MONOGRAFÍAS MATEMÁTICAS
UTFSM

ESTRUCTURAS ALGEBRAICAS
GRUPOS Y ANILLOS

$\cdot$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Departamento de Matemática
Universidad Técnica Federico Santa María

Rubén A. Hidalgo

ESTRUCTURAS ALGEBRAICAS
GRUPOS Y ANILLOS

PRIMERA EDICIÓN 2006

Rubén A. Hidalgo
Departamento de Matemática, Universidad Técnica Federico Santa María, Valparaíso, Chile.
E-mail : ruben.hidalgo@usm.cl
Url : http://docencia.mat.utfsm.cl/~rhidalgo

Este libro fué parcialmente patrocinado por los proyectos Fondecyt 1030252 y UTFSM 12.05.21.

ESTRUCTURAS ALGEBRAICAS
GRUPOS Y ANILLOS

PRIMERA EDICIÓN 2006

Rubén A. Hidalgo

A Betty, Cata y Pucky

INTRODUCCIÓN

El propósito de estas notas preliminares es presentar desde un punto básico (en lo posible) el concepto de grupos y anillos que puedan ser utilizados por estudiantes de Licenciatura en Matemáticas e Ingeniería Civil Matemática de nuestro Departamento de Matemática de la UTFSM.

Muchos de los fenómenos que encontramos en la naturaleza tienen ciertas simetrías con las cuales podemos sacar conclusiones que nos permitan entender tal situación de una manera simple. Muchos casos corresponden a problemas de la física y biología. Por ejemplo en física, conceptos como momentos angulares, tensores, etc., aparecen como propiedades de la teoría de grupos. En biología podemos entender moléculas y cristales por sus grupos de simetrías.

Muchos temas se han propuesto como ejercicios para que el estudiante pueda poner en práctica los conceptos ya estudiados. Por supuesto, esto podría tener la desventaja de producir una idea de aislamiento de los temarios tratados, lo cual no es nuestro propósito.

Es claro que en esta version priliminar existen muchos errores tipográficos y de temarios. Esperamos que durante el transcurso del curso los estudiantes puedan hacer las correcciones al escrito y así poder tener en le futuro unas notas mejoradas, las cuales deberán crecer con el tiempo.

Mis primeros agradecimientos van dirigidos a Betty, Cata y Pucky, a quienes quite tiempo de dedicación para escribir esta monografía, por su comprensión durante ese tiempo. Quiero también agradecer a todos aquellos quienes leyeron parte de estas notas y me indicaron algunos errores.

Valparaíso, Chile 2003 Rubén A. Hidalgo

TABLA DE MATERIAS

PARTE I

TEORÍA BÁSICA DE GRUPOS

En la naturaleza aparecen en diversas formas la idea de simetría, como es el caso de cristales, moléculas, movimiento de electrones por un campo simétrico, etc. Todos esos fenómenos tienen un concepto común el cual es la noción de un grupo.

CAPÍTULO 1

GRUPOS : VISIÓN CLÁSICA

En esta parte introduciremos el concepto de grupos desde un punto de vista clásico en una primera etapa y luego miraremos algunos ejemplos.

Definición 1.0.1. — Consideremos primero algún conjunto no vacío X (por ejemplo, representando una molécula, cristales, etc). Una *permutación* de X será por definición una función biyectiva $f : X \to X$. Denotemos por $Perm(X)$ al conjunto de las permutaciones de X.

Observemos que todo conjunto X posee la permutación trivial dada por la función identidad I_X. También, dada una permutación $f : X \to X$, siempre tenemos la permutación inversa $f^{-1} : X \to X$.

Ejercicio 1. — *Verificar que X es un conjunto finito sí y sólo si $Perm(X)$ es finito. En el caso que X es un conjunto finito de cardinalidad n, calcular la cardinalidad de $Perm(X)$.*

Dadas dos permutaciones $f, g \in Perm(X)$ del conjunto X, tenemos que al componerlas obtenemos nuevamente una permutación $g \circ f \in Perm(X)$. Esto como consecuencia del hecho que la composición de dos biyecciones es de nuevo una biyección. Así, tenemos en $Perm(X)$ una operación (binaria) dada por la composición, que satisface las siguientes propiedades :

(1) La operación de composición en $Perm(X)$ es *asociativa*, es decir,

$$f \circ (g \circ h) = (f \circ g) \circ h,$$

para todos $f, g, h \in Perm(X)$.

(2) La función identidad I_X es un *elemento neutro* para la composición, es decir,

$$f \circ I_X = f = I_X \circ f$$

para todo $f \in Perm(X)$.

(3) Toda permutación $f \in Perm(X)$ tiene un *elemento inverso* $f^{-1} \in Perm(X)$.

Definición 1.0.2. — Decimos que el par $(Perm(X), \circ)$ es el *grupo de permutaciones* del conjunto X.

Desde ahora en adelante usaremos indistintamente la notación $Perm(X)$ para denotar tanto al conjunto de permutaciones de X como al grupo de permutaciones de X ya que esto no produce confusión alguna.

Definición 1.0.3. — La cardinalidad de $Perm(X)$ es llamado el *orden* del grupo de permutaciones $Perm(X)$.

Notación : Sea $k \in \{0, 1, 2, 3, ...\}$. Si $k > 0$, entonces usaremos la notación f^k para denotar la composición de f consigo misma k veces. La notación f^{-k} indicará que hacemos la composición de f^{-1} consigo misma k veces. Por último, f^0 indicará el neutro I_X.

Ejemplo 1.0.4. — Consideremos $X = \{a, b, c\}$ un conjunto de tres elementos. Entonces $Perm(X) = \{I_X, A, A^2, B, A \circ B, A^2 \circ B\}$, donde

$$A : (a, b, c) = (b, c, a) \text{ y } B(a, b, c) = (b, a, c)$$

Es decir, $Perm(X)$ es un grupo de permutaciones de orden 6.

Ejercicio 2. — *Sea X un conjunto de $n > 0$ elementos. Determinar los elementos de $Perm(X)$. Verificar que el orden de $Perm(X)$ es $n!$.*

Hay veces en que no estaremos interesados en todas las permutaciones de un conjunto, pero sólo de algunas de ellas, por ejemplo, de aquellas que preservan cierta propiedad.

Definición 1.0.5. — Supongamos que tenemos un conjunto $X \neq \emptyset$ y un subconjunto $G \subset Perm(X)$ de algunas de las permutaciones de X. Si :
(1) Para todos. El conjunto G consiste $f, g \in G$ vale que $f \circ g \in G$;
(2) Para todo $f \in G$ vale que $f^{-1} \in G$,
entonces diremos que G es un *subgrupo de permutaciones* de X y esto lo denotaremos con el símbolo $G < Perm(X)$. La cardinalidad de G es llamado el *orden* del subgrupo de permutaciones G.

Observación 1.0.6. — Observar que las condiciones (1) y (2) obligan a tener $I_X \in G$ y que G satisface las mismas propiedades antes verificadas para $Perm(X)$.

Ejercicio 3. — *Calcular todos los subgrupos del grupo $Perm(X)$ del ejemplo 1.0.4.*

Ejemplo 1.0.7. — Sea X un conjunto no vacío y $p \in X$ un punto que hemos fijamos. Consideremos el conjunto G formado por las permutaciones de X que tienen la propiedad de dejar al punto p fijo. Entonces claramente valen las dos propiedades anteriores y vemos que G es un subgrupo de permutaciones de X. Por ejemplo, en el caso $X = \{a, b, c\}$ y $p = a$, entonces $G = \{I_X, A \circ B\}$.

Ejemplo 1.0.8. — Generalicemos un poco más el ejemplo anterior. Sea X un conjunto no vacío y $A \subset X$ un subconjunto que hemos fijamos. Consideremos el conjunto G formado por las permutaciones de X que tienen la propiedad de dejar invariante al subconjunto A, es decir, para cada $g \in G$ y cada $a \in A$ vale que $g(a) \in A$. Entonces G es un subgrupo de permutaciones de X. Observemos que cada $g \in G$, al restringirla a A, produce una permutación $\phi(g)$ de A. Luego tenemos inducida una función $\phi : G \to Perm(A)$, definida por tal restricción. Puede ocurrir que tengamos $g_1, g_2 \in G$ tales que $g_1 \neq g_2$ pero que sus restricciones coincidan en A ; luego, ϕ no es necesariamente una función inyectiva. Por otro lado, cada permutación $h \in Perm(A)$ puede ser extendida a una permutación $\psi(h) \in Perm(X)$ por extensión como la función identidad en $X - A$. Tenemos entonces una función, ahora inyectiva, $\psi : Perm(A) \to Perm(X)$. Observemos que $\psi(Perm(A))$ es un subgrupo de permutaciones de X (Verificar).

Ejemplo 1.0.9. — Si $X = V$ es un espacio vectorial sobre un cuerpo K, entonces el grupo $Perm(V)$ contiene como subgrupo a

$$GL(V) = \{L : V \to V : L \text{ es un isomorfismo de } V \}$$

es decir, los isomorfismos lineales de V es un subgrupo de permutaciones de V (las permutaciones que preservan la estructura de espacio vectorial).
Por otro lado, si $Q \subset V$, entonces

$$G = \{L \in GL(V) : L(Q) = Q\},$$

resulta también ser un subgrupo de $Perm(V)$.
Tenemos las contenciones

$$G \subset GL(V) \subset Perm(V)$$

Supongamos por ejemplo que Q es alguna figura geométrica dentro de V, que podría estar representando una molécula, una colección de electrones o un cristal. Entonces G estaría formado por aquellos isomorfismos que preservan tal configuración. Veamos esto de una manera un poco más concreta. Supongamos $V = \mathbb{R}^2$, $K = \mathbb{R}$ y Q un polígono regular de $n \geq 3$ lados con centro en el orígen $(0, 0)$ y uno de sus vértices localizado en $(1, 0)$. Entonces todo elemento de G debe obligatoriamente ser una rotación (de determinante positivo o negativo). Más aún, si R es la rotación positiva en ángulo π/n, S es la reflexión $S(x, y) = (x, -y)$ y $T = R \circ S \circ R^{-1}$, entonces se puede verificar que todo elemento de G se obtiene con todas las posibles composiciones entre T y S y que este tiene orden $2n$ (mirar la figura de la tapa para $n = 6$).

Ahora, supongamos que en el espacio vectorial real V tenemos un producto interior Euclidiano $\langle , \rangle$. Por ejemplo, en $\mathbb{R}^n$ podemos usar el producto punto

$$\langle (x_1, ..., x_n), (y_1, ..., y_n) \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

Denotemos por $O_{\langle , \rangle}$ al conjunto de todas los isomorfismos $L \in GL(V)$ tales que preservan tal producto, es decir,

$$\langle L(x), L(y) \rangle = \langle x, y \rangle, \quad \text{para todos } x, y \in V$$

Si V es de dimensión finita, digamos n, entonces podemos considerar una base $\beta = \{v_1, ..., v_n\}$ de V y formar la matriz simétrica $A \in GL(n, \mathbb{R})$ cuyo coeficiente $a_{ij} =< v_i, v_j >=< v_j, v_i >$. Entonces escribiendo $x = x_1 v_1 + \cdots + x_n v_n$, $y = y_1 v_1 + \cdots + y_n v_n$, vale que

$$< x, y >= (x_1 \cdots x_n) A \, {}^t(y_1 \cdots y_n)$$

De esta manera si $M \in M(n, \mathbb{R})$ es la matriz que representa a la transformación lineal $L : V \to V$ en la base β, entonces tenemos que $L \in O_{\langle , \rangle}$ sí y sólo si

$$M A \, {}^t M = A$$

Llamamos a $O_{\langle , \rangle}$ el *grupo de isometrías* del espacio Euclidiano $(V, \langle , \rangle)$. Se tiene que $O_{\langle , \rangle}$ es un subgrupo de permutaciones de $Perm(V)$. Este tipo de permutaciones (llamados isometrías de $(V, \langle , \rangle)$) son los que interesan para el estudio de algunos fenómenos de la naturaleza.

Ejercicio 4. — *Verificar y completar los detalles del ejercicio anterior.*

Ejercicio 5. — *Para cada entero $n \geq 3$ considere el polígono regular P de n lados centrado en el orígen en $\mathbb{R}^2$. Use el producto punto usual*

$$\langle (a, b), (c, d) \rangle = ac + bd$$

y determine las isometrías de P.

CAPÍTULO 2

GRUPOS : VISIÓN MODERNA

La pregunta natural es si existe en el fondo alguna diferencia entre un grupo de simetrías $Perm(X)$ y alguno de sus subgrupos. La verdad es que, excepto por la propiedad que uno es subconjunto del otro, no hay diferencia conceptual entre ellos. Es por esta razón que es preferible usar la siguiente definición más moderna de grupos y subgrupos.

Definición 2.0.10. — Un conjunto $G \neq \emptyset$ junto a una función

$$* : G \times G \to G$$

llamada una operación binaria en G es llamado un grupo si valen las siguientes propiedades :

(1) La operación binaria $*$ es *asociativa*, es decir,

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3,$$

para todos $g_1, g_2, g_3 \in G$.

(2) Existe un *elemento neutro* para la operación binaria $*$, denotado por I_G, que satisface :

$$g * I_G = g = I_G * g$$

para todo $g \in G$.

(3) Todo elemento $g \in G$ tiene un *elemento inverso* respecto a la operación binaria $*$, es decir que existe un elemento $g^{-1} \in G$ tal que $g * g^{-1} = I_G = g^{-1} * g$.

Ejercicio 6. — *Verificar que el elemento neutro y los inversos son únicos en un grupo.*

Dado un grupo $(G, *)$ y un subconjunto $H \subset G$, que resulta ser un grupo con la misma operación $*$, es llamado un *subgrupo* de G.

Ejercicio 7. — *Sea $(G, *)$ un grupo y $H \neq \emptyset$ un subconjunto de G. Verificar que H es un subgrupo de G sí y sólo si :*

(1) Para cada $h \in H$ se tiene que $h^{-1} \in H$; y

(2) Si $h_1, h_2 \in G$, entonces $h_1 * h_2 \in H$.
Concluir que $I_H = I_G$ y que todo inverso en H es inverso en G.

Definición 2.0.11. — Dado cualquier grupo $(G, *)$ diremos que la cardinalidad de G es el *orden de* G y lo denotaremos por $|G|$. De la misma manera, por cada elemento $g \in G - \{I_G\}$ llamaremos el orden de g, denotado por $o(g)$, al entero positivo k más pequeño tal que $g^k = I_G$ en caso de existir, o $o(g) = \infty$ en caso contrario. Diremos que el orden del neutro es 1.

Es claro que todo grupo de permutaciones y todo subgrupo de permutaciones es un grupo (donde $* = \circ$) en la versión moderna. Antes de verificar que todo grupo, en la notación moderna, es un subgrupo de permutaciones de algún conjunto, necesitaremos un concepto que permita comparar grupos, estos son los homomorfismos.

Ejercicio 8. — *Calcular todos los subgrupos aditivos de $\mathbb{Z}$.*

Ejemplo 2.0.12. — Consideremos el grupo $\mathbb{R}$ con la operación binaria de la suma usual de número reales. Recordemos del curso de análisis 1 que $\mathbb{R}$ es un espacio normado, la norma siendo el valor absoluto. Un subgrupo H de $\mathbb{R}$ tiene dos posibilidades : ser un subconjunto discreto (es decir, no tiene puntos de acumulación) o no serlo. En caso que H no sea discreto entonces existe una sucesión $x_n \in H$ que converge hacia un número real p. Entonces $y_n = x_{n+1} - x_n \in H$ nos dá una sucesión que converge hacia $0 \in H$. Escojamos cualquier intervalo abierto $(a, b) \subset \mathbb{R}$. Entonces podemos escoger y_n de manera que $z = |y_n| < (b - a)$. Es claro que $z \in H$ y que $kz = z + \cdots + z \in H$ para todo $k \in \mathbb{Z}$. Como existe $k_0 \in \mathbb{Z}$ tal que $k_0 z \in (a, b)$, tenemos que si H no es discreto, entonces debe ser un subconjunto denso de $\mathbb{R}$. Ahora, si H es discreto, entonces lo anterior también nos dice que $w = \text{mínimo}\{h \in H : h > 0\} > 0$. Ahora, consideremos $w\mathbb{Z} = \{kw : k \in \mathbb{Z}\}$. Se tiene que $w\mathbb{Z}$ es un subgrupo de $\mathbb{R}$ y también de H. Si $w\mathbb{Z} \neq H$, entonces es posible encontrar $k \in \mathbb{Z}$ y $h \in H$ tales que $(k-1)w < h < kw$. Pero en este caso, $0 < kw - h < h$. Como $kw - h \in H$, obtenemos una contradicción con la minimalidad de w. En consecuencia, el hemos obtenido lo siguiente :

Teorema 2.0.13. — *Todo subgrupo aditivo de $\mathbb{R}$ es o bién denso o de la forma $w\mathbb{Z}$ para cierto $w > 0$.*

Ejemplo 2.0.14. — Sea K un cuerpo (por ejemplo, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) y denotemos por $GL(n, K)$ al conjunto de las matrices de tamaño $n \times n$, con coeficientes en K, que son invertibles. Entonces, con la operación de jultiplicación de matrices, obtenemos que $GL(n, K)$ es un

grupo. Este grupo es un modelo del grupo $GL(V)$ donde V es un espacio vectorial sobre K y dimensión n. Definamos la relación de equivalencia

$$A \equiv B \quad \text{ sí y sólo si existe } \lambda \in K - \{0\} \text{ tal que } \quad B = \lambda A$$

Sea $PGL(n, K)$ el conjunto de las clases de equivalencia y denotemos por

$$\pi : GL(n, K) \to PGL(n, K)$$

la proyección natural que asocia a cada matriz $A \in GL(n, K)$ su clase de equivalencia $\pi(A) := [A] \in PGL(n, K)$. Si definimos la operación

$$[A] \cdot [B] := [AB]$$

la cual está bién definida, entonces obtenemos en $PGL(n, K)$ una estructura de grupo, cual es llamado el *grupo proyectivo lineal*.
Observemos que el *grupo especial lineal* $SL(n, K)$, formado de las matrices de $GL(n, K)$ de determinante 1, satisface que $\pi(SL(n, K)) = PSL(n, K)$ es un subgrupo de $PGL(n, K)$.

Ejercicio 9. —
(1) Verificar que $PSL(n, \mathbb{C}) = PGL(n, \mathbb{C})$.
(2) ¿Es verdad lo anterior con $\mathbb{C}$ *reemplazado por* $\mathbb{R}$ *?*

Ejemplo 2.0.15. — Un *grafo* $\mathcal{G}$ es una colección disjunta de objetos llamados "vértices" y objetos llamados "ejes" que conectan dos vértices (puede ocurrir que los dos vértices conectados por un eje sean el mismo). Un automorfismo del grafo $\mathcal{G}$ es una función bijectiva al nivel de vértices y al nivel de ejes, es decir, este envía vértices en vértices y envía ejes en ejes. Denotamos por $Aut(\mathcal{G})$ al conjunto de los automorfismos del grafo $\mathcal{G}$. Junto con la operación de composición de funciones obtenemos una estructura de grupo para $Aut(\mathcal{G})$.

Ejercicio 10. — *Completar los detalles del ejemplo anterior.*

Observación 2.0.16 **(Grupos Abelianos)**. — Antes de terminar con esta sección, observemos que hay ejemplos de grupos $(G, *)$ (como es el ejemplo del grupo aditivo $\mathbb{Z}$) que tienen la siguiente propiedad, los cuales llamaremos un *grupo Abeliano* :
(*) Propiedad *commutativa* : Para todo par de elementos $x, y \in G$ vale que $x * y = y * x$.

Ejemplo 2.0.17. — Es claro que no todo grupo puede ser Abeliano. Un ejemplo típico es el grupo $Perm(X)$ cuando la cardinalidad de X es al menos 3. Otro ejemplo es el siguiente. Sea $Gl(n, \mathbb{Z})$ el conjunto de las matrices cuadradas de tamaño $n \times n$ con coeficientes enteros e invertibles. Usando como la operación binaria el producto usual de matrices, tenemos que para $n \geq 2$ este da un grupo no Abeliano.

Ejercicio 11. — *Determinar que todos los subgrupos del grupo Abeliano $\mathbb{Z}$ son de la forma $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.*

La operación conjuntista dada por la intersección nos permite construir subgrupos de algún grupo a partir de otros.

Proposición 2.0.18. — *Sea $(G, *)$ un grupo y $\{H_j : j \in J\}$ una colección cualquiera de subgrupos de G. Entonces $\bigcap_{j\in J} H_j$ es de nuevo un subgrupo de G.*

Demonstración. — Supongamos que $x, y \in \bigcap_{j\in J} H_j$. Entonces $x, y \in H_j$, para cada $j \in J$. Como H_j es subgrupo, entonces $x * y, x^{-1} \in H_j$ y, como consecuencia, $x * y, x^{-1} \in \bigcap_{j\in J} H_j$. □

Ejercicio 12. — *Verificar que la unión de subgrupos no es necesariamente un subgrupo. Dar un ejemplo.*

Ejemplo 2.0.19. — Un ejemplo de un grupo es dado por las rotaciones Euclidianas en $\mathbb{R}^3$. Consideremos dos ángulos de rotación $\alpha, \beta \in \mathbb{R}$ y consideremos las rotaciones en $\mathbb{R}^3$ dadas por

$$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} \cos(\beta) & -\sin(\beta) & 0 \\ \sin(\beta) & \cos(\beta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

tenemos $A \circ B = B \circ A$, pero con las rotaciones

$$C = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad D = \begin{pmatrix} \cos(\beta) & 0 & -\sin(\beta) \\ 0 & 1 & 0 \\ \sin(\beta) & 0 & \cos(\beta) \end{pmatrix}$$

tenemos $C \circ D \neq D \circ C$.

Para analizar conjuntos finitos muy pequeños con alguna operación binaria dada, uno puede utilizar tablas de multiplicación para analizar si estamos en presencia de un grupo on no. Por ejemplo, consideremos el conjunto $G = \{e, a, b, c, d, f\}$ y definamos la operación binaria dada por la siguiente tabla :

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Lo que esta tabla nos dice, por ejemplo, que el coeficiente $(2,3)$, es decir, e es igual a $a*b$.

Ejercicio 13. — *Verificar que la tabla anterior dota a G de una estructura de grupo de orden 6 que no es Abeliano. Obtener todos los subgrupos.*

Ejemplo 2.0.20. — Consideremos un grupo $(G,*)$ de orden par. Entonces $G-\{I_G\}$ es un conjunto de cardinalidad impar. Consideremos la función

$$\tau : G \to G : x \mapsto x^{-1}$$

Observamos que τ es una bijección, es su propia inversa y que $\tau(I_G) = I_G$. Así, tenemos una bijección $\tau : G-\{I_G\} \to G-\{I_G\}$. Como τ es su propia función inversa, tenemos que para cada $x \in G-\{I_G\}$ vale que $\tau(\{x,x^{-1}\}) = \{x,x^{-1}\}$. Esto nos obliga a tener al menos un elemento $x \in G-\{I_G\}$ con $\tau(x) = x$, es decir, G tiene al menos un elemento de orden 2.

Ejemplo 2.0.21. — Supongamos que tenemos un grupo $(G,*)$ con la propiedad que todos sus elementos diferentes del neutro son de orden 2. Si $x,y \in G$, entonces $x*y*x^{-1}*y^{-1} = x*y*x*y = (x*y)^2 = I_G$, es decir, G es un grupo Abeliano.

Ejercicio 14. — *Sea $(G,*)$ un grupo y dos elementos $x,y \in G$ de ordenes $n > 1$ y $m > 1$ respectivamente. Supongamos que $x*y = y*x$, es decir que conmutan. Verificar que el orden de $x*y$ es el mínimo común múltiplo $M.C.M.(n,m)$ entre n y m.*

Ejercicio 15. — *Consideremos el grupo de las matrices cuadradas de tamaño 2×2 invertible reales, es decir $G = GL(2,\mathbb{R})$ con la operación binaria dada por multiplicación usual de matrices. Sean*

$$x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

Verificar que $o(x) = 4$, $o(y) = 3$ y $o(x*y) = \infty$. Comparar al ejercicio anterior.

Ejemplo 2.0.22. — Sea p un número primo y sea $G = \{1,2,3,...,p-1\}$. Considere la operación binaria $*$ de la siguiente manera : si $a,b \in G$ entonces $a*b$ denota el resto de dividir $ab \in \mathbb{Z}$ por p.

Tarea : Verificar que este es un grupo conmutativo de orden $p-1$ (Ind. Si $a \in G$ entonces $(a,p) = 1$, es decir, a no es divisible por p. Más adelante veremos que existen enteros n,m tales que $na+mp = 1$). Verificar que si p no fuese un número primo, entonces la operación $*$ definida no determina una estructura de grupo en G.

Al grupo construido lo denotaremos por $(\mathbb{Z}/p\mathbb{Z})^*$. Si n es un entero positivo tal que $(n,p)=1$, es decir, p no divide n. Entonces $n=ap+r$ cierto $r\in G$. Más adelante veremos que si G es un grupo finito de orden N y $x\in G$, entonces vale que $x^N=1$, donde $1\in G$ denota al elemento neutro. Luego $r^{p-1}=1$ en $(G,*)$, es decir, vale la igualdad $r^{p-1}=1+bp$ en $\mathbb{Z}$ para cierto entero b. Luego, en $\mathbb{Z}$ tenemos que :

$$n^p = nn^{p-1} = n(ap+r)^{p-1} = nr^{p-1} + pq, \text{ cierto entero } q$$

es decir

$$n^p = n(1+bp) + pq = n + p(nb+q)$$

De donde concluimos el siguiente

***Teorema 2.0.23* (*Pequeño teorema de Fermat*)**. — *Sean p un primo y n un entero cualquiera, entonces*

$$n^p \equiv n \ \textit{módulo } p$$

Ejercicio 16. — *Para cada número entero positivo q consideramos la función*

$$e(q) = \#\{k\in\{1,2,3,...,q-1\} : (q,k)=1\}$$

llamada la función de Euler. *Verificar que*
(i) si p es un número primo, $t>0$ un entero, entonces

$$e(p^t) = p^t\left(1-\frac{1}{p}\right)$$

(ii) Si q,r son enteros positivos y $(q,r)=1$, entonces $e(qr)=e(q)e(r)$.
(iii) Sea $G=\{\{k\in\{1,2,3,...,q-1\} : (q,k)=1\}$ y considere la operación binaria $*$ dada por : si $a,b\in G$, entonces $a*b$ denota el resto al dividir ab por q. Verificar que $(G,*)$ es un grupo abeliano de orden $e(q)$ (Ind. Más adelante veremos que si $(k,q)=1$, entonces existen enteros $n,m\in\mathbb{Z}$ de manera que $nq+mr=1$).

Podemos entonces concluir la siguiente generalización al teorema de Fermat.

***Teorema 2.0.24* (*Teorema de Euler*)**. — *Si $q,n\in\mathbb{Z}$, $q>0$, son tales que $(q,n)=1$, entonces*

$$n^{e(q)} \equiv 1 \ \textit{módulo } q$$

Ejemplo 2.0.25. — Consideremos un número primo p y formemos el grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Busquemos los elementos de orden 2, es decir $a\in\{1,2,...,p-1\}$ tal que $a*a=1$, es decir, a^2-1 sea divisible por p. Como $a^2-1=(a-1)(a+1)$ y $(a-1)<p$, debemos tener que $(a+1)$ debe ser divisible por p, dando como única solución $a=p-1$.

En particular, como todo otro elemento de $\{2, 3, ..., p-2\}$ tiene inverso diferente, tenemos que $1 * 2 * 3 * \cdots * (p-1) = (p-1)$, es decir,

$$(p-1)! \equiv -1 \text{ módulo } p$$

Ejercicio 17. — *Supongamos que $(G, *)$ es un grupo finito donde la ecuación $x^2 = I_G$ tiene como única solución a $x = I_G$. Calcular el valor en G del producto de todos los elementos de G.*

Ejercicio 18. — *Sea $(G, *)$ un grupo de orden par. Verificar que $\#\{x \in G : o(x) = 2\}$ es impar (Ind. Use la función biyectiva dada por inversión, es decir, $G \to G : x \mapsto x^{-1}$).*

Ejemplo 2.0.26 **(Grupo Fundamental)**. — Consideremos un espacio topológico (X, Υ) y escojamos un punto $p \in X$. Sea $A(p)$ el conjunto de todas las funciones continuas $\gamma : [0,1] \to X$ tal que $\gamma(0) = \gamma(1) = p$. Para $\gamma_1, \gamma_2 \in A(p)$, definamos la operación binaria $*$ dada por

$$\gamma_1 * \gamma_2 = \begin{cases} \gamma_1(2t), & 0 \leq t \leq \frac{1}{2} \\ \gamma_2(2t-1), & \frac{1}{2} \leq t \leq 1 \end{cases}$$

Desgraciadamente, esta operación binaria no es asociativa, es decir, en general tenemos que $\gamma_1 * (\gamma_2 * \gamma_3) \neq (\gamma_1 * \gamma_2) * \gamma_3$. Para arreglar esto, definimos una relación de equivalencia $\sim$ sobre $A(p)$ definida de la siguiente manera. Sean $\gamma_1, \gamma_2 \in A(p)$, entonces decimos que ellas son homotópicamente equivalentes relativo al punto p, es decir,

$$\gamma_1 \sim \gamma_2$$

si existe una función continua $F : [0,1] \times [0,1] \to X$ tal que
(i) $F(t,0) = \gamma_1(t)$, para todo $t \in [0,1]$;
(ii) $F(t,1) = \gamma_2$, para todo $t \in [0,1]$;
(iii) $F(0,s) = F(1,s) = p$, para todo $s \in [0,1]$.
Lo importante de esta relación de equivalencia es que si tenemos $\gamma_1, \gamma_2, \widetilde{\gamma}_1, \widetilde{\gamma}_2 \in A(p)$ tales que $\gamma_1 \sim \widetilde{\gamma}_1$ y $\gamma_2 \sim \widetilde{\gamma}_2$, entonces

$$\gamma_1 * \gamma_2 \sim \widetilde{\gamma}_1 * \widetilde{\gamma}_2$$

Denotemos por $[\gamma]$ la clase de equivalencia de $\gamma \in A(p)$ y por $\pi_1(X, p)$ al conjunto de las clases de equivalencia. Podemos hacer descender la operación $*$ hasta $\pi_1(X, p)$, es decir,

$$[\gamma_1] * [\gamma_2] := [\gamma_1 * \gamma_2]$$

Ahora la operación es asociativa. Si $e_p \in A(p)$ es el camino constante $e_p(t) = p$, entonces se tiene que $[e_p] * [\gamma] = [\gamma] = [\gamma] * [e_p]$, es decir, $[e_p]$ es un neutro para tal operación.
Dado cualquier camino $\gamma \in A(p)$, tenemos su camino de vuelta $\gamma^{-1}(t) := \gamma(1-t) \in A(p)$. En este caso, tenemos que $[\gamma] * [\gamma^{-1}] = [e_p] = [\gamma^{-1}] * [\gamma]$, es decir, $[\gamma^{-1}]$ es inverso de $[\gamma]$ para esta operación.

Hemos obtenido que $(\pi_(X, p), *)$ define un grupo, llamado *grupo fundamental* de X basado en el punto p.

Ejercicio 19. — *Completar los detalles del ejemplo anterior.*

CAPÍTULO 3

HOMOMORFISMOS DE GRUPOS Y AUTOMORFISMOS

Definición 3.0.27. — Sean $(G_1, *_1)$ y $(G_2, *_2)$ dos grupos y $\phi : G_1 \to G_2$ una función. Diremos que ϕ es un *homomorfismos de grupos* si vale que

$$\phi(x *_1 y) = \phi(x) *_2 \phi(y), \quad \text{para todos } x, y \in G_1$$

Observación 3.0.28. — Sea $\phi : (G_1, *_1) \to (G_2, *_2)$ un homomorfismo de grupos. Entonces para cada $x \in G_1$ tenemos que

$$\phi(x) = \phi(x *_1 I_{G_1}) = \phi(x) *_2 \phi(I_{G_1})$$

luego, vale que

$$\phi(I_{G_1}) = I_{G_2}$$

Definición 3.0.29. — En caso que un homomorfismo de grupos sea inyectivo, diremos que es un monomorfismo. Si este es sobreyectivo, entonces hablamos de un epimorfismo o homomorfismo sobreyectivo. Un *isomorfismo de grupos* es un homomorfismo biyectivo. En este caso diremos que los respectivos grupos son *grupos isomorfos*. la idea es que grupos isomorfos son el mismo desde el punto de vista algebraico. Cuando $G_1 = G_2 = G$, usaremos la palabra *automorfismo* de G para denotar a un isomorfismo $\phi : G \to G$.

Ejercicio 20. —

(i) Verificar que las funciones $\phi : G \to Perm(A)$ y $\psi : Perm(A) \to Perm(X)$ del ejemplo 1.0.8 son homomorfismos de grupos.

(ii) Deducir del ejemplo 2.0.12 que todo subgrupo aditivo no denso de $\mathbb{R}$ es isomorfo a $\mathbb{Z}$.

(iii) Sea $(G, *)$ un grupo, X un conjunto y $F : G \to X$ una función biyectiva. Verificar que es posible dotar de una operación binaria $\circ$ a X de manera que $(X, \circ)$ es un grupo

y $F : (G, *) \to (X, \circ)$ *es un isomorfismo de grupos. Ver además que tal operación binaria es única.*

(iv) Sean $(G_1, *_1)$ *y* $(G_2, *_2)$ *dos grupos y* $\phi : G_1 \to G_2$ *un homomorfismo de grupos. Verificar que :*

(iv.1)

$$Ker(\phi) = \phi^{-1}(I_{G_1}) = \{g \in G_1 : \phi(g) = I_{G_2}\}$$

es un subgrupo de G_1*, llamado el núcleo de* ϕ*.*

(iv.2)

$$Im(\phi) = \{h \in G_2 : \text{ existe } g \in G_1 \text{ tal que } \phi(g) = h\}$$

es un subgrupo de G_2*, llamado la imágen de* ϕ*.*

(iv.3) ϕ *es monomorfismo sí y sólo si* $Ker(\phi) = \{I_{G_1}\}$*. En este caso ver que* $\phi : G_1 \to Im(\phi)$ *es un isomorfismo.*

(iv.4) ϕ *es epimorfismo sí y sólo si* $Im(\phi) = G_2$*.*

(v) Verificar que la función logaritmo $Log : (\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \cdot)$ *es un isomorfismo. Determinar la inversa.*

(vi) Sea $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ *junto a la operación dada por la multiplicación usual de números complejos, denotada por* $\cdot$*. Verificar que tenemos un grupo Abeliano. Para cada número real* $a \in \mathbb{R}$ *defina la función*

$$F_a : (S^1, \cdot) \to (S^1, \cdot) : w = e^{i\theta} \mapsto w^a = e^{ia\theta}$$

Verificar que F_a *es un homomorfismo de grupos. Calcular* $Ker(F_a)$*.*

(vii) Sea $(G, *)$ *un grupo para el cual la función de inversión*

$$J : (G, *) \to (G, *) : x \mapsto x^{-1}$$

es un homomorfismo de grupos. Verificar que $(G, *)$ *es un grupo Abeliano.*

Ejemplo 3.0.30. — Sea $(G, *)$ un grupo finito y supongamos que tenemos un automorfismo involutivo sin puntos fijos no triviales, es decir, un automorfismo $T : (G, *) \to (G, *)$ de $(G, *)$ tal que $T \circ T = I$ y $T(x) = x$ sólo vale para $x = I_G$. Veamos que esto obliga a tener $(G, *)$ Abeliano. En efecto, primero consideremos el subconjunto de G siguiente

$$K = \{x^{-1} * T(x) : x \in G\} \subset G$$

La igualdad $x^{-1} * T(x) = y^{-1} * T(y)$ es equivalente a tener $T(y * x^{-1}) = y * x^{-1}$, la condición sobre los puntos fijos de T asegura $x = y$. En particular, $K = G$. De esta manera, podemos escribir cada elemento de G como $u = x^{-1} * T(x)$. Ahora, $T(u) = T(x^{-1} * T(x)) = T(x)^{-1} * x = u^{-1}$, es decir, T en la nueva representación es dada por inversión. El ejercicio anterior, parte (vii), asegura que $(G, *)$ es Abeliano.

Ejemplo 3.0.31. — Dado un grupo $(G, *)$ definamos la siguiente operación binaria

$$\overline{*} : G \times G \to G : (x, y) \mapsto x \,\overline{*}\, y := y * x$$

Sean $x, y, z \in G$. Entonces :

(i) $(x \overline{*} y) \overline{*} z = Z * (y * x) = (z * y) * x = x \overline{*} (y \overline{*} z)$, es decir, $\overline{*}$ es una operación asociativa.

(ii) $x \overline{*} I_G = I_G * x = x = x * I_G = I_G \overline{*} x$, es decir, tenemos un elemento neutro, el cual coincide con el elemento neutro para la operación binaria $*$.

(iii) $x \overline{*} x^{-1} = x^{-1} * x = I_G = x * x^{-1} = x^{-1} \overline{*} x$, es decir, cada elemento de G tiene un inverso respecto a la operación binaria $\overline{*}$ el cual es el mismo como para la operación binaria $*$.

Luego, $(G, \overline{*})$ resulta ser un grupo. Si consideramos la función

$$\tau : (G, *) \to (G, \overline{*}) : x \mapsto x^{-1}$$

entonces obtenemos que

$$\tau(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = x^{-1} \overline{*} y^{-1} = \tau(x) \overline{*} \tau(y)$$

es decir, τ es homomorfismo de grupos. Como además τ es una bijección, tenemos que es un isomorfismo de grupos. Llamaremos al grupo $(G, \overline{*})$ el *grupo reflejado* del grupo $(G, *)$.

Ejercicio 21. — *Verificar que $I : (G, *) \to (G, \overline{*}) : x \mapsto x$ no es un homomorfismo si G no es un grupo Abeliano.*

Definición 3.0.32. — Dado un grupo $(G, *)$, definimos el conjunto Aut(G), formado por todos los automorfismos de $(G, *)$. Un isomorfismo $\phi : (G, *) \to (G, \overline{*})$ será llamado un *antiautomorfismo* de $(G, *)$. Denotaremos por Aut$^-(G)$ al conjunto de los antiautomorfismos de $(G, *)$.

Ejercicio 22. — *Verificar que Aut(G) es un grupo con la regla de composición y de hecho un subgrupo de $Perm(G)$. Si $(G, *)$ es un grupo Abeliano, entonces Aut$(G) =$ Aut$^-(G)$, es decir, todo antiautomorfismo es también un automorfismo. ¿Qué pasa para grupos no Abelianos ? ¿Es Aut$^-(G)$ un grupo bajo la regla de composición ?*

Definición 3.0.33. — Algunos automorfismos de $(G, *)$ se pueden obtener por conjugación, es decir, para cada $g \in G$ la función

$$\phi(g) : G \to G : k \mapsto g * k * g^{-1}$$

resulta ser un automorfismo de $(G, *)$, llamados *automorfismos interiores*. Denotaremos por $Int(G)$ al conjunto de los automorfismos interiores de G.

Ejercicio 23. — *Verificar que $Int(G)$, con la operación de composición, es un subgrupo de Aut(G) y luego un subgrupo de $Perm(G)$.*

Ahora podemos continuar con nuestra verificación de que todo grupo es en efecto un subgrupo de permutaciones, obteniendo así que las versiones clásicas y modernas de grupo son lo mismo. Sea $(G, *)$ un grupo y consideremos al conjunto $X = G$. Entonces tenemos la función

$$\phi : G \to Perm(G)$$

definida por

$$\phi(g) : G \to G : k \mapsto g * k$$

Este es un ejemplo de lo que definiremos más adelante como la acción de un grupo.

Ejercicio 24. — *Verificar que $\phi : G \to Perm(G)$ es un monomorfismo.*

De lo anterior tenemos el clásico teorema de Caeley, del cual vemos que la noción clásica y la moderna son equivalentes.

