Capítulo 2

Grupos

2.1. Recuerdos

Antes de comenzar con el curso propiamente tal, recordaremos algunos temas de cursos anteriores, que utilizaremos durante este semestre, que es importante tener a la mano.

2.1.1. Relaciones de Equivalencia

Dado un conjunto A, definimos una *relación* en A, como un subconjunto R de $A \times A$. Si $(a, b) \in R$ anotaremos $a\ R\ b$ y diremos que a está relacionado con b.

Diremos que la relación es *refleja* si todo elemento está relacionado consigo mismo. Es decir, R es releja si para cada $a \in A$ implica que $a\ R\ a$.

Diremos que la relación es *simétrica* si cada vez que a está relacionado con b, entonces b está relacionado con a. Es decir, R es simétrica si para cada $a, b \in A$ con $a\ R\ b$, implica que $b\ R\ a$.

Diremos que la relación es *transitiva* si cada vez que a está relacionado con b y b está relacionado con c, entonces a está relacionado con c. Es decir, R es transitiva si para cada $a, b, c \in A$ con $a\ R\ b$ y $b\ R\ c$, implica que $a\ R\ c$.

Si una relación $\sim$ es refleja, simétrica y transitiva, entonces diremos que $\sim$ es una relación *de equivalencia.*

Ejemplo 2.1.1 *Sean z y w en $\mathbb{C}$ definimos la relación $z \sim w$ si y solo si $|z| = |w|$. Es una relación de equivalencia (*[**Ejercicio**]*). Por ejemplo, 0 está relacionado solamente con el mismo, en cambio 1 está relacionado con todos los números complejos del círculo unitario $S^1 = \{z \in \mathbb{C}/\ |z| = 1\}$ y solamente con ellos. En general el complejo z está relacionado con todos los complejos del círculo de centro en el origen que pasa por z. Además para cada x, y reales no negativos distintos, x no está relacionado con y, más aún cada número complejo está relacionado con uno y solo un elemento de $[0, \infty) \subseteq \mathbb{C}$.*

Ejemplo 2.1.2 *Sean $p(x)$ y $q(x)$ en $\mathbb{R}[x]$ el conjunto de polinomios con coeficientes en $\mathbb{R}$ definimos la relación $p(x) \sim q(x)$ si y solo si $r(x) = x^2 + 1$, divide la diferencia $p(x) - q(x)$. Es una relación de equivalencia (*[**Ejercicio**]*). Por ejemplo, -1 es equivalente al polinomio x^2. Además cada polinomio es equivalente a un único polinomio de grado a lo más 1. (*[**Ejercicio**]*)*

Ejemplo 2.1.3 *Fijemos $0 < m \in \mathbb{N}$ y sean a y b en $\mathbb{Z}$ cualesquiera. Definimos la relación $a \sim b$ si y solo si m divide a $b - a$. Es una relación de equivalencia.(*[**Ejercicio**]*) Si $m = 1$ entonces, todo número entero es equivalente a cualquier otro número entero. Si $m = 2$ entonces todo número entero es equivalente 0 o a 1. Más generalmente, para cualquier número entero m, todo número entero está relacionado con uno y solo uno de los números del conjunto $\{0, 1, 2, 3, \ldots, n-2, n-1\}$.*

Ejemplo 2.1.4 *Consideremos $A = \mathbb{N} \times \mathbb{N} = \{(a, b)/\ a, b \in \mathbb{N}\}$ y la relación $(a, b) \sim (m, n)$ si y solo si $a+n = b+m$. Ésta es una relación de equivalencia. Por ejemplo $(0, 0) \sim (m, m)$ para todo $m \in \mathbb{N}$.*

Ejemplo 2.1.5 *Consideremos $A = \mathbb{Z} \times \mathbb{Z}^\times = \{(a, b)/\ a, b \in \mathbb{Z},\ b \neq 0\}$ y la relación $(a, b) \sim (m, n)$ si y solo si $an = bm$. Ésta es una relación de equivalencia.(*[**Ejercicio**]*) Por ejemplo $(1, 1) \sim (m, m)$ para todo $m \in \mathbb{Z}^\times$.*

Ejemplo 2.1.6 *Si $[x]$ denota la parte entera de $x \in \mathbb{R}$, definida por $[x] = \sup\{n \in \mathbb{Z}/\ n \leq x\}$. En $\mathbb{R}$ definimos la relación $x \sim y$ si y solo si $[x] = [y]$. Ésta es una relación de equivalencia.(*[**Ejercicio**]*) Para cada $x \in \mathbb{R}$ existe un único $n \in \mathbb{Z}$ tal que $x \sim n$. El conjunto de todos los elementos de $\mathbb{R}$ que son equivalentes a x es $[[x], [x] + 1)$.*

Ejemplo 2.1.7 *Si $A = \mathbb{R}^2 \setminus \{0\} = \{v \in \mathbb{R}^2/\ v \neq (0, 0)\}$. Definamos en A la relación $v \sim u$ si y solo si existe $\lambda \in \mathbb{R}^\times$ tal que $u = \lambda u$. Ésta es una relación*

de equivalencia.([**Ejercicio**]*) Para cada elemento $v \in A$ existe un elemento u de $S^1 = \{u \in \mathbb{R}^2 / \ ||u|| = 1\}$ tal que $v \sim u$. Sin embargo, tal u no es único. Existe un subconjunto S de S^1 tal que cada elemento de A está relacionado con uno y solo un elemento de S.(*[**Ejercicio**]*)*

Ejemplo 2.1.8 *Si $A = \mathbb{R}^3 \setminus \{0\} = \{v \in \mathbb{R}^3 / \ v \neq (0,0,0)\}$. Definamos en A la relación $v \sim u$ si y solo si existe $\lambda \in \mathbb{R}^\times$ tal que $u = \lambda u$. Ésta es una relación de equivalencia.(*[**Ejercicio**]*) Para cada elemento $v \in A$ existe un elemento u de $S^2 = \{u \in \mathbb{R}^2 / \ ||u|| = 1\}$ tal que $v \sim u$. Sin embargo, tal u no es único. Existe un subconjunto S de S^2 tal que cada elemento de A está relacionado con uno y solo un elemento de S.(*[**Ejercicio**]*)*

A continuación recordaremos algunas propiedades de las relaciones de equivalencia.

2.1.2. Propiedades de las Relaciones de Equivalencia. Conjunto Cuociente.

En lo que sigue A será un conjunto no vacío y $\sim$ una relación de equivalencia en A.

Dado $a \in A$, al conjunto de todos los elementos de A que son equivalentes con a se llama la *clase de equivalencia de a* y se denota por $[a]$ o $\overline{a}$. Es decir,

$$[a] = \{x \in A / \ x \sim a\}$$

Como $\sim$ es simétrica se tiene que:

$$[a] = \{x \in A / \ x \sim a\} = \{x \in A / \ a \sim x\}$$

Consideremos dos clases de equivalencia, digamos $[a]$ y $[b]$. Si $z \in [a] \cap [b]$ quiere decir que $a \sim z$ y $z \sim b$, entonces por transitividad se tiene que $a \sim b$. Consideremos ahora $x \in [a]$, es decir $x \sim a$ y como $a \sim b$, entonces por transitividad se tiene que $x \sim b$ es decir $x \in [b]$. Reciprocamente si $y \in [b]$ y $a \sim b$, entonces $y \in [a]$. Es decir

Propiedad 2.1.1 *Sean $a, b \in A$ entonces:*

i) $[a] = [b]$ *si y solo si* $a \sim b$

ii) $[a] \cap [b] = \emptyset$ *si y solo si* $a \not\sim b$

Como la relación $\sim$ es refleja, entonces se tiene que todo $x \in A$ pertenece a alguna clase de equivalencia ($x \in [x]$). Por lo tanto las clases de equivalencias cubren todo A.

Por ejemplo, para la relación en $\mathbb{Z}$ definida por $a \sim b$ si y solo si 3 divide a $b - a$, existen solo 3 clases de equivalencia, a saber son las clases $[0], [1]$ y $[2]$. Es importante notar que los *representantes* de las clases son escogidos arbitrariamente, es decir, podemos decir que las clases $[300], [12001]$ y $[962]$ son las mismas clases que las anteriores. Como para cualquier número entero a se tiene que existe un número entero q y un entero r tal que

$$a = 3q + r, \text{ con } 0 \leq r < 3$$

Entonces $a \sim 0$, o $a \sim 1$ o $a \sim 2$. Es decir,

$$\mathbb{Z} = \bigcup_{i=0}^{2} [i]$$

Además esta unión es disjunta

Observación 2.1.1 (IMPORTANTE) *En general A es la unión disjunta de las clases de equivalencia.*

Al conjunto de todas las clases de equivalencias de A vía la relación $\sim$ se llama el *conjunto cuociente* y lo denotamos por

$$A/\sim = \{[a]/\ a \in A\}$$

Ejemplo 2.1.9 *Para la relación de equivalencia del ejemplo (2.1.2), podemos observar que* $[x^2] = [-1]$, *además se tiene que existe una relación biunívoca entre* $\mathbb{R}[x]/\sim$ *con el conjunto de los números complejos* $\mathbb{C}$ *definida por*

$$\phi : \mathbb{R}[x]/\sim \longrightarrow \mathbb{C}$$

definida por $\phi([ax+b]) = a+bi$. *Si definimos en* $\mathbb{R}[x]/\sim$ *la suma* $[p(x)]+[q(x)]$ *como* $[p(x)+q(x)]$ *y la multiplicación* $[p(x)][q(x)]$ *como* $[p(x)q(x)]$, *se tiene que tanto la suma como la multiplicación están bien definidas (*[**Ejercicio**]*) y además* $[x]^2 = -[1]$, *además* $\phi([p(x)] + [q(x)]) = \phi([p(x)]) + \phi([q(x)])$ *y además* $\phi([p(x)][q(x)]) = \phi([p(x)])\phi([q(x)])$. *Es decir, en cierto sentido que precisaremos más adelante* $\mathbb{C}$ *y* $\mathbb{R}[x]/\sim$ *son la misma cosa.*

Ejemplo 2.1.10 *Para la relación de equivalencia del ejemplo (2.1.4), podemos definir una suma en le cuociente* $\mathbb{N} \times \mathbb{N}/\sim$ *como* $[(m,n)] + [(a,b)] = [(m+a, n+b)]$, *ésta es una suma que está bien definida (*[**Ejercicio**]*). Además notamos que* $[(m,0)] = [(n,0)]$ *si y solo si* $m = n$ *y además* $[(m,0)]+[(n,0)] = [(m+n,0)]$. *También podemos definir una multiplicación*

$$[(m,n)][(a,b)] = [(ma+nb, mb+na)]$$

Ésta multiplicación está bien definida ([**Ejercicio**]*) y al igual que con la suma se observa que* $[(m,0)(n,0)] = [(mn,0)]$. *Es decir, la función:*

$$i : \mathbb{N} \to \mathbb{N} \times \mathbb{N}/\sim$$

definida por $i(m) = [(m,0)]$ *es inyectiva y además* $i(m) + i(n) = i(m+n)$ *y* $i(m)i(n) = i(mn)$. *Es decir, podemos decir que en* $\mathbb{N} \times \mathbb{N}/\sim$ *existe una "copia de* $\mathbb{N}$*," a saber los elementos de la forma* $[(m,0)]$. *La clase* $[(0,0)]$ *es neutro aditivo y* $[(1,0)]$ *es neutro multiplicativo. Lo interesante es que* $[(m,0)] + [(0,m)] = [(m,m)] = [(0,0)]$. *Es decir el inverso aditivo de* $[(m,0)]$ *existe y es* $[(0,m)]$. *Es decir, lo elementos de* $\mathbb{N}$ *tienen inversos aditivos en* $\mathbb{N} \times \mathbb{N}/\sim$, *más aún todo elemento de* $\mathbb{N} \times \mathbb{N}/\sim$ *tiene inverso aditivo, de hecho* $[(a,b)] + [(b,a)] = [(0,0)]$. *De hecho, una forma de construir* $\mathbb{Z}$ *a partir de* $\mathbb{N}$ *es definiendo* $\mathbb{Z}$ *como* $\mathbb{N} \times \mathbb{N}/\sim$.

