LISTA DE EJERCICIOS - ÁLGEBRA

GEM - 2021

Caleb - Michaell

Pregunta 1. Sea G un grupo abeliano, pruebe que el conjunto

$$T(G) = \{g \in G : |g| < \infty\}$$

es un subgrupo de G denominado el **subgrupo de torsión**. De un ejemplo donde $T(G)$ no sea subgrupo. Halle $T(\mathbb{Z} \times \mathbb{Z}_n)$.

Solución. Veamos:

- $T(G)$ **es un subgrupo.** En efecto, como $|1| = 1$ se tiene que $1 \in T(G)$ así es no vacío. Sean $a, b \in T(G)$ entonces $|a| = n < \infty$ y $|b| = m < \infty$. Luego:
  - $(ab)^{mn} = (a^n)^m (b^m)^n = 1$ y con esto $|ab| < \infty$ es decir $ab \in T(G)$.
  - $(a^{-1})^n = (a^n)^{-1} = 1$ y con esto $|a^{-1}| < \infty$ es decir $a^{-1} \in T(G)$.
- **Si** G **no es abeliano.** Consideremos por ejemplo $G = \mathrm{GL}_2(\mathbb{R})$ el cual no es abeliano. Las matrices:

  $$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

  cumplen que $A^2 = B^2 = I$ osea $A, B \in T(G)$. Sin embargo $|AB| = \infty$ por lo que $AB \notin T(G)$.
- **Grupo de torsión de** $\mathbb{Z} \times \mathbb{Z}_n$**.** Afirmamos que $T(\mathbb{Z} \times \mathbb{Z}_n) = \langle (0, \overline{1}) \rangle$. En efecto, sea $(m, \overline{r}) \in \mathbb{Z} \times \mathbb{Z}_n$ entonces tiene orden $k < \infty$. Si $k = 0$ entonces es evidente, supongamos que $k \neq 0$. Luego:

  $$k(m, \overline{r}) = (km, \overline{kr}) = (0, \overline{0}) \implies m = 0$$

  Así $(m, \overline{r}) = (0, \overline{r}) = r(0, \overline{1}) \in \langle (0, \overline{1}) \rangle$. Recíprocamente, sea $r(0, \overline{1}) \in \langle (0, \overline{1}) \rangle$ entonces $n(0, \overline{r}) = (0, \overline{nr}) = (0, \overline{0})$ por lo que tiene orden finito y así está en $T(\mathbb{Z} \times \mathbb{Z}_n)$.

Pregunta 2. Un grupo abeliano no trivial se denomina **divisible** si para todo $a \in G$ y k un entero no nulo existe $x \in G$ tal que $x^k = a$.

a) $(\mathbb{Q}, +)$ es divisible.

b) Si G es finito, no es divisible.

c) Sean A, B grupos abelianos, pruebe que $A \times B$ es divisible si y solo si A y B son divisibles.

Solución.

a) Sea $a/b \in \mathbb{Q}$ y $k \neq 0$. Entonces:

$$\frac{a}{b} = k\left(\frac{a}{bk}\right)$$

Como $a/bk \in \mathbb{Q}$ se tiene que es un grupo divisible.

b) Supongamos que $G = \{g_1, \ldots, g_n\}$ es un grupo divisible de orden $n > 1$.

Todo elemento g_i de G tiene orden finito k_i, basta considerar el grupo generado por este elemento y ver que este tiene orden finito. Sean $k = k_1 \cdots k_n \neq 0$ y $g \neq 1$ en G, como G es divisible, existe $x \in G$ tal que:

$$1 = x^k = g \neq 1$$

Algo imposible, así si G es finito no puede ser divisible.

c) Supongamos primero que $A \times B$ es divisible. Sea $a \in A$ y $k \neq 0$, luego para cualquier $b \in B$ se tiene que $(a, b) \in A \times B$ y así existe $(x, y) \in A \times B$ tal que $(x, y)^k = (x^k, y^k) = (a, b)$. Esto implica que $x^k = a$ probando que A es divisible. Análogamente se procede para el caso de B.

