi$,

(ii) Por la proposición 3.3, $-s = (-1) * s = \varphi(-1) * \varphi(r) = \varphi(-r) \in img\varphi$

(iii) Por definición de homomorfismo, $\varphi(1) = 1$

y

(iv) $s * s' = \varphi(r) * \varphi(r') = \varphi(r * r') \in img\varphi$.

Por lo tanto, $img\varphi$ es un subanillo de S.

Definimos la *imagen de un subconjunto* $I \subset R$ como $\varphi(I) = \{\varphi(r) : r \in I \subset R\}$.

Ejemplo 3.5. Consideremos al campo $F = Frac(R)$ para el dominio R, Sea

$$i : R \to F$$
$$i : r \mapsto [r, 1]$$

entonces, para $r, r' \in R$

(i) $i(r + r') = [r + r', 1] = [r, 1] + [r', 1] = i(r) + i(r')$,

(ii) $i(r * r') = [r * r', 1] = [r, 1] * [r', 1] = i(r) * i(r')$,

y

(iii) $i(1) = [1, 1] = 1_{Frac(R)}$.

Por lo que i es un homomorfismo de anillos. Llamamos al homomorfismo i el homomorfismo *inclusión*.

Ejemplo 3.6. El mapeo $\pi : \mathbb{Z} \to \mathbb{Z}_n$, definido por $\pi : a \to [a]$, es un homomorfismo suprayectivo de anillos.

Sean $r, r' \in R$, y el mapeo $\pi : R \to R/I$ como $r \mapsto I + r$. Entonces

$$\begin{aligned} \pi(1_R) &= I + 1 = 1_{R/I}, \\ \pi(r + r') &= I + (r + r') = (I + r) + (I + r') = \pi(r) + \pi(r'), \\ &\text{y} \\ \pi(r * r') &= I + (r * r') = (I + r) * (I + r') = \pi(r) * \pi(r'). \end{aligned}$$

En general, definimos el *mapeo natural* entre un anillo y su anillo cociente como el homomorfismo suprayectivo de anillos π.

Definición 3.7. El *núcleo* de un homomorfismo $\varphi : R \to S$ es el conjunto

$$ker\varphi = \{r \in R : \varphi(r) = 0\},$$

Notemos que el axioma (iii) de la definición de homomorfismo nos excluye el caso $ker\varphi = R$. Además, el 0 siempre pertenece al núcleo. Por lo cual, este nunca es vacío.

Ejemplo 3.8. *El mapeo natural*

$$\begin{aligned} \pi : & R \to R/I \\ & r \mapsto I + r \end{aligned}$$

tiene a I como núcleo, ya que, para todo $s \in I$, tenemos que $I + s = I$; y si $s \notin I$, entonces $s + I \neq I$.

Teorema 3.9. *Si $\varphi : R \to S$ es un homomorfismo de anillos, entonces $ker\varphi$ es un ideal propio de R. Además, φ es un mapeo inyectivo si, y sólo si, $ker\varphi = \{0\}$.*

Demostración. Sean $a, b \in ker\varphi$ y $r \in R$, entonces

$$\varphi(r * a) = \varphi(r) * \varphi(a) = \varphi(r) * 0 = 0,$$

y

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0.$$

Por lo tanto, $r * a, a - b \in ker\varphi$, entonces $ker\varphi$ es un ideal en R. Como φ es un homomorfismo de anillos, $\varphi(1) = 1 \neq 0$, por lo que $ker\varphi$ es un ideal propio de R.

Supongamos que $ker\varphi = \{0\}$. Si $\varphi(r) = \varphi(r')$, entonces

$$0 = \varphi(r) - \varphi(r') = \varphi(r - r')$$

por lo que $r - r' \in ker\varphi$ de donde $r - r' = 0$ y $r = r'$. Por lo tanto, φ es un homomorfismo inyectivo.

Por otro lado, si φ es un homomorfismo inyectivo y si $r \neq 0$, entonces $\varphi(r) \neq \varphi(0) = 0$. Por lo cual, $ker\varphi = \{0\}$.

□

Ejemplo: Proposición 3.10. *Sean I un ideal del anillo R y J un ideal del anillo S. Sea $\varphi : R \to S$ un isomorfismo de anillos tal que $\varphi(I) = J$. Entonces, la función $\hat{\varphi} : R/I \to S/J$ dada por $r + I \mapsto \varphi(r) + J$ es un isomorfismo de anillos.*

Demostración. Sea $r + I = r' + I$, entonces

$$\begin{aligned} \hat{\varphi}(r + I) - \hat{\varphi}(r' + I) &= (\varphi(r) + J) - (\varphi(r') + J) \\ &= (\varphi(r) - (\varphi(r')) + J \\ &= \varphi(r - r') + J. \end{aligned}$$

Ya que $\varphi(I) = J$ y $r - r' \in I$, entonces $\varphi(r - r') \in J$ y $\hat{\varphi}$ está bien definida.

Ahora, si $r + I \in ker\hat{\varphi}$ entonces $\varphi(r) + J = J$ y $\varphi(r) \in J$. Por lo tanto, $r \in I$ y $r + I = I$. Por lo tanto, $\hat{\varphi}$ es inyectiva. Si $s + I \in S/J$, ya que φ es un

isomorfismo, y en particular es suprayectiva, existe $r \in R$ tal que $\varphi(r) = s$. Por lo tanto, $\hat{\varphi}$ es suprayectiva.

Por lo tanto, $\hat{\varphi}$ es un isomorfismo de anillos.

□

Ejemplo 3.11. El homomorfismo de anillos $i : R \to Frac(R)$ es una inyección. Si $r \in keri$ tenemos que $i(r) = [r, 1] = 0_{Frac(R)} = [0, 1]$, de donde $r*1 = 1*0$, entonces $r = 0$. Por lo tanto, $keri = \{0\}$ e i es un homomorfismo inyectivo.

Consideremos i restringido al conjunto $imgi$, esto es:

$$i|^{imgi} : R \to imgi$$
$$i|^{imgi} : r \mapsto i(r) = [r, 1]$$

Ya que i es un homomorfismo inyectivo y suprayectivo en su imagen, $i|^{imgi}$ es un isomorfismo de anillos.

Teorema (Primer Teorema de Isomorfismos) 3.12. *Sean R y S anillos y $\phi : R \to S$ un homomorfismo suprayectivo de anillos. Entonces S es isomorfo a $R/ker\phi$ por el isomorfismo $[r] \mapsto \phi(r)$. Además, hay una correspondencia biyectiva entre el conjunto de los ideales de S y el conjunto de los ideales de R que contienen a $ker\phi$. Esta correspondencia puede obtenerse asociando a cada ideal J de S el ideal I de R definido por*

$$I = \{a \in R : \phi(a) \in J\}.$$

Con I así definido, R/I es isomorfo al anillo S/J.

Demostración. Consideremos al mapeo $\varphi : R/ker\phi \to S$ dado por $[r] \mapsto \phi(r)$. Notemos que si existen $r, r' \in R$ tales que $r + ker\phi = r' + ker\phi$, entonces $r - r' \in ker\phi$ y $\phi(r - r') = 0$; de donde $\phi(r) - \phi(r') = 0$ y $\phi(r) = \phi(r')$. Por lo tanto, φ está bien definido. Además:

(i) $\varphi(r + s + I) = \phi(r + s) = \phi(r) + \phi(s) = \varphi(r + I) + \varphi(s + I)$,

(ii) $\varphi(r * s + I) = \phi(r * s) = \phi(r) * \phi(s) = \varphi(r + I) * \varphi(s + I)$.

Por lo cual φ es un homomorfismo de anillos.

Ahora, si $r+I \in ker\varphi$ entonces $\phi(r) = 0$ y $r \in ker\phi$; de donde $[r] = [0]$. Por lo tanto, φ es un homomorfismo de anillos inyectivo. Por lo tanto, $S \cong R/ker\phi$.

Notemos que para cada ideal J en S, tenemos que para el conjunto correspondiente I:

(i) Ya que $0 \in J$ tenemos que $0 = \phi(0) \in I$.

(ii) Si $r, r' \in I$ entonces $\phi(r), \phi(r') \in J$ y $\phi(r) - \phi(r') \in J$, de donde $\phi(r - r') \in J$ y $r - r' \in I$.

(iii) Si $a \in I$ y $r \in R$, entonces $\phi(a * r) = \phi(a) * \phi(r) \in J$, ya que J es un ideal, y $a * r \in I$.

Por lo tanto, I es un ideal en R. Llamemos ψ a esta correspondencia. Sea $\psi(J) = \psi(J')$. Si $s \in J \subset S$, existe $r \in R$ tal que $\phi(r) = s$; por lo que $r \in I$, $s = \phi(r) \in J'$ y $J \subset J'$. De forma análoga, $J' \subset J$ y $J = J'$. Por lo tanto, ψ es una inyección.

Ahora, si I es un ideal de R que contiene a $ker\phi$ le asociamos el conjunto J_I dado por $J_I = \{\phi(r) \in S : r \in I\}$. Notemos que, si $s \in I$, al ser ϕ un suprayectivo, existe $r \in I$ tal que $\phi(r) = I$

(i) Ya que $0 \in I$ y $0 = \phi(0) \in J_I$.

(ii) Si $s, s' \in J_I$, existen $r, r' \in I$ tales que $\phi(r) = s$ y $\phi(r') = s'$, de donde $r - r' \in I$ y $s - s' = \phi(r - r') \in J_I$.

(iii) Si $a \in J_I$ y $s \in S$, existen $a' \in I$ y $r \in R$ tales que $\phi(r) = s$ y $\phi(a') = a$, de donde $a' * r \in I$ y $\phi(a') * \phi(r) = \phi(a' * r) \in J_I$.

Por lo tanto, para todo ideal I de R que contiene a $ker\phi$, existe J_I tal que $\psi(J_I) = I$. Por lo tanto, ψ es suprayectiva y ψ es una biyección. $\square$

Proposición 3.13. *En la demostración del teorema anterior (3.12), si $\varphi : R \to S$ es homomorfismo suprayectivo, establecemos que la imagen de un ideal es un ideal. Además, tenemos que la imagen de un ideal principal, es un ideal principal.*

Demostración. Sea $\varphi : R \to S$ un homomorfismo de anillos. Sea I un ideal principal del anillo R generado por a. Si $s \in \varphi(\langle a \rangle)$, entonces existe $s' \in I \subset R$ tal que $\varphi(s') = s$. Además, existe $r \in R$ tal que $s' = r * a$. De donde, ya que φ es suprayectivo, $s = \varphi(s') = \varphi(r * a) = \varphi(r) * \varphi(a)$. Por lo tanto, $\varphi(\langle a \rangle)$ es el ideal principal generado por $\varphi(a)$, $\langle \varphi(a) \rangle$.

□

Teorema 3.14. *Todo subcampo primario es isomorfo al campo $\mathbb{Q}$ de los números racionales, o bien, al campo $\mathbb{Z}_p$ de los números enteros módulo un número primo p.*

Demostración. Sean F un campo y P su subcampo primario. Como P es un campo, P contiene a 0 y a 1, por lo tanto, contiene a los elementos n^* ($n \in \mathbb{Z}$) dados por:

$$n^* = \begin{cases} 1_F + 1_F + \ldots + 1_F \ (n \text{ veces}) & \text{si } n > 0 \\ 0_F & \text{si } n = 0 \\ -(-n)^* & \text{si } n < 0 \end{cases}$$

Notemos que el mapeo $* : \mathbb{Z} \to P$ es un homomorfismo de anillos. Tenemos dos casos.

Caso 1. $n^* = 0_F$ para alguna $n \neq 0$.
Ya que $(-n)^* = 0_F$, existe un entero positivo mínimo p tal que $p^* = 0_F$. Si p no es un primo, existen r y s positivos enteros menores que p tales que $p = r * s$, entonces $r^* * s^* = p^* = 0_F$, de donde $r^* = 0_F$ o $s^* = 0_F$, contradiciendo nuestra elección de p. Por lo tanto, p es primo. Los elementos n^* forman un anillo isomorfo a $\mathbb{Z}_p$, que es un campo por el teorema 2.27. Ya que P es el menor subcampo de F, P es un campo.

Caso 2. $n^* \neq 0$ si $n \neq 0$. Entonces, P debe contener todos los elementos m^*/n^* donde m y n son enteros con $n \neq 0$. Por el mapeo $P \to \mathbb{Q}$ que manda m^*/n^* a m/n, los elementos de la forma m^*/n^* generan un subcampo isomorfo a $\mathbb{Q}$ que necesariamente, al ser $\mathbb{Q}$ un subcampo del subcampo primario P, debe de ser todo P.

□

Definición 3.15. La *característica de un campo* F es 0 si el subcampo primario de F es isomorfo a $\mathbb{Q}$, y es p si el subcampo primario de F es isomorfo a $\mathbb{Z}_p$.

Notemos que todos los campos finitos, ya que no pueden ser isomorfos a $\mathbb{Q}$, son necesariamente de característica p para algún p primo.

Lema 3.16. *Sean F un campo de característica $p > 0$ y $a, b \in F$. Para $n\mathbb{Z}$ denotemos por $n * a$ el producto $n^* * a$. Entonces:*

(*i*) $p * a = 0$.

(*ii*) $(a+b)^p = a^p + b^p$.

(*iii*) $(a+b)^{p^k} = a^{p^k} + b^{p^k}$

Demostración. Sea P el campo primario de F. Entonces $P \cong \mathbb{Z}_p$, de donde:

(*i*) Para todo $a \in F$ tenemos que $(1_F + ... + 1_F) * a = 0 * a = 0$.

(*ii*) Por el teorema del binomio (8.1), tenemos que

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} * a^i * b^{p-i} + b^p.$$

Ya que $p|\binom{p}{i}$, tenemos que $\binom{p}{i} \in p * \mathbb{Z}_p = 0$ y $(a+b)^p = a^p + b^p$.

(*iii*) Si $k = 1$, tenemos el inciso (*ii*). Supongamos que la proposición es válida para $k = n$. Sea $k = n + 1$, entonces

$$(a+b)^{p^{k+1}} = [(a+b)^{p^k}]^p = [a^{p^k} + b^{p^k}]^p = a^{p^{k+1}} + b^{p^{k+1}}.$$

□

Ejemplo: Mapeo de Frobenius 3.17. *Sea F un campo de característica $p > 0$, entonces el mapeo $\phi : F \to F$ dado por $a \mapsto a^p$ es un homomorfismo de anillos, llamado el* homomorfismo de Frobenius.

Demostración. Sean $a, b \in F$. Notemos que, por el teorema 3.16

(i) $\phi(1) = 1^p = 1$,

(ii) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$
y

(iii) $\phi(a * b) = (a * b)^p = a^p * b^p$.

Por lo tanto, ϕ es un homomorfismo de anillos. □

Notemos que el homomorfismo de Frobenius es inyectivo. Sean F un campo de característica p y sean $a, b \in F$ tales que $a^p = b^p$. Entonces, por ser F de característica p, tenemos que $0 = a^p - b^p = (a-b)^p$. Por lo tanto, $a - b = 0$ y $a = b$.

Lema 3.18. *Si K es un subcampo de L, entonces K y L tienen la misma característica.*

Demostración. Al ser K un subcampo de L, ambos tienen el mismo subcampo primario.

□

Definición 3.19. Un ideal I de un anillo R es un *ideal primo*, si es propio y $a * b \in I$ implica que $a \in I$ o $b \in I$.

Teorema 3.20. *Un ideal propio I en R es un ideal primo si, y sólo si, R/I es un dominio.*

Demostración. Sea I un ideal primo. Si $0 = (a+I) * (b+I) = a * b + I$, entonces $a * b \in I$. Como I es un ideal primo, ya sea $a \in I$ o $b \in I$; de donde $a + I = 0$ o $b + I = 0$. Por lo tanto, R/I es un dominio.

Sea R/I un dominio. Si $a * b \in I$, entonces $0 = a * b + I = (a+I) * (b+I)$. Como R/I es un dominio, $a + I = 0$ o $b + I = 0$; de donde $a \in I$ o $b \in I$. Por lo tanto, I es un ideal primo.

□

Definición 3.21. Un polinomio $p(x)$ de $F(x)$, F un campo, es *irreducible en F* si $\partial(p) \geq 1$ y no existen $f(x), g(x) \in F[x]$ tales que $p(x) = f(x) * g(x)$, $\partial(f) < \partial(p)$ y $\partial(g) < \partial(p)$.

En general, si R es un anillo, decimos que $a \in R$, $a \neq 1$, es irreducible si no existen $r, s \in R$, r y s no unidades, tales que $a = r * s$.

Definición 3.22. Un dominio entero R es un *dominio de factorización única* si para toda $a \in R$, $a \neq 0$, dados $p_1, ..., p_n \in R$ y $q_1, ..., q_m \in R$ elementos irreducibles tales que $a = p_1 * ... * p_n = q_1 * ... * q_m$, entonces $m = n$ y para toda q_i existe p_j tal que $q_i = u * p_j$, para alguna u unidad en R.

Teorema 3.23. *Si F es un campo, entonces el polinomio $p(x) \neq 0$ es irreducible en F si, y sólo si $\langle p(x) \rangle$ es un ideal primo de $F[x]$.*

Demostración. Supongamos que $p(x)$ es irreducible. Si $f(x), g(x) \in \langle p(x) \rangle$ entonces, $p(x)|f(x)*g(x)$. Por el Lema de Euclides 2.21 tenemos que $p(x)|f(x)$ o $p(x)|g(x)$, por lo cual, $f(x) \in \langle p(x) \rangle$ o $g(x) \in \langle p(x) \rangle$. Por lo tanto, $\langle p(x) \rangle$ es un ideal primo de $F[x]$.

Ahora, supongamos que $p(x)$ no es irreducible, por lo que existen polinomios $f(x), g(x) \in F[x]$ tales que $p(x) = f(x) * g(x)$ con $\partial(f) < \partial(p)$ y $\partial(g) < \partial(p)$. Por lo cual, ni $f(x)$, ni $g(x)$, pertenecen a $\langle p(x) \rangle$. Por lo tanto, $\langle p(x) \rangle$ no es un ideal primo. □

Definición 3.24. Un ideal I de un anillo R es un *ideal máximo* si es un ideal propio y no está propiamente contenido en otro ideal propio J de R.

Teorema 3.25. *Si R es dominio de ideales principales, entonces todo ideal primo I distinto a cero es un ideal máximo.*

Demostración. Sea I un ideal primo distinto a cero. Supongamos que existe un ideal $J \neq I$ tal que $I \subset J \subset R$. Ya que R es un dominio de ideales principales, existen $a, b \in R$, a y b distintos a cero, tales que $I = \langle a \rangle$ y $J = \langle b \rangle$. Ya que $a \in J$ entonces existe $r \in R$ tal que $b * r = a$, de donde $b * r \in I$. Como I es un ideal primo, ya sea $r \in I$ o $b \in I$. Si $b \in I$, entonces $J \subset I$, lo que es una contradicción. Entonces $r \in I$, de donde existe $s \in R$ tal que $r = s * a$, por lo cual $a = b * r = b * (s * a) = (b * s) * a$; por lo tanto $1 = b * s$ y $J = \langle b \rangle = R$. Por lo tanto, I es un ideal máximo. □

Teorema 3.26. *Un ideal propio I de un anillo R es un ideal máximo si, y sólo si, R/I es un campo.*

Demostración. Sea R/I un campo. Ya que R/I es un campo, todos sus elementos no cero son unidades y, por lo tanto, sus únicos ideales son $\{0\}$ y R/I. Por el Teorema de la Correspondencia (3.12), existe un mapeo inyectivo entre el conjunto de ideales principales de R/I y el conjunto de los ideales que contienen a I, $I \mapsto \{0\} \subset R/I$ y $R \mapsto R/I$. Por lo tanto, no hay

un ideal contenido propiamente entre I y R en R.

