0 Breve repaso

Definiciones y ejemplos

Definición 0.1 *Un grupo es un par $(G, *)$ en el que G es un conjunto cualquiera (finito o no) y $*$ es una operación*

$$*: G \times G \longrightarrow G$$

que cumple:

- $*$ *es asociativa:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in G$$
- *Existe elemento neutro:*
$$\exists e \in G \ni e * a = a * e = a, \ \forall a \in G$$
- *Existe simétrico*
$$\forall a \in G \, \exists \, b \in G \ni b * a = a * b = e,$$

Comprobaremos que el neutro de un grupo, así como el simétrico de cada elemento, es único.

Notación 0.2 Es común designar a un grupo por la letra que indica el conjunto subyacente omitiendo la operación que le da estructura de grupo.

Un grupo G se dice abeliano si la operación $*$ es conmutativa. En este caso se suele utilizar la notación aditiva: la operación se designa mediante el signo $+$, el elemento neutro se escribe 0_G y se denomina cero, y el simétrico de a se escribe $-a$, recibiendo el nombre de opuesto.

Para grupos en general, a la manera del producto numérico, si no hay lugar a confusión la operación $*$ se omite escribiéndose ab en lugar de $a * b$. Inspirados en la notación multiplicativa, el neutro se denomina uno y se escribe 1_G; finalmente el simétrico de a se dice inverso de a y se escribe a^{-1}.

Compruébese que $(a^{-1})^{-1} = a$ y que $(ab)^{-1} = b^{-1}a^{-1}$.

Ejemplos y contraejemplos

1. El origen de la teoría de grupos se sitúa en las permutaciones de las raíces de un polinomio. Brevemente por ahora[1], dado un conjunto E se llama permutación a una aplicación biyectiva del conjunto E en sí. La composición de aplicaciones dota al conjunto $\Sigma(E)$ de estructura de grupo, siendo el neutro la aplicación idéntica y el inverso de una permutación la aplicación inversa. Para el caso $E = \{1, \ldots, n\}$, $\Sigma(E)$ se escribe Σ_n ó S_n.

[1] pues este es el tópico fundamental del curso

2. Posteriormente el estudio de la estructura de la materia ha dado auge a la teoría de grupos considerando para un polígono regular de n lados el conjunto de movimientos del plano que lo transforman en sí mismo. Asimismo la composición de aplicaciones nos da un grupo que recibe el nombre de grupo del polígono de n lados. Se tienen así el **grupo del triángulo, grupo del cuadrado, grupo del exágono**... Por ejemplo el grupo del triángulo consiste de los giros de $120^o, 240^o$ con centro el baricentro, las simetrías respecto de las alturas y la identidad.

   Este ejemplo tipo será asimismo objeto de particular estudio en este curso.

3. El desarrollo de la teoría de grupos ha llegado a identificar como tales

$$(\mathbf{Z},+),(\mathbf{Q},+),(\mathbf{R},+),(\mathbf{C},+),(\mathbf{Z}/m\mathbf{Z},+),(\text{Matrices},+),\ldots$$

   caso particular del grupo aditivo de un anillo $(A,+,.)$ y

$$(\mathbf{Q}^*,.),(\mathbf{R}^*,.),(\mathbf{C}^*,.),(\mathbf{Z}/p\mathbf{Z},.),(\text{Matrices regulares},.),\ldots$$

   caso particular del grupo $\mathcal{U}(A)$ de las unidades del anillo $(A,+,.)$.

4. Sin embargo, no son grupos

$$(\mathbf{N},+),(\mathbf{Z},.),(\mathbf{Q},.),(\mathbf{R},.),(\mathbf{C},.),(\text{Matrices},.)$$

En los ejemplos anteriores puede observarse que las permutaciones del conjunto de vocales débiles $\{i,u\}$ son permutaciones del conjunto de vocales $\{a,e,i,o,u\}$, el grupo del triángulo es parte del grupo del exágono, que $(\mathbf{Z},+)$ lo es de $(\mathbf{Q},+)$, ... manteniéndose además los elementos neutros y simétricos. Reciben el nombre de subgrupos. Más precisamente,

