Subgrupos

Sésar

1. Definición

Definition 1. Sea $(G, *)$ un grupo. Decimos que $\varnothing \neq H \subseteq G$ es un **subgrupo** de G si $(H, *)$ es un grupo.

$$H \leq G$$

Remark 1. Supongamos que $H \leq G$. Entonces por ser $e \in G$ el elemento neutro del grupo G, tenemos que para todo $h \in H \subseteq G$, $h * e = e * H = h$. Por tanto, el elemento neutro de H es también e. Por otro lado, Si $h \in H$, en particular, existe un $k \in H$ tal que $k * h = h * k = e$ y como $h, k \in H \subseteq G$, entonces se deduce que $k = h^{-1}$. Es decir, la inversa de todo elemento H es la inversa en G y está contenido en H.

Proposition 1. Sean $(G, *)$ grupo y $H \subseteq G$. Entonces $H \leq G$ si y solo si

1. $h_1 * h_2 \in H$ para todo $h_1, h_2 \in H$.
2. $e \in H$.
3. Para todo $h \in H$, $h^{-1} \in H$.

Demostración. Supongamos primero que $H \leq G$. Entonces por definición, como $(H, *)$ es un grupo, en particular $*$ es una operación binaria en H, luego $*$ es cerrado en H. Por otro lado, Por la observación anterior, $e \in H$ y para todo $h \in H$, $h^{-1} \in H$.

Supongamos ahora que en H se cumplen las tres propiedades. En primer lugar, como $e \in H$, entonces $H \neq \varnothing$. Por otro lado, por la primera propiedad, podemos concluir que $*$ es una operación binaria en H. Basta con comprobar los axiomas de un grupo. La operación, al ser asociativa para todo G, en particular, lo es para todo elemento de H. Por otro lado, el elemento neutro de H es el elemento neutro de G y por la segunda propiedad, $e \in H$. Finalmente, La tercera propiedad nos dice que siempre existe el inverso de cualquier elemento, luego $h \in H$. $\square$

Remark 2. Bajo los supuestos de la primera y tercera condición, la segunda condición —$e \in H$— es equivalente a decir que $H \neq \varnothing$. Si el elemento neutro está contenido en H, entonces en particular H no es vacío. Por otro lado, si $H \neq \varnothing$, entonces existe un $h \in H$. Por la tercera propiedad, $h^{-1} \in H$ y como suponemos que la operación es cerrada, entonces $e = h * h^{-1} \in H$.

Corollary 1. $H \leq G$ si y solo si $e \in H$ y $h_1 * h_2^{-1} \in H$ para todo $h_1, h_2 \in H$.

Demostración. Si $H \leq G$, en particular para todo $h_1, h_2 \in H$, tenemos que $h_2^{-1} \in H$, y por ser la operación cerrada en G, $h_1 * h_2^{-1} \ni H$. Contrariamente, tomando $h_1 = e$ y $h_2 = h$, entonces $h_1 * h_2^{-1} = h^{-1} \in H$. De esta manera, como $h_1, h_2 \in H$, entonces $h_2^{-1} \in H$ y por tanto, $h_1 * h_2 = h_1 * (h_2^{-1})^{-1} \in H$. □

Corollary 2. Sea $H \subseteq G$ y H finito. Entonces $H \leq G$ si y solo si $h_1 * h_2 \in H$ para todo $h_1, h_2 \in H$.

Demostración. La primera implicación es directa. Por otro lado, como la operación es cerrada en H, en particular $h^n \in H$ para todo $n \geq 1$. Como H es finito, entonces por el principio del palomar, existe al menos un $n_0 \leq |H|$ tal que $h^{n_0} = e$, por lo que $e \in H$. Finalmente, $h^{n_0} = h^{n_0 - 1} * h = h * h^{n_0 - 1} = e$, luego $h^{-1} = h^{n_0 - 1} \in H$. □

Definition 2. Sea G grupo. Definimos el **centro** de G como

$$Z(G) := \{g \in G \mid g * x = x * g, \ \forall x \in G\}.$$

Proposition 2. $Z(G) \leq G$.

