PESQUIMAT 24(1): 1–8 (2021)
http://dx.doi.org/10.15381/pesquimat.v24i1.20511

ISSN:1560-912X/ ISSN-E:1609-8439
Facultad de Ciencias Matemáticas – UNMSM

El Teorema de Iwasawa

Carlos Mejía Alemán [1] ***Mario Enrique Santiago Saldaña*** [2]

Resumen: Sean G un grupo, Ω un conjunto y $K = \{g \in G \mid \omega * g = \omega, \ \forall \omega \in \Omega\}$ el núcleo de Ω donde G actua sobre el conjunto Ω. Mostraremos que G/K es simple en el caso que el grupo G verifique ser primitivo sobre Ω, así como también que sea igual a su subgrupo derivado y por último si $\alpha \in \Omega$ entonces G_α tiene un subgrupo A que es abeliano y normal tal que $G =< A^g \mid g \in G >$, donde G_α es el estabilizador de α en G.

Para finalizar daremos una aplicación de que el grupo alternante A_5 es simple.

Palabras clave: acción, transitivo, grupo primitivo, bloque y núcleo.

The Iwasawa's Theorem

Abstract: Let G be a group, Ω a set and $K = \{g \in G \mid \omega * g = \omega, \ \forall \omega \in \Omega\}$ the nucleus of Ω where G acts on the set Ω. We will show that G/K is simple in the case that the group G verifies to be primitive on Ω, as well as that it is equal to its derived subgroup and finally if $\alpha \in \Omega$ then G_α has a subgroup A that is abelian and normal such that $G =< A^g \mid g \in G >$, where G_α is the stabilizer of α in G. To finish we will give an application that the alternating group A_5 is simple.

Keywords: action, transitive, primitive group, block and kernel.

Recibido: 11/01/2021. *Aceptado:* 17/04/2021. *Publicado online:* 30/06/2021.

[1]UNAJMA, Facultad de Ingeniería. e-mail:cmejia@unajma.edu.pe
[2]UNMSM, Facultad de Ciencias Matemáticas, e-mail:msantiagos@unmsm.edu.pe

1. Introducción

En preliminares recordaremos las definiciones de subgrupos, subgrupos normales, subgrupos conmutadores y grupo de permutaciones. Definiremos también conjuntos transitivos y bloques.

Se verá la definición de bloques triviales y de grupos primitivos así como también la definición de estabilizador y por último definiremos el nucleo de un conjunto donde G actua sobre dicho conjunto.

En el punto 3 que es donde se demostrará el teorema de Iwasawa, utilizaremos las definiciones anteriores y dos afirmaciones para caracterizar a los grupos primitivos en el teorema 3.2 y por último demostraremos el teorema central de este trabajo que tiene por nombre el Teorema de Iwasawa. Este teorema nos permite saber cuando un grupo cociente G/K es simple teniendo tres hipótesis, la primera es que G sea un grupo primitivo, la segunda es que el grupo derivado de G sea igual a G y por último si $\alpha \in \Omega$ entonces G_α tiene un subgrupo A que es abeliano y normal tal que $G =< A^g \mid g \in G >$, donde $K = \{g \in G \mid \omega * g = \omega, \ \ \forall \omega \in \Omega\}$ es el nucleo de Ω.

En el punto 4, que es una aplicación del teorema de Iwasawa demostraremos que el grupo alternante A_5 es simple o sea que sus únicos subgrupos normales son los triviales.

De las aplicaciones del Teorema de Iwasawa, una de las más importantes es la siguiente: el grupo especial lineal proyectivo $PSL(n, \mathbb{F})$ es simple excepto para $PSL(2, \mathbb{F}_3)$ y $PSL(2, \mathbb{F}_2)$, donde $\mathbb{F}$ es un cuerpo finito. Esta aplicación no será presentada en este trabajo, lectores interesados pueden consultar las referencias [1], [2] y [3].

2. Preliminares

Recordemos que si G es un grupo y A, B son subconjuntos no vacíos de G podemos definir el conjunto $AB := \{ab \mid a \in A, b \in B\}$.

Teorema 2.1 *Sean G un grupo y H un subgrupo de G, lo que denotamos con $H \leq G$. Son equivalentes:*

(i) $g^{-1}hg \in H$, *para cada* $g \in G$ *y cada* $h \in H$.