Si I es un ideal máximo, por el mapeo ya mencionado, R/I solo tiene como ideales a I y a sí mismo. Por lo tanto, por el lema 2.12, R/I es un campo. □

Corolario 3.27. *Todo ideal máximo I de un anillo R es un ideal primo.*

Demostración. Si I es un ideal máximo, entonces, por el teorema anterior, R/I es un campo. Ya que todo campo es un dominio entero (proposición 2.16), R/I es un dominio, por lo que I es un ideal primo (teorema 3.20). □

Capítulo 4

Polinomios Irreducibles

Sea F un anillo. Denotemos por x al elemento dado por $x = (c_0 = 0, c_1 = 1, c_2 = 0, ...) \in F[x]$. Notemos que $x^2 = x * x = (0, 0, 1, ...)$, ya que $c_i * c_j \neq 0$ si y sólo si $i = 1$ y $j = 1$, por lo que $c_{i+j} = c_2 = 1$. Por inducción, ya que $c_i * c_j \neq 0$ si, y sólo si, $i + j = k$ tenemos que $x^k = (c_0 = 0, c_1 = 0, ..., c_{k-1} = 0, c_k = 1, c_{k+1} = 0, ..)$. Tomando en cuenta lo anterior, podemos denotar a un polinomio $f(x) \in F[x]$ como:

$$\begin{aligned} f(x) &= (c_0, c_1, ..., c_n, 0, ...) \\ &= (c_0, 0, 0, ...) + (0, c_1, 0, 0, ...) + ... + (0, ..., 0, c_n, 0, ...) \\ &= c_0 * (1, 0, 0, ...) + c_1 * (0, 1, 0, ...) + ... + c_n * (0, ..., 0, 1, 0, ...) \\ &= c_0 + c_1 * x + ... + c_n * x^n \\ &= \sum_{i=0}^{n} c_i * x^i \end{aligned}$$

De ahora en adelante, usaremos esta notación.

Sean $f(x) = \sum_{i=0}^{n} c_i * x^i \in R[x]$ un polinomio sobre el anillo R y $r \in R$, llamamos a la evaluación del polinomio $f(x)$ en r, denotada por $f(r)$, al resultado de la suma

$$f(r) = \sum_{i=0}^{n} c_i * r^i.$$

Ejemplo 4.1. Sean R un anillo y $R[x]$ su anillo de polinomios. Consideremos a la función

$$\begin{aligned} e_s :&R[x] \to R \\ e_s :&f(x) \to f(s). \end{aligned}$$

Notemos que, para $f(x), g(x) \in R[x]$:

(i) $e_s(f(x) + g(x)) = f(s) + g(s) = e_s(f(x)) + e_s(g(x))$,

(ii) $e_s(f(x) * g(x)) = f(s) * g(s) = e_s(f(x)) * e_s(g(x))$

y

(iii) $e_s(c) = c$.

Por lo tanto, e_s es un homomorfismo de anillos, llamado el *mapeo evaluación en s*.

Proposición 4.2. *Sean R un anillo y $f(x), g(x)$ polinomios en $R[x]$ distintos a cero. Entonces:*

(i) $\partial(f + g) \leq \max\{\partial(f), \partial(g)\}$.

Además, si R es un dominio entero, tenemos que:

(ii) $\partial(f * g) = \partial(f) + \partial(g)$

Demostración. Sean $f(x) = \sum_{i=0}^{n} a_i * x^i$ y $g(x) = \sum_{j=0}^{m} b_j * x^j$ dos polinomios distintos a cero,

(i) $f(x) + g(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k) * x^k$. Si $a_{\max\{n,m\}} + b_{\max\{n,m\}} = 0$ tenemos la desigualdad; de lo contrario nos da la igualdad.

(ii) $f(x)*g(x) = \sum_{k=0}^{n+m} q_k * x^k$ donde $q_k = \sum_{i+j=k} a_i * b_j$ y, al ser R un dominio entero, tenemos que $q_{n+m} = a_n * b_n \neq 0$.

□

Ejemplo 4.3. Sea $\sigma : R \to S$ un homomorfismo de anillos, consideremos el mapeo $\sigma^* : R[x] \to S[x]$, dado por

$$\sigma^* : \sum a_i * x^i \mapsto \sum \sigma(a_i) * x^i.$$

Notemos que:

(*i*) $\sigma(a_i + b_i) * x^i = (\sigma(a_i) + \sigma(b_i)) * x^i$, por lo que $\sigma^*(f(x) + g(x)) = \sigma^*(f(x)) + \sigma^*(g(x))$.

(*ii*) $\sigma(a_i * b_j) * x^k = (\sigma(a_i) * \sigma(b_j)) * x^k$, por (i) tenemos que $\sigma^*(\sum a_i * b_j) = \sum \sigma(a_i) * \sigma(b_i)$, de donde $\sigma^*(f(x) * g(x)) = \sigma^*(f(x)) * \sigma^*(g(x))$
y

(*iii*) $\sigma^*(1) = \sigma(1) = 1_S = 1_{S[x]}$.

Por lo tanto, σ^* es un homomorfismo de anillos.

Teorema 4.4. *Sean R un dominio, F un campo y $\sigma : R \to F$ un homomorfismo de anillos. Si $\partial(\sigma^*(p(x))) = \partial(p)$ y $\sigma^*(p(x))$ es irreducible en $F[x]$, entonces, $p(x)$ no es el producto de dos polinomios $f(x), g(x) \in R[x]$, con $\partial(f), \partial(g) < \partial(p)$.*

Demostración. Supongamos que $p(x) \in R[x]$ es el producto de dos polinomios $f(x), g(x) \in R[x]$, $p(x) = f(x) * g(x)$, con $\partial(f) < \partial(p)$ y $\partial(g) < \partial(p)$. En $F[x]$, tenemos que $\sigma^*(p(x)) = \sigma^*(f(x)) * \sigma^*(g(x))$.

Si $\sigma^*(p(x))$ irreducible, entonces podemos suponer que $\partial(\sigma^*(g(x))) = 0$. De donde

$$\begin{aligned} \partial(p) &= \partial(\sigma^*(p(x))) \\ &= \partial(\sigma^*(f(x))) + \partial(\sigma^*(g(x))) \\ &= \partial(\sigma^*(f(x))) \\ &\leq \partial(f) \\ &< \partial(p) \end{aligned}$$

Lo que es una contradicción. Por lo tanto, $\sigma^*(p(x))$ no es irreducible.

□

Definición 4.5. Sea R un anillo Euclidiano (8.5). El máximo común divisor de los coeficientes de un polinomio en $R[x]$ siempre existe y es único (8.8).

Un polinomio $\sum_{i=0}^{n} a_i * x^i \in \mathbb{Z}[x]$ es llamado un polinomio *primitivo* si el máximo común divisor de sus coeficientes es 1.

Lema de Gauss 4.6. *El producto de dos polinomios primitivos $f(x), g(x) \in \mathbb{Z}[x]$ es un polinomio primitivo.*

Demostración. Supongamos que $f(x) * g(x)$ es un polinomio no primitivo, es decir, existe $p \in \mathbb{Z}$ primo que divide a todos los coeficientes de $f(x)*g(x)$. Sea $\pi : \mathbb{Z} \to \mathbb{Z}_p$ el mapeo natural (3.6). Consideremos el homomorfismo de anillos $\pi^* : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Entonces, tenemos que

$$\pi^*(f(x) * g(x)) = \pi^*(f(x)) * \pi^*(g(x)).$$

Ya que p divide a todos los coeficientes de $f(x) * g(x)$, $\pi^*(f(x) * g(x)) = 0$, por lo cual $\pi^*(f(x)) * \pi^*(g(x)) = 0$. Ya que $f(x)$ y $g(x)$ son polinomios primitivos p no divide a todos sus coeficientes, por lo cual $\pi^*(f(x)) \neq 0$ y $\pi^*(g(x)) \neq 0$. Luego, tenemos una contradicción, ya que $\mathbb{Z}_p$ es un campo por el teorema 2.27.

Por lo tanto, $f(x) * g(x)$ es un polinomio primitivo. □

Lema 4.7. *Todo polinomio $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$ tiene una factorización única de la forma*

$$f(x) = c_f * f^*(x),$$

donde $c_f \in \mathbb{Q}$, $c_f > 0$, y $f^*(x) \in \mathbb{Z}[x]$ es un polinomio primitivo.

Demostración. Sea $f(x) = \sum_{i=0}^{n} (a_i/b_i) * x^i \in \mathbb{Q}[x]$. Sean $B = b_0 * ... * b_n$ y $g(x) \in \mathbb{Z}[x]$ un polinomio tal que $g(x) = B * f(x)$. Sea d el mínimo común múltiplo de los coeficientes de $g(x)$ y definimos $D = d^*$ donde $d^* = -d$ si $-d * B > 0$ o $d^* = d$ si $d * B \geq 0$. Tenemos que $(B/D) * f(x) = (1/D) * g(x)$ es un polinomio primitivo (en $\mathbb{Z}[x]$). Si $c_f = D/B$ y $f^*(x) = (B/D) * f(x)$ tenemos la factorización deseada.

Supongamos que existe otra factorización $f(x) = e * h(x)$. Entonces, tenemos que $c_f * f^*(x) = f(x) = e * h(x)$, de donde $f^*(x) = (e/c_f) * h(x)$. Sean u y v números enteros primos relativos entre si tales que $e/c_f = u/v$. Notemos que u/v debe de ser positivo, ya que e y c_f lo son. De donde $v * f^*(x) = u * h(x)$ y v es un divisor común de los coeficientes del polinomio $u * h(x) \in \mathbb{Z}[x]$. Gracias a que $(u, v) = 1$, por el Lema de Euclides (8.10),

v es un divisor común de los coeficientes de $h(x)$ y $v = 1$ o $v = -1$, ya que $h(x)$ es primitivo. De forma análoga, $u = 1$ o $u = -1$. Por lo tanto, $e/c_f = u/v = 1$, $e = c_f$ y $f^*(x) = h(x)$. □

El número racional positivo c_f es llamado el *contenido de* $f(x)$.

Corolario 4.8. *Si* $f(x) \in \mathbb{Z}[x]$, *entonces* $c_f \in \mathbb{Z}$.

Demostración. Sea d el mínimo común múltiplo de los coeficientes de $f(x)$, entonces tenemos que $(1/d) * f(x) \in \mathbb{Z}[x]$ es un polinomio primitivo. Ya que $f(x) = d * ((1/d) * f(x))$ es un producto de un entero d y un polinomio primitivo, por 4.7, $c_f = d \in \mathbb{Z}$. □

Teorema de Gauss 4.9. *Si* $f(x) \in \mathbb{Z}[x]$ *no es el producto de dos polinomios de grado mayor a* 0, *entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$.

Demostración. Si $f(x) = g(x) * h(x) \in \mathbb{Q}[x]$, entonces existen constantes $c_g, c_h \in \mathbb{Q}$ y $g^*(x), h^*(x) \in \mathbb{Z}[x]$ polinomios primitivos tales que $f(x) = c_g * c_h * g^*(x) * h^*(x)$. Pero, por el corolario 4.8, $c_f = c_g * c_h \in \mathbb{Z}$. Por lo tanto, $f(x) = (c_f * g^*(x)) * h^*(x)$ es una factorización en $\mathbb{Z}[x]$. □

Definición 4.10. Sea $f(x) \in R[x]$ un polinomio sobre el anillo R. Una raíz de $f(x)$ es un elemento $\alpha \in S$, S un anillo que contiene a R, tal que $f(\alpha) = 0$.

Proposición 4.11. Sean $\sigma : F \to E$ un homomorfismos inyectivo de anillos, $p(x)$ un polinomio en $F[x]$. Entonces $\alpha' = \sigma(\alpha)$ es raíz del polinomio $\sigma^*(f[x])$ si, y sólo si α es una raíz de $f(x)$, donde σ^* es el homomorfismo definido en 4.3.

Demostración. Sea $f(x) = \sum_{i=0}^{n} a_i * x^i$ entonces $\sigma^*(f(x)) = \sum_{i=0}^{n} \sigma(a_i) * x^i$. Sea α una raíz de $f(x)$, entonces

$$\begin{aligned}
\sigma^*(f(x))(\alpha') &= \sum_{i=0}^{n} \sigma(a_i) * (\alpha')^i \\
&= \sum_{i=0}^{n} \sigma(a_i * \alpha^i) \\
&= \sigma(\sum_{i=0}^{n} a_i * \alpha *^i) \\
&= \sigma(0) = 0.
\end{aligned}$$

Por lo tanto, α' es raíz de $\sigma^*(f[x])$.

Por otro lado, sea α' raíz de $\sigma^*(f[x])$ entonces, al ser σ inyectiva:

$$\begin{aligned}\sigma(f(\alpha)) &= \sigma(\sum_{i=0}^{n} a_i * (\alpha)^i) \\ &= \sum_{i=0}^{n} \sigma(a_i) * (\alpha')^i \\ &= \sum_{i=0}^{n} \sigma(a_i * \alpha'^i) \\ &= \sum_{i=0}^{n} \sigma(a_i) * (\alpha' *^i) \\ &= 0.\end{aligned}$$

Por lo tanto, $f(\alpha) = 0$ y α es raíz de $f(x)$. □

Corolario 4.12. *Si F es un campo y $p(x) \in F[x]$ es irreducible, entonces el anillo cociente $F[x]/\langle p(x)\rangle$ es un campo que contiene un campo isomorfo a F y una raíz de $p(x)$.*

Demostración. Ya que $p(x)$ es irreducible, el ideal principal $I = \langle p(x)\rangle$ es un ideal primo (teorema 3.23). Como $F[x]$ es un dominio de ideales principales, I es un ideal máximo, de donde $E = F[x]/I$ es un campo (teorema 3.26).

Ahora, consideremos el mapeo $\pi : F \to F'$, donde

$$F' = \{a + I : a \in F\} \subset E,$$

dado por $\pi(a) = a + I$, que por 3.6 es un isomorfismo. Por lo cual E, contiene un subcampo isomorfo a F.

Por último, consideremos al elemento $\alpha = x + I \in E$. Sea

$$p(x) = \sum_{i=0}^{n} a_0 * x^i.$$

Entonces:

$$\begin{aligned} p(\alpha) &= a_0 + a_1 * \alpha + ... + a_n * \alpha^n \\ &= a_0 * (x+I)^0 + a_1 * (x+I) + ... + a_n * (x+I)^n \\ &= a_0 * (x^0 + I) + a_1 * (x+I) + ... + a_n * (x^n + I) \\ &= (a_0 + I) + (a_1 * x + I) + ... + (a_n * x^n + I) \\ &= (\sum_{i=0}^{n} a_0 * x^i) + I \\ &= p(x) + I = I = 0 + I, \end{aligned}$$

ya que $I = \langle p(x) \rangle$. Por lo tanto, $\alpha \in E$ es una raíz de $\pi^*(p(x))$ y, por la proposición 4.11, contiene a una raíz de $p(x)$. □

Teorema 4.13. *Sean $f(x) \in F[x]$ y $a \in F$. Entonces existe $q(x) \in F[x]$ tal que*

$$f(x) = q(x) * (x - a) + f(a).$$

Demostración. Por el algoritmo de la división (8.11), existen $q(x), r(x) \in F[x]$ tales que

$$f(x) = (x - a) * g(x) + r(x),$$

donde $r(x) = 0$ o $\partial(r) < 1 = \partial(x - a)$, $r(x)$ es una constante. Evaluando $f(x)$ en a tenemos que $f(a) = q(a) * (a - a) + r = r$. De donde r es la constante $f(a)$.

□

Corolario 4.14. *Sea $f(x) \in F[x]$. Entonces $a \in F$ es una raíz de $f(x)$ si, y sólo si, $x - a$ divide a $f(x)$.*

Demostración. Si a es una raíz de $f(x)$, entonces $f(a) = 0$. Por el teorema 4.13, tenemos que $f(x) = q(x) * (x - a)$. De manera análoga, si $f(x) = q(x) * (x - a)$, evaluando en a tenemos que $f(a) = q(a) * (a - a) = q(a) * 0 = 0$. □

Definición 4.15. El elemento $\alpha \in F$ es una *raíz de $p(x) \in F[x]$ de multiplicidad $m \in \mathbb{N}$* si $(x - \alpha)^m | p(x)$, y $(x - \alpha)^{m+1}$ no divide a $p(x)$.

Definición 4.16. El elemento $\alpha \in F$ es una *raíz n-ésima de unidad* si es raíz del polinomio $x^n - 1 \in F[x]$ para algún $n \in \mathbb{N}$. Una raíz n-ésima de unidad α es *primitiva* si $1 - \alpha^m = 0$ para $m > 0$ implica que $m \geq n$.

Lema 4.17. *Sean $n \in \mathbb{N}$ y F un campo. Entonces, todas las raíces raíces n-ésimas de la unidad en F forman un subgrupo del grupo multiplicativo de F, $(F^{\#}, *)$, donde $F^{\#} = F - \{0\}$.*

Demostración. Sea G el conjunto de todas las raíces n-ésimas de unidad. Si $a, b \in G$, entonces

(*i*) $1 - 1^n = 1 - 1 = 0$ y $1 \in G$;

(*ii*) Notemos que como $1 - a^n = 0 = 1 - b^n$ entonces $a^n = b^n = 1$ y $(a * b)^n = a^n * b^n = 1$. Por lo tanto, $a * b \in G$;

(*iii*) además, ya que $a^n = 1$, tenemos que

$$1 = 1^{-1} = (a^n)^{-1} = a^{-n} = (a^{-1})^n$$

de donde $a^{-1} \in G$;

por lo tanto, G es un subgrupo de $F^{\#}$ y, por el teorema 8.23, G es cíclico. □

Capítulo 5

Extensiones de Campos

Definición 5.1. Si F es un subcampo del campo E, entonces se dice que E es una *extensión del campo* F, y se denota por E/F. Si E, K y F son campos tales que $E \subset K \subset F$, decimos que $E \subset K \subset F$ es una *cadena de extensiones* y K es un *campo intermedio* de la extensión E/F.

Notemos que si E/F es una extensión, entonces ambos campos tienen el mismo subcampo primario.

