Álgebra Moderna 1: Teoría de Grupos

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

29 de octubre de 2021

1. Grupos

Un conjunto no vacío G es un grupo si en él se define una operación binaria (a menudo llamada producto $(\cdot)$, pero no necesariamente), la cual cumple con las siguientes propiedades:

1. **Cerradura:** Si $a \in G$ y $b \in G$, entonces $a \cdot b \in G$.
2. **Asociatividad:** Para todo $a, b, c \in G$, se cumple $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. **Neutro:** Existe $e \in G$ tal que para todo $a \in G$ se cumple $a \cdot e = e \cdot a = a$.
4. **Inversos:** Para todo $a \in G$, existe $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$, con $e \in G$ neutro.

Un grupo G con operación $(\cdot)$ a veces se denota por $(G, \cdot)$.

Grupos abelianos

Un grupo $(G, \cdot)$ es abeliano o conmutativo si para todo $a \in G$ y $b \in G$, se cumple $a \cdot b = b \cdot a$ (es decir, si posee la propiedad conmutativa).

Orden de un grupo

El orden de un grupo $(G, \cdot)$, denotado $o(G)$, es la cardinalidad del conjunto G. En otras palabras, es la cantidad de elementos que el conjunto G posee.

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

2. Ejemplos de grupos

Enteros bajo la suma

El conjunto $(\mathbb{Z}, +)$ forma un grupo abeliano infinito, donde $0 \in \mathbb{Z}$ es el neutro aditivo y para cada $a \in \mathbb{Z}$, su inverso es $-a \in \mathbb{Z}$.

Las unidades bajo el producto

Sea $G = \{1, -1\}$, entonces el conjunto $(G, \cdot)$ forma un grupo abeliano de orden 2, con elemento neutro $1 \in G$, y con cada elemento siendo su propio inverso.

Un grupo simétrico

Sea S_3 el grupo de todas las biyecciones de un conjunto de tres elementos en sí mismo, con la operación de composición de funciones. Otra forma de ver este grupo es como todas las posibles permutaciones que se pueden realizar en tres objetos. Este es un grupo no abeliano de orden $3! = 6$.

Grupos cíclicos

Sea $n \in \mathbb{Z}^+$, y defínase a $(G, \cdot)$ como el conjunto de todos los símbolos a^k para $k \in \{0, 1, \ldots, n-1\}$, donde $a^i \cdot a^j = a^{i+j}$ si $i + j \leq n$, $a^i \cdot a^j = a^{i+j-n}$ si $i + j > n$, y $a^0 = a^n = e$. Este es llamado un grupo cíclico de orden n, y es abeliano.

Matrices cuadradas

Sea $(M_{n\times n}, \cdot)$ el conjunto de matrices cuadradas de $n \times n$ con el producto usual de matrices y con entradas en $\mathbb{R}$. Este es un grupo no abeliano infinito.

3. Lemas preliminares

Lema 2.1:

Si $(G, \cdot)$ es un grupo, entonces:

- **Unicidad del neutro:** El neutro (la identidad) de G es único.
- **Unicidad de los inversos:** Para todo $a \in G$, su inverso $a^{-1} \in G$ es único.
- **Inverso del inverso:** Para todo $a \in G$, el inverso de su inverso es a mismo $((a^{-1})^{-1} = a)$.
- **Inverso de una operación:** Para todo $a, b \in G$, se cumple $(a \cdot b)^{-1} = b^{-1}a^{-1}$.

Lema 2.2:

Si $(G, \cdot)$ es un grupo con $a, b \in G$, entonces las ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen soluciones únicas para $x, y \in G$. Esto es,

- **Cancelación izquierda:** Si $a \cdot u = a \cdot v$, entonces $u = v$.
- **Cancelación derecha:** Si $u \cdot a = v \cdot a$, entonces $u = v$.

4. Subgrupos

Un subconjunto no vacío H de un grupo G es llamado un subgrupo de G si, bajo la operación de G, el conjunto H forma un grupo.