(ii) $g^{-1}Hg = H$, *para cada* $g \in G$.

(iii) $gH = Hg$, *para cada* $g \in G$.

Demostración. Ver [5], página 153.

Definición 2.2 *Sean G un grupo y $H \leq G$. Decimos que H es un **subgrupo normal** de G, lo cual denotamos con $H \lhd G$, si H satisface una de las equivalencias del teorema anterior.*

Sabemos que si G es un grupo entonces sus subgrupos triviales son subgrupos normales de G.

Definición 2.3 *Si los únicos subgrupos normales de un grupo G son los triviales entonces G es llamado **grupo simple**.*

Teorema 2.4 *Sean G un grupo, $H \lhd G$ y $N \leq G$. Se cumplen:*

(i) $HN = NH$ *y* $HN \leq G$.

(ii) Si G es un grupo abeliano entonces G/H también es un grupo abeliano.

(iii) Si $H \leq N$ *entonces* $H \lhd N$.

Demostración. Ver [5], página 157.

Definición 2.5 *Sean G un grupo y $G' = \langle [a,b] \mid a,b \in G\rangle$, donde $[a,b] = a^{-1}b^{-1}ab$ es llamado el conmutador de a y b. Así definido G' es llamado el* ***subgrupo conmutador*** *de G o también el subgrupo derivado de G.*

Teorema 2.6 *Sean G un grupo y G' el conmutador de G. Se cumplen:*

(i) $G' \lhd G$.

(ii) G/G' *es abeliano.*

(iii) Si $N \lhd G$ *tal que* G/N *es abeliano entonces* $G' \subseteq N$.

Ver [5], página 154.

Teorema 2.7 *Sean* $H \lhd G$ *y* $K \leq G$.*Se cumple* $K/H \cap K \cong KH/H$.

Demostración. Ver [5], página 166.

Definición 2.8 *Sean G un grupo, Ω un conjunto. Decimos que G actua sobre Ω si la aplicación*

$$\begin{array}{rcc} * : \Omega \times G & \longrightarrow & \Omega \\ (\omega, g) & \mapsto & \omega * g \end{array}$$

satisface lo siguiente:

(i) $\omega * (g_1 g_2) = (\omega * g_1) * g_2$ *, para cada* $\omega \in \Omega$ *y cualesquiera* $g_1, g_2 \in G$

(ii) $\omega * 1 = \omega$ *, para cada* $\omega \in \Omega$

Ejemplos 2.9

1. *Dado el conjunto* $\Omega = \{1, 2, 3, ..., n\}$, *definimos el grupo de permutaciones denotado por* $S_n = \{\pi : \Omega \longrightarrow \Omega \mid \pi \text{ biyectiva}\}$ *con la operación composición.*

   Se cumple que S_n *actua sobre* Ω, *donde*

$$\begin{array}{rcc} * : \Omega \times S_n & \longrightarrow & \Omega \\ (\omega, \pi) & \mapsto & \omega * \pi = \pi(\omega). \end{array}$$

2. *Sea* $\mathbb{V}$ *un* $\mathbb{K}$*-espacio vectorial donde* $\mathbb{V} = \mathbb{K}^n$.

   Definimos el grupo lineal $GL(\mathbb{V}) = \{f : \mathbb{V} \longrightarrow \mathbb{V} \mid f \text{ es lineal e invertible}\}$ *con la operación de composición.*

   Se cumple que $GL(\mathbb{V})$ *actua sobre* $\mathbb{V}$ *donde*

$$\begin{array}{rcc} * : \mathbb{V} \times GL(\mathbb{V}) & \longrightarrow & \mathbb{V} \\ (v, f) & \longmapsto & v * f = f(v). \end{array}$$

3. *Sea G un grupo. Se cumple que G actua sobre G donde*

$$\begin{array}{rcc} * : G \times G & \longrightarrow & G \\ (\omega, g) & \longmapsto & \omega * g = \omega g. \end{array}$$

4. *Sea G un grupo. Se cumple que G actua sobre G donde*

$$\begin{array}{rcc} *: G \times G & \longrightarrow & G \\ (\omega, g) & \longmapsto & \omega * g = g^{-1}\omega. \end{array}$$

