Notas del curso de Algebra Moderna I

Luis Valero Elizondo

21 de Agosto del 2004

Índice general

Introducción.

Estas son las notas del curso de Teoría de Grupos (Algebra Moderna I) impartido por Luis Valero Elizondo en la licenciatura de la Universidad Michoacana de San Nicolás de Hidalgo, Morelia, Michoacán, México.

Escribí estas notas para que ustedes (mis alumnos) no tengan que perder tiempo en clase escribiendo. Si se ponen a hacer cuentas, notarán que pasan la mayor parte del tiempo de una clase típica escribiendo, y muy poco tiempo pensando o haciendo activamente matemáticas. En mi clase van a escribir mucho, pero escribirán ideas que se les ocurran a ustedes para resolver los cientos de ejercicios que hay en estas páginas. De vez en cuando yo pasaré al pizarrón para explicar algo, pero la mayor parte del tiempo la van a pasar trabajando en grupos resolviendo ya sea estos ejercicios o las muchas actividades que haremos durante el curso.

Para que ustedes puedan aprovechar al máximo este curso, es indispensable que le dediquen muchas horas de esfuerzo dentro y fuera del salón de clases. Antes de cada clase es muy importante que lean con cuidado el material que vamos a cubrir, que usualmente consistirá de dos secciones de estas notas (pues son secciones muy cortas). Yo les mandaré constantemente mensajes de correo electrónico a todos para decirles qué secciones tienen que preparar, así como para informarles de cualquier cosa relevante, como exámenes próximos o aclaraciones de dudas que hayan salido en clase, o lo que se llegara a necesitar. Por esta razón es importante que tengan una dirección de correo electrónico y que la chequen diariamente. También antes de clase deben intentar hacer todos los ejercicios de las secciones que lean. La mayor parte de estos ejercicios son sencillos, y los podrán hacer sin problema. Los ejercicios más difíciles usualmente están precedidos por ejercicios auxiliares para facilitar su solución. En cualquier caso, incluso si no les sale uno o varios ejercicios, ya habrán pasado un tiempo razonable pensando en ellos, y eso nos será de utilidad cuando cubramos ese material en la clase.

Dentro de la clase vamos a hablar acerca del material que prepararon, y nos vamos a ir con bastante rapidez. Si no prepararon la lección, entonces la clase será tan aburrida como oír gente hablando de una película que no han visto. Si no leyeron las definiciones, no van a saber ni siquiera de lo que estamos hablando; y si leyeron las notas sin haber hecho los ejercicios, no van a poder entender lo que hagamos porque les faltará familiaridad con el tema. No tiene nada de vergorzoso haber intentado los ejercicios y estar atorado en uno o varios; de hecho yo estaré en la mejor disposición de ayudarlos y aclararles sus dudas. Pero es muy importante que ustedes hagan un esfuerzo por aprenderse las definiciones, y que le dediquen al menos 10 minutos a cada ejercicio antes de darse por vencidos. Noten que esto involucra un compromiso de parte de ustedes de al menos unas 4 o 5 horas por semana fuera del salón de clases para dedicarle a mi materia.

Además de los ejercicios tradicionales, incluí varios ejercicios para hacer con ayuda de una computadora. Yo les recomiendo ampliamente el paquete para álgebra GAP (*Groups, Algorithms and Programming*), que está disponible en los laboratorios de cómputo de la Escuela de Físico-Matemáticas de la Universidad Michoacana. Pregunten al encargado del laboratorio al que vayan qué tienen que hacer para correr GAP (probablemente basta que tecleen "gap" en la pantalla seguido de la tecla "Enter"). Ya una vez en GAP, tecleen "?" y la tecla "Enter" para pedir ayuda (por ejemplo, para correr el tutorial). El manual de GAP está incluído en el programa, y se puede consultar en cualquier momento. Por ejemplo, tecleando "?group" y "Enter", GAP les dirá cómo construir grupos. GAP está escrito en inglés.

Los que deseen tener GAP en su computadora personal pueden bajarlo sin costo de `http://www-gap.dcs.st-and.ac.uk/~gap` En este lugar hay otra copia del manual y mayor información acerca de GAP.

Al final de estas notas hay un índice analítico, para facilitarles la vida si necesitan encontrar una definición. Casi siempre cerca de una definición hay ejercicios que tienen que ver con ella, y que les pueden servir de inspiración cuando estén resolviendo otros ejercicios. Por ejemplo, si están atorados en un problema sobre grupos simples, les convendría echarle un vistazo a la Sección 6.7 sobre grupos simples, repasar la definición y ver si alguno de los ejercicios de esa sección les sirve para resolver su problema.

Espero que estas notas les ayuden a entender mejor la teoría de grupos, y que aprendamos y nos divirtamos mucho en nuestro curso.

Capítulo 1

Grupos.

1.1. Operaciones binarias.

Definición 1. Sea C un conjunto no vacío. Una **operación binaria** en C es una función $* : C \times C \longrightarrow C$. Usualmente uno escribe $a * b$ en lugar de $*(a, b)$.

Ejercicio 2. Mencione veinte conjuntos con operaciones binarias.

Definición 3. Sea C un conjunto finito no vacío con una operación binaria $*$. Una **tabla** para la operación binaria $*$ en C es una matriz cuadrada cuyos renglones y columnas están indexados por los elementos de C, y donde la entrada de la tabla ubicada en el renglón a-ésimo y la columna b-ésima (con $a, b \in C$) es el elemento $a * b$. Por ejemplo, la operación binaria $*$ en el conjunto $\{a, b\}$ definida por

$$a * a = a; \qquad a * b = b; \qquad b * a = a; \qquad b * b = b$$

está dada por la siguiente tabla:

$*$	a	b
a	a	b
b	a	b

Computadora 4. Sea $C = \{a, b\}$ un conjunto con dos elementos. Calcule todas las posibles operaciones binarias en C calculando todas sus posibles tablas.

Definición 5. Sea C un conjunto. Una operación binaria $*$ en C es **asociativa** si $a * (b * c) = (a * b) * c$ para todos $a, b, c \in C$.

Ejercicio 6. Mencione diez conjuntos con operaciones binarias asociativas y cinco conjuntos con operaciones binarias que no son asociativas.

Computadora 7. Mencione cuáles de las operaciones binarias del Ejercicio 4 son asociativas.

Ejercicio 8. Sea C un conjunto y sea $*$ una operación binaria asociativa en C. Sean $a, b, c, d \in C$. Demuestre que $a*(b*(c*d)) = (a*b)*(c*d) = ((a*b)*c)*d$.

Ejercicio 9. Sea $*$ una operación binaria asociativa en un conjunto C. Sea n un entero mayor o igual a 3 y sean $a_1, a_2, \ldots, a_n \in C$. Considere una manera fija de asociar para multiplicar $a_1, a_2, \ldots, a_n$ en este orden. Suponga que la última multiplicación es

$$b = (a_1 * \ldots a_i) * (a_{i+1} * \ldots * a_n),$$

con $1 \leq i \leq n-1$. Demuestre por inducción que b es igual a una expresión de la forma $a_1 * (a_2 * \ldots a_n)$, es decir, a una manera de asociar en donde la última multiplicación fue de a_1 con una expresión que involucra a $a_2, a_3, \ldots, a_n$ en este orden. Concluya que b es igual a $a_1 * (a_2 * (\ldots * (a_{n-1} * a_n))) \ldots)$, y por lo tanto dos maneras cualesquiera de multiplicar los elementos $a_1, a_2, \ldots, a_n$ de C en este orden dan el mismo elemento de C.

1.2. Semigrupos.

Definición 10. Un **semigrupo** es un par ordenado $(E, *)$, donde E es un conjunto no vacío y $*$ es una operación binaria asociativa en E. Usualmente denotamos un semigrupo $(E, *)$ simplemente por E.

Ejercicio 11. Mencione diez semigrupos.

Definición 12. Sean E un semigrupo y $a \in E$. Definimos $a^1 = a$, e inductivamente $a^{n+1} = a^n * a$ para todo entero positivo n.

Ejercicio 13. Para cada uno de los siguientes semigrupos E, calcule a^2 y a^3 para a en E arbitrario.

(1) $E = \mathbb{Z}$ con la multiplicación.
(2) $E = \mathbb{Z}$ con la suma.

Ejercicio 14. Sean E un semigrupo, $a \in E$, n, m enteros positivos. Demuestre que $a^n * a^m = a^{n+m}$.

Ejercicio 15. Sean E un semigrupo, $a \in E$, n, m enteros positivos. Demuestre que $(a^n)^m = a^{nm} = (a^m)^n$.

1.3. Grupos.

Definición 16. Un **grupo** es un semigrupo $(G, *)$ que contiene un elemento 1 tal que:

(i) $1 * g = g$ para todo $g \in G$;

(ii) para todo $g \in G$, existe un elemento $h \in G$ tal que $h * g = 1$.

Usualmente uno escribe G para referirse al grupo $(G, *)$, y uno escribe gh en lugar de $g * h$.

Ejercicio 17. Mencione diez grupos.

Ejercicio 18. Sea G un conjunto con un sólo elemento. Demuestre que existe una única operación binaria en G, y que G con esa operación binaria es un grupo. A este tipo de grupo se le llama grupo **trivial**.

Ejercicio 19. Sea G un grupo y sea $1 \in G$ tal que $1g = g$ para todo $g \in G$. Sea $h \in G$ tal que $hh = h$. Demuestre que $h = 1$. Concluya que 1 es el único elemento de G tal que $1g = g$ para todo $g \in G$.

Ejercicio 20. Sea G un grupo, y sea $1 \in G$ tal que $1g = g$ para todo $g \in G$. Sean $g, h \in G$ tales que $hg = 1$.

(1) Demuestre que $ghgh = gh$. Concluya que $gh = 1$.

(2) Simplifique ghg de dos maneras para demostrar que $g1 = g$.

(3) Sea $k \in G$ tal que $kg = 1$. Use (1) y (2) para demostrar que $h = k$.

Ejercicio 21. Sea G un grupo. Entonces

(i) Existe un único elemento $1 \in G$ con $1g = g$ para todo $g \in G$; más aún, tenemos que $1g = g = g1$ para todo $g \in G$. El elemento 1 se llama la **identidad** del grupo G, y usualmente se denota 1. Cuando uno está trabajando con varios grupos simultáneamente, a veces uno escribe 1_G para referirse al elemento identidad del grupo G.

(ii) Para todo $g \in G$ existe un único elemento $h \in G$ tal que $hg = 1$; más aún, tenemos que $hg = 1 = gh$. El elemento h se llama el **inverso** de g, y usualmente se denota g^{-1}.

Notación 22. Al interpretar una expresión que involucre productos e inversos, el inverso se aplica a la expresión inmediata únicamente. Es decir, la expresión $ab^{-1}cd^{-1}$ se debe interpretar como $a(b^{-1})c(d^{-1})$.

Ejercicio 23. Sea C un conjunto con al menos dos elementos y con operación binaria $*$ dada por $a * b = b$ para cualesquiera $a, b \in C$.

(1) Demuestre que $*$ es asociativa.
(2) Demuestre que existe $1 \in C$ tal que $1 * a = a$ para todo $a \in C$.
(3) Demuestre que para todo $a \in C$ existe $b \in C$ tal que $ab = 1$.
(4) Demuestre que $(C, *)$ no es un grupo.

Ejercicio 24. Para cada uno de los siguientes grupos, describa el elemento identidad y el inverso de un elemento g cualquiera.

(1) Los enteros $\mathbb{Z}$ con la suma.
(2) Los racionales distintos de cero con la multiplicación.

Definición 25. Sea G un grupo y sea $\sim$ una relación de equivalencia en G. Decimos que $\sim$ **preserva la operación** del grupo G si para todos $g, h, k, l \in G$ se tiene que si $g \sim h$ y $k \sim l$ entonces $gk \sim hl$.