Lema 2.3:

Un subconjunto no vacío H de G es un subgrupo de G si y solo si:

- **Cerradura:** Si $a, b \in H$, entonces $ab \in H$.
- **Cerradura de inversos:** Si $a \in H$, entonces $a^{-1} \in H$.

Lema 2.4:

Un subconjunto finito y no vacío H de G es un subgrupo de G si y solo si este es cerrado.

Ejemplos de subgrupos

Multiplos de enteros

Sea $\mathbb{Z}$ con la suma, y sea H el conjunto de todos los múltiplos de algún $n \in \mathbb{Z}$. En este caso, H es un subgrupo de $\mathbb{Z}$.

Biyecciones fijadas

Sea S un conjunto cualquiera, y sea $A(S)$ el conjunto de todas las biyecciones de S en sí mismo. Considérese a $A(S)$ con la operación de composición de funciones (este es un grupo). Si $x \in S$ y se toma $H(x) = \{\phi \in A(S) \mid \phi(x) = x\}$ (las biyecciones que dejan fijo a x), entonces $H(x)$ es un subgrupo de $A(S)$. Si se definiera $H(y)$ de la misma forma, $H(x) \cap H(y)$ sería el conjunto de biyecciones que dejan fijos a x y y, el cual también es subgrupo de $A(S)$.

Grupos cíclicos (generados)

Sea G un grupo, y sea $a \in G$. Se define $(a) = \{a^k \mid k \in \mathbb{Z}\}$ como el subgrupo cíclico de G generado por a.

Subgrupo generado por un subconjunto

Sea G un grupo y W un subconjunto cualquiera de G. Sea (W) el conjunto con todas las posibles operaciones entre todas las potencias de elementos de W. Este conjunto es el subgrupo de G generado por W, y es el subgrupo más pequeño de G que contiene a W. Además, (W) es la intersección de todos los subgrupos de G que contienen a W.

Congruencia módulo subgrupo

Sea G un grupo y H un subgrupo de G. Para $a, b \in G$, se dice que a es congruente a b módulo H (escrito $a \equiv b \mod H$) si $ab^{-1} \in H$.

Lema 2.5:

La relación $a \equiv b \mod H$ es una relación de equivalencia.

Clase lateral derecha

Si G es un grupo, H es un subgrupo de G y $a \in G$, se define $Ha = \{ha \mid h \in H\}$ como una la clase lateral derecha de H en G.

Lema 2.6:

Sea G un grupo y H un subgrupo de G. Para todo $a \in G$, se tiene $Ha = \{x \in G \mid a \equiv x \mod H\}$. Esto nos dice que Ha es la clase de equivalencia de a en G. Por lo tanto, todo par de clases laterales derechas de H en G deben ser exactamente la misma o completamente disjuntas.

Lema 2.7:

Sea G un grupo y H un subgrupo de G. Entonces, existe una biyección entre cualquier par de clases laterales derechas de H en G. Si H es un grupo finito, esto simplemente significa que la cardinalidad de cualquier par de clases laterales derechas de H en G es la misma.

Índice de un subgrupo

Si G un grupo y H es un subgrupo de G, el índice $i_G(H)$ de H en G es el número de clases laterales derechas distintas de H en G. En el caso de grupos finitos, es claro que $i_G(H) = o(G)/o(H)$.

Orden de un elemento

Si G es un grupo y $a \in G$, el orden de a en G es el entero positivo m más pequeño tal que $a^m = e$.

Teorema 2A (Lagrange):

Si G es un grupo finito y H es un subgrupo de G, entonces $o(H) \mid o(G)$.

Corolario 1 del teorema 2A:

Si G es un grupo finito y $a \in G$, entonces $o(a) \mid o(G)$.

Corolario 2 del teorema 2A:

Si G es un grupo finito y $a \in G$, entonces $a^{o(G)} = e$.