Recíprocamente, sea $(a, b) \in A \times B$ y $k \neq 0$, como A y B son divisibles, existen $x \in A$ e $y \in B$ tales que $x^k = a$ e $y^k = b$. Luego $(x, y)^k = (x^k, y^k) = (a, b)$, esto prueba que $A \times B$ es divisible.

Pregunta 3. Sea G un grupo abeliano de orden pq con $(p, q) = 1$. Pruebe que si existen $a, b \in G$ tales que $|a| = p$ y $|b| = q$ entonces G es cíclico.

Solución. Se tiene que $(ab)^{pq} = (a^p)^q(b^q)^p = 1$ por lo que $|ab| \mid pq$. Como se tiene:

$$(ab)^{q|ab|} = 1 = (ab)^{p|ab|}$$

entonces $q \mid p|ab|$ y $p \mid q|ab|$. Como $(p, q) = 1$ se sigue que $q \mid |ab|$ y $p \mid |ab|$. Esto implica que $pq \mid |ab|$ y así $pq = |ab|$. Finalmente $\langle ab \rangle$ es un subgrupo y además tiene orden pq, se sigue que $G = \langle ab \rangle$.

Daniel - Cristopher

Pregunta 1. Pruebe los siguientes items:

a) Para $a, b \in \mathbb{R}$ definimos $\tau_{ab}(x) = ax + b$ para todo $x \in \mathbb{R}$. Pruebe que el conjunto

$$G = \{\tau_{ab} : a \neq 0\}$$

es un grupo con la composición de funciones.

b) Pruebe que el subconjunto $H = \{\tau_{ab} \in G : a \in \mathbb{Q}\}$ es un subgrupo de G.

Solución.

a) Veamos que la aplicación es cerrada, sean $\tau_{ab}, \tau_{cd} \in G$. Entonces:

$$\tau_{ab}\tau_{cd}(x) = \tau_{ab}(cx + d) = (ac)x + (ad + b) = \tau_{ac,ad+b}(x)$$

Así $\tau_{ab}\tau_{cd} = \tau_{ac,ad+b} \in G$. La composición es asociativa, el elemento neutro es τ_{10} pues $\tau_{ab}\tau_{10} = \tau_{ab}$ y el elemento inverso de τ_{ab} es $\tau_{\frac{1}{a},-\frac{b}{a}}$.

b) Claramente $\tau_{10} \in H$ por lo que es no vacío. Dados $\tau_{q_1b_1}, \tau_{q_2b_2} \in H$ se tiene:

$$\tau_{q_1b_1}\tau_{q_2b_2} = \tau_{q_1q_2,q_1b_2+b_1}$$

Como q_1 y q_2 son números racionales, entonces q_1q_2 también es racional y así $\tau_{q_1b_1}\tau_{q_2b_2} \in H$. También:

$$\tau^{-1}_{q_1b_1} = \tau_{\frac{1}{q_1},-\frac{b_1}{q_1}}$$

Como q_1 es racional entonces q_1^{-1} también es racional y así $\tau^{-1}_{q_1b_1} \in H$.

Pregunta 2. Sea G un grupo, definimos el **centro** de G como el conjunto:

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

a) Pruebe que $Z(G) \leq G$.

b) Sea $H \leq G$ un subgrupo abeliano, pruebe que $\langle H \cup Z(G)\rangle$ es abeliano.