Teorema 5.2. *Si F es un campo y $f(x) \in F[x]$ tiene grado $n \geq 0$, entonces toda extensión E/F contiene a lo más n raíces de $f(x)$.*

Demostración. Sea $f(x)$ un polinomio de grado n. Supongamos que E contiene $a_1, ..., a_{n+1}$ raíces distintas de $f(x)$. Por el corolario 4.14, $(x-a_1)|f(x)$ y existe $g_1(x) \in E[x]$ tal que $f(x) = (x-a_1)*g_1(x)$. Ya que $a_1 \neq a_2$ tenemos que $x - a_1$ y $x - a_2$ son primos relativos y, por el lema de Euclides (2.21), existe $g_2(x) \in E[x]$ tal que $f(x) = (x - a_1) * (x - a_2) * g_2(x)$. Procediendo de esta forma sucesivamente con todas las $n + 1$ raíces de $f(x)$, llegamos a que existe $g_{n+1}(x) \in E[x]$ tal que $f(x) = g_{n+1}(x) * \prod_{i=1}^{n+1}(x - a_i)$. Lo cual es una contradicción, ya que el polinomio $g_{n+1}(x) * \prod_{i=1}^{n+1}(x - a_i)$ tiene un grado mayor a $n + 1$ y $f(x)$ es de grado n.

□

Lema 5.3. *Sean L/F una extensión de campos y $\alpha \in L$, sea $p(x) \in F[x]$ un polinomio mónico irreducible en $F[x]$ con α como raíz. Entonces:*

(*i*) $\partial(p) \leq \partial(f)$ *y* $p(x)|f(x)$ *para todo* $f(x) \in F[x]$ *que posee a* α *como raíz.*

(*ii*) $p(x)$ *es el único polinomio mónico en* $F[x]$ *de grado* $\partial(p)$ *que posee a* α *como raíz.*

Demostración. Sea $I = \{q(x) \in F[x] : q(\alpha) = 0\}$. Sean $f(x) \in F[x]$ y $q(x), g(x) \in I$. Notemos que $f(\alpha) * q(\alpha) = f(\alpha) * 0 = 0$ y $q(\alpha) - g(\alpha) = 0 - 0 = 0$, de donde I es un ideal.

(*i*) Si $f(x) \in I$, entonces $d(x) = (f(x), p(x)) \in I$, ya que $d(x)$ es una combinación lineal de $f(x)$ y $p(x)$ (teorema 2.19). Como $p(x)$ es un polinomio irreducible sus únicos divisores mónicos son 1 y $p(x)$, y ya que $1(\alpha) \neq 0$, tenemos $d(x) = p(x)$ y $p(x)|f(x)$ y $\partial(p) \leq \partial(f)$.

(*ii*) Sea $q(x)$ un polinomio mónico en I tal que $\partial(q) = \partial(p)$, entonces $q(x) - p(x) \in I$. Si $p(x) - q(x) \neq 0$, entonces $\partial(p - q) > 0$ y $\partial(q - p) < \partial(p)$, lo que es una contradicción de (i).

□

Teorema 5.4. *Si* L/K *es una extensión de campos, entonces las operaciones*

$$(\lambda, u) \mapsto \lambda * u \quad (\lambda \in K, u \in L) \tag{5.5}$$

$$(u, v) \mapsto u + v \quad (u, v \in L) \tag{5.6}$$

definen en L *la estructura de un espacio vectorial sobre el campo* K*.*

Demostración. Todas las siguientes propiedades son consecuencia de que K y L son campos.

Para todos u, v, w elementos de L tenemos que:

1. $u + v = v + u$.
2. $(u + v) + w = u + (v + w)$.
3. Existe un elemento $0 \in L$ tal que $0 + u = u$ para todo $u \in L$.
4. Para cualquier $u \in L$ existe $-u \in L$ tal que $u + (-u) = 0$.

5. Si $\lambda \in K$ entonces $\lambda * (u + v) = \lambda * u + \lambda * v$.

6. Si 1_K es la unidad de K, entonces $1_K * u = u$.

7. Si $\lambda, \mu \in K$, entonces $(\lambda * \mu) * u = \lambda * (\mu * u)$.

Por lo tanto, L es un espacio vectorial sobre K. □

Definición 5.7. Se define al *grado de la extensión* L/K como la dimensión de L vista como un espacio vectorial sobre el campo K y se denota por $[L : K]$. La extensión L/K es una *extensión finita* si $[L : K]$ es un número finito.

Sea E/F una extensión de campos. Notemos que si E es un campo finito, entonces E/F es una extensión finita, ya que toda base de E/F debe de estar contenida en E.

Teorema 5.8. *Sean F un campo y $p(x) \in F[x]$ un polinomio irreducible de grado d. Entonces el anillo cociente $E = F[x]/\langle p(x)\rangle$ es una extensión de un campo isomorfo a F que contiene a una raíz de $p(x)$ y $[E : F] = d$.*

Demostración. Sean $I = \langle p(x)\rangle$ y $\alpha = x + I \in E$. Por 4.12, α es una raíz y E es una extensión de un campo F' isomorfo a F. Consideremos al conjunto $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$.

Si para toda i, $0 \leq i \leq d-1$, existen c_i, no todas 0, tales que $\sum_{i=0}^{d} c_i \alpha^i = 0$ entonces α es una raíz del polinomio en E dado por $f(x) = \sum_{i=0}^{d} c_i x^i$ con $\partial(f) < d$, lo que es una contradicción del lema 5.3. Por lo tanto, $\{1, ..., \alpha^{d-1}\}$ es linealmente independiente.

Sea $s \in E$. Existe $f(x) \in F[x]$ tal que $s = f(x) + I$. Por el algoritmo de la división (8.11), existen polinomios $q(x), r(x) \in F[x]$ tales que $f(x) = q(x) * p(x) + r(x)$, con $\partial(r) < \partial(p) = d$, de donde $s = f(x) + I = r(x) + I$ y el conjunto $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ genera a E.

Por lo tanto, $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ es un base de E sobre F' y $E = F[x]/\langle p(x)\rangle$ es una extensión del campo F' de grado d.

□

Definición 5.9. Sean L/K una extensión de campos y $\alpha_1, ..., \alpha_n \in L$. Llamamos a la intersección de todos los subcampos que contienen al conjunto $\{\alpha_1, ..., \alpha_n\}$ y a K *el campo obtenido al adjuntar* $\{\alpha_1, ..., \alpha_n\}$ *a* K. Se denota como $K(\alpha_1, ..., \alpha_n)$.

Una extensión L/K se dice que es una *extensión simple* si se obtiene al adjuntar un solo elemento a K, esto es:

$$K = L(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in K[x] \text{ y } g(\alpha) \neq 0\}$$

Proposición 5.10. *Sean E/F una extensión de campos y $\alpha, \beta \in E$. Entonces,*

$$F(\alpha, \beta) = F(\alpha + \beta, \beta). \tag{5.11}$$

Demostración. Claramente, $\alpha + \beta \in F(\alpha, \beta)$. Al ser $F(\alpha + \beta, \beta)$ el campo más pequeño que contiene a $\alpha + \beta$ y a β, por definición, tenemos que $F(\alpha + \beta, \beta) \subset F(\alpha, \beta)$. Por otro lado, tenemos que $\alpha = (\beta + \alpha) - \beta$, por lo cual, $\alpha \in F(\alpha + \beta, \beta)$ y $F(\alpha, \beta) \subset F(\alpha + \beta, \beta)$. Por lo tanto, $F(\alpha, \beta) = F(\alpha + \beta, \beta)$.

□

Definición 5.12. Sean L/K una extensión de campos y $\alpha \in L$. Se dice que α *es algebraico sobre* K si α es raíz de algún polinomio no cero en $K[x]$; de lo contrario decimos que α *es trascendental sobre* K.

Una extensión L/K es una *extensión algebraica* si todo elemento $\alpha \in L$ es algebraico sobre K.

Un campo F es *algebraicamente cerrado* si para todo $f(x) \in F[x]$ con $\partial(f) \geq 1$, $f(x)$ tiene una raíz $\alpha \in F$. Sea E/F una extensión de campos. Decimos que E es la *cerradura algebraica de* F, denotada por $\overline{F} = E$, si E es algebraicamente cerrado y ningún subcampo intermedio de la extensión lo es.

Teorema 5.13. *Si L/K es una extensión finita, entonces es una extensión algebraica.*

Demostración. Sean $[L : K] = n$ y $\alpha \in L$. En cualquier espacio vectorial de dimensión n, cualquier conjunto de más de n vectores es linealmente

dependiente. Por lo tanto, existen escalares $c_i \in K$, $0 \leq i \leq n$ y $c_i \neq 0$ para alguna i, tales que:

$$\sum_{i=0}^{n} c_i \alpha^i = 0$$

por lo cual, existe un polinomio distinto de cero en $K[x]$ con α como raíz, por lo tanto α es algebraico sobre K para toda $\alpha \in L$ y L/K es una extensión algebraica. □

Teorema 5.14. *Sea L/K una extensión de campos, y sea $\alpha \in L$ un elemento algebraico sobre K. Entonces:*

(*i*) *Existe un polinomio mónico irreducible $p(x) \in K[x]$ que tiene a α como raíz.*

(*ii*) *$K[x]/\langle p(x)\rangle \cong K(\alpha)$; existe un isomorfismo*

$$\Phi : K[x]/\langle p(x)\rangle \to K(\alpha)$$

que deja fijo a K en $K[x]/\langle p(x)$, K identificado con su imagen bajo el mapeo natural π, con

$$\Phi(x + \langle p(x)\rangle) = \alpha.$$

(*iii*) *$p(x)$ es el único polinomio mónico de grado mínimo en $K[x]$ que tiene a α como raíz.*

(*iv*) *$[K(\alpha) : K] = \partial(p)$, es decir, el grado de la extensión $K(\alpha)/K$ es igual al grado del polinomio mónico único $p(x)$ que tiene a α como raíz.*

Demostración. (*i*) Sea $\varphi : K[x] \to L$ el mapeo dado por $f(x) \mapsto f(\alpha)$. Notemos que φ es un homomorfismo de anillos, ya que es la restricción del mapeo evaluación $e_\alpha : L[x] \to L$ en $K[x] \subset L[x]$. Ya que α es algebraico, $ker\varphi$ es un ideal, diferente de $\{0\}$, en $K[x]$; ya que $K[x]$ es un dominio de ideales principales (teorema 2.14), $ker\varphi = \langle p(x)\rangle$ para algún polinomio mónico $p(x) \in K[x]$. Como K es un campo, $img\varphi$ es un dominio. Por el primer teorema de isomorfismos (3.12), $K[x]/ker\varphi \cong img\varphi$, de donde $ker\varphi = \langle p(x)\rangle$ es un ideal primo (teorema 3.20). Por lo tanto, por el teorema 3.23, $p(x)$ es polinomio irreducible en $K[x]$.

(*ii*) El primer teorema de isomorfismos nos dice que el mapeo

$$\Phi : K[x]/\langle p(x)\rangle \to img\varphi,$$

dado por $f(x)+\langle p(x)\rangle \mapsto f(\alpha)$, es un isomorfismo de anillos; de donde, para el polinomio x, $\Phi : x + \langle p(x)\rangle \mapsto \alpha$ y $\Phi : c + \langle p(x)\rangle \mapsto c$ para $c \in K$. Por lo que podemos decir que Φ deja fijo a K bajo π, esto es $\Phi(\pi(k)) = k$ para toda $k \in K$.

Finalmente, $img\varphi = img\Phi = \{f(\alpha) : f(x) \in K[x]\}$ es un subcampo de L, ya que $p(x)$ es irreducible (corolario 4.12). Notemos que $img\Phi$ está contenido en cualquier campo que contenga a K y α, por lo que $img\Phi = K(\alpha)$.

(*iii*) Está dado por el lema 5.3, inciso (*ii*).

(*iv*) Por el teorema 5.8, ya que $K[x]/\langle p(x)\rangle \cong K(\alpha)$, tenemos que $[K(\alpha) : K] = \partial(p)$.

□

Definición 5.15. El polinomio $p(x)$ dado por el teorema 5.14 es llamado *polinomio irreducible de α sobre K*.

Definición 5.16. Decimos que un polinomio *se descompone o separa* en un campo E si es el producto de factores lineales (polinomios de grado 1) con coeficientes en E. Un *campo de descomposición* del polinomio $f(x) \in F[x]$ es una extensión de campos E/F en la cual $f(x)$ se descompone, y no se descompone en ningún subcampo propio de E.

Notemos que $f(x)$ se descompone sobre F si, y sólo si, F contiene todas las raíces de $f(x)$ (corolario 4.14).

Lema 5.17. *Si $F \subset K \subset E$ es una cadena de extensiones y el grado de las extensiones $[E : K]$ y $[K : F]$ es finito, entonces la extensión E/F es finita y*

$$[E : F] = [E : K] * [K : F].$$

Demostración. Sea $\{\alpha_1, ..., \alpha_n\}$ una base para la extensión E/K, y sea $\{\beta_1, ..., \beta_m\}$ una base para K/F. Consideremos al conjunto $V = \{\beta_j * \alpha_i : 1 \leq i \leq n \text{ y } 1 \leq j \leq m\}$. Este conjunto claramente posee $[E : K] * [K : F]$ elementos.

Sea $r \in E$, entonces existen $b_1, ..., b_n$ en K tales que $r = \sum_{i=1}^{n} b_i * \alpha_i$. Además, tenemos que para cada b_i existen c_{ij} en F tales que $b_i = \sum_{j=1}^{m} c_{ij} * \beta_j$, por lo tanto, $r = \sum_{j=1}^{m} \sum_{i=0}^{n} c_{ij} * \beta_j * \alpha_i$. Por lo tanto, V genera a E.

Ahora, supongamos que $\sum_{j=1}^{m} \sum_{i=0}^{n} c_{ij} * \beta_j * \alpha_i = 0$ para alguna sucesión de c_{ij} en F. Tenemos que para $b_i = \sum_{j=0}^{m} c_{ij} * \beta_j \in K$, al ser α_i una base, $b_i = 0$ para toda i. De manera análoga, por la independencia lineal de β_j sobre F, tenemos que $c_{ij} = 0$ para toda i, j. Por lo tanto, V es linealmente independiente y una base de E/F. □

Proposición 5.18. *Sea E/F una extensión de campos. El subconjunto*

$$K = \{\alpha \in E : \alpha \text{ es algebraica sobre } F\}$$

es un subcampo de E que contiene a F y la extensión K/F es una extensión algebraica.

Demostración. Trivialmente, 0 y 1 son algebraicos. Sean α y β dos elementos de K y $f(x), g(x)$ dos polinomios mónicos irreducibles en F que tienen a α y β como raíces respectivamente, además $\partial(f) = d$ y $\partial(g) = d'$. Entonces, por el lema 5.17, tenemos que $[F(\alpha, \beta) : F] \leq [F(\alpha), F] * [F(\beta), F] = d * d'$. Por lo tanto, la extensión $F(\alpha, \beta)/F$ es finita. Por el teorema 5.13, la extensión $F(\alpha, \beta)/F$ es algebraica. Luego, $\alpha * \beta$ y $\alpha + \beta$ son algebraicos. Además, notemos que $\alpha^{-1} \in F(\alpha)$, de donde α^{-1} es algebraica y $\alpha^{-1} \in K$. □

Teorema de Kronecker 5.19. *Sea $f(x) \in F[x]$ con $\partial(f) = n$, donde F es un campo. Existe un campo E que contiene a F donde $f(x)$ se descompone tal que $[E : F] \leq n!$.*

Demostración. Por inducción sobre n. Si $\partial(f) = 1$, entonces $f(x)$ es lineal y $E = F$. Supongamos que, para todo $f(x) \in F[x]$ tal que $\partial(f) \leq n$, existe un campo que contiene a F en el cual $f(x)$ se descompone.

Sea $f(x) \in F[x]$ tal que $\partial(f) > n$. El teorema 5.8 nos da un campo K que contiene a F y a una raíz $\beta \in K$ de $p(x)$, con $[K : F] = n$. Por lo tanto, existe $h(x) \in K[x]$ tal que $p(x) = (x - \beta) * h(x)$ en $K[x]$. Por hipótesis de inducción, existe un campo E que contiene a K en el cual $h(x)$ se descompone. Por lo tanto, $f(x)$ se descompone en E y

$$[E : F] = [E : K] * [K : F] \leq (n - 1)!n = n!.$$

□

Teorema 5.20. *Si F es un campo, entonces todo polinomio $f(x) \in F[x]$ tiene un campo de descomposición E.*

Demostración. Por el teorema 5.19, existe una extensión de campos K/F en el cual $f(x)$ se descompone. Sean $\alpha_1, \alpha_2, ..., \alpha_k$ todas las raíces de $f(x)$ en K. Definimos al campo E como $E = F(\alpha_1, \alpha_2, ..., \alpha_k)$. Por construcción, E contiene a todas las raíces de $f(x)$ y al campo F, además es el menor campo con esta propiedad. □

Sean F un campo, $p(x)$ un polinomio en $F[x]$ y E un campo de descomposición de $p(x)$. Notemos que, por los teoremas 5.19 y 5.13, la extensión $[E : F]$ es una extensión algebraica.

Lema 5.21. *Sean $\sigma : F \to F'$ un isomorfismo entre los campos F y F' y $\sigma^* : F[x] \to F'[x]$ el isomorfismo definido en 4.3. Sean $p(x) \in F[x]$ un polinomio irreducible y $p^*(x) = \sigma^*(p(x)) \in F'[x]$.*

Si β es una raíz de $p(x) \in F[x]$ en alguna extensión E de F y β' es una raíz de $p^*(x) \in F[x]$ en alguna extensión E' de F, entonces existe un isomorfismo único $\hat{\sigma} : F(\beta) \to F'(\beta')$ que extiende a σ tal que $\hat{\sigma}(\beta) = \beta'$.

Demostración. El isomorfismo $\sigma : F \to F'$ nos transporta el ideal $\langle p(x) \rangle$ en el ideal $\langle p^*(x) \rangle$ (proposición 3.13). Consideremos al isomorfismo (proposición 3.10) $\sum : F[x]/\langle p(x) \rangle \to F'[x]/\langle p^*(x) \rangle$ dado por $f(x) + \langle p(x) \rangle \mapsto \sigma^*(f(x)) + \langle p^*(x) \rangle$. Definimos a $\hat{\sigma}$ como la composición de funciones

$$F(\beta) \xrightarrow{\phi^{-1}} F[x]/\langle p(x) \rangle \xrightarrow{\sum} F'[x]/\langle p^*(x) \rangle \xrightarrow{\phi} F'(\beta').$$

Donde $\phi(f(x) + \langle p(x) \rangle) = f(\beta)$ es el isomorfismo dado por el teorema 5.14. Al ser composición de isomorfismos, $\sum$ es un isomorfismo.