Corolario 3 del teorema 2A (Euler):

Sean $n \in \mathbb{Z}^+$ y $a \in \mathbb{Z}$ primos relativos, y defínase $\phi(k)$ como la cantidad de enteros positivos menores a k que son primos relativos de k. Entonces, $a^{\phi(n)} \equiv 1 \mod n$.

Corolario 4 del teorema 2A (Fermat):

Sea $p \in \mathbb{Z}^+$ un número primo y $a \in \mathbb{Z}$ un entero cualquiera. Entonces, $a^p \equiv a \mod p$.

Corolario 5 del teorema 2A:

Si G es un grupo finito cuyo orden es un número primo, entonces G es un grupo cíclico.

5. Un principio de conteo

Lema 2.8:

Sea G un grupo con subgrupos H y K. El conjunto $HK = \{hk \mid h \in H, k \in K\}$ es un subgrupo de G si y solo si $HK = KH$.

Corolario del lema 2.8:

Si H y K son subgrupos del grupo abeliano G, entonces HK es un subgrupo de G.

Teorema 2B:

Si H y K son subgrupos de un grupo G, entonces $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}$.

Corolario del teorema 2B:

Si H y K son subgrupos de un grupo G y se tiene $o(H) > \sqrt{o(G)}$ y $o(K) > \sqrt{o(G)}$, entonces $H \cap K \neq (e)$.

6. Subgrupos normales y grupos cociente

Subgrupos normales

Un subgrupo N de G es llamado un subgrupo normal de G si para todo $g \in G$ y $n \in N$, se cumple $gng^{-1} \in N$. De forma equivalente, N es normal en G si y solo si $gNg^{-1} \subseteq N$ para todo $g \in G$.

Lema 2.9:

Un subgrupo N de G es un subgrupo normal de G si y solo si $gNg^{-1} = N$ para todo $g \in G$. Esto equivale a que N es normal en G si y solo si $gN = Ng$.

Lema 2.10:

Un subgrupo N de G es un subgrupo normal de G si y solo si toda clase lateral izquierda de N en G es una clase lateral derecha de N en G.

Lema 2.11:

Un subgrupo N de G es un subgrupo normal de G si y solo si el producto de dos clases laterales derechas de N en G es una clase lateral de N en G.

Conjunto cociente

Sea G un grupo y H un subgrupo de G. Se define al conjunto cociente G/H como todas las clases laterales derechas de H en G. Bajo el producto de clases laterales se define un producto en el conjunto cociente.

Teorema 2C:

Si G es un grupo y N es un subgrupo normal de G, entonces G/N es también un grupo. Este es llamado el grupo cociente de G sobre N.

Lema 2.12:

Si G es un grupo finito y N es un subgrupo normal de G, entonces $o(G/N) = o(G)/o(N) = i_G(N)$.

7. Homomorfismos de grupos

Sean G y $\overline{G}$ grupos. Un mapeo $\phi : G \to \overline{G}$ es llamado un homomorfismo de G en $\overline{G}$ si para todo $a, b \in G$ se cumple $\phi(ab) = \phi(a)\phi(b)$.

Monomorfismos y epimorfismos de grupos

Un homomorfismo inyectivo es llamado un monomorfismo y un homomorfismo sobreyectivo es llamado un epimorfismo.

Isomorfismos de grupos

Un homomorfismo $\phi : G \to \overline{G}$ es llamado un isomorfismo de G en $\overline{G}$ si ϕ es un mapeo biyectivo.

Grupos isomorfos

Dos grupos G y $\overline{G}$ son isomorfos ($G \approx \overline{G}$) si existe un isomorfismo $\phi : G \to \overline{G}$.

Ejemplos de homomorfismos

Los homomorfismos triviales

El mapeo $\phi : G \to G$ tal que $\phi(x) = e$ para todo $x \in G$ es un homomorfismo. De igual manera, $\phi : G \to G$ tal que $\phi(x) = x$ para todo $x \in G$ es un homomorfismo.