***Teorema 3.0.34* (Teorema de Caeley)**. — *Todo grupo $(G, *)$ es isomorfo a un subgrupo del grupo $Perm(G)$. De hecho, tal subgrupo está contenido en el subgrupo de $Perm(G)$ formado por los automorfismo interiores de G.*

Ejemplo 3.0.35. — Consideremos dos conjunto X e Y y supongamos que existe una función biyectiva $f : X \to Y$. Entonces tenemos que para cada $h \in Perm(X)$ vale que $\phi_f(h) = f \circ h \circ f^{-1} \in Perm(Y)$. La función $\phi_f : Perm(X) \to Perm(Y)$ es un isomorfismo de grupos. Como todo conjunto X de cardinalidad $n > 0$ es biyectivo con el conjunto de los n primeros índices $\{1, 2, ..., n\}$, podemos identificar (módulo isomorfismos) el grupo $Perm(X)$ con el grupo $Perm(\{1, 2, ..., n\}) := \mathcal{S}_n$, llamado el *grupo simétrico de n letras*. Este grupo lo analizaremos en una sección futura.

Ejercicio 25. — *Dar un ejemplo de un grupo de orden n para cada $n \in \{1, 2, 3, 4, ...\}$.*

Ejemplo 3.0.36. — Sea $(G, *)$ un grupo finito de orden n. Por el teorema de Caeley, existe un monomorfismo $\phi : (G, *) \to \mathcal{S}_n$. Por otro lado, podemos construir un monomorfismo

$$\psi : \mathcal{S}_n \to GL(n, \mathbb{Z})$$

definido por

$$\psi((1, 2, ..., n)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

$$\psi((1,2)) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Luego, tenemos un monomorfismo

$$\psi \circ \phi : (G, *) \to GL(n, \mathbb{Z})$$

Ahora veremos que los automorfismos interiores de un grupo sirven para medir que tan lejos esta un grupo de ser Abeliano.

Proposición 3.0.37. — *Sea $(G, *)$ un grupo. Entonces $Int(G) = \{I\}$, donde $I : G \to G$ denota al automorfismo identidad sí y sólo si G es Abeliano.*

Demonstración. — Sea $(G, *)$ un grupo Abeliano, $g \in G$ y consideremos el automorfismo interno $\phi_g : G \to G$ definido por g. Entonces $\phi_g(h) = g*h*g^{-1} = g*g^{-1}*h = h$, es decir, $\phi_g = I$. Recíprocamente, si tenemos que $Int(G) = \{I\}$, entonces para $g, h \in G$ vale que $\phi_g(h) = h$, lo cual es equivalente a tener $g*h = h*g$. Como esto lo hemos hecho para cualquier par de elementos de G, tenemos que G es Abeliano como queríamos. □

Ejemplo 3.0.38. —

(1) Consideremos el grupo aditivo $\mathbb{Z}$. Como este grupo es Abeliano, tenemos que $Int(\mathbb{Z}) = \{I\}$. Ahora, sea $\phi : \mathbb{Z} \to \mathbb{Z}$ un automorfismo. Sabemos que los únicos generadores de $\mathbb{Z}$ son -1 y 1. Así, $\phi(1) \in \{-1, 1\}$. Si $\phi(1) = 1$, entonces es claro que $\phi(k) = k$ para cada $k \in \mathbb{Z}$ y luego obtenemos el automorfismo identidad I. Si $\phi(1) = -1$, entonces $\phi(k) = -k$ para cada $k \in \mathbb{Z}$ obteniendo $\phi = -I$. De esta manera obtenemos que $Aut(\mathbb{Z})$ es un grupo cíclico de orden 2.

(2) Consideremos un grupo G cíclico de orden n y sea x un generador de G. Luego

$$G = \{I_G, x, x^2, x^3, ..., x^{n-1}\}.$$

Sea $e(n)$ la función de Euler evaluada en n. Más adelante veremos que el número total de generadores de G es $e(n)$. Al ser G Abeliano tenemos que $Int(G)$ es trivial. Sea $\phi \in Aut(G)$. Entonces $\phi(x)$ puede tomar como valor cualquiera de los generadores de G. Además, una vez indicado el valor de $\phi(x)$ tenemos determinado completamente el automorfismo ϕ ya que $\phi(x^l) = \phi(x)^l$ por ser este un homomorfismo de grupo. De esta manera obtenemos que $|Aut(G)| = e(n)$.

Ejercicio 26. —

(1) Si n es un número primo, $e(n) = n - 1$.

(2) Calcular $e(n)$ para $n = 2, 3, 4, 5, 6, 7, , 8, 9, 10$.

(3) Sea G_n un grupo cíclico de orden n. Verificar que existe un isomorfismo de grupos entre $Aut(G_n)$ y $\mathbb{Z}/n\mathbb{Z}^*$.
(5) Calcular $Aut(Perm(X))$ para un conjunto X de cardinalidad $2, 3, 4$.

Proposición 3.0.39. — *Sea $\phi : G \to K$ un homomorfismo de grupos.*
(1) Si H es subgrupo de G, entonces $\phi(H)$ es subgrupo de K.
(2) Si U es subgrupo de K, entonces $\phi^{-1}(U)$ es un subgrupo de G conteniendo a Ker(ϕ).

Ejercicio 27. — *Demostrar la proposición anterior.*

Ejercicio 28. — *Sea (X, Υ) un espacio topológico y sean $p, q \in X$ en la misma componente arcoconexa. Verificar que los grupos fundamentales $\pi_1(X, p)$ y $\pi_1(X, q)$ son isomorfos. ¿Qué pasa si p y q están en componentes diferentes ?*

CAPÍTULO 4

GENERADORES

Consideremos un grupo $(G, *)$ y un subconjunto $A \subset G$. Lo más probable es que A no sea un subgrupo de G. Podemos preguntarnos por el subgrupo de G más pequeño que contenga A.
Lo que podemos intentar es considerar la intersección de todos los subgrupos de G que contenga a A, es decir

$$\langle A \rangle = \bigcap_{\substack{H<G \\ A \subset H}} H$$

Esta intersección es no vacía ya que G es uno de los subgrupos conteniendo A.
Como la intersección de subgrupos de un grupo dado es nuevamente un subgrupo, tenemos que en efecto $\langle A \rangle$ es un subgrupo de G.

Definición 4.0.40. — El grupo $\langle A \rangle$ es llamado el subgrupo de G generado por A. En caso que $\langle A \rangle = G$, decimos que A es un conjunto de generadores de G. En este caso decimos también que los elementos de A son generadores de G.

Ejercicio 29. — *Buscar generadores para los grupos del ejemplo 1.0.9.*

CAPÍTULO 5

GRUPOS CÍCLICOS

Definición 5.0.41. — Aquellos grupos que se pueden generar con un sólo elemento son llamados *grupos cíclicos*.

Tenemos dos tipos de casos ; grupos cíclicos finitos y grupos cíclicos infinitos. Observemos que si $(G, *)$ es un grupo cíclico finito, con un generador x, entonces $|G| = o(x)$. El primer resultado básico es el siguiente.

Proposición 5.0.42. — *Todo grupo cíclico es Abeliano*

Demonstración. — Sea x un generador del grupo cíco G. Entonces todo elemento de G es de la forma x^a para algún $a \in \mathbb{Z}$. Como

$$x^a * x^b = x^{a+b} = x^{b+a} = x^b * x^a$$

tenemos lo deseado □

Ejemplo 5.0.43. —

(1) En ejercicio 1.0.4 tenemos que S y T son generadores de $Perm(X)$. Más aún, este no puede ser cíclico. De hecho, el grupo $Perm(X)$ no puede ser cíclico cuando la cardinalidad de X es al menos 3.
(2) El grupo aditivo $\mathbb{Z}$ tiene como generador a 1 (también lo es -1 y no hay otros) y, en particular, es un grupo cíclico.
(3) El conjunto aditivo $\mathbb{R}$ no puede ser generado con un número finito de generadores (la razón de esto lo tendremos que ver mucho más adelante). Este no puede ser un grupo cíclico como consecuencia del siguiente.

***Ejemplo 5.0.44* (Grupos Cíclicos infinitos)**. — Sea G un grupo un grupo cíclico infinito, digamos generado por x.

(i) Sea H un subgrupo de G diferente de $\{I\}$ y consideremos la menor potencia positiva de x, digamos x^m, contenida en H. Entonces el grupo cíclico generado por x^m está contenido en H. Si esta contención fuese estricta, entonces debe existir $x^n \in H - \langle x^m \rangle$. Esto nos dice que existe $s > 0$ tal que $(s-1)m < n < sm$. Esto nos segura que $x^{sm-n} \in H$ contradiciendo la minimalidad de m. En particular, todo subgrupo de un grupo cíclico infinito es también un grupo cíclico infinito.

(ii) Si x^n es otro generador de G, entonces debe existir un entero $r \in \mathbb{Z}$ de manera que $x^{nr} = x$, es decir, $x^{nr-1} = I$. Como x tiene orden infinito, esto obliga a tener $nr = 1$, es decir, $n \in \pm 1$. En consecuencia, si x genera un grupo cíclico infinito, entonces x^{-1} es el único generador diferente de x.

(iii) La función $\phi : \mathbb{Z} \to G$, definida por $\phi(k) = x^k$, resulta ser un isomorfismo de grupos.

***Ejemplo 5.0.45* (Grupos Cíclicos finitos).** — Sea G un grupo cíclico de orden n, digamos generado por x, luego $o(x) = n$.

(i) Sea H un subgrupo de G, diferente de $\{I_G\}$. Si consideramos la menor potencia de x contenido en H, digamos x^m, entonces H es un grupo cíclico generado por x^m. En efecto, si no fuese esto cierto, deberiamos tener alguna potencia $x^k \in H$ que no estén $\langle x^m \rangle = \{I_G, x^m, x^{2m}, ..., x^{rm}\}$. En tal caso, debemos tener que $(s-1)m < k < sm$, para algún $s \in \{1, ..., r\}$. Pero en tal caso, $x^{k-(s-1)m} \in H$ y obtenemos una contradicción de la minimalidad de m.

(ii) Si escogemos $d > 0$ un divisor de n, entonces existe un y único subgrupo de G de orden igual a d. En efecto, si tomamos $y = x^{\frac{n}{d}}$, entonces el grupo generado por y es de orden d. Esto no da la existencia. Para ver la unicidad, supongamos que H es un subgrupo de G de orden d. Por (i), $H = \langle x^m \rangle$ donde m lo podemos escoger dividiendo n y tal que $\frac{n}{m} = d$. Luego $m = \frac{n}{d}$.

(iii) Sea $m \in \{1, 2, 3, ..., n\}$, $y = x^m$ y H el subgrupo generado por y. Por el teorema de Lagrange, $|H| = o(y) = t$ divide n. En particular, podemos escribir $n = tq$ para cierto $q \in \{1, 2, 3, ..., n-1\}$. Consideremos K el subgrupo generado por $z = x^q$, el cual tiene orden t. Por (ii) tenemos que $H = K$. En particular, existe un entero a tal que $x^{am} = x^q$. Esto último dice que existen enteros a, b tales que $am + bn = q$, es decir $M.C.D.(m, n) = q$ (máximo común divisor entre m y n).

(iv) De (iii) vemos que x^m genera G sí y sólo si $M.C.D.(m, n) = 1$, es decir $(m, n) = 1$.

(v) La función $\phi : \mathbb{Z}/n\mathbb{Z} \to G$, definida por $\phi([k]) = x^k$, resulta ser un isomorfismo de grupos.

***Proposición 5.0.46*.** — *Sea G un grupo cíclico de orden n, digamos generado por x.*

(a) Para $k \in \{1, 2, ..., n-1\}$ tenemos que x^k genera G sí y sólo si $(k, n) = 1$, es decir, k y n son relativamente primos. En particular, la cantidad de generadores de G es $e(n)$.

(b) Todo subgrupo de G es cíclico y está generado por una potencia x^d, donde d divide n, y tiene orden n/d. Además hay exáctamente un subgrupo de cada posible orden.

(c) Sean $k \in \{1, 2, ..., n-1\}$ y $q = M.C.D.(k, n)$. Entonces x^k y x^q generan el mismo subgrupo.

Proposición 5.0.47. — *Sean n, m enteros y $q = M.C.D.(n, m)$. Entonces existen enteros $a, b \in \mathbb{Z}$ tales que*

$$q = an + bm$$

En particular, si $(m, n) = 1$, entonces existen enteros $a, b \in \mathbb{Z}$ tales que

$$1 = an + bm$$

Demonstración. —

(1) Usando grupos cíclicos finitos. Es claro lo anterior cuando $n = m$. Supongamos entonces que $n > m$. Consideremos el grupo cíclico de orden n generado por un elemento x. Ahora procedemos como en (iii) del ejemplo anterior.

(2) Usando grupos cíclicos infinitos. Podemos verificar la proposición de la siguiente manera. Consideremos el grupo cíclico infinito $\mathbb{Z}$ y sea H su subgrupo generado por n y m. Sabemos que H debe ser cíclico, digamos generado por $r \in \{0, 1, 2, ...\}$. Como $n, m \in H$, tenemos que r divide a ambos n y m y como consecuencia, r divide a $d = M.C.D.(n, m)$. Esto último nos dice que el grupo cíclico generado por d está contenido en H. Pero, como d divide a ambos n y m, tenemos que H está contenido en el grupo cíclico generado por d. Como consecuencia, $H = \langle d \rangle$.

□

Ejercicio 30. — *Generalizar lo anterior, es decir, verificar que dados enteros $n_1, ..., n_m$ y $d = M.C.D.(n_1, ..., n_m)$, entonces existen enteros $r_1, ..., r_n$ tales que*

$$d = r_1 n_1 + \cdots + r_m n_m$$

CAPÍTULO 6

GRUPOS COCIENTES

Partamos con un grupo $(G, *)$ y un subgrupo H de este. Podemos definir la relación de equivalencia siguiente : Sean $x, y \in G$, diremos que ellos son equivalentes por H a la derecha si existe $h \in H$ tal que $y = x * h$. La clase de equivalencia derecha de x la denotaremos por xH. De manera similar, diremos que ellos son equivalentes por H a la izquierda si existe $h \in H$ tal que $y = h * x$. La clase de equivalencia izquierda de x es denotada por Hx.

Ejercicio 31. — *Verificar que las anteriores son relaciones de equivalencia*

Consideremos la relación de equivalencia derecha de H en G (lo que haremos es similar para la otra relación de equivalencia). Denotemos por G/H al conjunto de las clases de equivalencias derechas de los elementos de G y por $\pi_H : G \to G/H$ a la proyección natural, es decir, $\pi_H(x) = xH$. Observemos que H es la clase de equivalencia de I_G. Tomemos una clase cualquiera, digamos xH. Entonces la función $f : H \to xH$, definida por $f(h) = xh$, es una función biyectiva. De esta manera, la cardinalidad de toda clase de equivalencia es igual al orden de H, es decir a $|H|$.

Definición 6.0.48. — Denotemos por $[G : H]$ la cardinalidad del conjunto de clases G/H, también llamado el *índice de* H en G.

Usando el hecho que dos clases de equivalencia coinciden o son disjuntos, obtenemos el siguiente :

Teorema 6.0.49 **(Teorema de Lagrange)**. — *Si G tiene orden finito, entonces*

$$|G| = [G : H]|H|$$

Ejercicio 32. — *Usar el teorema de Lagrange para obtener lo siguiente. Sea G un grupo finito y sean subgrupos $K < H < G$. Entonces $[G : K] = [G : H][H : K]$*

Si tomamos un elemento $g \in G$, donde $(G, *)$ es algún grupo, entonces el subgrupo generado por él $\langle g \rangle$ tienen orden igual a $o(g)$. Una primera aplicación de este resultado es el siguiente :

Corolario 6.0.50. — *Sea $(G, *)$ un grupo de orden finito, H un subgrupo de G y $g \in G$. Entonces $|H|$ y $o(g)$ dividen al orden de G como consecuencia del teorema de Lagrange.*

Lo anterior, por ejemplo, nos permite ver que un grupo de orden 6 no puede tener elementos ni subgrupos de orden 4. Una segunda aplicación es la siguiente caracterización.

Proposición 6.0.51. — *Sea G un grupo finito de orden p, donde p es algún primo. Entonces G es necesariamente un grupo cíclico.*

Demonstración. — Tomemos cualquier elemento $x \in G - \{I_G\}$. Por la proposición anterior, $o(x)$ divide al número primo p. Como $o(x) > 1$, necesariamente $o(x) = p$. Consideremos el subgrupo cíclico de G dado por $\langle x \rangle$. Como el orden de $\langle x \rangle$ coincide con $o(x) = p$, tenemos que $G = \langle x \rangle$. □

Ejemplo 6.0.52. — Consideremos un grupo $(G, *)$ de orden 4. Si G contiene un elemento de orden 4, digamos x, entonces $G = \langle x \rangle$, es decir, G es un grupo cíclico de orden 4. Supongamos ahora que G no contiene elementos de orden 4. Como el orden de cada elemento no trivial (es decir diferente del neutro) debe dividir 4, debemos tener que todos ellos tienen orden 2. Sea $x \in G - \{I_G\}$. Luego $\langle x \rangle$ está formado por el neutro I_G y x. Como G tiene orden 4, podemos escoger otro elemento $y \in G - \langle x \rangle$. Tenemos que y tiene orden 2. Como $(x*y)^2 = I_G$, $x^2 = y^2 = I_G$, tenemos $x*y = y*x$. Consideremos el subgrupo H de G generado por x e y. Tenemos que $H = \{I_G, x, y, x*y\}$ ($x*y \neq x, y$ ya que $x, y \neq I_G$). Pero $|H| = 4$, lo cual dice que $G = H$. Ahora, consideremos $\mathcal{K} = \langle x \rangle \times \langle y \rangle$ con la operación binaria $\triangle$ definida componente a componente (en cada factor usamos la operación $*$). Este grupo es llamado el *grupo de Klein*. Consideremos la función

$$F : K \to G : (x^a, y^b) \mapsto x^a * y^b$$

Tenemos que F es un isomorfismo de grupos. Además, como $\mathcal{K}$ no es cíclico, obtenemos que módulo isomorfismos sólo hay dos grupos.

Ejercicio 33. — *Verificar que la operación binaria para $\mathcal{K}$ dota de la estructura de un grupo Abeliano a $\mathcal{K}$, que F es en efecto un isomorfismo de grupos. Calcular y comparar las tablas de multiplicación de estos dos tipos de grupos de orden 4.*

Ejercicio 34. — *Verificar que dos grupos cíclicos finitos del mismo orden son siempre isomorfos.*

Ejercicio 35. — *Determinar, módulo isomorfismos, los grupos de orden* $n \in \{1, 2, ..., 7\}$.

Volvamos a mirar la proyección

$$\pi_H : G \to G/H : x \mapsto xH$$

Una pregunta natural es la posibilidad de dotar a G/H de una estructura de grupo que sea compatible con la de G por medio de ϕ_H. Compatibilidad significa que haga π_H de un homomorfismo de grupos. En la mayoría de los casos esto no será posible, pero existen ciertos subgrupos que permiten esto. Tratemos de forzar una operación binaria $\triangle$ en G/H para que haga de π_H un homomorfismo. Primero, debemos tener

$$\pi_H(x * y) = \pi_H(x) \triangle \pi_H(y)$$

lo que es equivalente a decir

$$(x * y)H = x * H \triangle y * H$$

para todos $x, y \in G$. Luego tenemos forzada nuestra operación binaria a ser definida como :

$$\triangle : G/H \times G/H \to G/H : (xH, yH) \mapsto (x * y)H$$

Para que esta función tenga sentido, debemos asegurarnos que lo anterior no dependa de los representantes de las clases respectivas, es decir, si $x'H = xH$, $y'H = yH$, entonces $(x' * y')H = (x * y)H$. Pero $x' = x * h_1$ e $y' = y * h_2$ para ciertos $h_1, h_2 \in H$. Luego lo anterior es equivalente a tener

$$(x * h_1 * y * h_2)H = (x * y)H$$

es decir

$$(h_1 * y)H = yH$$

o de manera equivalente

$$y^{-1} * h_1 * y \in H$$

En resumen, para que lo anterior tenga sentido, debemos tener la propiedad

$$zH = Hz, \text{ para todo } z \in G$$

Definición 6.0.53. — Un subgrupo H de G con la propiedad que

$$zH = Hz, \text{ para todo } z \in G$$

es llamado un *subgrupo normal* de G.

Proposición 6.0.54. — *Sea H un subgrupo normal de G. Entonces G/H resulta ser un grupo con la operación binaria $\triangle$ con la cual $\pi_H : G \to G/H$ es un homomorfismo de grupos cuyo núcleo es exactamente H. Este grupo cociente es también llamado el* grupo de las clases laterales *de H en G. Más aún, (i) si G es Abeliano, entonces G/H también es Abeliano ; y (ii) si G es cíclico, entonces G/H también es cíclico.*

Demonstración. — La asociatividad de $\triangle$ es heredada por la de $*$. Por otro lado, $H \triangle H = H$ (H es la clase de I_G), lo cual nos está forzando a tomar H como elemento neutro $I_{G/H}$. Hasta ahora todo camina bién. Sea $xH \in G/H$ y tratemos de buscar un candidato para el inverso. Por la condición de hacer π_H de un homomorfismo, estamos obligados a tener

$$\pi_H(x^{-1}) = \pi_H(x)^{-1}$$

lo cual es equivalente a pedir que

$$(xH)^{-1} = x^{-1}H$$

Esta definición funciona correctamente y tenemos que G/H resulta ser un grupo con la operación binaria $\triangle$ con la cual $\pi_H : G \to G/H$ es un homomorfismo de grupos cuyo núcleo es exactamente H.
La definición de la operación $\triangle$ asegura que si $*$ es commutativa, entonces también lo es $\triangle$. Por otro lado, si G es cíclico generado por x, entonces xH es generador de G/H.

□

Ejemplo 6.0.55. — Sea H un subgrupo de índice dos en un grupo G (con operación binaria de grupo dada por $*$). Entonces podemos escribir

$$G = H \cup xH = H \cup Hx$$

para cualquier $x \in G - H$, donde las uniones son disjuntas. Tomemos $g \in G$. entonces (i) $g \in H$, en cuyo caso $g * h * g^{-1} \in H$, para todo $h \in H$, o (ii) $g = x * h_1 = h_2 * x$, para ciertos $h_1, h2 \in H$. Ahora, si $h \in H$, entonces $g * h * g^{-1} = x * h_1 * h *_3^{-1} * x^{-1} = x * h_4 * x^{-1}$, donde $h_4 \in H$. Si tenemos $x * h_4 * x^{-1} \notin H$, entonces $x * h_4 * x^{-1} \in x * H$, lo cual dice que $h_4 * x^{-1} \in H$. Esto último asegura que $x \in H$, una contradicción. Hemos verificado el siguiente.

Proposición 6.0.56. — *Todo subgrupo de índice dos es necesariamente un subgrupo normal.*

Ejemplo 6.0.57. — Consideremos el grupo, con la regla de composición, de todos los difeomorfismos de $\mathbb{R}^n$. Sea H el subgrupo de los difeomorfismos con jacobiano positivo (difeomorfismos que preservan la orientación). Como el jacobiano de una composición es el producto de los respectivos jacobianos, tenemos entonces que H es un subgrupo de índice dos y luego un subgrupo normal.

Ejemplo 6.0.58. —
(1) Si G es un grupo Abeliano, entonces todo subgrupo es necesariamente normal.

(2) Consideremos $X = \{1, 2, 3\}$ y $G = Perm(X)$. Tenemos que

$$A = \begin{cases} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \end{cases} \text{ y } B = \begin{cases} 1 & \to & 2 \\ 2 & \to & 1 \\ 3 & \to & 3 \end{cases}$$

forman un conjunto de generadores de G (comparar con el ejemplo 1.0.4). Los subgrupos de G son, aparte del trivial $\{I_G\}$ y del total G, los subgrupos de orden dos $\langle B\rangle$, $\langle A \circ B\rangle$, $\langle A^2 \circ B\rangle$ y el grupo de orden tres $\langle A\rangle$, todos ellos cíclicos. Como $B \circ A \circ B = A^3$, tenemos que $\langle A\rangle$ es subgrupo normal de G. Pero $A \circ B \circ A^{-1} = A^2 \circ B$, $A \circ A \circ B \circ A^{-1} = A \circ B$ y $A \circ A^2 \circ B \circ A^{-1} = B$, tenemos que ninguno de los tres subgrupos de orden dos es subgrupo normal. Observemos también que $[G : \langle A\rangle] = 2$, luego $G/\langle A\rangle$ es un grupo de orden dos (luego cíclico).

Ejercicio 36. — *Considere el grupo multiplicativo de las matrices reales de tamaño $n \times n$ y determinante no cero (es decir, la invertibles). Calcular todos su subgrupos normales.*

Ejemplo 6.0.59. — Consideremos el grupo aditivo $\mathbb{Z}$ y sea $n \in \{2, 3, 4, 5, ...\}$. Entonces se tiene que $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ es un subgrupo de $\mathbb{Z}$ y, como este es Abeliano, es también subgrupo normal. Se tiene que $[\mathbb{Z} : n\mathbb{Z}] = n$ y, como consecuencia,

$$\mathbb{Z}/n\mathbb{Z}$$

es un grupo Abeliano de orden n, llamado el *grupo de las clases residuales de orden* n. Este es un grupo cíclico de orden n (luego todo grupo cíclico de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Como consecuencia, el grupo de Klein es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, con la operación binaria componente a componente.

Ejemplo 6.0.60. — Volvamos al grupo de automorfismos de un grupo G, $Aut(G)$. Ya habíamos definido el subgrupo de $Aut(G)$ dado por los automorfismos interiores, $Int(G)$. Para cada $g \in G$, tenemos el automorfismo interior $\phi_g : G \to G$, definido por $\phi_g(h) = g * h * g^{-1}$. Sea $T \in Aut(G)$. Entonces,

$$T \circ \phi_g \circ T^{-1} = \phi_{T(g)}$$

obteniendo que $Int(G)$ es un subgrupo normal de $Aut(G)$. El grupo cociente

$$Out(G) = Aut(G)/Int(G)$$

es llamado el *grupo de automorfismos exteriores* de G. Así, si G es un grupo Abeliano, entonces $Aut(G) = Out(G)$.

Ejercicio 37. — *Calcular $Out(Perm(X))$ para X como en el ejemplo 1.0.4.*

Proposición 6.0.61. — *Consideremos un homomorfismo de grupos $\phi : G \to K$, donde $(G, *)$ y $(K, \cdot)$ son ciertos grupos. Entonces tenemos que Ker(ϕ) es un subgrupo normal de G. De hecho, si U es un subgrupo normal del grupo $\phi(G)$, entonces $\phi^{-1}(U)$ es subgrupo normal de G. Recíprocamente, si H es un subgrupo normal de G, entonces $\phi(H)$ es un subgrupo normal de $\phi(G)$.*

Demonstración. — (i) Sea $h \in$ Ker(ϕ) y $g \in G$. Entonces

$$\phi(g * h * g^{-1}) = \phi(g) \cdot \phi(h) \cdot \phi(g)^{-1} = I_K$$

(ii) Sea U subgrupo normal de $\phi(G)$, entonces sabemos que $\phi^{-1}(U)$ es un subgrupo de G. Por otro lado, si $h \in \phi^{-1}(U)$ y $g \in G$, entonces $\phi(g*h*g^{-1}) = \phi(g)\cdot\phi(h)\cdot\phi(g)^{-1} \in U$, obteniendo la normalidad de $\phi^{-1}(U)$. (iii) Sea H un subgrupo normal de G. Ya sabemos que $\phi(H)$ es un subgrupo de $\phi(G)$. Ahora, si tomamos $t \in \phi(G)$ y $k \in \phi(H)$, entonces existen $g \in G$ y $h \in H$ tales que $\phi(g) = t$ y $\phi(h) = k$. Luego $t \cdot k \cdot t^{-1} = \phi(g) \cdot \phi(h) \cdot \phi(g)^{-1} = \phi(g * h * g^{-1}) \in \phi(H)$.

□

El resultado anterior nos permite considerar el grupo cociente $G/$Ker(ϕ) para cada homomorfismo de grupos $\phi : G \to K$. Podemos entonces definir la nueva función $\widehat{\phi} : G/\text{Ker}(\phi) \to K$ como

$$\widehat{\phi}(x\text{Ker}(\phi)) = \phi(x)$$

Proposición 6.0.62 **(Primer teorema del isomorfismo)**. —
La función $\widehat{\phi} : G/Ker(\phi) \to K$ está bién definida y es un monomorfismo.

Demonstración. — Para ver que está bién definida basta ver que si $x \in G$ y $h \in$ Ker(ϕ) entonces $\phi(x * h) = \phi(x)$. Ahora,

$$\widehat{\phi}(x\text{Ker}(\phi)\triangle x\text{Ker}(\phi)) = \widehat{\phi}((x * y)\text{Ker}(\phi)) = \phi(x * y) =$$
$$= \phi(x) \cdot \phi(y) = \widehat{\phi}(x\text{Ker}(\phi)) \cdot \widehat{\phi}(y\text{Ker}(\phi))$$

□

Corolario 6.0.63. — *La función $\widehat{\phi} : G/Ker(\phi) \to \phi(G)$ es un isomorfismo. En particular ; si G tiene orden finito, entonces tenemos que $|\phi(G)| = [G : Ker(\phi)]$.*

Ejemplo 6.0.64. — Sean $\phi : G \to K$ un homomorfismo de grupos y H un subgrupo de G. Podemos restringir nuestro homomorfismo a H, $\phi|_H : H \to K$. Ahora, Ker$(\phi|_H) =$ Ker$(\phi) \cap H$. Luego tenemos un isomorfismo entre $\phi(H)$ y $G/(H \cap \text{Ker}(\phi))$.
Como consecuencia de esto es que si H es además un subgrupo normal de G, entonces usando $K = G/H$, tenemos una biyección, dada por $\phi = \pi_H$, entre los subgrupos (normales) de G/H y los subgrupos (normales) de G que contienen a H.

Para nuestro siguiente ejemplo necesitaremos el subgrupo generado por la unión de dos subgrupos, lo cual pasamos a mirar inmediatamente. Supongamos que tenemos un grupo $(G, *)$ y dos subgrupos de este, digamos H y K. Podemos entonces mirar el subgrupo de G generado por H y K, es decir, $\langle H \cup K \rangle$. Es claro que

$$HK = \{h * k : h \in H, k \in K\} \subset \langle H \cup K \rangle$$

Luego, la igualdad $\langle H \cup K \rangle = HK$ es cierta sí y sólo si HK es un subgrupo de G. El siguiente resultado nos permite ver cuando ocurre esta situación.

Proposición 6.0.65. — *HK es subgrupo de G sí y sólo si $HK = KH$.*

Demonstración. — Supongamos que HK es un subgrupo de G. En tal caso consideremos un elemento $h * k \in HK$. Tenemos que su inverso $(h * k)^{-1} = k^{-1} * h^{-1}$ pertenece a KH. Como todo elemento de HK (por ser subgrupo) es inverso de alguno de sus otros elementos, tenemos la contención $HK \subset KH$. Por otro lado, dado $k*h \in KH$, entonces $h^1 * k^{-1} \in HK$. Al ser HK subgrupo tenemos que este debe contener al inverso, es decir $k * h \in HK$, obteniendo la contención $KH \subset HK$.
Veamos ahora el recíproco y supongamos la igualdad $HK = KH$. Sean $h_1 * k_1, h_2 * k_2 \in HK$. Luego $(h_1 * k_1) * (h_2 * k_2) = h_1 * (k_1 * h_2) * k_2$. Pero la igualdad $HK = KH$ asegura que $k_1 * h_2 = h_3 * k_3$, así, $(h_1 * k_1) * (h_2 * k_2) = (h_1 * h_3) * (k_3 * k_2) \in HK$. También, si $h * k \in HK$, entonces $(h * k)^{-1} = k^{-1} * h^{-1} \in KH = HK$. Como consecuencia, HK es un subgrupo de G. □

Observación 6.0.66. — Si tenemos H, K subgrupos de G y uno de ellos es un subgrupo normal, entonces la condición $HK = KH$ vale trivialmente. Más aún, si ambos son subgrupos normales, entonces HK también lo es.

Ejercicio 38. — *Verificar la observación anterior.*

Suponiendo que G es un grupo de orden finito, tenemos que HK (independiente de ser o no un subgrupo) tiene una cardinalidad finita. Para ver que valor tiene esta, consideremos la función

$$F : H \times K \to HK : (h, k) \mapsto h * k$$

Por la definición de HK, F es una función sobreyectiva. También sabemos que $|H \times K| = |H||K|$. Por otro lado, si $\alpha \in HK$, entonces

$$F^{-1}(\alpha) = \{(h, k) \in H \times K : h * k = \alpha\}$$

Ahora, si $(h_1, k_1), (h_2, k_2) \in F^{-1}(\alpha)$, entonces $h_1 * k_1 = h_2 * k_2$, lo cual asegura que $h_2^{-1} * h_1 = k_2 * k_1^{-1} = x \in H \cap K$. Entonces $h_2 = h_1 * x^{-1}$, $k_2 = x * k_1$. En forma recíproca, si $x \in H \cap K$ y $(h, k) \in F^{-1}(\alpha)$, entonces $F(h * x^{-1}, x * k) = \alpha$. Como

consecuencia, $\#F^{-1}(\alpha) = |H \cap K|$. De esta manera, como preimágenes de valores diferentes son disjuntos y la unión de todas la preimágenes es $H \times K$, obtenemos

$$\#HK = \frac{|H||K|}{|H \cap K|}$$

Ejemplo 6.0.67 **(Segundo Teorema del isomorfismo)**. — Sean $(G, *)$ un grupo, H, K subgrupos de G y supongamos que H es además subgrupo normal de G. De esta manera nos aseguramos que HK es subgrupo de G. Como H es también subgrupo de HK, tenemos que H es subgrupo normal de HK. Consideremos la proyección $\pi : HK \to HK/H : x \mapsto xH$. Consideremos las restricción a K, es decir, $\pi|_K : K \to HK/H$. Tenemos que Ker$(\pi|_K) = K \cap H$. Veamos ahora que $\pi|_K$ es sobreyectiva. En efecto, si $z = (h * k)H \in HK/H$, entonces como $HK = KH$, tenemos que $h * k = k_1 * h_1$ y luego $\pi|_K(k_1) = z$. En consecuencia, tenemos un isomorfismo

$$\frac{K}{K \cap H} \cong \frac{HK}{H}$$

Ejemplo 6.0.68 **(Tercer Teorema del isomorfismo)**. — Consideremos un grupo $(G, *)$ y dos subgrupos normales de G, digamos K y H, tales que $K < H$. Consideremos la función

$$\phi : G/K \to G/H : gK \mapsto gH$$

Entonces ϕ resulta ser un homomorfimos sobreyectivo. Por otro lado,

$$\text{Ker}(\phi) = \{gK : g \in H\} = H/K$$

es decir

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

Ejemplo 6.0.69. — Consideremos un grupo finito $(G, *)$ y H un subgrupo normal de G tal que $([G : H], |H|) = 1$, es decir, $[G : H]$ y $|H|$ son relativamente primos. Veamos que no existe otro subgrupo de G del mismo orden que H. En efecto, supongamos que existe K subgrupo (no necesariamente normal) de G tal que $|K| = |H|$. Tomemos el homomorfismo $\phi : K \to G/H : k \mapsto kH$. Entonces, Ker$(\phi) = K \cap H$ y $K/(K \cap H) \cong \phi(K)$. En particular, $[K : K \cap H]$ divide $[G : H]$, por el teorema de Lagrange, es decir,

$$[G : H] = [K : K \cap H]M = |K|R$$

para ciertos enteros positivos M, R. Esto dice que $|H| = |K|$ divide $[G : H]$, una contradicción a menos que $K = H$.

Ejercicio 39. —

(i) Sea $(G, *)$ un grupo y sean H, K dos subgrupos de G. Suponga que $[G : H] < \infty$ y $[G : K] < \infty$. Verificar que $[G : H \cap K] < \infty$

(ii) Sea S^1 el grupo multiplicativo de los números complejos de valor absoluto 1 con la operación usual de producto. Consideremos el grupo aditivo $(\mathbb{R}, +)$ y su subgrupo normal $\mathbb{Z}$. Verificar que el siguiente es un isomorfismo de grupos

$$P : \mathbb{R}/\mathbb{Z} \to S^1 : x\mathbb{Z} \to e^{2x\pi i}$$

(iii) Sea $(G, *)$ un grupo y sea $H = \langle x^2 : x \in G\rangle$. Verificar que H es subgrupo normal de G y que el grupo cociente G/H es un grupo Abeliano.

(iv) Sea $(G, *)$ un grupo y sea $n > 1$ un entero positivo fijo. Supongamos que para todo $x, y \in G$ vale la igualdad $(x * y)^n = x^n * y^n$. Defina

$$G_n = \langle x : o(x) = n\rangle$$

$$G^n = \langle x^n : x \in G\rangle$$

Verificar que ambos son grupos normales de G y que $G/G_n \cong G^n$ (Ind. Utilizar el homomorfismo $\phi : G \to G^n : x \mapsto x^n$).

CAPÍTULO 7

ALGUNOS SUBGRUPOS NORMALES Y ABELIANIZACIÓN DE GRUPOS

Dado un grupo $(G, *)$, existe la posibilidad que este sea Abeliano, pero en general no es así. La condición de ser Abeliano es equivalente a que la ecuación

$$[x : y] = x * y * x^{-1} * y^{-1} = I_G$$

sea siempre valida para cualquier $x, y \in G$.

Definición 7.0.70. — Cada expresión

$$[x : y] = x * y * x^{-1} * y^{-1}$$

es llamada un *conmutador* de x e y. Denotamos por $[G, G]$ al subgrupo de G generado por todos los conmutadores.

Ejercicio 40. — *Sea $(G, *)$ un grupo. Verificar que*

$$[G, G] = \{x_1 * x_2 * \cdots * x_n * x_1^{-1} * x_2^{-1} * \cdots * x_n^{-1} : x_j \in G,\ n \geq 2\}$$

y concluir que $[G, G]$ es un subgrupo normal de G.
(Ind. $(a * b * a^{-1} * b^{-1}) * (c * d * c^{-1} * d^{-1}) =$
$a * (b * a^{-1}) * b^{-1} * c * (d * c^{-1}) * d^{-1} * a^{-1} * (a * b^{-1}) * b * c^{-1} * (c * d^{-1}) * d$*)*

Proposición 7.0.71. — *La intersección arbitraria de subgrupos normales de un grupo $(G, *)$ es un subgrupo normal.*

Demonstración. — Sean $\{H_j : j \in J\}$ una colección de subgrupos normales de G. Ya habíamos verificado que la intersección de estos subgrupos es un subgrupo de G. Ahora sólo necesitamos verificar la normalidad. Sea $g \in G$ y $h \in H = \bigcap_{j \in J} H_j$. Entonces, $h \in H_j$, para cada $j \in J$. Como H_j es subgrupo normal, tenemos que $g * h * g^{-1} \in H_j$, para cada $j \in J$ y, como consecuencia, $g * h * g^{-1} \in H$. □

Observemos que si G es Abeliano, entonces $[G,G] = \{I_G\}$. Recíprocamente, $[G,G] = \{I_G\}$ asegura que $[x:y] = I_G$ siempre vale para cualquier $x, y \in G$, obteniendo que G es Abeliano. Es decir, tenemos que

Proposición 7.0.72. — *Un grupo $(G,*)$ es Abeliano sí y sólo si $[G,G] = \{I_G\}$.*

Luego, si $(G,*)$ no es un grupo Abeliano, entonces $[G,G] \neq \{I_G\}$ nos dá un subgrupo normal no trivial de G. La normalidad de $[G,G]$ nos permite mirar el grupo

$$G^{abel} = G/[G,G]$$

el cual es llamado la *abelianización* de G.