Ahora, supongamos que existe un isomorfismo $\hat{\sigma}'$ que extiende a σ tal que $\hat{\sigma}'(\beta) = \beta'$. Sea $s \in F(\beta)$, entonces existen $f(x) = \sum_{i=0}^{n} a_i * x^i$ y $g(x) = \sum_{j=0}^{m} b_j * x^j$ en $F[x]$ tales que $s = f(\beta)/g(\beta)$. Luego

$$\begin{aligned}
\hat{\sigma}'(s) &= \hat{\sigma}'((\sum_{i=0}^{n} a_i * \beta^i) * (\sum_{j=0}^{m} b_j * \beta^j))^{-1} \\
&= (\sum_{i=0}^{n} \hat{\sigma}'(a_i * \beta^i)) * (\sum_{j=0}^{m} \hat{\sigma}'(b_j * \beta^j))^{-1} \\
&= (\sum_{i=0}^{n} a_i * \beta'^i) * (\sum_{j=0}^{m} b_j * \beta'^j)^{-1} \\
&= (\sum_{i=0}^{n} \hat{\sigma}(a_i) * \hat{\sigma}(\beta^i)) * (\sum_{j=0}^{m} \hat{\sigma}(b_j) * \hat{\sigma}(\beta^j))^{-1} \\
&= \hat{\sigma}(s).
\end{aligned}$$

Por lo tanto, el homomorfismo es único. □

Definición 5.22. Sea $f(x) \in F[x]$ un polinomio con una factorización en polinomios irreducibles, no necesariamente distintos, de la forma

$$f(x) = a * p_1(x) * ... * p_m(x)$$

con $a \in F$. Decimos que $f(x)$ *es separable* si para cada $p_i(x)$, toda raíz es de multiplicidad 1. Campos en los cuales todo polinomio no constante es separable son llamados campos *perfectos*.

Definición 5.23. Si E/F es una extensión de campos, un elemento algebraico $\alpha \in E$ es llamado *separable* si su polinomio irreducible es separable. Una extensión algebraica L/K es una extensión separable si para toda $\alpha \in L$, α es separable.

Lema 5.24. *Sea E/F una extensión algebraica separable y sea K un campo intermedio entre E y F formando la cadena de extensiones $E \supset K \supset F$. Entonces las extensiones E/K y K/F son separables.*

Demostración. Claramente, K/F es una extensión separable, al ser K subconjunto de E.

Sean $\alpha \in E$ y $p_F(x)$, $p_K(x)$ los polinomio mónicos irreducibles con α como raíz (teorema 5.14) en $F[x]$ y $K[x]$ respectivamente. Notemos que, por el lema 5.3 $p_K(x)|p_F(x)$ en $K[x]$. Pero α es separable sobre F, por lo que $p_F(x)$ es separable sobre F, de donde, $p_K(x)$ es separable sobre K. Por lo tanto, E/K es una extensión separable □

Lema 5.25. *Sea E/F una extensión de campos, ambos campos de característica p, y sea $\alpha \in E$ algebraico sobre F. Entonces α es separable sobre F, si y sólo si $F(\alpha^p) = F(\alpha)$.*

Demostración. Notemos que α es raíz del polinomio $(t-\alpha)^p = t^p - \alpha^p \in F(\alpha^p)[t]$, por lo que el polinomio mónico irreducible de α sobre $F(\alpha^p)$ debe dividir a $t^p - \alpha^p$ y, por lo tanto, debe de ser de la forma $(t-\alpha)^s$ para algún $s \leq p$.

Si α es separable sobre F, entonces es separable sobre $F(\alpha^p) \supset F$. Por lo tanto, el polinomio $(t-\alpha)^s$ no tiene raíces de multiplicidad mayor a 1 y $s = 1$, es decir, $t - \alpha \in F(\alpha^p)[t]$. Por lo tanto, $\alpha \in F(\alpha^p)$ y $F(\alpha^p) = F(\alpha)$.

Ahora, supongamos α no es separable sobre F. Entonces, por el corolario 8.27, su polinomio mónico irreducible debe de ser de la forma $g(x^p)$ para algún polinomio $g(x) \in F[x]$. Por el teorema 5.14, inciso (iv), tenemos que $[F(\alpha) : F] = p * \partial(g)$. Por otro lado, tenemos que α^p es raíz del polinomio $g(x)$, entonces $[F(\alpha^p) : F] = \partial(g)$ y $[F(\alpha^p) : F] < [F(\alpha) : F]$. Por lo tanto, $F(\alpha^p) \neq F(\alpha)$. □

Teorema 5.26. Sea E/F una extensión de campos. Consideremos al conjunto

$$E_s = \{a \in E : a \text{ es separable sobre } F\}.$$

Entonces, el conjunto E_s es un campo y la extensión E_s/F es una extensión separable.

Demostración. Sean $\alpha, \beta \in E_s$. Por la proposición 5.18 tenemos que $\alpha+\beta$ y $\alpha * \beta$ son algebraicos. Sean $g(x)$, $f(x)$ y $p(x)$ los polinomios mónicos irreducibles en $F[x]$ con $\alpha+\beta$, $\alpha*\beta$ y α^{-1} como raíces respectivamente. Entonces, tenemos dos casos.

Si F es de característica 0, por el corolario 8.27, $f(x)$, $g(x)$ y $p(x)$ no tienen raíces de multiplicidad mayor a 1. Por lo tanto $\alpha+\beta$, $\alpha*\beta$ y α^{-1} pertenecen a E_s.

Ahora, supongamos que F es de característica p. Por los lemas 3.16 y 5.25 tenemos las siguientes igualdades:

$$F(\alpha^p) = F(\alpha),$$
$$F(\alpha+\beta) = F(\alpha^p+\beta^p) = F((\alpha+\beta)^p),$$
y
$$F(\alpha*\beta) = F((\alpha*\beta)^p) = F(\alpha^p*\beta^p).$$

Luego, por el lema 5.25, $\alpha+\beta$, $\alpha*\beta$ y α^{-1} son separables, y por lo tanto, pertenecen a E_s.

Finalmente, los polinomios mónicos x y $x-1$ son claramente separables y poseen a 0 y al 1 como raíces respectivamente, por lo que $0,1 \in E_s$. Por lo tanto, E_s es un subcampo de E. □

El conjunto E_s es el campo llamado la *cerradura separable de F en E*.

Lema 5.27. *Sean E/F una extensión de campos y $f(x) \in F[x]$. Si $\sigma : E \to E$ es un automorfismo que deja fijo a F, y si $\alpha \in E$ es una raíz de $f(x)$, entonces $\sigma(\alpha)$ también es una raíz de $f(x)$.*

Demostración. Sea $f(x) = \sum_{i=0}^{n} c_i * x^n$, entonces $f(\alpha) = \sum_{i=0}^{n} c_i * \alpha^n = 0$. Aplicando σ, tenemos que

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(\alpha)) \\ &= \sigma(c_0) + \sigma(c_1) * \sigma(\alpha) + ... + \sigma(c_n) * \sigma(\alpha)^n \\ &= c_0 + c_1 * \sigma(\alpha) + ... + c_n * \sigma(\alpha)^n \\ &= f(\sigma(\alpha)). \end{aligned}$$

Ya que σ deja fijo a F. Por lo tanto, $\sigma(\alpha)$ es una raíz de $f(x)$. □

Teorema 5.28. *Sea $\sigma : F \to F'$ un isomorfismo de campos. Sea, para $f(x) \in F[x]$, el polinomio $f^*(x) = \sigma^*(f(x))$ (ejemplo 4.3) una correspondencia entre polinomios de $F[x]$ y $F'[x]$; sean E un campo de descomposición de $f(x)$ sobre F y E' un campo de descomposición de $f^*(x)$ sobre F'. Entonces:*

(*i*) *Existe un isomorfismo $\tilde{\sigma} : E \to E'$ que extiende a σ.*

(*ii*) *Si $f(x)$ es separable, entonces σ tiene exactamente $[E : F]$ número de $\tilde{\sigma}$ extensiones.*

Demostración. (*i*) Si $[E : F] = 1$, entonces $E = F$ y F es un campo de descomposición de $f(x)$; por lo cual, $f(x)$ es producto de factores lineales de $F[x]$. Al ser σ un isomorfismo, $f^*(x)$ es también el producto de factores lineales en $F'[x]$, por lo cual, F' es campo de descomposición de $f^*(x)$ y $E' = F'$. Definimos a $\tilde{\sigma}$ como $\tilde{\sigma} = \sigma$.

Ahora, supongamos que $[E : F] > 1$. Podemos elegir un factor irreducible $p(x)$ de $f(x)$ tal que $\partial(p) \geq 2$ y con β como raíz. Claramente, β debe de ser raíz de $f(x)$ y, por ende, $\beta \in E$. Sean $p^*(x)$ su polinomio correspondiente y β' una raíz de $p^*(x)$, por el lema 5.21, existe un isomorfismo único $\hat{\sigma} : F(\beta) \to F'(\beta')$ que extiende a σ, además $\hat{\sigma}(\beta) = \beta'$. Tenemos que E es un campo de descomposición de $f(x)$ sobre $F(\beta)$ y E' es un campo de descomposición de $f^*(x)$ sobre $F'(\beta')$. Tenemos que el grado de la extensión $[E : F]$ es $[E : F] = [E : F(\beta)] * [F(\beta) : F]$, y ya que $[F(\beta) : F] \geq 2$, tenemos que $[E : F(\beta)] < [E : F]$. Por inducción sobre $[E : F]$, existe $\tilde{\sigma} : E \to \ : E'$ que extiende a $\hat{\sigma}$ que a su vez extiende a σ.

(*ii*) Si $[E : F] = 1$, entonces $E = F$ y únicamente existe una extensión de $\tilde{\sigma}$, $\tilde{\sigma} = \sigma$. Supongamos que $[E : F] > 1$, sea $f(x) = p(x) * g(x)$ donde $p(x)$ es un polinomio irreducible de grado d. Si $d = 1$ entonces empezamos de nuevo con $g(x)$ en vez de $f(x)$ (Notemos que tenemos que llegar a un polinomio irreducible con grado mayor a 1, ya que $[E : F] > 1$). Supongamos que $d > 1$. Sea β una raíz de $p(x)$. Si $\tilde{\sigma}$ es una extensión de σ en E, entonces $\tilde{\sigma}(\beta) = \beta'_i$ es una raíz de $p^*(x)$. Ya que $f^*(x)$ es separable en E', $p^*(x)$ tiene exactamente d número de β'_i raíces en E'; por el lema 5.21, existen d número de $\hat{\sigma}_i : F(\beta) \to F'(\beta'_i)$ que extienden a σ. Ahora, tenemos que E es un

campo de descomposición de $f(x)$ sobre $F(\beta)$ y E' es un campo de descomposición de $f^*(x)$ sobre $F'(\beta_i')$. Ya que $[E:F] = d*[E:F(\beta)]$, $[E:F(\beta)] = [E:F]/d$, por inducción sobre $[E:F]$, para cada uno de los $\hat{\sigma}_i$ isomorfismos, $1 \leq i \leq d$, $\hat{\sigma}_i$ tiene exactamente $[E:F]/d$ extensiones en E. Entonces, tenemos que para cada ϕ homomorfismo que extienda a σ, $\phi|_{F(\beta)} = \hat{\sigma}_i$ para alguna i. Por lo tanto, σ tiene $[E:F]$ número de $\tilde{\sigma}$ extensiones.

□

Corolario 5.29. *Sea $f(x) \in F[x]$. Cualesquiera dos campos de descomposición de $f(x)$ sobre F son isomorfos por un isomorfismo que deja fijo a F.*

Demostración. En el primer inciso del teorema 5.28, elegimos $F = F'$ y a σ como el isomorfismo identidad. □

Definición 5.30. Sea E/F una extensión de campos. Consideremos el conjunto dado por

$$Gal(E/F) = \{\sigma : E \to E : \sigma \text{ es un automorfismo que deja fijo a } F\}$$

y la operación binaria composición, '$\circ$'. Sean $f, g \in Gal(E/F)$ y $a \in F$, entonces:

(*i*) $I \circ f = f \circ I = f$ donde $I \in Gal(E/F)$ es el automorfismo identidad en E.

(*ii*) $f \circ g(a) = f(g(a)) = f(a) = a$. Por lo tanto $f \circ g \in Gal(E/F)$.

(*iii*) Ya que f es un isomorfismo, existe f^{-1} tal que $f \circ f^{-1}$ es un automorfismo y $f \circ f^{-1} = I$. De donde $f^{-1}(f(a)) = a$ y $f^{-1}(a) = a$. Por lo tanto, $f^{-1} \in Gal(E/F)$.

Por (*i*), (*ii*) y (*iii*) tenemos que $(Gal(E/F), \circ)$ es un grupo, llamado el Grupo de Galois de la extensión E/F.

Teorema 5.31. *Si $f(x) \in F[x]$ es un polinomio separable y E es su campo de descomposición, entonces*

$$|Gal(E/F)| = [E:F].$$

Demostración. Usando el teorema 5.28 inciso (ii), si tomamos $F' = F$, $E' = E$ y $\sigma = I : F \to F'$ entonces hay exactamente $[E : F]$ automorfismos de E que dejan fijo a F. □

Lema 5.32. *Sean $F \subset K \subset E$ extensiones de campo, donde K es el campo de descomposición de un polinomio $f(x) \in F[x]$. Si $\sigma \in Gal(E/F)$, entonces $\sigma|_K \in Gal(K/F)$.*

Demostración. Sean $\alpha_1, ..., \alpha_n$ todas las raíces distintas de $f(x)$, de donde tenemos que $K = F(\alpha_1, ..., \alpha_n)$. Ya que $\sigma(F) = F$, por el lema 5.27, tenemos que para toda α_i, $\sigma(\alpha_i)$ es raíz de $f(x)$ y, por ser K el campo de descomposición de $f(x)$, $\sigma(\alpha_i) \in K$. Entonces, tenemos que

$$\sigma(K) = \sigma(F(\alpha_1, ..., \alpha_n)) = F(\sigma(\alpha_1), ..., \sigma(\alpha_n)) = K.$$

Y, ya que σ deja fijo a F, $\sigma|_K \in Gal(K/F)$. □

Lema 5.33. *Sea K/F una extensión finita, entonces existe una extensión E/F tal que E es un campo de descomposición para algún polinomio $f(x) \in F[x]$; con K como campo intermedio.*

Demostración. Si K/F es una extensión finita, entonces es una extensión algebraica (teorema 5.13), por lo que existen $\{\alpha_1, ..., \alpha_n\} \subset K$ tales que $F(\alpha_1, ..., \alpha_n) = K$; y cada α_i tiene un polinomio irreducible $p_i(x)$ que tiene a α_i como raíz.

Sea $f(x) = \prod_{i=0}^{n} p_i(x)$. Por el teorema de Kronecker (5.19) existe un campo de descomposición E de $f(x)$ que contiene a $F(\alpha_1, ..., \alpha_n) = K$. □

Teorema 5.34. *Sean $F \subset K \subset E$ extensiones de campos tales que la extensión K/F es el campo de descomposición de un polinomio $f(x) \in F[x]$ y E/F es el campo de descomposición de un polinomio $g(x) \in F[x]$. Entonces el grupo $Gal(E/K)$ es un subgrupo normal (8.16) de $Gal(E/F)$, y*

$$Gal(E/F)/Gal(E/K) \cong Gal(K/F).$$

Demostración. Consideremos el homomorfismo

$$\begin{aligned} \psi : &Gal(E/F) \to Gal(K/F) \\ &\sigma \mapsto \sigma|_K. \end{aligned}$$

Por el lema 5.32, está bien definido. Sean $\sigma_1, \sigma_2 \in Gal(E/F)$ y $a \in K$, entonces

(i)

$$\begin{aligned}\psi(\sigma_1 \circ \sigma_2)(a) &= (\sigma_1 \circ \sigma_2)|_K(a) \\ &= (\sigma_1 \circ \sigma_2)(a) \\ &= \sigma_1(\sigma_2(a)) \\ &= \sigma_1|_K(\sigma_2|_K(a)) \\ &= (\psi(\sigma_1) \circ \psi(\sigma_2))(a)\end{aligned}$$

por lo que ψ es un homomorfismo de grupos.

Si $\psi(\sigma) = I_K$, entonces, para toda $a \in K$, $\sigma(a) = \sigma|_K(a) = a$ y σ es un automorfismo de E que deja fijo a K, es decir $\sigma \in Gal(E/K)$ y $ker\psi \subset Gal(E/K)$. Ahora, si $\sigma \in Gal(E/K)$ entonces, para toda $a \in K$, $a = \sigma|_K(a) = \sigma(a)$ de donde $\psi(\sigma) = I_K$ y $ker\psi = Gal(E/K)$. Por el Primer Teorema de Isomorfismos para grupos (8.19), $Gal(E/K)$ es un subgrupo normal de $Gal(E/F)$.

Sea $\tau \in Gal(K/F)$. Por el teorema 5.28, ya que E y K son campo de descomposición de $f(x), g(x) \in F[x]$ respectivamente, existe un automorfismo $\hat{\tau}$ en E que extiende a τ y $\psi(\hat{\tau}) = \tau$. Por lo tanto, ψ es suprayectiva y $img\psi = Gal(K/F)$. Por Primer Teorema de Isomorfismos para grupos (8.19) tenemos que $Gal(E/F)/Gal(E/K) \cong Gal(K/F)$. $\square$

Capítulo 6

El Teorema Fundamental de la Teoría de Galois

Definición 6.1. Sean G un grupo, F un campo y $F^{\#} = F - \{0\}$ el grupo multiplicativo $(F^{\#}, *_F)$. *Un carácter* del grupo G en F es un homomorfismo de grupos $\sigma : G \to F^{\#}$.

Definición 6.2. Sea E un campo. Consideremos al conjunto

$$V(G, E) = \{\sigma : \sigma \text{ es una función de } G \text{ en } E\}.$$

Las operaciones

$$\begin{aligned} + :& V(G,E) \times V(G,E) \to V(G,E) \\ & (\sigma, \tau) \mapsto (\sigma + \tau) \\ \text{y} & \\ * :& E \times V(G,E) \to V(G,E) \\ & (c, \sigma) \mapsto (c * \sigma), \end{aligned}$$

donde $(\sigma + \tau)(x) = \sigma(x) + \tau(x)$ y $(c * \sigma)(x) = c * \sigma(x)$ para toda $x \in G$, definen en $V(G, E)$ la estructura de un espacio vectorial sobre E. Decimos que el conjunto $\{\sigma_1, ...\sigma_n\} \subset V(G, E)$ es *independiente* si es linealmente independiente.

Lema 6.3. Sean G un grupo y F un campo. Todo conjunto $\{\sigma_1, ..., \sigma_m\}$ de σ_i caracteres distintos de G en F es independiente.

Demostración. Sea $\{\sigma_1, ..., \sigma_m\}$ un conjunto de σ_i caracteres. Si $n = 1$, entonces $a_1 * \sigma_i(x) = 0$ implica que $a_1 = 0$ y $\{\sigma_1\}$ es linealmente independiente. Supongamos que la proposición es cierta para m.