Demostración. En primer lugar, como $e * x = x * e = x$ para todo $x \in G$, entonces $e \in Z(G)$. Por otro lado, si $g_1, g_2 \in Z(G)$, tenemos que $(g_1 * g_2^{-1}) * x = g_1 * (g_2^{-1} * x) = g_1 * (x^{-1} * g_2)^{-1} = g_1 * (g_2 * x^{-1})^{-1} = g_1 * (x * g_2^{-1}) = (g_1 * x) * g_2 = x * (g_1 * g_2)$. Por lo tanto, $g_1 * g_2^{-1} \in Z(G)$. □

Corollary 3. G es abeliano si y solo si $Z(G) = G$.

Demostración. Si G es abeliano, entonces para todo $g \in G$, tenemos que $g * x = x * g$ para todo $x \in G$, por lo que $g \in Z(G)$, por lo que tenemos que $G \leq Z(G)$ y por tanto $G = Z(G)$.

Por otro lado, si $Z(G) = G$, entonces para todo $g \in G$, entonces $g \in Z(G)$, luego g conmuta con todo elemento $x \in G$ y por tanto G es abeliano. □

Definition 3. Sea G grupo. Definimos el **centralizador** de un subconjunto $S \subseteq G$ como

$$C_G(S) := \{g \in G \mid g * x = x * g, \ \forall x \in S\}.$$

Proposition 3. $C_G(S) \leq G$.

Demostración. En primer lugar, como $e * x = x * e = x$ para todo $x \in S$, entonces $e \in C_G(S)$. Por otro lado, si $g_1, g_2 \in C_G(S)$, tenemos que para todo $x \in S$, $(g_1 * g_2^{-1}) * x = g_1 * (g_2^{-1} * x) = g_1 * (x^{-1} * g_2)^{-1} = g_1 * (g_2 * x^{-1})^{-1} = g_1 * (x * g_2^{-1}) = (g_1 * x) * g_2 = x * (g_1 * g_2)$. Por lo tanto, $g_1 * g_2^{-1} \in C_G(S)$. □

Remark 3. Si $S = \{a\}$, entonces denotamos el centralizador de S como $C_G(a) = \{g \in G \mid g * a = a * g\}$.

Lemma 1. $C_G(S) = \bigcap_{a \in S} C_G(a)$.

Demostración. $g \in C_G(S)$ si y solo si $g * a = a * g$ para todo $a \in S$, es decir, $g \in C_G(a)$ para todo $a \in S$, o lo que es lo mismo, $g \in \bigcap_{a \in S} C_G(a)$. □

Remark 4. Notemos que $Z(G) = C_G(G)$.

Corollary 4. $Z(G) = \bigcap_{g \in G} C_G(g)$.

Demostración. Basta con observar que $Z(G) = C_G(G) = \bigcap_{g \in G} C_G(g)$. □

2. Subgrupo generado

Lemma 2. La intersección arbitraria de subgrupos es un subgrupo.

Demostración. Supongamos que $\{H_i\}_{i \in I}$ es una familia de subgrupos del grupo $(G, *)$. En particular, como $e \in H_i$ para todo $i \in I$, entonces $e \in \bigcap_{i \in I} H_i$. Por otro lado, sean $h_1, h_2 \bigcap_{i \in I} H_i$. Entonces $h_1, h_2 \in H_i$ para todo $i \in H$, y por el corolario, $h_1 * h_2^{-1} \in H_i$ para todo $i \in H$, es decir, $h_1 * h_2^{-1} \in \bigcap_{i \in I} H_i$. Por tanto, estamos en las condiciones del corolario, por lo que $\bigcap_{i \in I} H_i \leq G$. □

Definition 4. Sea $(G, *)$ grupo y $S \subseteq G$. Definimos el **subgrupo generado** por S como

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H.$$

Utilizando un lenguaje más cercano, el subgrupo generado por un subconjunto S es la intersección de todos lo subgrupos $H \leq G$ tales que contienen a S.

Remark 5. Si $S = \{a_1, \ldots, a_n\}$ es finito, solemos denotar el subgrupo generado por S como $\langle a_1, \ldots, a_n \rangle$.

Proposition 4. Sea $S \subseteq G$.