5. *Sea G un grupo. Se cumple que G actua sobre G donde*

$$\begin{array}{rcc} *: G \times G & \longrightarrow & G \\ (\omega, g) & \longmapsto & \omega * g = \omega^{g} = g^{-1}\omega g. \end{array}$$

Definición 2.10 *Sea G un grupo que actua sobre Ω. Decimos que Ω es **transitivo** si para cada par $\alpha, \beta \in \Omega$ existe $g \in G$ tal que $\alpha * g = \beta$.*

Ejemplos 2.11

1. *En los ejemplos anteriores tenemos que Ω, G y $\mathbb{V}$ son transitivos.*

Definición 2.12 *Sea G un grupo que actua sobre Ω y sea $\triangle \subseteq \Omega$. Decimos que $\triangle$ es un **bloque** de G si $\triangle g = \triangle$ o $\triangle g \cap \triangle = \emptyset$, para cada $g \in G$, donde $\triangle g = \{\omega * g \mid \omega \in \triangle\}$.*

Ejemplos 2.13

1. *$\triangle = \{\omega\}$ es un bloque de G.*

2. *$\triangle = \Omega$ es un bloque de G.*

Estos bloques son llamados **bloques triviales** de G.

Definición 2.14 *Sea G un grupo que actua sobre Ω y supongamos que Ω es transitiva. Decimos que G es un grupo **primitivo** o que G es primitivo sobre Ω si sólo posee bloques triviales.*

Ejemplos 2.15

1. *$GL(\mathbb{V})$ no es primitivo sobre $\mathbb{V} - \{0\}$.*

2. *S_n es primitivo sobre $\Omega = \{1, 2, 3, ..., n\}$.*

3. *El grupo alternante A_n es primitivo sobre si mismo para cada $n \geq 3$.*

Definición 2.16 *Sea G un grupo que actua sobre Ω. Definimos el **estabilizador** de α en G por $G_\alpha = \{g \in G \mid \alpha * g = \alpha\}$, donde $\alpha \in \Omega$.*

Teorema 2.17 *Sea G un grupo que actua sobre Ω. Se cumplen las siguientes afirmaciones:*

(i) $G_\alpha \leq G$

(ii) Si $\beta \in \Omega$ es tal que $\beta = \alpha * g$ con $g \in G$ entonces $(G_\alpha)^g \subseteq G_\beta$, donde $(G_\alpha)^g := g^{-1}G_\alpha g$

Prueba.
La parte (i) es fácil de ver. Veamos (ii). Dado $h \in (G_\alpha)^g = g^{-1}G_\alpha g$ entonces existe $j \in G_\alpha$ tal que $h = g^{-1}jg$. Ya que $j \in G_\alpha$ entonces $\alpha * j = \alpha$. Ahora $\beta * h = (\alpha * g) * (g^{-1}jg) = \alpha * (jg) = (\alpha * j) * g = \alpha * g = \beta$. Por tanto $h \in G_\beta$.

Definición 2.18 *Sea G un grupo que actua sobre Ω y $K = \{g \in G \mid \omega * g = \omega, \ \forall \omega \in \Omega\} \subseteq G$. El subconjunto K es llamado el **núcleo** de Ω.*

Teorema 2.19 *Si G es un grupo que actua sobre Ω y K es el nucleo de Ω entonces $K \lhd G$.*

Prueba.

Es fácil ver que $K = \bigcap_{\alpha\in\Omega} G_\alpha$ entonces $K \leq G$. Ahora probemos $g^{-1}Kg = K$ para cada $g \in G$. Dados $g \in G$ y $k \in K$ tenemos que $g^{-1}kg \in g^{-1}Kg$. Por otro lado $\omega * (g^{-1}kg) = ((\omega * g^{-1}) * k) * g = (\omega * g^{-1}) * g = \omega$. Esto quiere decir que para cada $\omega \in \Omega$ tenemos que $\omega * (g^{-1}kg) = \omega$, luego $g^{-1}Kg \subseteq K$.

3. El teorema de Iwasawa

Antes de enunciar y demostrar el teorema de Iwasawa vamos a caracterizar a los grupos primitivos ya que tal caracterización es fundamental para la prueba de dicho teorema.