Sea $n > m$. Supongamos que existen $a_1, ..., a_n \in F$, no todas cero y con $a_n = 1$, tales que, para toda $x \in G$,

$$a_1 * \sigma_1(x) + ... + 1 * \sigma_n(x) + a_n * \sigma_n(x) = 0 \text{ para toda } x \in G.$$

Podemos suponer que $a_i \neq 0$ para toda i, de lo contrario, podemos aplicar la hipótesis de inducción. Ya que, para toda $i \neq j$, $\sigma_i \neq \sigma_j$ existe $y \in G$ donde $\sigma_n(y) \neq \sigma_1(y)$. Entonces, evaluando en $x * y$ tenemos

$$\begin{aligned} 0 &= a_1 * \sigma_1(y * x) + ... + 1 * \sigma_n(y * x) \\ &= a_1 * \sigma_1(y) * \sigma_1(x) + ... + 1 * \sigma_n(y) * \sigma_n(x) \end{aligned}$$

multiplicando por el inverso de $\sigma_n(y)$:

$$\begin{aligned} 0 =& a_1 * \sigma_1(y) * \sigma_1(x) * \sigma_n(y)^{-1} + ... + a_{n-1} * \sigma_{n-1}(y) * \sigma_{n-1}(x) * \sigma_n(y)^{-1} \\ &+ (1) * \sigma_n(x) \end{aligned}$$

De donde,

$$\begin{aligned} 0 =& (a_1 * \sigma_1(x) + ... + 1 * \sigma_n(x)) \\ &- (a_1 * \sigma_1(y) * \sigma_1(x) * \sigma_n(y)^{-1} + ... + \sigma_n(x)) \\ =& a_1 * [1 - \sigma_n(y)^{-1} * \sigma_1(y)] * \sigma_1(x) + ... + 1 * [\sigma_n(x) - \sigma_n(x)] \\ =& a_1 * [1 - \sigma_n(y)^{-1} * \sigma_1(y)] * \sigma_1(x) + ... \\ &+ a_{n-1} * [1 - \sigma_n(y)^{-1} * \sigma_{n-1}(y)] * \sigma_{n-1}(x). \end{aligned}$$

Ahora, por hipótesis de inducción, cada coeficiente es igual a 0. Ya que $a_i \neq 0$, tenemos que $1 - \sigma_n(y)^{-1} * \sigma_1(y) = 0$ de donde $\sigma_n(y)^{-1} * \sigma_1(y) = 1$ y $\sigma_n(y) = \sigma_1(y)$ lo que es una contradicción. Por lo tanto, $a_i = 0$ y el conjunto es independiente. □

Corolario 6.4. *Todo conjunto $\{\sigma_1, ..., \sigma_n\}$ de σ_i automorfismos distintos en un campo F es independiente.*

Demostración. Consideremos el grupo multiplicativo de F, $F^\# = F - \{0\}$. Notemos que si $\sigma_i \neq \sigma_j$ entonces $\sigma_i|_{F^\#} \neq \sigma_j|_{F^\#}$. Luego, para toda i, $\sigma_i|_{F^\#} : F^\# \to F^\#$ es un homomorfismo de grupos y $\sigma_i|_{F^\#}$ es un carácter. Por 6.3, el conjunto $\{\sigma_1|_{F^\#}, ..., \sigma_n|_{F^\#}\}$ es independiente y, por lo tanto $\{\sigma_1, ..., \sigma_n\}$ también lo es. □

Teorema 6.5. Si E/F es una extensión finita, entonces $Gal(E/F)$ es un grupo finito y su orden $|Gal(E/F)| \leq [E : F]$.

Demostración. Sean $[E : F] = n$ y $\{v_1, ..., v_n\}$ una base de E sobre F. Supongamos que existen $n + 1$ automorfismos σ_i distintos en $Gal(E/F)$. Consideremos el sistema de ecuaciones con $n + 1$ incógnitas:

$$\begin{aligned} \sigma_1(v_1) * x_1 + ... + \sigma_{n+1}(v_1) * x_{n+1} = 0 \\ ..... \\ \sigma_1(v_n) * x_1 + ... + \sigma_{n+1}(v_n) * x_{n+1} = 0. \end{aligned}$$

Ya que el sistema tiene n ecuaciones, existe una solución no trivial $(a_1, ..., a_{n+1})$ sobre E, es decir $a_i \neq 0$ para alguna i. Luego, para toda $i \leq n$,

$$\sigma_1(v_i) * a_1 + ... + \sigma_{n+1}(v_i) * a_{n+1} = 0.$$

Sea $s \in E$, entonces existen $\alpha_1, ..., \alpha_n \in F$ tales que $s = \sum_{j=1}^{n} \alpha_j * v_j$. Luego, ya que σ deja fijo a F:

$$\begin{aligned} &\sigma_1(s) * a_1 + ... + \sigma_{n+1}(s) * a_{n+1} \\ &\quad = \sigma_1(\sum_{j=1}^{n} \alpha_j * v_j) * a_1 + ... + \sigma_{n+1}(\sum_{j=1}^{n} \alpha_j * v_j) * a_{n+1} \\ &\quad = [\sum_{j=1}^{n} \sigma_1(\alpha_j * v_j)] * a_1 + ... + [\sum_{j=1}^{n} \sigma_{n+1}(\alpha_j * v_j)] * a_{n+1} \\ &\quad = \sum_{j=1}^{n} \alpha_j * \sigma_1(v_j) * a_1 + ... + \sum_{j=1}^{n} \alpha_j * \sigma_{n+1}(v_j) * a_{n+1} \\ &\quad = \sum_{i=1}^{n+1} \sum_{j=1}^{n} \alpha_j * \sigma_i(v_j) * a_i \\ &\quad = \sum_{j=1}^{n} \sum_{i=1}^{n+1} \alpha_j * \sigma_i(v_j) * a_i \\ &\quad = \sum_{j=1}^{n} \alpha_j * (\sum_{i=1}^{n+1} \sigma_i(v_j) * a_i) \end{aligned}$$

$$\begin{aligned} &= \sum_{j=1}^{n} \alpha_j * 0 \\ &= \sum_{j=1}^{n} 0 \\ &= 0. \end{aligned}$$

Lo que es una contradicción al corolario 6.4.

□

Definición 6.6. Sea $Aut(F)$ el grupo de los automorfismos $\sigma : F \to F$ en un campo F. Sea G un subgrupo de $Aut(F)$. Consideremos el conjunto

$$F^G = \{a \in F : \sigma(a) = a \text{ para toda } \sigma \text{ en } G\ \}.$$

Sean $a, b \in F^G$ y $\sigma \in G$, entonces

(i) Ya que σ es un homomorfismo, $\sigma(0) = 0$ por lo que $0 \in F^G$,

(ii) $\sigma(1) = 1$ por lo que $1 \in F^G$,

(iii) $\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$ de donde $a + b \in F^G$,

(iii) $\sigma(-a) = -a$ y $\sigma(a^{-1}) = a^{-1}$ de donde $-a, a^{-1} \in F^G$

y, por último,

(v) $\sigma(a * b) = \sigma(a) * \sigma(b) = a * b$ de donde $a * b \in F^G$;

por lo tanto F^G es un subcampo de F llamado el *campo fijo* de G en F.

Ejemplo 6.7. Sean E/F una extensión de campos y $G = Gal(E/F)$, su Grupo de Galois. Si $a \in F$ y $\sigma \in Gal(E/F)$, entonces $\sigma(a) = a$ ya que σ deja fijo a F. Por lo tanto, $a \in E^G$ y $F \subset E^G \subset E$ es una cadena de extensiones. Es decir, E^G/F y E/E^G son extensiones de campos.

Lema 6.8. *Sean E un campo y $G = \{\sigma_1, ..., \sigma_n\} \subset Aut(F)$, entonces, el grado de la extensión E/E^G es*

$$[E : E^G] \geq n.$$

Demostración. Supongamos que el lema es falso, entonces existe r tal que $[E : E^G] \leq r < n$. Sea $\{\alpha_1, ...\alpha_r\}$ una base para el espacio vectorial E/E^G. Consideremos el siguiente sistema de ecuaciones lineales con n incógnitas:

$$\begin{gathered}\sigma_1(\alpha_1) * x_1 + ... + \sigma_n(\alpha_1) * x_n = 0 \\ \sigma_1(\alpha_2) * x_1 + ... + \sigma_n(\alpha_2) * x_n = 0 \\ ..... \\ \sigma_1(\alpha_r) * x_1 + ... + \sigma_n(\alpha_r) * x_n = 0\end{gathered}$$

Ya que $r < n$ existe una solución $(x_1, ..., x_n)$ no trivial. Si $\beta \in E$ existen $b_j \in E^G$ tales que $\beta = \sum_{j=0}^{r} b_j * \alpha_j$. Multiplicando la fila i por b_i obtenemos:

$$b_i * \sigma_1(\alpha_i) * x_1 + ... + b_i * \sigma_n(\alpha_i) * x_n = 0$$

Ya que $b_i \in E^G$ tenemos que $\sigma_k(b_i) = b_i$ para toda $k \leq n$, de donde:

$$\sigma_1(b_i * \alpha_i) * x_1 + ... + \sigma_n(b_i * \alpha_i) * x_n = 0.$$

Luego, al sumar todas las filas del sistema de ecuaciones tenemos:

$$\sigma_1(\beta) * x_1 + ... + \sigma_n(\beta) * x_n = 0,$$

lo que es una contradicción al corolario 6.4. □

Teorema 6.9. *Sea E un campo. Si $G = \{\sigma_1, ..., \sigma_n\}$ es un subgrupo de $Aut(E)$, entonces*

$$[E : E^G] = |G| = n.$$

Demostración. Si $[E : E^G] \leq |G|$ entonces, por el lema 6.8, $[E : E^G] = |G|$. Supongamos que $[E : E^G] > n$. Sean $\{v_1, ..., v_{n+1}\} \subset E$ un conjunto de vectores linealmente independientes sobre E^G. Consideremos el siguiente sistema de ecuaciones con $n + 1$ incógnitas:

$$\begin{gathered}\sigma_1(v_1) * x_1 + ... + \sigma_1(v_{n+1}) * x_{n+1} = 0 \\ ..... \\ \sigma_n(v_1) * x_1 + ... + \sigma_n(v_{n+1}) * x_{n+1} = 0.\end{gathered}$$

Ya que el sistema tiene n ecuaciones, existe una solución no trivial $(x_1, ..., x_{n+1})$ sobre E. Sin perdida de generalidad, podemos elegir una solución con el menor número r de elementos distintos de cero de la forma $(a_1, ..., a_r, 0, ..., 0)$ donde $a_i \neq 0$, $r > 1$ y $a_r = 1$, reordenando el índice de los vectores v_j si es necesario. Notemos que no todos los a_i pueden pertenecer a E^G. Si todos pertenecieran a E^G tendríamos que

$$\begin{aligned} 0 &= \sigma_j(v_1) * a_1 + ... + \sigma_j(v_r) * a_r \\ &= \sigma_j(v_1 * a_1) + ... + \sigma_j(v_r * a_r) \\ &= \sigma_j(v_1 * a_1 + ... + v_r * a_r) \end{aligned}$$

y, al ser σ un isomorfismo, $v_1 * a_1 + ... + v_r * a_r = 0$ lo que es una contradicción a la independencia lineal del conjunto de vectores. Podemos suponer que a_1 no pertenece a E^G. Por lo tanto, existe σ_k tal que $\sigma_k(a_1) \neq a_1$.

En la fila j de nuestro sistema de ecuaciones tenemos

$$0 = \sigma_j(v_1) * a_1 + ... + \sigma_j(v_{r-1}) * a_{r-1} + \sigma_j(v_r).$$

Aplicando σ_k obtenemos

$$\sigma_k \circ \sigma_j(v_1) * \sigma_k(a_1) + ... + \sigma_k \circ \sigma_j(v_{r-1}) * \sigma_k(a_{r-1}) + \sigma_k \circ \sigma_j(v_r) = 0.$$

Ya que G es un grupo, $\{\sigma_k \circ \sigma_1, ..., \sigma_k \circ \sigma_n\}$ es una permutación de $\{\sigma_1, ..., \sigma_n\}$. Sea $\sigma_k \circ \sigma_j = \sigma_i$, de donde

$$\sigma_i(v_1) * \sigma_k(a_1) + ... + \sigma_i(v_{r-1}) * \sigma_k(a_{r-1}) + \sigma_i(v_r) = 0.$$

Restando esta última ecuación a la forma original de la fila i obtenemos:

$$\begin{aligned} 0 &= \sigma_i(v_1) * [a_1 - \sigma_k(a_1)] + ... + \sigma_i(v_{r-1}) * [a_{r-1} - \sigma_k(a_{r-1})] - [\sigma_i(v_r) - \sigma_i(v_r)] \\ &= \sigma_i(v_1) * [a_1 - \sigma_k(a_1)] + ... + \sigma_i(v_{r-1}) * [a_{r-1} - \sigma_k(a_{r-1})] \end{aligned}$$

donde $a_1 - \sigma_k(a_1) \neq 0$. Por lo tanto, tenemos una solución no trivial con un número de elementos diferentes a cero menor que r, lo que es una contradicción. □

Corolario 6.10. *Si G, H son subgrupos finitos de $Aut(F)$ tales que $F^G = F^H$, entonces $G = H$.*

Demostración. Sea $F^G = F^H$. Supongamos que $G \neq H$ y $|G| = n$. Podemos suponer, sin perdida de generalidad, que existe $\sigma \in H$ que no pertenece a G. Entonces, ya que σ deja a fijo a $F^H = F^G$, F^G queda fijo bajo $|G \cup \{\sigma\}| = n + 1$ elementos y $F^G \subset F^{G\cup\{\sigma\}}$, de donde $[F : F^G] \geq [F : F^{G\cup\{\sigma\}}]$. Por el lema 6.8 tenemos que $[F : F^{G\cup\{\sigma\}}] \geq n + 1$. Por otro lado, usando el teorema 6.9, tenemos que $[F : F^G] = n$.

Por lo tanto,

$$n = [F : F^G] \geq [F : F^{G\cup\{\sigma\}}] \geq n + 1$$

lo que es una contradicción. Entonces $G = H$. □

Teorema 6.11. *Sean E/F una extensión finita y $G = Gal(E/F)$ su grupo de Galois. Entonces, las siguientes condiciones son equivalentes:*

(*i*) $F = E^G$.

(*ii*) *Todo polinomio irreducible $p(x) \in F[x]$ con una raíz en E es separable y tiene todas su raíces en E, se descompone en E.*

(*iii*) *E es un campo de descomposición para algún polinomio separable $f(x) \in F[x]$.*

Demostración. Sea $p(x) \in F[x]$ un polinomio irreducible con $\alpha \in E$ como raíz. Por el teorema 6.5 $\{\sigma(\alpha) : \sigma \in G\}$ es finito, por lo cual podemos suponer que tiene la forma $\{\alpha_1 = \sigma_1(\alpha)), ..., \alpha_n = \sigma_n(\alpha)\}$. Definamos $g(x) \in E[x]$ de la forma

$$g(x) = \prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=1}^{n} a_i * x^i.$$

Supongamos (i). Notemos que, para toda $\sigma \in G$ y α_i, $\sigma(\alpha_i) = \alpha_j$ para alguna $j \leq n$ entonces $\sigma(g(x)) = g(x)$ y σ deja fijo a los coeficientes de $g(x)$. Por lo tanto, $a_1, ..., a_n \in E^G = F$ y $g(x) \in F[x]$ es un polinomio sin raíces repetidas. Ya que $p(x)$ y $g(x)$ comparten la raíz α, $(p(x), g(x)) \neq 1$. Como $p(x)$ es un polinomio irreducible, entonces $p(x)|g(x)$, de donde $p(x)$ no tiene raíces repetidas en $E[x]$ y todas sus raíces pertenecen a E. Por lo tanto, $p(x)$ es un polinomio separable con E como campo de descomposición e (i) implica (ii).

Ahora supongamos (ii). Sea $\alpha_1 \in E$ tal que no pertenezca a F. Ya que E/F es una extensión finita E/F es una extensión algebraica y existe un polinomio irreducible $p_1(x) \in F[x]$ con α_1 como raíz. Entonces, $p_1(x)$ es separable y se descompone en E, por lo que su campo de descomposición

K_1 es un subconjunto de E, $K_1 \subset E$. Si $K_1 = E$ entonces (iii). Supongamos $K_1 \neq E$, entonces existe $\alpha_2 \in E$ tal que no pertenece a K_1. Entonces, existe un polinomio mónico irreducible y separable $p_2(x) \in F[x]$ con α_2 como raíz. Sea $K_2 \subset E$ el campo de descomposición del polinomio separable $p_1(x) * p_2(x)$. Si $K_2 = E$ entonces (iii), de lo contrario reiteramos la misma construcción. Ya que E/F es una extensión finita, este proceso debe de terminar en algún momento y $K_m = E$ para alguna $m \in \mathbb{N}$. Por lo tanto, (ii) implica (iii).

Finalmente, supongamos (iii). Por el teorema 5.31, $|G| = [E : F]$. Y por teorema 6.9, $|G| = [E : E^G]$. Por lo tanto, $[E : F] = [E : E^G]$ y, ya que $F \subset E^G$, $F = E^G$. Por lo tanto, (iii) implica (i). □

Definición 6.12. Sea E/F una extensión de campos finita. Si E/F cumple con las condiciones equivalentes del teorema 6.11, decimos que es una *extensión normal o extensión de Galois.*

Notemos que por 6.5 $Gal(E/F)$ es finito, y por el teorema 6.9, si $G = Gal(E/F)$, G es un subgrupo de $Aut(E)$ y, al ser E/F una extensión de Galois, tenemos que

$$|Gal(E/F)| = [E : E^G] = [E : F]. \tag{6.13}$$

Proposición 6.14. *Si E/F es una extensión de Galois y K es un campo intermedio, entonces la extensión E/K es una extensión de Galois.*

Demostración. Ya que E/F es de Galois, entonces E es un campo de descomposición para un polinomio $f(x) \in F[x] \subset K[x]$. Por lo tanto, E es un campo de descomposición para un polinomio $f(x) \in K[x] \subset E[x]$ y E/K es una extensión de Galois. □

Definición 6.15. Sea E/F una extensión de campos finita. Sean K y B un campos intermedios de la extensión. Si existe un isomorfismo $\vartheta : K \to B$ que deja fijo a F entonces decimos que B *es un campo conjugado de* K.

Teorema 6.16. *Sea E/F una extensión de Galois, y sea K un campo intermedio de la extensión. Entonces las siguientes condiciones son equivalentes:*

(i) *K no tiene campos conjugados distintos de K.*

(ii) *Si $\sigma \in Gal(E/F)$, entonces $\sigma|_K \in Gal(K/F)$.*

(iii) *K/F es una extensión de Galois.*

Demostración. Si existe $\sigma \in Gal(E/F)$ tal que $\sigma|_K \notin Gal(K/F)$ entonces, ya que σ y $\sigma|_K$ dejan fijo a F, y $\sigma|_k$ no es un automorfismo, existe $k \in K$ tal que $\sigma(k) \notin K$. Ya que σ es un automorfismo, $\sigma|_K : K \to img(\sigma|_K)$ es un isomorfismo y existe un campo $img(\sigma|_K)$ distinto de K tal que $K \cong (\sigma|_K)$. Por lo tanto, (i) implica (ii).

Ahora supongamos (ii). Ya que la extensión K/F es finita, es una extensión algebraica y, para $\alpha \in K$ existe un polinomio $p(x) \in F[x]$ irreducible con $\alpha \in K$ como raíz. Ya que $K \subset E$ y E/F es una extensión de Galois, por el teorema 6.11, $p(x)$ es un polinomio separable y todas su raíces se encuentran en E. Sea $\alpha' \in E$ otra raíz de $p(x)$. Por el lema 5.21, tomando a $F' = F$, existe un isomorfismo $\tau : F(\alpha) \to F(\alpha')$ tal que deja fijo a F y $\tau(\alpha) = \alpha'$ y que, usando el teorema 5.28 y al E/F ser de Galois, extiende a $\sigma \in Gal(E/F)$. Por hipótesis ((ii)), $\sigma(K) = K$ y $\alpha' = \sigma(\alpha) \in \sigma(K) = K$. Por lo tanto, K contiene a todas las raíces de $p(x)$ y $p(x)$ se descompone en K. Por lo tanto, K/F es una extensión de Galois.