Ejemplo 2.1.11 *Para la relación de equivalencia del ejemplo (2.1.5), podemos definir una suma en le cuociente* $\mathbb{Z} \times \mathbb{Z}^\times/\sim$ *como* $[(m,n)] + [(a,b)] = [(bm+an, nb)]$, *ésta es una suma que está bien definida (*[**Ejercicio**]*). Además notamos que* $[(m,1)] = [(n,1]$ *si y solo si* $m = n$ *y además* $[(m,1)]+[(n,1)] = [(mn,1)]$. *También podemos definir una multiplicación*

$$[(m,n)][(a,b)] = [(ma,nb)]$$

Ésta multiplicación está bien definida ([**Ejercicio**]*) y al igual que con la suma se observa que* $[(m,1)(n,1)] = [(mn,1)]$. *Es decir, la función:*

$$i : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}^\times/\sim$$

definida por $i(m) = [(m,1)]$ *es inyectiva y además* $i(m) + i(n) = i(m+n)$ *y* $i(m)i(n) = i(mn)$. *Es decir, podemos decir que en* $\mathbb{Z} \times \mathbb{Z}^\times/\sim$ *existe una "copia de* $\mathbb{Z}$*," a saber los elementos de la forma* $[(m,1)]$. *La clase* $[(0,1)]$ *es neutro aditivo y* $[(1,1)]$ *es neutro multiplicativo. Lo interesante es que*

$[(m,1)][(1,m)] = [(m,m)] = [(1,1)]$. *Es decir el inverso multiplicativo de* $[(m,1)]$ *existe y es* $[(1,m)]$. *Es decir, lo elementos de* $\mathbb{Z}$ *tienen inversos aditivos en* $\mathbb{Z} \times \mathbb{Z}^{\times}/\sim$, *además todo elemento no neutro aditivo de* $\mathbb{Z} \times \mathbb{Z}^{\times}/\sim$ *tiene inverso multiplicativo, de hecho* $[(a,b)][(b,a)] = [(ab,ab)] = [(1,1)]$. *De hecho, una forma de construir* $\mathbb{Q}$ *a partir de* $\mathbb{Z}$ *es definiendo* $\mathbb{Q}$ *como* $\mathbb{Z} \times \mathbb{Z}^{\times}/\sim$.

Ejemplo 2.1.12 *Para la relación de equivalencia del ejemplo (2.1.7), al cuociente* $\mathbb{R}^2 \setminus \{0\}/\sim$ *se la recta proyectiva real y es lo mismo que cuocientar el círculo* $S^1 = \{u \in \mathbb{R}^2 / \ ||u|| = 1\}$ *por la relación* $u \sim v$ *si y solo si* $u = -v$ *o* $u = v$. *(***[Ejercicio]***)*

Ejemplo 2.1.13 *Para la relación de equivalencia del ejemplo (2.1.8), al cuociente* $\mathbb{R}^3 \setminus \{0\}/\sim$ *se le llama el plano proyectivo real y es lo mismo que cuocientar la esfera* $S^2 = \{u \in \mathbb{R}^3 / \ ||u|| = 1\}$ *por la relación* $u \sim v$ *si y solo si* $u = -v$ *o* $u = v$. *(***[Ejercicio]***)*

Ejemplo 2.1.14 (Ejemplo de una suma mal definida) *Para la relación de equivalencia del ejemplo (2.1.6),* $(x, y \in \mathbb{R},\ x \sim y \iff [x] = [y])$. *En el cuociente* $\mathbb{R}/\sim$ *uno estaría tentado a sumar las clases como la suma de los representantes. Esto es:*

$$\overline{x} + \overline{y} = \overline{x+y}$$

Pero esta suma no está bien definida, pues por ejemplo $\overline{0,5} = \overline{0,25} = \overline{0}$ *y en cambio*

$$\overline{0,5+0,5} = \overline{1} \neq \overline{0} = \overline{0,25+0,25}$$

Es por esto que cuando uno define operaciones, o funciones en el cuociente a partir de los representantes, se debe demostrar que éstas están bien definidas.

2.1.3. $\mathbb{Z}_m$

Si $0 < m \in \mathbb{N}$ es fijo, consideramos la relación de equivalencia en $\mathbb{Z}$ definida por $a \sim b$ si y solo si m divide a $b - a$. En este caso diremos que a es congruente a b módulo m y anotaremos

$$a \equiv b \bmod m$$

Si $a \in \mathbb{Z}$ entonces existen q y r enteros tales que:

$$a = mq + r, \text{ con } 0 \leq r < m$$

Como $a - r = mq$ es divisible por m se tiene que $r \equiv b \bmod m$. Es decir,

Todo número entero es congruente módulo m a un número natural menor que m.

Además si $0 \leq r < r' < m$, entonces $0 < r' - r < m$, luego m no divide a $r' - r$, es decir, $r \not\equiv r' \bmod m$. Es decir

Todo número entero es congruente módulo m a un único número natural menor que m.

En este caso al conjunto de todas las clases de equivalencia lo anotamos por $\mathbb{Z}_m$. Así tenemos

$$\mathbb{Z}_m = \mathbb{Z}/\sim = \{[0], [1], [2], \ldots, [m-1]\}$$

En $\mathbb{Z}_m$ definimos una suma, por

$$[a] + [b] = [a + b]$$

Tenemos que mostrar que esta suma está bien definida, esto es, si tomamos otro representante de la clase de $[a]$ y otro representante de la clase de $[b]$, debemos mostrar que producen la misma suma en el cuociente.

Notemos que $x \in [a]$, es equivalente a decir que existe $q \in \mathbb{Z}$ tal que

$$x = a + mq.$$

Del mismo modo $y \in [b]$ es equivalente a decir que existe $p \in \mathbb{Z}$ tal que

$$y = b + mp,$$

por lo tanto

$$x + y = a + mq + b + mp = a + b + m(q + p) \in [a + b].$$

Por lo tanto $[x + y] = [a + b]$.

Ésta suma de clases, está estrechamente relacionada con la suma de $\mathbb{Z}$, por ejemplo $[a] + [0] = [a]$, es decir la clase del cero es el neutro de la suma recién definida. Como la clase $[m]$ es igual a la clase $[0]$, entonces se tiene que:

$$[m - a] + [a] = [m] = [0]$$

Es decir, la clase $[m - a]$ es el inverso aditivo de $[a]$ en $\mathbb{Z}_m$. Además como la suma es asociativa y conmutativa en $\mathbb{Z}$ y como la suma en $\mathbb{Z}_m$ se define a partir de la suma en $\mathbb{Z}$, se tiene que la suma en $\mathbb{Z}_m$ también es conmutativa y asociativa. En resumen:

Propiedad 2.1.2 *La suma definida en $\mathbb{Z}_m$ como $[a]+[b]=[a+b]$ es asociativa y conmutativa. Hay un elemento neutro, a saber la clase del cero y el inverso de $[a]$ es $[m-a]$.*

Del mismo modo como definimos la suma, podemos definir la multiplicación:

$$[a][b]=[ab]$$

Al igual que antes mostraremos que esta multiplicación está bien definida. Notamos que decir que $a' \in [a]$ es lo mismo que decir que $a'=a+mk$ para cierto $k \in \mathbb{Z}$. Del mismo modo, $b' \in [b]$ es equivalente a $b'=b+mt$ para cierto $t \in \mathbb{Z}$. Por lo tanto

$$a'b'=(a+mk)(b+mt)=ab+m(at+kb+mkt) \in [ab]$$

Es decir

$$[a'b']=[ab]$$

Notamos que $[a][1]=[a]$ para cualquier $a \in \mathbb{Z}$, por lo tanto la multiplicación definida como arriba en $\mathbb{Z}_m$, tiene un elemento neutro, a saber la clase $[1]$. Además como la multiplicación es conmutativa y asociativa en $\mathbb{Z}$, entonces:

Propiedad 2.1.3 *La multiplicación definida en $\mathbb{Z}_m$ como $[a][b]=[ab]$ es asociativa y conmutativa. Hay un elemento neutro, a saber la clase del uno.*

Por ejemplo, a continuación mostramos la tabla de la suma y de la multiplicación de $\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Por ejemplo, el inverso aditivo de $[2]$ es $[4]$, o dicho de otro modo $-[2]=4$. También $-[3]=[3]$ y $-[5]=[1]$

$\times$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Notamos que [2] no tiene inverso multiplicativo, ni tampoco [3], ni tampoco [4]. Los únicos que tienen inversos son [1] y [5], (de hecho cada uno de ellos es su propio inverso). Notamos además que $[3]^2 = [3] = -[3]$, también $[2]^2 = [4] = -[2]$ y para no ser menos $[5]^2 = [1] = -[5]$. Es decir, la ecuación $x^2 + x = 0$ tiene más de dos soluciones en $\mathbb{Z}_6$.
Más generalmente, si $m = pq$ con $p > 1$ y $q > 1$, entonces, $p < m$ y $q < m$. Es decir, $[p] \neq [0] \neq [q]$ y sin embargo

$$[p][q] = [m] = 0$$

Si $[p]$ tuviera inverso multiplicativo en $\mathbb{Z}_m$, existirían r y k enteros tales que

$$pr = 1 + km$$

$$pr - km = 1$$

$$p(r - kq) = 1$$

Pero no existe ningún número entero mayor que 1 que divida a 1. Por lo tanto tal r y tal k no existen. Es decir, $[p]$ no tiene inverso multiplicativo en $\mathbb{Z}_m$.

En cambio si p es primo y si $1 \leq n < p$, entonces n y p no tienen divisores comunes. Es decir, el MCD$(p, n) = 1$, por lo tanto existen s y t enteros tales que:

$$sp + tn = 1$$

$$tn = 1 + (-s)p$$

Es decir $[t][n] = [1]$, o lo que es lo mismo, $[t]$ es el inverso multiplicativo de $[n]$ en $\mathbb{Z}_p$. En resumen:

Propiedad 2.1.4 *Todo elemento no nulo en $\mathbb{Z}_p$ tiene inverso multiplicativo si y solo si p es primo.*

También vale la pena tener presente que:

Propiedad 2.1.5 *La multiplicación definida en $\mathbb{Z}_p$, con p primo, es asociativa y conmutativa. Hay un elemento neutro, a saber la clase del uno y todo elemento no nulo tiene inverso multiplicativo.*

2.2. Preliminares

En esta sección daremos las definiciones básicas de teoría de grupos y los primeros resultados. También acordaremos algunas notaciones que en general no son del todo universales.