Solución.

a)
- Claramente $1 \in Z(G)$ pues $1x = x1$ para todo $x \in G$, así $Z(G) \neq \emptyset$.
- Sea $a \in Z(G)$ y $x \in G$ arbitrario, entonces:

$$xa^{-1} = (ax^{-1})^{-1} = (x^{-1}a)^{-1} = a^{-1}x$$

Con esto $a^{-1} \in Z(G)$.
- Sean $a, b \in Z(G)$ y $x \in G$ arbitrario, entonces:

$$x(ab) = (xa)b = (ax)b = a(xb) = a(bx) = (ab)x$$

Con esto $ab \in Z(G)$.

b) Primero veamos que todo elemento de $\langle H \cup Z(G)\rangle$ es de la forma $x = ab$ con $a \in H$ y $b \in Z(G)$. Sea $x \in \langle H \cup Z(G)\rangle$ entonces x tiene la forma:

$$x = z_1^{\epsilon_1} \dots z_r^{\epsilon_r}$$

donde $\epsilon_i \in \{-1, 1\}$ y $z_i \in H \cup Z(G)$. Procederemos por inducción sobre r el número de factores.

- Si $r = 1$ es evidente, pues $x = z$ y dependiendo si $z \in H$ o $z \in Z(G)$ (o en ambos) podemos expresar $x = 1z = z1$.
- Suponemos válido para r y sea $x = z_1^{\epsilon_1} \dots z_{r+1}^{\epsilon_{r+1}}$. Por hipótesis inductiva tenemos que $z_1^{\epsilon_1} \dots z_r^{\epsilon_r} = ab$ con $a \in H$ y $b \in Z(G)$. Así:

  $$x = (ab)z_{r+1}^{\epsilon_{r+1}}$$

  Si $z_{r+1} \in Z(G)$ entonces se tendría lo pedido, caso contrario $z_{r+1} \in H$ por lo que conmutando tenemos que $x = (az_{r+1}^{\epsilon_{r+1}})b$ y tendríamos lo pedido también. (Note que no hemos usado que H es abeliano, esto se cumple para cualquier subgrupo H).

Ahora, sean $x, y \in \langle H \cup Z(G)\rangle$ por lo anterior podemos escribir $x = a_1b_1$ e $y = a_2b_2$ con $a_i \in H$ y $b_i \in Z(G)$. Luego usando que H es abeliano tenemos que:

$$xy = (a_1b_1)(a_2b_2) = a_1(a_2b_1)b_2 = (a_2a_1)(b_2b_1) = (a_2b_2)(a_1b_1) = yx$$

Pregunta 3. Si G es un grupo infinito, pruebe que es cíclico si y solo si es isomorfo a cada uno de sus subgrupos propios no triviales.

Solución.

($\Rightarrow$) Si G es cíclico infinito, sabemos que es isomorfo a $\mathbb{Z}$ (dígamos que ψ es tal isomorfismo). Los subgrupos propios de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ con $n \in \mathbb{Z} - \{1\}$, cada uno de estos es isomorfo a $\mathbb{Z}$ basta considerar $\varphi : n\mathbb{Z} \to \mathbb{Z}$ definido por:

$$\varphi(nz) = z$$

Claramente φ es biyectivo y también un homomorfismo pues:

$$\varphi(nz_1 + nz_2) = \varphi(n(z_1 + z_2)) = z_1 + z_2 = \varphi(nz_1) + \varphi(nz_2)$$

Vía el isomorfismo ψ para cualquier subgrupo H de G $psi(H)$ será un subgrupo de $\mathbb{Z}$ y por lo tanto isomorfo a Z. Tomando inversa se llega que H es isomorfo a G.

($\Leftarrow$) Para $x \neq 1$ se tiene que $\langle x\rangle$ es G o no lo es. Si lo fuera, ya tendríamos que G es cíclico, caso contrario $\langle x\rangle$ es un subgrupo propio de G. Luego por hipótesis existe $\varphi : \langle x\rangle \to G$ un isomorfismo. Para cada $g \in G$ existe $r \in \mathbb{Z}$ tal que $\varphi(x)^r = \varphi(x^r) = g$, esto prueba que $G = \langle \varphi(x)\rangle$. (No hemos usado que G es infinito).

Guido - Jhonatan

Pregunta 1. Sean $H, K \leq G$, denotaremos $H \vee K = \langle H \cup K \rangle$. Pruebe que si G es un grupo abeliano entonces:

$$H \vee K = \{ab \,|\, a \in H, b \in K\}$$

¿Qué sucede si G no es abeliano? de un ejemplo.