Subgrupos. Generación de subgrupos

Definición 0.3 *Dado un grupo G se dice subgrupo a una parte no vacía S de G que cumple*

$$a,b\in S \Longrightarrow ab^{-1}\in S$$

Se escribe $S\leq G$. Nótese que al ser S no vacío, existe $a\in S$ y el neutro $1_G=aa^{-1}$ debe pertenecer a S. Asimismo, si $a\in S$, $a^{-1}=1_Ga^{-1}\in S$; finalmente, la restricción de la operación a S es cerrada en S en el sentido de que

$$a,b\in S \Longrightarrow a,b^{-1}\in S \Longrightarrow a(b^{-1})^{-1}=ab\in S$$

Es decir, como no podía ser menos, un subgrupo de un grupo es, por sí solo, un grupo.

Ejemplos y contraejemplos

1. $(\mathbf{Z},+)\leq(\mathbf{Q},+)\leq(\mathbf{R},+)\leq(\mathbf{C},+)$

2. $Gl(n, \mathbf{Q}) \leq Gl(n, \mathbf{R}) \leq Gl(n, \mathbf{C})$
3. Dado un grupo G, el conjunto de elementos que conmutan con todos los demás
$$\mathbf{Z}(G) = \{x \in G \mid xy = yx, \forall y \in G\}$$
es un subgrupo de G que se dice centro de G. Claramente, si G es abeliano $\mathbf{Z}(G) = G$; $\mathbf{Z}(S_3) = 1$ y el centro del grupo del cuadrado está formado por el giro de 180^o y la identidad. Estas afirmaciones quedarán justificadas convenientemente.
4. $(\mathbf{N}, +) \not\leq (\mathbf{Z}, +)$, pues $2 \in \mathbf{N}$, pero $-2 \notin \mathbf{N}$.

Observación 0.4 Es fácil probar ya, como se hace con los subespacios en álgebra lineal, que la intersección de subgrupos es un nuevo subgrupo lo que da lugar cómodamente a la siguiente

Definición 0.5 *Dado un subconjunto E de un grupo G se dice subgrupo generado por E a la intersección de subgrupos de G que contienen a E:*
$$< E >= \bigcap \{S \leq G \mid E \subseteq S\}$$

Observación 0.6 Nótese que $E \subseteq < E >$ y que $< \emptyset >= 1_G$; ahora bien, tan cómoda definición da muy poca o nula información acerca de los elementos de $< E >$, cuando E es no vacío. Introduciendo el concepto de potencia en un grupo
$$a \in G, n \in \mathbf{N} \Longrightarrow \begin{cases} a^n = \overbrace{a \cdots a}^{n} \\ a^0 = 1_G \\ a^{-n} = (a^n)^{-1} \end{cases}$$
podemos enunciar

Proposición 0.7 *Dado un subconjunto no vacío E de G,*
$$< E >= \{x_1^{n_1} \cdots x_r^{n_r} \mid x_i \in E, n_i \in \mathbf{Z}\}$$

Demostración: Es claro que si S es un subgrupo de G conteniendo a E debe contener a las potencias de sus elementos y a los productos de éstas, lo que da el " $\supseteq$ ".

Recíprocamente el conjunto S de la derecha, contiene a E por lo que es no vacío; si $x_1^{n_1} \cdots x_r^{n_r}$ y $y_1^{m_1} \cdots y_r^{m_r}$ son dos elementos de S, pruebe el lector que $(z_1 \cdots z_n)^{-1} = z_n^{-1} \cdots z_1^{-1}$ y
$$(x_1^{n_1} \cdots x_r^{n_r})(y_1^{m_1} \cdots y_r^{m_r})^{-1} = x_1^{n_1} \cdots x_r^{n_r} y_r^{-m_r} \cdots y_1^{-m_1} \in S$$
por lo que S es un subgrupo de G conteniendo a E y se tiene el otro contenido.

En un grupo finito G se llama orden a la cantidad de elementos que posee. Se escribe $|G|$. Es clásico el siguiente

Teorema 0.8 (Lagrange) *El orden de un subgrupo S de G es divisor del orden de G.*

Demostración: Basta construir las denominadas clases a izquierda

$$xS = \{xs \mid s \in S\}$$

y ver que G es la unión disjunta de dichas clases, todas ellos de tamaño $|S|$.