Para nosotros un grupo es un conjunto no vacío G provisto de una operación binaria, que anotaremos por yuxtaposición, la cual es asociativa, esto es

$$g(hk) = (gh)k, \quad \forall\, g, h, k \in G \tag{2.1}$$

Existe un elemento unidad, esto es

$$\text{Existe } 1 \in G \text{ tal que } 1g = g1 = g, \quad \forall\, g \in G \tag{2.2}$$

Todo elemento tiene inverso, esto es

$$\text{Para todo } g \in G, \text{existe } g^{-1} \in G \text{ tal que } gg^{-1} = g^{-1}g = 1 \tag{2.3}$$

Un grupo *abeliano o conmutativo* es un grupo que además satisface

$$gg' = g'g \quad \forall\, g, g' \in G \tag{2.4}$$

Comunmente para grupos abelianos utilizaremos la notación aditiva y en vez de 1 utilizaremos 0 para denotar al neutro de la operación. Por ejemplo, $(\mathbb{Z}, +)$ es un grupo, que a menos que se diga otra cosa denotaremos por $\mathbb{Z}$ y también $\mathbb{Z}_m$ con la suma módulo m es un grupo, que a menso que se diga otra cosa anotaremos por $\mathbb{Z}_m$.

Observación 2.2.1 *Si 1 y e son neutros de un grupo G, entonces $1e = 1$ pues e es neutro, pero por otra parte $1e = e$, pues 1 es neutro. Por lo tanto $1 = 1e = e$. Es decir, el neutro de un grupo es único.*

Observación 2.2.2 *Si z y y son inversos de x, un elemento de un grupo G. Es decir, estamos suponiendo que $xy = yx = xz = zx = 1$. Entonces*

$$z = 1z = (yx)z = y(xz) = y$$

Es decir, el inverso de un elemento de un grupo es único.

Si G tiene un número infinito de elementos decimos que G es infinito o que tiene orden infinito y anotamos $|G| = \infty$. Si G tiene un número finito de elementos, digamos n, decimos que G es un grupo finito de orden n y anotamos $|G| = n$.

Si H es un conjunto no vacío contenido en un grupo G tal que bajo la operación de G es un grupo, diremos que es un subgrupo de G y anotamos $H \leq G$. Por ejemplo G es subgrupo de G y $\{1\}$ son subgrupos de G y lso llamaremos los subgrupos triviales de G. Si G es subgrupo de G y $H \neq G$, entonces diremos que H e sun subgrupo propio de G.

Observación 2.2.3 *Sea H es un conjunto no vacío en un grupo G. Si H es cerrado bajo la operación de G, entonces la asociatividad de los elementos de H se hereda de G, es decir $x(yz) = (xy)z$ para todos los tríos de a, b, c de H, pues son elementos de G. Entonces si H es un subconjunto de G, que contiene al 1 de G, es cerrado bajo la multiplicación y tiene los inversos multiplicativos de todos sus elementos, entonces $H \leq G$.*

Ejemplo 2.2.1 *Sea H un subgrupo no trivial de $\mathbb{Z}$. Si $h \in H$ entonces su inverso aditivo también está en H, es decir, H siempre tiene números positivos. Además si $h \in H$ y $0 \neq m \in \mathbb{N}$ entonces $mh = h + h + h + \cdots + h \in H$, también $0h = 0 \in H$ y por último $-mh = (-h) + (-h) + \cdots + (-h) \in H$. Es decir, si $h \in H$, entonces $mh \in H$ para cada $m \in \mathbb{Z}$. Sea a el menor entero positivo de H, y sea $b \in H$. Por algoritmo de la división en $\mathbb{Z}$ se tiene que existen m y r enteros tales que:*

$$b = ma + r, \quad con\, 0 \leq r < a$$

Pero como tanto b y ma están en H se tiene que $r = b + (-ma) \in H$, si r es positivo contradice la minimalidad de a, por lo tanto $r = 0$. Es decir, para cada $b \in H$ se tiene que existe $m \in \mathbb{Z}$ tal que $b = ma$. Es decir, todo elemento de H es un múltiplo de a. Es decir, si H es un subgrupo no trivial

de $\mathbb{Z}$, *entonces* H *es el conjunto de los múltiplos de un entero fijo. Como* $\mathbb{Z}$ *son los múltiplos de* 1 *y* $\{0\}$ *son los múltiplos de* 0. *Entonces todo subgrupo de* $\mathbb{Z}$ *es de la forma*

$$a\mathbb{Z} = \{ak/\ k \in \mathbb{Z}\}$$

Si H es un subgrupo de G tal que $gHg^{-1} \subseteq H$ para cualquier elemento $g \in G$, diremos que H es un subgrupo normal de G y anotamos $H \trianglelefteq G$. Todo subgrupo de un grupo abeliano es normal.

Observación 2.2.4 *Si* $H \trianglelefteq G$ *entonces para cualquier* $g \in G$ *se tiene que* $gHg^{-1} \subseteq H$, *por lo tanto* $H \subseteq g^{-1}Hg\ \forall g \in G$. *Como* g^{-1} *recorre todo* G *si* g *lo hace, entonces* $H \subseteq gHg^{-1}\ \forall g \in G$. *Es decir,* $H \trianglelefteq G$ *si y solo si* $H = gHg^{-1},\ \forall g \in G$.

Observación 2.2.5 *Si* $H \trianglelefteq G$, *y* $g \in G$. *Tomemos* $gh \in gH$, *entonces* $gh = ghg^{-1}g$, *como* $ghg^{-1} \in H$, *entonces* $(ghg^{-1})g \in Hg$. *Por lo tanto* $gH \subseteq Hg$. *De forma similar se puede mostrar que* $Hg \subseteq gH$. *Es decir,* $H \trianglelefteq G$ *implica que* $gH = Hg$ *para cualquier* $g \in G$. *El recíproco también es cierto.*[**Ejercicio**]

Observación 2.2.6 *Si* G *es un grupo y* N *es un subgrupo normal de* G *y* H *un subgrupo de* G *que contiene a* N, *entonces* N *es normal en* H.[**Ejercicio**]

Si G es un grupo, el conjunto de los elementos que conmutan con todos los elementos de G se llama *el centro* de G y se anota por $Z(G)$ (o simplemente Z si el grupo está subentendido), esto es

$$Z(G) = \{x \in G/\ xg = gx,\ \ \forall g \in G\},$$

además el centro de G es un subgrupo abeliano normal en G. [**Ejercicio**]

Si $H \leq G$, entonces la relación $g \sim k \iff k^{-1}g \in H$, es una relación de equivalencia en G. De hecho, como H es subgrupo de G, entonces $1 \in H$, por lo tanto $g^{-1}g = 1 \in H$, es decir $g \sim g$. Hemos comprobado que $\sim$ es refleja. Por otra parte $g \sim k$ es equivalente a $k^{-1}g \in H$, como H es subgrupo de G, se tiene que $g^{-1}k = (k^{-1}g)^{-1} \in H$, o sea $k \sim g$. Hemos probado que $\sim$ es simétrica.

Además $g \sim k$ es equivalente a $k^{-1}g \in H$, y $k \sim t$ es equivalente a $t^{-1}k \in H$, como H es subgrupo de G, se tiene que $(t^{-1}k)(k^{-1}g) \in H$, pero

$$(t^{-1}k)(k^{-1}g) = t^{-1}(kk^{-1})g = t^{-1}g \in H$$

es decir $g \sim t$. Hemos probado que $\sim$ es transitiva.

A la cantidad de distintas clases de equivalencia se le llama el índice de H en G, y anotamos $|G : H|$ o también $[G : H]$. La clase de g es $gH = \{gh/\ h \in H\}$, además notamos que si $gh = gh'$ entonces $h = h'$, es decir la función

$$\phi : H \to gH$$

definida por $\phi(h) = gh$, es una función inyectiva. Además por definición de gH también es epiyectiva. Es decir, gH tiene tantos elementos como H. En particular si G es finito y como G es la unión disjunta de clases laterales, se tiene que $|G| = m|H|$ donde $m = [G : H]$ es la cantidad de clases distintas, luego se tiene que si G es finito

$$[G : H] = \frac{|G|}{|H|}$$

y además $|H|$ divide a $|G|$, a este resultado se le conoce como el teorema de Lagrange, que enunciamos a continuación:

Teorema 2.2.1 (Teorema de Lagrange) *El orden de un subgrupo de un grupo finito divide al orden del grupo.*

Observación 2.2.7 *Si G es finito y $K \leq H \leq G$, entonces*

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \times \frac{|H|}{|K|} = [G : H] \times [H : K]$$

Si $[G : H]$ y $[H : K]$ son finitos, entonces el resultado sigue siendo cierto, aunque G no sea finito.[**Ejercicio**]

Observación 2.2.8 *Si $h \in H \subseteq G$, entonces $hH \subseteq H$. Además si $h' \in H$ entonces $h^{-1}h' \in H$, pues H es subgrupo de G. Por lo tanto $h' = hh^{-1}h' \in hH$. Es decir $hH = H$.*

Ejemplo 2.2.2 *Todo subgrupo de índice dos en un grupo G es normal en G.*

Demostración:
Sea G un grupo y H un subgrupo de índice 2. Entonces si $g \notin H$, se tiene que gH es el conjunto de los elementos que no están en H, pues si $gh \in H$ con $h \in H$ implicaría que $g \in H$. Lo mismo ocurre con Hg. Luego si $g \notin H$ se tiene que $gH = Hg = G \setminus H$, es decir que $gHg^{-1} = H$ y si $g \in H$ entonces se tiene trivialmente que $gHg^{-1} = H$, luego para todo $g \in G$ se tiene que $gHg^{-1} = H$. ■

En el caso en que H es normal en G se tiene que la operación

$$g_1Hg_2H = g_1g_2H$$

está bien definida en $G/\sim$, de hecho si $g_1H = g_1'H$ y $g_2H = g_2'H$, entonces existen h_1 y h_2 tales que $g_1h_1 = g_1'$ y $g_2h_2 = g_2'$. Así tenemos:

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H$$

Como H es normal en G se tiene que $g_2H = Hg_2$, por lo tanto:

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H = g_1h_1Hg_2 = g_1Hg_2$$

De nuevo, como H es normal en G se tiene que $g_2H = Hg_2$, por lo tanto:

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H = g_1h_1Hg_2 = g_1Hg_2 = g_1g_2H$$

Además H es el neutro de G/H y $g^{-1}H$ es el inverso de gH. Así tenemos que $G/\sim$ es un grupo, al que llamamos el *grupo cuociente* y denotamos por G/H.

Ejemplo 2.2.3 *Como $\mathbb{Z}$ es abeliano, todo subgrupo de $\mathbb{Z}$ es normal en $\mathbb{Z}$, además todo subgrupo de $\mathbb{Z}$ es de la forma $m\mathbb{Z}$, en este caso el cuociente $\mathbb{Z}/m\mathbb{Z}$ es $\mathbb{Z}_m$.*

Sean G y G' dos grupos y sea 1 el neutro de G y $1'$ el neutro de G' y sea además f una función $f : G \to G'$ que satisface

$$f(gh) = f(g)f(h) \ \ \forall\, g, h \in G$$

y además

$$f(1) = 1',$$

entonces diremos que f es un *homomorfismo* (de grupos) o *morfismo* (de grupos), o simplemente morfismo si la estructura se subentiende. Si f es inyectivo, diremos que es un *monomorfismo.* Si f es epiyectivo, diremos que f es un *epimorfismo.* Si f es biyectivo, diremos que f es *isomorfismo,* en ese caso diremos que G es isomorfo a G' y anotaremos $G \cong G'$.