Solución. Procederemos por doble inclusión:

($\subseteq$) Veamos que todo elemento de $\langle H \cup K \rangle$ es de la forma $x = ab$ con $a \in H$ y $b \in K$. Sea $x \in \langle H \cup K \rangle$ entonces como G es abeliano:

$$x = z_1^{\alpha_1} \dots z_n^{\alpha_n}$$

donde $z_i \in H \cup K$ y $\alpha_i \in \mathbb{Z}$. Procederemos por inducción sobre n el número de factores.

- Si $n = 1$ es evidente, pues $x = z$ y dependiendo si $z \in H$ o $z \in K$ (o en ambos) podemos expresar $x = 1z = z1$.
- Suponemos válido para n y sea $x = z_1^{\alpha_1} \dots z_{n+1}^{\alpha_{n+1}}$. Por hipótesis inductiva tenemos que $z_1^{\alpha_1} \dots z_n^{\alpha_n} = ab$ con $a \in H$ y $b \in K$. Así:

  $$x = (ab) z_{n+1}^{\alpha_{n+1}}$$

  Si $z_{n+1} \in K$ entonces se tendría lo pedido, caso contrario $z_{n+1} \in H$ por lo que conmutando tenemos que $x = (a z_{n+1}^{\alpha_{n+1}})b$ y tendríamos lo pedido también.

($\supseteq$) Si $x = ab$ con $a \in H$ y $b \in K$, es evidente que $x \in \langle H \cup K \rangle$.

Si G no es abeliano no es cierto lo anterior, consideremos $G = \mathrm{GL}_2(\mathbb{Z}_2)$. Sean los subgrupos de las matrices triangulares.

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G : a, b, c \in \mathbb{Z}_2 \right\}$$

$$K = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G : a, b, c \in \mathbb{Z}_2 \right\}$$

La matriz:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H \vee K$$

pero no está en HK como se puede verificar fácilmente.

Pregunta 2. Resuelva los siguientes items:

a) Halle todos los subgrupos de $\mathbb{Z}_{45}$.

b) Si $x \in G$ con $|x| = |G| < \infty$ entonces $G = \langle x \rangle$.

c) Pruebe que $\mathbb{Q} \times \mathbb{Q}$ no es cíclico.

Solución.

a) Los divisores de 45 son $1, 3, 5, 9, 15$ y 45. Por lo tanto tiene 6 subgrupos:

- $\mathbb{Z}_{45} = \langle \overline{1} \rangle$ (orden 45).
- $\langle \overline{3} \rangle$ (orden 15).
- $\langle \overline{5} \rangle$ (orden 9).
- $\langle \overline{9} \rangle$ (orden 5).
- $\langle \overline{15} \rangle$ (orden 3).
- $\langle \overline{0} \rangle$ (orden 1).

b) El subgrupo $\langle x \rangle$ tiene orden $|x|$. Como G tiene la misma cantidad de elementos necesariamente deben ser iguales.

c) Supongamos que fuera cíclico entonces $\mathbb{Q} \times \mathbb{Q} = \langle (q_1, q_2) \rangle$ donde $q_1, q_2 \in \mathbb{Q}$, necesariamente q_1 y q_2 son no nulos pues si alguno lo fuera no se podría generar $\mathbb{Q} \times \mathbb{Q}$. Consideremos $(0, q_2) \in \mathbb{Q} \times \mathbb{Q}$ entonces existe $k \in \mathbb{Z}$ tal que:

$$(0, q_2) = k(q_1, q_2) = (kq_1, kq_2) \implies k = 0 \wedge k = 1$$

Algo imposible por lo que $\mathbb{Q} \times \mathbb{Q}$ no es cíclico.

Pregunta 3. Si G es cíclico y solo tiene un generador pruebe que $|G| \leq 2$.