Afirmación 1.
Si $H \leq G$ y $G_\alpha \leq H$ entonces $\alpha H = \{\alpha * h \mid h \in H\}$ es un bloque de G.
En efecto:
Sabemos que αH es un bloque de G sí y solo si $\alpha Hg = \alpha H$ ó $\alpha Hg \cap \alpha H = \emptyset$.
Si $g \in H$ es fácil ver que $\alpha Hg = \alpha H$.
Si $g \notin H$ y supongamos que $\alpha Hg \cap \alpha H \neq \emptyset$ entonces $g \in H$.
Por lo tanto $\alpha Hg \cap \alpha H = \emptyset$.

Afirmación 2.
Si $\alpha \in\triangle$ donde $\triangle$ es un bloque de G entonces $G_\alpha \leq G_\triangle \leq G$ donde $G_\triangle := \{g \in G \mid\triangle g =\triangle\}$.
En efecto:
Dado $g \in G_\alpha$ entonces $\alpha * g$=α luego $\alpha \in\triangle$g $\cap$ $\triangle$, entonces $\triangle g =\triangle$.
Por lo tanto $g \in G_\triangle$.

Definición 3.1 *Sean G un grupo que actua sobre Ω, que es transitivo, $\alpha \in \Omega$ fijo. Definimos las siguientes aplicaciones:*

$$\begin{array}{rcl} \varphi : \mathcal{F} & \longrightarrow & \mathcal{G} \\ H & \mapsto & \alpha H \end{array}$$

$$\begin{array}{rcl} \psi : \mathcal{G} & \longrightarrow & \mathcal{F} \\ \triangle & \mapsto & G_\triangle \end{array}$$

donde $\mathcal{F} := \{H \leq G \mid G_\alpha \leq H\}$, $\mathcal{G} := \{\triangle \mid \triangle$ es un bloque de G y $\alpha \in\triangle\}$.

Afirmación 3.
$\psi \circ \varphi = id_{\mathcal{F}}$.
En efecto:
Dado $H \in \mathcal{F}$ entonces $(\psi \circ \varphi)(H) = \psi(\alpha H) = G_{\alpha H} := \{g \in G \mid \alpha Hg = \alpha H\}$. Es fácil ver que $H \subseteq G_{\alpha H}$.
Ahora, dado $g \in G_{\alpha H}$ entonces $\alpha Hg = \alpha H$ y consideremos $m \in \alpha Hg$ entonces $m = \alpha * (h_1 g) = \alpha * h_2$ para ciertos $h_1, h_2 \in H$, luego $\alpha * (h_1 g h_2^{-1}) = \alpha$ y resulta que $h_1 g h_2^{-1} \in G_\alpha$, pero dado que $H \in \mathcal{F}$ entonces $G_\alpha \subseteq H$. Esto quiere decir, que $h_1 g h_2^{-1} \in H$, luego $g \in H$ entonces tenemos que $G_{\alpha H} \subseteq h$.
Por lo tanto $(\psi \circ \varphi)(H) = H$.

Afirmación 4.
$\varphi \circ \psi = id_{\mathcal{G}}$.
En efecto:
Dado $\triangle \in \mathcal{G}$ entonces $(\varphi \circ \psi)(\triangle) = \varphi(G_\triangle) = \alpha G_\triangle$.
Sea $\omega \in \alpha G_\triangle$ entonces existe $g \in G_\triangle$ tal que $\omega = \alpha * g$ de donde $\triangle$g $\cap \triangle = \emptyset$, luego $\triangle$g=$\triangle$, pero $\omega \in \triangle$g=$\triangle$ entonces $\omega \in \triangle$.
Por lo tanto $\alpha G_\triangle \subseteq \triangle$.
Dado $\omega \in \triangle$ entonces existe $g \in G$ tal que $\omega = \alpha * g$, pues Ω es transitiva. Tenemos que $g \in G_\triangle$ pues $\triangle$g=$\triangle$ ya que $\omega \in \triangle \cap \triangle$g$\neq \emptyset$. Por lo tanto $\triangle \subseteq \alpha G_\triangle$.

Teorema 3.2 *Sea G un grupo que actua sobre Ω.*
Entonces G un grupo primitivo sí y sólo si G_α es un subgrupo maximal de G para algún $\alpha \in \Omega$.