Ejemplo 2.2.4 *Si X es un conjunto cualquiera, el conjunto de todas las biyecciones de X en si mismo con la operación composición es un grupo, llamado el grupo de permutaciones de X, cuyo neutro es la función id_X. A tal grupo lo denotaremos por Σ_X. Si existe una biyección $\phi : X \to Y$ entonces para cada $\sigma \in \Sigma_X$ la función $\Phi(\sigma) = \phi \circ \sigma \circ \phi^{-1}$ es un elemento de Σ_Y, además Φ define un isomorfismo entre Σ_X y Σ_Y. Es decir, el grupo de permutaciones solo depende de la cardinalidad de X, y no de los elementos de X, en particular si X es finito, digamos que tiene n elementos entonces Σ_X lo denotamos por Σ_n y sin restricción podemos pensar que $X = \{1, 2, 3, 4, \ldots, n\}$. El orden de Σ_n es $n!$.*

Si $X = \{1, 2, 3, \ldots, n\}$ y si $\sigma \in \Sigma_n$, entonces denotaremos

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Por ejemplo la función de $\{1, 2, 3\}$ en sí mismo que lleva el 1 al 2, el 2 al 3 y el 3 al 1, la denotamos por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Los seis elementos de Σ_3 son:

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Para denotar la función que fija a 3 y permuta al 1 con el 2 lo denotamos también por (12). Más generalmente, si $\sigma \in \Sigma_n$ es tal que $\sigma(k_1) = k_2$, $\sigma(k_2) = k_3$, $\sigma(k_3) = k_4, \ldots \sigma(k_r) = k_1$, y σ funciona como la identidad en el resto de elementos de $\{1, 2, 3, \ldots n\}$ entonces σ lo denotaremos por $(k_1 k_2 k_3 k_4 \ldots k_r)$ y lo llamaremos un ciclo de largo r. Según esta notación, se tiene que:

$$\Sigma_3 = \{(1), (12), (13), (23), (123), (132)\}$$

A la identidad la anotaremos por 1.

Notamos que $\{1, (12)\}$, $\{1, (13)\}$, $\{1, (23)\}$, *son los únicos subgrupos de orden* 2 *y* $H = \{1, (123), (132)\}$ *es el único subgrupo de orden* 3. *Además el índice de* H *en* G *es* 2, *por lo tanto* $H \trianglelefteq G$.

Además notemos que $(12)(13) = (132)$, *en cambio* $(13)(12) = (123)$ *por lo tanto* Σ_3 *no es conmutativo. Más aún, si* $n \geq 3$ *consideremos los ciclos de largo* 2, (12) *y* (13) *en* Σ_n, *entonces*

$$(12)(13) \neq (13)(12).$$

Es decir, Σ_n *no es abeliano para* $n \geq 3$.

Además $\Sigma_2 = \{1, (12)\}$ *y* $\Sigma_1 = \{1\}$, *ambos claramente abelianos. Es decir,* Σ_n *es conmutativo si y solo si* $n = 1$ *o* $n = 2$.

Observación 2.2.9 *Si* x *es un elemento de un grupo* G *tal que* $xx = x$, *entonces* $xxx^{-1} = xx^{-1}$ *por lo tanto* $x = 1$. *Es decir, en un grupo el* 1 *es el único elemento idempotente.*[1]

Observación 2.2.10 *Si* $ab = 1$, *entonces* $ba = b(ab)a = (ba)^2$ *por lo anterior se tiene que* $ba = 1$. *Es decir, el inverso iazquierdo (o derecho) de un elemento es el inversod el elemento.*

Observación 2.2.11 *Si* G *y* G' *son grupos con neutros* 1 *y* $1'$, *respectivamente y si* $f : G \to G'$ *es tal que* $f(xy) = f(x)f(y)$ *para cualesquiera* $x, y \in G$, *entonces* $f(1) = f(1 \times 1) = f(1)f(1)$. *Por la observación anterior tenemos que* $f(1) = 1'$. *Es decir,* f *es un morfismo.*

Observación 2.2.12 *Si* G *y* G' *son grupos con neutros* 1 *y* $1'$, *respectivamente y si* $f : G \to G'$ *es un morfismo, entonces*

$$1' = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$$

Entonces $f(x^{-1}) = (f(x))^{-1}$.

[1]Un elemento e se dice idempotente si $e^2 = e$. Por ejemplo, [3] es idempotente en $\mathbb{Z}_6$. Por ejemplo, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ es idempotente en $M_2(\mathbb{R})$. Lo que muestra que tanto $M_2(\mathbb{R})$ como $\mathbb{Z}_6$ no son grupos con la multiplicación.

Sea G un grupo y $f : G \to G$ un isomorfismo, en este caso le llamamos un automorfismo. El conjunto

$$Aut(G) = \{f : G \to G / \ f \text{ es automorfismo}\}$$

es un grupo con la operación composición. [**Ejercicio**]

Si G es un grupo y $g \in G$ entonces la función $f_g : G \to G$ definida por $f_g(x) = gxg^{-1}$ es un automorfismo, de hecho $f_{g^{-1}}$ es la inversa de f_g y se llama un automorfismo interior de G. El conjunto

$$Inn(G) = \{f_g / \ g \in G\}$$

es un subgrupo de $Aut(G)$.[**Ejercicio**]

Observación 2.2.13 *Una observación inmediata es que H es normal en G si y solo si $f_g(H) = H$, para cualquier automorfismo interior.*

Un subgrupo H de un grupo G que es invariante por cualquier automorfismo $\sigma \in Aut(G)$, esto es $\sigma(H) \subseteq H$, se llama un subgrupo *característico.*

Observación 2.2.14 *Todo subgrupo caracacterístico es normal.*

Observación 2.2.15 *Si H es un subgrupo característico de un grupo finito G, entonces $\sigma(H) = H \ \forall \sigma \in Aut(G)$. De hecho, podemos definir por restricción un morfismo de $\overline{\sigma} : H \to H$, como $\overline{\sigma}$ es inyectivo, entonces $|Im(\overline{\sigma})| = |H|$ pero como $\overline{\sigma}(H) \subseteq H$ y H es finito, se tiene que $Im(\overline{\sigma}) = \sigma(H) = H$.*

Observación 2.2.16 *Si H es el único subgrupo de orden $|H|$ en G, con G finito, entonces H es característico.*[**Ejercicio**]

Observación 2.2.17 *Si H es el único subgrupo de orden $|H|$ en G, con G finito, entonces H es normal en G.*[**Ejercicio**]

Proposición 2.2.1 *Si $H \trianglelefteq G$ y K es característico en H, entonces K es normal en G.*

Demostración:
Sea f_g un automorfismo interior de G, cualquiera, como H es normal, f_g define un automorfismo de H por restricción, sea τ esa restricción, es decir, $\tau \in Aut(H)$.
Como K es característico en H se tiene que $\tau(K) \subseteq K$, luego $gKg^{-1} \subseteq K$. ■

Si $f : G \to G'$ es un morfismo de grupos, entonces el conjunto $Ker(f) = \{g \in G/\ f(g) = 1\}$ se llama el kernel de f, el cual es un subgrupo normal de G. De hecho,

- $1 \in Ker(f)$.
- Si $x, y \in Ker(f)$ entonces $f(xy) = f(x)f(y) = 1 \times 1 = 1$, luego $xy \in Ker(f)$
- Si $x \in Ker(f)$, entonces $1 = f(xx^{-1}) = f(x)f(x^{-1}) = 1 \times f(x^{-1}) = f(x^{-1})$. Luego $x^{-1} \in Ker(f)$.

Observación 2.2.18 *Si $\phi : G \to G'$ es un morfismo de grupos que no es inyectivo, entonces existen $x \neq x$ en G tales que $\phi(x) = \phi(x')$, o equivalentemente $\phi(x)(\phi(x'))^{-1} = \phi(xx'^{-1}) = 1'$. Es decir, $1 \neq xx'^{-1} \in Ker(\phi)$. Reciprocamente si $1 \neq z \in Ker(\phi)$, entonces $\phi(z) = 1' = \phi(1)$, luego ϕ no es inyectiva. Es decir:*

$\phi : G \to G'$ *morfismo de grupos es inyectivo si y solo si* $Ker(\phi) = \{1\}$.

Si $f : G \to G'$ es morfismo de grupos, el conjunto $Im(f) = \{f(g)/\ g \in G\}$ es un subgrupo (no necesariamente normal) de G. **[Ejercicio]**

Proposición 2.2.2 *Todo subgrupo normal es el kernel de algún morfismo.*

Demostración:
Sea $H \trianglelefteq G$ y consideremos el grupo cuociente G/H, para terminar la demostración basta notar que la proyección canónica

$$\pi : G \to G/H$$

definida por $\pi(g) = gH$, es un morfismo, de hecho

$$\pi(gg') = gHg'H = gg'H = \pi(gg')\ \forall g, g' \in G$$

cuyo kernel es H. ■

Observación 2.2.19 *Si K y H son subgrupos entonces $H \cap K$ es un subgrupo de G.* [**Ejercicio**]

Si S es un subconjunto de G entonces la intersección de todos los subgrupos de G que contienen a S es un subgrupo de G, llamado el *subgrupo generado por* S y lo denotamos por $< S >$. En particular, si $S = \{g\}$ entonces $< S >$ se llama el *subgrupo cíclico generado por* g, y lo denotamos por $< g >$, al orden de $< g >$ le llamamos el orden de g. Si existe $g \in G$ tal que $G =< g >$, entonces decimos que G es un grupo cíclico.

Si $g \in G$, donde G es un grupo. Si definimos $g^0 = 1$ e inductivamente $g^n = gg^{n-1}$ para $0 < n \in \mathbb{N}$, entonces tenemos todas las potencias naturales de g. Además si n es entero positivo, entonces definimos g^{-n} por $(g^{-1})^n$. Así tenemos definidas todas las potencias enteras de g.

Observación 2.2.20 *Si G es un grupo y $g \in G$, entonces para cada $n, m \in \mathbb{Z}$ se tiene que $g^{n+m} = g^n g^m = g^m g^n$. Además $(x^m)^n = x^{mn}$ para cualesquiera $m, n \in \mathbb{Z}$. (*[**Ejercicio**]*)*

Observación 2.2.21 *Si G es un grupo y $g \in G$, entonces $< g >= \{g^n / \ n \in \mathbb{Z}\}$. De hecho $1 = g^0$, y por la observación anterior se tiene que $g^n g^m = g^{n+m}$ y por definición $g^{-n}g^n = 1$. Entonces $\{g^n / \ n \in \mathbb{Z}\}$ es un grupo y $g^1 = g \in \{g^n / \ n \in \mathbb{Z}\}$. Entonces $< g >\subseteq \{g^n / \ n \in \mathbb{Z}\}$. Reciprocamente si $g \in H \leq G$ entonces $g^n \in H$, $\forall n \in \mathbb{Z}$ por lo tanto $\{g^n / \ n \in \mathbb{Z}\} \subseteq H$, es decir*

$$\{g^n / \ n \in \mathbb{Z}\} \subseteq \bigcap_{g \in H \leq G} H =< g > .$$

Observación 2.2.22 *Si $g \in G$ de orden finito. Entonces $< g >= \{g^k / \ k \in \mathbb{Z}\}$ tiene un número finito de elementos. Entonces existen k y k' enteros distintos tales que $g^k = g^{k'}$, sin restricción supondremos que $k > k'$, entonces $g^{k-k'} = 1$. Si denotamos $m = k - k' > 0$ entonces $g^m = 1$. Sea n el menor entero positivo tal que $g^n = 1$, entonces $H = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$ es el grupo generado por g. De hecho, 1 es su propio inverso y si $0 < k < n$ consideremos $g^k \in H$ entonces $g^{n-k} \in H$ y $g^{n-k} = (g^k)^{-1}$. Además si g^k y $g^{k'}$ con $k + k' < n$, son elementos de H cuyo producto $g^k g^{k'} = g^{k+k'}$ es también un elemento de H. Si $k + k' \geq n$, se tiene que $0 \leq k + k' - n < n$, entonces*

$$g^k g^{k'} = g^{k+k'} = g^{n+(k+k'-n)} = g^n g^{k+k'-n} = g^{k+k'-n}$$

elemento que vive en H.