Observación 0.9 Análogamente, existen las clases a derecha $Sx = \{sx \mid s \in S\}$. Curiosamente puede ocurrir que $xS \neq Sx$, pero de esto hablaremos a continuación.

Definición 0.10 *El número $|G|/|S|$ se dice índice de S en G y se escribe $[G : S]$.*

Grupo cociente. Subgrupos normales

Debe ser conocida la estructura de conjunto cociente a partir de una relación de equivalencia. Si tenemos ahora un grupo consideraremos relaciones de equivalencia $\sim$ que sean *compatibles o estables* con la operación del grupo; más precisamente

$$a \sim b, c \sim d \Longrightarrow ac \sim bd$$

Obsérvese que esto es lo que pasa en $\mathbf{Z}$ con la relación de congruencia (módulo m)

$$a \equiv b \iff a - b = \dot{m}$$

Tal compatibilidad permite dotar al cociente de estructura de grupo como indica la siguiente

Proposición 0.11 *Sea G un grupo y $\sim$ una relación de equivalencia en G compatible con su operación. Entonces, el conjunto cociente $G/\sim$ puede ser dotado de una operación que le da estructura de grupo. Se dice grupo cociente de G. Además, si G es abeliano, el cociente lo es.*

Demostración:

Definimos $(.): G/\sim \times G/\sim \longrightarrow G/\sim$ mediante $[x][y] = [xy]$ Es claro que se trata de una operación, muy fácil de ver que es asociativa, que el neutro es $[1_G]$ y que $[x]^{-1} = [x^{-1}]$. Finalmente, la conmutatividad se heredará de la posible conmutatividad en G.

Observación 0.12 ¿Es posible describir en términos de G las relaciones de equivalencia estables?, o lo que es lo mismo ¿describir todos los grupos cocientes de un grupo? Observemos algunos hechos notables de este tipo de relaciones de equivalencia:

1. $x \sim y \iff xy^{-1} \sim 1_G$
2. $x \sim y \iff x^{-1} \sim y^{-1}$ (se deduce fácilmente de la anterior)

3. La clase del neutro $[1_G]$ es un subgrupo N de G, pues
$$x, y \sim 1_G \Longrightarrow x, y^{-1} \sim 1_G, 1_G^{-1} \Longrightarrow xy^{-1} \sim 1_G 1_G^{-1} = 1_G$$
4. Las clases de equivalencia son de la forma
$$xN = \{y \in G \mid y = xn, n \sim 1_G\}$$
En efecto,
$$\begin{array}{rcl} y \in [x] & \iff & y \sim x \iff y^{-1} \sim x^{-1} \iff y^{-1}x \in N \iff \\ & \iff & y^{-1}x = n, n \in N \iff y = xn_1 \in xN \end{array}$$

Puestas así las cosas nos podemos plantear que las relaciones de equivalencia en G compatibles con su producto tienen como conjunto soporte a las denominadas clases laterales a izquierda
$$\{xN \mid x \in G, N \leq G\}$$

Sin embargo, la afirmación es incorrecta como lo muestra el siguiente

Ejemplo En S_3, el grupo simétrico de grado 3, consideramos el subgrupo N formado por 1 y la transposición (1 2). Entonces, las clases xN son
$$\{1, (1\ 2)\}$$
$$\{(1\ 3), (1\ 2\ 3)\}$$
$$\{(2\ 3), (1\ 3\ 2)\}$$
Sin embargo, la relación de equivalencia que produce esta partición no es compatible, pues
$$(1\ 3\ 2) = (1\ 3)(2\ 3) \not\sim (1\ 2\ 3)(1\ 3\ 2) = 1$$

Debemos en consecuencia buscar una propiedad más. Esta se deduce fácilmente de la observación directa de la operación en el grupo cociente considerando las clases a derecha
$$Nx = \{nx \mid n \in N, x \in G\}$$
como lo indica la siguiente