1. $S \subseteq \langle S \rangle$.
2. $\langle S \rangle \leq G$.
3. $\langle S \rangle$ es el subgrupo de G más pequeño que contiene a S.

Demostración. En primer lugar, dado que nos fijamos en los subgrupos $H \leq G$ tales que $S \subseteq H$. En particular, la intersección de todos ellos también contiene a S, por lo que $S = \bigcap_{S \subseteq H \leq G} H = \langle S \rangle$. Además, Por el Lema anterior, la intersección de subgrupos es un subgrupo, luego $\langle S \rangle \leq G$.

Finalmente, para probar que es el menor subgrupo con estas características, basta probar que si existe un $K \leq G$ tal que $S \subseteq K$, entonces $\langle S \rangle \leq K$. Pero esto es fácil de ver porque como $S \subseteq K \leq G$, entonces en particular, la intersección de todos ellos estará contenido en K. □

Corollary 5. Si $H \leq G$, entonces $\langle H \rangle = H$.

Demostración. Por un lado, tenemos que $H \leq \langle H \rangle$. Por otro lado, H es el subgrupo que contiene a H, por lo que $\langle H \rangle \leq H$. □

Proposition 5. Si $S \subseteq T \subseteq G$, entonces $\langle S \rangle \leq \langle T \rangle$.

Demostración. Notemos que si $T \subseteq H \leq G$, entonces $S \subseteq H \leq G$. Por lo tanto, el conjunto de subgrupos de cumplan con la segunda condición contiene a los subgrupos de cumplan con la primera y por tanto, $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H \leq \bigcap_{T \subseteq H \leq G} H = \langle T \rangle$. □

Theorem 1. Sea $\varnothing \neq S \subseteq G$. Entonces

$$\langle S \rangle = \{s_1^{n_1} * \ldots * s_k^{n_k} \mid s_i \in S,\ n_i \in \mathbb{Z}\}$$

Demostración. En primer lugar, fijémonos que si $s_1, \ldots, s_n \in S \subseteq \langle S \rangle$, entonces por ser $\langle S \rangle \leq G$, tenemos que $s_1^{n_1} * \ldots * s_k^{n_k} \in \langle S \rangle$, por lo que $\{s_1^{n_1} * \ldots * s_k^{n_k}\} \subseteq \langle S \rangle$. Por otro lado, fijémenos que este conjunto $\{s_1^{n_1} * \ldots * s_k^{n_k} \mid s_i \in S,\ n_i \in \mathbb{Z}\}$ es un subgrupo. Esto es porque como S no es vacío y los productos de elementos de S están contenidos en el grupo, luego la operación es cerrada en S. Por tanto, es un subgrupo que contiene a S y por definición del subgrupo generado, $\langle S \rangle \leq \{s_1^{n_1} * \ldots * s_k^{n_k} \mid s_i \in S,\ n_i \in \mathbb{Z}\}$. □

Remark 6. Notemos que por definición, si $S = \varnothing$, entonces el grupo trivial es el subgrupo más pequeño que contiene al conjunto vacío, por lo que $\langle \varnothing \rangle = \{e\}$.

3. Teorema de Lagrange

Lemma 3. Sea G grupo y $H \leq G$. Definamos las siguientes relaciones binarias:

$$x \mathcal{L}_H y \Leftrightarrow x^{-1} y \in H \quad x \mathcal{R}_H \Leftrightarrow x y^{-1} \in H.$$

Entonces ambos $\mathcal{L}_H$ y $\mathcal{R}_H$ son RBE.

Demostración. La pueba para ambos casos son análogos, luego sólo mostraremos para el caso de la relación $\mathcal{L}_H$. En primer lugar, notemos que para todo $x \in G$, $e = x^{-1}x \in H$, luego $x\mathcal{L}_H x$, luego la relación es reflexiva. Por otro lado, si $x\mathcal{L}_H x$, entonces $x^{-1}y \in H$ y como H es un subgrupo. $(x^{-1}y)^{-1} = y^{-1}x \in H$, luego $y\mathcal{L}_H x$ y la relación es simétrica. Finalmente, supongamos que $x\mathcal{L}_H y$ e $y\mathcal{L}_H z$. Entonces $x^{-1}y, y^{-1}z \in H$ y como H es cerrado para la operación, $x^{-1}yy^{-1}z = x^{-1}z \in H$, por lo que $x\mathcal{L}_H z$, probando de esta manera que es transitiva. □

Definition 5. Sea G grupo y $H \leq G$. Una **clase lateral** por la (izquierda / derecha) es una clase de equivalencia de ($\mathcal{L}_H$ / $\mathcal{R}_H$).

