8

2-9

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

SOBRE LOS ORDENES DE LOS GRUPOS LINEALES ESPECIALES PROYECTIVOS PSL(n,q).

T E S I S

PARA OBTENER EL TITULO DE:

MATEMATICO

P R E S E N T A:

MARIA CONCEPCION GONZALEZ ENRIQUEZ

MEXICO, D. F. MARZO 1990

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

I N D I C E

I N T R O D U C C I O N

En la teoría de grupos , el estudio de los grupos simples es de gran importancia ya que todos los grupos finitos están constituidos de bloques elementales, los cuales son los grupos simples.

Un grupo simple es un grupo que no contiene subgrupos normales que no sean el mismo o el formado por la identidad, entendiendose como subgrupo normal, aquel subgrupo que bajo automorfismos internos permanece invariante.

Actualmente se cree que la clasificación de los grupos simples finitos ha sido terminada. Es conocido que un grupo finito simple no cíclico es o un grupo Alternante, o un grupo del tipo de Lie, o uno de los 26 grupos simples esporádicos (llamados así porque no pertenecen a ninguna familia infinita). El último paso de dicha clasificación se hizo en febrero de 1981 cuando Simon Norton, mostró la unicidad del grupo esporádico Fisher-Griess F_1, conocido como el monstruo por su gran orden : 808,017,424,794,512,875,866,459,904,961,710,757,005,754,268,000, 000,000. (aproximádamente 10^{54}).

Al encontrarse el último de los grupos simples esporádicos el problema de la clasificación de los grupos simples había terminado, faltando solamente escribir con detalle el tratado sobre dicha clasificación, que según estimaciones de algunos matemáticos ocupados en tal problema serian necesarias por aquélla época alrededor de 5,000 páginas.

Así pues los grupos finitos simples están clasificados en las familias infinitas de : los grupos cíclicos de orden primo, los grupos alternantes A_n, $n \geq 5$, los llamados grupos del tipo de Lie entre los cuales se encuentran los grupos Lineales Especiales Proyectivos PSL(n,q) y la colección de los 26 grupos que no pertenecen a familia infinita alguna, denominados grupos simples esporádicos.

En el primer capítulo del presente trabajo se demuestra la simplicidad de los grupos alternantes A_n, $n \geq 5$ y la de los grupos lineales especiales proyectivos PSL(n,q), con $(n,q) \neq (2,2)$

y (n,q) ≠ (2,3).

Los grupos Alternantes A_r, están formados por las permutaciones pares efectuadas sobre n objetos.

Para n > 1, el grupo Lineal Especial SL(n,q), es el grupo de transformaciones lineales invertibles del espacio vectorial de dimensión n sobre el campo F con q elementos, cuyo determinante es 1, y el grupo Lineal Especial Proyectivo PSL(n,q), es el grupo cociente SL(n,q)/Z(SL(n,q)), donde Z(SL(n,q)) es el centro de SL(n,q).

En el segundo capítulo se demuestra que sólo existen tres casos en que grupos lineales especiales proyectivos diferentes tienen el mismo número de elementos, de los cuales en un sólo caso no existe isomorfismo entre dichos grupos :

$|PSL(2,4)| = |PSL(2,5)|$ y $PSL(2,4) \cong PSL(2,5)$

$|PSL(2,7)| = |PSL(3,2)|$ y $PSL(2,7) \cong PSL(3,2)$

$|PSL(4,2)| = |PSL(3,4)|$ y $PSL(4,2) \ncong PSL(3,4)$

Y de seis casos en que grupos lineales especiales proyectivos tienen su orden igual al de algún grupo Alternante A_m :

$|PSL(2,3)| = |A_4|$ $PSL(2,3) \cong A_4$

$|PSL(2,4)| = |PSL(2,5)| = |A_5|$ $PSL(2,4) \cong A_5 \cong PSL(2,5)$

$|PSL(2,9)| = |A_6|$ $PSL(2,9) \cong A_6$

$|PSL(3,4)| = |PSL(4,2)| = |A_8|$ $PSL(3,4) \ncong A_8 \cong PSL(4,2)$.

Esta cuestión de que todos los grupos PSL(n,q) tienen diferentes órdenes entre dos distintos grupos PSL(n,q) o entre un grupo PSL(n,q) y algún grupo alternante A_m, salvo los casos anteriores, se mantuvo abierta por mucho tiempo, hasta que Emil Artin (1898-1962) lo probó.

Con estas excepciones se confirma que los grupos lineales especiales proyectivos forman una familia infinita diferente a la de los grupos Alternantes A_m y que son diferentes entre sí.