Ejercicio 26. Sea G un grupo y sea $\sim$ una relación de equivalencia en G que preserva la operación del grupo. Sea $G/{\sim}$ el conjunto de clases de equivalencia de G. Definamos una operación binaria $*$ en $G/{\sim}$ como sigue: Dados $C, D \in G/{\sim}$, escojamos representantes $g \in C$ y $h \in D$; el producto $C * D$ de las clases de equivalencia es la clase que contiene a gh. Demuestre que esta operación binaria $*$ en $G/{\sim}$ está bien definida, y que $G/{\sim}$ con $*$ es un grupo, llamado el **grupo cociente** de G módulo la relación de equivalencia $\sim$. Un elemento C de $G/{\sim}$ se suele denotar $\bar{g}$, donde g es un elemento de C, llamado un **representante** de C.

Capítulo 2

Ejemplos de grupos.

2.1. Grupo aditivo de los enteros módulo *n*.

Definición 27. Sea n un entero positivo. Definimos una relación $\equiv_n$ en los elementos de $\mathbb{Z}$ dada por

$$a \equiv_n b \text{ si y sólo si } n \text{ divide a } a - b.$$

Si a y b están relacionados, decimos que son **congruentes módulo *n***.

Ejercicio 28. Sea n un entero positivo. Demuestre que $\equiv_n$ es una relación de equivalencia en $\mathbb{Z}$.

Ejercicio 29. Sea n un entero positivo. Demuestre que $\equiv_n$ preserva la suma de $\mathbb{Z}$. Concluya que $\mathbb{Z}/\equiv_n$ es un grupo. Demuestre que este grupo tiene exactamente n elementos. Este grupo se llama el **grupo aditivo de los enteros módulo *n***, y se denota C_n.

Ejercicio 30. Calcule la tabla de C_5.

2.2. Grupos simétricos.

Ejercicio 31. Demuestre que la composición de dos funciones biyectivas es biyectiva. Demuestre que la función inversa de una función biyectiva es biyectiva. Sea C un conjunto. Demuestre que la función identidad $id_C : C \longrightarrow C$ es biyectiva.

Ejercicio 32. Sea C un conjunto, y sea S_C el conjunto de las funciones biyectivas de C en sí mismo. Demuestre que S_C junto con la composición de funciones es un grupo. A los elementos de S_C se les llama **permutaciones** del conjunto C. Cuando C es el conjunto $\{1, 2, \ldots, n\}$ con n un entero positivo, escribimos S_n en lugar de S_C, y lo llamamos el **grupo simétrico de grado** $\boldsymbol{n}$.

Ejercicio 33. Sea C un conjunto. Demuestre que S_C es trivial si y sólo si C tiene a lo más un elemento.

2.3. Permutaciones y notación cíclica.

Definición 34. Sea n un entero mayor o igual a dos, y sean $a_1, \ldots, a_m$ elementos distintos de $\{1, \ldots, n\}$. El **ciclo** determinado por la sucesión ordenada $a_1, \ldots, a_m$, denotado $(a_1, \ldots, a_m)$, es la permutación α de S_n dada por

$$\alpha(a) = \begin{cases} a_{i+1} & \text{si } a = a_i \text{ con } i < m \\ a_1 & \text{si } a = a_m \\ a & \text{si } a \notin \{a_1, \ldots, a_m\} \end{cases}$$

Este ciclo tiene **longitud** m; también se dice que α es un m-ciclo.

Observación 35. Note que un mismo ciclo se puede escribir de formas distintas; por ejemplo, (1,2,3)=(3,1,2)=(2,3,1). Note también que (1,2,3) denota un ciclo en S_3, pero también denota un ciclo en S_4 (a saber, la función que fija al 4 y rota 1, 2 y 3), y también denota un ciclo en S_n para cualquier $n \geq 3$.

Notación 36. Al elemento identidad de un grupo simétrico lo denotamos $()$, y se le suele llamar permutación **trivial**.

Ejercicio 37. Calcule el producto (1,2)(2,3).

Computadora 38. Calcule el producto (1,2)*(2,3).

Ejercicio 39. Calcule la tabla de S_3.

Definición 40. Decimos que dos ciclos $(a_1, \ldots, a_m)$ y $(b_1, \ldots, b_t)$ son **disjuntos** (o **ajenos**) si $\{a_1, \ldots, a_m\}$ y $\{b_1, \ldots, b_t\}$ son conjuntos disjuntos. Decimos que una colección de ciclos son disjuntos si son disjuntos dos a dos.

Ejercicio 41. Demuestre que si dos ciclos son ajenos, entonces conmutan. Demuestre con un ejemplo que hay ciclos distintos no disjuntos que conmutan.

Definición 42. Sean n un entero mayor o igual a dos, $\alpha \in S_n$ y $a \in \{1, \ldots, n\}$. Decimos que a es un **punto fijo** bajo α si $\alpha(a) = a$.

Ejercicio 43. Considere la permutación $\alpha \in S_{13}$ dada por la siguiente tabla:

a	1	2	3	4	5	6	7	8	9	10	11	12	13
$\alpha(a)$	7	4	10	5	2	6	3	11	9	1	8	13	12

Calcule los puntos fijos de α.

Ejercicio 44. Escriba a la permutación α como producto de ciclos ajenos en S_{13}.

Ejercicio 45. Calcule el número de puntos fijos de la permutación (1,3) vista como elemento de S_3.

Ejercicio 46. Calcule el número de puntos fijos de la permutación (1,3) vista como elemento de S_8.

2.4. Grupos generales lineales.

Ejercicio 47. Sean n un entero positivo y k un campo. El conjunto de matrices invertibles de tamaño $n \times n$ con coeficientes en k se denota $GL_n(k)$; algunos autores lo denotan $GL(n, k)$. Demuestre que $GL_n(k)$ junto con la multiplicación de matrices es un grupo, llamado el **grupo general lineal** de grado n sobre el campo k. Si el campo k es el campo finito con q elementos, uno suele escribir $GL(n, q)$ en lugar de $GL_n(k)$.

Ejercicio 48. Calcule la tabla de $GL(2, 2)$.

2.5. Grupos diédricos.

Definición 49. Sea C un conjunto, y sea $\sim$ una relación en C (no necesariamente una relación de equivalencia). Decimos que una función biyectiva $f\colon C \longrightarrow C$ es una **simetría con respecto a** $\sim$ si para cualesquiera $a, b \in C$, se tiene que $a \sim b$ si y sólo si $f(a) \sim f(b)$.

Ejercicio 50. Sea C un conjunto, y sea $\sim$ una relación en C. Demuestre que la función identidad de C es una simetría con respecto a la relación $\sim$.

Ejercicio 51. Sea C un conjunto, y sea $\sim$ una relación en C. Demuestre que la función inversa de una simetría con respecto a la relación $\sim$ es también una simetría con respecto a la relación $\sim$.

Ejercicio 52. Sea C un conjunto, y sea $\sim$ una relación en C. Demuestre que la composición de dos simetrías con respecto a la relación $\sim$ es una simetría con respecto a la relación $\sim$.

Ejercicio 53. Sea C un conjunto, y sea $\sim$ una relación en C. Demuestre que las simetrías con respecto a $\sim$ forman un grupo con la composición de funciones. Este grupo se llama el **grupo de simetrías con respecto a la relación** $\sim$.

Ejercicio 54. Sea C un conjunto. Demuestre que existe una relación en C cuyo grupo de simetrías es S_C.

Definición 55. Sea n un entero mayor que 2, sea D un polígono regular de n vértices y sea C el conjunto de los n vértices del polígono. Defina la relación $\sim$ de adyacencia en C, es decir, $a \sim b$ si y sólo si a y b son vértices adyacentes. El grupo de simetrías con respecto a esta relación se llama el **grupo diédrico** de orden $2n$, y se denota D_{2n}.

Ejercicio 56. Demuestre que D_6 es el grupo de permutaciones de un conjunto con tres elementos.

2.6. Productos directos externos.

Definición 57. Sean G y H grupos. El **producto directo externo** de G y H, denotado $G \times H$, es el conjunto de pares ordenados (g, h), donde $g \in G$, $h \in H$, con la operación binaria $(g, h)(k, l) = (gk, hl)$.

Ejercicio 58. Demuestre que el producto directo externo de dos grupos es un grupo.

Capítulo 3

Nociones básicas.

3.1. Algunas propiedades de los grupos.

Ejercicio 59. Sea G un grupo y sean $g, h \in G$. Demuestre que $(gh)^{-1} = h^{-1}g^{-1}$.

Ejercicio 60. Sea G un grupo y sean $g_1, \ldots, g_n$ elementos de G. Demuestre que $(g_1 \ldots g_n)^{-1} = g_n^{-1} \ldots g_1^{-1}$.

Ejercicio 61. (Ley de la cancelación izquierda) Sea G un grupo y sean $g, h, k \in G$ tales que $gh = gk$. Demuestre que $h = k$.

Ejercicio 62. (Ley de la cancelación derecha) Sea G un grupo y sean $g, h, k \in G$ tales que $hg = kg$. Demuestre que $h = k$.

Ejercicio 63. Sea G un grupo finito con tabla T que describe su operación binaria. Demuestre que en cualquier renglón de T aparecen todos los elementos de G sin repetición. Demuestre lo mismo para las columnas de T.

Ejercicio 64. Sea G un grupo y sea $g \in G$. Demuestre que $(g^{-1})^{-1} = g$.

Ejercicio 65. Sean G un grupo, $g \in G$, y n un entero positivo. Demuestre que $(g^n)^{-1} = (g^{-1})^n$.

Definición 66. Sea G un grupo. Para $g \in G$, definimos las **potencias** de g como sigue: Defina $g^0 = 1$; si n es un entero positivo, entonces defina g^n como en la Definición 12, y defina g^{-n} como $(g^{-1})^n$.

Ejercicio 67. Repita el Ejercicio 13 pero con g^{-2} y g^{-3} en lugar de g^2 y g^3.

Ejercicio 68. Sean G un grupo, $g \in G$, n, m enteros (no necesariamente positivos). Demuestre que $(g^n)^m = g^{nm} = (g^m)^n$.

Ejercicio 69. Sean G un grupo, $g \in G$, n, m enteros (no necesariamente positivos). Demuestre que $g^n g^m = g^{n+m}$.

3.2. Grupos abelianos.

Definición 70. Dos elementos g y h en un grupo **conmutan** si $gh = hg$. Un grupo es **abeliano** si para todos $g, h \in G$, se tiene que g y h conmutan. Usualmente en un grupo abeliano se usa **notación aditiva**, es decir, uno escribe $g + h$ en lugar de gh o $g * h$, y el elemento identidad se denota 0 en vez de 1.

Ejercicio 71. Mencione cinco grupos abelianos.

Ejercicio 72. Sea C un conjunto. Demuestre que S_C es abeliano si y sólo si C tiene a lo más dos elementos.

Ejercicio 73. Sean n un entero positivo y k un campo. Demuestre que $GL_n(k)$ es abeliano si y sólo si $n = 1$.

Ejercicio 74. Sea n un entero mayor o igual a 3. Demuestre que D_{2n} no es abeliano.

Ejercicio 75. Sea G un grupo. Demuestre que G es abeliano si y sólo si para cualesquiera $g, h \in G$ se tiene que $(gh)^{-1} = g^{-1}h^{-1}$.

3.3. Orden.

Definición 76. El **orden** de un grupo G, denotado $|G|$, es el número de elementos de G.

Ejercicio 77. Sea n un entero positivo. Demuestre que el orden de S_n es $n!$.

Ejercicio 78. Sea n un entero mayor o igual a 3. Demuestre que en D_{2n} hay exactamente n elementos que son rotaciones del polígono regular de n vértices, y otros n elementos que son reflexiones de dicho polígono. Demuestre que estos son todos los elementos de D_{2n}, por lo que el orden de D_{2n} es efectivamente $2n$.

Ejercicio 79. Sean n un entero positivo y q la cardinalidad de un campo finito. Calcule el orden de $GL(n, q)$.

Definición 80. Sea G un grupo, y sea $g \in G$. Si existe un entero positivo m tal que $g^m = 1$, decimos que el **orden** del elemento g es n donde n es el menor entero positivo tal que $g^n = 1$. De no existir tal entero positivo, decimos que el orden de g es infinito.

Ejercicio 81. Calcule el orden de cada uno de los elementos de C_6.