Proposición 7.0.73. — *El grupo cociente G^{abel} es un grupo Abeliano.*

Demonstración. — sean $x[G,G], y[G,G] \in G^{abel}$. Luego,

$$[x[G,G] : y[G,G]] = x[G,G] \triangle y[G,G] \triangle (x[G,G])^{-1} \triangle (y[G,G])^{-1} =$$
$$= x[G,G] \triangle y[G,G] \triangle x^{-1}[G,G] \triangle y^{-1}[G,G] = (x * y * x^{-1} * y^{-1})[G,G] =$$
$$= [G,G]$$

□

Definición 7.0.74. — Otro de los subgrupos de $(G,*)$ que mide la cercanía de G a ser Abeliano es el siguiente :

$$Z(G) = \{g \in G : [g,x] = I_G \text{ para todo } x \in G\}$$

llamado el *centralizador* de G. También podemos hablar del *centralizador de un elemento* g del grupo G que está definido por

$$Z(G;g) = \{x \in G : g * x = x * g\}$$

Ejercicio 41. — *Verificar que $Z(G;g)$ es un subgrupo de G y que $Z(G;g) = G$ sí y sólo si $g \in Z(G)$.*

Proposición 7.0.75. — *$Z(G)$ es siempre un subgrupo normal de G.*

Demonstración. — Es claro que $I_G \in Z(G)$, luego $Z(G) \neq \emptyset$. Sean $x, y \in Z(G)$, entonces $[x,w] = [w,x] = [y,w] = [w,y] = I_G$, vale para cada $w \in G$. Pero, para cada $w \in G$, tenemos que $x * [x^{-1} : w] * X^{-1} = [w,x] = I_G$ asegurando que $[x^{-1} : w] = I_G$ y, como consecuencia, $x^{-1} \in Z(G)$. También, para cada $w \in G$, tenemos que $[x * y, w] = [x,w] = I_G$ y, como consecuencia, $x * y \in Z(G)$. Hemos verificado que $Z(G)$ es un subgrupo de G.

Sea $g \in G$, $x \in Z(G)$. entonces $[g * x * g^{-1}, y] = g * x * g^{-1} * y * g * x^{-1} * g^{-1} * y^{-1}$. Pero $x \in Z(G)$ dice que x conmuta con cada elemento de G, luego $[g * x * g^{-1}, y] = I_G$, es decir, $g * x * g^{-1} \in Z(G)$, con lo cual obtenemos la normalidad de $Z(G)$ en G. □

Observemos que si G es Abeliano, entonces $Z(G) = G$. Recíprocamente, si $Z(G) = G$, entonces $[y, x] = I_G$ es válido para todo $x, y \in G$, es decir, G es Abeliano ; luego tenemos el siguiente.

Proposición 7.0.76. — *Un grupo $(G, *)$ es Abeliano sí y sólo si $Z(G) = G$.*

Proposición 7.0.77. — *Si $(G, *)$ no es un grupo Abeliano, entonces $G/Z(G)$ no puede ser un grupo cíclico. En particular, $[G : Z(G)]$ no puede ser un primo.*

Demonstración. — Sea $(G, *)$ un grupo que no es Abeliano, es decir $G \neq Z(G)$. Supongamos por el contrario que $G/Z(G)$ es un grupo cíclico. Podemos escoger $u \in G - Z(G)$ tal que $uZ(G)$ genera $G/Z(G)$. Tomemos un elemento $x \in G - Z(G)$. Existe $a \in \{1, 2, ..., p-1\}$ tal que $xZ(G) = u^a Z(G)$. Para cada $y \in Z(G)$ tenemos $[x : y] = I_G$. Para $y \in G - Z(G)$ tenemos que $yZ(G) = u^b Z(G)$, para cierto $b \in \{1, ..., p-1\}$. Esto nos dice que podemos encontrar $z, w \in Z(G)$ tales que $x = u^a * z$, $y = u^b * w$. En particular,

$$[x : y] = (u^a * z) * (u^b * w) * (u^a * z)^{-1} * (u^b * w)^{-1} =$$
$$= u^a * z * u^b * w * z^{-1} * u^{-a} * w^{-1} * u^{-b} = u^{a+b-a-b} = I_G$$

Como consecuencia, $x \in Z(G)$, una contradicción. □

Proposición 7.0.78. — *Sea G un grupo finito y $x_1, x_2 \in G$ elementos de orden 2 tales que $x_1 * x_2$ tiene orden n. Entonces $Z(G; x_j)$ tiene orden a lo más $2|G|/n$, para $j = 1, 2$.*

Demonstración. — Sea H el subgrupo de G generado por x_1 y x_2. Denotemos por D_n el grupo dihedral de orden $2n$ generado por a y b, con las relaciones

$$a^n = b^2 = (ab)^2 = 1$$

Entonces tenemos un homomorfismo sobreyectivo $\phi : D_n \to H$, definido por : $\phi(b) = x_1$ y $\phi(a) = x_2 * x_1$. Ahora, el núcleo de ϕ es un subgrupo normal de D_n. Pero los únicos subgrupo normales de D_n son los subgrupos triviales $\{1\}$, D_n y los subgrupos cíclicos generados por una potencia no trivial de a. Los últimos dos casos obligarán tener que el cociente $D_n/Ker(\phi) \cong H$ es trivial ó el elemento a se proyecta a un elemento de orden menor a n, una contradicción. Luego $\phi : D_n \to H$ es un isomorfismo. Ahora, se puede verificar que $Z(H; x_j)$ es isomorfo a $\mathbb{Z}/2\mathbb{Z}$ si n es impar ó bién isomorfo a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ si n es par. En cualquier caso, el orden de $Z(H; x_j)$ es a lo más 4.
Consideremos una descomposición en clases laterales izquierda de G por H, es decir

$$G = H * z_1 \cup H * z_2 \cup H * z_3 \cup \cdots \cup H * z_n$$

donde $n = [G : H]$ y $z_1 = I_G$. Tenemos que $Z(G; x_j) \cap H = Z(H; x_j)$. Supongamos que tenemos dos elementos de $Z(G; x_j)$ en la misma $H * z_l$, digamos $g_1 = h_1 * z_l, g_2 = h_2 * z_l \in Z(G; x_j)$. Entonces $h_1 * h_2^{-1} = g_1 * g_2^{-1} \in H \cap Z(G; x_j) = Z(H; x_j)$. Luego el orden de $Z(G; x_j) \cap H * z_l$ es el mismo orden de $Z(H; x_j)$. Como tenemos la descomposición disjunta

$$Z(G; x_j) = (Z(G; x_j) \cap H) \cup (Z(G; x_j) \cap H * z_2) \cup \cdots \cup (Z(G; x_j) \cap H * z_n),$$

tenemos de lo anterior que el orden de $Z(G; x_j)$ es igual a $[G : H]$ veces el orden de $Z(H; x_j)$, es decir a lo más $4|G|/|H| = 2|G|/n$. □

Ejemplo 7.0.79. — Consideremos un grupo $(G, *)$ y denotemos por G_{tor} el subgrupo generado por todos los elementos de orden finito de G. Si h tiene orden finito y $g \in G$, entonces $g * h * g^{-1}$ tiene el mismo orden finito que h. Como los elementos de G_{tor} son de la forma $x_1 * x_2 * \cdots * x_n$, donde $x_j \in G$ tienen orden finito, obtenemos que G_{tor} es un subgrupo normal de G. Es claro que si G es de orden finito, entonces $G = G_{tor}$. Podemos tener grupos G de orden infinito con $G = G_{tor}$, por ejemplo, considere G el grupo generado por las reflexiones de Möbius $A(z) = -\overline{z}$ y $B(z) = -\overline{z} + 1$. Este grupo contiene a la translación $B \circ A(z) = z + 1$ y luego G es infinito. Por otro lado, $A, B \in G_{tor}$ asegura que $G = G_{tor}$. De manera más general, si G puede ser generado por elementos de ordenes finito, entonces $G = G_{tor}$. Si G no contiene elementos de orden finito diferentes del neutro, entonces $G_{tor} = \{I_G\}$. Un grupo que tiene la propiedad que sus elementos diferentes de la identidad no tienen orden finito, es decir, $G_{tor} = \{I_G\}$ son llamados *grupos sin torsión*.

Dado un subgrupo H de un grupo dado $(G, *)$, lo más probable que ocurra es que H no sea un subgrupo normal de G. Una de las cosas que podemos hacer es considerar el subgrupo normal más pequeño de G que contenga a H,

$$\langle\langle H \rangle\rangle$$

el cual resulta ser la intersección de todos los subgrupos normales de G que contienen a H. Tal colección sobre la que hacemos la intersección no es vacía ya que G pertenece trivialmente a esta. Llamamos a tal subgrupo normal la *cápsula normal* del subgrupo H. El siguiente es claro por la definición.

Proposición 7.0.80. — *$H = \langle\langle H \rangle\rangle$ sí y sólo si H es subgrupo normal de G.*

Otra cosa que podemos hacer es considerar el *normalizador* de H, definido por

$$N_G(H) = \{g \in G : g * H * g^{-1} = H\}$$

Puede ocurrir que $N_G(H)$ no sea un subgrupo normal de G. Es claro que cada $h \in H$ debe pertenecer a $N_G(H)$, ya que si $t \in H$, entonces $h^{-1} * t * h \in H$ y luego $h * (h^{-1} * t * h) * h^{-1} = t$. De esta manera, H es un subgrupo de $N_G(H)$. Como cada elemento de $N_G(H)$ tiene la propiedad de conjugar H en si mismo, obtenemos que :

Proposición 7.0.81. — *H es subgrupo normal de $N_G(H)$.*

CAPÍTULO 8

PRODUCTOS DE GRUPOS

8.1. Producto Directo de Grupos

Una de las maneras de producir nuevos grupos a partir de algunos dados es por medio del producto directo. Sea $\{(G_j, *_j) : j \in J\}$ una colección no vacía de grupos (finita o infinita). Formemos el producto cartesiano

$$\prod_{j\in J} G_j = \{f : J \to \bigcup_{j\in J} G_j : f(j) \in G_j\}$$

La operación binaria es dada por

$$f * g(j) = f_j *_j g_j$$

Proposición 8.1.1. — *La operación binaria así definida define en* $\prod_{j\in J} G_j$ *una estructura de grupo, llamado el* producto directo *de los grupos* G_j, $j \in J$.

Demonstración. — La asociatividad es equivalente a la asociatividad coordenada a coordenada. El neutro es dado por I, donde $I(j) = I_{G_j}$. El inverso de cada $f \in \prod_{j\in J} G_j$ es dado por $f^{-1}(j) = f_j^{-1}$. □

Observación 8.1.2. — Cuando cada grupo G_j es un grupo Abeliano, usualmente hablamos de la en vez del producto directo y se acostumbra a denotarlo por

$$\bigoplus_{j\in G} G_j$$

Ejercicio 42. — *Supongamos que* G_k, $k = 1, 2, 3, ..., n$ *son* n *grupos finitos. Verificar que* $|\prod_{j=1}^{n} G_j| = \prod_{j=1}^{n} |G_j|$.

Por cada $k \in J$ tenemos de manera natural la inclusión

$$i_k : G_k \to \prod_{j\in J} G_j$$

definido por

$$i_k(x) : J \to \prod_{j\in J} G_j : j \to \begin{cases} I_{G_j} & j \neq k \\ x & j = k \end{cases}$$

Ejercicio 43. — *Verificar que $i_k : G_k \to \prod_{j\in J} G_j$ es un monomorfismo, con lo cual podemos mirar cada G_k como subgrupo de su producto directo.*

Proposición 8.1.3. — *Consideremos dos grupos cíclicos $(H, *)$ y $(K, \cdot)$ de ordenes p y q, respectivamente. Supongamos que p y q son relativamente primos, es decir el único factor positivo entero común es 1. Entonces el producto directo $H \times K$ es un grupo cíclico de orden pq.*

Demonstración. — Consideremos dos números enteros positivos p, q que sean relativamente primos, es decir no hay factores positivos comunes diferentes de 1. Sea $(Z, \diamond)$ un grupo cíclico de orden pq. Sean x, y y w generadores de H, K y Z, respectivamente. Consideremos la función

$$\phi : H \times K \to Z : (x^a, y^b) \mapsto w^{aq+bp}$$

Este es claramente un homomorfismo de grupos. Por otro lado, si $\phi(x^a, y^b) = I_Z$, entonces $aq + bp \equiv 0$ módulo pq. Luego, p/aq y q/bp y, como p y q son relativamente primos, tenemos que p/a y q/b, es decir, $x^a = I_H$ y también $y^b = I_K$. De esta manera obtenemos que ϕ es un monomorfismo. Como la cardinalidad de $H \times K$ y Z es la misma, pq, tenemos gratis la sobreyectividad y luego el isomorfismo deseado. □

8.2. Producto Débil de Grupos

Al igual que en la sección anterior, consideremos una colección de grupos $\{(G_j, *_j) : j \in J\}$ y consideremos su producto directo $\prod_{j\in J} G_j$. El subconjunto

$$\prod_{j\in J}^{debil} G_j$$

de $\prod_{j\in J} G_j$ definido por aquellas funciones $f : J \to \bigcup_{j\in J} G_j$ tales que $f(j) \in G_j$, para cada $j \in J$ y $f(j) = I_{G_j}$ con la posible excepción de un número finito de valores de j, resulta ser un subgrupo, llamado el *producto débil* de los grupos G_j, $j \in J$. Observemos que si $\#J < \infty$, entonces el producto directo y el producto débil coinciden.

Ejercicio 44. — *Verificar que $\prod_{j\in J}^{debil} G_j$ es en efecto un subgrupo de $\prod_{j\in J} G_j$.*

Ejemplo 8.2.1. — Los productos débiles de grupos Abelianos tienen cierta propiedad universal que pasamos a ver. Supongamos que tenemos una colección de grupos Abelianos $\{(G_j, *_j) : j \in J\}$ y consideremos su producto débil $G = \prod_{j\in J} G_j$. Es claro que G (de hecho el producto directo) es un grupo Abeliano. Supongamos que tenemos un grupo Abeliano K y una colección de homomorfismos $\phi_j : G_j \to A$, para cada $j \in J$. Por cada $f \in \prod_{j\in J}^{debil} G_j$ podemos considerar el producto $h(f) = \prod_{j\in G} \phi_j(f(j))$ (el producto en la operación binaria de K), el cual tiene sentido ya que, excepto por un número finito de ídices $j \in J$, vale que $\phi_j(f(j)) = I_K$, y los grupos involucrados al ser Abelianos no importa el orden para el producto. Se puede verificar que $h : G \to K$ es un homomorfismo que satisface $h \circ i_j = \phi j$, para todo $j \in J$.

Ejercicio 45. — *Completar los detalles del ejemplo anterior y deducir que $h : G \to K$ es único con la propiedad de ser homomorfismo y $h \circ i_j = \phi j$, para todo $j \in J$.*

8.3. Producto Directo Interno

Supongamos que tenemos un grupo $(G, *)$ y una colección de subgrupos $\{H_j : j = 1, 2, ..., n\}$. Diremos que G es *producto directo interno* de los subgrupos H_j, $j = 1, 2, ..., n$, si

$$\phi : \prod_{j\in\{1,2,...,n\}} H_j \to G : f \mapsto \prod_{j=1}^{n} f(j) = f(1) * f(2) * \cdots * f(j)$$

resulta ser un isomorfismo. De esta definición es claro que cada elemento $g \in G$ se puede escribir de manera única como $g = h_1 * h_2 * \cdots * h_n$, donde $h_j \in H_j$.

8.4. Producto Semidirecto de Grupos

Consideremos dos grupos $(H, *)$, $(K, \circ)$ y un homomorfismo de grupos $\phi : K \to Aut(H)$. El conjunto $K \times H$ junto con la operación binaria

$$(k_1, h_1) \cdot_\phi (k_2, h_2) = (k_1 \circ k_2, h_1 * \phi(k_1)(h_2))$$

resulta ser un grupo llamado el *producto semidirecto* de los grupos K y H el cual denotamos por $G = K \ltimes H$. En este caso, el elemento neutro es dado por $(1_K, 1_H)$, donde 1_K y 1_H denotan los elementos neutros de K y H, respectivamente. El elemento inverso de (k, h) es dado por $(k^{-1}, \phi(k^{-1})(h^{-1}))$. Observemos también que $\{1_K\} \times H$ y $K \times \{1_H\}$ resultan ser subgrupos de $K \ltimes H$ y se tiene que las inclusiones

$$j_H : H \to \{1_K\} \times H : h \mapsto (1_K, h)$$

$$j_K : K \to K \times \{1_H\} : k \mapsto (k, 1_H)$$

resultan ser isomorfismos. Más aún, el subgrupo $j_H(H) = \{1_K\} \times H$ resulta ser un subgrupo normal de $K \ltimes H$.

Ejercicio 46. — *Verificar que*

(i) la operación binaria $\cdot_\phi$ define una estructura de grupo ;

(ii) las funciones j_H y j_K son efectivamente isomorfismos ;

(iii) $j_H(H)$ es subgrupo normal de $K \ltimes H$.

Ejemplo 8.4.1. — Supongamos que tenemos un grupo $(G, *)$ que contenga dos subgrupos H y K, donde H es normal en G, $H \cap K = \{1_G\}$ y $G = HK$. Consideremos el homomorfismo de grupos $\phi : K \to Aut(H)$ donde $\phi(k)(h) = k * h * k^{-1}$ y formemos el producto semidirecto $K \ltimes H$. Tenemos que $\phi : K \ltimes H \to G : (k, h) \to k * h$ resulta ser un isomorfismo de grupos. Diremos que G es el *producto semidirecto interno* de K y G.

Ejercicio 47. —
(1) Completar los detalles del ejemplo anterior.

(2) Sean G un grupo abeliano, H y K subgrupos de G tales que $G = HK$ y $H \cap K = \{1_G\}$. Verificar que $G \cong H \times K$.

(3) Sea G un grupo, $H, K < G$ tales que $H \lhd G$ y $HK = G$. Verificar que $\psi : K \ltimes H \to G : (k, h) \mapsto kh$ define un isomorfismo.

(4) Sean H, G, K grupos, $i : H \to G$, $\pi : G \to K$, $\tau : K \to G$ homomorfismos de grupos tales que :
(i) i es inyectivo ;
(ii) π es sobreyectivo ;
(iii) $i(H) = Ker(\pi)$;
(iv) $\pi \circ \tau = I_K$.
Las condiciones (i), (ii) y (iii) dicen que la sucesión corta siguiente es exacta.

$$1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$$

Verificar que $\psi : K \ltimes H \to G : (k, h) \mapsto \tau(k)h$ define un isomorfismo.

CAPÍTULO 9

PRODUCTO LIBRE DE GRUPOS

Ahora procederemos a generar un nuevo grupo a partir de unos ya dados, pero de manera de no producir nuevas relaciones entre los elementos. En el caso de productos directos o débiles, por ejemplo, cuando los grupos involucrados son Abelianos, el resultado nos da un grupo Abeliano, es decir hay más relaciones que las originales (sólo valían en cada grupo).

Nuevamente, consideremos una colección no vacía de grupos $\{(G_j, *_j) : j \in J\}$. Definimos una *palabra reducida* (en estos grupos) de *longitud* $n > 0$ a una sucesión finita $(x_1, ..., x_n)$, donde cada x_j pertenece a alguno de nuestros grupos y tienen las siguientes dos propiedades :

(i) ningún x_j es el neutro del grupo a cual pertenece ; y

(ii) dos términos consecutivos no pertenecen al mismo grupo.

Denotaremos por 1 la palabra de longitud 0 (usualmente llamada la palabra vacía). Sea G la colección de tales palabras. Ahora procederemos a construir una operación $\cdot$ binaria sobre este conjunto.

$$1 \cdot 1 := 1$$
$$1 \cdot (x_1, ..., x_n) := (x_1, ..., x_n)$$
$$(x_1, ..., x_n) \cdot 1 := (x_1, ..., x_n)$$

Ahora supongamos que tenemos dos palabras de longitudes positivas, digamos $(x_1, ..., x_n)$ y $(y_1, ..., y_m)$. Queremos definir

$$(x_1, ..., x_n) \cdot (y_1, ..., y_m)$$

Caso 1 : Si x_n y y_1 no pertenecen al mismo grupo, entonces definimos

$$(x_1, ..., x_n) \cdot (y_1, ..., y_m) = (x_1, ..., x_n, y_1, ..., y_m)$$

Caso 2 : Si x_n y y_1 pertenecen al mismo grupo G_j, pero $x_n *_j y_1 \neq I_{G_j}$, entonces definimos

$$(x_1, ..., x_n) \cdot (y_1, ..., y_m) = (x_1, ..., x_{n-1}, x_n *_j y_1, y_2..., y_m)$$

Caso 3 : Si x_n y y_1 pertenecen al mismo grupo G_j, $x_n *_j y_1 = I_{G_j}$, entonces exigimos, siguiendo las definiciones anteriores,

$$(x_1, ..., x_n) \cdot (y_1, ..., y_m) = (x_1, ..., x_{n-1}) \cdot (y_2, ..., y_m)$$

La operación binaria que hemos definido recibe también el nombre de *yuxtaposición*. Observemos que la,operación binaria es asociativa por definición, 1 es neutro y cada palabra reducida $(x_1, ..., x_n)$ tiene como inversa (respecto a esta operación) a la palabra reducida $(x_n^{-1}, ..., x_1^{-1})$.

Definición 9.0.2. — Al grupo obtenido de esta manera es llamado el *producto libre* de los grupos $\{(G_j, *_j) : j \in J\}$.

Notación. Desde ahora en adelante identificaremos cada palabra reducida $(x_1, ..., x_n)$, de longitud $n > 0$, con $x_1 x_2 \cdots x_n$ (es decir, no haremos uso del símbolo " $\cdot$ " ni de los paréntesis.

Observación 9.0.3. — Cuando tenemos un número finito de grupos, G_1,..., G_n, entonces se estila usar la notación

$$G_1 * G_2 * \cdots * G_n$$

para denotar su producto libre. Observemos que la definición del producto libre no depende de ningún orden en los grupos factores, es decir, si $\sigma \in \mathcal{S}_n$, entonces

$$G_1 * G_2 * \cdots * G_n = G_{\sigma(1)} * G_{\sigma(2)} * \cdots * G_{\sigma(n)}$$

De manera análoga, para el producto libre arbitrario denotamos este por $\prod_{j \in J} * G_j$.

Ejemplo 9.0.4. — Consideremos $G_1 = \{I_1, x\}$ (es decir, un grupo de orden 2, luego $x^2 = I_1$) y $G_2 = \{I_2, y, y^2\}$ (es decir, un grupo de orden 3, luego $y^3 = I_2$). Entonces una lista de algunas de las palabras reducidas de $G_1 * G_2$ son las siguientes :
Longitud 0 : 1
Longitud 1 : x, y, $y^2 = y^{-1}$
Longitud 2 : xy, xy^2, yx, y^2x

Una propiedad universal del producto libre de grupos es el siguiente. Consideremos una colección de grupos $\{(G_j, *_j) : j \in J\}$ y su producto libre de grupos $\prod_{j \in J} * G_j$. Entonces, por cada $k \in J$ tenemos naturalmente un monomorfismo $i_k : G_k \to \prod_{j \in J} * G_j$ (a cada $x \in G_k - \{I_{G_k}\}$ le asigna la palabra x de longitud 1, y a I_{G_k} le asigna 1). Sea $(K, \circ)$ un grupo y supongamos que tenemos homomorfismos $\phi_j : G_j \to K$, para cada $j \in J$. Definamos la función $h : \prod_{j \in J} * G_j \to K$ de la siguiente manera. $h(1) = I_K$, y si $x_1 x_2 \cdots x_n$ es una palabra reducida de longitud $n > 0$, donde $x_r \in G_{j_r}$, entonces $h(x_1 x_2 \cdots x_n) = \phi_{j_1}(x_1) \circ \phi_{j_2}(x_2) \circ \cdots \circ \phi_{j_n}(x_n)$. Resulta que h es un homomorfismo que satisface que $h \circ i_j = \phi_j$, para cada $j \in J$.

Ejercicio 48. — *Verificar que h es en efecto un homomorfismo de grupos y que está únicamente definido por la condición $h \circ i_j = \phi_j$, para cada $j \in J$.*

Ejemplo 9.0.5. — Consideremos un espacio topológico (X, τ) arco-conexo y localmente arco-conexo. Sean A, B abiertos arconexos tales que $A \cup B = X$ y $A \cap B$ sea arco-conexo y simplemente conexo. Entonces, si $p \in A \cap B$, tenemos que

$$\pi_1(X, p) = \pi_1(A, p) * \phi_1(B, p)$$

CAPÍTULO 10

PRODUCTO LIBRE AMALGAMADO

Consideremos dos grupos $(G_1, *_1)$, $(G_2, *_2)$ y subgrupos $H_j < G_j$, para $j = 1, 2$. Supongamos que tenemos un isomorfimo de grupos

$$\phi : H_1 \to H_2$$

En el producto libre $G_1 * G_2$ consideremos el subgrupo normal más pequeño K que contega todas las palabras de la forma

$$h^{-1}\phi(h), \text{ donde } h \in H_1$$

Definición 10.0.6. — El grupo cociente

$$G_1 *_\phi G_2 = G_1 * G_2/K$$

es llamado el *producto libre amalgamado por* $\phi : H_1 \to H_2$.

Observemos que si $H_1 = \{I_{G_1}\}$, entonces $G_1 *_\phi G_2 = G_1 * G_2$.

Ejemplo 10.0.7. — Consideremos un espacio topológico (X, τ) arco-conexo y localmente arco-conexo. Sean A, B abiertos arconexos tales que $A \cup B = X$ y $A \cap B$ sea arco-conexo. Entonces, si $p \in A \cap B$, tenemos que

$$\pi_1(X, p) = \pi_1(A, p) *_\phi \phi_1(B, p)$$

donde $\phi : \pi_1(A \cap B, p) < \pi_1(A, p) < \pi_1(A \cup B, p) \to \pi_1(A \cap B, p) < \pi_1(B, p) < \pi_1(A \cup B, p)$ es el isomorfismo de amalgación.

CAPÍTULO 11

HNN-EXTENSIÓN

Sean $(G, *)$ un grupo y H, K dos subgrupos de G. Supongamos que tenemos un isomorfismo $\phi : H \to K$. Consideremos un grupo cíclico infinito $\langle t \rangle$.
En el producto libre $G * \langle t \rangle$ consideremos el subgrupo normal más pequeño K que contega todas las palabras de la forma

$$tht^{-1}\phi(h)^{-1}, \text{ donde } h \in H$$

Definición 11.0.8. — El grupo cociente

$$G*_{\phi} = G * \langle t \rangle / K$$

es llamado la *HNN-extensión de G por $\phi : H \to K$*.

Ejemplo 11.0.9. — Consideremos un espacio topológico (X, τ) arco-conexo y localmente arco-conexo. Sean A, B abiertos arconexos tales que $A \cap B = \emptyset$. Supongamos que tenemos un homeomorfismo $F : A \to B$ y consideramos el espacio topológico X_F obtenido al identificar cada punto $a \in A$ con cada punto $F(a) \in B$. Entonces, si $p \in X_F$, tenemos que

$$\pi_1(X_F, p) = \pi_1(X, p)*_{\phi}$$

donde $\phi : \pi_1(A, p) < \pi_1(X, p) \to \pi_1(B, p) < \pi_1(X, p)$ es el isomorfismo de HNN-extensión.

CAPÍTULO 12

GRUPOS LIBRES

La construcción anterior de productos libres podemos usarla para construir cierto grupo a partir de un conjunto dado S. Este grupo tiene la propiedad de ser generado por S y ser el *más grande* con tal propiedad.
Supongamos que $S = \{x_j : j \in J\} \neq \emptyset$. Entonces por cada $j \in J$ definimos el grupo

$$F_j = \{1_j = x_j^0, x_j^{\pm 1}, x_j^{\pm 2}, ..., x_j^{\pm n}, ...\}$$

con la operación binaria $*_j$ definida por

$$1_j *_j 1_j = 1_j$$

$$1_j *_j x_j^n = x_j^n = x_j^n *_j 1_j$$

$$x_j^n *_j x_j^m = x_j^{n+m}$$

Ejercicio 49. — *Verificar que $(F_j, *_j)$ es un grupo cíclico infinito generado por x_j, luego isomorfo al grupo aditivo $\mathbb{Z}$. Establecer dicho isomorfismo.*

Definición 12.0.10. — Consideremos un conjunto no vacío $S = \{x_j : j \in J\} \neq \emptyset$ y $\{(F_j, *_j) : j \in J\}$ los grupos cíclicos arriba construidos. El producto libre

$$F(S) = \prod_{j \in J} * F_j$$

es llamado el *grupo libre* generado por S. La cardinalidad de S es llamado el *rango del grupo libre generado por S*.

Por la propiedad universal vista para los productos libres, vemos que si $(K, \%)$ es cualquier grupo para el cual existe un monomorfismo desde cada F_j hacia este, entonces existe un homomorfismo desde $\prod_{j \in J} * F_j$ hacia K. Esto dice que el grupo libre es el grupo más grande posible respecto al conjunto de generadores S.

Ejercicio 50. — *Verificar que todo grupo libre de rango* 1 *es isomorfo al grupo aditivo* $\mathbb{Z}$.

CAPÍTULO 13

GRUPOS ABELIANOS FINITAMENTE GENERADOS

13.1. Grupos Abelianos Libres

Dado un conjunto $S = \{x_j : j \in J\} \neq \emptyset$, consideremos el grupo libre generado por S, es decir $F(S)$. Este grupo no es Abeliano y de hecho no hay relaciones entre los diferentes generadores x_j.

Definición 13.1.1. — La abelianización de $F(S)$, es decir

$$F(S)^{abel} = F(S)/[F(S), F(S)]$$

es llamado el *grupo libre abeliano* generado por el conjunto S. El rango de $F(S)^{abel}$ es el rango de $F(S)$, es decir, la cardinalidad de S.

Ejercicio 51. — *Sea $S = \{x_1, ..., x_n\}$. Verifique que*

$$F(S)^{abel} \cong \bigoplus_{j=1}^{n} \mathbb{Z}$$

Supongamos que tenemos un grupo Abeliano $(G, *)$ que es generado por el conjunto $\{x_j : j \in J\} \subset G$. Consideremos un conjunto $S = \{y_j : j \in J\}$ y formemos el grupo libre $F(S)$. Entonces tenemos un homomorfismo sobreyectivo natural dado por

$$\phi : F(S) \to G$$

definido por la propiedad que $\phi(y_j) = x_j$, $j \in J$. Entonces tenemos que el subgrupo de conmutadores $[F(S), F(S)]$ es subgrupo del núcleo de tal homomorfismo, es decir, tenemos inducido un homomorfismo sobreyectivo

$$\phi^{abel} : F(S)^{abel} \to G$$

El núcleo K de ϕ^{abel} es exactamente $\pi_{[F(S),F(S)]}(\text{Ker}(\phi))$, donde $\pi_{[F(S),F(S)]} : F(S) \to F(S)^{abel}$ es la proyección natural. Tenemos ahora un isomorfismo

$$G \cong F(S)^{abel}/K$$

13.2. Grupos Abelianos Finitamente Generados

En el caso particular que $(G,*)$ es grupo Abeliano finitamente generado, digamos por x_1,...,x_n, entonces de lo anterior tenemos que

$$G \cong \left(\bigoplus_{j=1}^{n} \mathbb{Z} \right) / K$$

es decir, G es la imágen homomorfa de un grupo Abeliano libre de rango finito. Ahora, en este caso, tenemos el siguiente resultado que puede encontrarse en [**3**].

Proposición 13.2.1. — *Sea F un grupo abeliano libre de rango finito n y K un subgrupo no trivial de G. Entonces existen una base $\{x_1, ..., x_n\}$ de F y enteros positivos d_1,..., d_s, para cierto $s \leq n$, de manera que d_j divide d_{j+1} y K tiene base dada por $\{x_1^{d_1}, ..., x_s^{d_s}\}$. En particular,*

$$F/K \cong \left(\bigoplus_{j=1}^{n-s} \mathbb{Z} \right) \oplus \left(\bigoplus_{k=1}^{s} \mathbb{Z}/d_k\mathbb{Z} \right)$$

Luego, como consecuencia de la proposición 13.2.1, tenemos que

$$G \cong \left(\bigoplus_{j=1}^{l} \mathbb{Z} \right) \oplus \left(\bigoplus_{k=1}^{s} \mathbb{Z}/d_k\mathbb{Z} \right),$$

donde d_1,...., d_s son enteros positivos tales que d_j divide d_{j+1}. Observemos que necesariamente en este caso tenemos

$$G_{tor} = \bigoplus_{k=1}^{s} \mathbb{Z}/d_k\mathbb{Z}.$$

CAPÍTULO 14

GRUPOS COMO COCIENTE DE GRUPOS LIBRES

Consideremos un conjunto $S \neq \emptyset$ y el grupo libre $F(S)$ generado por S. En la sección anterior usamos el subgrupo normal dado por los conmutadores, es decir $[F(S), F(S)]$ para obtener un grupo Abeliano $F(S)^{abel} = F(S)/[F(S), F(S)]$. De manera más general, supongamos que tenemos dado un subgrupo normal de $F(S)$, digamos N, entonces tenemos un grupo cociente $G = F(S)/N$ y un homomorfismo sobreyectivo natural $\pi_N : F(S) \to G$. Tenemos que $\pi_N(S) \subset G$ es un conjunto de generadores de G. Cada palabra $w \in N$ determina una relación entre los generadores inducidos por S en G y estas son todas. De hecho, no es necesario considerar todas las palabras de N para ver todas las relaciones en G; basta considerar un conjunto $R \subset N$ de generadores de N. Así, todas las relaciones en G son consecuencia de las relaciones en R. Más aún, supongamos que $T \subset R$ es tal que N es el subgrupo normal de $F(S)$ más pequeño que contiene T, entonces todas las relaciones en G son consecuencias de las relaciones inducidas por T.

Ejemplo 14.0.2. — Sea $S = \{x, y\}$ y $F(S) \cong \mathbb{Z} * \mathbb{Z}$ el grupo libre de rango 2 generado por S. Tomemos un entero positivo n y consideremos $T = \{x^2, y^n, (xy)^2 := xyxy\}$. En este caso, el grupo cociente $G = F(S)/N$ está generado por

$$\pi_n(x) = X,\ \pi_N(y) = Y$$

y satisfacen las relaciones

$$X^2 = Y^n = (XY)^2 = 1$$

La relación $(XY)^2$ nos dice que todos los elementos de G pueden escribirse como X^aY^b, donde $a = 0, 1$ y $b = 0, 1, ..., n-1$. Esto nos dice que G tiene a lo más $2n$ elementos. Por otro lado, si dos elementos de esta forma coinciden, entonces debemos tener en $F(S)$ una relación $x^ay^b = 1$, lo cual es sólo posible para $a = b = 0$. En particular, $|G| = 2n$. El grupo que hemos construido es llamado el *grupo dihedral* de orden $2n$ y usualmente denotado por D_n.

Ejercicio 52. —

(1) Sea n un entero positivo y sean las siguientes transformaciones de Möbius $U(z) = e^{\pi i/2n}z$ y $V(z) = 1/z$. Considere el subgrupo de $Perm(\mathbb{C})$ H generado por U y V. Verifique que $H \cong D_n$.

(2) Considere un polígono regular $P \subset \mathbb{R}^2$ de $n \geq 3$ lados. Considere el grupo de isometrías de P respecto al producto interior usual, digamos $Isom(P)$. Verificar que $Isom(P)$ contiene un subgrupo de índice dos (luego normal) que es isomorfo a D_n.

Ejemplo 14.0.3. — Sea $S = \{x\}$ y $F(S) \cong \mathbb{Z}$ el grupo libre generado por S. Sea $T = \{x^n\}$, para algún $n \in \{1, 2, 3, ...\}$. Entonces $G = F(S)/N$ resulta ser un grupo cíclico de orden n.

En forma recíproca, partamos de un grupo $(G, *)$ y tomemos un conjunto S de generadores de G. Formemos el grupo libre $F(S)$ generado por S y consideremos la función

$$Q : F(S) \to G$$

definida por la regla

$$Q(1) = I_G$$
$$Q(x_1x_2 \cdots x_n) = x_1 * x_2 * \cdots * x_n$$

Ejercicio 53. — *Verificar que Q es un homomorfismo sobreyectivo.*

Sea $N = \text{Ker}(Q)$. Entonces tenemos que $F(S)/\text{Ker}(Q) \cong G$, es decir, todo grupo puede obtenerse por el procedimiento anterior. Lo más importante de todo lo dicho en esta sección es que cada grupo puede ser representado por medio de

Generadores y Relaciones

es decir, de la forma

$$G = \langle S, T \rangle$$

Ejemplo 14.0.4. —

$$D_n = \langle X, Y : X^2, Y^n, (XY)^n \rangle$$

el grupo dihedral de orden $2n$, que resulta ser el grupo de isometrías Euclidianas de un polígono regular plano de n lados,

$$\mathbb{Z}/n\mathbb{Z} = \langle A : A^n \rangle = \langle U, V : U^n, UV \rangle$$

el grupo cíclico finito de orden n, que resulta ser el grupo de isometrías Euclidianas de los rayos que unen $(0, 0)$ con cada raíz $n-$ésima de la unidad,

$$\mathcal{A}_4 = \langle A, B : A^3, B^2, (AB)^3 \rangle$$

este grupo es llamado el grupo alternante en cuatro letras y resulta ser el grupo de isometrías Euclidianas de una pirámide regular centrada en $(0, 0, 0) \in \mathbb{R}^3$,

$$\mathcal{S}_4 = \langle A, B : A^4, B^2, (AB)^3 \rangle$$

este grupo es el grupo simétrico en cuatro letras (isomorfo a $Perm(\{1,2,3,4\})$) y resulta ser el grupo de isometrías Euclidianas de un cubo regular centrado en $(0,0,0) \in \mathbb{R}^3$,

$$\mathcal{A}_5 = \langle A, B : A^5, B^2, (AB)^3 \rangle$$

este grupo es llamado el grupo alternante en cinco letras y resulta ser el grupo de isometrías Euclidianas de un icosaedro regular centrado en $(0,0,0) \in \mathbb{R}^3$.

Ejercicio 54. — *Calcular las tablas de multiplicación de cada uno de los grupos anteriores y determinar sus órdenes. Represente estos grupos por medio de transformaciones (extendidas) de Möbius y también por rotaciones espaciales.*

CAPÍTULO 15

GRUPOS DE PERMUTACIONES FINITOS

Como hemos visto al comienzo de estas notas, podemos mirar todo grupo como subgrupo de un grupo de permutaciones $Perm(X)$ para cierto conjunto no vacío X. Esto nos está diciendo que sería bueno el poder entender un poco más tales grupos. Para simplificar el trabajo, consideraremos sólo conjuntos finitos. Como todo conjunto X finito de cardinalidad $n > 0$ es biyectivo al conjunto $\{1, 2, 3, ..., n\}$, y tenemos que en este caso $Perm(X)$ y $Perm(\{1, 2, ..., n\})$ son necesariamente isomorfos, bastará considerar $X = \{1, 2, ..., n\}$. Como habíamos dicho antes, usaremos el símbolo $\mathcal{S}_n$ para denotar $Perm(\{1, 2, ..., n\})$. Este grupo recibe también el nombre de *grupo simétrico* de n letras. Antes que nada, veamos algunas notaciones que nos simplificarán el trabajo.

Definición 15.0.5. — El símbolo $(a_1, a_2, ..., a_k)$, donde $k \in \{2, 3, ..., n\}$, $a_j \in \{1, 2, ..., n\}$ y $a_j \neq a_r$ para $j \neq r$, denotará la permutación que envía a_1 en a_2, a_2 en a_3,..., a_{k-1} en a_k, a_k en a_1 y fija todos los otros elementos. Este es llamado un *cíclo* de longitud k. Cuando $k = 2$ hablamos de *transposiciones* en vez de decir un cíclo de longitud dos.

La operación de dos cíclos corresponde a la composición de las dos permutaciones que definen, es decir de derecha hacia la izquierda, por ejemplo $(1, 2)(2, 3) = (1, 2, 3)$, $(2, 3)(1, 2) = (1, 3, 2)$.