Solución. Como G es cíclico entonces $G = \langle x \rangle$ para algún $x \in G$. Se sabe que x^{-1} también es un generador, entonces debemos tener que $x = x^{-1}$. Esto último implica que $x^2 = 1$ por lo que tenemos:

$$|x| = |G| \mid 2$$

Así $|G| \leq 2$ y hemos probado lo pedido.

Juan Paucar - Marco

Pregunta 1. Diga si los siguientes subconjuntos son grupos:

a) $\{a + ia : a \in \mathbb{R}\} \subseteq \mathbb{C}$.

b) Dado $n \in \mathbb{N}$, $\left\{\frac{a}{b} \in \mathbb{Q} : (b, n) = 1\right\}$.

c) El subconjunto de $2-$ciclos en S_n con $n \geq 3$.

d) Los números pares con el 0 en $\mathbb{Z}$.

Solución.

a) Sí es un grupo, pues dados $(a + ia), (b + ib)$ se tiene que:

$$(a + ia) - (b + ib) = (a - b) + i(a - b)$$

b) Sí es un grupo, consideremos a/b y c/d con $(b, n) = 1 = (d, n)$. Tenemos que:

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

Ahora afirmamos que $(bd, n) = 1$, en efecto, si p es un primo tal que $p \mid bd$ y $p \mid n$. Entonces $p \mid b$ o $p \mid d$, en ambos casos también divide a n por lo que dividiría a su mcd, como este es 1 se tiene que $p \mid 1$ algo imposible. Por lo tanto no existe ningún primo que divida a bd y n, así $(bd, n) = 1$. Esto prueba que la diferencia está en el conjunto.

c) No es grupo, basta considerar por ejemplo en S_3 el producto $(1\ 2)(1\ 3) = (1\ 3\ 2)$.

d) Si es un grupo pues la resta de dos pares sigue siendo par.

Pregunta 2. Sea $f : G \to H$ un homomorfismo de grupos, si $|f(a)|$ es finito pruebe que $|a|$ es infinito o $|f(a)|$ divide a $|a|$.

Solución. Supongamos que $|a|$ es finito, luego:

$$1 = f(1) = f(a^{|a|}) = f(a)^{|a|}$$

Así como $|f(a)|$ es finito, se tiene que $|f(a)|$ divide a $|a|$.

Pregunta 3. Un isomorfismo de un grupo a si mismo, se denomina un **automorfismo**. El conjunto de todos los autormorfismo de un grupo G forma un grupo con la composición de funciones y se denota por $\mathrm{Aut}(G)$. Pruebe que $\mathrm{Aut}(\mathbb{Z}_n)$ es isomorfo a $(\mathbb{Z}_n^\times, \cdot)$. (Sugerencia: considere el mapa $f \mapsto f(\overline{1})$ y pruebe que es un isomorfismo.)

Solución. Consideremos la función $\varphi : \mathrm{Aut}(\mathbb{Z}_n) \to (\mathbb{Z}_n^\times, \cdot)$ definida por $\varphi(f) = f(\overline{1})$.

- φ **está bien definida.** En efecto, solo resta ver que para un f arbitrario se tiene que $f(\overline{1})$ es coprimo con n. Esto es cierto pues $\mathbb{Z}_n = \langle f(\overline{1})\rangle$ y por lo visto en teoría se sabe que esto solo se da si $(f(\overline{1}), n) = 1$.

- φ **es un homomorfismo.** Sean $f, g \in \mathrm{Aut}(\mathbb{Z}_n)$ entonces:

$$\varphi(f \circ g) = (f \circ g)(\overline{1}) = f(g(\overline{1})) = f(g(\overline{1})\overline{1}) = g(\overline{1})f(\overline{1}) = \varphi(f)\varphi(g)$$

- φ **es inyectivo.** Si $\varphi(f) = \varphi(g)$ entonces:

$$f(\overline{x}) = f(x\overline{1}) = xf(\overline{1}) = xg(\overline{1}) = g(\overline{x})$$

- φ **es sobreyectivo.** Consideremos $\overline{x} \in \mathbb{Z}_n^\times$, entonces $(x, n) = 1$. Así existen enteros a, b tales que $ax + bn = 1$. Vamos a definir un automorfismo $f : \mathbb{Z}_n \to \mathbb{Z}_n$.