C A P I T U L O I

SIMPLICIDAD DE LOS GRUPOS ALTERNANTES A_n Y LOS GRUPOS LINEALES ESPECIALES PROYECTIVOS PSL(n,q)

NOCIONES BASICAS

Un GRUPO, como se sabe, es un conjunto $\mathbb{G} \neq \emptyset$, con una operación binaria $*$ definida en él, tal que

i) Para todo $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.

ii) Existe un elemento $e \in \mathbb{G}$, tal que para todo $g \in \mathbb{G}$,

$$g * e = e * g = g .$$

iii) Para cada $g \in \mathbb{G}$, existe un elemento $g^{-1} \in \mathbb{G}$, tal que

$$g * g^{-1} = g^{-1} * g = e .$$

NOTACION. Si $g_1, g_2 \in \mathbb{G}$ se escribirá $g_1 * g_2 = g_1 g_2$.

DEFINICION. Un grupo $\mathbb{G}$ es ABELIANO, si $g_1 g_2 = g_2 g_1$, para todo $g_1, g_2 \in \mathbb{G}$.

DEFINICION. Un SUBGRUPO $\mathbb{H}$ de un grupo $\mathbb{G}$, es un subconjunto $\mathbb{H} \subseteq \mathbb{G}$, tal que $\mathbb{H}$ es un grupo con la misma operación $*$ definida en $\mathbb{G}$.

NOTACION. Si $\mathbb{H}$ es subgrupo de $\mathbb{G}$, se escribirá $\mathbb{H} < \mathbb{G}$.

DEFINICION. Un subgrupo $\mathbb{N}$ de un grupo $\mathbb{G}$, es un subgrupo NORMAL en $\mathbb{G}$, si para todo $n \in \mathbb{N}$ y para todo $g \in \mathbb{G}$, $gng^{-1} \in \mathbb{N}$.

Esta definición tiene varias formas equivalentes, por ejemplo, $\mathbb{N}$ es normal en $\mathbb{G}$ si y soló si $g\mathbb{N}g = \mathbb{N}$, para todo $g \in \mathbb{G}$, o si y sólo si $gN = Ng$, para todo $g \in \mathbb{G}$.

NOTACION. Si $\mathbb{N}$ es un subgrupo normal de $\mathbb{G}$, se escribirá $\mathbb{N} \lhd \mathbb{G}$.

DEFINICION. Un grupo $\mathbb{G}$ es SIMPLE, si los únicos subgrupos normales que contiene $\mathbb{G}$ son él mismo y el subgrupo trivial, formado por el elemento identidad.

En este trabajo sólo se consideran grupos finitos.

Es inmediato del Teorema de Lagrange que los grupos cíclicos de orden primo son simples. Así se tiene una familia infinita de grupos finitos simples, uno por cada número primo que existe. Cabe hacer la observación de que éstos son los únicos grupos finitos simples y abelianos.

OTROS RESULTADOS.

NOTACION. p siempre denotará un número primo.
NOTACION. $|\mathbb{G}|$, denotará el orden del grupo $\mathbb{G}$.

PRIMER TEOREMA DE SYLOW. Sea $\mathbb{G}$ un grupo con $|\mathbb{G}| = p^n m$, donde $n \geq 1$, $(p,m) = 1$, entonces
i) $\mathbb{G}$ contiene un subgrupo de orden p^i para cada i, $1 \leq i \leq n$.
ii) Todo subgrupo $\mathbb{H}$ de $\mathbb{G}$, de orden p^i es un subgrupo normal de algún subgrupo de $\mathbb{G}$ de orden p^{i+1} para $1 \leq i < n$.

DEFINICION. Un p-SUBGRUPO DE SYLOW DE $\mathbb{G}$, es un subgrupo de $\mathbb{G}$ de orden p^r , donde $p^r | |\mathbb{G}|$ y $p^{r+1} \nmid |\mathbb{G}|$.

SEGUNDO TEOREMA DE SYLOW . Sea p tal que $p||\mathbb{G}|$, $\mathbb{H}_1$, $\mathbb{H}_2$ p-subgrupos de Sylow de un grupo $\mathbb{G}$, entonces $\mathbb{H}_1$ y $\mathbb{H}_2$ son subgrupos conjugados de $\mathbb{G}$, es decir, existe $g \in \mathbb{G}$ tal que $\mathbb{H}_1 = g^{-1}\mathbb{H}_2 g$.

TERCER TOREMA DE SYLOW. Si G es un grupo y $p||\mathbb{G}|$, entonces el número s de p-subgrupos de Sylow es tal que $s \equiv 1 \pmod p$ y $s | |\mathbb{G}|$

PROPOSICION 1. Si $\mathbb{K} \triangleleft \mathbb{G}$ y $\mathbb{H} < \mathbb{G}$ entonces $(\mathbb{K} \cap \mathbb{H}) \triangleleft \mathbb{H}$.