Ejercicio 55. — *Calcular la cantidad de cíclos de logitud $k \in \{2, 3, ..., n\}$ que hay en $\mathcal{S}_n$.*

Ejemplo 15.0.6. — Consideremos $n = 3$. En este caso tenemos que $\mathcal{S}_3$ está formado por el neutro I, las transposiciones $a = (1, 2)$, $b = (1, 3)$, $c = (2, 3)$ y los cíclos de longitud tres $d = (1, 2, 3)$ y $e = (1, 3, 2)$. Observemos que $e = d^{-1}$, $dad^{-1} = c$ y $d^{-1}ad = b$. Es decir que $\mathcal{S}_3$ está generado por a y d. Observemos que valen las relaciones $a^2 = I$, $d^3 = I$ y como $ad = (2, 3)$, entonces $(ad)^2 = I$.

Ejercicio 56. — *Verificar que toda otra relación $\mathcal{S}_3$ es consecuencia de las tres relaciones dadas en ele ejemplo anterior. Verifique que existe un isomorfismo entre $\mathcal{S}_3$ y el grupo dihedral D_3.*

Ahora, si consideramos una permutación $\sigma \in \mathcal{S}_n$, entonces podemos escribirla como producto de un número finito y disjunto de cíclos. Para ver esto, primero consideramos el subconjunto $J \subset \{1, 2, ..., n\}$ que son los puntos fijos de la permutación σ. Entonces, tomamos el menor elemento $a_1 \in \{1, 2, ..., n\} - J$ y formamos el cíclo

$$C_1 = (a_1, a_2 = \sigma(a_1), a_3 = \sigma^2(a_1), ..., a_{k_1} = \sigma^{k_1-1}(a_1))$$

donde $\sigma^{k_1}(a_1) = a_1$. Ahora, consideramos el menor elemento de $\{1, 2, ..., n\} - (J \cup \{a_1, a_2, ..., a_k\})$, digamos b_1. Entonces formamos el cíclo

$$C_2 = (b_1, b_2 = \sigma(b_1), b_3 = \sigma^2(b_1), ..., b_{k_2} = \sigma^{k_2-1}(b_1))$$

donde $\sigma^{k_2}(b_1) = b_1$. Como el conjunto $\{1, 2, ..., n\}$ es finito, obtenemos por este procedimiento una colección finita de cíclos, digamos C_1,..., C_r, de respectivas longitudes k_1,..., k_r. La inyectividad de σ asegura que dos cualquiera de tales cíclos deben ser disjuntos. Ahora no es difícil darse cuenta que

$$\sigma = C_1 C_2 \cdots C_r$$

y además el orden de los cíclos no afecta al producto. En particular, hemos obtenido el siguiente resultado.

Proposición 15.0.7. — *El grupo simétrico $\mathcal{S}_n$ está generado por todos su cíclos.*

Por otro lado, cada cíclo puede escribirse como producto de transposiciones. En efecto, consideremos un cíclo $(a_1, ..., a_k)$, entonces tenemos que

$$(a_1, ..., a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)$$

es decir, tenemos el siguiente.

Proposición 15.0.8. — *El grupo simétrico $\mathcal{S}_n$ está generado por todas sus transposiciones.*

Corolario 15.0.9. — *El grupo simétrico $\mathcal{S}_n$ está generado por el cíclo de longitud n dado por $a = (1, 2, 3, ..., n)$ y la transposición $b = (1, 2)$.*

Demonstración. — Primero que nada, observemos que $b_n = a^{-1}ba = (n, 1)$, $b_{n-1} = a^{-2}ba^2 = (n-1, n)$, $b_{n-2} = a^{-3}ba^3 = (n-2, n-1)$,..., $b_2 = aba^{-1} = (2, 3)$. Definamos $b_1 = b$. Segundo, $c_3 = bb_2b = (1, 3)$, $c_4 = c_3b_3c_3 = (1, 4)$, $c_5 = c_4b_4c_4 = (1, 5)$,..., $c_{n-1} = c_{n-2}b_{n-2}c_{n-2} = (1, n-2)$. Hasta ahora hemos logrado obtener todas las transposiciones de la forma $(1, k)$, $k = 2, 3, ..., n$. Ahora, conjugando estas transposiciones

por a^t, donde $t = 1, 2, 3, ..., n-1$, obtendremos todas las transposiciones posibles. El resultado entonces sigue de la proposición anterior. □

Sea $\mathcal{A}_n$ el subconjunto de $\mathcal{S}_n$ formado por todos los productos de un número par de transposiciones junto a la permutación trivial I. Entonces como

$$((a_1, a_2)(a_3, a_4) \cdots (a_{2k+1}, a_{2k}))^{-1} = (a_{2k+1}, a_{2k})(a_{2k-1}, a_{2k-2}) \cdots (a_1, a_2)$$

tenemos que $\mathcal{A}_n$ contiene los inversos de sus elementos. Por otro lado, si hacemos el producto de dos elementos de $\mathcal{A}_n$, entonces el resultado sigue siendo un producto de un número par de transposiciones.

Proposición 15.0.10. — *$\mathcal{A}_n$ es un subgrupo de $\mathcal{S}_n$ llamado el* grupo alternante *en n letras.*

Nuestra definición del grupo alternante $\mathcal{A}_n$ no deja afuera la posibilidad de que sea todo el grupo $\mathcal{S}_n$. El siguiente resultado nos dice que esto no es cierto.

Proposición 15.0.11. — *No es posible escribir una misma permutación como el producto de un número par de ciertas transposiciones y también como el producto de un número impar de otras transposiciones.*

Demonstración. — Supongamos que tenemos una permutación $\sigma \in \mathcal{S}_n$ que puede escribirse de dos maneras diferentes como :

$$\sigma = \theta_1 \theta_2 \cdots \theta_{2k-1}$$

$$\sigma = \mu_1 \mu_2 \cdots \mu_{2r}$$

donde θ_j, μ_l son transposiciones. Entonces tenemos que la identidad $I = \sigma\sigma^{-1}$ de poder escribirse como un producto impar de transposiciones. Supongamos entonces que tenemos

$$I = \tau_1 \tau_2 \cdots \tau_s$$

donde τ_j son transposiciones. Queremos ver que obligatoriamente s debe ser par, dando una contradicción a lo anterior. Sea $m \in \{1, 2, ..., n\}$ tal que aparezca en alguna de las transposiciones τ_j y consideremos τ_{j_m} la primera transposición (de derecha a izquierda) que contenga m. Debemos tener $j_m > 1$ ya que si $j_m = 1$, entonces I no fija a m, una contradicción. Miremos las posibilidades para $\tau_{j_m - 1}\tau_{j_m}$:

$$\begin{aligned}
(m, x)(m, x) &= I \\
(m, y)(m, x) &= (m, x)(x, y) \\
(y, z)(m, x) &= (m, x)(y, z) \\
(x, y)(m, x) &= (m, y)(x, y)
\end{aligned}$$

Esto dice que podemos reemplazar $\tau_{j_m - 1}\tau_{j_m}$ por otro par de transposiciones de manera que ahora la primera transposición (de derecha a izquierda) conteniendo m sea $\tau_{j_m - 1}$, o

bien la cantidad de transposiciones nuevas a decrecido en 2. Además en las nuevas transposiciones sólo aparecen los enteros que ya aparecían en las transposiciones originales. Como no podemos llevar m a la primera transposición, debemos en algún momento hacer decrecer en un número par de transposiciones antes de hacer desaparecer m de todas las nuevas transposiciones. Si procedemos de esta manera por cada valor en las restantes transposiciones y lo eliminamos, entonces la cantidad de transposiciones decrece en un número par positivo. Luego, s debe ser par. □

Por ejemplo, la transposición $(1,2) \notin \mathcal{A}_n$. Pero como el producto de dos permutaciones, cada una de ellas siendo el producto de un número impar de transposiciones, resulta ser un producto de un número par de ellas, obtenemos que $[\mathcal{S} : \mathcal{A}_n] = 2$ y luego $\mathcal{A}_n$ es un subgrupo normal de índice dos en el grupo simétrico $\mathcal{S}_n$. Las permutaciones en $\mathcal{A}_n$ son llamadas *permutaciones pares* y las que no son llamadas *permutaciones impares*.

Proposición 15.0.12. — *El grupo alternante $\mathcal{A}_n$ es un subgrupo normal de $\mathcal{S}_n$, de hecho, un subgrupo de índice dos.*

Demonstración. — Si tomamos dos permutaciones $\sigma \in \mathcal{A}_n$, $\mu \in \mathcal{S}_n$, entonces $\sigma\mu\sigma^{-1}$ es producto par de transposiciones. De esta manera, obtenemos la normalidad. Otra manera de ver esto es que $\mathcal{A}_n$ tiene índice 2 y, como consecuencia de la proposición 6.0.56, este es un subgrupo normal. □

Ya hemos visto que un cíclo de longitud $k \geq 2$ puede escribirse ccomo un producto de $(k-1)$ transposiciones. Luego, todo cíclo de longitud impar pertenece a $\mathcal{A}_n$. Por otro lado, el siguiente resultado dice que todo cíclo de longitud par no puede pertenecer a $\mathcal{A}_n$ ya que este es subgrupo normal diferente a $\mathcal{S}_n$ y este último es generado por todos sus cíclos.

Proposición 15.0.13. — *Todo cíclo de longitud $k \geq 2$ es conjugado al cíclo $(1,2,3,...,k)$.*

Demonstración. — Sea el cíclo $x = (a_1, ..., a_k)$ y considere cualquier permutación σ que satisface $\sigma(a_j) = j$. Entonces $\sigma x \sigma^{-1} = (1,2,...,k)$. □

Por lo anterior, todo cíclo de longitud 3 pertenece a $\mathcal{A}_n$. El siguiente muestra que estos le generan.

Proposición 15.0.14. — *El subgrupo $\mathcal{A}_n$ está generado por todos los cíclos de longitud* 3.

Demonstración. — Un cíclo de longitud 3, digamos $(a,b,c) = (a,c)(a,b)$, pertenece a $\mathcal{A}_n$. Como las permutaciones de $\mathcal{A}_n$ se escriben como producto de un número par de

transposiciones, bastará con verificar que el producto de dos transposiciones diferentes es producto de cíclos de longitud 3. Esto se ve como sigue :

$$(a,b)(a,c) = (a,c,b)$$
$$(a,b)(c,d) = (a,b)(a,c)(c,a)(c,d) = (a,c,b)(c,d,a)$$

□

Ejemplo 15.0.15. — Por lo dicho anteriormente, cada permutación puede escribirse como producto disjunto de cíclos. Como hay cíclos de diferentes longitudes, podemos preguntarnos cuantos cíclos de una longitud dada hay. La permutación identidad, el neutro, diremos que es un cíclo de longitud 0. Para cada $k \in \{1,2,...,n\}$ denotemos por n_k el número de diferentes cíclos de longitud k que tenemos en el grupo simétrico $\mathcal{S}_n$. Es claro que $n_1 = n$ y que para $k \in \{2,3,...,n\}$ tenemos que

$$n_k = (k-1)! \left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!(k-1)!}{k!(n-k)!}$$

ya que para formar un k-cíclo, debemos escoger k índices diferentes en $\{1,2,3,...,n\}$ y además tener en cuenta que un cíclo no cambia por una permutación cíclica de sus componentes.

Ahora, tomemos una permutación $\sigma \in \mathcal{S}_n$ y escribamosla como producto de cíclos disjuntos. En esta descripción aparecen una cantidad v_2 de transposiciones, una cantidad v_3 de cíclos de longitud 3,..., una cantidad v_n de cíclos de longitud n. Es claro que $v_n \in \{0,1\}$ y que si $v_n = 1$, entonces σ es un cíclo de longitud n. Denotemos por v_1 la cantidad de puntos fijos por σ en el conjunto $\{1,2,...,n\}$. Debemos tener la igualdad

$$v_1 + 2v_2 + 3v_3 + \cdots + nv_n = n$$

ya que la permutación σ actúa sobre n puntos. Por ejemplo, tomemos $n = 6$ y consideremos la permutación $\sigma = (1,2)(3,4)$. Entonces tenemos $v_1 = 2$, $v_2 = 2$, $v_3 = v_4 = v_5 = v_6 = 0$.

Dos permutaciones con el mismo tipo de descomposición en ciclos, es decir, que corresponden a los mismos v_1, v_2,..., v_n, son siempre conjugados en $\mathcal{S}_n$. En forma recíproca, dos permutaciones que son conjugadas tienen la misma descomposición. Diremos que dos permutaciones son de la misma clase si estos son conjugados. Esto define una relación de equivalencia en $\mathcal{S}_n$. Podemos preguntarnos por la cantidad de clases de conjugación diferentes hay. Para resolver esto, nos conviene que escribamos el sistema lineal

$$\left\{ \begin{array}{ccccccccc} v_1 & + & v_2 & + & \cdots & v_n & = & \mu_1 \\ & + & v_2 & + & \cdots & v_n & = & \mu_2 \\ & & & & & \vdots & = & \vdots \\ & & & & & v_n & = & \mu_n \end{array} \right.$$

restricto a las condiciones

$$\mu_1 + \mu_2 + \cdots + \mu_n = n$$
$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \geq 0$$

De esta manera, primero buscamos todas las soluciones $(\mu_1, ..., \mu_n)$ satisfaciendo las dos últimas propiedades y luego por cada solución analizamos el sistema lineal por el método de Cramer. En otras palabras, la cantidad de diferentes clases de conjugación en $\mathcal{S}_n$ es igual al número de soluciones $(\mu_1, ..., \mu_n)$ de las dos ecuaciones anteriores.
Por ejemplo, consideremos $n = 3$, es decir, $\mathcal{S}_3$. En este caso, las soluciones son dadas por $(\mu_1, \mu_2, \mu_3) \in \{(1, 1, 1), (2, 1, 0), (3, 0, 0)\}$. Para el primer triple $(1, 1, 1)$ tenemos $v_1 = v_2 = 0$ y $v_3 = 1$, es decir los 3-cíclos (forman una clase de conjugación formada de dos 3-cíclos). Para el segundo triple $(2, 1, 0)$ tenemos $v_1 = v_2 = 1$ y $v_3 = 0$, es decir los 2-cíclos (forman una clase de conjugación formada de tres 2-cíclos). Para el tercer triple $(3, 0, 0)$ tenemos $v_2 = v_3 = 0$ y $v_1 = 3$, es decir la clase formada de sólo la permutación trivial.

Observación 15.0.16. — La cantidad de clases de conjugación en el grupo $\mathcal{S}_n$ es importante en la teoría de representaciones lineales (que veremos en un próximo capítulo). Tal número coincide con el número de representaciones irreducibles de tal grupo.

También podemos ver cual es el número de permutaciones en $\mathcal{S}_n$ que tienen una descomposición similar (mismos valores de v_k), es decir, cuantas permutaciones pertenecen a una clase de conjugación dada. Para esto, primero hay que escoger v_1 puntos fijos, es decir,

$$\left(\begin{array}{c} n \\ v_1 \end{array} \right) = \frac{n!}{v_1!(n - v_1)!}$$

posibilidades. Ahora hay que escoger de los restantes puntos v_2 pares disjuntos y sin importar su orden, es decir,

$$\frac{1}{v_2!} \left(\begin{array}{c} n - v_1 \\ 2 \end{array} \right) \left(\begin{array}{c} n - v_1 - 2 \\ 2 \end{array} \right) \left(\begin{array}{c} n - v_1 - 4 \\ 2 \end{array} \right) \cdots \left(\begin{array}{c} n - v_1 - 2(v_2 - 1) \\ 2 \end{array} \right) =$$

$$= \frac{(n - v_1)!}{2^{v_2} v_2!(n - v_1 - 2v_2)!}$$

Ahora hay que escoger de los restantes puntos v_3 trios disjuntos y sin importar su orden, es decir,

$$\frac{1}{v_3!} \left(\begin{array}{c} n - v_1 - 2v_2 \\ 3 \end{array} \right) \left(\begin{array}{c} n - v_1 - 2v_2 - 3 \\ 3 \end{array} \right) \cdots \left(\begin{array}{c} n - v_1 - 2v_2 - 3(v_3 - 1) \\ 3 \end{array} \right) =$$

$$= \frac{(n - -v_1 - 2v_2)!}{3^{v_3} v_3!(n - v_1 - 2v_2 - 3v_3)!}$$

En forma similar para los restantes. Uno obtiene que el número total que buscamos es el producto de todos los anteriores, es decir

$$\frac{n!}{v_1! 2^{v_2} v_2! 3^{v_3} v_3! \cdots n^{v_n} v_n!}$$

Ejercicio 57. —

(i) Verificar que $\mathcal{A}_n$, $n \geq 5$ es un grupo simple, es decir, no posee subgrupos normales no triviales. Analizar los casos $\mathcal{A}_3$ y $\mathcal{A}_4$.

(ii) Calcular $Z(\mathbb{S}_n)$.

PARTE II

ACCIÓN DE GRUPOS Y APLICACIONES

En este capítulo estudiaremos las propiedades de los grupos por medio de acciones sobre conjuntos como grupo de permutaciones. Como aplicación de estos conceptos obtendremos los teoremas de Sylow, los cuales dan información sobre grupos finitos. Luego miraremos un ejemplo particular que corresponde a las representaciones lineales.

CAPÍTULO 16

ACCIÓN DE GRUPOS SOBRE CONJUNTOS

Definición 16.0.17. — Una *acción por la izquierda de un grupo* $(G, *)$ *sobre un conjunto* $X \neq \emptyset$ es por definición un homomorfismo

$$\phi : (G, *) \to (Perm(X), \circ)$$

Un homomorfismo

$$\phi : (G, *) \to (Perm(X), \overline{\circ})$$

donde $(Perm(X), \overline{\circ})$ es el grupo reflejado de $(Perm(X), \circ)$, es llamada una *acción por la derecha de un grupo* $(G, *)$ *sobre el conjunto* X. Si el homomorfismo en cuestión es además inyectivo, entonces hablamos de una *acción fiel*.

Consideremos el isomorfismo natural

$$\tau : (Perm(X), \circ) \to (Perm(X), \overline{\circ}) : \sigma \mapsto \sigma^{-1}$$

y una representación por la izquierda $\phi : (G, *) \to (Perm(X), \circ)$. Entonces tenemos que $\tau \circ \phi : (G, *) \to (Perm(X), \overline{\circ})$ nos dá una acción por la derecha, la cual es fiel sí y sólo si ϕ es fiel. Recíprocamente, si tenemos una acción por la derecha $\psi : (G, *) \to (Perm(X), \overline{\circ})$, entonces $\tau^{-1} \circ \psi : (G, *) \to (Perm(X), \circ)$ nos dá una acción por la izquierda, la cual es fiel sí y sólo si ψ es fiel.
Lo anterior nos permite tener una biyección natural entre las acciones por la derecha y acciones por la izquierda de un grupo dado $(G, *)$ sobre un conjunto fijo X.

$$\{\text{Acciones por la izquierda}\} \to \{\text{Acciones por la derecha}\}$$

$$\phi \mapsto \psi = \tau \circ \phi$$

Por lo tanto, desde ahora en adelante nos preocuparemos de acciones por la izquierda; los resultados equivalentes para acciones por la derecha se obtienen usando la relación anterior.

Observación 16.0.18. — A veces una acción por la izquierda $\phi : (G, *) \to (Perm(X), \circ)$ se escribe como una función

$$\eta : G \times X \to X : (g, x) \mapsto \eta(g, x) := \phi(g)(x)$$

la cual satisface las siguientes propiedades :
(i) $\eta(I_G, x) = x$, para todo $x \in X$;
(ii) $\eta(g * h, x) = \eta(g, \eta(h, x))$;
(iii) $\eta(g, \cdot) : X \to X : x \mapsto \eta(g, x)$ define una permutación de X.

Ejercicio 58. — *Considere una función $\eta : G \times X \to X$ satisfaciendo*
(i) $\eta(I_G, x) = x$, para todo $x \in X$;
(ii) $\eta(g * h, x) = \eta(g, \eta(h, x))$;
(iii) $\eta(g, \cdot) : X \to X : x \mapsto \eta(g, x)$ define una permutación de X.
Verifique que existe un homomorfismo $\phi : (G, *) \to (Perm(X), \circ)$ de manera que $\eta(g, x) := \phi(g)(x)$. Más aún, verifique que condición (i) es consecuencia de las las otras dos (Ind. Llame $T = \eta(I_G, \cdot) \in Perm(X)$. Si $x \in X$, entonces (ii) dice que $T(T(x)) = T(x)$ y (iii) dice que T es invertible.)

Ejemplo 16.0.19. — Consideremos un espacio topológico (X, τ), su σ-álgebra de Borel $\mathcal{A}$ y una medida de probabilidad $P : \mathcal{A} \to [0, 1]$. Supongamos que tenemos una acción fiel $\phi : (G, *) \to Perm(X)$, donde $(G, *)$ es un grupo finito o numerable, tal que $\phi(g) : X \to X$ es un homomorfismo para cada $g \in G$. Consideremos la relación de equivalencia

$$x \cong y \text{ sí y sólo si existe } g \in G \text{ tal que } \phi(g)(x) = y$$

y denotemos por X/G al conjunto de las clases de equivalencia y por $\pi : X \to X/G$ a la proyección natural. Podemos dotar a X/G de la topología cociente ; entonces π se torna continua y abierta (ya que la acción es por homeomorfismos). Denotemos por $\mathcal{A}_{X/G}$ el σ-álgebra de Borel del espacio X/G. Entonces la propiedad que tiene π nos asegura que

$$\mathcal{A}_{X/G} = \{\pi(A) : A \in \mathcal{A}\}$$

Podemos entonces construir la función $P^* : \mathcal{A}_{X/G} \to [0, 1]$ definida por

$$P^*(\pi(A)) = P(\pi^{-1}(A)) = P(\sum_{g \in G} \phi(g)(A))$$

Por ejemplo, supongamos que escogemos $A \in \mathcal{A}$ de manera que $A \cap \phi(g)(A) = \emptyset$ para todo $g \in G$ y $P(A) > 0$. Entonces tendremos que

$$P^*(\pi(A)) = \sum_{g \in G} P(\phi(g)(A))$$

En esta situación tendremos que si G es infinito, entonces para cada sucesión $\{g_n\}$ en G vale que

$$\lim_{n \to +\infty} P(\phi(g_n)(A)) = 0$$

y, en particular, no podemos pedir a $\phi(G)$ estar contenido en el grupo de homeomorfismos de X que preservan la medida P.

Ejemplo 16.0.20. — Recordemos de las primeras secciones del capítulo anterior el homomorfismo de grupos

$$\phi : (G, *) \to (Perm(G), \circ) : g \mapsto \phi(g)$$

donde

$$\phi(g)(x) = g * x * g^{-1}$$

En este caso tenemos una acción por la izquierda del grupo $(G, *)$ sobre el conjunto G.

Ejemplo 16.0.21. — Consideremos una función diferenciable

$$X : \Omega \subset \mathbb{R}^n \to \mathbb{R}^n$$

donde Ω es una región del espacio $\mathbb{R}^n$. Miremos el sistema dinámico

$$x' = X(x)$$

Por el teorema de existencia y unicidad de soluciones, tenemos que para cada $p \in \Omega$ existe una única solución $x(\cdot, p) : \mathbb{R} \to \Omega$ del sistema anterior con la condición $x(0, p) = p$. Más aún como $x(t) = x(t + s, p)$ es también solución del sistema para la condición $x(0) = x(s, p)$, tenemos la relación

$$x(t + s, p) = x(s, x(t, p))$$

Esta relación nos permite construir la acción del grupo aditivo $\mathbb{R}$ sobre Ω como

$$\phi : (\mathbb{R}, +) \to (Perm(\Omega), \circ) : t \mapsto x(t, \cdot)$$

donde

$$x(t, \cdot) : \Omega \to \Omega : p \mapsto x(t, p).$$

Definición 16.0.22. — Supongamos que tenemos una acción $\phi : (G, *) \to (Perm(X), \circ)$.

(i) La *órbita* de un punto $x \in X$ por la acción anterior es el conjunto de puntos que recorre x por efecto de $\phi(G)$, es decir,

$$Orb(x) = \{\phi(g)(x) : g \in G\} \subset X$$

(ii) El *estabilizador* de un punto $x \in X$ por la acción anterior es el conjunto de elementos de G que tienen a x como punto fijo, es decir,

$$Stab(x) = \{g \in G : \phi(g)(x) = x\} \subset G$$

Proposición 16.0.23. — *Para cada $x \in X$ tenemos que el estabilizador $Stab(x)$ es un subgrupo de $(G, *)$.*

Demonstración. — Como $\phi(I_G) = I$, la permutación identidad, tenemos que $I_G \in Stab(x)$, luego, $Stab(x) \neq \emptyset$. Si $g \in Stab(x)$, entonces $\phi(g)(x) = x$, luego $\phi(g)^{-1}(x) = x$. Así, $\phi(g^{-1})(x) = \phi(g)^{-1}(x) = x$, es decir, $\phi(g^{-1}) \in Stab(x)$. Sean $g, h \in Stab(x)$, es decir $\phi(g)(x) = x = \phi(h)(x)$. Entonces, $\phi(g * h)(x) = \phi(g)(\phi(h)(x)) = \phi(g)(x) = x$, es decir $g * h \in Stab(x)$. □

Ejercicio 59. — *Verificar que dada una acción*

$$\phi : (G, *) \to (Perm(X), \circ)$$

la relación

$$x \equiv y \text{ sí y sólo si existe } g \in G \text{ tal que } \phi(g)(x) = y$$

define una relación de equivalencia en X. Las clases de equivalencia son las órbitas. Al conjunto de las clases de equivalencia la denotaremos por $X/\phi(G)$ o simplemente por X/G en caso de no haber confusión de la acción.

Es claro que para cada $x \in X$, la representación $\phi(G)$ actúa como permutaciones del conjunto $Orb(x)$, por definición de órbita. Luego tenemos una función inducida $F : G \to Orb(x) : g \mapsto F(g) := \phi(g)(x)$. Esta función es sobreyectiva. Observemos además que $F(g) = F(h)$ es equivalente a tener $t = g^{-1} * h \in Stab(x)$. Recíprocamente, para cada $t \in Stab(x)$ y cada $g \in G$ vale que $F(g * t) = F(g)$. En otras palabras, tenemos el siguiente :

Proposición 16.0.24. — *Para cada $x \in X$ tenemos una biyección natural entre el conjunto de clases laterales $G/Stab(x)$ y la órbita $Orb(x)$. En particular,*

$$\#Orb(x) = [G : Stab(x)]$$

Ejemplo 16.0.25. — Una acción $\phi(G, *) \to (Perm(X), \circ)$ es llamada una *acción transitiva* si existe un punto $x_0 \in X$ tal que su órbita es todo X, es decir, $Orb(x_0) = X$. Como todo punto $x \in X$ pertenece a $Orb(x_0)$, tenemos que $Orb(x) = X$. En este caso la proposición 16.0.24 nos dice que $[G : Stab(x)]$ es independiente de $x \in X$. De hecho, si tomamos $g \in G$ tal que $\phi(g)(x_0) = x$, entonces

$$Stab(x) = g * Stab(x_0) * g^{-1}$$

Reemplazando X por la órbitas de los puntos de X, la última parte del ejemplo anterior nos dá el siguiente.

Proposición 16.0.26. — *Sea $\phi(G, *) \to (Perm(X), \circ)$ una acción. Si dos puntos $x, y \in X$ pertenecen a la misma órbita, entonces sus estabilizadores son conjugados en G.*

Ejemplo 16.0.27. — Consideremos X como el conjunto de todos los subgrupos de G y la acción

$$\phi : (G, *) \to (Perm(X), \circ) : g \mapsto \phi(g)$$

definida por

$$\phi(g) : X \to X : H \mapsto g * H * g^{-1}$$

En este ejemplo, H es subgrupo normal de G sí y sólo si $Orb(H) = \{H\}$.

Ejercicio 60. — *Sea $(G, *)$ un grupo finito y H un subgrupo de G. Considere la acción*

$$\phi : (H, *) \to (Perm(G), \circ) : h \mapsto \phi(h)$$

donde

$$\phi(h) : G \to G : g \mapsto h * g$$

Verifique que para todo $g \in G$ vale que $Stab(g) = \{I_G\}$ y que $\#Orb(g) = |H|$. Utilice el hecho que G es la unión disjunta de sus órbitas para reobtener el teorema de Lagrange.

Ejemplo 16.0.28. — Consideremos un grupo de transformaciones de Möbius, con la regla de la composición, digamos G. Entonces tenemos una acción natural $\phi : (G, \circ) \to (Perm(\widehat{\mathbb{C}}), \circ)$ dada por biholomorfismos :

$$A : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}} : z \mapsto \phi(A)(z) = \frac{az + b}{cz + d}$$

$a, b, c, d \in \mathbb{C}, \quad ad - bc = 1$. El estudio de este tipo de acciones es parte del estudio de grupos Kleinianos que verán en el seminario de geometría compleja.

Consideremos un conjunto finito $X \neq \emptyset$, un grupo finito $(G, *)$, una acción $\phi : (G, *) \to (Perm(X), \circ)$ y el conjunto $U = \{(g, x) \in G \times X : g \in Stab(x)\}$. Por cada $g \in G$ denotemos por $Fix(g) = \{x \in X : \phi(g)(x) = x\}$ al conjunto de puntos fijos en X por g en la acción dada. Entonces, podemos ver que

$$\#U = \sum_{g \in G} \#Fix(g)$$

Por otro lado, por cada $x \in X$, podemos ver que existen tantos pares $(x, g) \in U$ como elementos en $Stab(x)$; luego,

$$\#U = \sum_{x \in X} |Stab(x)|$$

y como $|G|/|Stab(x)| = [G : Stab(x)] = \#Orb(x)$, tenemos que

$$\#U = |G| \sum_{x \in X} 1/\#Orb(x)$$

Escojamos una colección maximal, digamos $x_1, ..., x_r \in X$, de elementos no equivalentes por G, es decir, cuyas órbitas son disjuntas y la unión de ellas es todo X. Entonces, como

la suma sobre cada órbita $Orb(x)$ del valor $1/\#Orb(x)$ dá el valor 1, la igualdad anterior pude escribirse como

$$\#U = |G|r$$

obteniendo de esta manera la siguiente relación entre los puntos fijos de los elementos de G, $|G|$ y $\#X/G$.

***Proposición 16.0.29* (Igualdad de Burnside).** — *Sea $\phi : (G, *) \to (Perm(X), \circ)$ una acción de un grupo finito $(G, *)$ sobre un conjunto finito. Denotemos por r la cardinalidad del conjunto cociente $X/\phi(G)$, es decir, el número de classes diferentes (órbitas diferentes). Entonces*

$$\sum_{g \in G} \#Fix(g) = r|G|$$

y en particular,

$$r = \textit{ número de órbitas } = \frac{1}{|G|} \sum_{g \in G} \#Fix(g)$$

Ejemplo 16.0.30. — Veamos una aplicación de la igualdad anterior. Supongamos que tenemos un tetraedro $T \subset \mathbb{R}^3$ centrado en el orígen. Este tetraedro tiene 4 caras, las cuales queremos pintar de cuatro clores diferentes, digamos de azul, verde, lila y rojo. Es claro que hay $4! = 24$ posibles maneras de hacer esto : (i) la elección de la cara que pintaremos con azul nos da 4 posibilidades, (ii) la eleción dejada para la que pintaremos de verde es 3, (iii) la eleción para la que pintaremos de lila es 2, (iV) queda luego sólo una posible cara que pintar de rojo. Si consideramos el grupo de isometrías Euclidianas (rotaciones) que dejan invariante T, vemos que cada eleción va a parar a otra elección que en la práctica no es diferente de la anterior, sólo la estaremos mirando desde otra posición. Como el grupo de tales isometrías es $\mathcal{A}_4$, el grupo alternante de 4 letras, cuyo orden es 12, vemos que en realidad hay sólo dos maneras totalmente diferentes de pintarlo, $2 = [\mathcal{S}_2 : \mathcal{A}_4]$. Ahora, miremos esto utilizando la igualdad de Burnside. En este caso consideremos

$$X = \{(C_{i_1}, C_{i_2}, C_{i_3}, C_{i_4}) : i_1, i_2, i_3, i_4 \in \{1, 2, 3, 4\}, i_j \neq i_k, j \neq k\}$$

donde cada cuádruple está formada por las cuatro caras de T, es decir $\#X = 24$ y el grupo $G = \mathcal{A}_4$. La acción de $\mathcal{A}_4$ es dada por permutaciones de las 4 coordendas (en cada cuádruple). Lo que necesitamos encontrar es entonces r, es decir, la cantidad de órbitas diferentes. Para cada $g \in G - \{I_G\}$ se tiene $Fix(g) = \emptyset$ y $\#Fix(I_G) = 24$. Así, en este caso la cantidad de órbitas posibles es $r = 24/12 = 2$ como era lo esperado.

Definición 16.0.31. — Todo grupo de orden una potencia de un primo p es llamado un p-grupo.

Ejemplo 16.0.32. — Volvamos a la acción por conjugación

$$\phi : (G, *) \to (Perm(G), \circ) : g \mapsto \phi(g)$$

donde

$$\phi(g)(x) = g * x * g^{-1}$$

Supongamos que G tiene orden finito, entonces tenemos las siguientes propiedades
(i) dos órbitas coinciden o son disjuntas,
(ii) cada elemento $x \in Z(G)$ tiene como órbita $Orb(x) = \{x\}$,
(iii) la unión de las órbitas es todo G.
Como consecuecia de todo esto tenemos la *ecuación de las clases*

$$|G| = |Z(G)| + \#Orb(x_1) + \#Orb(x_2) + \cdots + \#Orb(x_r)$$

donde $x_1, ..., x_r$ es una colección maximal de elementos no conjugados en $G - Z(G)$.

Supongamos que $|G| = p^n$, es decir, un p-grupo. Ya que
(i) $\#Orb(x_j) > 1$, pues $x_j \notin Z(G)$, y
(ii) $\#Orb(x_j)$ divide $|G| = p^n$ por la proposición 16.0.24,
tenemos que

$$\#Orb(x_j) = p^{n_j} \text{ para algún } n_j \in \{1, 2, ..., n\}$$

Como consecuencia p debe dividir $|Z(G)|$ y, en particular, tenemos el siguiente.

Proposición 16.0.33. — *Sea p un número primo y $(G, *)$ un p-grupo. Entonces $Z(G)$ tiene al menos p elementos.*

Anteriormente habíamos visto que todo grupo de orden un número primo es un grupo cíclico, luego Abeliano. Usando el resultado anterior podemos obtener el siguiente.

Corolario 16.0.34. — *Si $(G, *)$ es un grupo de orden p^2, donde p es un número primo, entonces $(G, *)$ es Abeliano.*

Demonstración. — Por el teorema de Lagrange, $|Z(G)|$ divide p^2. La proposición anterior nos dice entonces que $|Z(G)| \in \{p, p^2\}$. En el caso que $|Z(G)| = p^2$ tendremos $G = Z(G)$ y luego G es Abeliano. Supongamos por el contrario que $|Z(G)| = p$, es decir $(G, *)$ no es Abeliano. Entonces la proposición 7.0.77 nos dá una contradicción. □

Ejemplo 16.0.35. — Generalizemos el ejemplo anterior como sigue. Sea $(G, *)$ un grupo finito y una acción $\phi : (G, *) \to (Perm(X), \circ)$ sobre un conjunto finito. Sea $r = \#X/G$, es decir, podemos escoger $x_1, ..., x_r \in X$ puntos conórbitas diferentes y cuya unión es todo X, es decir, tenemos

$$\#X = \sum_{j=1}^{r} \#Orb(x_j)$$

Denotemos por

$$X_G = \{x \in X : \phi(g)(x) = x \text{ para todo } g \in G\}$$

Entonces, podemos suponer que $x_1, .., x_s \in X_G$ y $x_{s+1}, ..., x_r \notin X_G$. De esta manera, $\#Orb(x_j) = 1$ para $j = 1, ..., s$ y $\#Orb(x_j) > 1$ para $j = s+1, ..., r$. Así, hemos obtenido una fórmula que generaliza la ecuación de clases para la acción particular de conjugación cuando $X = G$.

Proposición 16.0.36 **(Generalización de la ecuación de clases)**
Sea $(G, *)$ un grupo finito y una acción $\phi : (G, *) \to (Perm(X), \circ)$ sobre un conjunto finito X. Sea $x_1, ..., x_r$ puntos conórbitas diferentes y cuya unión es todo X. Supongamos que $x_1, .., x_s \in X_G$ y $x_{s+1}, ..., x_r \notin X_G$. Entonces

$$\#X = \#X_G + \sum_{j=s+1}^{r} \#Orb(x_j)$$

Proposición 16.0.37. — *Sea p un número primo y $(G, *)$ un p-grupo. Entonces*

$$\#X \equiv \#X_G \text{ módulo } p$$

Demonstración. — Tenemos la igualdad

$$\#X = \#X_G + \sum_{j=s+1}^{r} \#Orb(x_j)$$

y sabemos que $\#Orb(x_j) = [G : Stab(x_j)]$. Pero para $j \geq s+1$ también sabemos que $Stab(x_j) \neq G$ y, por el teorema de Lagrange, $|Stab(x_j)|$ es una potencia de p no maximal. Luego, $\sum_{j=s+1}^{r} \#Orb(x_j)$ es divisible por p como queremos. □

Ejemplo 16.0.38. — Consideremos un grupo finito $(G, *)$ y p un número primo que divida $|G|$. Denotemos por G^p el producto cartesiano de p copias de G y consideremos el conjunto

$$X = \{(g_1, g_2, ..., g_p) \in G^p : g_1 * g_2 * \cdots * g_p = I_G\}$$

Observemos que $\#X = |G|^{p-1}$ ya que cualquier elección de $g_1, ..., g_{p-1} \in G$ nos permite elegir $g_p = g_{p-1}^{-1} * g_{p-2}^{-1} * \cdots * g_2^{-1} * g_1^{-1}$. Consideremos el subgrupo cíclico del grupo simétrico $\mathcal{S}_p$ generado por el cíclo $\sigma = (1, 2, 3, ..., p)$ y la acción natural $\phi : \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z} \to Perm(X)$ dada por la permutación cíclica de las coordenadas.
Usando la proposición 16.0.37

$$\#X \equiv \#X_{\langle\sigma\rangle} \text{ módulo } p$$

y el hecho que p divide $\#X$, tenemos que $\#X_{\langle\sigma\rangle}$ también es divisible por p. Como $(I_G, I_G, ..., I_G) \in X_{\langle\sigma\rangle}$, tenemos necesariamente que $\#X_{\langle\sigma\rangle}$ es un múltiplo positivo de p, en particular, existen al menos p elementos de $X_{\langle\sigma\rangle}$. Pero $(g_1, ..., g_p) \in X_{\langle\sigma\rangle}$ sí y sólo si $g_1 = g_2 = \cdots = g_p = g$ y $g^p = I_G$. Este ejemplo nos muestra que existe $g \in G - \{I_G\}$ de orden p.

***Proposición 16.0.39* (Teorema de Cauchy).** — *Sea $(G,*)$ un grupo finito y p un número primo que divide a $|G|$. Entonces existen elementos de G con orden p.*

Este resultado nos da una definición equivalente para un p-grupo como sigue.