  Ponemos $f(\overline{1}) = \overline{x}$ y $f(\overline{0}) = \overline{0}$, entonces $f(\overline{y}) = \overline{xy}$. Veamos que esta función así definida es un automorfismo.

  - f está bien definida pues si $\overline{y_1} = \overline{y_2}$ entonces $y_1 - y_2 = kn$ con $k \in \mathbb{Z}$. Entonces $\overline{xy_1} = \overline{xy_2}$ con lo que $f(\overline{y_1}) = f(\overline{y_2})$.
  - f es un homomorfismo pues:

$$f(\overline{y_1} + \overline{y_2}) = f(\overline{y_1 + y_2}) = \overline{x(y_1 + y_2)} = \overline{xy_1} + \overline{xy_2} = f(\overline{y_1}) + f(\overline{y_2})$$

  - f es inyectivo, pues si $f(\overline{y_1}) = f(\overline{y_2})$ entonces $\overline{xy_1} = \overline{xy_2}$. Luego se tiene que $x(y_1 - y_2) = kn$ con $k \in \mathbb{Z}$. Así:

$$\overline{y_1 - y_2} = (\overline{ax})\overline{y_1 - y_2} = \overline{akn} = \overline{0}$$

    Así $\overline{y_1} = \overline{y_2}$ y f es inyectiva.
  - f es sobreyectivo. En efecto, dado $\overline{y} \in \mathbb{Z}_n$ como $ax + bn = 1$ entonces $y = yax + ybn$ y tomando clases:

$$\overline{y} = \overline{yax} + \overline{ybn} = \overline{yax} = f(\overline{ay})$$

  Ahora $f(\overline{1}) = \overline{x}$ por lo que $\varphi(f) = \overline{x}$ probando que φ es sobreyectiva.

Miller

Pregunta 1. Sea G un grupo con $|G| = n > 2$, pruebe que no existe subgrupo H tal que $|H| = n - 1$. ¿Existirá un subgrupo con $n - 2$ elementos?

Solución. Supongamos que si exista y sea $a \in H$ un elemento cualquiera. Luego se tiene que $a^{n-1} = 1$ y $a^n = 1$, así:

$$a = a^{n-1}a = a^n = 1$$

Entonces $|H| = 1 = n - 1$ por lo que $n = 2$ algo imposible.

Pregunta 2. Sea $Z_n = \langle r \rangle \leq D_{2n}$, para $a \in \mathbb{Z}$ definimos $\sigma_a : Z_n \to Z_n$ por:

$$\sigma_a(x) = x^a$$

a) σ_a es un isomorfismo si y solo si $(a, n) = 1$.

b) $\sigma_a = \sigma_b$ si y solo si $a \equiv b \pmod{n}$.

c) Un isomorfismo de un grupo a si mismo, se denomina un **automorfismo**. Pruebe que el conjunto de todos los automorfismos de un grupo G, denotado por $\mathrm{Aut}(G)$, es un grupo con la composición de funciones.

d) El mapa $\overline{a} \mapsto \sigma_a$ es un isomorfismo entre $(\mathbb{Z}_n)^\times$ y $\mathrm{Aut}(Z_n)$. Concluya que $\mathrm{Aut}(Z_n)$ es un grupo abeliano.

Solución.

a) ($\Rightarrow$) Pongamos que $(a, n) = d$, entonces $a = dk_1$ y $n = dk_2$ con $k_1, k_2 \in \mathbb{Z}$. Luego como σ_a es un isomorfismo:

$$\sigma_a(r^{k_2}) = r^{k_2 a} = r^{k_2 d k_1} = (r^n)^{k_1} = 1 \implies r^{k_2} = 1$$

Así $n \mid k_2$ por lo que $k_2 = nk_3$ con $k_3 \in \mathbb{Z}$, reemplazando:

$$k_2 = dk_2k_3 \implies dk_3 = 1 \implies d = 1$$

($\Leftrightarrow$) Veamos que σ_a es biyectiva.