Funciones exponenciales

Sea $G = \mathbb{R}$ bajo la suma y $\overline{G} = \mathbb{R}$ bajo el producto. Entonces, el mapeo $\phi : G \to \overline{G}$ con $\phi(x) = b^x$ con $b \geq 0$ es un homomorfismo.

Funciones exponenciales

Sea $G = \mathbb{Z}$ bajo la suma. Entonces, el mapeo de $\phi : G \to G$ con $\phi(x) = 2x$ es un homomorfismo.

Lema 2.13:

Sea G un grupo y N un subgrupo normal de G. Defínase el mapeo $\phi : G \to G/N$ con $\phi(x) = Nx$ para todo $x \in G$. Entonces, ϕ es un homomorfismo sobreyectivo.

Núcleo o kernel de un homomorfismo

Si $\phi : G \to \overline{G}$ es un homomorfismo, se denota $K_\phi = \{x \in G \mid \phi(x) = \overline{e}\}$ al núcleo o kernel de ϕ (aquí, el símbolo $\overline{e}$ denota al neutro de $\overline{G}$).

Lema 2.14:

Si $\phi : G \to \overline{G}$ es un homomorfismo, entonces:

- $\phi(e) = \overline{e}$, donde e es el neutro de G y $\overline{e}$ es el neutro de $\overline{G}$.
- $\phi(x^{-1}) = [\phi(x)]^{-1}$ para todo $x \in G$.

Lema 2.15:

Si $\phi : G \to \overline{G}$ es un homomorfismo con kernel K, entonces K es un subgrupo normal de G.

Lema 2.16:

Si $\phi : G \to \overline{G}$ es un homomorfismo sobreyectivo con $\overline{g} \in \overline{G}$ y $\phi(g) = \overline{g}$, entonces

$$K_\phi g = \{x \in G \mid \phi(x) = \overline{g}\}.$$

Corolario del lema 2.16:

Un homomorfismo sobreyectivo $\phi : G \to \overline{G}$ con kernel K_ϕ es un isomorfismo si y solo si $K_\phi = (e)$.

El isomorfismo induce una relación de equivalencia

En efecto, el isomorfismo de grupos induce una relación de equivalencia. Esto nos permite hablar de dos grupos isomorfos como prácticamente el mismo objeto con una representación distinta.

Teorema 2D (primer teorema de isomorfismos):

Sea $\phi : G \to \overline{G}$ un homomorfismo sobreyectivo con kernel K. Entonces, $G/K \approx \overline{G}$.

Grupos simples

Un grupo es simple si sus únicos subgrupos normales son los triviales. Esto es, un grupo es simple si únicamente posee como imágenes homomórficas a sus subgrupos triviales.

Grupos simples abelianos de orden finito

Todo grupo simple abeliano de orden finito tiene orden par.

Teorema 2α (Cauchy):

Si G es un grupo abeliano finito y p es un número primo tal que $p \mid o(G)$, entonces existe un elemento no nulo $a \in G$ tal que $a^p = e$.

Teorema 2β (Sylow):

Si G es un grupo abeliano finito y p es un número primo tal que $p^k \mid o(G)$ pero $p^{k+1} \nmid o(G)$, entonces G tiene un subgrupo de orden p^k.

Corolario del teorema 2β:

El subgrupo de orden p^k para G mencionado en el teorema es único.

Lema 2.17:

Sea $\phi : G \to \overline{G}$ un homomorfismo sobreyectivo con kernel K. Para un $\overline{H}$ subgrupo de $\overline{G}$, se define $H = \{x \in G \mid \phi(x) \in \overline{H}\}$. Entonces, H es un subgrupo de G que contiene a K. Si $\overline{H}$ es normal en $\overline{G}$, entonces H es normal en G. Además, esto fabrica una biyección entre todos los subgrupos de $\overline{G}$ y todos los subgrupos de G que contienen a K.