***Corolario 16.0.40*.** — *Sea p un número primo. Entonces un grupo finito $(G,*)$ es un p-grupo sí y sólo si todo elemento de G diferente del neutro tiene orden una potencia de p.*

Demonstración. — Es claro que si G es un p-grupo, es decir $|G| = p^n$ para cierto $n > 0$, entonces, por el teorema de Lagrange, todo elemento diferente del neutro tiene orden una potencia de p. Recíprocamente, supongamos que todo elemento de G, diferente del neutro tiene orden una potencia de p. Si G no es un p-grupo, entonces debe existir un número primo $q \neq p$ que divide $|G|$. Por el teorema de Cauchy, debe entonces existir un elemento de orden q, una contradicción. □

***Ejemplo 16.0.41*.** — Consideremos un grupo finito $(G,*)$, p un número primo que divide $|G|$ y H us p-subgrupo de G. Consideremos la acción

$$\phi : (H,*) \to (Perm(G/H), \circ)$$

donde

$$\phi(h)(gH) = (h * g)H$$

En este caso tenemos de la proposición 16.0.37 la equivalencia

$$\#G/H \equiv \#(G/H)_H \text{ módulo } p$$

En este caso,

$$(G/H)_H = \{gH : (h * g)H = gH, h \in H\} =$$
$$= \{gH : (g^{-1} * h * g) \in H, h \in H\}$$

es decir, $(G/H)_H$ coincide con las clases laterales de los elementos del normalizador $N_G(H)$, el cual es $N_G(H)/H$. En particular, como $\#G/H = [G : H]$, obtenemos

$$[G : H] \equiv [N_G(H) : H] \text{ módulo } p$$

***Ejemplo 16.0.42*.** — Sea $(G,*)$ un grupo y H un subgrupo de índice n. Formemos el conjunto $X = G/H$ de las clases de equivalencia laterales derechas de G por H. Como $\#X = [G : H] = n$, tenemos un isomorfismo natural entre $(Perm(X), \circ)$ y $\mathcal{S}_n$. Tenemos la acción

$$\phi : (G,*) \to (Perm(X), \circ) \cong \mathcal{S}_n$$

dada por

$$\phi(g)(xH) = (g * x)H$$

Escribamos $X = \{x_1H, x_2H, ..., x_nH\}$. En este caso, podemos mirar Ker(ϕ) que nos dá los elementos de G que hacen de tal acción no fiel.

$$\text{Ker}(\phi) = \bigcap_{j=1}^{n} Stab(x_jH) = \bigcap_{j=1}^{n} \{g \in G : (g * x_j)H = x_jH, j = 1, 2, ..., n\} =$$

$$= \bigcap_{j=1}^{n} \{g \in G : x_j^{-1} * g * x_j \in H\} =$$

$$= \bigcap_{j=1}^{n} x_jHx_j^{-1} \subset H$$

Este ejemplo tiene dos simples consecuencias.

Proposición 16.0.43. — *Si $(G, *)$ es un grupo, finito ó infinito, que contiene un subgrupo de índice finito $n > 1$, entonces contiene también un subgrupo normal de índice finito.*

Demonstración. — Basta escoger $K =$ Ker(ϕ) del ejemplo ya que $[G : K] = [G : H][H : K]$, $[G : H]$ es finito y $[H : K] \leq n!$. □

Proposición 16.0.44. — *Sea $(G, *)$ un grupo simple, es decir, no contiene subgrupos normales diferente de los triviales. Supongamos que existe H subgrupo de G de índice $n > 1$. Entonces existe un monomorfismo $\phi : (G, *) \to \mathcal{S}_n$.*

Demonstración. — Del ejemplo tenemos que $K =$ Ker(ϕ). Pero como $(G, *)$ es simple, tenemos dos posibilidades : (i) $K = \{I_G\}$, en cuyo caso estamos en lo deseado, ó (ii) $K = G$, en cuyo caso obliga a tener $H = G$, una contradicción. □

Ejemplo 16.0.45. — Consideremos un grupo $(G, *)$ y una acción fiel transitiva $\phi : (G, *) \to (Perm(X), \circ)$ sobre algún conjunto $X \neq \emptyset$ de cardinalidad. finita $n > 1$. Como $n = \#X = \#Orb(x) = [G : Stab(x)]$, entonces $H = Stab(x)$ es un subgrupo de índice $n > 1$. Por lo visto anteriormente, el grupo $(G, *)$ debe contener un subgrupo normal de índice finito. Desgraciadamente, H no es normal. En efecto, si existe $h \in H - \{I_G\}$ tal que para todo $g \in G$ $g * h * g^{-1} \in H$, entonces $\phi(g * h * g^{-1})(x) = x$, es decir, $h \in Stab(\phi(g^{-1})(x))$, para cada $g \in G$. En particular,

$$h \in \bigcap_{x \in X} Stab(x) = \text{Ker}(\phi) = \{I_G\}$$

pués la acción es fiel, dando una contradicción. Más aún, esto también asegura que $Stab(x)$ es un grupo simple.

Recíprocamente, supongamos que tenemos un grupo $(G, *)$ el cual contiene un subgrupo H de índice finito n que no es normal en G y el cual es además simple (como fué el caso de $Stab(x)$ en el caso anterior). Procedamos a mirar la acción vista en el ejemplo anterior

$$\phi : (G, *) \to (Perm(X), \circ) \cong \mathcal{S}_n$$

dada por

$$\phi(g)(xH) = (g * x)H$$

Ya habíamos visto que $K = \text{Ker}(\phi) < H$, y como H es simple, tenemos que (i) $K = \{I_G\}$, en cuyo caso la acción es fiel, ó (ii) $K = H$, en cuyo caso H es subgrupo normal de G, lo cual no es imposible por nuestra elección de H. Luego, ϕ es acción fiel. Por otro lado, como $\phi(g)(H) = gH$, tenemos que la acción es transitiva.

Este ejercicio nos dá el siguiente resultado.

Proposición 16.0.46. — *Sea $(G, *)$ un grupo y un entero $n > 1$. Entonces existe una acción transitiva $\phi : (G, *) \to \mathcal{S}_n$ sí y sólo si existe un subgrupo H de índice n que no es normal y simple.*

CAPÍTULO 17

LOS TEOREMAS DE SYLOW

En esta sección veremos tres resultados muy importantes en la teoría de grupos finito, los llamados *teoremas de Sylow*. Estos resultados son consecuencia de mirar ciertas acciones y utilizar la proposición 16.0.37 el cula nos permite contar módulo un primo.

***Teorema 17.0.47* (Teoremas de Sylow).** — *Sea $(G, *)$ un grupo finito, p un número primo y $|G| = p^a q$, donde $(p, q) = 1$, es decir, p y q son relativamente primos. Entonces :*

(i) Para cada $k \in \{1, 2, ..., a\}$ existe un subgrupo de orden p^k. Un subgrupo de orden maximal p^a será llamado un p-subgrupo de Sylow de G ;

(ii) Todo subgrupo de orden p^k, donde $k \in \{1, 2, ..., a-1\}$, es subgrupo normal de un subgrupo de orden p^{k+1} ;

(iii) Dos p-subgrupos de Sylow de G son conjugados ;

(iv) El número N_p de p-subgrupos de sylow satisface

$$N_p \equiv 1 \text{ módulo } p, \ N_p \text{ divide } |G|$$

Además, si H es cualquier p-subgrupo de Sylow de G, entonces

$$N_p = [G : N_G(H)]$$

Demonstración. —

Parte (i) y (ii). Por el teorema de Cauchy, tenemos listo el caso $k = 1$. Ahora, veremos que la existencia de un p-subgrupo de orden p^k, donde $k \in \{1, 2, ..., a-1\}$, asegura la existencia de un p-subgrupo de orden p^k, obteniendo de esta forma parte (i) del teorema. Para esto, consideremos un subgrupo H de orden p^k, $k < a$. Luego $[G : H]$ es divisible por p. Consecuencia de la equivalencia del ejemplo 16.0.41 es que $[N_G(H) : H]$ también es divisible por p. Ahora, como H es subgrupo normal de $N_G(H)$, tenemos el grupo cociente $N_G(H)/H$ de orden divisible por p. El teorema de Cauchy asegura la existencia de un elemento $zH \in H_G(H)/H$ de orden p, es decir $z^p H = H$. Consideremos el homomorfismo sobreyectivo natural $\pi : N_G(H) \to N_G(H)/H$ y sea $K = \pi^{-1}(\langle zH \rangle)$. Es claro que $H = \text{Ker}(\pi)$ es subgrupo normal de K (al serlo de $N_G(H)$), obteniendo también como consecuencia parte (ii), y tiene orden p^{k+1} como queríamos.

Parte (iii). Consideremos dos p-subgrupos de Sylow, digamos H y K. Consideremos la acción

$$\phi : (K, *) \to (Perm(G/H), \circ)$$

dada por

$$\phi(k)(gH) = (k * g)H$$

Como consecuencia de la proposición 16.0.37 tenemos la equivalencia

$$\#G/H = [G : H] = \#(G/H)_K \text{ módulo } p$$

Como $[G : H]$ ya no es divisible por p, el conjunto

$$(G/H)_K = \{gH : (k * g)H = gH, k \in K\}$$

no puede ser vacío. Escojamos $gH \in (G/H)_K$, luego para cada $k \in K$ vales que $(k * g)H = gH$, es decir $g^{-1} * k * g \in H$. Como H y K tienen el mismo orden, $g^{-1}Kg = H$.

Parte (iv). Tomemos un p-subgrupo de Sylow H y denotemos por X al conjunto de todos los p-subgrupos de Sylow. Miremos la acción

$$\phi : (H, *) \to (Perm(X), \circ)$$

dada por

$$\phi(h)(K) = hKh^{-1}$$

La proposición 16.0.37 nos dice que

$$N_p = \#X \equiv \#X_H \text{ módulo } p$$

Pero en este caso X_H esta formado por todos los p-subgrupos de Sylow K tales que H está contenido en $N_G(K)$, luego, H es p-subgrupo de Sylow de $N_G(K)$.
Sea $K \in X_H$. Por lo anterior H es p-subgrupo de Sylow de $N_G(K)$. Como K también es p-subgrupo de Sylow de $N_G(K)$, tenemos por (iii) que ellos son conjugados por un elemento de $N_G(K)$. Pero todo elemento de $N_G(K)$ conjuga K en si mismo, obteniendo que $K = H$. Como consecuencia

$$X_H = \{H\}$$

es decir

$$N_p \equiv 1 \text{ módulo } p$$

Ahora, usemos la acción $\phi : (G, *) \to (Perm(X), \circ)$, también dada por conjugación, es decir $\phi(g)(K) = gKg^{-1}$. Por (iii) sólo existe una órbita. Además, para cada $K \in X$ vale que $Stab(K) = N_G(K)$. En particular, tomando uno de los p-subgrupos de Sylow de G, digamos H, obtenemos

$$N_p = \#X = \#Orb(H) = [G : N_G(H)]$$

y como $[G : N_G(H)]$ divide $|G|$, entonces N_p divide $|G|$. □

CAPÍTULO 18

APLICACIONES DE LOS TEOREMAS DE SYLOW

18.1. Aplicación 1

Sea p un número primo dado. Hemos visto que todo grupo $(G, *)$ de orden p es necesariamente un grupo cíclico, es decir, isomorfo a $\mathbb{Z}/p\mathbb{Z}$. También hemos visto que todo grupo $(G, *)$ de orden p^2 es Abeliano. Analizemos esta situación con mayor detalle. Si existe un elemento de orden p^2, entonces este elemento es un generador de $(G, *)$ y tenemos que $(G, *)$ es un grupo cíclico, es decir, isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$. Supongamos ahora que no hay elementos de orden p^2. Luego, por el teorema de Lagrange, todo elemento, diferente del neutro, tiene orden p. Podemos escoger $x, y \in G - \{I_G\}$, tales que $\langle x\rangle \cap \langle y\rangle = \{I_G\}$. Denotemos por $H = \langle x\rangle$ y por $K = \langle y\rangle$. Como G es Abeliano, $HK = KH$, es decir HK es subgrupo de G. Además como $\#(H \cap K) = 1$, tenemos que $\#HK = |H||K| = p^2$ y luego $HK = G$. Consideremos la función

$$\phi : H \times K \to G = HK : (x^a, y^b) \mapsto x^a y^b,$$

donde $H \times K$ es producto directo de los dos grupos cíclicos, la cual es claramente un homomorfismo de grupos (gracias a que G es Abeliano) sobreyectivo. Por otro lado, como $H \cap K = \{I_G\}$, tenemos que es también inyectiva, es decir, $G \cong H \times K$ y, como consecuencia, G es producto directo interno de sus subgrupos H y K. En este caso, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Podemos resumir estos resultados de la siguiente manera :

Proposición 18.1.1. — *Sea p un número primo.*
(i) Si $(G, *)$ es un grupo de orden p, entonces $G \cong \mathbb{Z}/p\mathbb{Z}$.
(ii) Si $(G, *)$ es un grupo de orden p^2, entonces $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ó bién $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Ahora, supongamos que tenemos un grupo $(G, *)$ de orden pq, donde $p < q$ son número primos. Si existe un elemento de orden pq, entonces $G \cong \mathbb{Z}/pq\mathbb{Z}$. Supongamos ahora que no existe tal elemento. Por el teorema de Lagrange, todo elemento de G, diferente del neutro, tiene orden p ó q. Por el teorema de Cauchy, existe un elemento $x \in G$ de orden p y existe un elemento $y \in G$ de orden q. Sean $H = \langle x\rangle$ y por $K = \langle y\rangle$. Es claro que $H \cap K = \{I_G\}$ ya que todo elemento de $H - \{I_G\}$ es de orden p y todo elemento de

$K - \{I_G\}$ es de orden q. De esta manera, $\#HK = |H||K| = pq$ y luego

$$G = HK = \{x^a y^b : a \in \{0, 1, ..., p-1\}, b \in \{0, 1, ..., q-1\}\}$$

Tenemos que H es un p-subgrupo de Sylow y K es un q-subgrupo de Sylow. En este caso, por el teorema de Sylow,

$$N_q = 1 + rq, \text{ cierto } r \in \{0, 1, 2, ...\}$$

y además

$$N_q / pq$$

luego,

$$N_q \in \{1, p, q, pq\}$$

Observemos que $N_q = 1 + rq$ no puede ser q ni puede ser pq ya que en tal caso estaremos diciendo que 1 es divisible por q. Por otro lado, si $N_q = p$, entonces $p = N_q = 1 + rq$ para algún $r > 0$, una contradicción al hecho que $p < q$. De esta manera, tenemos que $N_q = 1$ y, como consecuencia del teorema de Sylow, K es un subgrupo normal de G. Esto nos dice que existe un valor $\alpha \in \{1, 2, 3, ..., q-1\}$ de manera que

$$x * y * x^{-1} = y^\alpha$$

De esta manera, tenemos que

$$G = \langle x, y : x^p, y^q, x * y * x^{-1} y^{-\alpha} \rangle$$

Si $\alpha = 1$, entonces tenemos que G es Abeliano ya que $x * y = y * x$. En este caso, podemos proceder de la misma manera como lo hicimos en el caso p^2 para obtener que $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ (lo último como consecuencia de la proposición 8.1.3). Esta es la situación obligada si tenemos que q no es congruente a 1 módulo p. En efecto, si estamos bajo tal condición, entonces

$$N_p = 1 + sp, \text{ cierto } s \in \{0, 1, 2, ...\}$$

y

$$N_p / pq$$

Pero N_p no puede ser p ni pq ya que en tal caso 1 sería divisible por p. Luego, $N_p \in \{1, q\}$. Pero $q = N_p = 1 + sp$ dice que q es congruente a 1 módulo p lo que contradice nuestro supuesto, luego $N_p = 1$ y, como consecuencia, H también es subgrupo normal de G. Luego, debe existir $\beta \in \{1, 2, ..., p-1\}$ tal que

$$y * x * y^{-1} = x^\beta$$

y luego, si $\beta > 1$, tenemos que

$$y * x = x^\beta * y = x^{\beta-1} * x * y = x^{\beta-1} * y^\alpha * x$$

de lo cual

$$y = x^{\beta-1} * y^\alpha$$

es decir, $x^{\beta-1} \in H \cap K = \{I_G\}$, con lo cual obtenemos una contradicción. En resumen :

Proposición 18.1.2. — *Sean $p < q$ números primos y $(G, *)$ un grupo de orden pq. Entonces*
(i) G es Abeliano y

$$G \cong \mathbb{Z}/pq\mathbb{Z}$$

(ii) G no es Abeliano y existe $\alpha \in \{2, 3, ..., q-1\}$ tal que

$$G = \langle x, y : x^p, y^q, x * y * x^{-1} y^{-\alpha} \rangle$$

(iii) Si q no es congruente a 1 módulo p, entonces estamos en el caso (i).

Ejemplo 18.1.3. — Sea $(G, *)$ un grupo de orden 10. En este caso $p = 2$, $q = 5$ y q es congruente a 1 módulo p. Si $(G, *)$ es Abeliano, entonces tenemos

$$G \cong \mathbb{Z}/10\mathbb{Z}$$

En el caso que G no sea Abeliano, entonces las posibilidades para α son $\alpha = 2, 3, 4$.
El caso $\alpha = 4$ nos da el grupo dihedral

$$G = \langle x, y : x^2, y^5, (x * y)^2 \rangle \cong D_5$$

En el caso $\alpha = 2$ tenemos

$$G = \langle x, y : x^2, y^5, x * y = y^2 * x \rangle =$$
$$= \langle x, y : x^2, y^5, y^{-1} * x = x * y^{-2} \rangle$$

si tomamos $z = y^3$, entonces

$$G = \langle x, z : x^2, z^5, z^3 * x = x * z \rangle$$

que corresponde al caso $\alpha = 3$. Es decir, en el caso de orden 10 sólo tenemos 3 grupos no isomorfos.

Ejercicio 61. — *Determinar los grupos de orden 8 no isomorfos.*

18.2. Aplicación 2

Consideremos un grupo Abeliano finito $(G, *)$ y un entero positivo n que divide al orden de G. Si escribimos

$$|G| = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

la descomposición en números primos diferentes, entonces

$$n = p_{j_1}^{s_1} p_{j_2}^{s_2} \cdots p_{j_b}^{s_b}$$

donde

$$1 \leq j_1 < j_2 < \cdots < j_b \leq m$$

y

$$s_i \in \{1, 2, ..., r_{j_i}\}$$

Por el teorema de Sylow, existen subgrupos H_1,..., H_b, donde

$$|H_i| = p_{j_i}^{s_i}, \quad i = 1, ..., b$$

Consideremos $\mathcal{H} = H_1 H_2 \cdots H_b = \{x_1 * x_2 * \cdots * x_b : x_j \in H_j\}$. Al ser G un grupo Abeliano, uno puede verificar que $\mathcal{H}$ es realmente un subgrupo de G y de orden n, luego el subgrupo deseado. De esta manera, tenemos el siguiente recíproco del teorema de Lagrange para grupos Abelianos.

Proposición 18.2.1. — *Sea $(G, *)$ un grupo Abeliano finito y n un entero positivo que divide al orden de G. Entonces existe un subgrupo de G de orden n.*

Ejercicio 62. — *Verificar en la construcción dada anteriormente que existe un isomorfismo entre el producto directo $H_1 \times H_2 \times \cdots H_b$ y el grupo $\mathcal{H}$. Deducir que todo grupo Abeliano finito es siempre isomorfo a un grupo de la forma*

$$(\mathbb{Z}/n_1\mathbb{Z})^{a_1} \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^{a_r}$$

Comparar esto con la descomposición hecha en el capítulo anterior, sección **Grupos Abelianos libres**.

18.3. Aplicación 3

Definición 18.3.1. — Diremos que un grupo es *simple* si no tiene subgrupos no triviales que sean normales.

Ejemplo 18.3.2. — Ejemplos de grupos simples son los siguientes.

(i) todo grupo cíclico de orden un número primo es un grupo simple, pero un grupo cíclico de orden un número que no sea primo no es simple.

(ii) El grupo dihedral

$$D_n = \langle x, y : x^2, y^n, (x * y)^2 \rangle$$

tiene al subgrupo normal $\langle y \rangle$, luego no es simple.

(iii) Por la clasificación de los grupos Abelianos finitos, vemos que todo grupo Abeliano de orden que no sea un número primo no puede ser simple.

(iv) Si tenemos un grupo de orden p^n, donde p es un número primo y $n \geq 2$, entonces por el teorema de Sylow este grupo no es simple ya que posse un subgrupo de orden p^{n-1} que es normal.

(v) Si tenemos un grupo de orden pq, donde $p < q$ son números primos, entonces ya habíamos visto que necesariamente $N_q = 1$ y luego todo q-subgrupo de Sylow es normal, luego el grupo no puede ser simple.

(vi) Si tenemos un grupo de orden $p^n q$, donde $p < q$ son números primos tales que q no es congruente a 1 módulo p y $n \geq 2$, entonces el grupo no es simple. En efecto, tenemos que $N_p = 1 + rp$ para algún entero $r \in \{0, 1, 2, ...\}$ y además debe dividir $p^n q$. Esto obliga a tener que los factores primos de N_q están contenidos en $\{p, q\}$. Como 1 no es divisible por p, entonces $N_p \in \{1, q\}$. Pero $N_p = q$ nos dice que q es congruente a 1 modulo p, lo cual hemos descartado en nuestra hipótesis. Luego, $N_p = 1$ y, como consecuencia, un $p-$subgrupo de Sylow es subgrupo normal.

(vii) Sea $(G, *)$ un grupo de orden $2q^n$, donde $q > 2$ es un número primo y $n \in \{1, 2, 3, ...\}$. Entonces G no es simple. En efecto, consideremos $N_q = 1 + rq$, $r \in \{0, 1, 2, ...\}$, que debe dividir $2q^n$. Esto obliga a tener que los factores primos de N_q están contenidos en $\{2, q\}$. Como 1 no es divisible por q, debemos tener $N_q \in \{1, 2\}$. Pero $N_q = 2$ no es posible para ningún valor de r, luego $N_q = 1$.

(viii) Consideremos un grupo de orden $6q$, donde $q > 5$ es un número primo. Entonces el grupo no puede ser simple. En efecto, en este caso, $N_q = 1 + qr$, cierto $r \in \{0, 1, 2, 3, ..\}$, que divide $6q$. Como 1 no es divisible por q, tenemos que $N_q \in \{1, 2, 3, 6\}$. Es claro que no podemos lograr los valores $2, 3, 6$ con ningún r, luego $N_q = 1$ y todo q-subgrupo de Sylow es normal.

(ix) Ningún grupo de orden 30 es simple. En efecto, en este caso como $30 = 2 \times 3 \times 5$, miremos $N_5 = 1 + 5r$, cierto $r \in \{0, 1, 2, 3, ..\}$, que divide 30. Como 1 no es divisible por 5, tenemos que $N_5 \in \{1, 6\}$. Si $N_5 = 1$ tenemos que todo 5-subgrupo de Sylow es normal. Supongamos por el contrario que $N_5 = 6$. Entonces tenemos $6 \times 4 = 24$ elementos diferentes de orden 5 en nuestro grupo (diferentes del neutro). Por otro lado, $N_3 = 1 + 3t$, cierto $t \in \{0, 1, 2, 3, ..\}$, divide 30, luego $N_3 \in \{1, 10\}$. Si $N_3 = 1$, entonces todo 3-subgrupo de Sylow es normal. Si colocamos $n_3 = 10$, tendremos $2 \times 10 = 20$ elementos diferentes de orden 3. En total ya tenedríamos $1 + 24 + 20 > 30$ elementos diferentes en el grupo, una contradicción.

(x) Ningún grupo de orden 36 es simple. En efecto, como $36 = 2^2 3^2$, entonces $N_3 = 1 + 3r$, algún $r \in \{0, 1, 2, ...\}$, divide 36. Como 1 no es divisible por 3, $N_3 \in \{1, 2, 4\}$. Pero $N_3 = 2$ no puede lograrse con ninguna de las posibles r. Así, $N_3 \in \{1, 4\}$. Si $N_3 = 1$, entonces todo 3-subgrupo de Sylow es normal. Supongamos que $N_3 = 4$. Consideremos un 3-subgrupos de Sylow, digamos H. Tenemos que $|H| = 9$. Consideremos el conjunto $X = \{g * H * g^{-1} : g \in G\}$ que tiene cardinalidad $N_3 = 4$. Miremos la acción

$$\phi : (G, *) \to (Perm(X), \circ)$$

dada por conjugación. Como $|G| = 36 > 24 = |Perm(X)|$, tenemos que $K =$ Ker(ϕ) es un subgrupo normal de orden mayor que 1. Pero también tenemos que K es necesariamente un subgrupo de $N_G(H)$, y como $[G : N_G(H)] = N_3 = 4$, tenemos que K es subgrupo propio de G. Entonces K es subgrupo normal no trivial.

(xi) Ningún grupo de orden 48 es simple. Como $48 = 2^4 3$, podemos mirar $N_3 = 1 + 3r$, algún $r \in \{0, 1, 2, ...\}$, dividiendo 48. De esta manera obtenemos $N_3 \in \{1, 3\}$. Si $N_3 = 1$, entonces todo 3-subgrupo de Sylow es normal. Supongamos que $N_3 = 3$ y tomemos dos 3-subgrupos de Sylow diferentes, digamso H_1 y H_2. Luego, $|H_j| = 16$.

Como

$$48 \geq \#H_1H_2 = \frac{|H_1 \times H_2|}{|H_1 \cap H_2|}$$

obtenemos que

$$|H_1 \cap H_2| \geq \frac{16^2}{48} > 5$$

Por el teorema de Lagrange, $|H_1 \cap H_2|$ divide $|H_1| = 16$ y, como consecuencia, $|H_1 \cap H_2| = 8$ (ya que $H_1 \neq H_2$). De esta manera, $H_1 \cap H_2$ es subgrupo de índice 2 en H_j, $j = 1, 2$, y como consecuencia, subgrupo normal. Esto nos dice que H_1 y H_2 son subgrupos de $N_G(H_1 \cap H_2)$. Es decir, $|N_G(H_1 \cap H_2)|$ debe dividir 48, y ser divisible por 16 (al contener H_1 y H_2) y por el orden del grupo $\langle H_1, H_2 \rangle$, generado por H_1 y H_2, que tiene la forma $16k$, con cierto $k \geq 2$ (ya que $H_1 \neq H_2$). De esto vemos que $N_G(H_1 \cap H_2) = G$ y, en particular, $H_1 \cap H_2$ es subgrupo normal no trivial de G.

(xii) Sea $(G, *)$ un grupo de orden 160. Entonces G no es simple. En efecto, como $160 = 2^5 5$, miremos $N_5 = 1 + 5r$, cierto $r \in \{0, 1, 2, ..\}$, que divide 160. Tenemos que $N_5 \in \{1, 5\}$. Si $N_5 = 1$, entonces todo 5-subgrupo de Sylow es normal. Supongamos que $N_5 = 5$ y escojamos un 5-subgrupo de Sylow H, luego $|H| = 2^5 = 32$. Además, tenemos por el teorema de Sylow que $[G : N_G(H)] = N_5 = 5 > 1$, con lo cual vemos que $N_G(H)$ es subgrupo propio de G. Consideremos el conjunto X formado por todos los 5-subgrupos de Sylow, luego $\#X = N_5 = 5$, y la acción por conjugación $\phi : (G, *) \to (Perm(X), \circ)$. Sea K el subgrupo normal de G dado por Ker(ϕ). Como todo $g \in K$ debe fijar H, tenemos que $g \in N_G(H)$, es decir, $K < N_G(H)$ y luego $K \neq G$. Por otro lado, como $160 = |G| > 120 = |Perm(X)$, tenemos que ϕ no es monomorfismo, es decir, $K \neq \{I_G\}$. Luego, K es subgrupo normal no trivial de G.

Ejercicio 63. — *Encontrar todos los grupos simples de orden menor que* 60. *Verificar que* $\mathcal{A}_5$ *es grupo simple de orden* 60.

18.4. Aplicación 4

Definición 18.4.1. — Diremos que un grupo G es *orientable* si existe un homomorfismo sobreyectivo $\phi : G \to \mathbb{Z}/2\mathbb{Z}$. En tal caso el par (G, ϕ) es llamado un grupo *orientado*. El núcleo $Ker(\phi) := G^+$ es llamado el subgrupo de elementos que preservan orientación. Es claro que G^+ es un subgrupo de índice dos y luego un subgrupo normal de G. Los elementos de $G - G^+$ son llamados elementos que revierten orientación.

Una consecuencia directa de los teoremas de Sylow es el siguiente :

Proposición 18.4.2. — *Sea* (G, ϕ) *un grupo orientado finito tal que* 2 *divide* $|G|$. *Si* 2^n *es la máxima potencia de* 2 *que divide a* G, *entonces* G *tiene a los más* 2^{n-1} *elementos de orden* 2 *que revierten orientación y que no son conjugados en* G.

Demonstración. — Denotemos por H un 2-subgrupo de Sylow. Sabemos que cada elemento de orden 2 en G tiene un conjugado en H. Luego debemos contar cuantos elementos de H pueden revertir orientación. Ya que el producto de dos elementos de H preserva orientación, tenemos que $H^+ := H \cap G^+$ es de índice 2 en H, es decir, $|H^+| = 2^{n-1}$ y como tenemos la unión disjunta $H = H^+ \cup T$, donde T denota el subconjunto de los elementos de H que revierten orientación, tenemos que $\#T = 2^{n-1}$. □

Observación 18.4.3. — El resultado anterior ha sido utilizado por G. Gromadzki (On ovals on Riemann surfaces, *Revista Matemática Iberoamericana* **16** (2000), 515-527) para obtener información sobre el número máximo de ovalos de reflexiones en superficies de Riemann cerradas.

PARTE III

ANILLOS

Hasta ahora hemos estudiado estructuras donde sólo está involucrada una operación binaria. Ahora miraremos estructuras donde aparecen dos estructuras.

CAPÍTULO 19

DEFINICIÓN Y EJEMPLOS

Definición 19.0.4. — Un *anillo* es por definición un triple $(R, +, \cdot)$ donde R es un conjunto no vacío y $+, \cdot : R \times R \to R$ son dos operaciones binarias sobre R, llamadas suma y multiplicación repectivamente, tales que :
(1) $(R, +)$ es un grupo abeliano ;
(2) vale la propiedad asociativa para la operación de multiplicación, es decir, para $r, s, t \in R$ se tiene

$$r \cdot (s \cdot t) = (r \cdot s) \cdot t$$

(3) para $r, s, t \in R$ vale la propiedad distributiva :

$$r \cdot (s + t) = r \cdot s + r \cdot t$$

$$(r + s) \cdot t = r \cdot t + s \cdot t$$

Observación 19.0.5. — Al neutro de la operación de suma lo denotaremos por 0, al inverso de $r \in R$ respecto a la suma lo denotaremos por $-r$ y rs denotará $r \cdot s$. Si $r \in R$ y $n > 0$ es un entero, entonces denotaremos por r^n al proceso de multiplicar r consigo mismo n veces.

Ejercicio 64. — *Sea $(R, +, \cdot)$ un anillo. Verificar las siguientes propiedades :*
(i) $r0 = 0r = 0$*, para todo $r \in R$; concluir que si $\#R > 1$, entonces 0 no puede ser neutro multiplicativo.*
(ii) $r(-s) = (-r)s = -(rs)$*, para todo $r, s \in R$; concluir que $(-r)(-s) = rs$.*

Ejemplo 19.0.6. — Los primeros ejemplos de anillos que tenemos son $\mathbb{Z}$, el anillo de los números enteros ; $\mathbb{Q}$, el anillo de los números racionales ; $\mathbb{R}$, el anillo de los números reales ; $\mathbb{C}$, el anillo de los números complejos.

Ejemplo 19.0.7. — Otro ejemplo es considerar un entero positivo $m > 0$ y considerar $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$, el conjunto de los enteros múltiplos de m. Usando las operaciones usuales de suma y multiplicación de números entros, se tiene un anillo.

De este último ejemplo observamos, tomando $m > 1$, que hay anillos que no poseen un neutro para la multiplicación.

Definición 19.0.8. — Diremos que un anillo tiene *unidad* si existe un neutro para la multiplicación, el cual denotaremos por 1.

Ejercicio 65. — *Verificar que la unidad es única.*

Por otro lado, si miramos el anillo $\mathbb{Z}$, entonces podemos observar que un anillo con unidad puede que no tenga inversos multiplicativos de sus elementos diferentes de 0.

Definición 19.0.9. — Diremos que un anillo con unidad con la propiedad que todo sus elementos diferentes de cero tienen inverso multiplicativo es un *anillo de división*.

El anillo $\mathbb{Z}$ es un dominio entero, el cual no es de división. Pero $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios enteros que además son de división.

Ejercicio 66. — *Sea $(R, +, \cdot)$ un anillo con unidad y sea $r \in R$ un elemento que posee un inverso multiplicativo en R. Verificar que tal inverso multiplicativo es único.*

Observación 19.0.10. — Si $r \in R$, entonces denotaremos por $r^{-1} \in R$ a su inverso multiplicativo, en caso de existir. Así, si $r \in R$ posee un inverso r^{-1} y $n < 0$ es un entero, entonces denotaremos por r^n al elemento $(r^{-1})^{-n}$.

***Ejemplo 19.0.11* (Anillo de un grupo)**. — Sea $(G, *)$ un grupo y $(R, +, \cdot)$ un anillo. Formamos el conjunto $R[G]$ cuyos elementos son combinaciones lineales finitas de elementos de G con coeficientes en R, es decir, objetos de la forma

$$r_1 g_1 + \cdots + r_n g_n$$

donde $r_j \in R$ y $g_j \in G$. Definimos la suma como,

$$(r_1 g_1 + \cdots + r_n g_n) + (s_1 g_1 + \cdots + s_n g_n) = (r_1 + s_1)g_1 + \cdots + (r_n + s_n)g_n$$

y el producto como

$$\sum_{j=1}^{n} r_j g_j \sum_{i=1}^{m} s_i h_i = \sum_{j=1}^{n} \sum_{i=1}^{m} r_j s_i g_j * h_i$$

De esta manera obtenemos un anillo $(R[G], +, \cdot)$ llamado el *anillo del grupo G respecto al anillo R.*

Ejercicio 67. — *Si $G = \langle x : x^3 \rangle$ y $R = \mathbb{Z}/5\mathbb{Z}$, describir los elementos de $R[G]$ y las tablas de suma y multiplicación.*

***Ejemplo 19.0.12* (Anillo de polinomios)**. — Consideremos un anillo $(R, +, \cdot)$ y una variable desconocida $x \notin R$. Formemos el conjunto $R[x]$ formado por todas las series

$$\sum_{j=0}^{\infty} r_j x^j$$

donde asumimos que sólo un número finito de los coeficientes r_j pueden ser diferente de cero. Llamamos a cada uno de esos objetos un *polinomio* con coeficientes en R y variable desconocida x. Al mayor valor $n\{0, 1, 2, ...\}$ tal que $r_n \neq 0$ le llamamos el *grado del polinomio*. Usualmente no escribimos los términos donde $r_j = 0$; por jemplo si $r_1 = 2$, $r_3 = 1$ y todos los demás $r_j = 0$, entonces escribimos este polinomio como $2x + x^3$. También acostumbramos a denotar $r_0 x^0$ como r_0. Definimos la suma de polinomios como

$$\left(\sum_{j=0}^{\infty} r_j x^j\right) + \left(\sum_{j=0}^{\infty} s_j x^j\right) = \left(\sum_{j=0}^{\infty} (r_j + s_j) x^j\right)$$

y definimos el producto de polinomios como

$$\left(\sum_{j=0}^{\infty} r_j x^j\right) \cdot \left(\sum_{i=0}^{\infty} s_i x^i\right) = \left(\sum_{k=0}^{\infty} \left(\sum_{i+j=k} r_j s_i\right) x^k\right)$$

Obtenemos de esta manera un anillo, llamado el *anillo de polinomios con coeficientes en el anillo R.*

Ejercicio 68. — *Verificar que el anillo $R[x]$ tiene unidad sí y sólo si R lo tiene.*

Ejemplo 19.0.13. — Siguiendo con el ejemplo anterior, podemos partir de un anillo R y formar el nuevo anillo $R[x]$. Pero ahora podemos formar el anillo $R[x][y]$, es decir, los polinomios en la variable y y coeficientes en $R[x]$. En forma inductiva, podemos formar el anillo $R[x_1][x_2] \cdots [x_n]$ formado por los polinomios en la variable x_n y coeficientes en el anillo $R[x_1][x_2] \cdots [x_{n-1}]$. Los elementos de $R[x_1][x_2] \cdots [x_n]$ son llamados polinomios en varias variables y coeficientes en R. Usualmente escribimos este anillo como $R[x_1, ..., x_n]$.

Ejemplo 19.0.14. — Consideremos un anillo $(R, +, \cdot)$ y un entero $n \geq 1$. Consideremos el conjunto $M(n, R)$ formado por todas las matrices de tamaño $n \times n$ y coeficientes en R. La suma y producto usual de matrices hacen de este un anillo. La matriz 0, es decir, todos sus coeficientes igual a $0 \in R$, es el $) \in M(n, R)$. En este caso, si R tiene una unidad $1 \in R$, entonces la matriz identidad es unidad en $M(n, R)$. Supongamos $n \geq 2$,

entonces se puede ver que la operación de multiplicación no es conmutativa ; por ejemplo, si $n = 2$, consideremos

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

entonces tenemos que

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{y} \quad BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Este último ejemplo nos muestra que existen anillos en los cuales la operación de multiplicación no es conmutativa.

Definición 19.0.15. — Diremos que un anillo R es un *anillo conmutativo* si para todo par $x, y \in R$ vale que $xy = yx$.

El ejemplo anterior también nos muestra que es posible tener dos elementos diferentes de 0 que al multiplicarlos obtenemos como resultado 0.

Definición 19.0.16. — Sea R un anillo. Dos elementos $x, y \in R - \{0\}$ tales que $xy = 0$ son llamados *divisores de cero del anillo*.

Ejercicio 69. — *Ver que un anillo de división no puede contener divisores de cero.*

Definición 19.0.17. — Un anillo con unidad, sin divisores de cero y conmutativo es llamado un *dominio entero*.

Ejercicio 70. — *Todo anillo de división conmutativo es un dominio entero.*

Definición 19.0.18. — Un anillo de división conmutativo es llamado un *cuerpo*.

Así, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son ejemplos de cuerpos.

Ejemplo 19.0.19. — Consideremos el grupo abeliano $\mathbb{R}^4$ con la suma usual dada componente a componente, es decir,

$$(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)$$

Si denotamos por

$$1 = (1, 0, 0, 0), \quad i = (0, 1, 0, 0), \quad j = (0, 0, 1, 0), \quad k = (0, 0, 0, 1),$$

entonces podemos escribir

$$(a, b, c, d) = a1 + bi + cj + dk$$

Usaremos la identificación $a1 = a$, luego

$$(a, b, c, d) = a + bi + cj + dk$$

En esta notación la suma queda expresda como :

$$(x_1 + x_2 i + x_3 j + x_4 k) + (y_1 + y_2 i + y_3 j + y_4 k)$$
$$||$$
$$(x_1 + y_1) + (x_2 + y_2)i + (x_3 + y_3)j + (x_4 + y_4)k$$

Procedemos a definir una multiplicación como sigue :

$$(x_1 + x_2 i + x_3 j + x_4 k) \cdot (y_1 + y_2 i + y_3 j + y_4 k)$$
$$||$$
$$(x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4) + (x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)i$$
$$+$$
$$(x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2)j + (x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1)k$$

Obtenemos de esta manera un anillo con unidad, siendo esta 1. Denotamos este anillo por $\mathcal{Q}$ y le llamamos el anillo de los *cuaternios*. En este anillo tenemos las propiedades

$$i^2 = j^2 = k^2 = -1$$

$$ij = k, \;\; jk = i, \;\; ki = j, \;\; ji = -k, \;\; kj = -i, \;\; ik = -j,$$

en particular, este anillo no es conmutativo. Por otro lado, si tomamos un elemento diferente de 0, digamos $a + bi + cj + dk \in \mathcal{Q}$, entonces este tiene inverso multiplicativo dado por

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk)$$

En este ejemplo tenemos un anillo que es casi un cuerpo, pero falla la conmutatividad de la multiplicación.

Definición 19.0.20. — Un anillo de división no conmutativo es llamado un *cuerpo no conmutativo* ó *semicuerpo*.

Ejemplo 19.0.21. — Consideremos una colección de anillos $(R_1, +, \cdot)$,..., $(R_n, +, \cdot)$ y formemos el producto cartesiano $R_1 \times \cdots \times R_n$. Consideremos la suma y multiplicación definidas componente a componente, es decir,

$$(r_1, ..., r_n) + (s_1, ..., s_n) = (r_1 + s_1, ..., r_n + s_n)$$
$$(r_1, ..., r_n) \cdot (s_1, ..., s_n) = (r_1 s_1, ..., r_n s_n)$$

donde $r_j, s_j \in R_j$, para $j = 1, 2, ..., n$. Así obtenemos un anillo llamado el *producto directo* de los anillos. Observemos que este anillo tiene unidad sí y sólo si cada anillo

componente lo tiene. Por otro lado, si todos los anillos R_j son dominios enteros, y $n \geq 2$, entonces el producto directo ya no es dominio entero ya que $(1, 0, ..., 0) \cdot (0, 1, 0, ..., 0) = (0, ..., 0)$.