Ejercicio 82. Calcule el orden de cada uno de los elementos de S_3.

Ejercicio 83. Sea G un grupo, y sea $g \in G$. Demuestre que g tiene orden uno si y sólo si $g = 1$.

Ejercicio 84. Sea G un grupo, y sea $g \in G$ con $g \neq 1$. Demuestre que g tiene orden dos si y sólo si $g = g^{-1}$.

Ejercicio 85. Sea G un grupo tal que todo elemento distinto de 1 tiene orden dos. Demuestre que G es abeliano.

Ejercicio 86. Sea G un grupo, y sea $g \in G$ un elemento de orden finito n. Sea m un entero cualquiera. Demuestre que $g^m = 1$ si y sólo si m es un múltiplo de n.

Ejercicio 87. Sea G un grupo, y sea $g \in G$ un elemento de orden finito n. Sean $m,\ t$ enteros positivos tales que $n = mt$. Demuestre que el orden de g^m es t.

Ejercicio 88. Sea G un grupo, sea $g \in G$ un elemento de orden finito n, y sean m, t enteros cualesquiera. Demuestre que $g^m = g^t$ si y sólo si n divide a $m - t$. Concluya que el conjunto $\{1, g, g^2, \ldots, g^{n-1}\}$ contiene a todas las posibles potencias de g sin repetición.

Ejercicio 89. Sea G un grupo, y sea $g \in G$ un elemento de orden infinito. Demuestre que para cualesquiera enteros $n,\ m$ se tiene que $g^n = g^m$ si y sólo si $n = m$. Concluya que G tiene orden infinito.

Ejercicio 90. Sea G un grupo, y sea $g \in G$. Demuestre que el orden de g es menor o igual al orden de G.

3.4. Conjugación.

Definición 91. Sea G un grupo y sea $g \in G$. Un **conjugado** de g en G es un elemento de la forma hgh^{-1}, donde $h \in G$. Se denota hgh^{-1} por ${}^{h}g$. Recuerde que por convención (véase 22), hgh^{-1} denota $hg(h^{-1})$.

Ejercicio 92. Sea G un grupo arbitrario. Demuestre que la relación "g es conjugado a h en G."es una relación de equivalencia en G. Las clases de equivalencia bajo esta relación se llaman **clases de conjugación** de G.

Ejercicio 93. Calcule las clases de conjugación de S_3.

Ejercicio 94. Demuestre que un grupo es abeliano si y sólo si todas sus clases de conjugación son conjuntos de cardinalidad uno.

3.5. Conjugación en los grupos simétricos.

Ejercicio 95. Sean n un entero mayor o igual a dos, $\alpha \in S_n$ y $a, b \in \{1, \ldots, n\}$. Decimos que a esta **conectado** a b bajo α si existe $m \in \mathbb{Z}$ tal que $\alpha^m(a) = b$. Demuestre que "estar conectado bajo α" es una relación de equivalencia en $\{1, \ldots, n\}$. Sus clases de equivalencia se llaman las **órbitas** de la permutación α en $\{1, \ldots, n\}$.

Ejercicio 96. Calcule las órbitas de la permutación del Ejercicio 43.

Ejercicio 97. Sean n un entero mayor o igual a dos, $\alpha \in S_n$ una permutación no trivial, y Ω una órbita de α en $\{1, \ldots, n\}$. Demuestre que la restricción de α a Ω es un ciclo. Concluya que la permutación α o es un ciclo, o bien se puede escribir como un producto de ciclos disjuntos.

Ejercicio 98. Sea n un entero mayor o igual a dos, y $\theta_1, \ldots, \theta_m$ ciclos disjuntos en S_n. Sea $\alpha = \theta_1 \ldots \theta_m$. Demuestre que las órbitas de α están determinadas por los ciclos $\theta_1, \ldots, \theta_m$. Demuestre que cada uno de los ciclos θ_i es la restricción de α a una de sus órbitas. Concluya que la factorización de una permutación no trivial como producto de ciclos ajenos es única salvo el orden de los ciclos.

Definición 99. Sea n un entero mayor o igual a dos, y sea α en S_n. La **estructura cíclica** de α es la sucesión $m_1, m_2, \ldots$, donde m_1 es el número de puntos fijos de α en $\{1, \ldots, n\}$, y m_i con $i \geq 2$ es el número de i-ciclos que aparecen en cualquier descomposición de α como producto de ciclos disjuntos.

Ejercicio 100. Calcule la estructura cíclica de la permutación del Ejercicio 43.

Ejercicio 101. Sean $\alpha = (1, 2, 3)(4, 5)(6, 7, 8, 9)$ y $\beta = (1, 3, 5)(2, 7)$. Calcule $\alpha\beta\alpha^{-1}$ como producto de ciclos ajenos.

Ejercicio 102. Sea n un entero positivo, y sean α y β en S_n. Demuestre que $\alpha\beta\alpha^{-1}$ es la permutacion que tiene la misma estructura ciclica que β y que se obtiene aplicando α a los simbolos en β.

Ejercicio 103. Sea n un entero positivo. Demuestre que dos permutaciones son conjugadas en S_n si y solo si tienen la misma estructura ciclica.

Ejercicio 104. Calcule el número de clases de conjugación de S_4.

Capítulo 4

Homomorfismos.

4.1. Homomorfismos.

Definición 105. Sean $(G, *)$ y $(H, \circ)$ grupos. Un **homomorfismo** $\varphi : G \longrightarrow H$ es una función tal que $\varphi(g * h) = \varphi(g) \circ \varphi(h)$ para todo $g, h \in G$. Note que por esta vez escribimos explícitamente las dos operaciones binarias involucradas. Con nuestra convención usual, escribiríamos $\varphi(gh) = \varphi(g)\varphi(h)$. Un **monomorfismo** es un homomorfismo inyectivo. Un **epimorfismo** es un homomorfismo suprayectivo. Un **isomorfismo** es un homomorfismo biyectivo. Un **endomorfismo** es un homomorfismo de un grupo en sí mismo. Un **automorfismo** es un isomorfismo de un grupo en sí mismo. Dos grupos G y H son **isomorfos**, denotado $G \cong H$, si existe un isomorfismo de G en H. Cuando los grupos G y H tienen más estructura que la de grupo (como por ejemplo $\mathbb{Q}$ y $\mathbb{R}$, que son campos), uno suele decir **homomorfismo de grupos** en vez de "homomorfismo".

Ejercicio 106. Mencione diez ejemplos de homomorfismos de grupos.

Ejercicio 107. Sean G y H grupos. Demuestre que la función $\varphi : G \longrightarrow H$ dada por $\varphi(g) = 1_H$ para todo $g \in G$ es un homomorfismo (donde 1_H denota al elemento identidad de H). Este homomorfismo se llama el **homomorfismo trivial** de G en H.

Ejercicio 108. Demuestre que la composición de dos homomorfismos es un homomorfismo.

Ejercicio 109. Dé ejemplos de lo siguiente:

(1) Un monomorfismo de grupos que no es epimorfismo.
(2) Un epimorfismo de grupos que no es monomorfismo.
(3) Un endomorfismo de grupos que no es isomorfismo.
(4) Un homomorfismo de grupos que no es monomorfismo ni epimorfismo.
(5) Un isomorfismo de grupos que no es automorfismo.

4.2. Algunas propiedades de los homomorfismos.

Ejercicio 110. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que φ manda al elemento identidad de G en el elemento identidad de H, es decir, $\varphi(1_G) = 1_H$.

Ejercicio 111. Sean G y H grupos, $\varphi : G \longrightarrow H$ un homomorfismo, y sea $g \in G$. Demuestre que φ manda inversos en inversos, es decir, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Ejercicio 112. Sean G y H grupos, $\varphi : G \longrightarrow H$ un homomorfismo, y sea $g \in G$. Demuestre que φ preserva potencias, es decir, para cualquier entero n se tiene que $\varphi(g^n) = \varphi(g)^n$.

Ejercicio 113. Sean G y H grupos y $\varphi : G \longrightarrow H$ un homomorfismo. Sea $g \in G$ un elemento de orden finito. Demuestre que $\varphi(g)$ tiene orden finito, y que de hecho el orden de $\varphi(g)$ es un divisor del orden de g.

4.3. Isomorfismos.

Ejercicio 114. Sea G un grupo. Demuestre que la **función identidad** de G, es decir, $id_G : G \longrightarrow G$ dada por $id_G(g) = g$ para toda g en G, es un automorfismo del grupo G.

Ejercicio 115. Sean G un grupo y $g \in G$. Defina la función $\varsigma_g : G \longrightarrow G$ por $\varsigma_g(h) = ghg^{-1}$ para todo $h \in G$. Demuestre que ς_g es un automorfismo de G, llamado un automorfismo **interno**.

Ejercicio 116. Demuestre que la composición de dos isomorfismos es un isomorfismo.

Ejercicio 117. Demuestre que el inverso de un isomorfismo es un isomorfismo.

Ejercicio 118. Sea G un grupo. Demuestre que el conjunto de los automorfismos de G es un grupo con la composición de funciones. Este grupo se llama el **grupo de automorfismos** de G.

Ejercicio 119. Sean G, H, K grupos.
(i) Demuestre que $G \cong G$.
(ii) Demuestre que si $G \cong H$, entonces $H \cong G$.
(iii) Demuestre que si $G \cong H$ y $H \cong K$, entonces $G \cong K$.

Ejercicio 120. Encuentre un criterio para que dos grupos finitos sean isomorfos en términos de sus tablas.

4.4. Grupos de orden menor o igual a 8.

Ejercicio 121. Sean G y H grupos triviales (es decir, cada uno tiene un sólo elemento). Demuestre que G y H son isomorfos. Este hecho se enuncia diciendo que existe un único grupo trivial **hasta isomorfismo**. Debido a este hecho, uno usualmente dice **el** grupo trivial para referirse a un grupo trivial.

Ejercicio 122. Sea $G = \{1, g\}$ un grupo de orden dos. Demuestre que la operación binaria de G está forzosamente dada por la tabla

$*$	1	g
1	1	g
g	g	1

Ejercicio 123. Demuestre que dos grupos cualesquiera de orden dos son isomorfos. Debido a este hecho, uno usualmente dice **el** grupo de orden dos para referirse a un grupo de orden dos.

Ejercicio 124. Sea $G = \{1, g, h\}$ un grupo de orden tres. Demuestre que la operación binaria de G está forzosamente dada por la tabla

$*$	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

Ejercicio 125. Demuestre que dos grupos cualesquiera de orden tres son isomorfos. Debido a este hecho, uno usualmente dice **el** grupo de orden tres para referirse a un grupo de orden tres.

Computadora 126. Demuestre que existen sólo dos grupos de orden 4 hasta isomorfismo, a saber, C_4 y $C_2 \times C_2$.

Computadora 127. Demuestre que existe un único grupo de orden 5 hasta isomorfismo, a saber, C_5.

Computadora 128. Demuestre que existen sólo dos grupos de orden 6 hasta isomorfismo, a saber, C_6 y S_3. Concluya que S_3 es el único grupo no abeliano de orden 6 hasta isomorfismo.

Computadora 129. Demuestre que existe un único grupo de orden 7 hasta isomorfismo, a saber, C_7.

Computadora 130. Demuestre que existen sólo cinco grupos de orden 8 hasta isomorfismo, a saber, C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, y otro grupo no abeliano que se denota Q_8, llamado el grupo de los **cuaternios**.

Capítulo 5

Subgrupos.

5.1. Subgrupos.

Definición 131. Un subconjunto no vacío S de un grupo G es un **subgrupo** de G si para todos $g, h \in S$ se tiene que g^{-1} y gh están en S. Si S es un subgrupo de G, lo denotamos $S \leq G$. Decimos que S es un subgrupo **propio** de G si $S \leq G$ y $S \neq G$, y lo denotamos $S < G$. Para algunos autores $S < G$ significa que S es un subgrupo de G (que puede o no ser propio).

Ejercicio 132. Sean n un número entero, y sea $n\mathbb{Z}$ el conjunto de **múltiplos de $\boldsymbol{n}$**, es decir, $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Demuestre que $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.