Teorema 2E:

Sea $\phi : G \to \overline{G}$ un homomorfismo sobreyectivo con kernel K, y sea $\overline{N}$ un subgrupo normal de $\overline{G}$. Si se define $N = \{x \in G \mid \phi(x) \in \overline{N}\}$, entonces $G/N \approx \overline{G}/\overline{N}$. Además, de manera equivalente, se tiene $G/N \approx (G/K)/(N/K)$.

8. Automorfismos de grupos

Un automorfismo de grupos se define como un isomorfismo de un grupo en sí mismo. Se denotará por $\mathbb{A}(G)$ al conjunto de automorfismos de G. En efecto, $\mathbb{A}(G)$ es un subgrupo de $A(G)$ (todas las biyecciones de G en sí mismo) bajo la composición de funciones.

Lema 2.18:

Si G es un grupo, entonces $\mathbb{A}(G)$ (el conjunto de automorfismos de G) es un grupo bajo la composición de funciones.

Automorfismos internos

Si G es un grupo y $x \in G$, entonces $T_x(g) = x^{-1}gx$ es el automorfismo interno de G asociado a x.

Grupo de automorfismos internos

Sea $\mathbb{J}(G) = \{T_x \in \mathbb{A}(G) \mid x \in G\}$ el conjunto de automorfismos internos de G. Este conjunto es un grupo bajo la composición de funciones.

Centro de un grupo

Si G es un grupo, entonces el centro de G es $Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}$.

El centro es normal

Si G es un grupo, entonces $Z(G)$ es un subgrupo normal de G.

Lema 2.19:

Si G es un grupo, entonces $\mathbb{J}(G) \approx G/Z(G)$.

Lema 2.20:

Si G es un grupo, si $\phi \in \mathbb{A}(G)$, y si $a \in G$ es de orden positivo, entonces $o\big(\phi(a)\big) = o(a)$.

9. Teorema de Cayley

Teorema 2F (Cayley):

Todo grupo es isomorfo a un subgrupo de $A(S)$ para algún conjunto S.

Nota sobre el teorema de Cayley

Una demostración del teorema de Cayley viene de tomar $S = G$ y proponer para $g \in G$ el mapeo $\tau_g : G \to G$, con $\tau_g(x) = xg$ para todo $x \in G$. Este resulta siendo parte de $A(G)$ y cumpliendo $\tau_g\tau_h = \tau_{gh}$, con lo cual $\psi : G \to A(S)$ con regla $\psi(g) = \tau_g$ es un isomorfismo.

Teorema 2G:

Si G es un grupo, H es un subgrupo de G, y S es el conjunto de todas las clases laterales derechas de H en G, entonces existe un homomorfismo $\theta : G \to A(S)$ cuyo kernel es el subgrupo normal más grande de G contenido en H.

Nota sobre el teorema anterior

La demostración del teorema anterior es parecida a la del teorema de Cayley, pero viene de tomar un subgrupo H de G y definir $S = \{Hg \mid g \in G\}$ (que no necesariamente es un grupo, esto solo ocurre si H es normal en G). Luego, para cada $g \in G$ se define $t_g : S \to S$ con $t_g(Hx) = Hxg$. Este resulta siendo parte de $A(G)$ y cumpliendo $t_g t_h = t_{gh}$, con lo cual $\theta : G \to A(S)$ con regla $\theta(g) = t_g$ es un homomorfismo. Luego, se juega con el kernel para llegar a que es el subgrupo normal más grande de G contenido en H.

Lema 2.21:

Si G es un grupo finito y H es un subgrupo de G tal que $o(G) \nmid i_G(H)!$, entonces H debe contener un subgrupo normal no trivial de G. En particular, G no puede ser simple.

10. Grupos de permutaciones

Si S es un conjunto no vacío con $\theta \in A(S)$ y $s_1, s_2 \in S$, se dice que s_1 es congruente a s_2 módulo θ si y solo si existe $k \in \mathbb{Z}$ tal que $\theta^k(s_1) = s_2$. Esto se denota $s_1 \equiv s_2 \mod \theta$.