Ejercicio 71. — *Consideremos un entero positivo $d > 0$ con la propiedad que $\sqrt{d} \notin \mathbb{Z}$. Consideremos los conjuntos*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

Consideramos la suma usual de números complejos y el producto usual de números complejos. Verificar que los anteriores son dominios enteros, que $\mathbb{Q}[\sqrt{d}]$ es un cuerpo y $\mathbb{Z}[\sqrt{d}]$ no lo es. Verificar que $\mathbb{Q}[\sqrt{d}]$ es el cuerpo más pequeño dentro de $\mathbb{R}$ que contiene al dominio entero $\mathbb{Z}[\sqrt{d}]$.

Ejercicio 72. — *Por cada entero positivo $m > 0$ consideremos el grupo cíclico $\mathbb{Z}/m\mathbb{Z}$. Definamos la multiplicación $a \cdot b$, donde $a, b \in \{0, 1, ..., m - 1\}$, como el resto módulo m del entero $ab \in \mathbb{Z}$. Verificar que de esta manera obtenemos un anillo con unidad y conmutativo. Verificar que este anillo tiene divisores de cero sí y sólo si m no es un número primo. En el caso que m es un número primo, verificar que este es de hecho un cuerpo. Más adelante daremos un argumento de este hecho.*

La situación del ejemplo anterior es caso particular del siguiente hecho.

Teorema 19.0.22. — *Todo dominio entero finito es un cuerpo.*

Demonstración. — Sea $R = \{0, 1, r_1, ..., r_n\}$. Basta verificar que todo elemento diferente de 0 tiene un inverso multiplicativo. Para eso, sea $r \in R$, $r \neq 0$. Como la colección

$$r, rr_1, ..., rr_n$$

son dos a dos diferentes y distintos de 0, alguno de ellos debe ser igual a 1. □

En algunos de los ejemplos anteriores hemos visto que hay anillos que están contenidos en otros anillos (con las operaciones inducidas). Estos son llamados *subanillos*.

Ejercicio 73. — *Sea $(R, +, \cdot)$ un anillo y $S \subset R$ un subconjunto no vacío. Verificar que S define un subanillo de R sí y sólo si*
(i) para todo $s \in S$, $-s \in S$;
(ii) si $s, r \in S$, entonces $s - r \in S$;
(iii) si $r, s \in S$, entonces $sr \in S$.

Ejercicio 74. — *Sea $(R, +, \cdot)$ un anillo y $r \in R$. Consideremos el subconjunto*

$$I_r = \{rx : x \in R\}$$

Verificar que I_r es un subanillo de R. Verificar además que el grupo abeliano $(I_r, +)$ está generado por $\{r^n : n \in \{1, 2, ...\}\}$

Ejercicio 75. — *Verificar que la intersección arbitraria de subanillos de un anillo es un subanillo. Sea $r \in R$. Sea $\langle r \rangle$ la intersección de todos los subanillos de R que contienen a r. Entonces $\langle r \rangle$ es el subanillo más pequeño de R que contiene a r.*

Ejemplo 19.0.23. — Sea R una anillo con la propiedad que $x^2 = x$ es válido para todo $x \in R$. Si consideramos $r, s \in R$ obtenemos que

$$r + s = (r + s)^2 = r^2 + s^2 + rs + sr = r + s + rs + sr$$
$$r - s = (r - s)^2 = r^2 + s^2 - rs - sr = r + s - rs - sr$$

de donde obtenemos

$$rs + sr = 0 \quad \text{y} \quad rs + sr = 2s$$

es decir, $s+s = 0$, de donde $s = -s$ y luego $rs = sr$, es decir, R es un anillo conmutativo.

Ejemplo 19.0.24. — Sea $(G, *)$ un grupo abeliano y consideremos el conjunto Hom(G) formado por todos los homomorfismo de grupo $h : G \to G$ (endomorfismos). Usando la suma

$$(f + g)(x) := f(x) * g(x)$$

y la regla de composición de funciones como multiplicación, tenemos el anillo de endomorfismos de G. En este caso, el neutro aditivo es dado por la funci'on $0(x) = e$, donde $e \in G$ denota el neutro del grupo G. El inverso aditivo de f es el homomorfismo $-f(x) := f(x)^{-1}$. Este anillo tiene unidad dada por el automorfismo identidad. En general este anillo no es conmutativo, pero por ejemplo Hom$(\mathbb{Z}, +)$ si lo es ya que cada homomorfismo de grupo para $\mathbb{Z}$ es de la forma $f(x) = ax$, para cierto $a \in \mathbb{Z}$.

CAPÍTULO 20

HOMOMORFISMOS DE ANILLOS

Al igual que en el caso de grupos, existen funciones que nos permiten relacionar anillos. Estas funciones deben preservar las dos operaciones binarias en juego. De manera más precisa :

Definición 20.0.25. —

(1) Dados dos anillos $(R, +, \cdot)$ y $(S, +, \cdot)$, diremos que una función $h : R \to S$ es un *homomorfismo de anillos* si para todo par $r_1, r_2 \in R$ valen las siguientes :
   (i) $h(r_1 + r_2) = h(r_1) + h(r_2)$
   (ii) $h(r_1 r_2) = h(r_1)h(r_2)$

(2) Si el homomorfismo de anillos $h : R \to S$ es biyectiva, entonces decimos que es un *isomorfismo de anillos*, en cuyo caso decimos que los anillos son *anillos isomorfos*.

Ejercicio 76. —

(i) Si $h : R \to S$ es un homomorfismo de anillos, entonces $h(0) = 0$, $h(-r) = -h(r)$.

(ii) Si $h : R \to S$ es un isomorfismo de anillos, entonces $h^{-1} : S \to R$ también lo es.

(iii) La propiedad de ser isomorfos es una relación de equivalencia en el conjunto de todos los anillos.

(iv) Si $h : R \to S$ es un homomorfismo de anillos, entonces

$$Ker(h) = \{r \in R : h(r) = 0\}$$

es un subanillo de R, llamado el núcleo de h y

$$Im(h) = \{s \in S : \text{ existe } r \in R \text{ tal que } h(r) = s\}$$

es un subanillo de S, llamado la imágen de h.

(v) Sea $h : R \to S$ un homomorfismo de anillos. Verificar que la imágen de subanillos de R son subanillos de S y, recíprocamente, la preimágen de subanillos de S son subanillos de R.

(vi) Si $h : R \to S$ es homomorfismo de anillos y R tiene unidad 1, entonces $h(1) = x$ debe satisfacer la ecuación $x^2 = x$ en S. Concluir que

(a) las funciones $h : \mathbb{Z} \to 2\mathbb{Z} : n \mapsto 2n$, y $h : \mathbb{Z} \to \mathbb{Z} : n \mapsto 2n$, no son homomorfismo de anillos ; y

(b) determinar todos los homomorfismos de anillos $h : \mathbb{Z} \to \mathbb{Z}$.

(vii) Calcular Hom$((\mathbb{Z}\times\mathbb{Z}, +))$ y verificar que este anillo no es isomorfo al anillo $\mathbb{Z}\times\mathbb{Z}$.

Ejemplo 20.0.26. — Sea R un anillo y variables x, y para formar los anillos de polinomios $R[x, y]$ y $R[y, x]$. Los polinomios en $R[x, y]$ son de la forma

$$\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} a_i^j x^i\right) y^j$$

y los de $R[y, x]$ son de la forma

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_i^j y^j\right) x^i$$

Podemos considerar la función $\phi : R[x, y] \to R[y, x]$, definida como

$$\phi\left(\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} a_i^j x^i\right) y^j\right) = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} a_i^j y^j\right) x^i$$

la cual defne un isomorfismo de anillos. De esta manera, podemos hablar indistintamente de uno u otro y usaremos cualquiera de las siguientes notaciones para representar un polinomio en las varaibles x, y y coeficientes en R :

$$\sum_{i,j=0}^{\infty} a_i^j x^i y^j = \sum_{i,j=0}^{\infty} a_i^j y^j x^i$$

Lo anterior se generaliza a más variables.

Ejercicio 77. — *Verificar los detalles del ejemplo anterior.*

Ejemplo 20.0.27. — Consideremos un anillo conmutativo R y su anillo de polinomios en una variable $R[x]$. Supongamos que S es un subanillo de R. Entonces tenemos que el anillo de polinomios $S[x]$ es un subanillo de $R[x]$. Para cada $r \in R$, definamos la función

$$E_r : S[x] \to R : \sum_{j=0}^{\infty} a_j x^j \mapsto \sum_{j=0}^{\infty} a_j r^j$$

Recordemos que los coeficientes a_j son igual a 0 con la posible excepción de un número finito de índices, luego la función anterior tiene sentido. Por la definición de suma y multiplicación de polinomios podemos verificar que E_r es de hecho un homomorfismo de anillos, llamado el *homomorfismo de evaluación en* r. Podemos además ver que si S tiene unidad 1, entonces tenemos el polinomio $x \in S[x]$, para el cual $E_r(x) = r$. Si identificamos S con los polinomios de grado cero, entonces $E_r : S \to R : s \mapsto s$ es un isomorfismo. El núcleo del homomorfismo E_r está formado por todos aquellos

polinomios $p \in S[x]$ tales que $E_r(p) = 0$. Diremos en tal caso que r es un *cero del polinomio* p.
Si consideramos por ejemplo el polinomio $1 + x^2 \in \mathbb{R}[x]$, entonces este no tiene ceros en $\mathbb{R}$, pero si tiene ceros en $\mathbb{C}$. En forma similar, si tomamos $S = \mathbb{Q}$, entonces el polinomio $2-x^2 \in \mathbb{Q}[x]$ no tiene ceros en $\mathbb{Q}$, pero si los tiene en $\mathbb{R}$. Así, podemos ver que es probable que un polinomio $p \in S[x]$ no tenga ceros en S, pero que exista un anillo R, conteniendo a S como subanillo, donde si tiene ceros. En un capítulo posterior nos preocuparemos de este problema para el caso en que nuestros anillos son cuerpos ya que esto simplificará mucho las operaciones.

Ejercicio 78. — *Verificar que*

$$\phi : \mathbb{C} \to M(2, \mathbb{R}) : x + iy \mapsto \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

es un isomorfismo.

CAPÍTULO 21

IDEALES Y ANILLOS COCIENTES

En el capítulo de grupos vimos que hay ciertos subgrupos muy especiales, estos son los subgrupos normales. Estos subgrupos tienen la propiedad de que el cociente resulta ser un grupo, el grupo cociente. A nivel de anillos podemos hacer lo mismo. Supongamos que tenemos un anillo $(R, +, \cdot)$ y un subanillo S de R. Entonces, al ser $(R, +)$ un grupo abeliano y S subgrupo de $(R, +)$, tenemos que este es subgrupo normal de manera trivial. Así, podemos formar el grupo cociente $(R/S, +)$ que es también un grupo abeliano. Tenemos la proyección natural

$$\pi : R \to R/S : r \mapsto r + S$$

que es un homomorfismo sobreyectivo de grupos. Hasta ahora no hemos involucrado la operación de multiplicación. Nuestra pregunta natural es :
¿Es posible dotar a R/S de una multiplicación que le transforme en un anillo de manera que π resulte un homomorfismo de anillos ?
Observemos que la condición $\pi(r_1 r_2) = \pi(r_1)\pi(r_2)$ es equivalente a tener la definición de multiplicación siguiente :

$$r_1 r_2 + S = (r_1 + S)(r_2 + S) = r_1 r_2 + r_1 S + S r_2$$

Tomando $r_2 = 0$ obtenemos que $r_1 S \subset S$ y tomando $r_1 = 0$ obtenemos que $S r_2 \subset S$. Así, condiciones necesarias para que tenga sentido la multiplicación anterior es que

$$rS \subset S, \quad Sr \subset S$$

valga para todo $r \in S$. En forma recíproca, si valen las dos condiciones necesarias, entonces tenemos que $\pi(r_1 r_2) = \pi(r_1)\pi(r_2)$ es válida para todos $r_1, r_2 \in R$.
Por otro lado, una vez que tenemos la validéz de lo anterior, entonces es fácil ver que la propiedad distributiva es válida.

Definición 21.0.28. — Diremos que un subanillo S de un anillo R es un *ideal izquierdo* si para todo $r \in R$ vale que $rS \subset S$ y es un *ideal derecho* si para todo $r \in R$ vale que $Sr \subset S$. Un *ideal* es un subanillo que es ideal izquierdo y derecho.

Luego, lo anterior nos está diciendo lo siguiente : El tipo de anillos en el cual estaremos interesados es el siguiente.

Proposición 21.0.29. — *R/S es un anillo (llamado* anillo cociente*), que hace de la proyección $\pi : R \to R/S$ un homomorfismo de anillos, sí y sólo si S es un ideal de R.*

De lo anterior vemos que el equivalente, en la teoría de anillos, de los subgrupos normales son los ideales. También nos dimos cuenta que podemos ver cada subgrupo normal de un grupo como el núcleo de algún homomorfismo y que todo núcleo de un homomorfismo de grupos es subgrupo normal. Para los anillos tenemos la situación similar. Lo anterior nos permite ver cada ideal como el núcleo de algún homomorfismo de anillos. Por otro lado, si $h : R \to S$ es un homomorfismo de anillos, entonces Ker(h) es un ideal de R. En efecto, si $r_1, r_2 \in$ Ker(h), entonces $h(r_1 r_2) = h(r_1)h_(r_2) = 0$, luego $r_1 r_2 \in$ Ker(h), obteniendo que h es subanillo. Por otro lado, si $r \in R$ y $s \in$ Ker(h), entonces $h(rs) = h(r)h(s) = 0$, $h(sr) = h(s)h(r) = 0$ diciendo que $rs, sr \in$ Ker(h), es decir, Ker(h) es ideal.
Supongamos que tenemos un homomorfismo de anillos

$$h : R \to S.$$

Consideremos el ideal $K =$ Ker(h) y la proyección $\pi : R \to R/K$. Entonces podemos definir la nueva función

$$t : R/K \to S : r + K \mapsto h(r)$$

la cual estś bién definida y resulta ser un homomorfismo de anillos inyectivo ; luego los anillos $h(R)$ y R/K son isomorfos.

Ejercicio 79. — *Completar los detalles de lo anterior.*

Proposición 21.0.30. — *Sea R una anillo con unidad 1 y sea I un ideal de R. Si $1 \in I$, entonces $I = R$. En particular, los únicos ideales de un cuerpo R son $\{0\}$ y R.*

Demonstración. — Si $1 \in I$, entonces para todo $r \in R$ debemos tener $r = r \cdot 1 \in I$. Supongamos ahora que R es un cuerpo y que $I \neq \{0\}$. Sea $s \in I$, $s \neq 0$. Como R es cuerpo, existe $s^{-1} \in R$ y luego $1 = s^{-1}s \in I$. □

Ejercicio 80. —
(i) Determinar todos los ideales de $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$.
(ii) Verificar que si R es un anillo con unidad y S es un ideal de R, $S \neq R$, entonces el anillo cociente R/S tiene unidad.

Ejercicio 81. — *Verificar que la intersección arbitraria de ideales es un ideal.*

Ejemplo 21.0.31. — Sea R un anillo conmutativo y consideremos el homomorfismo de evaluación $E_0 : R[x] \to R$. Su núcleo es el ideal formado por todos los polinomios en $R[x]$ cuyo coeficiente constante es igual a 0. Luego $R/\text{Ker}(E_0)$ es un anillo conmutativo isomorfo a R. Cada clase de equivalencia en $R/\text{Ker}(E_0)$ es representado por un polinomio con término constante fijo.

Definición 21.0.32. — Sea $M \subset R$ un subconjunto de un anillo R. Definimos el *ideal generado por* M al ideal más pequeño que contiene a M, donotado por $\langle M \rangle$.

Una consecuencia del ejercicio anterior es el siguiente

Proposición 21.0.33. — *Sea $M \subset R$, donde R es un anillo. Entonces*

$$\langle M \rangle = \bigcap_{\substack{I \text{ Ideal de } R \\ M \subset I}} I$$

Ejercicio 82. — *Si un anillo R tiene unidad 1 y $r \in R$ es invertible, entonces $\langle r \rangle = R$.*

Definición 21.0.34. — Un ideal que se pueda generar con un elemento es llamado un *ideal principal*. Así, en un cuerpo tenemos tenemos que todo ideal es principal. Por supuesto, si R es cualquier anillo con unidad, entonces R es ideal principal.

Ejercicio 83. — *Sean $r_1, ..., r_n \in \mathbb{Z}$ tales que el ideal $I = \langle r_1, ..., r_n \rangle$ sea principal. Verificar que si d es el máximo común divisor de $\{r_1, ..., r_n\}$, entonces $I = \langle d \rangle$. Ind. Recordar que existen enteros $a_1, ..., a_n$ tales que $a_1 r_1 + \cdots a_n r_n = d$.*

Ejemplo 21.0.35. — Consideremos el anillo de polinomios $\mathbb{Z}[x]$, el cual es un dominio entero. Sea $I = \{\sum_{j=1}^{\infty} a_j x^j \in \mathbb{Z}[x] : a_0 = 0\}$. Entonces vemos que la propiedad de tener término constante igual a cero se preserva bajo suma y multiplicación, de lo cual obtenemos que I es un ideal de $\mathbb{Z}$. Consideremos el ideal principal $\langle x \rangle$ el cual está contenido en I. Como todo elemento de I es suma de productos de polinomios monomiales con el polinomio x, observamos que $I = \langle x \rangle$. Por otro lado, si consideramos el ideal J generado por los polinomios 2 y x, entonces este no puede ser principal. Esto por que si lo fuese, digamos generado por el polinomio q, entonces tener $qp = 2$ para algún polinomio p obliga a tener q de grado cero, es decir que $q \in \mathbb{Z}$. Además, als únicas posibilidades para q, módulo signo, son $q = 1$ ó $q = 2$. En el caso $q = 1$ diriamos que $J = \mathbb{Z}[x]$, pero el ideal J sólo contiene polinomios con coeficiente par. Si $q = 2$, entonces debe existir un polinomio f tal que $2f = x$, pero $2f$ tiene coeficientes pares. Luego, en cualquier caso obtenemos una contradicción y, en particular, obtenemos que J no es principal. En resumen, en el dominio entero $\mathbb{Z}[x]$ hay ideales que no son principales.

Ejercicio 84. — *Sea R un anillo conmutativo y $r \in R$.*
(i) Verificar que

$$I_r = \{x : rx = 0\}$$

es un ideal de R.
(ii) Verificar que si S es un ideal de R, entonces

$$\sqrt{S} = \{x \in R : x^n \in S \text{ para algún } n > 0\}$$

es un ideal de R; llamado el radical *de S.*

Ejercicio 85. — *Sea R un anillo y dos ideales U y V de R. Defina*

$$U + V = \{u + v : u \in U, v \in V\}$$

$$UV = \{\sum_{i=1}^{n} u_i v_i : u_i \in U, v_i \in V, n \in \{1, 2, 3, ...\}\}$$

Verificar que $U + V$ y UV son ideales de R, tales que $U, V \subset U + V$ y $UV \subset U \cap V$.

CAPÍTULO 22

IDEALES PRIMOS Y MAXIMALES

Ahora que sabemos que para construir anillos cocientes necesitamos cocientar anillos por ideales, podemos preguntarnos que tipo de ideal es necesario para que el cociente sea un dominio entero ó aún mejor un cuerpo. Consideremos un anillo R y un ideal I de R. Miremos el anillo cociente R/I. Si $I = R$, entonces R/I es el anillo $\{0\}$, el cual no tiene unidad. Supongamos entonces que I es ideal propio de R. Es claro que si R es conmutativo y tiene unidad, entonces R/I también es conmutativo y tiene unidad. Supongamos entonces que R es de tal tipo. Para obtener que R/I sea un dominio entero debemos asegurarnos que no tiene divisores de cero. La existencia de divisores de cero en R/I implica la existencia de dos elementos $x + I, y + I$, donde $x, y \notin I$, tales que $(x+I)(y+I) = I$, es decir, $xy \in I$. Luego, la no existencia de divisores de cero en R/I es equivalente a la propiedad siguiente :

si $x, y \in R$ son tales que $xy \in I$, entonces $x \in I$ ó $y \in I$.

Definición 22.0.36. — Un ideal propio de R con tal propiedad que si $x, y \in R$ son tales que $xy \in I$, entonces $x \in I$ ó $y \in I$, es llamado un *ideal primo*.

Ahora, para que además R/I sea un cuerpo, debemos tener que todo elemento $x + I$, donde $x \notin I$, posee un inverso, es decir, debe existir $y \notin I$ tal que $(x+I)(y+I) = 1+I$, lo cual es equivalente a tener $xy \in 1 + I$. Luego, tenemos que R/I es un cuerpo sí y sólo si

I es ideal primo y además para cada $x \in R - I$, existe $y \in R - I$ tal que $xy - 1 \in I$.

Definición 22.0.37. — Un ideal primo I con tal que para cada $x \in R - I$, existe $y \in R - I$ tal que $xy - 1 \in I$, es llamado un *ideal maximal*.

La razón de este nombre es la siguiente. Primero, si tenemos un ideal maximal I contenido estrictamente en otro ideal J de R, entonces existe $j \in J - I$. luego debe existir $h \in R - I$

tal que $hj - 1 \in I$. Esto dice que existe $i \in I$ tal que $hj - 1 = i$, con lo cual obtenemos $1 = hj - i \in J$, es decir $J = R$. En otras palabras, un ideal maximal no puede estar contenido propiamente en otro ideal propio de R. En forma recíproca, si tenemos un ideal propio I de R con la propiedad que no existe ideal propio de R conteniendolo, entonces tenemos

(i) Si $x \in R - I$ es tal que $x \notin I$, entonces consideremos el ideal generado por I y x. Como $x \notin I$, este ideal contiene estrictamente a I, luego debe ser R, es decir, $1 \in \langle x, I \rangle$. Como $1 \notin I$, tenemos que $1 = xy + i$, para cierto $i \in I$ y cierto $y \in R - I$.

(ii) Si $x, y \in R$ son tales que $xy \in I$. Supongamos que $x, y \notin I$. Por (i) tenemos que existen $u, v \notin I$ tales que $xu - 1, yv - 1 \in I$. En este caso, $xyuv - xu - yv + 1 = (xu - 1)(yv - 1) \in I$ y como $xy \in I$, tenemos que $xu - (yv - 1) = xu - yv + 1 \in I$ y, en particular, $xu \in I$. Est último junto a tener $xu - 1 \in I$ nos obliga atener $1 \in I$, una contradicción. Luego I debe ser primo.

De esta manera obtenemos la definición equivalente de un ideal maximal :

Teorema 22.0.38. — *Un ideal maximal es un ideal propio de R que no está contenido estrictamente en otro ideal propio de R.*

Resumiendo todo lo anterior, tenemos :

Proposición 22.0.39. — *Sea R un anillo conmutativo con unidad e I un ideal propio de R. Entonces :*

(1) R/I es un dominio entero sí y sólo si I es un ideal primo.

(2) R/I es un cuerpo sí y sólo si I es un ideal maximal.

(3) Todo ideal maximal es primo.

Ejemplo 22.0.40. — En un cuerpo $\mathbb{K}$ tenemos sólo dos ideales : $\{0\}$ y $\mathbb{K}$. En este caso $\{0\}$ es el único ideal propio y además es maximal y $\mathbb{K}/\{0\}$ es isomorfo a $\mathbb{K}$. Supongamos ahora que R es un anillo conmutativo con unidad de manera que sus únicos ideales son $\{0\}$ y R. Entonces $\{0\}$ es ideal maximal y como $R/\{0\}$ es isomorfo a R, tenemos que R debe ser un cuerpo.

Proposición 22.0.41. — *Sea R una anillo conmutativo con unidad. Entonces R es un cuerpo sí y sólo si sus únicos ideales son $\{0\}$ y R.*

Ejemplo 22.0.42. — Consideremos el domnio entero $\mathbb{Z}$. Sus subgrupos aditivos son de la forma $m\mathbb{Z}$, donde $m \in \{0, 1, 2, ...\}$. Estos son cerrados bajo la operación de multiplicación, luego son sus subanillos. Si multiplicamos cualquier entero por un múltiplo de m volvemos a tener un múltiplo de m, es decir, todos sus subanillos son ideales. Esto se

parece mucho al hecho que en un grupo abeliano todos sus subgrupos son normales. Estos ideales son principales, generado por m. Como sabemos que $\{0\}$ es siempre un ideal primo, consideremos $m > 1$ (el caso $m = 1$ nos dá todo el anillo $\mathbb{Z}$). En este caso, si tenemos dos enteros $a, b \in \mathbb{Z}$ tales que $ab \in m\mathbb{Z}$, entonces debe ocurrir que los factores primos de m se distribuyen en a y b. Así, m es un número primo sí y sólo si $m\mathbb{Z}$ es un ideal primo. Como todo ideal $m\mathbb{Z}$, donde $m = pq$, siempre está contenido en el ideal $p\mathbb{Z}$, también obsevamos que los ideales primos son maximales. Como consecuencia, para todo número primo p tenemos que el anillo cociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

Definición 22.0.43. — Los cuerpos $\mathbb{Z}/p\mathbb{Z}$, donde p es primo, y $\mathbb{Q}$ reciben el nombre de *cuerpos primos*.

Definición 22.0.44. — Supongamos que tenemos un anillo R con unidad. Si existe un entero $n > 0$ tal que $n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}} = 0$, diremos que el menor de tales enteros es la *característica* de R. En caso de no existir tal valor, decimos que la característica de R es 0.

Por ejemplo, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{\pm d}]$, donde $d > 0$ no es el cuadrado de un entero, tienen caraterística 0, mientras que los anillos $\mathbb{Z}/m\mathbb{Z}$ tienen característica m. Consideremos el homomorfismo

$$\Phi : \mathbb{Z} \to R : n \mapsto n \cdot 1$$

cuyo núcleo es $m\mathbb{Z}$, si m es la característica de R. En particular, si $m = 0$, entonces Φ es un homomorfismo inyectivo. Esto nos dá la siguiente in formación :

Proposición 22.0.45. — *Sea R un anillo con característica m.*
(1) Si $m = 0$, entonces R contiene un subanillo isomorfo a $\mathbb{Z}$.
(2) Si $m > 0$, entonces R contiene un subanillo isomorfo a $\mathbb{Z}/m\mathbb{Z}$.
(3) Si R es un cuerpo de característica 0, entonces este contiene un subcuerpo isomorfo a $\mathbb{Q}$.
(4) Si R es un cuerpo de característica m, entonces m debe ser primo y R contiene un subcuerpo isomorfo a $\mathbb{Z}/m\mathbb{Z}$.

Demonstración. — Lo único que falta por verificar es que la característica de un cuerpo R es cero ó un número primo. En efecto, supongamos que la característica es diferente de cero e igual a un valor $m > 0$. Usando el homomorfismo Φ obtenemos que R contiene un subanillo isomorfo a $\mathbb{Z}/m\mathbb{Z}$, el cual contiene divisores de cero para m no primo ; luego, m está obligado ser un número primo. □

Ejemplo 22.0.46. — Otro ejemplo importante de ideal maximal es el siguiente. Sea (X, τ) un espacio topológico y sea $p \in X$ algún punto que fijaremos. Denotemos por $\widehat{\mathcal{G}}_p$ al conjunto de todas las funciones a valores reales definidas en algún entorno abierto de p. Definimos en $\widehat{\mathcal{G}}_p$ la siguiente relación de equivalencia. Si

$$f : U_f \to \mathbb{R}, g : U_g \to \mathbb{R} \in \widehat{\mathcal{G}}_p,$$

entonces decimos que ellas son equivalentes si es posible encontrar un abierto $V \subset U_f \cap U_g$, $p \in V$, de manera que $f = g$ en V. Denotemos por $[f]$ la clase de equivalencia de $f : U_f \to \mathbb{R} \in \widehat{\mathcal{G}}_p$ y por $\mathcal{G}_p$ al conjunto de classes de equivalencia. Cada clase $[f]$ es llamada un germen de función real continua en p y $\mathcal{G}_p$ el anillo de funciones reales continuas en p. Para ver que $\mathcal{G}_p$ es en efecto un anillo, de hecho un dominio de intero, definimos las operaciones :

$$[f] + [g] = [f + g]; [f][g] = [fg],$$

donde las operaciones $f + g, fg$ están definidas en un abierto común de definición. El elemento unidad es dada por el germen de la función constante 1 y la denotamos por $[1]$. La definición de la relación de equivalencia nos asegura que si $[f] = [g]$, entonces $f(p) = 0$ sí y sólo si $g(p) = 0$. La continuidad nos asegura que si $[f]$ es tal que $f(p) \neq 0$, entonces existe $[1/f]$, en particular, $[f]$ es invertible. Más aún, los elementos invertibles de $\mathcal{G}_p$ son exáctamente las clases $[f]$ tales que $f(p) \neq 0$.
El conjunto

$$m_p = \{[f] \in \mathcal{G}_p : f(p) = 0\},$$

es un ideal maximal de $\mathcal{G}_p$. Esto es dado por :
(i) si $[f], [g] \in m_p$, es decir $f(p) = g(p) = 0$, entonces $(f + g)(p) = 0$ de donde $[f + g] \in m_p$;
(ii) si $[f] \in m_p$, entonces $-f(p) = 0$, es decir, $-[f] = [-f] \in m_p$;
(iii) si $[f] \in m_p$ y $[g] \in \mathcal{G}_p$, entonces $f(p)g(p) = 0$, luego, $[f][g] \in m_p$.
Como cada $[f]$ con $f(p) \neq 0$ es invertible, esto nos dice que m_p es de hecho el único ideal maximal de $\mathcal{G}_p$.

Ejercicio 86. — *Vea que si reemplazamos (X, τ) por un abierto de $\mathbb{R}^n$ y en vez de considerar funciones continuas consideramos funciones de clase C^k, entonces obtenemos el mismo resultado. Analice también el caso cuando reeplazamos X por un abierto del plano complejo y reemplazamos la continuidad por analiticidad.*

CAPÍTULO 23

CUERPO COCIENTE DE UN DOMINIO ENTERO

Hemos visto que todo cuerpo es en particular un dominio entero y que todo dominio entero finito es necesariamente un cuerpo. El anillo $\mathbb{Z}$ es un ejemplo de un dominio entero infinito que no es un cuerpo. Nos podemos preguntar si es posible encontrar un cuerpo, lo más pequeño posible, que contenga al dominio como subanillo. Veamos por ejemplo el dominio anterior $\mathbb{Z}$. Podemos ver que si el cuerpo $\mathbb{Q}$ le contiene como un subanillo. Por otro lado, si tenemos un cuerpo K conteniendo a $\mathbb{Z}$ y $n \in \mathbb{Z}$, entonces debe existir $n^{-1} \in K$ y, en particular, los elementos $nm^{-1} = \frac{n}{m} \in K$. De esta manera vemos que $\mathbb{Q}$ es el cuerpo más pequeño conteniendo a $\mathbb{Z}$. La construcción de $\mathbb{Q}$ puede realizarse de la siguiente manera. Consideremos el conjunto

$$Q = \{(r, s) \in \mathbb{Z}^2 : s \neq 0\}$$

y la función

$$L : Q \to \mathbb{Q} : (r, s) \mapsto \frac{r}{s}$$

Vemos que L es sobreyectiva pero no es inyectiva ya que es fácil ver que $L(r, s) = L(u, v)$ sí y sólo si $rv = su$. Consideremos la relación de equivalencia

$$(r, s) \cong (u, v) \iff rv = su$$

y denotemos por $\mathbb{Q}_{\mathbb{Z}}$ al conjunto de las clases de equivalencia. Así, podemos considerar la función inducida

$$L : \mathbb{Q}_{\mathbb{Z}} \to \mathbb{Q} : [(r, s)] \mapsto \frac{r}{s},$$

la cual es ahora una biyección. Podemos usar L para escribir las operaciones de suma y multiplicación de números racionales, obteniendo en $\mathbb{Q}_{\mathbb{Z}}$ las correspondientes operaciones :

$$[(r, s)] + [(u, v)] = [(rv + su, sv)]$$
$$[(r, s)] \cdot [(u, v)] = [(ru, sv)]$$

De esta manera obtenemos en $\mathbb{Q}_{\mathbb{Z}}$ una estructura de cuerpo el cual es isomorfo a $\mathbb{Q}$ por el isomomorfismo L. La función

$$J : \mathbb{Z} \to \mathbb{Q}_{\mathbb{Z}} : n \mapsto [(n, 1)]$$

resulta ser un homomorfismo inyectivo de anillos.
Lo anterior nos permite generalizar la construcción para cualquier dominio entero R. Consideramos el conjunto

$$Q = \{(r, s) \in \mathbb{R}^2 : s \neq 0\}$$

y la relación de equivalencia

$$(r, s) \cong (u, v) \Longleftrightarrow rv = su$$

Denotemos por $\mathbb{Q}_R$ al conjunto de las clases de equivalencia y definimos las correspondientes operaciones :

$$[(r, s)] + [(u, v)] = [(rv + su, sv)]$$
$$[(r, s)] \cdot [(u, v)] = [(ru, sv)]$$

Ejercicio 87. — *Verificar que las operaciones anteriores hacen de $\mathbb{Q}_R$ un cuerpo y que la función*

$$J : R \to \mathbb{Q}_R : r \mapsto [(r, 1)]$$

resulta ser un homomorfismo inyectivo de anillos.

Por otro lado, supongamos que tenemos un cuerpo $\mathbb{K}$ y un homomorfismo inyectivo $\Phi : R \to \mathbb{K}$. Entonces podemos definir la función

$$\Psi : \mathbb{Q}_R \to \mathbb{K} : [(r, s)] \mapsto \Phi(r)\Phi(s)^{-1}$$

Para ver que esta función está bién definida, observemos que si $(r, s) \cong (u, v)$, entonces $rv = su$. Luego $\Phi(rv) = \Phi(su)$, es decir, $\Phi(r)\Phi(v) = \Phi(s)\Phi(u)$ ó equivalentemente $\Phi(r)\Phi(s)^{-1} = \Phi(u)\Phi(v)^{-1}$.
La función Ψ es inyectiva ya que si $\Psi([(r, s)]) = \Psi([(u, v)])$, entonces $\Phi(r)\Phi(s)^{-1} = \Phi(u)\Phi(v)^{-1}$ ó equivalentemente $\Phi(rv) = \Phi(us)$. Com Φ es inyectiva, esto nos dice que $rv = us$, es decir, $[(r, s)] = [(u, v)]$.
Veamos que Ψ es de hecho un homomorfismo de anillos. Como todo cuerpo es conmutativo y Φ es homomorfismo, tenemos

$$\Psi([(r, s)] + [(u, v)]) = \Psi([rv + su, sv)] = \Phi(rv + su)\Phi(sv)^{-1} =$$
$$= (\Phi(r)\Phi(v) + \Phi(s)\Phi(u))\Phi(v)^{-1}\Phi(s)^{-1} = \Phi(r)\Phi(s)^{-1} + \Phi(u)\Phi(v)^{-1} =$$
$$= \Psi([(r, s)]) + \Psi([(u, v)])$$

$$\Psi([(r, s)] \cdot [(u, v)]) = \Psi([(ru, sv)] = \Phi(ru)\Phi(sv)^{-1} =$$
$$= \Phi(r)\Phi(s)^{-1}\Phi(u)\Phi(v)^{-1} = \Psi([(r, s)])\Phi([(u, v)])$$

Podemos resumir todo lo anterior en el siguiente :

Teorema 23.0.47. — *Sea R un dominio entero. Entonces existe un cuerpo $\mathbb{Q}_R$ y un homomorfismo inyectivo $J : R \to \mathbb{Q}_R$ de manera que si si $\mathbb{K}$ es cualquier cuerpo y $\Phi : R \to \mathbb{K}$ es un homomorfismo inyectivo, entonces existe un homomorfismo inyectivo $\Psi : \mathbb{Q}_R \to \mathbb{K}$ tal que $\Psi \circ J = \Phi$.*

Lo anterior nos está diciendo que el cuerpo $\mathbb{Q}_R$ es el cuerpo más pequeño conteniendo una copia isomorfa de R.

Definición 23.0.48. — Sea R un dominio entero. El cuerpo $\mathbb{Q}_R$ es llamado el *cuerpo de fracciones* del dominio R. Es costumbre denotar cada clase $[(r, s)]$ como la fracción $\frac{r}{s}$.

Ejercicio 88. — *Sea $d > 0$ un entero que no es cuadrado de otro entero y consideremos el dominio $\mathbb{Z}[\sqrt{d}]$. Verificar que su cuerpo de fracciones es isomorfo a $\mathbb{Q}[\sqrt{d}]$.*

CAPÍTULO 24

DOMINIOS EUCLIDIANOS, PRINCIPALES Y FACTORIZACIÓN ÚNICA

24.1. Dominios Euclidianos

Definición 24.1.1. — Diremos que un dominio entero D es un *Dominio Euclidiano* si existe una función

$$v : D - \{0\} \to \{0, 1, 2, ...\}$$

llamada una *valuación* en D que satisface las siguientes dos propiedades :
(v1) Para cada par $a, b \in D$, $b \neq 0$, existen $s, r \in D$ tales que

$$a = sb + r$$

donde $r = 0$ ó bién $v(r) < v(b)$. El valor r es llamado el *resto* de dividir a por b ;
(v2) Para cada par $a, b \in D - \{0\}$, se tiene que $v(a) \leq v(ab)$.

Ejemplo 24.1.2. —
(i) El dominio $D = \mathbb{Z}$ con la valuaci'on usual $v(n) = |n|$ es un dominio Euclidiano. En efecto, si tomamos dos enteros $a, b \in \mathbb{Z}$, donde $b \neq 0$, entonces se puede ver que existen enteros r, s tales que $a \in [sb, s(b + 1))$. Si $a = sb$, entonces $r = 0$. Si $a \neq sb$, entonces $r = a - sb$ y es claro en este caso que $|r| < |b|$. También es claro que si $a, b \in \mathbb{Z} - \{0\}$, entonces $|a| \leq |ab|$.
(ii) Si F es un cuerpo, entonces usando la valuación trivial $v(r) = 0$, obtenemos que F es dominio Euclidiano. En este caso, siempre ocurre que el resto $r = 0$.
(iii) Sea $D = F[x]$, donde F es un cuerpo y la valuación $v(p(x))$ siendo el grado del polinomio $p(x)$. Es claro que la función grado satisface ser una valuación usando la división usual de polinomios. Verificar los detalles.
(iv) El dominio entero $\mathbb{Z}[x]$ no es un dominio Euclidiano. Esto lo veremos más tarde.

Ejercicio 89. —

(1) Verificar que el dominio entero $\mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\}$*, llamado el anillo de los* enteros Gausianos*, resulta ser un dominio Euclidiano con la valuación* $v(a+bi) = a^2 + b^2$.

(2) Sea $d \in \{2, 3, 5, 6, ...\}$ *un entero que no es cuadrado de otro entero y consideremos el dominio entero* $\mathbb{Z}[\sqrt{d}]$*. Utilize* $v(a + b\sqrt{d}) = a - db^2$ *y verifique si este es dominio Euclidiano.*

(3) Sea $d \in \{2, 3, 5, 6, ...\}$ *un entero que no es cuadrado de otro entero y consideremos el dominio entero* $\mathbb{Z}[\sqrt{-d}]$*. Utilize* $v(a + b\sqrt{-d}) = a + db^2$ *y verifique si este es dominio Euclidiano.*

Ahora procedemos a enunciar el algoritmo de división que tenemos en todo dominio entero. De manera más precisa :

***Proposición 24.1.3* (Algoritmo de División).** — *Sea* D *un dominio Euclidiano respecto a la valuación* $v : D - \{0\} \to \{0, 1, 2, ..\}$*. Entonces para todo par* $p, q \in D - \{0\}$ *existen* $a, b \in D$ *tales que* $MCD(p, q) = ap + bq$*. En particular, si* p *y* q *son relativamente primos, entonces existen* $a, b \in D$ *tales que* $ap + bq = 1$.