Por último, supongamos (iii). Entonces K es un campo de descomposición de algún polinomio $f(x) \in F[x]$, es decir $K = F(\alpha_1, ..., \alpha_n)$ donde α_i son todas las raíces de $f(x)$. Por el lema 5.27, todo homomorfismo inyectivo $\vartheta : K \to E$ que deja fijo a F debe únicamente permutar las raíces de $f(x)$. Entonces

$$\vartheta(K) = \vartheta(F(\alpha_1, ..., \alpha_n)) = F(\alpha_1, ..., \alpha_n) = K.$$

Por lo tanto, todo campo conjugado de K es K. □

Definición 6.17. Una *retícula* es un conjunto parcialmente ordenado $(L, \preceq)$ en el cual para cualquier par de elementos $a, b \in L$ existe $d \in L$ tal que $d \preceq a$ y $d \preceq b$, y existe $c \in L$ tal que $a \preceq c$ y $b \preceq c$.

El elemento d es llamado una cota inferior y se denota por $a \wedge b$; el elemento c es llamado una cota superior y se denota por $a \vee b$.

Lema 6.18. *Si L y L' son retículas y $\gamma : L \to L'$ es una biyección tal que si $a \preceq b$, tenemos que $\gamma(b) \preceq \gamma(a)$ entonces*

$$\gamma(a \vee b) = \gamma(a) \wedge \gamma(b) \text{ y } \gamma(a \wedge b) = \gamma(a) \vee \gamma(b).$$

Demostración. Notemos que $a, b \preceq a \vee b$ implica que $\gamma(a), \gamma(b) \succeq \gamma(a \vee b)$, es decir, $\gamma(a \vee b)$ es un cota inferior de $\gamma(a)$ y $\gamma(b)$. Luego, $\gamma(a) \wedge \gamma(b) \succeq \gamma(a \vee b)$. Ya que γ es suprayectiva, existe $c \in L$ tal que $\gamma(c) = \gamma(a) \wedge \gamma(b)$. Entonces, $\gamma^{-1}(\gamma(c)) = \gamma^{-1}(\gamma(a) \wedge \gamma(b))$ de donde $c = a \vee b$ y, ya que γ revierte el

orden, $a, b \preceq a \vee b$. Por lo tanto, $\sigma(a) \wedge \sigma(b) = \sigma(c) = \sigma(a) \wedge \sigma(b)$.

Ahora, $a, b \preceq a \wedge b$ implica que $\gamma(a), \gamma(b) \succeq \gamma(a \vee b)$ y, de manera análoga al desarrollo anterior, $\gamma(a \wedge b) = \gamma(a) \vee \gamma(b)$. □

Ejemplo 6.19. Sea G un grupo. Definimos al conjunto

$$Sub(G) = \{H \subset G : H \text{ es un subgrupo de } G\}$$

y en él, el orden $H \preceq K$ si $H \subset K$. Entonces $(Sub(G), \preceq)$ es una retícula tal que

$$A \vee B = \langle A \cup B \rangle \text{ y } A \wedge B = A \cap B,$$

donde $\langle A \cup B \rangle$ es la intersección de todos los subgrupos de G que contienen a $A \cup B$.

Definición 6.20. Si K y B son subcampos del campo E, el *campo composición* de K y B, denotado por $K \vee B$ es la intersección de todos los subcampos de E que contienen a K y a B.

Ejemplos 6.21. Sea E/F una extensión de campos, definamos el conjunto

$$Lat(E/F) = \{K \subset E : K \text{ es un campo intermedio } E/F\}$$

y en él, el orden $K \preceq B$ si $K \subset B$. Entonces $(Lat(E/F), \preceq)$ es una retícula tal que $K \vee B$ es la composición de los subcampos K y B.

Teorema Fundamental de la Teoria de Galois 6.22. *Sea E/F una extensión de Galois con $G = Gal(E/F)$. Entonces existe una correspondencia biyectiva entre los subgrupos de G y los campos intermedios de E/F dada por*

$$\begin{aligned} \gamma : &Sub(G) \to Lat(E/F) \\ &H \mapsto E^H. \end{aligned}$$

El isomorfismo γ revierte ordenes y tiene un inverso $\delta : Lat(E/K) \to Sub(G)$ tal que $\delta : K \mapsto Gal(E/K)$. Además, sea K un campo intermedio de la extensión E/F, y sean A, H subgrupos de $Aut(E)$. Entonces:

(i) $E^{Gal(E/K)} = K$ *y* $Gal(E/E^H) = H$.

(*ii*) *Tenemos las siguientes igualdades:*

$$\begin{aligned} E^{A\vee H} &= E^A \cap E^H; \\ E^{A\cap H} &= E^A \vee E^H; \\ Gal(E/K \vee H) &= Gal(E/K) \cap Gal(E/H); \\ Gal(E/K \cap H) &= Gal(E/K) \vee Gal(E/H). \end{aligned}$$

(*iii*) $[K : F] = [G : Gal(E/K)]$ *y* $[G : H] = [E^H : F]$ *(definido en 8.17).*

(*iv*) K/F *es una extensión de Galois si, y sólo si,* $Gal(E/K)$ *es un subgrupo normal de* G.

Demostración. Sean H y A subgrupos de G. Si $A \leq H$ entonces $A \subset H$, por lo cual $E^H \subset E^A$ y $\gamma(H) \leq \gamma(A)$. Luego, si $\gamma(A) = \gamma(H)$ entonces $E^A = E^H$ y, por el corolario 6.10, $A = H$. Finalmente, consideremos la siguiente composición de funciones:

$$Lat(E/F) \xrightarrow{\delta} Sub(G) \xrightarrow{\gamma} Lat(E/F),$$

donde δ es el mapeo dado por $K \mapsto Gal(E/K)$. Por la proposición 6.14, la extensión E/K es de Galois para todo campo intermedio K; entonces, por el teorema 6.11 tenemos que $K = E^{Gal(E/K)}$, de donde $\gamma(\delta(K)) = \gamma(Gal(E/K)) = E^{Gal(E/K)} = K$ y $\gamma \circ \delta$ es una identidad. Por lo tanto, γ es suprayectiva y γ es una biyección con δ como inverso.

Luego:

(*i*) Ya que $\gamma \circ \delta$ es la función identidad, tenemos que $K = \gamma(\delta(K)) = \gamma(Gal(E/K)) = E^{Gal(E/K)}$ y $H = \delta(\gamma(H)) = \delta(E^H) = Gal(E/E^H)$.

(*ii*) Ya que γ y δ son biyecciones que revierten el orden, por el lema 6.18, se dan las siguientes igualdades:

$$\begin{aligned} E^{A\vee H} &= \gamma(A \vee H) = \gamma(A) \wedge \gamma(H) = E^A \cap E^H; \\ E^{A\cap H} &= \gamma(A \wedge H) = \gamma(A) \vee \gamma(H) = E^A \vee E^H; \\ Gal(E/K \vee H) &= \delta(K \vee H) = \delta(K) \wedge \delta(H) = Gal(E/K) \cap Gal(E/H); \\ Gal(E/K \cap H) &= \delta(K \wedge H) = \delta(K) \vee \delta(H) = Gal(E/K) \vee Gal(E/H). \end{aligned}$$

(*iii*) Por 6.13 tenemos que

$$[K : F] = [E : F]/[E : K] = |G|/|Gal(E/K)| = [G : Gal(E/K)]. \tag{6.23}$$

Además, ya que $Gal(E/E^H) = H$, tenemos que

$$\begin{aligned}[E^H : F] &= [E : F]/[E : E^H] \\ &= |G|/|Gal(E/E^H)| \\ &= [G : Gal(E/E^H)] = [G : H].\end{aligned}$$

(*iv*) Si K/F es de Galois, por el teorema 5.34, $Gal(E/K)$ es un subgrupo normal de G. Ahora, supongamos que H es un subgrupo normal de G. Sean $\sigma \in G$, $\tau \in H$ y $\alpha \in E^H$. Ya que H es normal, $\tau \circ \sigma(\alpha) = \sigma \circ \tau'$ para algún $\tau' \in H$; además $\sigma \circ \tau'(\alpha) = \sigma(\alpha)$ ya que τ' deja fijo a α. Por lo tanto, $\alpha \in E^H$ implica que $\sigma(\alpha) \in E^H$ y $\sigma(E^H) \subset E^H$. Luego, $\sigma(E^H) = E^H$ ya que ambos tienen la misma dimensión sobre F. Entonces, por el teorema 6.16, E^H/F es una extensión de Galois.

□

Corolario 6.24. *Una extensión de Galois E/F únicamente tiene un número finito de campos intermedios.*

Demostración. Por 6.5, el grupo $Gal(E/F)$ es finito y, por lo tanto, posee únicamente un número finito de subgrupos. □

Lema 6.25. *Si F es un campo finito de característica p, entonces $F^\#$ es un grupo cíclico y existe α tal que $F = \mathbb{Z}_p(\alpha)$.*

Demostración. Sea $|F| = q$. Ya que F es finito, $F^\#$ es un grupo finito y, por el teorema 8.23, es un grupo cíclico. Ahora, ya que F es de característica p, su subcampo primario es $\mathbb{Z}_p$ y $F/\mathbb{Z}_p$ es una extensión de campos. Sea α una raíz de unidad primitiva del polinomio $x^{q-1}-1$, es decir, $1 = \alpha^{q-1}$. Ya que α es primitiva y, por el teorema 7.3, $\alpha \in F$; luego, por el teorema 8.15, tenemos que $F^\# = \langle\alpha\rangle$. Entonces $\langle a\rangle \cup \{0\}$ tiene q elementos y $F = \mathbb{Z}_p(\alpha)$. □

Definición 6.26. *Sea F es un campo finito de característica p. El elemento $\alpha \in F$ del corolario 6.25 es llamado un elemento primitivo de F.*

Teorema 6.27. *Una extensión finita E/F es una extensión simple si, y sólo si, tiene un número finito de campos intermedios.*

Demostración. Supongamos que E/F una extensión simple, entonces existe $\alpha \in E$ tal que $E = F(\alpha)$. Ya que E/F es una extensión finita, E/F es una extensión algebraica y existe un polinomio mónico irreducible $p(x) \in F[x]$ con α como raíz. Sean B un campo intermedio, $g(x) \in B[x]$ el polinomio mónico irreducible con α como raíz y sean $g_1, ..., g_q \in B$ sus coeficientes. Si $B' = F(g_1, ..., g_q)$, $g(x)$ también es irreducible en B'. Ya que

$$E = F(\alpha) \subset B'(\alpha) \subset B(\alpha) \subset E,$$

tenemos que $E = B(\alpha) = B'(\alpha)$, de donde $[E : B] = [B(\alpha) : B]$ y $[E : B'] = [B'(\alpha) : B']$; de donde, ya que $\partial(g)$ es el mismo en B y B', por el teorema 5.14, tenemos que $[E : B] = [E : B']$. Por lo tanto $B = B'$ y por cada $g(x)|p(x)$ el campo intermedio B queda determinado de manera única. Pero sólo hay un número finito de divisores de $p(x)$, por lo tanto hay únicamente un número finito de campos intermedios.

Ahora, supongamos que la extensión E/F tiene únicamente un número finito de campos intermedios. Si F es un campo finito, entonces E es un campo finito al ser E/F una extensión finita; además, por el teorema 3.14, ambos tienen la misma característica p. Luego, por el lema 6.25, E/F es una extensión simple.

Supongamos que F es infinito. Ya que E/F es una extensión finita, existen $\alpha_1, ..., \alpha_n \in F$ tales que $E = F(\alpha_1, ..., \alpha_n)$. Si $n = 1$ entonces E/F es una extensión simple. Supongamos la proposición es valida para k. Sea $n = k + 1$. Entonces

$$F \subset F(\alpha_1, ..., \alpha_k) \subset F(\alpha_1, ..., \alpha_k, \alpha_k + 1) = E$$

es una cadena de extensiones. Por hipótesis de inducción, $F(\alpha_1, ..., \alpha_k)/F$ es una extensión simple, por lo tanto existe $\gamma \in E$ tal que $F(\alpha_1, ..., \alpha_k) = F(\gamma)$ y $E = F(\gamma, \alpha_{k+1})$. Consideremos todos los elementos de la forma $\beta_t = \gamma + t * \alpha_{k+1}$ donde $t \in F$; ya que F es infinito, hay un número infinito de β_t. Por hipótesis hay únicamente un número finito de campos intermedios, por lo que únicamente existen un número finito de campos intermedios de la forma $F(\beta_t)$. Por lo tanto, existen $t, t' \in F$, con $t \neq t'$, tales que $F(\beta_t) = F(\beta_{t'})$. Claramente $F(\beta_t) \subset F(\gamma, \alpha_{k+1})$. Ahora, $(t - t') * \alpha_{k+1} = \beta_t - \beta_{t'} \in F(\beta_t) = F(\beta'_t)$. Luego, ya que $t \neq t'$, $\alpha_{k+1} \in F(\beta_t)$ y $\gamma = \beta_t - t * \alpha_{k+1} \in F(\beta_t)$, tenemos que $F(\gamma, \alpha_{k+1}) \subset F(\beta_t)$. Por lo tanto $E = F(\gamma, \alpha_{k+1}) = F(\beta_t)$ y E/F es una extensión simple. □

Corolario 6.28. *Si E/F una extensión simple y K es un campo intermedio, entonces la extensión K/F es simple.*

Demostración. Por el teorema 6.27, E/F tiene únicamente un número finito de campos intermedios, por lo tanto K/F sólo tiene un número finito de campos intermedios. Por lo tanto, K/F es una extensión simple. □

Teorema del Elemento Primitivo 6.29. *Toda extensión finita separable K/F es una extensión simple.*

Demostración. Por 5.33, existe una extensión E/F tal que E es un campo de descomposición para algún polinomio $f(x) \in F[x]$; con K como campo intermedio. Ya que E es el campo de descomposición de $f(x) \in F[x]$ y $f(x)$ es separable por ser E/F una extensión separable, E/F es una extensión de Galois; y por el corolario 6.24, E/F tiene únicamente un número finito de campos intermedios. Por lo tanto, la extensión K/F posee únicamente un número finito de campos intermedios y, por el teorema 6.24, K/F es una extensión simple. □

Capítulo 7

Campos de Galois.

Teorema 7.1. *Si F es un campo finito, entonces F es de característica $p > 0$, y el número de elementos de F es p^n donde n es el grado de la extensión $F/\mathbb{Z}_p$.*

Demostración. Sea P el subcampo primario de F. Como F es finito, por el teorema 3.14, P es finito e isomorfo a $\mathbb{Z}_p$ para algún entero primo p. Por el teorema 5.4, F es un espacio vectorial sobre P. Este espacio vectorial tiene un número finito de elementos, entonces debe de tener una base finita. Por lo tanto existe n tal que $[F : P] = n$.

Sea $\{x_1, ..., x_n\}$ una base de F sobre P. Todo elemento de F se puede expresar de forma única por

$$\lambda_1 * x_1 + ... + \lambda_n * x_n \tag{7.2}$$

donde $\lambda_1, ..., \lambda_n \in P$. Ya que $|P| = p$, cada λ_j puede ser elegida de p diferentes formas, por lo cual existen p^n expresiones de la forma 7.2 diferentes. Por lo tanto, $|F| = p^n$ □

Entonces, por el teorema anterior, podemos concluir que todo campo finito tiene p^n elementos para algún p primo.

Teorema 7.3. *Sean p un número primo y $q = p^n$ donde n es un entero mayor a 0. Un campo F tiene q elementos si, y sólo si, F es un campo de descomposición del polinomio $f(x) = x^q - x$ sobre el subcampo primario de F, $\mathbb{Z}_p$.*

Demostración. Supongamos que $|F| = q$. Notemos que $(F - \{0\}, *)$ es un grupo de orden $q-1$. Por el teorema de Lagrange (8.18), para $a \in F$, $a \neq 0$, tenemos que $a^{q-1} = 1$ y a es raíz del polinomio $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Además, ya que $f(0) = 0^q - 0 = 0$, todo elemento de F es raíz de $f(x)$, por cual F es un campo de descomposición de $f(x)$ sobre $\mathbb{Z}$.

Ahora, supongamos que F es un campo de descomposición de $f(x)$ sobre $\mathbb{Z}_p$. Ya que la derivada $f'(x) = q * x^{q-1} - 1 = -1$ entonces $(f(x), f'(x)) = 1$ y, por 8.26, tenemos que $f(x)$ no tiene raíces de multiplicidad mayor a 1, por lo cual $f(x)$ tiene q raíces distintas. Consideremos el automorfismo dado por $\phi^n(x) = x^q = x^{p^n}$, donde ϕ es el mapeo de Frobenius. Sean E el conjunto de todas raíces de $f(x)$ y $a, b \in E$. Entonces, tenemos que:

(*i*) $(a*b)^q - (a*b) = a^q * b^q - a*b = a*b - a*b = 0$. Por lo cual $a*b \in E$.

(*ii*) $(a * a^{-1})^q - (a * a^{-1}) = 1^q - 1 = 0$. Por lo cual $a^{-1} \in E$ y $1 \in E$.

(*iii*) $(a+b)^q - (a+b) = (a^q + b^q) - (a+b) = (a+b) - (a+b) = 0$. Por lo cual $a + b \in E$.

(*iv*) $(a-a)^q - (a-a) = 0^q - a = 0$. Por lo cual $-a, 0 \in E$.

Además, claramente $0 \in E$. Por lo tanto, E es un campo y claramente $E = F$. □

Notemos que el teorema anterior nos garantiza la existencia de un campo con $q = p^n$ elementos, ya que el teorema de Kronecker nos garantiza la existencia de un campo de descomposición para el polinomio $x^q - x$.