Congruencia módulo permutación

La relación de congruencia módulo $\theta \in A(S)$ es una relación de equivalencia.

Ciclo

Si S es un conjunto no vacío con $\theta \in A(S)$ y $s \in S$, un ciclo de θ se refiere a un conjunto ordenado $(s, \theta(s), \theta^2(s), \ldots, \theta^{l-1}(s))$, donde l es el largo del ciclo.

Órbita

Si S es un conjunto no vacío con $\theta \in A(S)$ y $s \in S$, a la clase de equivalencia de s respecto a la congruencia módulo θ se le llama órbita de s bajo θ. La órbita simplemente es el ciclo sin orden.

Ejemplo de ciclos

Considérese $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ con el ciclo $(1, 3, 4, 2, 6)$. Este representa:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}.$$

Con esto, la notación se simplifica. Por ejemplo, $(1, 2, 3)(1, 8, 5, 6, 4) = (1, 2, 3, 8, 5, 6, 4)$.

Lema 2.22:

Toda permutación es el producto de sus ciclos.

Corolario del lema 2.22:

Toda permutación tiene una representación única como producto de ciclos disjuntos.

Lema 2.23:

Toda permutación es un producto de 2-ciclos (llamados transposiciones).

Permutación par e impar

Una permutación es par si puede ser expresada como el producto de un número par de transposiciones. Una permutación es impar si no es par. Bajo inspección, el producto de permutaciones pares es par. El producto de permutaciones impares es par. El producto de una permutación par con una impar es impar.

Grupo alternante

Se define a A_n como el subconjunto de S_n que posee únicamente permutaciones pares. Este recibe el nombre de grupo alternante.

Lema 2.24:

El conjunto A_n es un subgrupo normal de S_n, y $i_{S_n}(A_n) = 2$. Además, $o(A_n) = n!/2$.

11. Otro principio de conteo

Conjugado

Para $a, b \in G$, se dice que b es un elemento conjugado de a si existe $c \in G$ tal que $b = c^{-1}ac$. Esto se denota por $a \sim b$.

Lema 2.25:

La relación de conjugación ($\sim$) es una relación de equivalencia en G.

Clase de conjugados

Para $a \in G$, se define $C(a) = \{x \in G \mid a \sim x\}$ como la clase (de equivalencia) de conjugados de a en G. Claramente, consiste en todos los elementos $g^{-1}ag$ tales que $g \in G$. La cardinalidad de $C(a)$ se denota por c_a.

La base del principio de conteo

Si G es un grupo, entonces $o(G) = \sum_{a \in G} c_a$ puesto que la conjugación induce una partición de G.

El normalizador

Para $a \in G$, se define $N(a) = \{x \in G \mid xa = ax\}$ como el normalizador de $a \in G$. Claramente, $N(a)$ consiste de los elementos de G que conmutan con a.

Lema 2α:

Para $a \in G$, el normalizador $N(a)$ es un subgrupo de G.

Teorema 2H:

Si G es un grupo finito, entonces $c_a = o(G)/o\big(N(a)\big)$. En otras palabras, la cantidad de elementos en G conjugados a $a \in G$ es igual a $i_G\big(N(a)\big)$.

Corolario del teorema 2H (ecuación de clase):

Si G es un grupo finito, entonces $o(G) = \sum_{a \in G} \dfrac{o(G)}{o\big(N(a)\big)}$.

Lema 2.26:

Para $a \in G$, se tiene que $a \in Z(G)$ si y solo si $N(a) = G$. Si G es finito, $a \in Z(G)$ si y solo si $o(G) = o\big(N(a)\big)$.

Teorema 2I:

Si p es un número primo y $o(G) = p^n$, entonces $Z(G) \neq (e)$.

Corolario del teorema 2I:

Si p es un número primo y $o(G) = p^2$, entonces G es abeliano.