Observación 2.2.23 *Si $g \in G$ de orden finito. Entonces el orden de g es el menor entero positivo n tal que $g^n = 1$.*

Observación 2.2.24 *Si $g \in G$ de orden finito y $g^n = 1$, entonces n es un múltiplo del orden de g.* [**Ejercicio**]

Observación 2.2.25 *Si $1 \neq g \in G$ y p primo tal que $g^p = 1$, entonces p es el orden de g.*

Observación 2.2.26 *Si $g \in G$ de orden infinito. Entonces no existe entero $n \neq 0$ tal que $g^n = 1$.*

Observación 2.2.27 *Por el teorema de Lagrange se tiene que el orden de un elemento de un grupo finito divide al orden del grupo.*

Observación 2.2.28 *Si G es finito y $g \in G$, entonces $g^{|G|} = 1$.*

Observación 2.2.29 *Si G es cíclico con $< g >= G$, entonces $G =< g^{-1} >$.* *(*[**Ejercicio**]*)*

Ejemplo 2.2.5 *Si p es primo entonces $\mathbb{Z}_p^\times$ el conjunto de los elementos no nulos de $\mathbb{Z}_p$ es un grupo con la multiplicación. Además $\mathbb{Z}_p^\times$ tiene $p-1$ elementos. Por la observación anterior se tiene que para todo $[x] \in \mathbb{Z}_p^\times$ se tiene que:*

$$[x]^{p-1} = [1]$$

o dicho de otra forma

Si $x \in \mathbb{Z}$ y p no divide a x entonces $x^{p-1} \equiv 1 \mod(p)$.

El anterior resultado se conoce con el nombre de "Pequeño Teorema de Fermat."

Ejemplo 2.2.6 *Si G es un grupo cuyos elementos satisfacen $x^2 = 1$. Entonces si $x, y \in G$ se tiene que*

$$(xy)^2 = 1 = x^2y^2$$

es decir

$$(xy)(xy) = (xx)(yy)$$

multiplicando por $x^{-1} = x$ *por la izquierda se tiene que:*

$$yxy = xyy$$

multiplicando por $y^{-1} = y$ *por la derecha se tiene que:*

$$yx = xy$$

Es decir, G *es abeliano.*
En particular consideremos G *un grupo de orden* 4. *Entonces si en* G *hay un elemento* x *de orden* 4, *entonces* $G =< x >$. *Si* G *no tiene elementos de orden* 4, *entonces todos sus elementos, distintos del neutro, tienen orden* 2, *por lo de arriba se tiene que* G *es abeliano.Es decir, todo grupo de orden* 4 *es abeliano.*

Observación 2.2.30 *Si* $|G| = p$ *con* p *primo, consideremos* $1 \neq g \in G$, *entonces* $< g >$ *es un subgrupo no trivial de* G. *Por el teorema de Lagrange, se tiene que* $|g|$ *divide a* p *y no es* 1. *Por lo tanto* $|g| = p$ *es decir* $G =< g >$. *Es decir, todo grupo de orden primo es cíclico.*

Observación 2.2.31 *Si* G *es un grupo cíclico infinito, digamos* $G =< g >$, *y consideremos el grupo* $\mathbb{Z}$ *con la suma, entonces definamos la función:*

$$\phi : \mathbb{Z} \to G$$

por $\phi(n) = g^n$. *Esta función es un morfismo, pues* $g^n g^m = g^{n+m}$ *para cualesquiera* $n, m \in \mathbb{Z}$, *que es epiyectivo, pues todo elelemnto del grupo cíclioc generado por* g *e suna potencia de* g. *Además es inyectivo, pues si* $n \in Ker(\phi)$, *quiere decir que* $g^n = 1$, *pero como* g *es de orden infinito, se tiene que* $n = 0$. *Luego* G *es isomorfo a* $\mathbb{Z}$. *Es decir:*

Salvo isomorfismo, $\mathbb{Z}$ *es el único grupo cíclico infinito.*

Si H y K son subgrupos de un grupo G, el conjunto $KH = \{kh/\ k \in K,\ h \in H\}$ no es necesariamente un subgrupo de G. Por ejemplo, $H = \{1, (12)\}$ y $K = \{1, (2, 3)\}$ son subgrupos de Σ_3 y

$$KH = \{1, (23), (12), (132)\}$$

no es subgrupo de Σ_3. El siguiente resultado da condiciones necesarias y suficientes para que KH sea subgrupo de G.

Proposición 2.2.3 *Si H y K son subgrupos de G, entonces KH es subgrupo de G si y solamente si $KH = HK$.*

Demostración:
($\Rightarrow$)Sean $k \in K$ y $h \in H$, entonces $k^{-1}h^{-1} \in KH$, como KH es un grupo se tiene que $hk = (k^{-1}h^{-1})^{-1} \in KH$, luego $HK \subseteq KH$.

Por otra parte sea $z \in KH$, mostraremos que z está en HK. Sea $w = z^{-1} \in KH$, pues KH es subgrupo de G, entonces $w = kh$ para ciertos $k \in K$ y $h \in H$, entonces

$$z = w^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$$

Es decir, $KH \subseteq HK$ y como ya teníamos que $HK \subseteq KH$, entonces $HK = KH$.

($\Leftarrow$) Como H y K contienen a 1, entonces $1 \in HK = KH$. Sean ahora $k, k' \in K$ y $h, h' \in H$, entonces $kh \in KH$, luego $h^{-1}k^{-1} = (kh)^{-1} \in HK = KH$, luego $(kh)^{-1} \in KH$.

Además

$$(kh)(k'h') = k(hk')h'$$

como $HK = KH$ se tiene que $hk' = k_1h_1$, para ciertos $k_1 \in K$ y $h_1 \in H$, luego

$$(kh)(k'h') = k(k_1h_1)h' = kk_1(h_1h')$$

denotemos por $k_2 = kk_1 \in K$ y por $h_2 = h_1h' \in H$, entonces tenemos

$$(kh)(k'h') = k_2h_2 \in KH,$$

luego KH es un subgrupo de G. ■

Corolario 2.2.1 *Si G es un grupo, $H \leq G$ y $N \trianglelefteq G$, entonces $NH \leq G$*

Demostración:

Como N es normal, para cada $g \in G$ se tiene que $gN = Ng$, en particualr si $h \in H \subseteq G$ se tiene que $hN = Nh$. Por lo tanto $HN = NH$ y por el resultado anterior, tenemos que $HN \leq G$. ■

2.3. Teoremas de Isomorfismos y Acción de Grupos.

En esta sección estudiaremos los primeros resultados importantes de la Teoría de Grupos y estudiaremos algunos ejemplos de grupos con cierto detalle.

El primer teorema que estudiaremos es un teorema de isomorfismos, que es idéntico, al primer teorema del isomorfismo para espacios vectoriales, que se estudia en un curso de Álgebra Lineal, pero ahora en contexto de grupos. En el siguiente capítulo estudiaremos el correspondiente a este Teorema, para Anillos.

Teorema 2.3.1 (Primer Teorema del Isomorfismo) *Sea $\tau : G \to G'$ un morfismo de grupos entonces $G/Ker(\tau)$ es isomorfo a $Im(\tau)$.*

Demostración:

Denotemos por $K = Ker(\tau)$ y definamos $\tilde{\tau}(gK) = \tau(g)$ de G/K en $Im(\tau)$. Primero que nada debemos mostrar que $\tilde{\tau}$ está bien definida. Esto es, si $gK = g'K$, entonces debiéramos tener que $\tilde{\tau}(gK) = \tilde{\tau}(g'K)$. Para ello notemos que $gK = g'K$ significa que exsite $k \in Ker(\tau)$ tal que $g' = gk$, por lo tanto:

$$\tau(g') = \tau(gk) = \tau(g)\tau(k),$$

pero como $\tau(k) = 1$, se tiene que:

$$\tilde{\tau}(g'K) = \tau(g') = \tau(gk) = \tau(g)\tau(k) = \tau(g) = \tilde{\tau}(gK)$$

Es decir, $\tilde{\tau}$ es efectivamente una función, que por la definición de $Im(\tau)$ es epiyectiva.

Además $\tilde{\tau}(gKg'K) = \tilde{\tau}(gg'K) = \tau(gg') = \tau(g)\tau(g')$, es decir τ es un morfismo de grupos. Para finalizar la demostración, tomemos $gK \in Ker(\tilde{\tau})$, equivalentemente, $\tau(g) = 1'$, es decir, $g \in Ker(\tau) = K$. Es decir, si $K = Ker(\tilde{\tau})$, o sea, $Ker(\tilde{\tau})$ contiene solamente al neutro de G/K, por lo tanto $\tilde{\tau}$ es inyectiva. Es decir $\tilde{\tau}$ es un isomorfismo ■

Ejemplo 2.3.1 *Sea $g \in G$ un elemento de un grupo. Definamos $\phi_g : G \to G$ por conjugación, esto es, $\phi_g(x) = gxg^{-1}$ para cada $x \in G$, notamos que $\phi_{g^{-1}}$ es la función inversa de ϕ_g, por lo tanto, ϕ_g es biyectiva. Además*

$$\phi_g(x)\phi_g(x') = (gxg^{-1})(gx'g^{-1}) = gx(g^{-1}g)x'g^{-1} = gxx'g^{-1} = \phi_g(xx')$$

Por lo tanto ϕ_g es un morfismo biyectivo. En la sección anterior llamamos a ϕ_g un automorfismo interior de G y al conjunto de todos los automorfismos interiores lo denotamos por $Inn(G)$. Además notamos que

$$\phi_g \circ \phi_{g'}(x) = \phi_g(g'xg^{-1}) = g(g'xg'^{-1})g^{-1} = gg'x(gg')^{-1} = \phi_{gg'}(x) \ \forall x, g, g' \in G$$

Es decir, $\phi_g \circ \phi_{g'} = \phi_{gg'}$. Por lo tanto $\Phi : G \to Aut(G)$ definida por $\Phi(g) = \phi_g$ es un morfismo de grupos, además $Im(\Phi) = Inn(G)$.

Por otra parte

$$Ker(\Phi) = \{g \in G/ \ \phi_g = id_G\} = \{g \in G/ \ \phi_g(x) = x \ \forall x \in G\}$$

$$= \{g \in G/ \ gxg^{-1} = x \ \forall x \in G\} = \{g \in G/ \ gx = xg \ \forall x \in G\} = Z(G)$$

Entonces por el primer T. del isomorfismo se tiene que:

$$G/Z(G) \cong Inn(G)$$

Ejemplo 2.3.2 *Sea G un grupo finito y H un subgrupo de índice p, donde p es el menor primo que divide a G, entonces H es normal en G.*

Demostración:

Sea Ω el conjunto de todas las clases laterales de H en G, entonces $|\Omega| = p$, luego para cada $g' \in G$ definimos $\tau_{g'}$ de Ω en si mismo por $\tau'_g(gH) = g'(gH) = (g'g)H$, la cual es una biyección de Ω en si mismo. Pues si

$$\tau'_g(g_1H) = \tau'_g(g_2H) \iff (g'g_1)H = (g'g_2)H \iff g_2^{-1}g'^{-1}g'g_1 \in H$$

$$\iff g_2^{-1}g_1 \in H \iff g_1H = g_2H$$

Por lo tanto τ es inyectiva. Como τ va de Ω en si mismo y Ω es finito, entonces τ es biyectiva.