Prueba.
[$\Rightarrow$] *Sea $G_\alpha \leq H \subsetneq G$. Por afirmación 1, αH es un bloque de G y $\alpha \in \alpha H$.*
Por ser G primitivo tenemos que $\alpha H = \{\alpha\}$ o $\alpha H = \Omega$, en el primer caso $H \subseteq G_\alpha$, de donde $H = G_\alpha$, mostrando así que G_α es maximal.
Veamos que el segundo caso, $\alpha H = \Omega$, es imposible. En efecto, notemos primero que $\alpha G = \Omega$, pues, si $\beta \in \Omega$ cualquiera, por ser la acción transitiva, existe $g \in G$ ta que $\beta = \alpha * g \in \alpha G$, de donde $\Omega \subseteq \alpha G \subseteq \Omega$. Así $\varphi(G) = \alpha G = \Omega = \alpha H = \varphi(H)$, luego $G = H$ por ser φ biyección.Un absurdo, pues $H \subsetneq G$.
[$\Leftarrow$] *Sea $\triangle$ un bloque de G y supongamos que $\triangle \neq \Omega$. Afirmamos primero que $\triangle \neq \Omega$ entonces $G_\triangle \subsetneq G$. En efecto, sea $\alpha \in \triangle$, si $G_\triangle = G$, tenemos que $\psi(\triangle) = G_\triangle = G = \psi(\varphi(G))$ entonces por ser ψ biyección tenemos que $\triangle = \varphi(G) = \alpha G$, luego $\triangle = \{\alpha * g : g \in G\}$. Sea $\omega \in \Omega - \triangle$, como la acción es transitiva,existe $g \in G$ tal que $\omega = \alpha * g \in \triangle$ pues $\triangle = \{\alpha * g : g \in G\}$ y esto es un absurdo.*
Veamos ahora que $\triangle$ es un conjunto unitario. Sean $\alpha, \beta \in \triangle$, por afirmación 2 y por lo anterior tenemos que $G_\alpha \leq G_\triangle \subsetneq G$, $G_\beta \leq G_\triangle \subsetneq G$ y por maximalidad $G_\alpha = G_\triangle = G_\beta$ así $\psi(\{\alpha\}) = G_\alpha = G_\beta = \psi(\{\beta\})$, luego por ser ψ biyección $\{\alpha\} = \{\beta\}$, lo que implica que $\triangle$ es unitario.
Esto muestra que G es primitivo.

Teorema 3.3 (Teorema de Iwasawa) *Sea G un grupo que actua transitivamente sobre Ω tal que se cumplen:*

(i) *G es un grupo primitivo*

(ii) $G' = G$

(iii) *Si $\alpha \in \Omega$, G_α tiene un subgrupo A que es abeliano y normal de modo que $G = < A^g \mid g \in G >$.*

Entonces G/K es un grupo simple.

Prueba. *Sabemos que los subgrupos normales de G/K están en correspondencia con los subgrupos normales de G que contienen a K , luego basta probar que si $N \lhd G$ con $K \leq N$ entonces $N = G$ ó $N = K$.*
Supongamos que $N \neq K$ entonces tenemos $G_\alpha \leq NG_\alpha \leq G$, luego por el teorema 3.2 y la hipótesis (i) se tiene que G_α es un subgrupo maximal de G , entonces $G_\alpha = NG_\alpha$ ó $NG_\alpha = G$. Si se da el caso $G_\alpha = NG_\alpha$ se tiene que $N \subseteq G_\alpha$ entonces $N^g \subseteq (G_\alpha)^g$ y dado que $N \lhd G$ tenemos que $N = N^g := g^{-1}Ng$, luego $N = N^g \subseteq (G_\alpha)^g$. Ahora tomemos $\beta \in \Omega$ arbitrario entonces existe $g \in G$ tal que $\beta = \alpha * g$ pues Ω es transitivo, luego por teorema 2.13 (ii) se

tiene que $(G_\alpha)^g \subseteq G_\beta$ *entonces tenemos que* $N \subseteq G_\beta$ *para cada* $\beta \in \Omega$ *luego* $N \subseteq \bigcap_{\beta\in\Omega} G_\beta = K$ *entonces* $N \subseteq K$ *y dado que* $K \leq N$ *conseguimos que* $N = K$ *lo cual es una contradicción. Por lo tanto nos queda el caso* $NG_\alpha = G$.