Proposición 0.13 *Sea N un subgrupo de G. Entonces,*
$$(xN)(yN) = (xy)N\ \forall x, y \in G \iff xN = Nx\ \forall x \in G$$

Demostración:
"Sólo si: En primer lugar, $xnx^{-1} = (xn)(x^{-1}1_G) \in xNx^{-1}N = 1_G N = N$. Ahora,
$$xn = (xnx^{-1})x = n_1 x \in Nx \Longrightarrow xN \subseteq Nx$$
Análogamente, $Nx \subseteq xN$
"Si": $xn_1yn_2 = x(n_1y)n_2 = x(yn_3)n_2 = (xy)n_4 \in (xy)N \Longrightarrow xNyN \subseteq (xy)N$
$$(xy)n = (x1_G)(yn) \in (xN)(yN) \Longrightarrow (xy)N \subseteq (xN)(yN)$$

Definición 0.14 *Un subgrupo N de G se dice normal*[2] *y se escribe $N \lhd G$ si $xN = Nx \, \forall x \in G$.*

Ejemplos y contraejemplos

1. El subgrupo $N = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$ del grupo simétrico de grado 3, es normal; de hecho
2. En un grupo todo subgrupo N de índice 2 es normal, pues
$$N \dot\cup xN = G = N \dot\cup Nx \Longrightarrow xN = Nx, \, \forall x \in G$$
3. Como habíamos anunciado el subgrupo $N = \{1, (1\ 2)\}$ del grupo simétrico de grado 3, no es normal. De hecho,
$$(1\ 3)N = \{(1\ 3), (1\ 2\ 3)\} \neq \{(1\ 3), (1\ 3\ 2)\} = N(1\ 3)$$

Proposición 0.15 $N \lhd G \iff xnx^{-1} \in N, \, \forall x \in G \, \forall n \in N$

Nótese que la condición de subgrupo normal es obvia en grupos abelianos; asimismo si N es normal en G lo es en cada subgrupo de G que lo contenga. El propio grupo y el neutro son subgrupos normales, obviamente; veremso que el centro siempre es normal. Un grupo sin subgrupos normales propios se dice simple.

Teorema 0.16 *Sea G un grupo.*

i) *Si una relación de equivalencia en G es compatible con su producto, la clase del neutro $[1_G]$ es un sugrupo normal de G.*

ii) *Si N es un sugrupo normal de G la reación $x \sim y \iff xy^{-1} \in N$ es de equivalencia y compatible con el producto de G. El grupo cociente se escribe G/N.*

iii) *La correspondencia*
$$N \longrightarrow \big(x \sim y \iff xy^{-1} \in N\big)$$
es una biyección entre el el conjunto de subgrupos normales de G y el conjunto de relaciones de equivalencia compatibles con su producto.

Demostración:

i) Vista en los resultados anteriores (0.12.3) y (0.13)

ii)

- Reflexiva: $xx^{-1} = 1_G \Longrightarrow x \sim x$
- Simétrica: $x \sim y \Longrightarrow xy^{-1} \in N \Longrightarrow yx^{-1} = (xy^{-1})^{-1} \in N \Longrightarrow y \sim x$
- Transitiva:
$$x \sim y, y \sim z \Longrightarrow (xy^{-1}) \in N, (yz^{-1}) \in N \Longrightarrow xz^{-1} = (xy^{-1})(yz^{-1}) \in N$$
- Compatible con el producto de G: Aquí está la clave; al ser N normal en G, $z^{-1}nz \in N, \, \forall z \in G \, \forall n \in N$; por tanto,

[2] invariante o distinguido

$$\begin{aligned} x \sim y, z \sim u \quad &\Longrightarrow \quad y = n_1 x, u = n_2 z \Longrightarrow \\ &\Longrightarrow \quad yu = n_1(xn_2)z = n_1(n_3 x)z = n_4 xz \Longrightarrow \\ &\Longrightarrow \quad xz \sim yu \end{aligned}$$

iii)

- Inyectiva: Sean N y M subgrupos normales de G tales que

  $$xy^{-1} \in N \iff xy^{-1} \in M$$

  Entonces,

  $$z \in N \iff z1_G^{-1} \in N \iff z1_G^{-1} \in M \iff z \in M$$

  y $N = M$.