Corolario 7.4. *Cualquier par de campos finitos de orden $q = p^n$, p un número primo, son isomorfos.*

Demostración. Por el teorema 7.3, todo campo de orden q es el campo de descomposición del polinomio $x^q - x$. Por el corolario 5.29, todo campo de descomposición es isomorfo. □

Llamamos al campo de orden $q = p^n$ el Campo de Galois de Orden q, *se denota por $GF(p^n) = GF(q)$.*

Proposición 7.5. *Todo campo finito F es un campo perfecto.*

Demostración. Sea F un campo finito y, por 7.3, de característica p para algún número primo p. Consideremos a ϕ, el Mapeo de Frobenius (3.17) en F. Al ser F un campo finito claramente ϕ es un isomorfismo, por lo cual,

para todo $a_i \in F$, existe b_i tal que $a_i = b_i^p$. Sea $q(x) = (b_0)^p + (b_1)^p x + ... + (b_n)^p x^n$ un polinomio irreducible en $F[x]$, y consideremos su derivada $q'(x) = (b_1)^p + 2(b_2)^p x + ... + n(b_n)^p x^{n-1}$. Supongamos que $q(x)$ no es separable. Ya que $q(x)$ es irreducible, sus únicos divisores son 1 y $q(x)$ y, por teorema 8.26, $(q(x), q'(x)) \neq 1$, entonces $(q(x), q'(x)) = q(x)$ y por lo tanto $q'(x) = 0$. Luego, por el lema 8.27, necesariamente $q(x)$ es de la forma

$$\begin{aligned} q(x) &= g(x^p) \\ &= (c_0)^p + (c_1)^p * x^p + ... + (c_s)^p * x^{p^s} \\ &= (c_0 + c_1 * x + ... + c_s * x^s)^p. \end{aligned}$$

Por lo tanto $q(x)$ no es irreducible, lo que es una contradicción. □

Lemma 7.6. *Si α es un elemento primitivo de $GF(p^n)$, entonces existe un polinomio irreducible $f(x) \in \mathbb{Z}_p[x]$ de grado n tal que tiene a α como raíz.*

Demostración. Al ser $GF(p^n)/\mathbb{Z}_p$ una extensión finita, entonces es una extensión algebraica y existe un polinomio irreducible $f(x) \in \mathbb{Z}_p[x]$ con α como raíz. Supongamos que $\partial(f) = d$. Entonces, por el teorema 7.1, $|\mathbb{Z}_p(\alpha)| = p^d$. Pero, ya que α es primitivo, $\mathbb{Z}_p(\alpha) = GF(p^n)$ y $p^d = p^n$. Por lo tanto $d = n$ y $\partial(f) = n$. □

Teorema 7.7. *$\langle\phi\rangle = Gal(GF(p^n)/GF(p)) \cong \mathbb{Z}_n$ donde ϕ es el automorfismo de Frobenius (3.17) en $GF(p^n)$.*

Demostración. Sean $F = GF(p^n)$ y $G = Gal(GF(p^n)/GF(p))$. Si α es un elemento primitivo de F entonces, por el lema 7.6, su polinomio irreducible $q(x) \in \mathbb{Z}_p[x]$ es de grado n y F contiene a lo más n de sus raíces. Ya que $F^\#$ es un grupo cíclico (lema 6.25), todos los elementos de F distintos a 0 son de la forma α^i. Luego, si $\sigma \in G$ y $\alpha^i \in F$, tenemos que $\sigma(\alpha_i) = \sigma(\alpha)^i$ y σ queda totalmente determinado por $\sigma(\alpha)$. Pero, ya que σ deja fijo a $GF(p)$, usando el lema 5.27, $\sigma(\alpha)$ es raíz de $q(x)$ y todos los elementos de F son raíces de $q(x)$. Por lo tanto, ya que F tiene a lo más n raíces de $q(x)$ y σ queda determinado por $\sigma(\alpha) \in F$, $|G| \leq n$.

Por otro lado, por la demostración del teorema 7.3, tenemos que $a^p - a = 0$ y $a^p = a$ para todo $a \in \mathbb{Z}_p$, de donde $\phi \in G$. Sea j el orden de ϕ. Supongamos que $j < n$. Ya que j es el orden de ϕ en G tenemos que $(a^p)^j = a$. Luego, todos los p^n elementos de F son raíces del polinomio $(x^p)^j - x$, que a lo más posee $p^j < p^n$ raíces, una contradicción. Por lo

tanto, el orden de ϕ es mayor o igual a n. Por lo tanto, ya que $|G| \leq n$, tenemos que $|G| = n$ y $\langle \phi \rangle = G$. □

Consideremos la extensión de campos $GF(p^n)/GF(p)$. Por el teorema 7.3, $GF(p^n)$ es un campo de descomposición de un polinomio $q(x) \in GF(p)$, por lo cual, la extensión $GF(p^n)/GF(p)$ es de Galois. Luego, por el teorema anterior, $Gal(GF(p^n)/GF(p)) \cong \mathbb{Z}_n$. Luego, por 6.13, tenemos que

$$[GF(p^n) : GF(p)] = |\mathbb{Z}_n| = n. \tag{7.8}$$

Como consecuencia directa del resultado anterior tenemos el siguiente lema:

Lema 7.9. *Sea E/F una extensión de campos finitos de grado $[E : F] = n$. Si K/F es una extensión de campos finitos tal que $[K : F] = n$, entonces $K = E$.*

Demostración. Como F es un campo finito, F es de característica $p > 0$; además existe $f \in \mathbb{N}$ tal que $F = GF(p^f)$ y el grado de la extensión $F/GF(p)$ es $[F : GF(p)] = f$. Además, ya que E y K son finitos y $F = GF(p^f)$, existen enteros $e, k \in \mathbb{N}$ tales que $E = GF(p^{f*e})$ y $K = GF(p^{f*k})$. Entonces, por el lema 5.17, tenemos que $[E : GF(p)] = [E : F] * [F : GF(p)] = n * f$ y $[K : GF(p)] = n * f$, es decir $[E : GF(p)] = [K : GF(p)]$. Por otro lado, por 7.8, tenemos que $[E : GF(p)] = [GF(p^{e*f}) : GF(p)] = e * f$ y $[K : GF(p)] = k * f$. Por lo tanto, $e * f = k * f$ y $e = k$. Por lo tanto, $K = GF(p^{f*k}) = E$. □

Teorema 7.10. *El Campo de Galois $GF(p^n)$ tiene exactamente un subcampo de orden p^d por cada divisor d de n.*

Demostración. Por el teorema 7.7, sabemos que $Gal(GF(p^n)/GF(p)) \cong \mathbb{Z}_n$ es un grupo cíclico de orden n; además, por el lema 8.20, todo grupo cíclico de orden n tiene exactamente un subgrupo de orden d_i por cada d_i divisor de n. Luego, ya que $\mathbb{Z}_n$ es un grupo finito, para todo subgrupo $H \subset \mathbb{Z}_n$ de de orden d_i tenemos que $[\mathbb{Z}_n : H_i] = n/d_i$ (8.18). Entonces, por el Teorema Fundamental de la Teoría de Galois (6.22), para el campo intermedio correspondiente K_i bajo γ tenemos que

$$n/d_i = [\mathbb{Z}_n : H_i] = [K_i : GF(p)].$$

Finalmente, por el teorema 7.1, tenemos que todos los campos intermedios de la extensión $GF(p^n)/GF(p)$ son de orden n/d_i, ya que $d_i | n$, n/d_i es un entero divisor de n de la forma d_j. Por lo tanto, tenemos un sólo subcampo intermedio de característica $d_j = n/d_i$ por cada d_j divisor de n. □

Corolario 7.11. *Sean $GF(p^n)$ y $GF(p^m)$ dos campos de Galois. Entonces $GF(p^m) \subset GF(p^n)$ si, y sólo si, $m|n$.*

Demostración. Sea $GF(p^m) \subset GF(p^n)$, entonces $GF(p^m)$ es un campo intermedio de la extensión $GF(p^n)/GF(p)$. Luego, por el teorema 7.10, m es un divisor de n y $m|n$.

Ahora, supongamos que $m|n$. Entonces, $GF(p^n)/GF(p^m)$ es una extensión y $GF(p^m) \subset GF(p^n)$. □

Notemos que, por el resultado anterior, todos los subcampos de un campo finito quedan determinados de forma única. Entonces, podemos suponer que toda extensión de campos finitos es de la forma $GF(p^{m*d})/GF(p^m)$.

Proposición 7.12. *Toda extensión de Campos de Galois de la forma*

$$GF(p^{n*d})/GF(p^n)$$

es una extensión simple.

Demostración. Por el teorema 7.10, $GF(p^{n*d})/GF(p^n)$ tiene un número finito de campos intermedios. Luego, por el teorema 6.27, $GF(p^{n*d})/GF(p^n)$ es una extensión simple. □

Teorema 7.13. *La cerradura algebraica de $GF(p)$, $\overline{GF(p)}$, es la unión de todos los campos de Galois de Característica p, es decir*

$$\overline{GF(p)} = \bigcup_{n\in\mathbb{N}} GF(p^n).$$

Demostración. Sean $E = \bigcup_{n\in\mathbb{N}} GF(p^n)$, $F = GF(p)$ y $f(x) = \sum_{i=0}^{r} a_i * x^i$ un polinomio en $F[x]$. Sea α una raíz de $f(x)$. Entonces, por el teorema 5.14, $[F(\alpha), F] \leq r$ es una extensión de grado finito; luego, ya que F es finito y $F(\alpha)$ está generado por una base finita sobre F, $F(\alpha)$ es un campo finito. Por lo tanto, existe un campo de Galois $GF(p^r)$ tal que

$$\alpha \in F(\alpha) = GF(p^r).$$

Por lo tanto, $\overline{GF(p)} \subset E$.

Por otro lado, usando el teorema 7.3, tenemos que para toda $n \in \mathbb{N}$ el polinomio $x - x^q$, donde $q = p^{2*n}$, tiene todas raíces en la extensión $GF(q) \supset GF(p^n)$, de donde $E \subset \overline{GF(p)}$. Por lo tanto, tenemos que $E = \overline{GF(p)}$. □

Notemos que, por el teorema anterior, podemos concluir dos propiedades importantes sobre los campos finitos: La cerradura algebraica de cualquier campo finito es un campo infinito; en consecuencia, ningún campo finito es algebraicamente cerrado.

Ejemplo: Construcción de un Campo finito. 7.14. Por el teorema 7.1, todo campo finito debe de tener p^n elementos, para algún $p \in \mathbb{N}$ primo. Si $n = 1$ entonces $GF(p) = \mathbb{Z}_p$ es el único campo con p elementos. Sea $n \geq 2$. Entonces, por 7.8, $F/\mathbb{Z}_p$ es una extensión de campos de grado $[F : \mathbb{Z}_p] = n$. Por otro lado, si $f(x)$ un polinomio irreducible en $GF(p)[x]$ de grado n con α como raíz, por el teorema 7.13, existe un campo de Galois F' que contiene a α. Luego, Por el teorema 5.14, tenemos que el campo F' es de la forma

$$F' = \mathbb{Z}_p(\alpha) = \mathbb{Z}_p[x]/\langle f(x)\rangle$$

donde $[F' : GF(p)] = \partial(p) = n$. Pero, por el lema 7.9, para todo campo F' tal que $[F' : GF(p)] = n$ tenemos que $F = F'$. Por lo tanto,

$$F = \mathbb{Z}_p[x]/\langle f(x)\rangle.$$

Capítulo 8

Apéndice

Teorema del Binomio 8.1. *Sean R un anillo y $n \in \mathbb{Z}$, $n \geq 1$. Entonces*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i * b^{n-i} \tag{8.2}$$

donde

$$\binom{n}{i} = \frac{n!}{i! * (n-i)!} \tag{8.3}$$

Además, para $0 < k < n$, tenemos que

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}, \tag{8.4}$$

igualdad llamada la Identidad de Pascal.

Demostración. Primero demostraremos la Identidad de Pascal

$$\begin{aligned}\binom{n}{k}+\binom{n}{k-1} &= \frac{n!}{k!*(n-k)!}+\frac{n!}{(k-1)!*(n-(k-1))!}\\ &= \frac{(n-k+1)*n!}{(n-k+1)*k!*(n-k)!}+\frac{kn!}{k*(k-1)!*(n-k+1)!}\\ &= \frac{(n-k+1)*n!+k*n!}{k!(n-k+1)!}\\ &= \frac{(n+1)*n!}{k!((n+1)-k)!}\\ &= \frac{(n+1)!}{k!((n+1)-k)!}\\ &= \binom{n+1}{k}.\end{aligned}$$

Ahora demostraremos el teorema del Binomio por inducción, sea $n = 1$ entonces

$$\begin{aligned}\sum_{i=0}^{1}\binom{1}{i}a^i*b^{1-i} &= \binom{1}{0}a^{1-0}*b^0+\binom{1}{0}a^{1-1}*b^1\\ &= 1*a*1+1*1*b\\ &= a+b\\ &= (a+b)^n.\end{aligned}$$

Supongamos que la proposición es valida para $n = m$. Si $n = m+1$ entonces

$$\begin{aligned}
(b+a)^{m+1} &= (b+a)*(b+a)^m \\
&= (b+a)*(b^m + a^m + \sum_{k=1}^{m-1} \binom{m}{k} * a^{m-k} * b^k) \\
&= b^{m+1} + a^{m+1} + a*b^m + b*a^m + \sum_{k=1}^{m-1} \binom{m}{k} * a^{m-k+1} * b^k + \sum_{k=1}^{m-1} \binom{m}{k} * a^{m-k} * b^{k+1} \\
&= b^{m+1} + a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} * a^{m-k+1} * b^k + \sum_{k=0}^{m-1} \binom{m}{k} * a^{m-k} * b^{k+1} \\
&= b^{m+1} + a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} * a^{m-k+1} * b^k + \sum_{j=1}^{m} \binom{m}{j-1} * a^{m+1-j} * b^j \\
&= b^{m+1} + a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1} \right] * a^{m+1-k} * b^k
\end{aligned}$$

Y, usando la Identidad de Pascal,

$$\begin{aligned}
(a+b)^{m+1} &= a^{m+1} + b^{m+1} + \sum_{k=1}^{m} \binom{m+1}{k} a^{m+1-k} b^k \\
&= \sum_{i=0}^{m+1} \binom{m}{i} b^i * a^{m-i}.
\end{aligned}$$

□

Además, notemos que si p es un número primo, $i \neq 0$ e $i \neq p$ entonces, $p|\binom{p}{i}$. Ya que

$$\binom{p}{i} = \frac{p!}{i! * (p-i)!} = \frac{p * (p-1)!}{i! * (p-i)!}$$

es un número positivo con p como factor, ya que, al ser p primo, no puede ser dividido por $i!$ o $(p-i)!$.

Definición 8.5. Un dominio entero R es llamado un *anillo euclidiano* si para todo $a \in R$, $a \neq 0$, existe un entero positivo $d(a)$ tales que para cualesquiera $a, b \in R$, $a, b \neq 0$:

(*i*) $d(a) \leq d(a * b)$.

(*ii*) Existe t, r, con $r = 0$ o $d(r) < d(b)$, tales que $a = t * b + r$.

Por ejemplo, $\mathbb{Z}$ es un anillo euclidiano.

Teorema 8.6. *Sean R un anillo euclidiano e I un ideal de R. Entonces existe a en R tal que $I = \langle a \rangle$. Esto es, R es un dominio de ideales principales.*

Demostración. Si $I = \{0\}$ entonces $a = 0$. Supongamos que $I \neq \{0\}$. Sean $a_0 \in I$, $a_0 \neq 0$, tal que $d(a_0)$ es mínimo. El elemento a_0 existe, ya que $I \neq \{0\}$ y $d(a) \in \mathbb{Z}^+$.

Sea $a \in I$. Al ser R un anillo euclidiano, existen $t, r \in R$ tales que $a = t * a_0 + r$ donde $r = 0$ o $d(r) < d(a_0)$. Ya que I es un ideal, $t * a_0 \in I$ y $t * a_0 - a \in I$, por lo cual $r \in I = 0 + I$. Si $r \neq 0$ tenemos una contradicción, ya que $d(r) < d(a_0)$. Por lo tanto, $r = 0$, $a = t * a_0$ e $I = \langle a_0 \rangle$. □

Corolario 8.7. *Todo anillo Euclidiano posee un elemento unitario.*

Demostración. Sea R un anillo Euclidiano. Por el teorema 8.6, todo ideal de R está generado por un elemento, en particular $R = \langle u \rangle$ para algún $u \in R$. Luego, existe $r \in R$ tal que $r * u = u$ y r es un elemento unitario.

□

Lema 8.8. *Sean R un anillo euclidiano y $a_1, ..a_n \in R$. Su máximo común divisor, denotado por $d = (a_1, .., a_n)$, existe y es una combinación lineal de $a_1, .., a_n$.*

Demostración. Consideremos al ideal $\langle a_1, a_2 \rangle$, el ideal generado por a_1, a_2. Ya que R es dominio de ideales principales, existe un generador de $\langle a_1, a_2 \rangle$. Sea d este generador, con $d = s * a_1 + t * a_2$.

Por 8.7, R tiene un elemento unidad, de donde $a_1 = 1 * a_1 + 0 * a_2$ y $a_2 = 0 * a_1 + 1 * a_2$, por lo cual, $a_1, a_2 \in \langle a_1, a_2 \rangle$ y $d | a_1, a_2$. Si $c | a_1, a_2$, entonces, $c | s * a_1, t * a_2$, $c | s * a_1 + t * a_2$ y $c | d$. Por lo tanto, d es el máximo común divisor de a_1 y a_2.

Por inducción, el teorema queda demostrado. □

Ejemplo 8.9. Sean $a_1, .., a_n$ números enteros positivos. Su máximo común divisor, denotado por $d = (a_1, .., a_n)$, existe y es una combinación lineal de $a_1, .., a_n$.

Ejemplo 8.10. *Sean R un anillo euclidiano, p y q primos relativos. Si $p|q * n$, entonces $p|n$.*

Demostración. Por el teorema 8.8 existen $s, t \in R$ tales que

$$p * s + q * t = 1.$$

Multiplicando por n tenemos que

$$n * (p * s + q * t) = 1 * n.$$
$$p * (n * s) + t * (q * n) = n$$

Ya que $p|q * n$, $p|n$.

□

Algoritmo de la Division 8.11. *Sean F un campo y $f(x), g(x) \in F[x]$, $g(x) \neq 0$, entonces existen polinomios $q(x), r(x) \in F[x]$ tales que*

$$f(x) = q(x) * g(x) + r(x)$$

con $r(x) = 0$ o $\partial(g) > \partial(r)$.

Demostración. Si $\partial(f) = -\infty$ entonces $f(x) = 0$ y $q(x) = r(x) = 0$. Si $\partial(g) = 0$ entonces $g(x) = (a_0 \neq 0, 0, ...)$ con $a_0 \in F$ y podemos tomar $q(x) = (k/a_0, 0, ...)$ y $r(c) = 0$.

Supongamos que la proposición es cierta para $\partial(f) < n$ y sea $f(x) \in F[x]$ tal que $\partial(f) = n > 0$. Si $\partial(f) < \partial(g)$ entonces $q(x) = 0$ y $r(x) = f(x)$. Supongamos que $\partial(f) \geq \partial(g)$, entonces tenemos que

$$g(x) = (a_0, ..., a_m) \qquad\qquad f(x) = (b_0, ..., b_n)$$

con $m \leq n$. Sea

$$f_1(x) = (0_0, ..., 0_{n-m-1}, b_n * a_m^{-1}) * g(x) - f(x)$$

que nos elimina la coordenada de índice mayor en $f(x)$, por lo que tenemos $\partial(f_1) < \partial(f)$. Por la hipótesis de inducción, existen $q_1(x), r_1(x) \in F[x]$ tales que $f_1(x) = g(x) * q_1(x) + r_1(x)$ y $\partial(r_1) < \partial(g)$. Sea

$$q(x) = (0_0, ..., 0_{n-m-1}, b_n * a_m^{-1}) - q_1(x) \qquad r(x) = -r_1(x)$$

entonces

$$\begin{aligned} g(x) * q(x) + r(x) &= (0_0, ..., 0_{n-m-1}, b_n * a_m^{-1}) * g(x) - q_1(x) * g(x) - r_1(x) \\ &= f(x) + f_1(x) - f_1(x) \\ &= f(x). \end{aligned}$$

□

Proposicion 8.12. *Sean R un anillo y $a, b, d \in R$. Si $d|a+b$ y $d|a$ entonces $d|b$.*

Demostración. Si $d|a + b$ y $d|a$ entonces existen $r, s \in R$ tales que $a = r * d$ y $a + b = s * d$. De donde $r * d + b = s * d$ y $b = s * d - r * d = (s - r) * d$. Por lo tanto, $d|b$. □

Definición 8.13. Sean $(G, *)$ un grupo y a un elemento de G. El orden del grupo G es $|G|$, la cardinalidad del grupo G. Decimos que a es un *elemento de orden* $n \in \mathbb{N}$ si $a^n = 1$, es decir $1 = a * a * ... * a$ n veces, y si para toda m tal que $a^m = 1$ tenemos que $n \leq m$.