Afirmación. $G = AN$. *En efecto: dado* $g \in G = NG\alpha$ *entonces* $g = nh$, *para ciertos* $n \in N$, $h \in G_\alpha$. *Ahora* $A^{g^{-1}} = A^{(nh)^{-1}} = (nh)A(nh)^{-1} = (nh)A(h^{-1}n^{-1}) = n(hAh^{-1})n^{-1}$ *y por ser* A *un grupo normal en* G_α *tenemos que* $n(hAh^{-1})n^{-1} = nAn^{-1}$, *luego* $A^{g^{-1}} = nAn^{-1}$. *Por teorema* 2.4 *(i) tenemos que* $AN = NA$ *pues* $N \lhd G$ *y* $A \leq G$, $nAn^{-1} \subseteq AN$ *y es fácil ver que* $nAn^{-1} \leq AN$, *luego* $A^{g^{-1}} \leq AN$, *para cada* $g \in G$ *entonces* $G = AN$ *pues* $G =< A^g \mid g \in G >$.

Tenemos que $G/N = AN/N \cong A/A \cap N$ *por teorema* 2.7 *y dado que* A *es abeliano entonces por teorema* 2.4 *parte (ii) obtenemos que* $A/A \cap N$ *es abeliano , luego* G/N *es abeliano,* $G' \subseteq N$ *por teorema* 2.6 *(iii) , pero por la hipótesis (ii)* $G' = G$ *entonces* $N = G$.

4. Aplicación

Como una aplicación sencilla del teorema de Iwasawa, mostraremos que el grupo alternante A_5 es un grupo simple. Antes enunciemos un lema, cuya prueba puede verse en [6] página 107.

Lema 4.1 *Para* $n \geq 3$, *todo elemento de* A_n *es un 3-cíclo o producto de 3-cíclos.*

Observación 1. Se sigue del lema anterior que el conjunto de los 3-cíclos genera todo A_5.

Ahora $G = A_5$ actúa sobre $\Omega = \{1, 2, 3, 4, 5\}$ mediante

$$\begin{array}{rcc} * : \Omega \times G & \longrightarrow & \Omega \\ (i, g) & \mapsto & i * g = g(i). \end{array}$$

Esta acción es transitiva, pues para $\alpha \neq \beta$ en Ω existe $g = (\alpha\beta)$ tal que $\alpha * g = g(\alpha) = \beta$. Notemos que, para α fijo arbitrario en Ω tenemos que: $g \in G_\alpha$ sí y solo si $g(\alpha) = \alpha$ sí y solo si g mueve solo 4 elementos sí y solo si g es un elemento de A_4, por lo tanto $G \cong A_4$, para todo $\alpha \in \Omega$.

Supongamos que G_α no es un subgrupo maximal de A_5, para algún $\alpha \in \Omega$. Entonces, existe $H < A_5$ ta que $G_\alpha \subsetneq H \subsetneq A_5$ entonces $\mid G_\alpha \mid < \mid H \mid < \mid A_5 \mid$ entonces $12 < \mid H \mid < 60$ pues $G \cong A_4$, pero por el teorema de Lagrange 12 divide a $\mid H \mid$ y $\mid H \mid$ divide a 60, concluímos que tal H no existe. Así G_α es un subgrupo maximal de A_5, para todo $\alpha \in \Omega$, y por teorema 3.2, $G = A_5$ es un grupo primitivo.
Para $\alpha = 5$, tenemos que $G_\alpha \cong A_4$ tiene como subgrupo normal y abeliano al conjunto $A = \{(1), (12)(34), (13)(24), (14)(23)\}$.

Recordemos que toda permutación de la forma $(ab)(cd)$, con a, b, c, d, distintos dos a dos es llamado un $(2, 2)$-cíclo.

Lema 4.2 *Todo* $(2, 2)$*-cíclo es conjugado a un elemento de* A.

Prueba. Los $(2, 2)$-cíclos que no estan en A son aquellos que contienen al número 5, tomemos uno de estos $(2, 2)$-cíclo y sin perder generalidad, asumamos que es de la forma $(b5)(cd)$, con b, c, d, distintos dos a dos y $b, c, d < 5$. Tenemos que $[(1b5)\underbrace{(1b)(cd)}_{\in A}(1b5)^{-1}] = (b5)(cd)$.