Teorema 2J (Cauchy):

Si p es un número primo y $p \mid o(G)$, entonces G posee un elemento de orden p.

Partición de un entero

Dado $n \in \mathbb{Z}^+$, los números $n_1, n_2, \ldots, n_r \in \mathbb{Z}^+$ con $n_1 \leq n_2 \leq \cdots \leq n_r$ son una partición de n si su suma es igual a n. Se denotará por $p(n)$ al número de particiones para n.

Ciclo de descomposición

Una permutación $\sigma \in S_n$ tiene ciclo de descomposición $\{n_1, n_2, \ldots, n_r\}$ si los ciclos disjuntos que factorizan a σ son de longitudes $n_1, n_2, \ldots, n_r$ con $n_1 \leq n_2 \leq \cdots \leq n_r$. Por ejemplo, $\sigma = (2,3)(4,5,6) \in S_9$ tiene ciclo de descomposición $\{1,1,1,1,2,3\}$.

Permutaciones conjugadas

Por el algoritmo desarrollado para el cálculo abreviado para permutaciones conjugadas, se deduce que dos permutaciones son conjugadas si y solo si tienen el mismo ciclo de descomposición.

Lema 2.27:

El número de clases conjugadas en S_n es $p(n)$, el número de particiones de n.

12. Teoremas de Sylow

Teorema 2K (Sylow):

Si p es un número primo y $p^k \mid o(G)$, entonces G tiene un subgrupo de orden p^k.

Corolario 1 del teorema 2K (Sylow):

Si p es un número primo tal que $p^k \mid o(G)$ pero $p^{k+1} \nmid o(G)$, entonces G tiene un subgrupo de orden p^k. Este tipo de subgrupo es llamado un p-subgrupo de Sylow.

Corolario 2 del teorema 2K (Sylow):

Si p es un número primo tal que $p^k \mid o(G)$ pero $p^{k+1} \nmid o(G)$, entonces G tiene subgrupos de orden p^m, donde $0 \leq m \leq k$.

Lema 2.28:

Sea p primo, y $n(k) \in \mathbb{Z}^+$ tal que $p^{n(k)} \mid p^k!$ pero $p^{n(k)+1} \nmid p^k!$. Entonces, $n(k) = 1 + p + \cdots + p^{k-1}$.

Lema 2.29:

Si p es un número primo, el grupo S_{p^k} tiene un p-subgrupo de Sylow.

Relación de doble subgrupo

Sea G un grupo con A y B subgrupos de G. Se define $x \asymp y$ si $y = axb$ para algún $a \in A$ y $b \in B$.

Lema 2.30:

La relación definida anteriormente ($\asymp$) es una relación de equivalencia en G. La clase de equivalencia de $x \in G$ es el conjunto $AxB = \{axb \mid a \in A, b \in B\}$ (clase lateral doble).

Lema 2.31:

Si A y B son subgrupos finitos de G, entonces $o(AxB) = \dfrac{o(A)o(B)}{o(A \cap xBx^{-1})}$.

Lema 2.32:

Sea G un subgrupo del grupo finito M, y sea Q un p-subgrupo de Sylow de M. Entonces, G tiene un p-subgrupo de Sylow $P = G \cap xQx^{-1}$ para algún $x \in M$.

Teorema 2L (Sylow 2):

Si p es un número primo tal que $p^k \mid o(G)$ pero $p^{k+1} \nmid o(G)$, entonces cualquier par de subgrupos A y B de G de orden p^k son conjugados. Es decir, $A = gBg^{-1}$.

Lema 2.33:

El número de p-subgrupos de Sylow en G es igual a $o(G)/o\big(N(P)\big)$, donde P es cualquier p-subgrupo de Sylow de G. En particular, este número divide a $o(G)$.

Teorema 2M (Sylow 3):

El número de p-subgrupos de Sylow en G, para un primo p dado, es de la forma $kp + 1$.

13. Productos directos

14. Grupos abelianos finitos