- Sobre: Sea $\sim$ una relación de equivalencia en G, compatible con su producto. Sea $N = [1_G]$; que, $N \lhd G$ es (0.13) y que $x \sim y \iff xy^{-1} \in N$ es (0.12.1).

Corolario 0.17 *Si G es finito y N es normal en G, $|G| = |N||G/N|$*

Demostración: Es consecuencia del teorema de Lagrange, pues los elementos de G/N son las clases laterales.

Observación 0.18 Otra de las cualidades de los subgrupos normales es que permite obtener producto de subgrupos.

Proposición 0.19 *Si $N \lhd G$ y $S \leq G$,*

$$NS = \{ns \mid n \in N, s \in S\}$$

es un subgrupo de G, y $N \cap S \lhd S$.

Demostración:

$$\begin{aligned} (n_1 s_1)(n_2 s_2)^{-1} &= (n_1 s_1)(s_2^{-1} n_2^{-1}) = n_1 s_3 n_2^{-1} = \\ &= n_1(s_3 n_2^{-1} s_3^{-1}) s_3 = n_1 n_3 s_3 = n_4 s_3 \in NS \end{aligned}$$

La normalidad de $N \cap S$ en S es sencilla de probar.

Homomorfismos. Teoremas de isomorfía.

El proceso de paso al cociente es consecuencia del intento de simplificar una estructura. Por ejemplo[3] es más sencillo operar en $\mathbf{Z}/mZ$ que en $\mathbf{Z}$ y a veces es suficiente operar en el primero para obtener las consecuencias pretendidas en el segundo. recuerde, al efecto, la escolar *prueba del nueve* para *garantizar* algunos resultados aritméticos. El lector interesado puede consultar el estupendo libro de Lipson *Elements of Algebra and Algebraic computing.*

[3] aunque al lector novel le pueda parecer paradójico

El paso de $\mathbf{Z}$ a $\mathbf{Z}/m\mathbf{Z}$ consiste en sustituir una clase de números enteros por uno sólo: los múltiplos de m por 0, los múltiplos de $m+1$ por 1,.... Más precisamente, se considera la correspondencia $p\colon \mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z}$ dada por

$$p(z) = \{z, z+m, z+2m, \ldots, z+km, \ldots\} = [z]$$

El interés reside en que al ser la relación $x \equiv y \iff x - y = \dot{m}$ compatible con la suma[4]

$$[z_1 + z_2] = [z_1] + [z_2] \text{ o mejor } p(z_1 + z_2) = p(z_1) + p(z_2)$$

En general, dado un grupo G y un subgrupo N normal la correspondencia $p\colon G \longrightarrow G/N$ dada por $p(x) = xN$, cumple

$$p(xy) = (xy)N = (xN)(yN) = p(x)p(y)$$

Este tipo de correspondencias recibe el nombre de proyecciones canónicas. Es el origen de la siguiente

Definición 0.20 *Dados dos grupos G y H se dice homomorfismo a una aplicación $f\colon G \longrightarrow H$ tal que $f(xy) = f(x)f(y)$.*

Ejemplos y contraejemplos

1. Las proyecciones canónicas, que nos han servido como introducción, de $\mathbf{Z}$ en $\mathbf{Z}/m\mathbf{Z}$ y en general de G en G/N.

2. $[z] \longrightarrow i^z$ es un homomorfismo del grupo (aditivo) $(\mathbf{Z}/4\mathbf{Z}, +)$ de los enteros módulo 4 en el grupo multiplicativo $(\{\pm 1, \pm i\}, .)$ de las raíces cuartas de la unidad.

3. Dado un cuerpo K, $\det\colon Gl(m, K) \longrightarrow K^*$ es un homomorfismo de grupos.

4. La traza es un homomorfismo entre los grupos aditivos $M_{m\times n}(K)$ y K, pero no un homorfismo entre $Gl(m, K)$ y K^* pues

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Como consecuencia de la definición se tiene

Proposición 0.21 *Si $f\colon G \longrightarrow H$ es un homomorfismo de grupos*

i) $f(1_G) = 1_H$
ii) $f(x^{-1}) = f(x)^{-1}$, $\forall x \in G$
iii) $f(S) \leq H \; \forall S \leq G$.