Demonstración. — Sean $p, q \in D - \{0\}$ y $d = MCD(p, q)$. Por la propiedad de división existen $r_1, t_1 \in D$ tales que $p = qt_1 + r_1$, donde $r_1 = 0$ ó $v(r_1) < v(q)$.
Si tenemos que $r_1 = 0$, entonces $MCD(p, q) = q$ y estamos listos tomando $a = 0, b = 1$.
Si tenemos que $r_1 \neq 0$, entonces podemos proceder como antes usando q en lugar de p y r_1 en lugar de q para obtener valores $r_2, t_2 \in D$ tales que $q = r_1t_2 + r_2$, donde $r_2 = 0$ ó $v(r_2) < v(r_1)$.
Si $r_2 = 0$, entonces tenemos que $MCD(p, q) = r_1$ y estaremos listos tomando $a = 1$ y $b = -t_1t_2$.
Si tenemos que $r_2 \neq 0$, entonces seguimos con este proceso inductivo. Como $v(q) > v(r_1) > v(r_2) > \cdots \geq 0$ y la valuación v toma valores enteros, este proceso terminará después de un número finito de pasos. □

24.2. Dominios de Ideales Principales

Definición 24.2.1. — Un dominio entero para el cual todo ideal es principal es llamado un *dominio de ideales principales*.

Ejemplo 24.2.2. —

(i) Todo cuerpo F es un dominio de ideales principales. Este hecho se debe a que los únicos ideales de un cuerpo son $\{0\}$ y $F =< 1 >$.

(ii) Sea D un dominio de idelaes principales. Entonces si $a_1, ..., a_n \in D - \{0\}$, existe un máximo común divisor $MCD(a_1, ..., a_n) \in D$ para ellos. Más aún, el ideal generado por $a_1, ..., a_n$ es igual al ideal generado por $MCD(a_1, ..., a_n)$. En particular, esto

nos asegura que dos máximos común divisores de tales elementos son uno el múltiplo del otro por un elemento invertible en D. En efecto, sea I el ideal generado por los elementos a_1,..., a_n. Como estamos en un ideal principal, existe $d \in D$ tal que $I =< d >$. En particular, todo divisor común a los elementos a_1,..., a_n debe dividir d ya que $d = r_1x_1 + \cdots + r_nx_n$ al pertenecer al ideal I generado por los elementos a_j. Por otro lado, como cada $a_j \in I =< d >$, tenemos que $x_j = s_jd$, con lo cual vemos que d divide a cada a_j, obteniendo en resumen que d es un máximo común divisor de a_1,..., a_n. Si tenemos $d_1 \in D$ otro máximo común divisor de estos elementos, entonces I es subanillo del ideal $< d_1 >$. Esto asegura que d_1 divide d, es decir $d = ad_1$. Como d_1 es máximo común divisor y d divide a los elementos a_1,..., a_n, debemos tener que d divide d_1, es decir $d_1 = bd$. Esto nos dice que $d_1 = bd = bad_1$, de donde $d_1(1-ba) = 0$. Pero $d_1 \neq 0$ y estamos en un dominio entero, es decir, no hay divisores de cero, luego $ab = 1$, es decir, a es invertible en D.

(iii) El dominio entero $\mathbb{Z}[x]$ no es dominio de ideales principales. En efecto, consideremos el ideal I generado por 2 y x. Es claro que I consiste de polinomios cuyo coeficiente constante es par. Por otro lado, si $\mathbb{Z}[x]$ fuese un dominio de idelaes principales, parte (ii) anterior nos dice que I seria generado por el $MCD(2, x) = 1$, es decir, $I = \mathbb{Z}[x]$, una contradicción.

24.3. Dominios de Factorización Única

Definición 24.3.1. — Sea D un dominio entero y $a \in D - \{0\}$. Diremos que que a es un *elemento irreducible* si no es invertible y no puede escribirse como producto de dos elementos ambos no invertibles.

Ejemplo 24.3.2. — Consideremos un dominio Euclidiano D con valuación $v : D - \{0\} \to \{0, 1, 2, ...\}$. Se puede verificar que los elementos invertibles de D es exactamente el conjuto

$$\{a \in D : a \text{ invertible}\} =$$
$$\{a \in D : v(a) = v(1)\} =$$
$$\{a \in D - \{0\} : v(b) = v(ab) \text{ para todos } b \in D - \{0\}\}$$

En efecto, si $a \in D$ es invertible, entonces $v(b) \leq v(ab) \leq v(a^{-1}ab) = v(b)$, es decir, $v(b) = v(ab)$. En particular, para $b = 1$ lo anterior asegura que $v(a) = v(1)$. Recíprocamente, si a es tal que $v(b) = v(ab)$ para algún $b \in D - \{0\}$, entonces al dividir b por ab obtenemos que

$$b = s(ab) + r$$

donde $r = 0$ ó $v(r) < v(ab) = v(b)$. Ahora, $r = b - s(ab) = (1 - sa)b$ de donde $v(b) \leq v(r) < v(b)$, una contradicción si $r \neq 0$. Así, $r = 0$ y $b = s(ab)$, es decir, $(1 - sa)b = 0$. Como D es dominio entero y $b \neq 0$, debemos tener $sa = 1$, es decir, a invertible.

Definición 24.3.3. — Un dominio entero D es llamado un *dominio de factorización única* si todo elemento $a \in D - \{0\}$ que no es invertible puede escribirse de manera única como producto de elementos irreducibles, es decir, si $a \in D - \{0\}$ no es invertible, entonces existen irreducibles $p_1, ..., p_n \in D$ tales que $a = p_1 \cdots p_n$. Más aún, si existe otra descomposición en irreducibles, digamos $a = q_1 \cdots q_m$, entonces $n = m$ y $q_j = t_j p_j$, donde $t_j \in D$ es invertible.

Ejemplo 24.3.4. — Si D es dominio de factorización única, entonces es posible calcular el máximo común múltiplo en D. En efecto, tomemos a, b en $D - \{0\}$. Escribimos las descomposiciones en factores irreducibles de ambos elementos. Podemos escribir

$$a = p_1 \cdots p_n p_{n+1} \cdots p_l$$

$$b = p_1 \cdots p_n q_1 \cdots q_s$$

donde ningun q_j es producto de un elemento p_i por un invertible. Así, tenemos que $MCD(a, b) = p_1 \cdots p_n$.

***Proposición 24.3.5* (Gauss)**. — *Si D es un dominio de factorización única, entonces $D[x]$ también lo es.*

Este resultado lo verificaremos en una sección posterior.

24.4. Relaciones entre Dominios

Ahora procedemos a mostrar el resultado más importante de esta sección.

Teorema 24.4.1. — *Todo dominio Euclidiano es un dominio de ideales principales y todo dominio de ideales principales es un dominio de factorización única.*

Ejemplo 24.4.2. — Como consecuencia del resultado anterior es que si F es un cuerpo, entonces al ser $F[x]$ un dominio Euclidiano (usando como valuación el grado de polinomios) se tiene que todo polinomio puede escribirse como producto (único módulo constantes) de polinomios irreducibles. También, todo ideal es principal y el ideal generado por polinomios (no ceros) $p_1(x)$,..., $p_n(x)$ es generado por un polinomio $q(x)$ que es máximo común divisor de ellos. En particular, si son relativamente primos, ellos generan todo $F[x]$.

Para verificar la proposición anterior, primero veremos que todo dominio Euclidiano es principal y luego que todo dominio de ideales principales es necesariamente un dominio de factorización única.

Proposición 24.4.3. — *Todo dominio Euclidiano es de ideales principales*

Demonstración. — Consideremos un ideal $I \neq \{0\}$ de D. Queremos ver que este es principal. Consideremos el conjunto

$$v(I) = \{v(x) : x \in I - \{0\}\} \subset \{0, 1, 2, 3, ...\}$$

Consideremos $a \in I$ tal que $v(a) =$ Mínimo$(v(I)$, el cual existe al ser $\{0, 1, 2, 3, ..\}$ discreto y bién ordenado. Podemos considerar el ideal principal generado por a, es decir, $< a >$, el cual es esta contenido en I. Supongamos que podemos escoger $x \in I - < a >$. Sabemos que existen valores $r, t \in D$ tales que $x = ta + r$, donde $r = 0$ ó $v(r) < v(a)$. Pero como $x \notin < a >$, $r \neq 0$. Así, tenemos que $r \in D - \{0\}$ es tal que $v(r) < v(a)$. pero, $r = x - ta \in I$, lo cual contradice la minimalidad de $v(a)$. Luego, $I =< a >$. □

Proposición 24.4.4. — *Todo dominio de ideales principales es dominio de factorización única*

Antes de proceder a dar una demostración de este hecho, recordemos que en un ideal principal tenemos los siguientes :

(1) Existencia de $MCD(x_1, ..., x_n)$;

(2) $< x_1, ..., x_n >=< MCD(x_1, ..., x_n) >$, en particular, existen $a_1, ..., a_n \in D$ tales que

$$MCD(x_1, ..., x_n) = a_1x_1 + \cdots + a_nx_n;$$

(3) Dos máximos común divisores de los mismos elementos son el múltiplo de un invertible por el otro.

Primeros necesitamos verificar que todo elemento no invertible $x \in D - \{0\}$, donde D es un dominio de ideales principales, puede descomponerse como un producto finito de elementos irreducibles. Esto es consecuencia del siguiente.

Lema 24.4.5. — *Sea D un dominio de ideales principales y $x \in D - \{0\}$, un elemento no invertible. Entonces x es producto finito de elementos irreducibles de D.*

Demonstración. — Sea $x \in D - \{0\}$ no invertible. Si este es irreducible, entonces estamos listos. Supongamos por el contrario que no lo es, es decir, $x = ab$, donde $a, b \in D$ no son invertibles. Es claro que

$$< x > \subsetneq < a > \quad \text{y} \quad < x > \subsetneq < b >$$

Supongamos que a o b no es irreducible, digamos a no es irreducible. Entonces podemos escribir $a = a_1a_2$, donde a_j no es invertible. Ahora tenemos

$$< x > \subsetneq < a > \subsetneq < a_1 > \quad \text{y} \quad < x > \subsetneq < a > \subsetneq < a_2 >$$

Si el lema que estamos verificando es falso, procediendo de esta manera obtendremos una sucesión infinita de ideales

$$I_1 \subsetneq I_2 \subsetneq \cdots$$

lo cual será contradicción al siguiente lema. □

Lema 24.4.6. — *Sea D un dominio de ideales principales. Entonces no es posible encontrar una sucesión infinita de ideales*

$$I_1 \subsetneqq I_2 \subsetneqq \cdots$$

Demonstración. — Supongamos que tenemos una colección de ideales

$$I_1 \subset I_2 \subset \cdots$$

Entonces

$$I = \cup_{j=1}^{\infty} I_j$$

resulta ser un ideal. Por otro lado, como D es principal, tenemos la existencia de un elemento $a \in D$ tal que $< a >= I$. Así, como $a \in I$, debe ocurrir que $a \in I_n$ para algún n, en cuyo caso tendremos que $I = I_n$ □

Ahora necesitamos verificar que la descomposición es única módulo factores irreducibles y permutación de factores. Esto es consecuencia del siguiente.

Lema 24.4.7. — *La descomposición en factores irreducibles en un dominio de ideales principales es única módulo multiplicación por invertibles y permutación de factores.*

Demonstración. — Supongamos que tenemos la igualdad

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

donde $p_j, q_i \in D$ son elementos irreducibles. Supongamos que $n \geq m$. Por el lema de Euclides más abajo, tenemos que p_1 divide algún q_j, digamos q_1. Entonces $q_1 = r_1 p_1$, donde $r_1 \in D$ es algún invertible. Factorizando en D el elemento p_1 en la igualdad anterior (ya que no hay divisores de cero), obtenemos la igualdad

$$p_2 \cdots p_n = r_1 q_2 \cdots q_m$$

Ahora procedemos con p_2 de la misma manera que con p_1 para ver que, módulo permutación de índices $q_2 = r_2 p_2$, donde $r_2 \in D$ es invertible y, en particular, tener la igualdad

$$p_3 \cdots p_n = r_1 r_2 q_3 \cdots q_m$$

Procediendo de esta manera, módulo permutación de índices, obtendremos que

$$q_j = r_j p_j, j = 1, ..., n$$

donde $r_j \in D$ es invertible, y la igualdad

$$1 = r_1 r_2 \cdots r_n q_{n+1} \cdots q_m$$

Si $m > n$, entonces esta última igualdad diría que q_m es invertible, una contradicción. Luego $m = n$ y obtenemos lo deseado. □

***Lema 24.4.8* (Euclides)**. — *Sea D un dominio de ideales principales, $p \in D$ un elemento irreducible y $a, b \in D$ tales que p divide ab. Entonces p divide a o divide b. En otras palabras, todo ideal generado por un elemento irreducible es un ideal primo.*

Demonstración. — Podemos asumir que $a, b \in D - \{0\}$. Podemos calcular un máximo común divisor $d = MCD(a, b)$ en el dominio de ideales principales D. Supongamos que p no divide a, en cuyo caso $MCD(p, a) = 1$. Sabemos que es posible encontrar valores $r, s \in D$ tales que $1 = rp + sa$. Luego, al multiplicar por b ontenemos $b = brp + sab$ y como p divide ambos sumandos del lado derecho, p debe dividir b. □

CAPÍTULO 25

ANILLO DE POLINOMIOS Y FACTORIZACIÓN UNICA

En esta sección nos preocuparemos de manera particular de los anillos de polinomios de dominios enteros y estudiaremos algunas propiedades que tienen estos.

Ejercicio 90. — *Sea D un dominio entero y considere el anillo de polinomios en una variable $D[x]$. Sean $P(x) \in D[x]$ y $Q(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ tal que $a_n \in D$ es un invertible. Verifique que es posible encontrar polinomios $T(x), R(x) \in D[x]$ tales que*

$$P(x) = Q(x)T(x) + R(x)$$

donde $R(x) = 0$ ó bién $grad(R) < grad(Q)$.

Ejemplo 25.0.9. — Consideremos un cuerpo k y el anillo de polinomios en una variable $k[x]$. Sabemos que $k[x]$ es un dominio Euclidiano usando como valuación el grado de polinomios. En particular, $k[x]$ es también un dominio de ideales principales y un dominio de factorización única. Ahora, si $R(x), S(x) \in k[x]$ son relativamente primos, tenemos que

$$1 = R(x)A(x) + S(x)B(x)$$

para ciertos polinomios $A(x), B(x) \in k[x]$. Así, si $T(x) \in k[x]$, entonces

$$T(x) = R(x)C(x) + S(x)D(x)$$

para ciertos polinomios $C(x), D(x) \in k[x]$. En este caso $C(x) = T(x)A(x)$ y $D(x) = T(x)B(x)$. El algoritmo de la división nos permite calcular efectivamente los polinomios $A(x), B(x)$ y luego $C(x), D(x)$. Una consecuencia de esta pequeña observación es la *descomposición en fracciones parciales* : Sean $P(x), Q(x) \in k[x]$ y supongamos que $Q(x) = Q_1(x)^{d_1} \cdots Q_n(x)^{d_n}$ es descomposición en polinomios irreducibles. Entonces es posible calcular de manera explícita polinomios $P_1(x), ..., P_n(x) \in k[x]$ tales que

$$\frac{P(x)}{Q(x)} = \sum_{j=1}^{n} \frac{P_j(x)}{Q_j(x)^{d_j}}$$

Ejercicio 91. — *Verifique la descomposición en fracciones parciales del ejemplo anterior. Utilize la observación hecha en el mismo ejemplo con*

$$R(x) = \frac{Q(x)}{Q_n(x)^{d_n}} = Q_1(x)^{d_1} \cdots Q_{n-1}(x)^{d_{n-1}}$$

$$S(x) = Q_n(x)^{d_n} \quad y \quad T(x) = P(x)$$

El ejemplo anterior nos dice que los dominio $k[x]$, donde k es un cuerpo, son dominios Euclidianos y, en particular, dominios de idelaes principales y de factorización única. Hemos visto que $\mathbb{Z}[x]$ no es un dominio Euclidiano ni dominio de ideales principales, pero aún queda la pregunta si este es un dominio de factorización única.

Teorema 25.0.10 **(Gauss)**. — *Si D es un dominio de factorización única, entonces $D[x]$ también lo es.*

Este resultado al ser usado de manera iterativa permite obtener el siguiente.

Corolario 25.0.11. — *Si D es un dominio de factorización única, entonces $D[x_1, ..., x_n]$ también lo es.*

Demostración del teorema de Gauss. — Sea D un dominio entero y k su cuerpo de fracciones. Entonces tenemos de manera natural la incrustación $D[x] \subset k[x]$. Sea $P(x) \in D[x]$; podemos escribir

$$P(x) = dP_1(x)$$

donde $P_1(x) \in D[x]$ tiene la propiedad que la colección de sus coeficientes son relativamente primos y $d \in D$ es el máximo común divisor de los coeficientes de $P(x)$. Como D es dominio de factorización única, tenemos una descomposición "única"

$$d = p_1 p_2 \cdots p_r$$

donde $p_j \in D$ son elementos irreducibles. También tenemos una descomposición "única" en polinomios irreducibles de $k[x]$, digamos

$$P_1(x) = Q_1(x)Q_2(x) \cdots Q_n(x)$$

$Q_1(x), ..., Q_n(x) \in k[x]$, polinomios irreducibles.
Ahora, cada polinomio $Q_j(x)$ puede escribirse como

$$Q_j(x) = \frac{a_j}{b_j} T_j(x)$$

donde $T_j(x) \in D[x]$ y de manera que los coeficientes de $T_j(x)$ son relativamente primos. Es claro que $T_j(x) \in k[x]$ es irreducible (es un múltiplo de $Q_j(x)$ por un invertible de $k[x]$). Luego, $T_j(x) \in D[x]$ debe también ser irreducible en $D[x]$. Tenemos la igualdad

$$P_1(x) = \frac{a_1 \cdots a_n}{b_1 \cdots b_n} T_1(x) \cdots T_n(x)$$

ó de manera equivalente

$$H(x) = b_1 \cdots b_n P_1(x) = a_1 \cdots a_n T_1(x) \cdots T_n(x) = L(x)$$

Luego, un máximo común divisor de los coeficientes del polinomio $H(x) \in D[x]$, es $b_1 \cdots b_n \in D$, y un máximo común divisor del polinomio $L(x) \in D[x]$, es $a_1 \cdots a_n \in D$. De esta manera tenemos la igualdad

$$a_1 \cdots a_n = b_1 \cdots b_n s$$

para cierto elemento invertible $s \in D$ ya que D es dominio de factorización única. Así,

$$\frac{a_1 \cdots a_n}{b_1 \cdots b_n} = s \in D$$

y, en particular,

$$P_1(x) = sT_1(x) \cdots T_n(x)$$

con lo cual finalmente tenemos la descomposición en factores irreducibles en $D[x]$

$$P(x) = p_1 p_2 \cdots p_r s T_1(x) \cdots T_n(x)$$

Esto nos ha permitido verificar al menos la existencia de una factorización en irreducibles en $D[x]$. Ahora debemos verificar su unicidad módulo invertibles y permutación de factores. □

Ejercicio 92. — *Verificar la unicidad del teorema anterior. Indicación : considere una igualdad*

$$p_1 \cdots p_n P_1(x) \cdots P_m(x) = q_1 \cdots q_r Q_1(x) \cdots Q_s(x)$$

donde $p_j, q_j \in D$ son irreducibles y $P_j(x), Q_j(x) \in D[x]$ son polinomios irreducibles. Vea que se puede suponer que cada polinomio $P_j(x), Q_j(x)$ tiene sus coeficientes relativamente primos. De esta manera, vea que existe $a \in D$ invertible tal $p_1 \cdots p_n = q_1 \cdots q_r a$ y que $r = n$, al ser D dominio de factorización única. Ahora, analize la igualdad $P_1 \cdots p_m = aQ_1 \cdots Q_s$ en $k[x]$, utilize que $k[x]$ es dominio de factorización única y el mismo tipo de ideas como en la demostración para completar el argumento.

CAPÍTULO 26

ANILLOS NOETHERIANOS

En esta sección veremos que todo ideal del anillo de polinomios $k[x_1, ..., x_n]$. donde k es un cuerpo es finitamente generado. Este resultado es de mucha importancia en el estudio de soluciones de sistemas infinitos polinomiales y, en particular, en geometría algebraica.

Definición 26.0.12. — Un anillo A conmutativo con unidad es llamado *Noetheriano* si todo ideal de A es finitamente generado.

Ejemplo 26.0.13. — Cuerpos y $\mathbb{Z}$ son ejemplos de anillos Noetherianos.

***Teorema 26.0.14* (Teorema Fundamental de Hilbert)**. — *Si A es un anillo Noetheriano, entonces $A[x_1, ..., x_n]$ también es Noetheriano.*

Corolario 26.0.15. — *Si k es un cuerpo, entonces $k[x_1, ..., x_n]$ es Noetheriano.*

Demostración del teorema fundamental de Hilbert. — Sólo es necesario verificar que $A[x]$ es anillo Noetheriano. Supongamos que tenemos un ideal I en $A[x]$. Deseamos encontrar un número finito de generadores de I.
Dado un polinomio $p(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, con $a_n \neq 0$, es decir $p(x)$ es de grado n, llamaremos al coeficiente a_n el coeficiente principal de $p(x)$. Definimos el coeficiente principal del polinomio cero como el $0 \in A$.
Sea $J \subset A$ el conjunto formado de los coeficientes principales de todos los polinomios en I.

Hecho 1. *J es un ideal de A.*

La razón de esto es :
(1) El coeficiente principal de la suma de dos polinomios es la suma de los coeficientes principales ;

(2) El coeficiente principal del polinomio $-p(x)$ es el opuesto aditivo del coeficiente principal de $p(x)$;
(3) El coeficiente principal del producto de dos polinomios es el producto de los coeficientes principales ;
(4) Si $p(x) \in I$ y $r \in A$, entonces el coeficiente principal de $rp(x)$ es r veces el coeficiente principal de $p(x)$.

Ahora que tenemos que J es un ideal de A, como A es Noetheriano, tenemos la existencia de un número finito de polinomios

$$p_1(x), ..., p_m(x) \in I$$

tal que J está generado por los coeficientes principales de ellos. Sea N el máximo de los grados de los polinomios $p_1(x)$,..., $p_m(x)$.
Para cada entero $k < N$ definimos como J_k al subconjunto de A formado de los coeficientes principales de todos aquellos polinomios en I de grado a lo más k.

Hecho 2. *J_k es un ideal de A.*

La razón de esto es muy similar a como vimos que J es un ideal. Se puede ver que J_k es cerrado bajo la suma y la resta. Veamos que J_k es cerrado bajo la multiplicación y que es ideal. Para esto, sea $a \in J_k$ y $r \in A$. Veremos que $ra \in J_k$ y tendremos ambos hechos válidos. Sea $p(x) \in I$ cuyo coeficiente principal es a y considere el polinomio de grado cero $q(x) = r \in A[x]$. Como I es un ideal de $A[x]$, tenemos que $p(x)q(x) = rp(x) \in I$. Ya que el coeficiente principal de $rp(x)$ es ra, estamos listos.

Ahora, al ser J_k un ideal en A, la condición de A ser Noetheriano nos asegura que podemos encontrar un número finito de polinomios

$$q_{k,1}(x), ..., q_{k,n_k}(x) \in I$$

de manera que sus coeficientes principales generan J_k.
Denotemos por $\widehat{I}$ al ideal de $A[x]$ generado por todos los polinomios anteriores :

$$p_1(x), ..., p_m(x), q_{0,1}(x), ..., q_{0,n_0}(x), ..., q_{N,1}(x), ..., q_{N,n_N}(x).$$

Por construcción, el ideal $\widehat{I} \subset I$ es finitamente generado.

Hecho 3. $I = \widehat{I}$.

Como sabemos que $\widehat{I} \subset I$, necesitamos ver que $I - \widehat{I} = \emptyset$. Supongamos por el contrario que existe $t(x) \in I - \widehat{I}$. Podemos escoger $t(x)$ de grado menor con tal propiedad. Sea $s \in A$ el coeficiente principal de $t(x)$.
(1) Supongamos que el grado de $t(x)$ es al menos N. Como $s \in J$, existen polinomios (monomios) $r_1(x), ..., r_m(x) \in A[x]$ tal que $u(x) = \sum_{j=1}^{m} r_j(x)p_j(x) \in \widehat{I}$ tiene coeficiente principal s y cuyo grado sea igual al de $t(x)$. Ahora, como $q(x) = t(x) - u(x) \in I$ tiene grado menor que $t(x)$, debe ocurrir (por la minimalidad de la elección de $t(x)$) que $q(x) \in \widehat{I}$. Esto nos dice que $t(x) = q(x) + u(x) \in \widehat{I}$, una contradicción.

(2) Si el grado de $t(x)$ es $k < N$, entonces $s \in J_k$ para cierto k. Ahora podemos encontrar polinomios (monomios) $r_{k,j}(x) \in A[x]$ de manera que $v(x) = \sum_{j=1}^{n_k} r_{k,j}(x)q_{k,j}(x) \in \widehat{I}$ tenga coeficiente principal igual s y cuyo grado coincida con el grado de $t(x)$. Ahora procedemos como en el caso (1) para obtener nuevamente una contradicción.

□

Ejemplo 26.0.16. — Sea k un cuerpo y supongamos que tenemos un sistema infinito

$$(*) \quad p_j(x_1, ..., x_n) = 0; \quad j \in \mathcal{A},$$

donde $p_j(x_1, ..., x_n) \in k[x_1, ..., x_n]$.
Denotemos por $V \subset k^n$ al conjunto de soluciones de tal sistema infinito. Sea $I(V) \subset k[x_1, ..., x_n]$ formado de aquellos polinomios $q(x_1, ..., x_n)$ tales que $q(a_1, ..., a_n) = 0$ para todo $(a_1, ..., a_n) \in V$.
Se tiene que $I(V)$ es un ideal de $k[x_1, ..., x_n]$. Luego, al ser $k[x_1, ..., x_n]$ un anillo Noetheriano, existen un número finito de polinomios

$$q_1(x_1, ..., x_n), ..., q_d(x_1, ..., x_n) \in I(V)$$

tales que generan $I(V)$.
Denotemos por $W \subset k^n$ al conjunto de soluciones del sistema finito de polinomios

$$\begin{cases} q_1(x_1, ..., x_n) & = & 0 \\ \vdots & & \vdots \\ q_d(x_1, ..., x_n) & = & 0 \end{cases}$$

Ya que

$$q_1(x_1, ..., x_n), ..., q_d(x_1, ..., x_n) \in I(V),$$

tenemos que $V \subset W$.
Por otro lado, como cada $p_j(x_1, ..., x_n)$ puede escribirse de la forma

$$p_j = \sum_{i=1}^{d} r_j q_i,$$

tenemos $W \subset V$. En consecuencia,

$$W = V.$$

Ejercicio 93. —
1.- Considere en $\mathbb{C}[x]$ el ideal I generado por todos los polinomios

$$p_k(x) = k + x^k, k = 1, 2, 3, ...$$

Ya que $\mathbb{C}[x]$ es dominio de ideales principales, I es generado por un polinomio. Encuentre tal generador.

2.- Considere en $\mathbb{Z}[x]$ el ideal I generado por los polinomios

$$p_{n,m}(x) = 2nx + 3m, n, m = 0, 1, 2, ...$$

Verificar que I está generado por 3 y $2x$.

PARTE IV

REPRESENTACIONES LINEALES DE GRUPOS

Para estudiar algunos grupos es útil usar algunas acciones especiales, con ciertas propiedades lineales. No pretenderemos escribir un capítulo demasiado preciso sobre representaciones lineales, sólo presentaremos algunos temas básicos que se relacionan con lo expuesto en los capítulos anteriores.

CAPÍTULO 27

REPRESENTACIONES LINEALES

Definición 27.0.17. — Una *representación lineal* de un grupo $(G, *)$ en un espacio vectorial V (sobre algún cuerpo $\mathcal{K}$, que para nuestro interés puede ser $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$) es por definición una acción

$$\phi : G \to GL(V)$$

La dimensión del espacio vectorial V es llamada el *grado de la representación*. Cuando el homomorfismo $\phi : G \to GL(V)$ es además inyectivo, es decir una acción fiel, entonces hablamos de una *representación fiel*.

Ejemplo 27.0.18. — Sea $(G, *)$ un grupo simple. Entonces cualquier representación lineal de G es fiel o es la representación trivial ($\phi(g) = I$, para todo $g \in G$). En efecto, dada una representación lineal $\phi : G \to GL(V)$ tenemos que Ker(ϕ) es un subgrupo normal de G. Como G es simple, tenemos que Ker$(\phi) = \{0\}$, en cuyo caso ϕ es fiel, o Ker$(\phi) = G$, en cuyo caso $\phi(g) = I$ para $g \in G$.

Ejemplo 27.0.19. — Dado un grupo $(G, *)$ y un cuerpo $\mathcal{K}$, siempre tenemos la representación de grado uno

$$1 : G \to GL(\mathcal{K}) = \mathcal{K}^* : g \mapsto 1$$

De manera más general, si V es un espacio vectorial sobre $\mathcal{K}$, entonces siempre tenemos la representación trivial

$$I : G \to GL(V) : g \mapsto I$$

Ejemplo 27.0.20. — Sea $G = \langle x : x^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Entonces tenemos también la representación de grado uno

$$(-1) : G \to GL(\mathbb{Q})$$

definida por

$$(-1)(I_G) = 1 \;\; (-1)(x) = -1$$

Ejemplo 27.0.21. — Consideremos un grupo $(G, *)$ y una representación de grado 1, digamos $\phi : G \to GL(V)$, es decir V es un espacio vectorial de dimensión uno sobre el cuerpo $\mathcal{K}$. Escojamos un vector no cero $v \neq 0$ en V; entonces $\{v\}$ es base de V. Para cada $g \in G$ tenemos que $\phi(g)(v) = \lambda_g v$ para algún valor $\lambda \in \mathcal{K}^* = \mathcal{K} - \{0\}$. Como ϕ es un homomorfismo de grupos, tenemos que $\phi(g_1 * g_2) = \phi(g_1)\phi(g_2)$, es decir $\lambda_{g_1 * g_2} = \lambda_{g_1}\lambda_{g_2}$, para todos $g_1, g_2 \in G$. Por ejemplo, $\lambda_{I_G} = 1$. Tenemos además un isomorfismo natural, dado por la base anterior, $L : GL(V) \to \mathcal{K}^* : \lambda v \mapsto \lambda$. Luego, podemos mirar la representación $L \circ \phi : G \to \mathcal{K}^* : g \mapsto \lambda_g$.
Observemos que si escogemos otro vector no cero de V, digamos $\widehat{v}$, entonces tenemos que $\widehat{v} = av$ para cierto $a \in \mathcal{K}^*$. Luego, no es dificil ver que $\phi(g)(\widehat{v}) = \lambda_g \widehat{v}$. En otras palabras, el valor $\lambda_g \in \mathcal{K}^*$ está únicamente determinado por $g \in G$ y ϕ, es decir, no depende del vector $v \in V - \{0\}$ escogido.
Suponiendo que $g \in G$ es de orden $o(g)$ finito, se tiene que $\lambda_g^{o(g)} = 1$, es decir, λ_g es una raiz $o(g)$-ésima de la unidad.

Ejercicio 94. — *Sea $(G, *)$ un grupo cíclico finito. Determinar las representaciones de grado 1 en (i) $\mathbb{Q}$, (ii) $\mathbb{R}$ y en (iii) $\mathbb{C}$.*

Observación 27.0.22. — Dados un grupo $(G, *)$, una representación lineal $\phi : G \to GL(V)$, donde V en un espacio vectorial V sobre un cuerpo $\mathcal{K}$, y un subanillo R de $\mathcal{K}$, podemos dotar de manera natural a V de una estructura de RG-módulo. La idea es la siguiente, primero consideramos un anillo $R[G]$ del grupo G respecto al anillo R. Ahora definimos la operación binaria

$$\sum_{j=1}^{n} r_j g_j \cdot v = \sum_{j=1}^{n} r_j \phi(g_j)(v)$$

la cual realiza a V como un $R[G]$-módulo.

CAPÍTULO 28

ALGUNOS EJEMPLOS DE REPRESENTACIONES

28.1. Representación regular dada por la acción de un grupo

Consideremos una acción de un grupo finito $(G, *)$ sobre un conjunto finito $X = \{x_1, ..., x_n\}$, digamos $\phi : G \to Perm(X)$. Consideremos un espacio vectorial V de dimensión n y una base $\{v_1, ..., v_n\}$. Entonces, podemos construir una representación lineal inducida por la acción anterior de la siguiente manera :

$$\Phi : G \to GL(V) : g \to \Phi(g)$$

definida por

$$\Phi(g)(\sum_{j=1}^{n} a_j v_j) = \sum_{j=1}^{n} a_j v_{g(j)}$$

donde $g(j) \in \{1, 2, ..., n\}$ es tal que $\phi(g)(x_j) = x_{g(j)}$. Lo que estamos haciendo es permutar los elementos de la base de la misma manera como se permutan los elementos de X.

Ejercicio 95. — *En el ejemplo anterior considere $X = G$ y la acción $\phi : G \to Perm(G)$ definida por $\phi(g) : G \to G : h \mapsto g * h$. La representación obtenida es llamada la* representación regular *del grupo G.*

28.2. Representación suma directa

Sea $(G, *)$ un grupo y V, W espacios vectoriales sobre un cuerpo $\mathcal{K}$. Consideremos dos representaciones lineales

$$\phi : G \to GL(V) \text{ y } \psi : G \to GL(W)$$

Entonces podemos formar el espacio producto $V \times W$ y construir la *representación producto ó suma directa*

$$(\phi, \psi) := \phi \oplus \psi : G \to GL(V \times W)$$

definida como

$$(\phi, \psi)(g) : V \times W \to V \times W : (v, w) \mapsto (\phi(g)(v), \psi(g)(w))$$

28.3. representación producto tensorial

Tambiém podemos hacer el producto tensorial de estos espacios vectoriales $V \otimes V$ y construir la *representación producto tensorial*

$$\phi \otimes \psi : G \to GL(V \otimes W)$$

definida como

$$\phi \otimes \psi(g) : V \otimes W \to V \otimes W : v \otimes w \mapsto \phi(g)(v) \otimes \psi(g)(w)$$

28.4. Representación wedge

Podemos considerar es el espacio vectorial wedge $V \wedge V$ y la *representación cuña*

$$\phi \wedge \phi : G \to GL(V \wedge V) : g \mapsto \phi \wedge \phi$$

donde

$$\phi \wedge \phi(g) : V \to V : v \mapsto \phi(g)(v) \wedge \phi(g)(v)$$

28.5. Representación Hom

Otro espacio vectorial que podemos formar es $\text{Hom}(V, W)$, el espacio vectorial de todas las funciones lineales de V en W. Dada una función lineal $L : V \to W$ y $g \in G$, podemos considerar la nueva función lineal

$$\text{Hom}(\phi, \psi)(g)(L) = \psi(g) \circ L \circ \phi(g^{-1}) : V \to W$$

de donde obtenemos una nueva representación lineal

$$\text{Hom}(\phi, \psi) : G \to GL(\text{Hom}(V, W)) : g \mapsto \text{Hom}(\phi, \psi)(g)$$

llamada la *representación homomorfismo*.

Ejemplo 28.5.1. — Sea $(G, *)$ un grupo y V un espacio vectorial sobre un cuerpo $\mathcal{K}$. Consideremos una representación lineal $\phi : G \to GL(V)$. Entonces podemos construir su representación dual $\phi^* : G \to GL(V^*)$ definida como sigue : Si $L : V \to \mathcal{K}$ es una función lineal, entonces para cada $g \in G$ tenemos que $L \circ \phi(g)^{-1} = L \circ \phi(g^{-1}) : V \to \mathcal{K}$ es de nuevo una función lineal. Definimos $\phi^*(g) : V^* \to V^* : L \mapsto L \circ \phi(g^{-1})$. Esta representación es la representación homomorfismo para $W = \mathcal{K}$.

28.6. Representación cociente

Supongamos que tenemos una representación lineal de un grupo $(G, *)$, digamos $\phi : G \to GL(V)$. Si H es un subgrupo de G, entonces tenemos gratis una representación lineal de H dada por restricción de ϕ a H, llamada la *representación restricción* a H. Si además H es subgrupo normal, entonces tenemos el grupo cociente G/H. Desgraciadamente no podemos hacer descender la representación lineal ϕ para obtener una representación lineal del cociente. Pero si tenemos que $\phi(h) = I$ para todo $h \in H$, entonces si lo podemos hacer como

$$\phi_{G/H} : G/H \to GL(V) : gH \mapsto \phi(g)$$

llamada la *representación cociente*.

CAPÍTULO 29

REPRESENTACIONES IRREDUCIBLES Y REDUCIBLES

Definición 29.0.1. — Consideremos una representación $\phi : G \to GL(V)$, donde V es un subespacio vectorial sobre un cuerpo $\mathcal{K}$. Si existe un subespacio propio $W \neq \{0\}$ de V que resulta invariante por cada una de las transformaciones $\phi(g)$, $g \in G$, entonces uno dice que la representación es una *representación reducible*; en caso contrario, decimos que esta es una *representación irreducible*. En el caso de existir $W \neq \{0\}$ invariante por $\phi(G)$, tenemos una representación natural $\phi|_W : G \to GL(W)$ definida por $\phi|_W(g) = \phi(g)$, la cual es llamada la *subrepresentación inducida* de ϕ.

Ejercicio 96. — *Si tenemos una representación $\phi : G \to GL(V)$, donde V es un espacio vectorial sobre $\mathbb{Q}$, entonces tenemos gratis representaciones reales y complejas (cada $\phi(g)$ es una matriz con coeficientes en $\mathbb{Q}$, luego con coeficientes en $\mathbb{R}$ y en $\mathbb{C}$). Puede ocurrir que ϕ sea una representación irreducible (sobre $\mathbb{Q}$) pero que no lo sea sobre $\mathbb{R}$ ó en $\mathbb{C}$. Dar un ejemplo de esta situación.*

El siguiente resultado para representaciones lineales de grupos finitos es de gran ayuda en el estudio de estos.

Proposición 29.0.2. — *Sea G un grupo finito y consideremos una representación $\phi : G \to GL(V)$ de grado finito. Entonces podemos escoger en V un producto interior Euclidiano (Hermitiano positivo definido en el caso complejo) $\langle , \rangle_G$, de manera que $\phi(G)$ es subgrupo del grupo se isometrías $O_{\langle , \rangle}$.*

Demonstración. — Sea $\langle , \rangle$ cualquier producto Euclidiano (Hermitiano positivo en el caso complejo) para V. Entonces basta considerar el producto promediado

$$\langle x, y \rangle_G = \Sigma_{g \in G} \langle \phi(g)(x), \phi(g)(y) \rangle$$

□

Observación 29.0.3. — En la hipótesis de la proposición anterior la condición de ser grado finito fué para asegurar la existencia de un producto interior para partir nuestro argumento. La finitud de G fué para estar seguros de que la suma usada fuese finita.

Ejercicio 97. — *Verificar que en caso que la representación es irreducible, entonces el producto interior construido en la demostración del teorema es único módulo producto por un escalar.*

Corolario 29.0.4. — *Sea G un grupo finito y consideremos una representación $\phi : G \to GL(V)$ de grado finito. Si W es un subespacio vectorial de V que es invariante por cada transformación $\phi(g)$, con $g \in G$, entonces existe un subespacio complementario a W que también es invariante.*

Demonstración. — Usando la proposición anterior, podemos asumir que $\phi(g)$ preserva un producto interior Euclidiano (Hermitiano positivo en el caso complejo) $\langle , \rangle$ para cada $g \in G$. Basta entonces escoger

$$W^{\perp} = \{v \in V : \langle v, w \rangle = 0, \text{ para todo } w \in W\}$$

□

CAPÍTULO 30

HOMOMORFISMOS DE REPRESENTACIONES

Podemos relacionar diferentes representaciones lineales del mismo grupo G sobre espacios vectoriales sobre el mismo cuerpo de la siguiente manera.