Más aún $\phi : g' \to \tau'_g$ es un morfismo de G en Σ_Ω que es isomorfo a Σ_p que tiene orden $p!$. Luego el kernel de ϕ ,$K = \{x \in G/ \ xgH = gH \ \forall g \in G\}$ está contenido en H, pues si $x \in K$, en particular $xH = H$ y además K es normal en G, pues es el kernel de un homomorfismo. Luego por el primer teorema del isomorfismo se tiene que G/K es isomorfo a un supgrupo de Σ_p, luego $[G : K]$, que es un divisor de $|G|$, divide a $p!$.

Tenemos que $[G : K] = [G : H][H : K]$, *por lo tanto* $[G : K] = pq$ *por lo tanto* $q = [H : K]$ *es un divisor de* $(p-1)!$, *por lo tanto si* r *es un divisor primo de* q, *entonces* $r < p$ *y como* $q = [H : K]$ *divide a* $|H|$ *y este a* $|G|$, *y* p *es el menor primo divosor de* $|G|$, *entonces tal* r *no existe, luego* $q = 1$, *es decir* $[H : K] = 1$. *Es decir,* $H = K$ *y como* K *es el kernel de un morfismo, entonces* $H = K$ *es normal en* G. ■

Ejemplo 2.3.3 *Sea* G *cíclico finito, y sea* $G =< g >$. *Definamos* $\phi(n) = g^n$ *una función de* $\mathbb{Z}$ *en* G. *Como* $g^{n+m} = g^n g^m$ *se tiene que* ϕ *es morfismo, además es epiyectivo. Además sabemos que* ϕ *no es inyectivo, por lo tanto existe* m *entero positivo tal que* $m\mathbb{Z} = Ker(\phi)$. *Por primer teorema del isomorfismo se tiene que*

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z} \cong G.$$

Además como $\mathbb{Z}_m \cong \mathbb{Z}_n$ *si y solamente si* $n = m$, *entonces para cada* m *entero positivo, existe un único grupo cíclico, salvo isomorfismos, de orden* m.

El siguiente resultado es un corolario del Primer Teorema del Isomorfismo.

Teorema 2.3.2 (Segundo Teorema del Isomorfismo) *Sean* K *y* N *subgrupos de* G, *con* N *normal en* G, *entonces* NK *es un subgrupo de* G *y* $N \cap K$ *es normal en* K, *además se tiene* $K/(N \cap K)$ *es isomorfo a* NK/N.

Demostración:

Como N es normal en G, entonces $NK = KN$, de lo que se desprende que NK es un subgrupo de G. Además como K contiene al 1, se tiene que $N \subseteq NK$, por tanto $N \trianglelefteq NK$. Consideremos el cuociente NK/N y $nkN \in NK/N$, como N es normal en G tenemos que:

$$nkN = kk^{-1}nkN = kN$$

Es decir, toda clase lateral de N en NK tiene un representante de K. Es decir, si gN es un elemento de NK/N entonces existe $k \in K$ tal que $gN = kN$. Es decir el conjunto $\{kN/\ k \in K\}$ es el conjunto de todas las clases laterales de N en NK.

Por lo tanto la función $\rho : K \to NK/N$ definida por $\rho(k) = kN$ es una función epiyectiva. Además

$$\rho(kk') = kk'N = (kN)(k'N) = \rho(k)\rho(k')$$

Por lo tanto ρ es un morfismo. Además

$$Ker(\rho) = \{k \in K / kN = N\} = \{k \in K / k \in N\} = N \cap K$$

Por lo tanto $N \cap K \trianglelefteq K$ y además por el P. T del isomorfismo:

$$K/(N \cap K) \cong NK/N \ \blacksquare$$

El siguiente también es un corolario del primer teorema del isomorfismo.

Teorema 2.3.3 (Tercer Teorema del Isomorfismo) *Sean K y H subgrupos normales de G, y $K \leq H$, entonces H/K es un subgrupo normal de G/K y además se tiene que $(G/K)/(H/K)$ es isomorfo a G/H.*

Demostración:

Primero que nada notemos que si $gK = g'K$ es equivalente a decir que existe $k \in K$ tal que $g' = gk$, pero como $K \subseteq H$ se tiene que $g' = gk$ con $k \in H$, por lo tanto $gH = g'H$. Es decir la función $\eta : G/K \to G/H$ definida por $\eta(gK) = gH$ está bien definida. Además notamos que es epiyectiva. Por otra parte

$$\eta((gK)(g'K)) = \eta(gg'K) = gg'H = gHg'H = \eta(gK)\eta(g'K)$$

Por tanto η es un morfismo y como notamos antes, es epiyectivo. Para terminar la demostración necesitamos conocer el $Ker(\eta)$.

$$Ker(\eta) = \{gK \in G/K \ / \ gH = H\} = \{gK \in G/K \ / \ g \in H\} = H/K$$

Por lo tanto H/K es normal en G/K y por primer teorema del isomorfismo se tiene que:

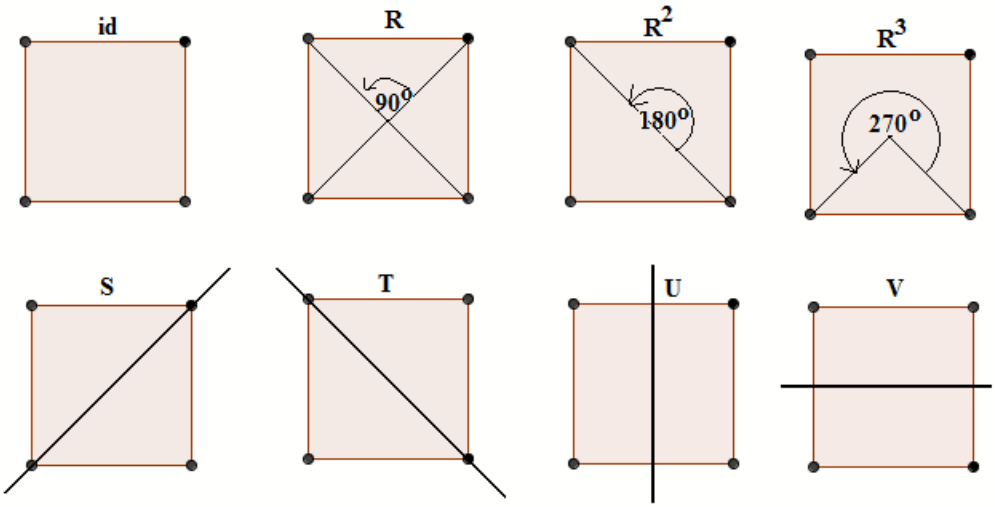
$$(G/K)/(H/K) \cong G/H \ \blacksquare$$

Cuidado

En el enunciado del anterior teorema aparece H, K normales en G y además $K \leq H$. Alguien podría decir, que es lo mismo que decir que $K \trianglelefteq H \trianglelefteq G$. Pero eso es falso, hay ejemplos de $K \trianglelefteq H \trianglelefteq G$, pero K no es normal en G.

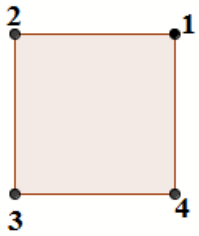
Ejemplo 2.3.4 *Consideremos el grupo de simetrías del cuadrado,* $D_4 = \{id = 1, R, R^2, R^3, S, T, U, V\}$, *donde* R *es la rotación en un ángulo recto y como centro la intersección de las diagonales del cuadrado. La rotación en un ángulo extendido es* R^2, *y la rotación en un ángulo de* $270°$ *es* R^3. *La reflexión respecto a una de las diagonales es* S, *la reflexión respecto a la otra diagonal es* T. *Las reflexiones respecto a la recta que pasa por los puntos medios de lados paralelos las denotamos por* U *y* V. *Tenemos además que*

$$S^2 = T^2 = U^2 = V^2 = (R^2)^2 = 1$$



Si en el cuadrado inicial, numeramos los vértices con los números del conjunto $\{1, 2, 3, 4\}$, *como se muestra abajo:*

Entonces cada una de las simetrás del cuadrado la podemos ver como una permutación de $\{1, 2, 3, 4\}$. *Así* R *transforma* $1 \to 2$, $2 \to 3$, $3 \to 4$ *y* $4 \to$



1. *Es decir, R visto en Σ_4 es* (1234). *Del mismo modo R^2 visto en Σ_4 es* $(13)(24)$, *del mismo modo R^3 es* (1432). *En este mismo sentido, S es* (24), T *corresponde a* (13), U *a* $(12)(34)$ *y V a* $(14)(23)$. *Por tanto podemos pensar D_4, llamado el grupo diedral de orden* 8, *como subgrupo de Σ_4.*

$$D_4 = \{1, (1234), (13)(24), (1432), (24), (13), (12)(34), (14)(23)\} \leq \Sigma_4$$

El conjunto $V_4 = \{1, (13)(24), (12)(34), (14)(23)\}$ es un subgrupo de D_4 llamado el grupo de Klein (que es isomorfo al grupo de simetrías del rectángulo no cuadrado). Como el índice de V_4 en D_4 es 2, *entonces*

$$V_4 \trianglelefteq D_4$$

Además $H = \{1, (12)(34)\}$ es un subgrupo de V_4. Como $[V_4 : H] = 2$ entonces $H \trianglelefteq V_4$. Pero

$$(1234)(12)(34)(1234)^{-1} = (1234)(12)(34)(1432) = (14)(23) \notin H$$

Es decir, H no es normal en D_4, pese a que $H \trianglelefteq V_4$ y $V_4 \trianglelefteq D_4$

Fin al ejemplo de Cuidado

Otra observación importante es reconocer la forma que tienen los subgrupos del grupo cuociente G/H, donde H es un subgrupo normal de G. En el tercer Teorema del Isomorfismo, el $Ker(\eta)$ resultó ser K/H donde η era un morfismo de G/H en otro grupo y $H \leq K \leq G$. Entonces la pregunta que surge es si todos los subgrupos de G/H tienen esa forma. Veamos:

Observación 2.3.1 *Consideremos un subgrupo $\mathcal{K}$ de G/H, donde H es un subgrupo normal de un grupo G. Entonces los elementos de $\mathcal{K}$ son clases laterales de H. Denotemos por $K = \{g/\ gH \in \mathcal{K}\}$. Como $\mathcal{K}$ es un subgrupo de G/H, se tiene que $\mathcal{K}$ contiene al neutro de G/H es decir H, entonces podemos afirmar que $gH \in \mathcal{K}$ para cada $h \in H$, es decir, $H \subseteq K$.*

Además si g y g' están en K, esto es gH y $g'H$ están en $\mathcal{K}$, entonces $gHg'H = gg'H \in \mathcal{K}$, pues $\mathcal{K}$ es subgrupo de G/H, entonces $gg' \in K$.

Para finalizar, si g está en K, esto es gH está en $\mathcal{K}$, entonces $(gH)^{-1} = g^{-1}H \in \mathcal{K}$, pues $\mathcal{K}$ es subgrupo de G/H, entonces $g^{-1} \in K$. Por lo tanto K es subgrupo de G que contiene a H. Es decir $\mathcal{K} = K/H$.

Reciprocamente, si G es un grupo que tiene a H como subgrupo normal y K es un subgrupo de G que contiene a H, entonces $H \trianglelefteq K$. Además K/H es un grupo bajo la misma operación que G/H es grupo. Entonces $K/H \leq G/H$.