Proposition 6. Sea G grupo y $H \leq G$. Entonces para todo $g \in G$.

$$[g]_{\mathcal{L}} = gH := \{gh \mid h \in H\}, \quad [g]_{\mathcal{R}} = Hg := \{hg \mid h \in H\}.$$

Demostración. Al igual que en la demostración del lema anterior, sólo mostraremos el caso para la clase lateral por la izquierda. Sea $g \in G$. Entonces $x \in [g]_{\mathcal{L}}$ si y solo si $g\mathcal{L}_H x$, es decir, $g^{-1}x \in H$. Esto es equivalente a decir que existe un $h \in H$ tal que $g^{-1}x = h \Leftrightarrow x = gh \in gH$. □

Proposition 7. Sea G grupo y $H \leq G$.
1. $|gH| = |Hg| = |H|$ para todo $g \in G$.
2. $|G/\mathcal{L}_H| = |G/\mathcal{R}_H|$.

Demostración. Veamos en primer lugar que toda clase lateral tiene la misma cardinalidad que el subgrupo dado. Dado un $g \in G$ arbitrario, definamos la siguiente aplicación:

$$\begin{aligned} f : H &\to gH \\ h &\mapsto gh. \end{aligned}$$

Basta comprobar que f es biyectiva. En primer lugar, es fácil comprobar que es sobreyectiva, pues si $x \in gH$, entonces $x = gh$ para un cierto $h \in H$, luego $f(h) = gh = x$. Por otro lado, Supongamos que $f(h_1) = f(h_2)$. Entonces $gh_1 = gh_2$ y por la propiedad cancelativa, $h_1 = h_2$, luego f es inyectiva.

Por otro lado, podemos tomar la aplicación $H \to Hg$ tal que $h \mapsto gh$ y demostrar de manera completamente análoga que es una aplicación biyectiva.

Por último, veamos que los conjuntos cocientes tienen la misma cardinalidad. Tomemos la siguiente aplicación:

$$\begin{aligned} \phi : G/\mathcal{L}_H &\to G/\mathcal{R}_H \\ gH &\mapsto Hg^{-1}. \end{aligned}$$

En primer lugar, es claramente sobreyectiva, pues si $x \in G/\mathcal{R}_H$, entonces $x = Hg^{-1}$ para un cierto $g \in G$, luego $\phi(gH) = Hg^{-1} = x$. Ahora, supongamos que $\phi(g_1H) = \phi(g_2H)$. Entonces $Hg_1^{-1} = Hg_2^{-1}$, es decir, $g_1^{-1}\mathcal{R}_H g_2^{-1}$. Por lo tanto, $g_1^{-1}(g_2^{-1})^{-1} = g_1^{-1}g_2 \in H$, esto es, $g_1\mathcal{L}_H g_2$, luego $g_1H = g_2H$. Esto demuestra que ϕ es inyectiva y, por tanto, biyectiva. □

Definition 6. Sea G grupo. Definimos el **índice** de $H \leq G$ como

$$[G : H] := |G/\mathcal{L}_H|.$$

Theorem 2 (Lagrange)**.** Sea G un grupo finito y $H \leq G$. Entonces

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

En particular, $|H|$ divide a $|G|$.