Ejercicio 133. Sea G un grupo. Demuestre que G mismo en un subgrupo de G.

Ejercicio 134. Sea G un grupo. Demuestre que $\{1\}$ es un subgrupo de G, llamado el **subgrupo trivial** de G, y denotado a veces 1 en vez de $\{1\}$.

Ejercicio 135. Sea G un grupo y S un subgrupo de G. Demuestre que $1 \in S$.

Ejercicio 136. Calcule todos los subgrupos de S_3.

Ejercicio 137. Sea S un subgrupo de $\mathbb{Z}$. Demuestre que existe un entero n tal que S es el conjunto de los múltiplos de n, es decir, $S = n\mathbb{Z}$.

Ejercicio 138. Demuestre que un subgrupo S de G es un grupo cuya operación binaria es la operación de G restringida a S, y que la inclusión $i : S \longrightarrow G$ es un homomorfismo. Demuestre que, inversamente, si $(S, \circ)$ y $(G, *)$ son grupos con $S \subseteq G$ y si la inclusión $i : S \longrightarrow G$ es un homomorfismo, entonces S es un subgrupo de G y $\circ$ es la restricción de $*$ a S.

Ejercicio 139. Dé un ejemplo de un grupo G y un subconjunto S tal que S no sea un subgrupo de G, pero que S sea un grupo con una operación distinta a la que hereda de G.

Ejercicio 140. Sea S un subconjunto de un grupo G. Demuestre que S es un subgrupo de G si y sólo si S es no vacío y para todos $g, h \in S$, se tiene que $gh^{-1} \in S$.

Ejercicio 141. Sea S un subgrupo de un grupo G, y sea $g \in G$. Demuestre que el conjunto gSg^{-1} definido como $\{ghg^{-1} \mid h \in S\}$ es un subgrupo de G, llamado el **conjugado** de S por g, y que se denota ${}^{g}S$.

Ejercicio 142. Demuestre que la intersección de cualquier familia de subgrupos de G es un subgrupo de G.

Ejercicio 143. Sea $\mathbb{K} = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Demuestre que $\mathbb{K}$ es un subgrupo de S_4. Al grupo $\mathbb{K}$ se le llama el **grupo cuatro de Klein**.

Ejercicio 144. Sea G un grupo abeliano. Demuestre que cualquier subgrupo de G es abeliano.

5.2. Generadores.

Ejercicio 145. Sea C un subconjunto de un grupo G. Demuestre que existe un único subgrupo de G que contiene a C y que está contenido en cualquier otro subgrupo de G que contiene a C. Este subgrupo se denota $< C >$, y se llama el **subgrupo generado por *C***. Decimos que el conjunto C **genera** al subgrupo $< C >$. Si $C = \{g_1, \ldots, g_n\}$, escribimos $< g_1, \ldots, g_n >$ en lugar de $< \{g_1, \ldots, g_n\} >$ y decimos que los $g_1, \ldots, g_n$ son los **generadores** del subgrupo $< g_1, \ldots, g_n >$.

Ejercicio 146. Sea G un grupo cualquiera. Demuestre que el subgrupo generado por el conjunto vacío es el subgrupo trivial.

Ejercicio 147. Calcule el subgrupo de S_3 generado por $(1,2,3)$.

Ejercicio 148. Sean G un grupo y $g \in G$. Demuestre que $< g >$ es el conjunto de todas las potencias de g.

Ejercicio 149. Sean G un grupo y $g \in G$. Demuestre que el orden de g es igual al orden del subgrupo $< g >$.

Definición 150. Sea C un subconjunto de un grupo G. Una **palabra** en C es un elemento $g \in G$ de la forma $g = g_1^{e_1} \dots g_n^{e_n}$, donde $g_i \in C$ y $e_i \in \{1, -1\}$. También se dice el 1 es una palabra en C, llamada la **palabra vacía**.

Ejercicio 151. Sea C un subconjunto de un grupo G. Demuestre que $< C >$ es el conjunto de todas las palabras en C.

Ejercicio 152. Sean S y T subgrupos del grupo G. Denote $S \bigvee T =< S \cup T >$. Demuestre que $S \bigvee T$ es el menor subgrupo de G que contiene tanto a S como a T.

5.3. Grupos cíclicos.

Definición 153. Un grupo G se llama **cíclico** si $G =< g >$ para algún $g \in G$. En este caso decimos que g es un **generador** de G.

Ejercicio 154. Demuestre que todo grupo de orden 1 debe ser cíclico.

Ejercicio 155. Demuestre que todo grupo de orden 2 debe ser cíclico.

Ejercicio 156. Demuestre que todo grupo de orden 3 debe ser cíclico.

Ejercicio 157. Sea G un grupo cíclico finito, y sea H un grupo cualquiera. Sea g un generador de G y sea h un elemento cualquiera de H. Demuestre que existe un homomorfismo $\varphi : G \longrightarrow H$ tal que $\varphi(g) = h$ si y sólo si el orden de h divide el orden de g. Demuestre que en tal caso, dicho homomorfismo es único.

Ejercicio 158. Sea G un grupo cíclico infinito, y sea H un grupo cualquiera. Sea g un generador de G y sea h un elemento cualquiera de H. Demuestre que existe un único homomorfismo $\varphi : G \longrightarrow H$ tal que $\varphi(g) = h$.

Ejercicio 159. Demuestre que todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.

Ejercicio 160. Sean G y H dos grupos isomorfos y sea $\varphi : G \longrightarrow H$ un isomorfismo. Demuestre que G es cíclico si y sólo si H es cíclico. Demuestre además que g es un generador de G si y sólo si $\varphi(g)$ es un generador de H.

Ejercicio 161. Demuestre que dos grupos cíclicos son isomorfos si y sólo si tienen el mismo orden.

Ejercicio 162. Sea G un grupo cíclico no trivial de orden finito. Demuestre que el orden de G es un número primo si y sólo si todo elemento no trivial de G es un generador de G.

Ejercicio 163. Sea G un grupo cíclico de orden n. Demuestre que para cada divisor m de n, existe un único subgrupo de G de orden m.

Ejercicio 164. Sea G un grupo no trivial cuyos únicos subgrupos son G y el trivial. Demuestre que G es un grupo cíclico finito y que su orden es un número primo.

Ejercicio 165. Sea G un grupo cíclico con generador g, y sea S un subgrupo no trivial de G. Sea n el menor entero positivo tal que $g^n \in S$. Demuestre que g^n genera a S. Concluya que cualquier subgrupo de G es cíclico.

5.4. Centralizadores y el centro.

Definición 166. Sea G un grupo. El **centro** de G, denotado $Z(G)$, es el conjunto de todas las $g \in G$ que conmutan con todos los elementos de G, es decir, $Z(G) = \{g \in G \mid gh = hg \text{ para toda } h \in G\}$.

Ejercicio 167. Calcule $Z(S_3)$.

Ejercicio 168. Sea G un grupo. Demuestre que $Z(G)$ es un subgrupo de G.

Ejercicio 169. Sea G un grupo. Demuestre que G es abeliano si y sólo si $Z(G) = G$.

Definición 170. Sea G un grupo, y sea $g \in G$. El **centralizador** de g en G, denotado $C_G(g)$, es el conjunto de todas las $h \in G$ que conmutan con g, es decir, $C_G(g) = \{h \in G \mid gh = hg\}$.

Ejercicio 171. Calcule $C_{S_3}((1,2))$.

Ejercicio 172. Sea G un grupo, y sea $g \in G$. Demuestre que $C_G(g)$ es el subgrupo abeliano de G más pequeño que contiene a g.

5.5. Productos de subconjuntos.

Definición 173. Sean C y D subconjuntos no vacíos de un grupo G. Definimos el **producto de los subconjuntos** C y D, denotado CD, como el conjunto $\{gh \mid g \in C \text{ y } h \in D\}$. También escribimos gC en lugar de $\{g\}C$, y Cg en lugar de $C\{g\}$.

Ejercicio 174. Sea G un grupo y sean C, D y E subconjuntos no vacíos de G. Demuestre que $(CD)E = C(DE)$. Por esta razón, uno denota este conjunto como CDE.

Ejercicio 175. Sea G un grupo, sea $g \in G$ y sean C y D subconjuntos no vacíos de G. Demuestre que $gC = D$ si y sólo si $C = g^{-1}D$.

Ejercicio 176. Sea G un grupo, sea $g \in G$ y sean C y D subconjuntos no vacíos de G. Demuestre que $Cg = D$ si y sólo si $C = Dg^{-1}$.

5.6. Clases laterales izquierdas

Definición 177. Sea S un subgrupo de un grupo G. Una **clase lateral izquierda** de S en G es un subconjunto de la forma gS, con $g \in G$. Decimos que g es un representante de gS. Análagomente, una **clase lateral derecha** de S en G es un subconjunto de la forma Sg, el cuál también tiene a g como representante.

Ejercicio 178. Sea S el subgrupo de S_3 generado por (1,2). Calcule las clases laterales izquierdas de S en S_3. Calcule también las clases laterales derechas de S en S_3.

Ejercicio 179. Repita el Ejercicio 178 tomando como subgrupo S al generado por (1,2,3).

Ejercicio 180. Sean G un grupo, S un subgrupo de G y $g \in G$. Demuestre que $gS = S$ si y sólo si $g \in S$. Enuncie y demuestre un resultado análogo para Sg.

Ejercicio 181. Sean G un grupo, S un subgrupo de G y $g, h \in G$. Demuestre que las siguientes condiciones son equivalentes:

(1) $gS = hS$;
(2) $h \in gS$;

(3) $g \in hS$;
(4) $g^{-1}h \in S$;
(5) $h^{-1}g \in S$;
(6) gS y hS son no disjuntas.

Ejercicio 182. Enuncie y demuestre un resultado análogo al del Ejercicio 181 para clases laterales derechas.

Ejercicio 183. Sea S el subgrupo de S_3 generado por (1,2). Demuestre que $(1,3)S \neq S(1,3)$. Concluya que $(1,3)S$ no es una clase lateral derecha de S en S_3.

Ejercicio 184. Sean G un grupo, S un subgrupo de G y $g, h \in G$. Demuestre que $gS = hS$ si y sólo si $Sg^{-1} = Sh^{-1}$.

Ejercicio 185. Sea G un grupo y sea S un subgrupo de G. Demuestre que la asignación que manda a cada clase lateral izquierda gS en Sg^{-1} es una biyección bien definida del conjunto de clases laterales izquierdas de S en G al conjunto de clases laterales derechas de S en G. Concluya que el número de clases laterales izquierdas de S en G es igual al número de clases laterales derechas de S en G.

Definición 186. Sea G un grupo y sea S un subgrupo de G. El **índice** de S en G, denotado $[G : S]$, es el número de clases laterales izquierdas de S en G.

Ejercicio 187. Calcule el índice del subgrupo generado por (1,2) en S_3.

Ejercicio 188. Calcule el índice del subgrupo generado por la clase del 8 en C_{12}.

Ejercicio 189. Calcule el índice del subgrupo generado por 5 en $\mathbb{Z}$.

5.7. Teorema de Lagrange.

Ejercicio 190. Sean G un grupo, S un subgrupo de G y $g \in G$. Demuestre que gS tiene la misma cardinalidad que S.

Ejercicio 191. (Teorema de Lagrange) Sea S un subgrupo de un grupo G. Demuestre que $[G : S]|S| = |G|$. Concluya que si G es finito, el orden del subgrupo S divide al orden del grupo G y $[G : S] = |G|/|S|$.

Ejercicio 192. Sean G un grupo finito y $g \in G$. Demuestre que el orden de g divide al orden de G.

Ejercicio 193. Sea G un grupo cuyo orden es un número primo. Demuestre que G es cíclico.

Capítulo 6

Subgrupos normales.

6.1. Subgrupos normales.

Definición 194. Sean G un grupo y N un subgrupo de G. Decimos que N es un **subgrupo normal** de G (o también se dice que N es normal en G), denotado $N \trianglelefteq G$, si $gNg^{-1} = N$ para toda $g \in G$. La notación $N \triangleleft G$ significa que N es un subgrupo normal de G distinto de G.