2.3.1. Acción de Grupos.

Sea X un conjunto y G un grupo a una función

$$G \times X \to X$$

denotada por yuxtaposición se llama una **acción** de G en X, si se tiene las siguientes condiciones

$$1x = x \ \ \forall x \in X$$

$$g'(gx) = (g'g)x \ \ \forall g, g' \in G \ \ x \in X.$$

También diremos que X es un $G-$**conjunto.**

Si G actúa en X, esta acción define una relación de equivalencia en X, a saber $x \sim x' \iff$ existe $g \in G$ tal que $x' = gx$. La clase de equivalencia de $x \in X$ se llama la **órbita** de x, y es $[x] = orb(x) = Gx = \{gx/\ g \in G\}$. Para $x \in X$ definimos el conjunto $\{g \in G/\ gx = x\}$ como el **estabilizador** de x y lo anotamos por $Stab(x)$. El conjunto $Stab(x)$ es un subgrupo de G. De hecho, $1x = x$ por lo tanto $1 \in Stab(x)$, además si $g, g' \in Stab(x)$, entonces

$$(gg')x = g(g'x) = gx = x,$$

Por lo tanto $gg' \in Stab(x)$. Por último si $g \in Stab(x)$ entonces $gx = x$, por lo tanto

$$g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = x,$$

entonces $g^{-1} \in G$, o sea, $Stab(x)$ es efectivamente un subgrupo de G.

Proposición 2.3.1 *La órbita de x tiene tantos elementos como clases laterales de $Stab(x)$ en G.*

Demostración:

Consideremos G un grupo actuando en el conjunto X, y consideremos $x \in X$. Denotemos por Y al conjunto de todas las clases laterales izquierdas de $stab(x)$ en G, (recordemos que $|Y| = [G : stab(x)]$) y por $H = stab(x)$. Ahora definamos

$$\mu : orb(x) \to Y, \;\; \mu(gx) = gH$$

Primero que todo notamos que μ está bien definida, pues si $gx = g'x$, entonces $g'^{-1}gx = 1x = x$, es decir $g'^{-1}g \in H = Stab(x)$, que es equivalente a decir que $gH = gH$. Además notamos que por la definición de μ, ésta es epiyectiva.

Ahora bien, si $\mu(gx) = \mu(g'x)$ tenemos que $gH = g'H$, es decir, existe $h \in H = stab(x)$ tal que $g' = gh$ entonces

$$g'x = (gh)x = g(hx) = gx.$$

Es decir, hemos demostrado que si $\mu(gx) = \mu(g'x)$, entonces $g'x = gx$, por lo tanto μ es inyectiva. Por lo tanto μ es biyectiva o equivalentemente

$$|Orb(x)| = [G : stab(x)] \;\; \blacksquare$$

Corolario 2.3.1 *Si G es finito la órbita de x es finita y*

$$|Orb(x)| = \frac{|G|}{|Stab(x)|}$$

Sea G un grupo y hagamos actuar G en si mismo por conjugación, es decir $(g, g') \to gg'g^{-1}$, al estabilizador de g' bajo esta acción particular se le llama el centralizador de g', y lo anotamos por $C_G(g')$ o simplemente $C(g)$ y es el conjunto $C_G(g') = \{g \in G/ \; gg' = g'g\}$. Notamos también que la órbita de g' tiene un solo elemento si y solo si $g' \in Z$.

Como G es la unión disjunta de las órbitas y si suponemos que G es finito se tiene que

$$|G| = z + \sum_{g'} |G : C(g')|$$

donde $|Z| = z$. A la de arriba se le llama la *ecuación de clases* o *fórmula de clases.*

Proposición 2.3.2 *Todo grupo cuyo orden es una potencia de un primo, tiene un centro no trivial.*

Demostración:

Sea G de orden p^n, con n número entero positivo y supongamos que $|Z(G)| = 1$, se tiene que para cualquier $x \neq 1$ $C(x) \neq G$, luego $|G : C(x)|$ no es 1, de hecho , es una potencia positiva de p, luego por la fórmula de clases se tiene que $|G| = 1 + kp$ para cierto $k \in \mathbb{N}$, pero p divide a $|G|$, lo cual es una contradicción. Luego $|Z(G)| > 1$. ■

Proposición 2.3.3 *Si G/Z es cíclico, entonces G es abeliano.*

Demostración:

Sea $G/Z =< gH >$, por lo tanto cualquier elemento de G se puede escribir en la forma $g^k z$ con $g \in G$ fijo, $k \in \mathbb{Z}$ y $z \in Z$, luego si $x = g^k z$ y $y = g^l z'$ se tiene que

$$xy = g^k z g^l z' = z g^k g^l z' = z g^l g^k z' = z g^l z' g^k = g^l z' g^k z = yx \quad \square$$

Corolario 2.3.2 *Si p es primo entonces todo grupo de orden p^2 es abeliano.*

Demostración:[**Ejercicio**]

Ahora bien consideremos un grupo G y $\mathcal{S}$ el conjunto de todos los subgrupos de G. Hagamos actuar G en $\mathcal{S}$, vía conjugación, esto es $(g, H) \to gHg^{-1}$. Ésta es efectivamente una acción, pues gHg^{-1} es un grupo ya que $1 = g1g^{-1} \in gHg^{-1}$, además $(ghg^{-1})(gh'g^{-1}) = ghh'g^{-1} \in gHg^{-1}$, y por último $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$. También se tiene que $1H1^{-1} = H$ y además $g(g'Hg^{-1}1)g^{-1} = (gg')H(gg')^{-1}$. Al estabilizador de H bajo esta acción particular se le llama el normalizador de H en G y se anota $N_G(H)$, o simplemente $N(H)$ y es el subgrupo más grande en G en el cual H es normal, a saber

$$N_G(H) == N(H) = \{g \in G/\ gHg^{-1} = H\}.$$

Observación 2.3.2 *Si H es un subgrupo de G y $g \in G$ al grupo gHg^{-1} se le llama un conjugado de H. Consideremos la función $\omega : H \to gHg^{-1}$ definida por $\omega(h) = ghg^{-1}$. Por definición ω es epiyectiva. Además si $\omega(h) = \omega(h')$, es decir, $ghg^{-1} = gh'g^{-1}$ entonces $h = h'$, es decir ω es inyectiva. Por lo tanto existe una biyección entre H y cualquier conjugado de él. Es decir, $|H| = |gHg^{-1}|$ para caulquier $g \in G$.*

Observación 2.3.3 *Un subgrupo H de un grupo G es normal en G si y solo si $N(H) = G$.*

Sea G un grupo actuando en un conjunto X, denotemos por $Fix_X(G)$ al conjunto de elementos de X que son fijos por todos los elementos de G, esto es, son aquellos elementos cuya órbita está compuesta por un solo elemento, equivalentemente, son aquellos que su estabilizador es todo G.

Proposición 2.3.4 *Si G es un grupo finito cuyo orden es una potencia de un primo p, el cual actúa en un conjunto finito X, entonces*

$$|Fix_X(G)| \equiv |X| \pmod{p}.$$

Demostración:

Consideremos $\{X_1, X_2, X_3, \ldots, X_n\}$ el conjunto de todas las orbitas distintas. Escojamos x_i un representante de cada órbita. Sea $1 \leq k \leq n$ tal que $x_i \in Fix(G)$ si y solo si $i \leq k$. Entonces $|X_i| = 1$ para cada $i \leq k$.

Por otra parte, como X es la unión disjunta de las órbitas se tiene que:

$$|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{k} |X_i| + \sum_{i=k+1}^{n} |X_i| = |Fix(G)| + \sum_{i=k+1}^{n} [G : Stab(x_i)]$$

Pero si $i > k$ entonces $x_i \notin Fix(G)$, es decir $Stab(x)$ es un subgrupo propio de G, es decir $stab(x_i) \neq G$. Por lo tanto $[G : Stab(x_i)] \neq 1$. Además como G tiene orden una potencia de p, por teorema de Lagrange $Stab(x)$ tiene orden una potencia de p, por lo tanto

$$[G : Stab(x_i)] = \frac{|G|}{|stab(x)|}$$

es una potencia de p distinta de 1. Por lo tanto p divide a $[G : Stab(x_i)]$ para cada $i > k$ y por tanto p divide a $\sum_{i=k+1}^{n} [G : Stab(x_i)]$. Por lo tanto la igualdad

$$|X| = |Fix(G)| + \sum_{i=k+1}^{n} [G : Stab(x_i)]$$

nos dice que

$$|X| \equiv |Fix(G)| \bmod p \ \blacksquare$$

Corolario 2.3.3 *Supóngase que H es un subgrupo de orden una potencia de un primo p de un grupo finito G, y supongase además que p divide a $|G : H|$, entonces p divide a $|N(H) : H|$.*

Demostración:

Hagamos actuar H en el conjunto X de las clases laterales izquierdas de H en G, por multiplicación izquierda. Esto es

$$H \times X \to X$$

definida por $(h, gH) \longmapsto (hg)H$. Así, por el resultado anterior, se tiene que

$$|Fix(H)| \equiv [G : H] \bmod p$$

Pero

$$Fix(H) = \{gH / hgH = gH \ \forall h \in H\} = \{gH / g^{-1}hg \in H \ \forall h \in H\}$$

$$= \{gH / g \in N(H)\}$$

Es decir, $Fix(H)$ es el conjunto de las clases laterales de H en $N(H)$. Por lo tanto:

$$[N(H) : H] \equiv [G : H] \bmod p$$

Como $[N(H) : H] \geq 1$ y por hipótesis p divide a $[G : H]$ entonces, se tiene que p divide a $|N(H) : H|$. $\blacksquare$

Un corolario evidente es el siguiente

Corolario 2.3.4 *En un grupo de orden una potencia de un primo p, todo subgrupo propio es un subgrupo propio de su normalizador.*

Demostración:[**Ejercicio**]

Una consecuencia clara de lo anterior es el siguiente corolario:

Corolario 2.3.5 *Sea p un número primo. En un grupo G de orden p^m, todo subgrupo de orden p^{m-1} es normal en G.*

Demostración:[**Ejercicio**]

Teorema 2.3.4 (Teorema de Cauchy) *Si G es un grupo finito y p un primo que divide a $|G|$, entonces existe un elemento en G que tiene orden p.*

Demostración:

Consideremos $\mathcal{S}$ el conjunto de las $p-$uplas de elementos de G, para los cuales el producto de todos los elementos de la $p-$upla es 1. Esto es

$$\mathcal{S} = \{(a_1, a_2, a_3, \ldots, a_n) \in G^p / \ a_1a_2a_3 \cdots a_p = 1\}$$

Consideremos ahora el ciclo de largo p, definido por $\sigma = (12345 \cdots p-1) \in \Sigma_p$. Éste es un elemento de orden p en Σ_p. Ahora bien, hagamos actuar el grupo cíclico generado por σ en $\mathcal{S}$, del siguiente modo

$$(\sigma^i, (a_1, a_2, a_3, \ldots, a_p)) \longmapsto (a_{\sigma^i(1)}, a_{\sigma^i(2)}, a_{\sigma^i(3)}, \ldots, a_{\sigma^i(p)})$$

Recordemos que si $ab = 1$, entonces $ba = 1$, por lo tanto, si $\mathbf{a} = (a_1, a_2, a_3, \ldots, a_p) \in \mathcal{S}$, entonces $a_1a_2a_3 \cdots a_p = 1$, es decir $a_2a_3 \cdots a_p$ es el inverso de a_1 por lo tanto $a_2a_3 \cdots a_pa_1 = 1$, es decir

$$(\sigma, \mathbf{a}) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, \ldots, a_{\sigma(p)}) \in \mathcal{S}$$