- Es inyectiva pues si $\sigma_a(r^p) = \sigma_a(r^q)$ entonces $r^{ap} = r^{aq}$. Esto implica que $n \mid a(p - q)$ y como $(a, n) = 1$ se sigue que $n \mid p - q$. Sin embargo $p - q < n$ por lo que necesariamente $p - q = 0$.
- Es sobreyectiva pues para $r^p \in \langle r \rangle$, como $(a, n) = 1$ existen enteros x, y tales que $1 = nx + ay$. Así:

$$r^p = r^{pnx} r^{pay} = (r^{py})^a = \sigma_a(r^{py})$$

b) ($\Rightarrow$) Se tiene que $\sigma_a(r) = \sigma_b(r)$ por lo que $r^a = r^b$ y así $n \mid a - b$ por lo que $a \equiv b \pmod{n}$ probando lo pedido.

($\Leftrightarrow$) Se tiene que $a - b = kn$ para algún entero k. Luego para $p \in \{0, \ldots, n - 1\}$:

$$\sigma_a(r^p) = r^{pa} = r^{p(b+kn)} = r^{bp} = \sigma_b(r^p)$$

c) Este hecho es evidente, pues la composición de isomorfismos sigue siendo isormosfimo. El elemento neutro será la identidad y la inversa la respectiva función inversa.

d) Veamos que $\varphi : (\mathbb{Z}_n^\times) \to \mathrm{Aut}(Z_n)$ definida por $\varphi(\overline{a}) = \sigma_a$ es un isomorfismo bien definido.

- Está bien definida. En efecto, si $\overline{a} = \overline{b}$ entonces por el item b) se concluye que $\sigma_a = \sigma_b$.
- Es un homomorfismo. En efecto, resta ver que:

$$\sigma_{ab}(x) = x^{ab} = (x^b)^a = \sigma_a(x^b) = \sigma_a(\sigma_b(x))$$

- Es inyectiva. En efecto, si $\varphi(\overline{a}) = \varphi(\overline{b})$ entonces $\sigma_a = \sigma_b$ y por b) se tiene que $\overline{a} = \overline{b}$.
- Es sobreyectiva. En efecto, dado $\psi \in \mathrm{Aut}(Z_n)$ se tiene que $Z_n = \langle \psi(r) \rangle$. Pongamos $\psi(r) = r^a$ lo anterior se cumple si y solo si $(a, n) = 1$. Por a) se tiene entonces que σ_a es un isomorfismo.

  Finalmente, para $p \in \{0, 1, \ldots, n-1\}$:

$$\sigma_a(r^p) = r^{ap} = \psi(r^p)$$

  Por lo que $\sigma_a = \psi$ y así $\varphi(\overline{a}) = \psi$.

Pregunta 3. Si G es un grupo que solo tiene un número finito de subgrupos, pruebe que es finito.

Solución. Si algún $x \in G$ tiene orden infinito, entonces el subgrupo $\langle x \rangle$ tendría orden infinito. Por lo visto en teoría, este subgrupo tiene una cantidad numerable de subgrupos contradiciendo la hipótesis. Así todos los elementos de G tienen orden finito.

Es evidente que:

$$G = \bigcup_{g \in G} \langle g \rangle$$

Ahora, como G solo tiene una cantidad finita de subgrupos, la colección $\{\langle g \rangle : g \in G\}$ debe ser finita podemos considerar que:

$$\{\langle g \rangle : g \in G\} = \{\langle x_1 \rangle, \ldots, \langle x_r \rangle\}$$

Así:

$$G = \bigcup_{i=1}^{r} \langle x_i \rangle \implies |G| \leq \sum_{i=1}^{r} |x_i| < \infty$$