Definición 8.14. Sean $(G, *)$ es un grupo y $a \in G$. Consideremos al conjunto

$$\langle a \rangle = \{a^r : r \in \mathbb{Z}\}.$$

Sean $a^n, a^m \in \langle a \rangle$, entonces:

(i) Ya que todo grupo es cerrado bajo $*$, $a^n \in G$ y $\langle a \rangle \subset G$.

(ii) $a^0 = 1$ y $1 \in \langle a \rangle$.

(iii) $a^n * a^m = a^{n+m} \in \langle a \rangle$.

(iv) $a^n * a^{-n} = a^{n-n} = a^0 = 1 \in \langle a \rangle$.

Por lo tanto $\langle a \rangle$ es un subgrupo de G llamado un *subgrupo cíclico de G* generado por a. Si existe $a \in G$ tal que $G = \langle a \rangle$, entonces G es llamado un *grupo cíclico* generado por a.

Notemos que todo elemento de G pertenece a un subgrupo cíclico de G.

Teorema 8.15. *Sea $(G, *)$ un grupo finito. Entonces:*

(i) Sea a un elemento de G de orden n, entonces $a^m = 1$ si, y sólo si, $n|m$.

(ii) Si $G = \langle a \rangle$ es un grupo cíclico de orden n, entonces a^k es un generador de G si, y sólo si, $(k, n) = 1$.

(iii) Si $a \in G$ tiene orden n, entonces $|\langle a \rangle| = n$.

Demostración. (i) Si $n|m$, entonces $m = n * k$ para algún $k \in \mathbb{Z}$. Entonces, tenemos que $1 = a^m = a^{n*k} = (a^n)^k = 1^k = 1$. Ahora, sea $a^m = 1$. Por el algoritmo de la división para números enteros, existen $q, r \in \mathbb{Z}$ tales que $m = n*q+r$, con $0 \leq r < n$. Entonces, tenemos que $a^r = a^{m-n*q} = a^m * a^{-n*q} = 1 * (1)^{-q} = 1$. Si $r > 0$ entonces tenemos una contradicción, ya que n es el menor natural tal que $a^n = 1$. Por lo tanto, $r = 0$ y $n|m$.

(ii) Sea $G = \langle a \rangle$. Si $G = \langle a^k \rangle$, entonces existe t entero tal que $a = a^{k*t}$. Por lo cual $a^{k*t-1} = 0$ y, por (i), $n|k*t-1$, de donde existe $v \in \mathbb{Z}$ tal que $n * v = k * t - 1$. Entonces, 1 es una combinación lineal de k y n, por 8.8 tenemos que $(k, n) = 1$.

Ahora, supongamos que $(k, n) = 1$, entonces existen $t, u \in \mathbb{Z}$ tales que $n * t + k * u = 1$; de donde

$$a = a^{n*t+k*u} = a^{n*t} * a^{k*u} = a^{k*u} \in \langle a^k \rangle$$

Por lo tanto, $\langle a^k \rangle = \langle a \rangle = G$.

(iii) Sea $a^i = a^j$ con $i, j \leq n$. Si $i \neq j$, entonces podemos suponer que $i < j$, de donde $a^{j-i} = 1$ con $j - i < n$, que es una contradicción. Por lo tanto, la cadena $1, a^2, ..., a^{n-1}$ no tiene elementos repetidos, y $G = \{1, a^2, ..., a^{n-1}\}$. Por lo tanto, $|G| = |\langle a \rangle| = |\{1, a^2, ..., a^{n-1}\}| = n$.

□

Definición 8.16. Sea G un grupo. Un subgrupo H es un *subgrupo normal de G* si, para toda $g \in G$,

$$gHg^{-1} = \{g * h * g^{-1} : h \in H\} = H.$$

Definición 8.17. Sean G un grupo, H un subgrupo de G y g un elemento de G. El conjunto $g * H$ dado por

$$g * H = \{g * h : h \in H\}$$

es un subconjunto de G llamado *clase lateral* derecha de H en G. *El índice de un subgrupo* H de G, denotado por $[G : H]$ es la cardinalidad del conjunto de todas clases laterales derechas de H en G.

Sea H un subgrupo normal de G. El conjunto $G/H = \{g * H : g \in G\}$, es grupo bajo la operación binaria

$$\begin{aligned} * :& G/H \times G/H \to G/H \\ & (g * H, g' * H) \mapsto (g * g') * H \end{aligned}$$

llamado *grupo cociente*.

Teorema de Lagrange 8.18. *Sea G un grupo finito. Si H es un subgrupo de G, entonces $|G| = [G : H] * |H|$.*

Demostración. Podemos definir una relación en G donde $x \sim y$ si existe $h \in H$ tal que $y = x * h$. Notemos que $x = y * h^{-1}$ implica $y \sim x$. Además, si $x \sim y$ y $y \sim z$, entonces, existen h_x, h_z tales que $x = h_x * y = h_x * (h_y * z) = (h_x * h_y) * z$ y $x \sim z$, por lo que tenemos una relación de equivalencia, cuyas clases son las clases laterales de H. Por lo cual, las clases laterales de H en G forman una partición en G. Además, si $x \in G$ notemos que el mapeo dado por $h \mapsto x * h$ es una biyección de H en $x * H$, por lo tanto $|H| = |x * H|$ y $|G|$ es el número de clases laterales por el número de elementos en H, $|G| = [G : H] * |H|$. □

Como consecuencia del teorema anterior, tenemos que el orden de $a \in G$ es un divisor de $|G|$, ya que el teorema 8.17 nos asegura que el orden de a es el número de elementos del subgrupo $H = \langle a \rangle$. Por lo tanto, $a^{|G|} = 1$ para toda $a \in G$. Además, si G es un subgrupo finito y H un subgrupo de de G, el índice es $[G : H] = |G|/|H|$

Primer Teorema de Isomorfismos para Grupos 8.19. *Si $\sigma : G \to K$ es un homomorfismo de grupos, entonces* $\ker \sigma$ *es un subgrupo normal de G y*

$$G/ker\sigma \cong im\sigma$$

Demostración. Sea $K = ker\sigma$. Sean $a, b \in K$ y $g \in G$. Notemos que

(*i*) ya que $\sigma(1) = 1$ entonces $1 \in K$,

(*ii*) $\sigma(a * b) = \sigma(a) * \sigma(b) = 1 * 1 = 1$ por lo cual $a * b \in K$,

(*iii*) $\sigma(a^{-1}) = \sigma(a)^{-1} = 1$ de donde $a^{-1} \in K$

y, además

(*iv*) $\sigma(g * a * g^{-1}) = \sigma(g) * \sigma(a) * \sigma(g^{-1}) = \sigma(g) * 1 * \sigma(g^{-1}) = 1$.

Por lo tanto $g * a * g^{-1} \in ker\sigma$ y $ker\sigma$ es un subgrupo normal de G.

Ahora, definamos a $\varphi : G/K \to im\sigma$ por $\varphi(g * K) = \sigma(g)$. Sea $g * K = g' * K$, entonces existe $k \in K$ tal que $g' = g * k$ y

$$\begin{aligned} \varphi(g' * K) &= \sigma(g') \\ &= \sigma(g * k) \\ &= \sigma(g) * \sigma(k) \\ &= \sigma(g) * 1 \\ &= \varphi(g * K) \end{aligned}$$

por lo que φ está bien definido. Ya que σ es un homomorfismo, y $im\varphi = im\sigma$, claramente φ también lo es. Ahora, si $\varphi(g * K) = K = 1 * K$ entonces $\sigma(g) = 1$ y $ker\varphi = K$. Por 3.9, φ es una inyección. Ya que $im\varphi = im\sigma$, φ es suprayectivo y, por lo tanto, φ es un isomorfismo. □

Lema 8.20. *Si $C = \langle a \rangle$ es un grupo cíclico de orden n, entonces C tiene un subgrupo cíclico de orden d_i por cada d_i divisor de n.*

Demostración. Sea $n = c_i * d_i$. Notemos que $(a^{c_i})^{d_i} = a^{c_i * d_i} = a^n = 1$. Si $(a^{c_i})^r = 1$ con $r \leq d_i$ entonces, por el teorema 8.15, $n | c_i * r$ y existe s entera tal que $c_i * r = n * s = d_i * c_i * s$, de donde $r = d_i * s \geq d_i$ y $r = d_i$. Por lo tanto tenemos un grupo subgrupo cíclico de orden d_i generado por $\langle a^{c_i} \rangle$.

Ahora, supongamos que $\langle x \rangle$ es un subgrupo de orden d_i. Entonces $x = a^m$ y $1 = x^{d_i} = a^{m * d_i}$; de donde existe k tal que $m * d_i = n * k$. Entonces, ya que $c_i * d_i = n$ y $c_i = n/d_i$ tenemos que $x = a^m = (a^{c_i})^k$ y $\langle x \rangle \subset \langle a^{c_i} \rangle$. Ya que los dos grupos tienen el mismo número de elementos, $\langle x \rangle = \langle a^{c_i} \rangle$.

Por lo tanto, C tiene exactamente un grupo cíclico de orden d_i por cada d_i divisor de n. Todos ellos cíclicos. □

Definición 8.21. La Función φ de Euler es el mapeo $\varphi : \mathbb{N} \to \mathbb{N}$ dado por

$$\varphi(1) = 1$$
$$\varphi(n) = |\{k \in \mathbb{Z} : 1 \leq k < n \text{ y } (k, n) = 1\}| \text{ si } n > 1.$$

Teorema 8.22. *Un grupo G de orden n es cíclico si, y sólo si, por cada divisor d de n existe a lo más un subgrupo cíclico de orden d.*

Demostración. Si G es cíclico por el lema 8.20 tenemos el resultado. Supongamos que en G, por cada divisor de n, existe a lo más un subgrupo cíclico de orden d.

Sea $C(G)$ es conjunto formado por todos los subgrupos cíclicos de G. Definamos en G la relación $a \cong b$ si $\langle a \rangle = \langle b \rangle$. Es claro que $\cong$ es una relación de equivalencia. Si $C \in C(G)$ es un subgrupo cíclico de G generado por a, entonces podemos definir la clase de equivalencia de a como

$$g(C) = [a] = \{b \in G : b \cong a\}$$

donde $C = \langle a \rangle$.

Entonces $g(C)$ es el conjunto de todos los generadores de C y $G = \bigcup_{C \in C(G)} g(C)$. Si G es de orden n, ya que las clases de equivalencia no tienen elementos en común, tenemos que $n = |G| = \sum_{C \in C(G)} |C|$.

Por el lema 8.15, a^k es un generador de G si, sólo si $(k, n) = 1$. Entonces, si φ es la Función de Euler 8.21 y d es el orden C, tenemos la siguiente identidad:

$$|g(C)| = \varphi(d).$$

De donde, por el lema 8.20, el subgrupo C solo tiene un subgrupo por cada b_i divisor de d, entonces

$$d = \sum_{C \in C(G)} |g(C)| = \sum_{b_i | d} \varphi(b_i).$$

Luego, ya que por hipótesis hay a lo más un subgrupo cíclico por cada d_i divisor de n, tenemos que $\sum_{C \in C(G)} |g(C)| \leq \sum_{d_i | n} \varphi(d_i) = n$ y $\sum_{C \in C(G)} |g(C)| =$

$\sum_{b_i|d} \varphi(b_i)$. Por lo tanto, hay exactamente un subgrupo cíclico por cada divisor de n. En particular $n|n$, de donde G es un grupo cíclico. □

Teorema 8.23. *Sean F un campo y $(F^{\#}, *)$, donde $F^{\#} = F - \{0\}$, su grupo multiplicativo. Entonces todo subgrupo finito G de $F^{\#}$ es un grupo cíclico.*

Demostración. Sean $|G| = n$ y d un divisor de n. Si C es un subgrupo cíclico de G de orden d entonces, por el Teorema de Lagrange (8.18), para todo $x \in C$ tenemos que $x^d = 1$. Si existiera otro subgrupo cíclico de orden d entonces existe un elemento $a \notin C$, por lo que $|G| \geq d + 1$, es decir, existe por lo menos $d + 1$ raíces distintas del polinomio $x^d - 1$, lo que es una contradicción al teorema 5.2. Por lo tanto G tiene a lo más un grupo cíclico de orden d. Por el teorema 8.22, G es un grupo cíclico. □

Definición 8.24. Sean R un anillo y $f(x) = \sum_{i=0}^{n} a_i * x^i$ un polinomio en $R[x]$. Llamamos al polinomio en $R[x]$ dado por $f'(x) = \sum_{j=0}^{n-1} (j+1) * a_{j+1} * x^j$ la *derivada de* $f(x)$.

Notemos que si $f'(x) \neq 0$ entonces $\partial(f) > \partial(f')$.

Proposición 8.25. *Sean R un anillo, $f(x) = \sum_{i=0}^{n} a_i * x^i$ y $g(x) = \sum_{j=0}^{m} b_j * x^j$ dos polinomios en $R[x]$ y $f'(x)$ y $g'(x)$ sus respectivas derivadas. Podemos suponer sin perdida de generalidad que $n \leq m$ y $f(x) = \sum_{j=0}^{m} a_j * x^j$ donde $a_j = 0$ si $n < j$. Sea $\alpha \in R$. Entonces:*

(i) $(f(x) + g(x))' = f'(x) + g'(x)$.

(ii) $(\alpha * f(x))' = \alpha * f'(x)$

(iii) $(f(x) * g(x))' = f(x) * g'(x) + f'(x) * g(x)$.

Demostración.

(i)

$$\begin{aligned}(f(x)+g(x))' &= \sum_{j=0}^{m-1}(j+1)*(a_{j+1}+b_{j+1})*x^j \\ &= \sum_{j=0}^{m-1}(j+1)*a_{j+1}*x^j + \sum_{j=0}^{m-1}(j+1)*b_{j+1}*x^j \\ &= f'(x)+g'(x).\end{aligned}$$

(ii)

$$\begin{aligned}(\alpha * f(x))' &= \sum_{j=0}^{m-1}\alpha*(j+1)*a_{j+1}*x^j \\ &= \alpha * \sum_{j=0}^{m-1}(j+1)*a_{j+1}*x^j \\ &= \alpha * f'(x).\end{aligned}$$

(iii) Sean $f(x)=x^i$ y $g(x)=x^j$. Entonces

$$\begin{aligned}(f(x)*g(x))' &= (x^{i+j})' \\ &= (i+j)*x^{i+j-1} \\ &= i*x^{i+j-1} + j*x^{i+j-1} \\ &= f'(x)*g(x) + f(x)*g'(x).\end{aligned}$$

Por (i), (ii) y el desarrollo anterior, $(f(x)*g(x))' = f(x)*g'(x)+' f(x)*g(x)$ para todo $f(x)$ y $g(x)$. □

Proposición 8.26. *Sean F un campo y $f(x) \in F[x]$ un polinomio mónico tal que tiene una factorización de la forma*

$$f(x) = \prod_{j=1}^{m}(x-a_j)$$

donde $a_i \in F$. Entonces, toda raíz de $f(x)$ es de multiplicidad uno si, y solo si, $(f(x), f'(x)) = 1$.

Demostración. Supongamos que toda raíz es de multiplicidad uno y que $(f(x), f'(x)) = d(x) \neq 1$. Entonces existe $p(x) \in F[x]$ de la forma $(x - a_k)$ tal que $p(x)|d(x)$. Podemos suponer, sin perdida de generalidad, que $k = m$, por lo que tenemos $f(x) = g(x) * p(x)$ donde $g(x) = \prod_{j=1}^{m-1} (x - a_j)$ y $p(x) = (x - a_m)$. Luego, $f'(x) = g'(x) * p(x) + g(x) * p'(x) = g'(x) * p(x) + g(x)$. Por 8.12, $p(x)|g(x)$, lo que es una contradicción por ser $g(x)$ producto de factores de la forma $(x - a_j)$ todos distintos a $p(x)$.

Ahora, supongamos que existe una raíz con multiplicidad mayor o igual a dos. Por lo que existe $p(x) = (x-a_k)*(x-a_k)$ tal que $p(x)|f(x)$.Podemos suponer, sin perdida de generalidad, que $k = m$, por lo que tenemos $f(x) = g(x)*p(x)$ donde $g(x) = \prod_{j=1}^{m-2} (x-a_j)$. Luego, $f'(x) = g'(x)*p(x)+g(x)*p'(x)$ donde $p'(x) = 2 * (x - a_k)$, por lo cual $p(x)|g(x) * p'(x)$ y $p(x)|f'(x)$. Por lo tanto, $(f(x), f'(x)) \neq 1$ □

Corolario 8.27. *Sean F un campo y $f(x)$ un polinomio irreducible en F, entonces:*

(*i*) *Si la característica de F es 0, entonces $f(x)$ no tiene raíces de multiplicidad mayor a 1.*

(*ii*) *Si la característica de F es $p > 0$, entonces $f(x)$ tiene una raíz múltiple si, y sólo si, es de la forma $f(x) = g(x^p)$.*

Demostración. Si $f(x)$ tiene una raíz múltiple entonces, por la proposición 8.26, $f(x)$ y $f'(x)$ son divisibles entre un polinomio $p(x)$ con $\partial(p) \geq 1$. Ya que $f(x)$ es un polinomio irreducible, en $F[x]$ solamente es divisible entre los polinomios 1 y $f(x)$, por lo cual $f(x)|f'(x)$. Pero lo anterior solo es posible si $f(x)' = 0$. Entonces, tenemos que

(*i*) Si F es característica 0, $f(x)$ debe de ser un polinomio de grado 0, por lo que no tiene ninguna raíz.

(*ii*) Si F es de característica p, entonces cada coeficiente debe ser cero, esto es, si a_j es un coeficiente en $f(x)$, $p * a_j = 0$. Por lo tanto $f(x)$ debe de ser de la forma $f(x) = g(x^p)$.

□

Bibliografía

[1] A. Baker, *An Introduction to Galois Theory*. Department of Mathematics, University of Glasgow, 2008.

[2] J. B. Fraleigh, *A First Course in Abstract Algebra*. Addison Wesley, 1999.

[3] I. N. Herstein, *Álgebra Moderna: grupos, anillos, campos, teoría de Galois*. Editorial Trillas, 1990.

[4] J. Rotman, *Galois Theory*, Second Edition. Springer, 1998.

[5] I. Stewart, *Galois Theory*. Chapman and Hall, 1989.