Demostración. Como G es finito, en particular H y $[G : H]$ son finitos. Como $G/\mathcal{L}_H$ consituye una partición de G, en particular podemos escribir $G = H \sqcup g_1 H \sqcup \ldots \sqcup g_n H$, donde $n = [G : H]$. Por lo tanto, $|G| = \sum_{i=1}^{[G:H]} |g_i H| = \sum_{i=1}^{[G:H]} |H| = |H| \sum_{i=1}^{[G:H]} 1 = |H|[G : H]$. □

Corollary 6. Si $K \leq H \leq G$ con G grupo finito, entonces

$$[G : K] = [G : H][H : K].$$

Demostración. Por un lado, como $K \leq G$, entonces por el Teoerma de Lagrange, $|G| = [G : K]|K|$. Por otro lado, $H \leq G$ y aplicando de nuevo el teorema, $|G| = [G : H]|H|$, pero a su vez $K \leq H$, luego $|H| = [H : K]|K|$, luego combinando las dos ecuaciones anteriores obtenemos que $|G| = [G : H][H : K]|K|$ y comparándola con la primera ecuaión se llega al resultado deseado. □

4. Subgrupos normales

Definition 7. Sea $N \leq G$. Decimos que N es un **subgrupo normal** $N \trianglelefteq G$ si para todo $n \in N$ y para todo $g \in G$, tenemos que $gng^{-1} \in N$.

Example 1. En todo grupo G, existen al menos dos subgrupos normales: $\{e\} \trianglelefteq G$ y $G \trianglelefteq G$.

Remark 7. Si definimos el conjunto $gNg^{-1} := \{gng^{-1} \mid n \in N\}$, entonces por definición de subgrupo normal, $N \trianglelefteq G$ implica que $gNg^{-1} \subseteq N$ para todo $g \in G$.

Proposition 8. Sea G grupo y $N \leq G$. Son equivalentes.

1. $N \trianglelefteq G$.
2. $gN = Ng$ para todo $g \in G$.
3. $gNg^{-1} = N$ para todo $g \in G$.

Demostración. En primer lugar, supongamos que N es un subgrupo normal y sea $g \in G$. Entonces para todo $n \in N$, tenemos que $gng^{-1} \in N$, luego existe un $n' \in N$ tal que $gng^{-1} = n' \Rightarrow gn =$

$n'g \in Ng$. Esto demuestra que $gN \subseteq Ng$. Como es cierto para todo $g \in G$, en particular $g^{-1}N \subseteq Ng^{-1} \Rightarrow Ng \subseteq gN$.

Por otro lado, supongamos ahora que las clases laterales coinciden. Entonces para todo $n \in N$, existe un $n' \in N$ tal que $gn = n'g \Rightarrow gng^{-1} = n' \in N$, luego $gNg^{-1} \subseteq N$. Como esto es cierto para todo $g \in G$, en particular, $g^{-1}Ng^{-1} \subseteq N \Rightarrow N \subseteq gNg^{-1}$.

Finalmente, tenemos que en particular se cumple que $gNg^{-1} \subseteq N$, luego para todo $n \in N$, $gng^{-1} \in N$, por lo que $N \trianglelefteq G$. □

Remark 8. En vista de la demostración anterior, para comprobar la normalidad de un subgrupo basta con probar que para todo $g \in G$ alguna de estas condiciones más débiles se cumple: $gN \subseteq Ng$ o equivalentemente $gNg^{-1} \subseteq N$.

Corollary 7. Sea $N \leq G$. Si $[G : N] = 2$, entonces $N \trianglelefteq G$.

Demostración. Si el índice de N es dos, en particular $G/\mathcal{L}_N = \{N, xN\}$ y $G/\mathcal{R}_N = \{N, Nx\}$ para un cierto $x \notin N$. Tomemos $g \in G$. Si $g \in N$, en particular $gN = N = Ng$ porque $g\mathcal{L}_N e$ y también $g\mathcal{R}_N e$. Si $g \notin N$, entonces $gN \neq N$, luego $gN = xN$ y de la misma manera $Ng = Nx$. Ahora bien, como las clases laterales forman una partición en G, tenemos que $G = N \sqcup gN = N \sqcup Ng$ y por lo tanto, $gN = Ng$. De esta manera, hemos probado que para todo $g \in N$, $gN = Ng$ y por la proposición, $N \trianglelefteq G$. □

Proposition 9. Si G es abeliano, entonces todo subgrupo es normal

Demostración. Sea $H \leq G$, $h \in H$ y $g \in G$. Entonces $ghg^{-1} = gg^{-1}h = h \in H$, luego $H \trianglelefteq G$. □

Proposition 10. Sean $H, N \leq G$. Si $N \trianglelefteq G$, entonces $N \cap H \trianglelefteq H$.