Ejercicio 195. Sean N el subgrupo de S_3 generado por (1,2,3), y S el subgrupo generado por (1,2). Demuestre que N es un subgrupo normal de S_3, pero que S no es un subgrupo normal de S_3.

Ejercicio 196. Demuestre que el grupo cuatro de Klein es un subgrupo normal de S_4.

Ejercicio 197. Sea G un grupo abeliano. Demuestre que todo subgrupo de G es normal en G.

Computadora 198. Encuentre un grupo no abeliano de orden ocho tal que todos sus subgrupos sean normales.

Ejercicio 199. Sean G un grupo y N un subgrupo de G. Demuestre que son equivalentes:

(1) N es un subgrupo normal de G
(2) $gNg^{-1} \subseteq N$ para toda $g \in G$.
(3) para cualesquiera $g, h \in G$, si $gh \in N$ entonces $hg \in N$.
(4) $gN = Ng$ para toda $g \in G$.
(5) El conjunto de clases laterales izquierdas de N en G coincide con el conjunto de clases laterales derechas de N en G.

Ejercicio 200. Sean G un grupo, S un subgrupo finito de G y $g \in G$. Demuestre que $gSg^{-1} = S$ si y sólo si $gSg^{-1} \subset S$.

Ejercicio 201. Sea $S_{\mathbb{Z}}$ el grupo de permutaciones del conjunto de números enteros. Sea $S = \{\alpha \in S_{\mathbb{Z}} \mid \alpha(n) = n \text{ para toda } n \leq 0\}$. Demuestre que S es un subgrupo de $S_{\mathbb{Z}}$. Encuentre un elemento $g \in S_{\mathbb{Z}}$ tal que $gSg^{-1} \subset S$, pero $gSg^{-1} \neq S$.

Ejercicio 202. Sean G un grupo, N un subgrupo normal de G y S un subgrupo de G. Demuestre que $NS = N \bigvee S = SN$. En particular, NS es un subgrupo de G.

Ejercicio 203. Sean G un grupo, N y M subgrupos normales de G Demuestre que $N \bigvee M$ es un subgrupo normal de G.

Ejercicio 204. Sean G un grupo y $N,\ S$ subgrupos de G con $N \leq S$. Demuestre que si N es un subgrupo normal de G, entonces N es un subgrupo normal de S.

Ejercicio 205. Demuestre que la normalidad de subgrupos no es transitiva, es decir, dé un ejemplo de subgrupos $M \leq N \leq G$ de un grupo G con M normal en N y N normal en G, pero tal que M no es normal en G.

Ejercicio 206. Sean G un grupo y $N,\ S$ subgrupos de G. Demuestre que si N es un subgrupo normal de G, entonces $N \cap S$ es un subgrupo normal de S.

Ejercicio 207. (Ley modular) Sean G un grupo y $N,\ M,\ L$ subgrupos normales de G con $N \leq M$. Demuestre que si $N \cap L = M \cap L$ y $NL = ML$, entonces $N = M$.

Ejercicio 208. (Ley de Dedekind) Sean G un grupo y $N,\ M,\ L$ subgrupos normales de G con $N \leq L$. Demuestre que $(NM) \cap L = N(M \cap L)$.

6.2. Productos directos internos.

Definición 209. Sea G un grupo con subgrupos normales N y M. Si $N \cap M = \{1\}$ y $NM = G$, entonces decimos que G es el **producto directo interno** de los subgrupos N y M.

Ejercicio 210. Demuestre que C_6 es el producto directo interno de un subgrupo de orden dos con un subgrupo de orden tres.

Ejercicio 211. Sea G un grupo con subgrupos normales N y M tales que G es el producto directo interno de N y M. Demuestre que para todo $g \in N$ y para todo $h \in M$ se tiene que $gh = hg$.

Ejercicio 212. Sea G un grupo con subgrupos normales N y M tales que G es el producto directo interno de N y M. Demuestre que $G \cong N \times M$.

6.3. Productos semidirectos internos.

Definición 213. Sea G un grupo, y sean N y S subgrupos de G. Decimos que el grupo G es el **producto semidirecto interno** de N por S, denotado $G = N \rtimes S$, si se cumplen las tres condiciones siguientes:

(i) N es normal en G;

(ii) $NS = G$;

(iii) $N \cap S = \{1\}$.

Ejercicio 214. Sea $G = S_3$, y sea S cualquier subgrupo de S_3 de orden dos. Demuestre que S_3 es el producto semidirecto interno de A_3 por S, pero que S_3 no es el producto directo interno de A_3 y S.

Ejercicio 215. Sea G un grupo, y sean S y T subgrupos de G tales que $S \cap T = \{1\}$. Demuestre que para cualesquiera $g, h \in S$ y $k, l \in T$, se tiene que $gk = hl$ si y sólo si $g = h$ y $k = l$.

Ejercicio 216. Sea G un grupo, y sean N y S subgrupos de G tales que $G = N \rtimes S$. Demuestre que $|G| = |N|\ |S|$.

Ejercicio 217. Sea G un grupo, y sean S y T subgrupos de G. Demuestre que son equivalentes las siguientes condiciones:

(i) G es el producto directo interno de S y T

(ii) G es el producto semidirecto interno de S por T y también el producto semidirecto interno de T por S.

6.4. Núcleos e imágenes.

Definición 218. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. El **núcleo** de φ, denotado $\mathrm{Ker}(\varphi)$, es el conjunto $\{g \in G \mid \varphi(g) = 1_H\}$. La **imagen** de φ, denotada $\mathrm{Im}(\varphi)$, es el conjunto $\{\varphi(g) \mid g \in G\}$.

Ejercicio 219. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que $\mathrm{Ker}(\varphi)$ es un subgrupo normal de G.

Ejercicio 220. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que φ es el homomorfismo trivial si y sólo si $\mathrm{Ker}(\varphi) = G$.

Ejercicio 221. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que φ es inyectivo si y sólo si $\mathrm{Ker}(\varphi)$ es el subgrupo trivial.

Ejercicio 222. Sean G y H grupos, y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que $\mathrm{Im}(\varphi)$ es un subgrupo de H. Dé un ejemplo en el que $\mathrm{Im}(\varphi)$ no sea un subgrupo normal de H.

6.5. Transposiciones.

Definición 223. Una **transposición** es un ciclo de longitud dos.

Ejercicio 224. Escriba el ciclo (1,2,3) como producto de dos transposiciones en S_3.

Ejercicio 225. Escriba el ciclo (1,2,3,4) como producto de transposiciones en S_4.

Ejercicio 226. Sea n un entero positivo. Demuestre que todo ciclo en S_n se puede escribir como producto de transposiciones.

Ejercicio 227. Sea n un entero positivo. Demuestre que toda permutación en S_n se puede escribir como producto de transposiciones.

Ejercicio 228. Sea n un entero mayor que 2. Demuestre que toda transposición en S_n se puede escribir como producto de transposiciones de la forma $(i, i+1)$ con $1 \leq i < n$. Concluya que S_n está generado por {(1,2), (2,3), (3,4), …, $(n-1, n)$}.

Ejercicio 229. Sea n un entero positivo. Demuestre que S_n está generado por $\{(1,2),(1,2,3,\ldots,n)\}$.

6.6. Grupos alternantes.

Ejercicio 230. Sea n un entero mayor o igual a 3, y sean τ y σ transposiciones distintas en S_n. Suponga que $\sigma(n) \neq n$ (es decir, n es uno de los dos puntos que σ mueve). Demuestre que existen transposiciones ρ y π tales que $\tau\sigma = \rho\pi$ y $\pi(n) = n$.

Ejercicio 231. Sea n un entero mayor o igual a 3, y sean $\tau_1, \tau_2, \ldots, \tau_m$ transposiciones en S_n tales que $\tau_1(n) \neq n$ y $\tau_i(n) = n$ para toda $2 \leq i \leq m$. Demuestre que $() \neq \tau_1 \ldots \tau_m$.

Ejercicio 232. Sea n un entero mayor o igual a 2, y sean $\tau_1, \tau_2, \ldots, \tau_m$ transposiciones en S_n tales que $() = \tau_1 \ldots \tau_m$. Demuestre que m es un número par.

Ejercicio 233. Sea n un entero positivo. Demuestre que dada una permutación fija α en S_n, el número de factores en cualquier factorización de α en transposiciones es siempre par o siempre impar. Si el número de transposiciones es par, la permutación α se llama **par**, y se dice que tiene **signo 1**; de lo contrario, la permutación α se llama **impar**, y se dice que tiene **signo -1**.

Ejercicio 234. Calcule las paridades de las siguientes permutaciones: (1,2), (1,2,3), (3,8,4), (1,2,3,4), (1,2)(3,4), (1,2)(3,4,5), (1,2,3,4,5).

Ejercicio 235. Sea n un entero mayor que 1. Demuestre que un ciclo de longitud n es par si y sólo si n es impar.

Ejercicio 236. Demuestre que el producto de dos permutaciones pares es una permutación par, el producto de dos permutaciones impares es par, y el producto de una permutación par por una impar es impar.

Ejercicio 237. Sea n un entero positivo. Demuestre que la función signo es un homomorfismo de grupos de S_n en el grupo multiplicativo $\{1, -1\}$. Su núcleo se llama el **grupo alternante de grado** n, y se denota A_n. Demuestre que A_n es un subgrupo normal de S_n de índice 2, y que consiste de todas las permutaciones pares de S_n.

Ejercicio 238. Calcule todos los elementos de A_3.

Ejercicio 239. Calcule todos los elementos de A_4.

Ejercicio 240. Sea n un entero mayor que o igual a 3. Demuestre que A_n es un grupo de orden $n!/2$.

Ejercicio 241. Sea n un entero mayor o igual a 3. Demuestre que A_n contiene todos los 3-ciclos de S_n.

Ejercicio 242. Sea n un entero mayor o igual a 3, y sea S un subgrupo no trivial de S_n. Demuestre que $S \cap A_n = \{1\}$ si y sólo si S es el subgrupo generado por una permutación impar de orden dos.

6.7. Grupos simples.

Definición 243. Un grupo no trivial G es **simple** si G no tiene subgrupos normales propios no triviales.

Ejercicio 244. Sea G un grupo abeliano. Demuestre que G es simple si y sólo si G es un grupo cíclico de orden primo.

Ejercicio 245. Sea n un entero mayor o igual a 3. Demuestre que S_n no es un grupo simple.

Ejercicio 246. Sean n un entero mayor o igual a 2 y k un campo. Demuestre que $GL_n(k)$ no es un grupo simple.

Ejercicio 247. Demuestre que A_4 no es un grupo simple.

Ejercicio 248. Sea G y H grupos y $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que si G es simple y φ no es el homomorfismo trivial, entonces φ es inyectivo.

6.8. Simplicidad de A_n para $n \geq 5$.

Computadora 249. Demuestre que A_5 es un grupo simple.

Computadora 250. Demuestre que todos los 3-ciclos de A_5 son conjugados en A_5.

Computadora 251. Demuestre que A_6 es un grupo simple.

Ejercicio 252. Sea n un entero mayor o igual a 5. Demuestre que el producto de dos transposiciones cualesquiera en S_n se puede escribir como producto de 3-ciclos. Concluya que A_n está generado por el conjunto de todos sus 3-ciclos.

Ejercicio 253. Sea n un entero mayor o igual a 5. Demuestre que todos los 3-ciclos de A_n son conjugados en A_n.

Ejercicio 254. Sea n un entero mayor o igual a 5 y sea N un subgrupo normal de A_n. Demuestre que si N contiene un 3-ciclo, entonces $N = A_n$.

Ejercicio 255. Sea n un entero mayor o igual a 5, y sea α una permutación no trivial en A_n. Demuestre que existe un 3-ciclo β en A_n que no conmuta con α.