Definición 30.0.5. — Sean $\phi : G \to GL(V)$ y $\psi : G \to GL(W)$ dos representaciones lineales de G, donde V y W son espacios vectoriales sobre el mismo cuerpo $\mathcal{K}$. Un homomorfismo entre estas representaciones es una función lineal $L : V \to W$ tal que $L(\phi(g)(v)) = \psi(g)(L(v))$, para todo $v \in V$ y todo $g \in G$. Cuando $L : V \to W$ es un isomorfismo lineal, entonces diremos que las representaciones son equivalentes, en cuyo caso tenemos $\psi(g) = L \circ \phi(g) \circ L^{-1}$ para todo $g \in G$. Denotamos por $\text{Hom}_G(\phi, \psi)$ al conjunto de todos lo homomorfismos de representaciones entre $\phi : G \to GL(V)$ y $\psi : G \to GL(W)$.

Observación 30.0.6. — No confundir las notaciones $\text{Hom}(\phi, \psi)$ y $\text{Hom}_G(\phi, \psi)$. La primera es una representación mientras la segunda es un conjunto, de hecho un espacio vectorial.

Ejercicio 98. — *Verificar que $\text{Hom}_G(\phi, \psi)$ es un subespacio vectorial del espacio vectorial $\text{Hom}(V, W)$, formado por todas las funciones lineales de V en W.*

Observación 30.0.7. — Consideremos una representación lineal $\phi : G \to GL(V)$, donde V es un espacio vectorial sobre un cuerpo $\mathcal{K}$.

(1) Habíamos visto que para cada anillo R en $\mathcal{K}$, podíamos construir el anillo $R[G]$ y hacer que V tuviese una estructura de $R[G]$-módulo. Un homomorfismo de V como $R[G]$-módulo es una función lineal $L : V \to V$ que respecta la multiplicación por elementos de $R[G]$, es decir $L(\sum_{j=1}^{n} r_j g_j \cdot v) = \sum_{j=1}^{n} r_j g_j \cdot L(v)$. Esto es equivalente a que valga la igualdad $L(g \cdot v) = g \cdot L(v)$, es decir, $L \circ \phi(g) = \phi \circ L$. Esto último decie que $L \in \text{Hom}_G(\phi, \phi)$. Es claro que vale el recíproco. De esta manera

$\text{Hom}_G(\phi,\phi)$ corresponde exactamente a los homorfismos de V como $R[G]$-módulo. En forma similar, $\text{Hom}_G(\phi,\psi)$ corresponde exactamente a los homorfismos de V en W como $R[G]$-módulos.

(2) Para $g \in G$, el isomorfismo de espacio vectorial $\phi(g) : V \to V$ no tiene por que pertenecer a $\text{Hom}_G(\phi,\phi)$. La condición para que $\phi(g) \in \text{Hom}_G(\phi,\phi)$ es que para todo $h \in G$ valga la igualdad $\phi(g)(h \cdot v) = h \cdot \phi(g)(v)$, es decir $\phi(g * h) = \phi(h * g)$. Por ejemplo, si la representación es fiel, entonces lo anterior es equivalente a tener $g \in Z(G)$. En todo caso, si $(G,*)$ es finito consideramos la función lineal promediada

$$L = \frac{1}{|G|}\sum_{g\in G}\phi(g) : V \to V$$

la cual satisface $L \in \text{Hom}_G(\phi,\phi)$.

Ejercicio 99. — *Verificar que la función lineal*

$$L := \frac{1}{|G|}\sum_{g\in G}\phi(g) : V \to V$$

satisface las siguientes propiedades :
(i) $Im(L) = \{v \in V : \phi(g)(v) = v$ *para todo* $g \in G\}$
(ii) $L \circ L = L$
(iii) Concluir que L *es una proyección.*

Ejemplo 30.0.8. — Consideremos un grupo $(G,*)$ y dos representación $\phi : G \to GL(V)$, $\psi : G \to W$, donde V y W son espacios vectoriales sobre un cuerpo $\mathcal{K}$. Supongamos que tenemos un homomorfismo de representaciones $L : V \to W$. Asociado a la función lineal L tenemos los dos subespacios siguientes :

$$\text{Ker}(L) = \{v \in V : L(v) = 0\}$$

$$\text{Im}(L) = \{w \in W : L(v) = w, \text{ para algún } v \in V\}$$

De la igualdad $L(\phi(g)(v)) = \psi(g)(L(v))$, para todo $v \in V$ y todo $g \in G$, es claro que $\text{Ker}(L)$ es un subespacio invariante de $\phi(G)$ y $\text{Im}(L)$ es un subespacio invariante por $\psi(G)$. En particular, si la representación $\phi : G \to GL(V)$ es irreducible, entonces $\text{Ker}(L) \in \{\{0\}, V\}$, es decir la función lineal L es inyectiva o es trivial $L \equiv 0$. De manera similar, si la representación $\psi : G \to GL(W)$ es irreducible, entonces tenemos que $\text{Im}(L) \in \{\{0\}, W\}$, es decir la función lineal L es sobreyectiva o es trivial $L \equiv 0$. Esto nos permite concluir el siguiente resultado.

Proposición 30.0.9 **(Lema de Schur)**. — *Sea* $(G,*)$ *un grupo y dos representaciones irreducibles* $\phi : G \to GL(V)$, $\psi : G \to GL(W)$, *donde* V, W *son espacios vectoriales sobre el mismo cuerpo. Si* $L : V \to W$ *es un homomorfismo entre esas representaciones, entonces* $L \equiv 0$ *o* L *es un isomorfismo.*

Corolario 30.0.10. — *Sea $(G,*)$ un grupo y dos representaciones irreducibles $\phi : G \to GL(V)$, $\psi : G \to GL(V)$, donde V es un espacio vectorial sobre el cuerpo de los números complejos $\mathbb{C}$. Si $L : V \to V$ es un homomorfismo entre esas representaciones, entonces existe $\lambda \in \mathbb{C}$ tal que para cada $v \in V$ vale que $L(v) = \lambda v$.*

Demonstración. — Como todo polinomio de coeficientes complejos de grado mayor o igual a uno tiene ceros complejos, tenemos que L tiene al menos un valor propio $\lambda \in \mathbb{C}$. La función lineal $N = L - \lambda I : V \to V$ sigue siendo un homomorfismo de las representaciones anteriores. Por el lema de Schur, tenemos que $N \equiv 0$ o N es isomorfismo. Pero al ser λ valor propio de L, entonces N tiene núcleo no trivial, luego $N \equiv 0$. □

Ejemplo 30.0.11. — Consideremos un grupo $(G,*)$ y representaciones $\rho_j : G \to GL(V_j)$, donde V_j son espacios vectoriales sobre el mismo cuerpo, $j = 1, 2, ..., N$. Entonces tenemos de manera natural el espacio vectorial producto $V_1 \times V_2 \times \cdots \times V_N$. Existe un monomorfismo natural

$$J : GL(V_1) \times GL(V_2) \times \cdots \times GL(V_N) \to GL(V_1 \times V_2 \times \cdots \times V_N)$$

dado por

$$J(L_1, L_2, ..., L_N)(v_1, v_2, ..., v_N) = (L_1(v_1), L_2(v_2), ..., L_N(v_N))$$

Esto nos permite construir la *representación producto*

$$(\rho_1, ..., \rho_N) : G \to GL(V_1 \times V_2 \times \cdots \times V_N)$$

definido por

$$(\rho_1, ..., \rho_N)(g) = J(\rho_1(g), ..., \rho_N(g))$$

Observemos que cada subespacio $\widehat{V}_j = \{(0, ..., 0, v, 0, ..., 0) \in V_1 \times \cdots \times V_N\}$ es invariante por $(\rho_1, ..., \rho_N)$. Luego esta representación es reducible. Matricialmente hablando, lo que estamos haciendo es formar una gran matriz a partir de matrices pequeñas colocandolas en manera diagonal.

El siguiente resultado nos dice que para entender las representaciones lineales de un grupo finito basta con entender las representaciones irreducibles.

Proposición 30.0.12. — *Sean $(G,*)$ un grupo finito y V un espacio vectorial de dimensión finita. Entonces, toda representación $\rho : G \to GL(V)$ es equivalente a una única representación producto, módulo isomorfismo de representaciones, donde cada representación involucrada es irreducible.*

Demonstración. — Como V tiene dimensión finita y G es de orden finito, podemos introducir un producto interior Euclidiano (Hermitiano positivo definido en el caso complejo) $\langle , \rangle$ de manera que $\rho(G) < O_{\langle , \rangle}$. Si la representación es irreducible, entonces no hay nada que verificar. Supongamos que existen subespacios invariantes no triviales. Tomemos uno de la menor dimensión posible, digamos V_1. Entonces sabemos que $W = V_1^{\perp}$ (espacio ortogonal a V_1 respecto a nuestro producto interior) también es invariante por

$\rho(G)$ por el corolario anterior. Tenemos que la representación inducida por ρ, digamos $\rho_1 : G \to GL(V_1)$ es irreducible por la minimalidad de la dimensión. Ahora miramos la representación $\rho : G \to GL(W)$ y procedemos de la misma manera como lo hemos hecho para V. Este proceso termina despues de un número finito de pasos debido a que V tiene dimensión finita y nos entrega una descomposición ortogonal $V = V_1 \times V_2 \times \cdots \times V_N$ y representaciones irreducibles $\rho_j = \rho : G \to GL(V_j)$. Ahora es claro por la construcción que $\rho : G \to GL(V)$ es equivalente al producto de las representaciones $\rho_j : G \to GL(V_j)$. Ahora necesitamos ver la unicidad módulo isomorfismos de representaciones. Para esto, supongamos que tenemos otra representación equivalente a la representación $\rho = (\rho_1, ..., \rho_N) : G \to GL(V_1) \times \cdots \times GL(V_N)$, digamos la representación $\eta = (\eta_1, ..., \eta_M) : G \to GL(W_1) \times \cdots \times GL(W_M)$, donde cada representación $\eta_j : G \to GL(W_j)$ es irreducible. Sea $L : V_1 \times \cdots V_N \to W_1 \times \cdots \times W_M$ el isomorfismo de tales representaciones. Entonces, $L(V_j)$ es un subespacio invariante por la representación η, luego debe coincidir por la irreducibilidad a una de los subespacios W_r. Así, L establece una biyección entre los espacios V_1,..., V_N y los espacios W_1,..., W_M, enparticular, $N = M$. □

Observación 30.0.13. — En el resultado anterior, tenemos que en la representación producto $\rho = (\rho_1, ..., \rho_N) : G \to GL(V_1) \times \cdots \times GL(V_N)$ en representaciones factores irreducibles, puede occurrir que dos de ellas, digamos $\rho_i : G \to GL(V_i)$ y $\rho_j : G \to GL(V_j)$, sean isomorfas. En ese caso, podemos reordenar los factores de manera que los factores $\rho_1 : G \to GL(V_1)$,..., $\rho_k : G \to GL(V_k)$ son los factores no equivalentes y escribir como

$$\rho = (\rho_1^{n_1}, ..., \rho_k^{n_k}) : G \to GL(V_1^{n_1}) \times \cdots \times GL(V_k^{n_k}),$$

donde n_j denota la cantidad de factores equivalentes a la representación ρ_j.

Ejemplo 30.0.14. — Consideremos el espacio vectorial real (podemos usar otros cuerpos) $V = \mathbb{R}^n$. Tenemos de manera natural una representación de grado n del grupo simétrico $\mathcal{S}_n$ actuando por permutaciones en las coordenadas de los vectores de V. De manera más precisa, consideremos los generadores $a = (1, 2, 3, ..., n), b = (1, 2)$. Entonces definimos

$$\rho_n(a) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

$$\rho_n(b) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

La representación $\rho_n : \mathcal{S}_n \to O_n < GL(\mathbb{R}^n) \cong GL(n, \mathbb{R})$ resulta ser reducible, donde O_n denota el subgrupo de las rotaciones. En efecto, si consideramos el subespacio vectorial de dimensión uno W generado por el vector $(1, 1, ..., 1, 1)$, entonces obtenemos que $\rho_n(g)(W) = W$, para cada $g \in \mathcal{S}_n$. Como $\rho_n(\mathcal{S}_n) < O_n$, tenemos que cada $\rho(g)$, $g \in \mathcal{S}_n$ es una simetría para el producto Euclidiano estandard (dado por el producto punto). En particular, $W^\perp$, el subespacio ortogonal a W, también resulta invariante, donde

$$W^\perp = \{(x_1, ..., x_n) \in \mathbb{R}^n : x_1 + x_2 + \cdots + x_n = 0\} \cong \mathbb{R}^{n-1}$$

Consideremos el isomorfismo

$$\eta : \mathbb{R}^{n-1} \to W$$

definido por

$$\eta(e_j) = E_j - E_n$$

donde $e_j \in \mathbb{R}^{n-1}$ (respectivamente, $E_j \in \mathbb{R}^n$) es el vector canónico con todas sus coordenadas igual a cero excepto la coordenada j-ésima que es igual a 1. Usando este isomorfismo, podemos mirar la representación inducida $\rho_n(\mathcal{S}_n)$ sobre W como una representación en $\mathbb{R}^{n-1}$, digamos

$$\rho_{n-1} : \mathcal{S}_n \to GL(\mathbb{R}^{n-1}),$$

definida por $\rho_{n-1}(g) = \eta^{-1}\rho(g)\eta$. Se puede ver que

$$\rho_{n-1}(a) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -1 & -1 & -1 & \cdots & -1 & -1 \end{pmatrix}$$

$$\rho_{n-1}(b) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Esta representación de grado $(n-1)$ es llamada la *representación estandard* del grupo $\mathcal{S}_n$. Se sabe que esta representación es irreducible. La idea es que si tomamos un vector $v \neq 0 \in \mathbb{R}^{n-1}$, entonces v, $\rho_{n-1}(a)(v)$, $\rho_{n-1}(a^2)(v)$,..., $\rho_{n-1}(a^{n-2})(v)$ resulta ser una base de $\mathbb{R}^{n-1}$. Por ejemplo, si $n = 3$ y $v = (u, v) \neq (0, 0)$, entonces la condición para

que v y $\rho_2(a)(v) = (-v, u-v)$ sean linealmente dependientes es equivalente a que exista $\lambda \in \mathbb{R}$ tal que el sistema lineal

$$\left\{ \begin{array}{rcrcl} \lambda u & + & v & = & 0 \\ -u & + & (1+\lambda)v & = & 0 \end{array} \right.$$

tenga como solución a (u, v). Esto obliga a que el determinante de la matriz asociada al sistema sea cero. Pero el determinante de tal matriz es $\lambda^2+\lambda+1$, el cual no tiene solución real, una contradicción.
De lo anterior tenemos la descomposición en factores irreducibles $\rho_n = (\rho_{n-1}, (-1))$, donde (-1) es la representación uno-dimensional que envía a las permutacions pares en -1 y a las impares en 1.

Ejercicio 100. — *Verificar la irreducibilidad de la representación $\rho_{n-1}(\mathcal{S}_n)$ del ejemplo anterior.*

Ejemplo 30.0.15. — El ejemplo anterior, para el caso $n = 3$, nos da una representación irreducible de $\mathcal{S}_3$ en el espacio vectorial real $\mathbb{R}^2$, más aún, en el espacio vectorial $\mathcal{Q}^2$. Miremos otras representaciones de este grupo. Podemos hacer actuar el grupo en si mismo como sigue

$$\phi : \mathcal{S}_3 \to Perm(\mathcal{S}_3) : \sigma \mapsto \phi(\sigma)$$

donde

$$\phi(\sigma) : \mathcal{S}_3 \to \mathcal{S}_3 : \tau \mapsto \sigma\tau$$

Por ejemplo, $\phi((1,2,3))$ actúa de la siguiente manera :

$$x_1 = I \mapsto (1,2,3) = x_2$$

$$x_2 = (1,2,3) \mapsto (1,3,2) = x_3$$

$$x_3 = (1,3,2) \mapsto I = x_1$$

$$x_4 = (1,2) \mapsto (1,3) = x_5$$

$$x_5 = (1,3) \mapsto (2,3) = x_6$$

$$x_6 = (2,3) \mapsto (1,2) = x_4$$

Luego podemos mirar en las coordenadas

$$\left[\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array} \right] \in \mathbb{Q}^6$$

que $\phi((1,2,3)$ puede ser representada por la matriz

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

En forma similar, $\phi((1,2))$ es dada por

$$\begin{aligned} x_1 = I &\mapsto (1,2) = x_4 \\ x_2 = (1,2,3) &\mapsto (2,3) = x_6 \\ x_3 = (1,3,2) &\mapsto (1,3) = x_5 \\ x_4 = (1,2) &\mapsto I = x_1 \\ x_5 = (1,3) &\mapsto (1,3,2) = x_3 \\ x_6 = (2,3) &\mapsto (1,2,3) = x_2 \end{aligned}$$

puede ser representada por la matriz

$$B = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

La función dada por

$$\psi : \mathcal{S}_3 \to GL(\mathbb{Q}^6)$$

definida por $\psi((1,2,3)) = A$ y $\psi((1,2)) = B$, define una representación racional de grado 6. Consideremos el subespacio $W < \mathbb{Q}^6$ de dimensión 3 correspondiente a tomar $w_1 = x_1 + x_4 = (1,0,0,1,0,0)$, $w_2 = x_2 + x_5 = (0,1,0,0,1,0)$, $w_3 = x_3 + x_6 = (0,0,1,0,0,1)$. Entonces W es invariante, es decir, la representación es reducible. Más aún, la representación en W es dada por

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

es decir, obtenemos la representación reducible ρ_3 del ejemplo anterior.

Ejemplo 30.0.16. — Consideremos el grupo más simple que tenemos, es decir, el grupo cíclico de orden dos

$$G = \langle x : x^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$$

Consideremos cualquier representación

$$\rho : G \to GL(V)$$

donde V es algún espacio vectorial sobre un cuerpo $\mathcal{K}$. Entonces si consideramos los espacios propios

$$V^+ = \{v \in V : \rho(x)(v) = v\}$$
$$V^- = \{v \in V : \rho(x)(v) = -v\}$$

entonces tenemos la descomposición

$$V = V^+ \oplus V^-$$

Escogiendo una base para V^+ y una base de V^-, obtenemos al juntarlas una base de V. En esta base, la representación es entonces equivalente a la representación

$$\eta : G \to GL(V^+ \times V^-) < GL(V^+) \times GL(V^-)$$

donde

$$\eta(x) = \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}$$

De aquí observamos que las únicas representaciones irreducibles de G son las siguientes dos de grado 1 :

$$\rho_+ : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto 1$$
$$\rho_- : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto -1$$

Ejemplo 30.0.17. — Consideremos ahora el grupo Abeliano más simple que no sea cíclico, es decir,

$$G = \langle x, y : x^2, y^2, (xy)^2 \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Consideremos cualquier representación

$$\rho : G \to GL(V)$$

donde V es algún espacio vectorial sobre un cuerpo $\mathcal{K}$. Entonces si consideramos los espacios propios

$$V^+ = \{v \in V : \rho(x)(v) = v\}$$
$$V^- = \{v \in V : \rho(x)(v) = -v\}$$

El hecho que $\rho(x)$ y $\rho(y)$ conmutan asegura que $\rho(y)$ deja a los subespacios V^+ y V^- invariantes. Entonces podemos escoger los subespacios siguientes :

$$V_+^+ = \{v \in V^+ : \rho(y)(v) = v\}$$
$$V_-^+ = \{v \in V^+ : \rho(y)(v) = -v\}$$
$$V_+^- = \{v \in V^- : \rho(y)(v) = v\}$$
$$V_-^- = \{v \in V^- : \rho(y)(v) = -v\}$$

Tenemos entoces que

$$V = V_+^+ \oplus V_-^+ \oplus V_+^- \oplus V_-^-$$

Podemos escoger una base de V adjuntando primero una bse de V_+^+, luego una base de V_-^+, luego una base de V_+^- y finalmente una base de V_-^-. En esta base, la representación es entonces equivalente a la representación

$$\eta : G \to GL(V_+^+ \times V_-^+ \times V_+^- \times V_-^-) < GL(V_+^+) \times GL(V_-^+) \times GL(V_+^-) \times GL(V_-^-)$$

donde

$$\eta(x) = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -I & 0 \\ 0 & 0 & 0 & -I \end{bmatrix} \quad \eta(y) = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & -I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \end{bmatrix}$$

Luego las representaciones irreducibles de G son las siguientes cuatro de grado 1 :

$$\rho_{++} : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto 1,\ y \mapsto 1$$
$$\rho_{+-} : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto 1,\ y \mapsto -1$$
$$\rho_{-+} : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto -1\ y \mapsto 1$$
$$\rho_{--} : G \to GL(\mathcal{K}) = \mathcal{K}^* : x \mapsto -1\ y \mapsto -1$$

CAPÍTULO 31

CARÁCTERES Y CONTEO DE REPRESENTACIONES IRREDUCIBLES

En esta sección veremos como determinar cuantas representaciones irreducibles no equivalentes sobre el cuerpo de los números complejos existen para cada grupo finito $(G, *)$. De manera más precisa.

Teorema 31.0.18. — *Sea $(G, *)$ un grupo finito. Entonces el número de representaciones irreducibles complejas no equivalentes es igual al número de clases de conjugación en G.*

Ejemplo 31.0.19. — Para el grupo simétrico $\mathcal{S}_n$ habíamos visto en la sección 15 que el número de clases de conjugación es igual al número de soluciones del sistema

$$\mu_1 + \mu_2 + \cdots + \mu_n = n$$

$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \geq 0$$

luego, ese número es exactamente la cantidad de representaciones irreducibles complejas no equivalentes de $\mathcal{S}_n$.

Necesitaremos algunos conceptos que iremos definiendo a continuación.

Definición 31.0.20. — Cada representación compleja $\phi : G \to GL(V)$, de un grupo $(G, *)$ (finito o infinito) de grado finito tiene asociada la función

$$\chi_\phi : G \to \mathbb{C} : g \mapsto Tr(\phi(g))$$

donde $Tr(\phi(g))$ denota la traza del automorfismo lineal $\phi(g) : V \to V$. A esta función la llamaremos el *carácter* de ϕ. Observemos que

$$\chi_\phi(I_G) = \dim(V)$$

Como conjugación preserva las trazas, vemos que el carácter de representaciones equivalentes es el mismo. Más aún, si $g, h \in G$, entonces vale que $\chi_\phi(g) = \chi_\phi(h * g * h^{-1})$; luego el carácter es constante en cada clase de conjugación en G.

Ejercicio 101. — *Ya que hemos hablado de producto de representaciones, digamos en este punto que si $\phi : G \to GL(V)$ y $\psi : G \to GL(W)$ son dos representaciones del grupo finito $(G, *)$, ambas de grado finito, entonces*

$$\chi_{(\phi,\psi)} = \chi_\phi + \chi_\psi$$

Verificar que el conjunto de los carácteres de todas las representaciones lineales de grado finito de un grupo finito $(G, *)$ no es necesariamente un espacio vectorial.

tenemos que el conjunto de los carácteres no define un espacio vectorial.

Definición 31.0.21. — El conjunto de las *funciones de clase* es

$$F(G) = \{f : G \to \mathbb{C} : \ f \text{ es constante en las clases de conjugación de } G\}$$

Definición 31.0.22. — Denotemos por $Car(G) \subset F(G)$ al conjunto de los carácteres de las representaciones de grado finito de G.

Ejercicio 102. — *Verificar que $F(G)$ es el espacio vectorial más pequeño que contiene $Car(G)$.*

Ejercicio 103. — *Calcular los carácteres asociados a las representaciones de grado finito de las secciones anteriores. En particular,*

(i) para la representación lineal asociado a una acción $\phi : G \to Perm(X)$, del grupo finito $(G, *)$ sobre un conjunto finito X, verificar que el carácter evaluado en $g \in G$ coincide con la cardinalidad de $Fix(\phi(g))$;

(ii) $\chi_{\phi\otimes\psi}(g) = \chi_\phi(g)\chi_\psi(g)$

(iii) $\chi_{\phi^*}(g) = \overline{\chi_\phi(g)}$

(iv) $\chi_{\phi\wedge\phi}(g) = \frac{1}{2}\left(\chi_\phi(g)^2 - \chi_\phi(g^2)\right)$

Ejercicio 104. — *Sea $\phi : G \to GL(V)$ una representación compleja de grado finito del grupo finito $(G, *)$ y $\chi_\phi : G \to \mathbb{C}$ su carácter asociado. Verificar que χ_ϕ permite conocer los valores propios de $\phi(g)$ para cada $g \in G$ (observe que si los valores propios de g son $\{\lambda_j\}$, entonces los valores propios de g^k son $\{\lambda_j^k\}$).*

Supongamos que tenemos una representación compleja de grado finito de un grupo finito $(G, *)$, digamos

$$\phi : G \to GL(V)$$

Como $\chi_\phi(I_G) = \dim(V)$, tenemos que el carácter determina el grado de la representación. Para esta acción tenemos que

$$V_G = \{v \in V : \eta(g)(v) = v \text{ para cada } g \in G\}$$

Ejercicio 105. — *Verificar que V_G es un subespacio vectorial de V y que la representación η es irreducible sí y sólo si $V_G = \{0\}$.*

Una manera de calcular explícitamente el subespacio vectorial V_G es la siguiente. Consideremos la función lineal dada por el promedio

$$L = \frac{1}{|G|} \sum_{g \in G} \eta(g) : V \to V \in \text{Hom}_G(\phi, \phi)$$

Tenemos que
(i) $L(v) \in V_G$, para cada $v \in V$;
(ii) $L(v) = v$, para cada $v \in V_G$.
De esta manera, $L : V \to V_G$ es una proyección sobre V_G y además

$$V_G = Fix(L)$$

en particular,

$$\dim(V_G) = Tr(L) = \frac{1}{|G|} \sum_{g \in G} Tr(\eta(g)) =$$

$$= \frac{1}{|G|} \sum_{g \in G} \chi_\eta(g)$$

En particular, si η es una representación irreducible, entonces necesariamente debemos tener

$$\sum_{g \in G} \chi_\eta(g) = 0$$

Consideremos ahora dos representaciones irreducibles

$$\phi : G \to GL(V) \text{ y } \psi : G \to GL(W)$$

podemos considerar el espacio vectorial $\text{Hom}_G(\phi, \psi)$ formado por todos los homomorfismos $M : V \to W$ de las dos representaciones. Como consecuencia del lema de Schur y su corolario, tenemos que

$$\dim(\text{Hom}_G(\phi, \psi)) = \begin{cases} 1 & \text{si } \phi \text{ y } \psi \text{ son equivalentes} \\ 0 & \text{en caso contrario} \end{cases}$$

Consideremos la representación homomorfismo

$$\eta = \text{Hom}(\phi, \psi) : G \to GL(Hom(V, W))$$

cuyo carácter asociado es dado por $\chi_\eta = \overline{\chi_\phi} \chi_\psi$

En este caso, tenemos que $\text{Hom}(V,W)_G = \text{Hom}_G(\phi,\psi)$.
Así, por lo anterior tenemos que

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_\phi(g)}\chi_\psi(g) = \frac{1}{|G|}\sum_{g\in G}\chi_\eta(g) = \dim(\text{Hom}_G(\phi,\psi)) =$$

$$= \dim(\text{Hom}(V,W))_G = \begin{cases} 1 & \text{si las representaciones son equivalentes} \\ 0 & \text{en caso contrario} \end{cases}$$

Esta fórmula nos permite definir un producto interior Hermitiano

$$(f_1,f_2) = \frac{1}{|G|}\sum_{g\in G}\overline{f_1(g)}f_2(g)$$

sobre el espacio vectorial $F(G)$ de las funciones de clases de G de manera que los carácteres de representaciones irreducibles no equivalentes forman un conjunto ortonormal. Una consecuencia de esta situación es la siguiente.

Proposición 31.0.23. — *Toda representación compleja de grado finito de un grupo finito $(G,*)$, digamos $\phi : G \to GL(V)$, está únicamente determinada, módulo equivalencia, por su carácter. Más aún, la representación es irreducible sí y sólo si $(\chi_\phi,\chi_\phi) = 1$.*

Demonstración. —

Situación Irreducible. Consideremos dos representaciones irreducibles $\phi : G \to GL(V)$ y $\psi : G \to GL(W)$, ambas de grado finito con el mismo carácter χ. Supongamos primero que ambas representaciones son irreducibles, entonces podemos utilizar lo hecho anteriormente para obtener nuestro resultado.

Situación General. Supongamos que la representación ϕ no es irreducible. Entonces, podemos encontrar representaciones irreducibles no equivalentes $\rho_j : G \to GL(V_j)$, para $j = 1,...,r$, de manera que $\rho = (\rho_1^{a_1},...,\rho_r^{a_r}) : G \to GL(V_1^{a_1}\times\cdots\times V_r^{a_r})$ es equivalente a ϕ. En este caso tenemos que

$$\chi_\phi = \chi_\rho = \sum_{j=1}^{r} a_j\chi_{\rho_j}$$

Como cada representación irreducible está determinada por su carácter, tenemos que la representación ϕ queda determinada por su carácter. Observemos que en este caso $(\chi_\phi,\chi_\phi) = \sum_{j=1}^{r} a_j^2$.

□

De lo anterior, vemos que las representaciones lineales de grado finito de un grupo finito $(G,*)$ quedan determinados, módulo equivalencia, por sus cácteres.
Supongamos que A_1,..., A_n son las diferentes clases de conjugación del grupo G, donde $A_1 = \{I_G\}$. Escojamos un representante de cada clase, digamos $g_j \in A_j$, $j = 2,3,...,n$.

Sea $a_j = \#A_j$. Si $f : G \to \mathbb{C}$ es una función de clase del grupo finito de G, entonces consideremos el vector

$$(f(I_G), f(g_2), ..., f(g_n)) \in \mathbb{C}^n$$

Esto nos permite construir una función lineal inyectiva

$$M : F(G) \to \mathbb{C}^n$$

y así considerar $F(G)$ como un subespacio de $\mathbb{C}^n$ y, en particular, considerar $Car(G)$ como un conjunto de vectores.
En el espacio vectorial $\mathbb{C}^n$ podemos considerar el producto interior Hermitiano

$$\langle (x_1, ..., x_n), (y_1, ..., y_n) \rangle = \frac{1}{|G|} \sum_{j=1}^{n} a_j \overline{x_j} y_j$$

Ejercicio 106. — *Verificar que este producto Hermitiano hace que M sea una isometría respecto al producto Hermitiano considerado anteriormente para $F(G)$.*

Ahora, los vectores en $\mathbb{C}^n$ que corresponden a los carácteres de representaciones irreducibles forman un conjunto ortonormal respecto al producto Hermitiano, en particular, se tiene la segunda consecuencia, una aproximación del teorema 31.0.18.

Proposición 31.0.24. — *El número de representaciones irreducibles no equivalente de grado finito de un grupo finito $(G, *)$ es a lo más el número de clases de conjugación en G.*

Ejemplo 31.0.25. — Consideremos $(G, *)$ un grupo finito y la acción $\phi : G \to Perm(G) : h \mapsto g * h$. Consideremos la representación lineal que esta define, es decir la representación regular de G, denotemosla por $\phi_G : G \to GL(V)$, donde $\dim(V) = |G|$. En este caso

$$\chi_{\phi_G}(g) = \begin{cases} 0 & \text{si } g \neq I_G \\ |G| & \text{si } g = I_G \end{cases}$$

En particular $\langle \chi_{\phi_G}, \chi_{\phi_G} \rangle = |G|^2$, con lo cual obtenemos que esta representación lineal no es irreducible para $|G| > 1$. En este caso, tenemos que ϕ_G es equivalente a la representación $\rho = (\rho_1^{a_1}, ..., \rho_r^{a_r})$, donde ρ_1,..., ρ_r son todas las repersentaciones irreducibles de G de grado finito y $a_j \in \{0, 1, 2, ...\}$ Habíamos observado que

$$a_j = \langle \rho_j, \rho \rangle = \langle \rho_j, \chi_{\phi_G} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\rho_j(g)} \chi_{\phi_G}(g) = \frac{1}{|G|} \overline{\rho_j(I_G)} \chi_{\phi_G}(I_G) =$$

$$= \overline{\rho_j(I_G)} = \text{grado de la representación } \rho_j > 0$$

Como consecuencia de esto vemos que en la representación regular ϕ_G del grupo G aparecen todas las representaciones irreducibles de G, cada una apareciendo exactamente

tantas veces como su grado. Una consecuencia simple de esto es que el número de representaciones irreducibles no equivalentes es finita (lo que ya sabíamos por la proposición anterior). Además, tenemos que

$$|G| = \langle \chi_{\phi_G}, \chi_{\phi_G} \rangle = \sum_{j=1}^{r} a_j^2$$

Proposición 31.0.26. — *La suma de los cuadrados de los grados de todas las representaciones irreducibles no equivalentes de un grupo finito es igual al orden de este.*

Ejemplo 31.0.27. — Para el grupo $\mathcal{S}_3$ tenemos a lo más tres representaciones irreducibles no equivalentes. Por la proposición anterior se puede ver que no hay sólo una representación irreducible ya que 6 no es un cuadrado de un entero. Si hubiesen sólo dos representaciones irreducibles, entonces estaríamos diciendo que 6 es suma de dos cuadrados, lo cual no es posible. De esta manera, obtenemos que deben haber exactamente tres representaciones irreducibles no equivalentes. Si denotamos por $a_1, a_2, a_3 \in \{1, 2, ..\}$ los grados de estas, entonces debemos tener $a_1^2 + a_2^2 + a_3^2 = 6$. De aquí vemos que la única posibilidad es dada por el siguiente trío, módulo permutación, $(1, 1, 2)$.

Ahora procedemos a verificar que el conjunto ortonormal de vectores que corresponden a las representaciones irreducibles de G es de hecho una base, obteniendo de esta manera la demostración del teorema 31.0.18.
Para esto supongamos que tenemos la posibilidad de escoger una función de clases de G, digamos $f \in F(G)$, que sea ortogonal a cada carácter de una representación irreducible de G. Bastará con verificar que $f = 0$.
Consideremos una representación lineal $\phi : G \to GL(V)$ de grado finito d. Definamos la función lineal $L : V \to V$ por

$$L(v) = \sum_{g \in G} f(g)\phi(g)(v)$$

Para cada $h \in G$ y cada $v \in V$, tenemos que

$$\phi(h) \circ L \circ \phi(h^{-1})(v) = \sum_{g \in G} f(g)\phi(h * g * h^{-1})(v) =$$

$$= \sum_{g \in G} f(h * g * h^{-1})\phi(h * g * h^{-1})(v) = \sum_{k \in G} f(k)\phi(k)(v) = L(v)$$

en particular, $L \in \mathrm{Hom}_G(\phi, \phi)$. Como consecuencia del corolario al lema de Schur vale que $L(v) = \lambda v$ para cierto valor $\lambda \in \mathbb{C}$, luego

$$\lambda d = Tr(L) = \sum_{g \in G} f(g)Tr(\phi(g)) = \sum_{g \in G} f(g)\chi_\phi(g) =$$

$$= |G|\langle \overline{f}, \chi_\phi \rangle = |G|\overline{\langle f, \overline{\chi_\phi} \rangle} = |G|\overline{\langle f, \chi_{\phi^*} \rangle}$$

y como χ_{ϕ^*} es una combinación lineal de los carácteres de las representaciones irreducibles que descomponen la representación ϕ, obtenemos finalmente

$$\lambda d = 0$$

y, en particular, $\lambda = 0$ como deseabamos para completar la demostración del teorema 31.0.18.

En resumen. Dado un grupo finito $(G, *)$, procedemos como sigue :
(1) determinamos la cantidad n de clases de conjugación y las respectivas cardinalidades $a_1 = 1$, a_2,..., a_n.
(2) consideramos el producto interior Hermitiano en $\mathbb{C}^n$ dado por

$$\langle (x_1, ..., x_n), (y_1, ..., y_n) \rangle = \frac{1}{|G|} \sum_{j=1}^{n} a_j \overline{x_j} y_j$$

(3) buscamos bases ortonormales de $\mathbb{C}^n$ con la propiedad de que la primera coordenada de cada vector involucrado sea un entero positivo y tal que la suma de los cuadrados de las primeras coordenadas sea igual al orden del grupo. Uno de los vectores involucrados siempre es $(1, 1, ..., 1)$ que corresponde a la representación trivial

$$1 : G \to \mathbb{C}^* : g \mapsto 1$$

Ejemplo 31.0.28. — Consideremos el grupo simétrico $\mathcal{S}_3$. En este caso tenemos 3 clases de conjugación $A_1 = \{I\}$, $A_2 = \{(1, 2), (1, 3), (2, 3)\}$ y $A_3 = \{(1, 2, 3), (1, 3, 2)\}$. De esto sabemos que hay exactamente tres representaciones irreducibles de $\mathcal{S}_3$. En $\mathbb{C}^3$ entonces consideramos el producto Hermitiano

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = \frac{1}{6} (\overline{x_1} y_1 + 3\overline{x_2} y_2 + 2\overline{x_3} y_3)$$

Si consideramos tres vectores $(a_j, b_j, c_j) \in \mathbb{C}^3$, donde $a_j \in \{1, 2, ...\}$, formando una base ortonormal, entonces debemos tener las ecuaciones ($i \neq j \in \{1, 2, 3\}$)

$$\begin{array}{rcl} a_j^2 + 3|b_j|^2 + 2|c_j|^2 & = & 6 \\ a_i a_j + 3\overline{b_i} b_j + 2\overline{c_i} c_j & = & 0 \end{array}$$

La igualdad $aj^2 + 3|b_j|^2 + 2|c_j|^2 = 6$ de donde podemos observar que $a_j \in \{1, 2\}$.
De esta información obtenemos que las tres representaciones irreducibles son de grado 1 y/o 2. Por un lado, siempre está la representación irreducible de grado 1 trivial

$$1 : \mathcal{S}_3 \to \mathbb{C}^* : g \mapsto 1$$

cuyo carácter corresponde al vector $(1, 1, 1)$. Otra representación irreducible de grado 1 es

$$-1 : \mathcal{S} \to \mathbb{C}^* : g \mapsto \begin{cases} -1 & \text{si } g \text{ tiene orden par} \\ 1 & \text{en caso contrario} \end{cases}$$

cuyo carácter corresponde al vector $(1,-1,1)$. La tercera representación irreducible tiene carácter correspondiente a un vector (a,b,c), donde $a \in \{1,2\}$ y valen las igualdades :

$$\begin{aligned} a^2+3|b|^2+2|c|^2 &= 6 \\ a+3b+2c &= 0 \\ a-3b+2c &= 0 \end{aligned}$$

De las dos últimas igualdades obtenemos al sumarlas $a=-2c$, de donde estamos obligados a tomar $a=2$, $c=-1$ y luego $b=0$. En particular, la tercera representación irreducible es dada por el vector $(2,0,-1)$ que es de grado 2. Esta representación es dada por $\phi : G \to GL(\mathbb{C}^2)$ tal que

$$\phi(1,2,3) = \begin{bmatrix} e^{\pi i/3} & 0 \\ 0 & e^{-\pi i/3} \end{bmatrix}$$

$$\phi(1,2) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

REFERENCIAS

[1] Burnside, W. *Theory of Groups of Finite Order*, Dover, 1955.

[2] Coxeter, H.S. and Moser, W.O. *Generators and Relations for Discrete Groups*, Springer-Verlag, 1965.

[3] Fraleigh, J.B. *A First Course in Abstract Algebra*, Addison-Wesley,1982.

[4] Fulton, W. and Harris, J.H. *Representation Theory*, Springer-Verlag, 1991.

[5] Jacobson, N. *Lecture in Abstract Algebra*, Princeton, vol.1, 1951, vol.2, 1953, vol.3, 1964.

[6] Herstein, I.N. *Topics in Algebra*, Blaisdell, 1964.

[7] Van der Waerden, B.L. *Modrn Algebra*, Ungar, vol.1, 1949, vol2, 1940.

INDICE