Demostración. Sea $x \in N \cap H$ y $h \in H$. En particular, $x \in N$ y $h \in G$ y como $N \trianglelefteq G$, entonces $hxh^{-1} \in N$. Pero como $x \in H$ también, entonces $hxh^{-1} \in H$, luego $hxh^{-1} \in N \cap H$. □

Corollary 8. Sean $N \leq H \leq G$. Si $N \trianglelefteq G \Rightarrow N \trianglelefteq H$.

Demostración. Por proposición, $N = N \cap H \trianglelefteq H$. □

Remark 9. De manera general, $N \trianglelefteq K \trianglelefteq G \not\Rightarrow N \trianglelefteq G$.

Definition 8. Un grupo es **simple** si sus únicos subgrupos normales son el trivial o el mismo grupo.

5. Producto de subgrupos

Definition 9. Sean $H, K \leq G$. Definimos el **producto de subgrupos** H y K como

$$H * K := \{h * k \mid h \in H,\ k \in K\}.$$

Proposition 11. Sean $H, K \leq G$.

$$H * K \leq G \Leftrightarrow H * K = K * H.$$

Bajo estas condiciones, $H * K = \langle H \cup K \rangle$.

Demostración. En primer lugar, supongamos que $H * K$ es un subgupo de G. Sean $h \in H$ y $k \in K$. Entonces como $H * K \leq G$, $(hk)(hk) \in H * K$, luego existen $h' \in H$ y $k' \in K$ tales que $hkhk = h'k'$. Por lo tanto, $kh = h^{-1}h'k'k^{-1} \in H * K$. Como esto es cierto para todo $h \in H$ y todo $k \in K$, entonces $K * H \subseteq H * K$. De manera análoga, llegamos a la conclusión de que $H * K \subseteq K * H$.

Supongamos ahora que $H * K = K * H$. Notemos que $e \in H * K$. Por otro lado, sean $h_1k_1, h_2k_2 \in H * K$. Entonces como $k_1h_2 \in K * H = H * K$, existen $h' \in H$ y $k' \in K$ tales que $k_1h_2 = h'k'$. Por lo que $h_1k_1h_2k_2 = h_1h'k'k_2 \in H * K$. Finalmente, si $hk \in H * K$. Entonces $(hk)^{-1} = k^{-1}h^{-1} \in K * H = H * K$.

Finalmente, es fácil comprobar que $H * K \subseteq \langle H \cup K \rangle$. por otro lado, como se cumple que $H \cup K \subseteq H * K$, tenemos que $\langle H \cup K \rangle \subseteq \langle H * K \rangle = H * K$. □

Remark 10. Aunque $H * K = K * N$, en general $hk \neq kh$.

Fijémonos además que como $H, K \subseteq H * K$, en las condiciones del teorema anterior tenemos el siguiente retículo de subgrupos: $\{e\} \leq H \cap K \leq H, K \leq H * K = K * H \leq G$.

Proposition 12. Sea $H \leq G$ y $N \trianglelefteq G$. Entonces

$$N \trianglelefteq H * N \leq G$$

Demostración. En primer lugar, supongamos que $hn \in H * N$. Entonces $hn = hnh^{-1}h$ y como $hnh^{-1} \in N$, entonces $hn \in N * H$. De la misma manera, si $nh \in N * H$, entonces $nh = hh^{-1}nh$ y como $h^{-1}nh \in N$, tenemos que $nh \in H * N$. Esto demuestra que $H * N = N * H$ y por proposición, $H * N \leq G$.

Finalmente, como $N \trianglelefteq G$ y $N \leq H * N \leq G$, tenemos que $N \trianglelefteq H * N$. □

Corollary 9. Si $N, K \trianglelefteq G$, entonces $N * K \trianglelefteq G$.

Demostración. Sean $nk \in N * K$ y $g \in G$. Entonces $gnkg^{-1} = (gng^{-1})(gkg^{-1})$. Como N y K son subgrupos normales de G, entonces $gng^{-1} \in N$ y $gkg^{-1} \in K$, por lo que $gnkg^{-1} \in N * K$. □