Inductivamente se meustra que $(\sigma^i, \mathbf{a}) \in \mathcal{S}$, además $(1, \mathbf{a}) = \mathbf{a}$ y

$$(\sigma^i\sigma^j, \mathbf{a}) = (\sigma^{i+j}, \mathbf{a}) = (\sigma^i, (\sigma^j, \mathbf{a}))$$

Por lo tanto, la función de arriba es efectivamente una acción de $< \sigma >$ en $\mathcal{S}$. Por la Proposición (2.3.4), se tiene que

$$|Fix(< \sigma >)| \equiv |\mathcal{S}| \bmod p$$

Pero notemos que para escojer $(a_1, a_2, a_3, \ldots, a_p) \in \mathcal{S}$ los primeros $p-1$ elementos, son cualesquiera de G y $a_p = (\prod_{i=1}^{p-1} a_i)^{-1}$, por lo tanto $|\mathcal{S}| = |G|^{p-1}$, pero como p divide a $|G|$ se tiene que p divide a $|\mathcal{S}|$, es decir

$$|\mathcal{S}| \equiv 0 \bmod p$$

Es decir,

$$|Fix(< \sigma >)| \equiv 0 \bmod p$$

Pero

$$Fix(< \sigma >) = \{\mathbf{a} \in \mathcal{S} / \ a_1 = a_2 = a_3 = \cdots = a_p\}$$

Como $\mathbf{1} = (1, 1, 1, \ldots, 1) \in Fix(< \sigma >)$ y como $|Fix(< \sigma >)| \equiv 0 \bmod p$ se tiene que p divide a $|Fix(< \sigma >)|$, por lo tanto hay otro un elemento en $Fix(< \sigma >)$ distinto de $\mathbf{1}$. Sea $x \in G$, $x \neq 1$ y $(x, x, x, x, \ldots, x) \in Fix(< \sigma >)$, es decir

$$\prod_{k=1}^{p} x = 1 \Leftrightarrow x^p = 1$$

Como p es primo, y $x \neq 1$, entonces p es el orden de x ■

Observación 2.3.4 *Sea p un número primo. Un grupo en el cual todo elemento tiene orden una potencia de p, se llama un $p-$* **grupo.** *El Teorema de Cauchy, permite asegurar que todo $p-$grupo finito tiene orden una potencia de p.*

Ejemplo 2.3.5 *Si G tiene orden 6, entonces hay elementos de orden 2 y elementos de orden 3 en G. Sean $x, y \in G$ de orden 2 y de orden 3, respectivamente. Notemos que $xy \neq 1$, pues si $xy = 1$ entonces $x^{-1} = y = x$, pero un elemento no puede tener a la vez orden 2 y orden 3. Si G es abeliano, entonces $(xy)^2 = x^2y^2 = y^2 \neq 1$ del mismo modo $(xy)^3 = x^3y^3 = x^3 \neq 1$, por lo tanto xy tiene orden 6. Por lo tanto G es el grupo cíclico de orden 6. Es decir, existe un único grupo abeliano de orden 6, salvo isomorfismos.*

Si G no es abeliano, podemos afirmar que x y y no conmutan **(¿Por qué?)**. *Además como $< y >$ es de índice 2 en G, podemos afirmar que $< y >$ es normal en G. Por lo tanto*

$$xyx^{-1} = xyx \in < y >$$

Si $xyx = 1$, *entonces* $xy = x$ *y* $y = 1$, *lo cual no puede ser.*

Si $xyx = y$, *entonces* $xy = yx$, *pero como* x *y* y *no conmutan, esto no puede ser.*

Entonces necesariamente $xyx = y^2$ *o equivalentemente* $xy = y^2x$ *o equivalentemente* $xy = y^{-1}x^{-1}$, *es decir* $(xy)^{-1} = xy$. *También podemos decir que* $yx = xy^2$ *que es lo mismo que decir que* $yx = x^{-1}y^{-1}$, *o sea,* $(yx)^{-1} = x^{-1}y^{-1}$. *Entonces podemos afirmar que* $xy \neq yx$ *y además ambos elementos son de orden* 2. *Es decir,* $xyxy = yxyx = 1$. *Además ambos* xy *y* yx *son distinto de* x, *pues* y *no es* 1.

Así tenemos que $G = \{1, x, y, y^2, xy, yx\}$. *Además notamos que como* $xyx = y^2$, *entonces* $xy^2 = yx$, y *como* $xy = y^2x$, *entonces* $yxy = x$ *y por lo mismo* $y^2xy = yx$ *y también* $yxy^2 = xy$. *Por lo tanto, la tabla de multiplicación de* G *es:*

	1	x	y	y^2	xy	yx
1	1	x	y	y^2	xy	yx
x	x	1	yx	xy	y^2	y
y	y	xy	y^2	1	yx	x
y^2	y^2	yx	1	y	x	xy
xy	xy	y	x	yx	1	y^2
yx	yx	y^2	xy	x	y	1

Por lo tanto existe un único grupo de orden 6 *no abeliano, salvo isomorfismo.*

Es decir, salvo isomorfismos $\mathbb{Z}_3$ *y* Σ_3 *son los únicos grupos con* 6 *elementos.*

En el caso particular de Σ_3 *tenemos que* $x = (12)$ *es de orden* 2 *y* $y = (123)$ *es de orden* 3. *Además* $xy = (12)(123) = (23)$ *y* $yx = (123)(12) = (13)$. *Es un ejercicio para el estudiante verificar que la tabla de multiplicación de* Σ_3 *es idéntica a la tabla de arriba.*

Teorema 2.3.5 (Teorema de Sylow) *Sea* G *un grupo finito de orden* $p^m r$, *donde* p *es primo que no divide a* r, *entonces:*

i) Para cada $1 \leq k \leq m$ *existe un subgrupo de* G *de orden* p^k. *Cada subgrupo de orden* p^i $(0 \leq i < m)$ *es normal en algún subgrupo de orden* p^{i+1}.

ii) Todos los subgrupos de orden p^m son conjugados entre si. Es decir, si P y Q son subgrupos de orden p^m, entonces existe $x \in G$ tal que $P = xQx^{-1}$

iii) Si n denota la cantidad de subgrupos de orden p^m, entonces $n = |G : N(H)|$, donde H es cualquier subgrupo de orden p^m, además n es congruente a 1 módulo p y además divide a r.

Demostración:

Por Teorema de Cauchy existe un elemento de orden p, sea g uno de esos elementos entonces $< g >$ es un subgrupo de orden p. Supongamos que H es un subgrupo de orden p^i con $1 \leq i < m$, entonces p divide a $[G : H]$ por Corolario (2.3.3) se tiene que p divide a $[N(H) : H]$ como H es normal en $N(H)$ se tiene que N/H es un grupo cuyo orden es divisible por p. Por T. de Cauchy, existe un subgrupo de orden p en $N(H)/H$. Sea $\mathcal{K}$ uno de esos grupos, por lo tanto existe subgrupo K de $N(H)$, tal que $H \trianglelefteq K \leq N(H)$ tal que $\mathcal{K} = K/H$, por lo tanto $[K : H] = p$, por lo tanto $|K| = p^{i+1}$. Por lo tanto inductivamente tenemos la parte (i).

Si P es un subgrupo de G de orden p^m, entonces xPx^{-1} es un subgrupo de orden p^m (por Observación (2.3.2)). Sea Q un $p-$ subgrupo de G y sea X el conjunto de todas las clases laterales de P en G. Hagamos actuar Q en X por multiplicación izquierda, esto es $(q, gP) \longmapsto (qg)P$ por Proposición (2.3.4) se tiene que

$$|Fix(Q)| \equiv |X| \pmod{p}$$

Como $|X| = [G : P]$ entonces p no divide a $|X|$, es decir $|X|$ no es congruente a cero módulo p. Por lo tanto $Fix(Q) \not\equiv 0 \pmod{p}$, es decir existe $yP \in Fix(Q)$, pero

$$Fix(Q) = \{gP \in X / qgP = gP,\ \forall q \in Q\} = \{gP \in X / g^{-1}qgP = P,\ \forall q \in Q\}$$

$$= \{gP \in X / g^{-1}qg \in P,\ \forall q \in Q\} = \{gP \in X / g^{-1}Qg \subseteq P\}$$

Es decir, existe yP en X tal que $y^{-1}Qy \subseteq P$, tomando $x = y^{-1}$ se tiene que $xQx^{-1} \leq P$. En particular si Q tiene orden p^m y como $|P| = p^m$, entonces $xQx^{-1} = P$. Lo que demuestra (ii).

Por la parte (ii) la cantidad de subgrupos de orden p^m en G corresponde al conjunto de conjugados de P, cierto P de orden p^m. Sea $\mathcal{S}$ la familia de subgrupos de G, y consideremos la acción de G en $\mathcal{S}$, por conjugación. Entonces la órbita de P, es el conjunto de subgrupos conjugados de P y además $orb(P) = [G : Stab(P)]$, pero $Stab(P) = N(P)$, por lo tanto si n denota la cantidad de subgrupos de orden p^m en G se tiene que

$$n = [G : N(P)].$$

Además

$$p^m r = [G : N(P)][N(P) : P]|P|$$
$$r = n[N(P) : P]$$

Entonces n divide a r.

Ahora consideremos $\mathcal{P}$ la familia de subgrupos de orden p^m en G y hagamos actuar P en $\mathcal{P}$ por conjugación $(p, Q) \longmapsto pQp^{-1}$, por la Proposición (2.3.4) se tiene que

$$|Fix(P)| \equiv n \pmod{p}$$

Pero $Q \in Fix(P)$ si y solo si $pQp^{-1} = Q$ para todo $p \in P$, es decir $P \subseteq N(Q)$, pero Q es un subconjunto de $N(Q)$ y además $Q \trianglelefteq N(Q)$ por lo tanto $xQx^{-1} = Q$ para cada $x \in N(Q)$, entonces Q es el único subgrupo de orden p^m en $N(Q)$, entonces $Q = P$. Es decir, $Fix(P) = \{P\}$, es decir $|Fix(P)| = 1$. Por lo tanto $n \equiv 1 \pmod{p}$, que termina por demostar (iii) y el T. de Sylow.■

A los subgrupos de orden p^m le llamamos $p-$subgrupos de Sylow. Notemos que la parte (ii) del Teorema dice, que todos los $p-$ subgrupos de Sylow son conjugados. Además la demostración de la parte (iii) dice que el único $p-$ subgrupo de Sylow en $N(P)$ es P.

Un resultado evidente es el siguiente

Corolario 2.3.6 *Un $p-$subgrupo de Sylow es normal si y solamente si es el único $p-$subgrupo de Sylow.*

Demostración:

$$1 = |G : N(H)| \iff N(H) = G \iff H \trianglelefteq G \ \blacksquare$$

Otro resultado evidente es el siguiente

Corolario 2.3.7 *Si P es un $p-$subgrupo de Sylow, entonces $N(N(P)) = N(P)$.*

Demostración:

Es claro que $N(P) \subseteq N(N(P))$, luego basta probar la contención en el otro sentido.

Sea $x \in N(N(P))$, entonces $xN(P)x^{-1} = N(P)$, pero como $P \leq N(P)$, se tiene que $xPx^{-1} \leq xN(P)x^{-1} = N(P)$, luego xPx^{-1} es un $p-$subgrupo de Sylow en $N(P)$, pero como P es normal en $N(P)$ se tiene que P es el único $p-$subgrupo de Sylow en $N(P)$, luego $xPx^{-1} = P$, de donde resulta que $x \in N(P)$, entonces $N(N(P)) \subset N(P)$ ■