Ejercicio 256. Sean n un entero mayor o igual a 6, α una permutación en A_n y β un 3-ciclo en A_n. Demuestre que $\alpha\beta\alpha^{-1}\beta^{-1}$ se puede escribir como producto de dos 3-ciclos. Concluya que existe un subgrupo S de A_n con las siguientes propiedades:
(i) S contiene a $\alpha\beta\alpha^{-1}\beta^{-1}$
(ii) S es conjugado a A_6 en S_n

Ejercicio 257. Sean n un entero mayor o igual a 6 y N un subgrupo normal no trivial de A_n. Demuestre que N contiene un subgrupo de A_n que es conjugado a A_6 en S_n. Concluya que existe un 3-ciclo que es elemento de N.

Ejercicio 258. Sea n un entero mayor o igual a 5. Demuestre que el grupo A_n es simple.

Ejercicio 259. Sea n un entero mayor o igual a 5. Demuestre que A_n es el único subgrupo normal propio no trivial de S_n.

6.9. Grupos especiales lineales.

Definición 260. Sean n un entero positivo, k un campo y k^* el grupo multiplicativo de los elementos distintos de cero de k. Sea $\varphi : GL_n(k) \longrightarrow k^*$ la función que a cada matriz le asocia su determinante. En álgebra lineal se demuestre que φ es un homomorfismo de grupos, es decir, que el determinante de un producto es el producto de los determinantes, y que una matriz cuadrada con coeficientes en un campo es invertible si y sólo si su determinante es diferente de cero. El núcleo de φ es un subgrupo normal de $GL_n(k)$, llamado el **grupo especial lineal** de grado n sobre el campo k, y denotado $SL_n(k)$. Al igual que con el grupo general lineal, si k es un campo finito con q elementos, uno usualmente escribe $SL(n, q)$ en lugar de $SL_n(k)$.

Ejercicio 261. Sea n cualquier entero positivo. Demuestre que $SL(n, 2) = GL(n, 2)$.

Ejercicio 262. Sea q la cardinalidad de un campo finito, y sea n cualquier entero positivo. Calcule el índice de $SL(n, q)$ en $GL(n, q)$.

Ejercicio 263. Sea k cualquier campo, y sea n un entero positivo. Demuestre que $SL_n(k)$ es abeliano si y sólo si $n = 1$.

6.10. Normalizadores.

Definición 264. Sean G un grupo y S un subgrupo de G. El **normalizador** de S en G, denotado $N_G(S)$, es el conjunto $\{g \in G \mid gSg^{-1} = S\}$.

Ejercicio 265. Sean G un grupo y S un subgrupo de G. Demuestre que $N_G(S)$ es un subgrupo de G.

Ejercicio 266. Sean G un grupo y S un subgrupo de G. Demuestre que S es un subgrupo normal de $N_G(S)$.

Ejercicio 267. Sean G un grupo y S un subgrupo de G. Demuestre que $N_G(S)$ es el mayor subgrupo de G que contiene a S como subgrupo normal, es decir, que si T es un subgrupo de G que contiene a S y S es normal en T, entonces $T \leq N_G(S)$.

Ejercicio 268. Sean G un grupo y S un subgrupo de G. Sea $NU_G(S) = \{g \in G \mid gSg^{-1} \leq S\}$. Demuestre que $NU_G(S)$ es cerrado bajo productos, y que $N_G(S) \leq NU_G(S)$. Muestre con un ejemplo que la contención puede ser propia.

Capítulo 7

Grupos cocientes.

7.1. Grupos cocientes.

Teorema y definición 269. *Sea G un grupo y sea N un subgrupo normal de G. Tenemos que el conjunto de clases laterales izquierdas de N en G forma un grupo con la operación $(gN)(hN) = ghN$. Este grupo se llama el **grupo cociente** de G entre N, y se denota G/N.*

Ejercicio 270. Sea G un grupo y sea N un subgrupo normal de G. Demuestre que el orden de G/N es el índice de N en G.

Ejercicio 271. Sea G un grupo abeliano. Demuestre que cualquier cociente de G es abeliano.

Ejercicio 272. Sea G un grupo cíclico. Demuestre que cualquier cociente de G es cíclico.

Ejercicio 273. Demuestre que existe un cociente de S_3 que es un grupo cíclico de orden dos.

Ejercicio 274. Demuestre que el grupo cociente $\mathbb{Q}/\mathbb{Z}$ es de orden infinito, pero que todos sus elementos son de orden finito.

Ejercicio 275. Sea G un grupo. Demuestre que si G no es abeliano, entonces $G/Z(G)$ no es cíclico.

Ejercicio 276. Sea G un grupo. Demuestre que $[G : Z(G)]$ no es un número primo.

Definición 277. Sea G un grupo y sea N un subgrupo normal de G. La función $\pi : G \longrightarrow G/N$ definida por $\pi(g) = gN$ se llama el **mapeo natural** de G en G/N.

Ejercicio 278. Sea G un grupo y sea N un subgrupo normal de G. Demuestre que el mapeo natural de G en G/N es un epimorfismo de grupos cuyo núcleo es N.

Ejercicio 279. Sea G un grupo y S un subgrupo de G. Demuestre que S es normal en G si y sólo si S es el núcleo de un homomorfismo de G en algún otro grupo.

Ejercicio 280. Sean G y H grupos. Demuestre que $G \times H$ contiene copias isomorfas de G y H como subgrupos normales, a saber, $G \times \{1\}$ y $\{1\} \times H$. Más aún, $G \times H$ también tiene cocientes isomorfos a G y H: $(G \times H)/(\{1\} \times H) \cong G$, y $(G \times H)/(G \times \{1\}) \cong H$.

7.2. Grupos proyectivos especiales lineales.

Ejercicio 281. Sean n un entero positivo y k un campo. Demuestre que el centro del grupo $SL_n(k)$ es el conjunto de matrices de la forma αI_n donde $\alpha \in k$ es tal que $\alpha^n = 1$.

Definición 282. Sean n un entero positivo y k un campo. El **grupo proyectivo especial lineal** de grado n sobre el campo k es el grupo cociente $SL_n(k)/Z(SL_n(k))$, y se denota $PSL_n(k)$. Al igual que con los grupos general lineal y especial lineal, si k es un campo finito con q elementos, uno usualmente escribe $PSL(n, q)$ en lugar de $PSL_n(k)$.

Ejercicio 283. Calcule el orden de $PSL(2, 3)$.

Ejercicio 284. Calcule el orden de $PSL(3, 3)$.

Ejercicio 285. Sea n un entero positivo. Demuestre que $PSL(n, 2)$ es isomorfo a $SL(n, 2)$.

Ejercicio 286. Sean n un entero positivo y sea k un campo finito con q elementos. Sea m el número de raíces n-ésimas de la unidad en el campo k. Calcule el orden de $PSL(n, q)$ en términos de n, q y m.

Computadora 287. Demuestre que $PSL(2, 4) \cong A_5 \cong PSL(2, 5)$.

Computadora 288. Demuestre que $PSL(2,9) \cong A_6$.

Computadora 289. Demuestre que $PSL(2,7) \cong PSL(3,2)$.

Computadora 290. Demuestre que $PSL(4,2) \cong A_8$.

7.3. Conmutadores y grupos abelianizados.

Definición 291. Sea G un grupo, y sean $g, h \in G$. El **conmutador** de g y h, denotado $[g,h]$, es el elemento $ghg^{-1}h^{-1}$. El **subgrupo conmutador** de G, denotado $[G,G]$ o G', es el subgrupo de G generado por todos los conmutadores en G. Note que el conjunto de los conmutadores puede no ser un subgrupo.

Ejercicio 292. Calcule $[S_3, S_3]$.

Computadora 293. Encuentre un grupo G de orden 270 tal que el conjunto $\{[g,h] \mid g, h \in G\}$ no sea un subgrupo de G.

Ejercicio 294. Sea G un grupo. Demuestre que $[G,G]$ es un subgrupo normal de G.

Ejercicio 295. Sea G un grupo, y sea N un subgrupo normal de G. Demuestre que G/N es abeliano si y sólo si N contiene a $[G,G]$.

Definición 296. Sea G un grupo. El cociente $G/[G,G]$ es un grupo abeliano, que se llama el **grupo abelianizado** de G.

Ejercicio 297. Calcule el grupo abelianizado de S_3.

Capítulo 8

Teoremas de isomorfismo.

8.1. Teoremas de isomorfismo.

Ejercicio 298. Sean G y H grupos, y sea $\varphi : G \longrightarrow H$ un homomorfismo con núcleo N. Demuestre que la función $\bar{\varphi} : G/N \longrightarrow H$ dada por $\bar{\varphi}(gN) = \varphi(g)$ está bien definida y es un monomorfismo.

Ejercicio 299. Sean G y H grupos, sea N un subgrupo normal de G y sea $\varphi : G \longrightarrow H$ un homomorfismo. Demuestre que la función $\bar{\varphi} : G/N \longrightarrow H$ dada por $\bar{\varphi}(gN) = \varphi(g)$ está bien definida si y sólo si $\mathrm{Ker}(\varphi)$ contiene a N. Demuestre que si $\bar{\varphi}$ está bien definida, entonces es un homomorfismo, y que $\bar{\varphi}$ es inyectiva si y sólo si $\mathrm{Ker}(\varphi) = N$.

Ejercicio 300. (Primer teorema de isomorfismo) Sean G y H grupos, y sea $\varphi : G \longrightarrow H$ un homomorfismo con núcleo N. Demuestre que N es un subgrupo normal de G y que G/N es isomorfo a la imagen de φ. Demuestre que la función $\bar{\varphi} : G/N \longrightarrow \mathrm{Im}(\varphi)$ dada por $\bar{\varphi}(gN) = \varphi(g)$ es un isomorfismo.

Ejercicio 301. Sean n un entero positivo y k un campo. Demuestre que $GL_n(k)/SL_n(k)$ es isomorfo al grupo multiplicativo de los elementos diferentes de 0 del campo k.

Ejercicio 302. Sean G y H grupos finitos. Demuestre que si $|G|$ y $|H|$ son primos relativos, entonces el único homomorfismo de G a H es el trivial.

Ejercicio 303. (Segundo teorema de isomorfismo) Sean G un grupo, S un subgrupo cualquiera de G y N un subgrupo normal de G. Entonces $S \cap N$ es normal en S y $S/(S \cap N)$ es isomorfo a $(NS)/N$.

Ejercicio 304. (Tercer teorema de isomorfismo) Sea G un grupo, y sean N y M subgrupos normales de G con $M \leq N$. Entonces N/M es un subgrupo normal de G/M y $(G/M)/(N/M)$ es isomorfo a G/N.

8.2. Teorema de la correspondencia.

Ejercicio 305. (Teorema de la correspondencia) Sean G un grupo, N un subgrupo normal de G y $\pi : G \longrightarrow G/N$ el mapeo natural. Para cada S subgrupo de G con $N \leq S$, defina $S^* = S/N = \pi(S) = \{sN \mid s \in S\}$. Demuestre lo siguiente:

(1) Para todo S subgrupo de G con $N \leq S$, se tiene que S^* es un subgrupo de G/N.

(2) La asignación $S \mapsto S^*$ es una biyección entre el conjunto $\{S \mid N \leq S \leq G\}$ y el conjunto de todos los subgrupos de G/N. El inverso de esta asignación manda a un subgrupo U de G/N en $\pi^{-1}(U) = \{g \in G \mid \pi(g) \in U\}$.

(3) $N \leq T < S$ si y sólo si $T^* < S^*$, en cuyo caso $[S : T] = [S^* : T^*]$.

(4) $N \leq T \lhd S$ si y sólo si $T^* \lhd S^*$, en cuyo caso $S/T \cong S^*/T^*$.

Ejercicio 306. Sea G un grupo. Demuestre que si H es un cociente abeliano de G, entonces H es isomorfo a un cociente del grupo abelianizado de G. En otras palabras, el grupo abelianizado de G es el mayor cociente abeliano de G.

Capítulo 9

G-conjuntos.

9.1. G-conjuntos.

Definición 307. Sea G un grupo. Un **G-conjunto** es un conjunto X en el que el grupo G **actúa**, es decir, existe una función $\cdot : G \times X \longrightarrow X$ (llamada la **acción** de G en X), para la cuál usamos la notación gx en lugar de $\cdot(g, x)$, y que cumple lo siguiente:

(i) Para todo x en X se tiene que $1x = x$, donde 1 denota la identidad del grupo G;

(ii) Para todos g, h en G y para todo x en X, se tiene que $(gh)x = g(hx)$.