[4] y también con el producto

Demostración: Clásica; se propone como ejercicio.

Observación 0.22 Como consecuencia, $\mathrm{Im}(f)$ es siempre un subgrupo. Entre homomorfismos se distinguen los inyectivos o **monomorfismos**, los suprayectivos o **epimorfismos** y los biyectivos o **isomorfismos**. Las proyecciones canónicas son siempre epimorfismos, pero no suelen ser monomorfismos[5]. Un bonito ejemplo de isomorfismo es el número 2 anterior. La inclusión de un subgrupo en un grupo es siempre un monomorfismo, pero no suele ser un epimorfismo[6].

Asociado a todo homomorfismo aparece siempre un subgrupo normal; dicho subgrupo mide su no inyectividad y da cociente isomorfo a la imagen:

Teorema 0.23 (Primer teorema de isomorfía) *Si* $f\colon G \longrightarrow H$ *es un homomorfismo,* $\ker f = \{x \in G \mid f(x) = 1_H\}$ *es un subgrupo normal de* G *que cumple:*

i) f *es monomorfismo* $\iff \ker f = 1_G$

ii) *El grupo cociente* $G/\ker f$ *es isomorfo a* $Im(f)$.

Demostración: Sea $x \in \ker f$

$$f(yxy^{-1}) = f(y)f(x)f(y^{-1}) = f(y)1_H f(y^{-1}) = f(y)f(y)^{-1} = 1_H$$

Por tanto, $yxy^{-1} \in \ker f$; es suficiente aplicar la caracterización (0.15)

i) Ahora, es claro que si f es inyectiva $\ker f$ sólo puede contener al neutro. Recíprocamente,

$$f(x) = f(y) \Longrightarrow f(xy^{-1}) = f(x)f(y)^{-1} = 1_H \Longrightarrow xy^{-1} \in \ker f = 1_G \Longrightarrow x = y$$

ii) Definimos $\varphi\colon G/\ker f \longrightarrow \mathrm{Im}(f)$ mediante $\varphi([x]) = f(x)$ Es rutinario comprobar que se trata de un isomorfismo. Nótese que $f = j \circ \varphi \circ p$ donde p denota la proyección canónica de G sobre $G/\ker f$ y j la inclusión de $\mathrm{Im}(f)$ en H.

[5] salvo el caso trivial de que el subgrupo normal sea el neutro

[6] salvo el caso trivial de que el subgrupo sea el total

Ejemplo El núcleo de la proyección canónica p de G en su cociente G/N es N, pues

$$xN = N \iff xN = 1_G N \iff x \sim 1_G \iff x \in N$$

Observación 0.24 Notemos pues que el concepto de subgrupo normal está asimismo estrechamente ligado al de homomorfismo toda vez que hemos probado ya el siguiente

Corolario 0.25 *$N \lhd G$ si y sólo si es el núcleo de algún homomorfismo.*

Corolario 0.26 (Segundo teorema de isomorfía) *Sean $N, S \leq G$, N normal. Entonces, $N \cap S$ es un subgrupo normal de S y*

$$S/(S \cap N) \cong NS/N$$

Demostración: Definimos la correspondencia $s \longrightarrow sN$, la clase de s en el grupo cociente NS/N. Es fácil probar que se trata de un homomorfismo de grupos; ahora $(ns)s^{-1} \in N \Longrightarrow (ns)N = sN$ y la antiimagen de $(ns)N$ es s. Por tanto, se trata de un epimorfismo.

Basta observar que su núcleo es precisamente $S \cap N$ y aplicar el primer teorema de isomorfía.

Corolario 0.27 (Teorema de la correspondencia inversa) *Sea $N \lhd G$.*

i) *Existe una biyección entre el conjunto de subgrupos S de G conteniendo N y el conjunto de subgrupos de G/N.*
ii) $[G : S] = [G/N : S/N]$
iii) $S \lhd G \iff S/N \lhd G/N$ *y* $(G/N)/(S/N) \cong G/S$

Demostración:

i) Si $N \leq S \leq G$, hemos comentado ya que $N \lhd S$ y cada clase sN del grupo cociente S/N es un elemento de G/N; por tanto, $S/N \leq G/N$. Veamos que la asignación $S \longrightarrow S/N$ es una biyección.