Observación 2. Del lema anterior se sigue que cada $(2,2)$-cíclo pertenece a un conjunto de la forma gAg^{-1}, para cierto $g \in A_5$.

Lema 4.3 *Todo 3-cíclo es producto de* $(2,2)$*-cíclos.*

Prueba. Sea (abc) un 3-cíclo cualquiera, tenemos que $\underbrace{(ab)(ed)}_{(2,2)-\text{cíclo}}\ \underbrace{(bc)(ed)}_{(2,2)-\text{cíclo}} = (abc)$.

Del lema anterior y las observaciones 1 y 2 concluimos que $G = A_5 =< gAg^{-1} : g \in G >$.

Veamos ahora que $G = G'$. En efecto: de lo anterior, bastará ver que todo $(2,2)$-cíclo está en G'. Sea (ab)(cd) un $(2,2)$-cíclo cualquiera, tenemos $(ab)(cd) = \underbrace{(abc)(abd)(abc)^{-1}(abd)^{-1}}_{\in G'}$.

Hasta aquí, hemos comprobado todas las hipótesis del teorema de Iwasawa para A_5. Resta calcular el núcleo K de Ω. En efecto: $g \in K$ sí y solo si $g(\alpha) = \alpha$, para todo $\alpha \in \Omega$ y esto último es equivalente a $g = (1)$, así $K = \{(1)\}$. Finalmente, por el teorema de Iwasawa tenemos que $G/K = A_5/\{(1)\} = A_5$ es simple.

Los interesados en conocer otras aplicaciones pueden ver las referencias [1] y [2].

5. Conclusión

Hemos visto que el grupo alternante A_5 es simple como una aplicación del teorema de Iwasawa. La prueba presentada es diferente de la usual.
Lo que motivó a los autores a presentar este trabajo es lo desconocido que es este teorema y la poca bibliografía en los idiomas, como el ingles, portugues y español. Los aportes que han dado los autores en este trabajo, son desmenuzar el teorema de Iwasawa y una prueba original de que A_5 es simple, utilizando el teorema de Iwasawa. Se puede generalizar que A_n donde $n \geq 5$, es simple utilizando el teorema de Iwasawa, ver [4], página 15. La aplicación más importante del teorema de Iwasawa es que el grupo especial lineal proyectivo $PSL(n, \mathbb{F})$ es simple excepto para $PSL(2, \mathbb{F}_3)$ y $PSL(2, \mathbb{F}_2)$, donde $\mathbb{F}$ es un cuerpo finito, $PSL(n, \mathbb{F}) = SL(n, \mathbb{F})/Z \cap SL(n, \mathbb{F})$, Z es el centro de $GL(n, \mathbb{F}) = \{A_{n\times n} \mid Det(A) \neq 0\}$ y $SL(n, \mathbb{F}) = \{A_{n\times n} \in GL(n, \mathbb{F}) \mid Det(A) = 1\}$. Si el cuerpo $\mathbb{F}$ es infinito entonces siempre $PSL(n, \mathbb{F})$ es simple. Los grupos $PSL(2, \mathbb{F}_2)$ y $PSL(2, \mathbb{F}_3)$ no son simples pues $PSL(2, \mathbb{F}_2) \cong S_3$ y el número de elementos de $PSL(2, \mathbb{F}_3)$ es 24. Para más información ver las referencias [1], [2] y [3].

Referencias bibliográficas

[1] Robert A. Wilson (2009). *The Finite Simple Groups.* Springer-Verlag London.

[2] D.E. Taylor (2002). *The Geometry of the Classical Groups.* Heldermann Verlag.

[3] Larry C. Grove (1990). *Classical groups and geometric algebra.* American Mathematical Society.

[4] Keith Conrad. Simplicity of A_n.
Recuperado de https://kconrad.math.uconn.edu/blurbs/grouptheory/transitive.pdf

[5] Arnaldo Garcia e Yves Lequain (2001). *Elementos de Álgebra.* Coleção Projeto Euclides IMPA.

[6] Joseph J. Rotman (2003). *Advanced Modern Algebra.* Prentice Hall.