Notación 308. En algunos casos, para evitar confusión con otras operaciones, denotaremos la acción de G en X por $g \cdot x$ en lugar de gx.

Ejercicio 309. Sea G un grupo y sea X el conjunto vacío. Demuestre que existe una única manera de definir una acción de G en X. A X se le llama el ***G*-conjunto vacío**.

Ejercicio 310. Sea G un grupo y sea X un conjunto con un único elemento. Demuestre que existe una única manera de definir una acción de G en X. A X se le llama un ***G*-conjunto trivial**.

Ejercicio 311. Sea G un grupo. Demuestre que G es un G-conjunto con acción dada por la multiplicación de G, es decir, para cualquier $g \in G$ y cualquier $x \in G$ definimos $g \cdot x = gx$. A G con esta acción se le llama el ***G*-conjunto regular**.

Ejercicio 312. Sea G un grupo. Demuestre que G es un G-conjunto con acción dada por la conjugación de G, es decir, para cualquier $g \in G$ y cualquier $x \in G$ definimos $g \cdot x = gxg^{-1}$.

Ejercicio 313. Sean G un grupo, S un subgrupo de G (no necesariamente normal) y $X = G/S = \{gS \mid g \in G\}$ el conjunto de clases laterales izquierdas de S en G. Demuestre que X es un G-conjunto con acción dada por traslación izquierda, es decir, para cualquier $g \in G$ y cualquier $hS \in X$, definimos $g \cdot (hS) = (gh)S$.

Ejercicio 314. Sea G un grupo y sea X la familia de todos los subgrupos de G. Demuestre que X es un G-conjunto con acción dada por conjugación, es decir, para cualquier $g \in G$ y cualquier $S \in X$, definimos $g \cdot S = gSg^{-1}$.

Ejercicio 315. Sea X un conjunto cualquiera. Demuestre que X es un S_X-conjunto con acción dada por la evaluación, es decir, $\alpha \cdot x = \alpha(x)$ para cualquier $\alpha \in S_X$ y cualquier $x \in X$.

Ejercicio 316. Sea n un entero positivo, k un campo, y V un k-espacio vectorial de dimensión n. Demuestre que V es un $GL_n(k)$-conjunto con acción dada por la multiplicación de matriz con vector, es decir, $A \cdot v = Av$ para cualquier $A \in GL_n(k)$ y cualquier $v \in V$.

Ejercicio 317. Sean G un grupo y X un G-conjunto. Para cada $g \in G$, sea $\mu_g : X \longrightarrow X$ la función dada por $\mu_g(x) = g \cdot x$. Demuestre lo siguiente:

(1) μ_1 es la función identidad de X.

(2) $\mu_{gh} = \mu_g \circ \mu_h$.

(3) $\mu_{g^{-1}} = \mu_g^{-1}$.

(4) Para cualquier $g \in G$, la función μ_g es una biyección de X en sí mismo, es decir, $\mu_g \in S_X$.

(5) La función $\mu : G \longrightarrow S_X$ dada por $\mu(g) = \mu_g$ es un homomorfismo de grupos.

Ejercicio 318. Sean G un grupo y X un conjunto. Demuestre que X es un G-conjunto si y sólo si existe un homomorfismo $\varphi : G \longrightarrow S_X$ tal que la acción de G en X está dada por la evaluación, es decir, $g \cdot x = \varphi(g)(x)$ para cualquier $g \in G$ y cualquier $x \in X$.

9.2. Teoremas de representación .

Ejercicio 319. (Teorema de Cayley) Demuestre que todo grupo G es isomorfo a un subgrupo de S_G. Concluya que todo grupo finito de orden n es isomorfo a un subgrupo de S_n.

Ejercicio 320. Sea G un grupo simple que contiene un subgrupo propio de indice n. Demuestre que G es isomorfo a un subgrupo de S_n.

Ejercicio 321. Sea G un grupo simple que contiene un subgrupo propio con n subgrupos conjugados. Demuestre que G es isomorfo a un subgrupo de S_n.

Definición 322. Sean n un entero positivo y k un campo. Decimos que una matriz A de tamaño $n \times n$ con coeficientes en k es una **matriz de permutación** si cumple lo siguiente:
(i) En todo renglón de A aparecen $n-1$ ceros y un uno.
(ii) En toda columna de A aparecen $n-1$ ceros y un uno.

Ejercicio 323. Calcule las matrices de permutación de tamaño 3×3 sobre el campo $\mathbb{F}_2$.

Ejercicio 324. Sean n un entero positivo y k un campo. Sea S el conjunto de matrices de permutación de tamaño n por n con coeficientes en k. Demuestre que S es un subgrupo de $GL_n(k)$ isomorfo a S_n.

Ejercicio 325. Sea G un grupo finito de orden n, y sea k un campo arbitrario. Demuestre que G es isomorfo a un subgrupo de $GL_n(k)$.

9.3. Orbitas y estabilizadores.

Definición 326. Sean G un grupo, X un G-conjunto y $x \in X$. La **órbita** de x bajo la acción de G es el subconjunto de X dado por $\{gx \mid g \in G\}$. El **estabilizador** de x, denotado G_x, es el subconjunto de G dado por $\{g \in G \mid gx = x\}$.

Ejercicio 327. Sean G un grupo, X un G-conjunto y $x \in X$. Demuestre que el estabilizador de x es un subgrupo de G.

Definición 328. Sean G un grupo y X un G-conjunto. Decimos que X es un G-conjunto **transitivo** si X consta de una única órbita.

Definición 329. Sean G un grupo, X un G-conjunto y $x \in X$. Decimos que x es un **punto fijo** bajo la acción de G si $gx = x$ para toda $g \in G$. El conjunto de todos los puntos fijos de X bajo G se denota X^G.

Ejercicio 330. Para cada uno de los G-conjuntos de los ejercicios 310, 311, 312, 313, 314, 315 y 316, calcule todas las órbitas, todos los estabilizadores y todos los puntos fijos. Determine cuáles de estos G-conjuntos son transitivos.

Ejercicio 331. Sea G un grupo que actúa en un conjunto X, y sean $x \in X$ y $g, h \in G$. Demuestre que $gx = hx$ si y sólo si $gG_x = hG_x$.

Ejercicio 332. Sea G un grupo que actúa en un conjunto X, y sean $g \in G$ y $x \in X$. Demuestre que $G_{gx} = gG_xg^{-1}$.

Ejercicio 333. Sea G un grupo que actúa en un conjunto X, y sea $x \in X$. Demuestre que el número de elementos en la órbita de x es $[G : G_x]$.

Ejercicio 334. Sea G un grupo y sea $g \in G$. Demuestre que el número de conjugados de g en G es $[G : C_G(g)]$. En particular, si G es un grupo finito, este número es un divisor del orden de G.

Ejercicio 335. Sea G un grupo y sea S un subgrupo de G. Demuestre que el número de conjugados de S en G es $[G : N_G(S)]$. En particular, si G es un grupo finito, este número es un divisor del orden de G.

Ejercicio 336. Sean G un grupo y X un G-conjunto. Demuestre que X es la unión disjunta de sus órbitas bajo G.

9.4. Ecuación de clase.

Ejercicio 337. Sea G un grupo finito. Demuestre que

$$|G| = |Z(g)| + \sum_i [G : C_G(g_i)]$$

donde cada g_i es un representante de cada clase de conjugacion de G con más de un elemento. Esta fómula se llama la **ecuación de clase** del grupo G.

Ejercicio 338. Sea G un grupo finito no trivial cuyo orden es una potencia de un número primo. Demuestre que el centro de G es no trivial.

Ejercicio 339. Sea G un grupo finito no trivial cuyo orden es una potencia de un número primo. Demuestre que G es simple si y sólo si G tiene orden p.

Ejercicio 340. Sea p un número primo y sea G un grupo de orden p^2. Demuestre que G es abeliano. Muestre con un ejemplo que este resultado no es válido para p^3.

Capítulo 10

Teoremas de Sylow.

10.1. p-grupos.

Definición 341. Sea p un numero primo. Un grupo P es un ***p*-grupo** si para todo elemento $g \in P$, el orden de g es una potencia de p.

Ejercicio 342. Sean p un número primo y P un grupo finito cuyo orden es una potencia de p. Demuestre que P es un p-grupo.

Ejercicio 343. Sean p un número primo y G un grupo abeliano. Sea G_p el conjunto de elementos de G cuyo orden es una potencia de p. Demuestre que G_p es un subgrupo de G, y por lo tanto G_p es un p-grupo. Muestre con un ejemplo que este resultado no es válido para grupos no abelianos.

Definición 344. Sea p un número primo. El grupo $(\mathbb{Q}/\mathbb{Z})_p$ (véase 343) se denota $\mathbb{Z}(p^\infty)$.

Ejercicio 345. Sea p un número primo. Demuestre que $\mathbb{Z}(p^\infty)$ es un p-grupo infinito. Demuestre que todos los subgrupos propios de $\mathbb{Z}(p^\infty)$ son grupos cíclicos finitos. Demuestre que para todo entero positivo n, $\mathbb{Z}(p^\infty)$ tiene un único subgrupo de orden p^n.

10.2. Teorema de Cauchy.

Definición 346. Sean G un grupo, p un numero primo y U un subgrupo de G. Decimos que U es un ***p*-subgrupo** de G si U es un p-grupo.

Ejercicio 347. Sea G un grupo. Demuestre que el subgrupo trivial es un p-subgrupo de G para todo primo p.

Ejercicio 348. Calcule todos los 2-subgrupos de S_3.

Computadora 349. Calcule todos los 2-subgrupos de S_4.

Ejercicio 350. Sea G un grupo abeliano finito, y sea p un número primo que divide el orden de G. Demuestre que existe un elemento en G de orden p.

Ejercicio 351. Sea G un grupo finito, y sea p un número primo que divide el orden de G. Demuestre que si p no divide a $|Z(G)|$, entonces existe $g \in G$ tal que $|C_G(g)| < |G|$ y p divide a $|C_G(g)|$.

Ejercicio 352. (Teorema de Cauchy) Sea G un grupo finito cuyo orden es divisible por un primo p. Demuestre que G contiene un elemento de orden p.

Ejercicio 353. Sean p un número primo y P un grupo finito. Demuestre que P es un p-grupo si y sólo si el orden de P es una potencia de p.

10.3. Teoremas de Sylow.

Definición 354. Sean G un grupo y p un número primo. Un subgrupo P de G es un ***p*-subgrupo de Sylow** de G si es un p-subgrupo maximal de G, es decir, si P es un p-subgrupo de G que no está contenido propiamente en ningún otro p-subgrupo de G.

Ejercicio 355. Sean G un grupo y p un número primo. Demuestre que si G es finito, entonces G tiene p-subgrupos de Sylow. Demuestre que p divide al orden de G si y sólo si todos los p-subgrupos de Sylow de G son no triviales.

Ejercicio 356. Sean G un grupo finito, p un número primo y U un p-subgrupo de G. Demuestre que existe un p-subgrupo de Sylow de G que contiene a U.

Ejercicio 357. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que el único elemento en $N_G(P)/P$ cuyo orden es una potencia de p es el elemento identidad. Concluya que si un elemento $g \in G$ es tal que $gPg^{-1} = P$ y el orden de g es una potencia de p, entonces $g \in P$.

Ejercicio 358. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que p no divide a $[N_G(P) : P]$.

Ejercicio 359. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que gPg^{-1} es un p-subgrupo de Sylow de G para toda $g \in G$.

Ejercicio 360. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que si P es el único p-subgrupo de Sylow de G entonces P es normal en G.

Ejercicio 361. Sean G un grupo finito, p un número primo y P un p-subgrupo de Sylow de G. Sea X el conjunto de todos los subgrupos conjugados a P. Demuestre que la cardinalidad de X es un divisor de $[G : P]$. Demuestre que P tiene un único punto fijo en X. Concluya que la cardinalidad de X es congruente con uno módulo p. Demuestre que si Q es otro p-subgrupo de Sylow de G, Q debe tener al menos un punto fijo en X. Concluya que todos los p-subgrupos de Sylow de G son conjugados a P.