Inyectiva:

Supongamos $N \leq S, T \leq G$ con $S/N = T/N$. Entonces,

$$\begin{aligned} s \in S \quad &\Longrightarrow \quad sN \in S/N = T/N \Longrightarrow sN = tN \Longrightarrow t^{-1}s \in N \leq T \\ &\Longrightarrow \quad s \in T \end{aligned}$$

Por tanto, $S \subseteq T$. Intercambiando sus papeles, $T \subseteq S$ y $S = T$.

Sobre:

Sea $\mathcal{H} \leq G/N$ y $S = \{s \in G \mid sN \in \mathcal{H}\}$. Entonces,

$$nN = N = 1_{G/N} = 1_{\mathcal{H}} \in \mathcal{H} \Longrightarrow n \in S \Longrightarrow N \subseteq S$$

Por otro lado,

$$\begin{aligned} s_1, s_2 \in S \quad &\Longrightarrow \quad s_1N, s_2N \in \mathcal{H} \Longrightarrow (s_1N)(s_2N)^{-1} \in \mathcal{H} \Longrightarrow \\ &\overset{0.11}{\Longrightarrow} \quad (s_1N)(s_2^{-1}N) \in \mathcal{H} \Longrightarrow s_1s_2^{-1}N \in \mathcal{H} \Longrightarrow \\ &\Longrightarrow \quad s_1s_2^{-1} \in S \end{aligned}$$

Así, $N \leq S \leq G$; basta ver que $S/N = \mathcal{H}$, pero esto es consecuencia de la propia construcción de S.

iii) La correspondencia $xN \longrightarrow xS$ es un epimorfismo de G/N en G/S cuyo núcleo es

$$\{xN \in G/N \mid xS = S\} = \{xN \in G/N \mid x \in S\} = S/N$$

ii) Puede omitir el lector su demostración en una primera lectura, pues su máximo interés es en el caso de ser S normal y, entonces, el resultado se deduce del isomorfismo en el apartado iii).

Para el caso general basta probar que la asignación

$$\{xS \mid x \in G\} \longrightarrow \{(xN)(S/N) \mid xN \in G/N\}$$

es biyectiva, lo que se obtiene de reiterar los argumentos anteriores:

$$xS = yS \Longrightarrow \cdots \Longrightarrow (xN)(S/N) = (yN)(S/N)$$

$$(xN)(S/N) = (yN)(S/N) \Longrightarrow \cdots \Longrightarrow xy^{-1} \in S \Longrightarrow xS = yS$$

El siguiente esquema-ejemplo puede arrojar algo de luz sobre lo que quiere decir el enunciado.

Sea $G = \mathbf{Z}/12\mathbf{Z}$ el grupo aditivo de los enteros módulo 12, y consideremos lo subgrupos

$$N = \{\overline{0}, \overline{6}\} \quad S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$$

Entonces,

G/S

$\overline{0}$	$\overline{6}$
$\overline{2}$	$\overline{8}$
$\overline{4}$	$\overline{10}$
$\overline{1}$	$\overline{7}$
$\overline{3}$	$\overline{9}$
$\overline{5}$	$\overline{11}$

G/N

$\overline{0}$	$\overline{6}$
$\overline{2}$	$\overline{8}$
$\overline{4}$	$\overline{10}$
$\overline{1}$	$\overline{7}$
$\overline{3}$	$\overline{9}$
$\overline{5}$	$\overline{11}$

S/N

$\overline{0}$	$\overline{6}$
$\overline{2}$	$\overline{8}$
$\overline{4}$	$\overline{10}$

$\overline{G}/\overline{S}$

$\overline{0}$	$\overline{6}$
$\overline{2}$	$\overline{8}$
$\overline{4}$	$\overline{10}$
$\overline{1}$	$\overline{7}$
$\overline{3}$	$\overline{9}$
$\overline{5}$	$\overline{11}$