Ejercicio 362. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que P es normal en G si y sólo si P es el único p-subgrupo de Sylow de G.

Ejercicio 363. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que p no divide a $[G : N_G(P)]$.

Ejercicio 364. Sean G un grupo, p un número primo y P un p-subgrupo de Sylow de G. Demuestre que p no divide a $[G : P]$. Concluya que el orden de P es la mayor potencia de p que divide al orden de G.

Ejercicio 365. (Teoremas de Sylow) Sea G un grupo finito, sea p un primo con $|G| = p^n m$, donde p no divide a m, y sea t el número de los p-subgrupos de Sylow de G. Demuestre que:

(i) Todos los p-subgrupos de Sylow de G son conjugados entre si.
(ii) El orden de cualquier p-subgrupo de Sylow de G es p^n.
(iii) t es un divisor de m, y t es congruente con uno modulo p.

10.4. Aplicaciones de los teoremas de Sylow.

Ejercicio 366. Sea G un grupo de orden 10. Demuestre que G tiene un único 5-subgrupo de Sylow. Concluya que G no es un grupo simple.

Ejercicio 367. Sean p un número primo, n y m enteros positivos con $m < n$, y P un p-grupo de orden p^n. Demuestre que existe un subgrupo normal de P de orden p^m.

Ejercicio 368. Sean G un grupo finito, p un número primo y n un entero positivo. Demuestre que si p^n divide al orden de G, entonces G contiene un subgrupo de orden p^n.

Ejercicio 369. (Argumento de Frattini) Sean G un grupo finito, p un número primo, N un subgrupo normal de G y P un p-subgrupo de Sylow de N. Demuestre que $G = N_G(P)N$.

Ejercicio 370. Sean G un grupo finito y p un número primo tal que la mayor potencia de p que divide al orden de G es p. Sea n el número de p-subgrupos de Sylow de G. Demuestre que G tiene exactamente $n(p-1)$ elementos de orden p.

Ejercicio 371. Sea G un grupo finito tal que $|G| = p^n m$ con p primo, n y m enteros, y $1 < m < p$. Demuestre que G tiene un único p-subgrupo de Sylow. Concluya que el grupo G no es simple.

Ejercicio 372. Sea G un grupo finito tal que $|G| = p^2 q$ con p, q primos distintos. Demuestre que G no es simple.

Ejercicio 373. Sea G un grupo de orden 30. Demuestre que si G fuera simple, entonces G tendría 24 elementos de orden 5 y 20 elementos de orden 3, excediendo los 30 elementos de G.

Ejercicio 374. Sea G un grupo de orden 48. Demuestre que si G fuera simple, entonces la acción por conjugación de G en sus 2-subgrupos de Sylow definiría un monomorfismo de G en S_3, lo cuál llevaría a una contradicción.

Ejercicio 375. Sea G un grupo simple no abeliano. Demuestre que el orden de G es mayor o igual a 60.

Capítulo 11

Series de subgrupos.

11.1. Series normales.

Definición 376. Sea G un grupo arbitrario. Una **serie normal** de G es una cadena de subgrupos $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ tales que $S_{i+1} \trianglelefteq S_i$ para toda $i = 0, \ldots, n-1$. Los **grupos factores** de dicha serie normal son los grupos S_i/S_{i+1} que no sean triviales, para $i = 0, \ldots, n-1$. La **longitud** de esta serie es el numero de inclusiones estrictas. Note que S_{i+1} es un subgrupo normal de S_i, pero puede no ser un subgrupo normal de G.

Ejercicio 377. Demuestre que la longitud de una serie normal es igual al número de grupos factores.

Ejercicio 378. Calcule una serie normal de A_4 de longitud tres. Demuestre que en cualquier serie normal de A_4 de longitud tres hay al menos un subgrupo que no es normal en A_4.

Ejercicio 379. Calcule una serie normal de S_4 de longitud cuatro.

Ejercicio 380. Sea G un grupo. Demuestre que G es simple si y sólo si todas sus series normales tienen longitud uno.

Ejercicio 381. Sea n un entero mayor o igual a 5. Demuestre que todas las series normales de S_n tienen longitud menor o igual a dos.

Definición 382. Sea G un grupo. Una serie normal $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ es un **refinamiento** de una serie normal $\{1\} = T_m \leq \cdots \leq T_1 \leq T_0 = G$ si la lista $T_0, T_1, \ldots, T_m$ es una sublista de $S_0, S_1, \ldots, S_n$.

Ejercicio 383. Calcules dos series normales de A_4 que no tengan ningún refinamiento en común.

Definición 384. Dos series normales de G son **equivalentes** si existe una correspondencia biyectiva entre los grupos factores de cada una tal que grupos factores correspondientes sean isomorfos.

Ejercicio 385. Sea G un grupo. Demuestre que la relación “ser equivalente a” en la familia de las series normales de G es una relación de equivalencia, es decir, que es reflexiva, simétrica y transitiva.

Ejercicio 386. Muestre dos series normales de S_4 de longitud dos que no sean equivalentes. Demuestre que cualesquiera dos series normales de S_4 tienen refinamientos equivalentes.

11.2. Series de composición.

Definición 387. Sea G un grupo. Una serie normal $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ de G es una **serie de composición** de G si para ninguna $i = 0, ..., n-1$ existe un subgrupo normal propio de S_i que contenga propiamente a S_{i+1}.

Ejercicio 388. Sea G un grupo. Demuestre que una serie normal de G es una serie de composición si y sólo si todos sus grupos factores son grupos simples.

Ejercicio 389. Sea G un grupo finito. Demuestre que existe una serie de composición de G.

Ejercicio 390. Sea G un grupo. Demuestre que una serie normal de G es una serie de composición de G si y sólo si es equivalente a cualquier refinamiento suyo.

Ejercicio 391. Demuestre que cualesquiera dos series de composición de S_4 son equivalentes.

Ejercicio 392. Sea n un entero mayor o igual a 5. Demuestre que cualesquiera dos series de composición de S_n son equivalentes.

Ejercicio 393. Sean G un grupo y N un subgrupo normal de G. Suponga que N y G/N son grupos simples. Demuestre que G tiene una serie de composición de longitud dos. Demuestre que cualquier serie de composición de G tiene longitud dos. Demuestre que cualesquiera dos series de composición de G son equivalentes.

11.3. Teorema de Jordan-Hölder.

Ejercicio 394. Sean $S_2 \trianglelefteq S_1$ y $T_2 \trianglelefteq T_1$ subgrupos de un grupo G.

(1) Sea $U = (S_1 \cap T_2)(S_2 \cap T_1)$. Demuestre que U es un subgrupo normal de $S_1 \cap T_1$.

(2) Construya un epimorfismo de $T_2(T_1 \cap S_1)$ en $S_1 \cap T_1/U$ con núcleo $T_2(T_1 \cap S_2)$.

(3) Repita los pasos anteriores intercambiando los papeles de S_i y T_i.

Ejercicio 395. (Lema de Zassenhaus) Sean $S_2 \trianglelefteq S_1$ y $T_2 \trianglelefteq T_1$ subgrupos de un grupo G. Demuestre que

$$S_2(S_1 \cap T_2) \trianglelefteq S_2(S_1 \cap T_1), \;\; T_2(T_1 \cap S_2) \trianglelefteq T_2(T_1 \cap S_1),$$

y que existe un isomorfismo

$$\frac{S_2(S_1 \cap T_1)}{S_2(S_1 \cap T_2)} \cong \frac{T_2(T_1 \cap S_1)}{T_2(T_1 \cap S_2)}.$$

Ejercicio 396. Sea G un grupo y sean $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ y $\{1\} = T_n \leq \cdots \leq T_1 \leq T_0 = G$ series normales de G. Para cualesquiera $1 \leq i \leq n$ y $0 \leq j \leq m$, defina $S_{i,j} = S_{i+1}(S_i \cap T_j)$

(1) Demuestre que los $S_{i,j}$ forman un refinamiento de $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ con nm términos.

(2) De manera análoga, defina $T_{i,j} = T_{j+1}(T_j \cap S_i)$. Demuestre que estos subgrupos forman un refinamiento de $\{1\} = T_n \leq \cdots \leq T_1 \leq T_0 = G$ con nm términos.

(3) Demuestre que $S_{i,j}/S_{i,j+1}$ es isomorfo a $T_{i,j}/T_{i+1,j}$. Concluya que los dos refinamientos construidos son equivalentes.

Ejercicio 397. (Teorema de Schreier) Demuestre que dos series normales cualesquiera de un mismo grupo G tienen refinamientos equivalentes.

Ejercicio 398. (Teorema de Jordan-Holder) Demuestre que dos series de composición cualesquiera de un mismo grupo G son equivalentes. Los grupos factores de una serie de composición de G se llaman los **factores de composición** de G .

Ejercicio 399. Sea G un grupo abeliano finito. Demuestre que los factores de composición de G son grupos cíclicos cuyos órdenes son números primos.

Ejercicio 400. Demuestre que los factores de composición de S_4 son grupos cíclicos cuyos órdenes son números primos.

Ejercicio 401. Sea n un entero mayor o igual a 5. Demuestre que los factores de composición de S_n son A_n y el grupo cíclico de orden dos.

11.4. Grupos solubles.

Definición 402. Sea G un grupo. Decimos que G es un grupo **soluble** si tiene una serie normal cuyos grupos factores son abelianos. Una tal serie normal se llama una **serie soluble** de G.

Ejercicio 403. Demuestre que todo grupo abeliano es soluble.

Ejercicio 404. Demuestre que S_4 es un grupo soluble.

Ejercicio 405. Sea G un grupo simple. Demuestre que G es soluble si y sólo si G es cíclico de orden primo.

Ejercicio 406. Sea n un entero mayor o igual a 5. Demuestre que A_n no es un grupo soluble.

Ejercicio 407. Sea G un grupo finito. Demuestre que G es soluble si y sólo si todos sus factores de composición son grupos cíclicos cuyos órdenes son números primos.

Ejercicio 408. Sea n un entero mayor o igual a 5. Demuestre que S_n no es un grupo soluble.

Ejercicio 409. Sean G un grupo soluble, $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ una serie soluble de G y T un subgrupo de G. Demuestre que $\{1\} = T \cap S_n \leq \cdots \leq T \cap S_1 \leq T \cap S_0 = T$ es una serie soluble de T. Concluya que cualquier subgrupo de un grupo soluble es soluble.

Ejercicio 410. Sean G un grupo soluble con una serie de composición, y N un subgrupo normal de G. Demuestre que existe una serie de composición que tiene a N como uno de sus términos. Use esto para construir una serie de composición soluble de G/N. Concluya que G/N es un grupo soluble.

Ejercicio 411. Demuestre que $\mathbb{Z}$ es un grupo soluble sin serie de composición.

Ejercicio 412. Sea G un grupo soluble (no necesariamente con serie de composición), y sean $\{1\} = S_n \leq \cdots \leq S_1 \leq S_0 = G$ una serie soluble de G y N un subgrupo normal de G.

(1) Demuestre que $\{1\} \leq N = NS_n \leq \cdots \leq NS_1 \leq NS_0 = G$ es una serie normal de G.

(2) Demuestre que $\{1\} = NS_n/N \leq \cdots \leq NS_1/N \leq NS_0/N == G/N$ es una serie normal de G/N.

(3) Demuestre que para toda $0 \leq i < n$ se tiene que $(NS_i/N)/(NS_{i+1}/N)$ es isomorfo a $S_i/(NS_{i+1})$, y que este último grupo es un cociente de S_i/S_{i+1}.

(4) Concluya que cualquier cociente de un grupo soluble es soluble.

Ejercicio 413. Sean G un grupo y N un subgrupo normal de G. Demuestre que si N y G/N son solubles, entonces G es soluble.

Ejercicio 414. Sean G y H grupos. Demuestre que $G \times H$ es soluble si y sólo si G y H son solubles.

Ejercicio 415. Sea p un número primo. Demuestre que todo p-grupo finito es soluble.

Bibliografía

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

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

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

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

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

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

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

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

Índice alfabético