DEMOSTRACION. Sea $\mathbb{M} = \mathbb{K} \cap \mathbb{H}$
considerando $m \in \mathbb{M}$, $h \in \mathbb{H}$, $\Rightarrow$ $m \in \mathbb{G}$, $h \in \mathbb{K}$

$m^{-1}hm \in \mathbb{K}$ $\quad (\mathbb{K} \triangleleft \mathbb{G})$

$m^{-1}hm \in \mathbb{H}$ $\quad \mathbb{H}$ es subgrupo

$\therefore$ $m^{-1}hm \in \mathbb{K} \cap \mathbb{H}$ ∎

Si $\mathbb{N} \triangleleft \mathbb{G}$ y $x \in \mathbb{G}$, $\mathbb{N}x = \{ nx \mid n \in \mathbb{N} \}$ se llama CLASE LATERAL DERECHA de $\mathbb{N}$ en $\mathbb{G}$.

Las clases laterales derechas de $\mathbb{N}$ en $\mathbb{G}$, forman una partición de $\mathbb{G}$.

Si $\mathbb{N} \triangleleft \mathbb{G}$, el producto de $\mathbb{N}x$ por $\mathbb{N}y$ es una clase lateral derecha, esto es, $\mathbb{N}x\mathbb{N}y = \mathbb{N}xy$.

$\mathbb{G}/\mathbb{N}$ es el conjunto de clases laterales derechas de $\mathbb{N}$ en $\mathbb{G}$.

$\mathbb{G}/\mathbb{N}$ es un grupo con el producto anterior de clases laterales.

Si $\mathbb{G}$ y $\mathbb{G}'$ son grupos, $f : \mathbb{G} \longrightarrow \mathbb{G}'$ es un HOMOMORFISMO, si para todo $x, y, \in \mathbb{G}$, $f(xy) = f(x)f(y)$.

NUCLEO de f = Núc $f = \{ x \in \mathbb{G} \mid f(x) = e \} = N$, $N \triangleleft \mathbb{G}$,
inversamente cada subgrupo $\mathbb{H} \triangleleft \mathbb{G}$ es el núcleo de un homomorfismo $\varphi : \mathbb{G} \longrightarrow \mathbb{G}/\mathbb{H}$, $\varphi(x) = \mathbb{H}x$, llamado el homomorfismo CANONICO.

Un homomorfismo φ de $\mathbb{G}$ sobre $\mathbb{G}'$ se dice que es un EPIMORFISMO.
Un homomorfismo φ de G en G' se dice ser ISOMORFISMO, si y sólo si φ es inyectivo y φ es sobre.

NOTACION. Si existe un isomorfismo de $\mathbb{G}$ en $\mathbb{G}'$ se dice que $\mathbb{G}$ y $\mathbb{G}'$ son ISOMORFOS y se escribe $\mathbb{G} \cong \mathbb{G}'$.

PRIMER TEOREMA DE ISOMORFISMO. Sea $\varphi : \mathbb{G} \longrightarrow \mathbb{G}'$ un homomorfismo con núcleo N y sea $\varphi_N : \mathbb{G} \longrightarrow \mathbb{G}/N$ el homomorfismo canónico. Entonces existe un único isomorfismo $\psi : \mathbb{G}/N \longrightarrow \varphi(\mathbb{G})$ tal que $\varphi(x) = (\psi\varphi_N)(x)$ para todo $x \in \mathbb{G}$.

SEGUNDO TEOREMA DE ISOMORFISMO. Sean $\mathcal{N}$ y $\mathcal{H}$ subgrupos de $\mathcal{G}$, tales que $\mathcal{N} \triangleleft \mathcal{G}$, entonces $(\mathcal{H} \cap \mathcal{N}) \triangleleft \mathcal{H}$, $\mathcal{HN}$ es un subgrupo de $\mathcal{G}$ y

$$\mathcal{H} / (\mathcal{H} \cap \mathcal{N}) \cong \mathcal{HN} / \mathcal{N} .$$

TERCER TEOREMA DE ISOMORFISMO. Si $\mathcal{H}/\mathcal{N}$ es un subgrupo normal de $\mathcal{G}/\mathcal{N}$ con $\mathcal{N} \leq \mathcal{H}$, entonces $\mathcal{N} \triangleleft \mathcal{G}$ y $\mathcal{G}/\mathcal{H} \cong (\mathcal{G}/\mathcal{N})/(\mathcal{H}/\mathcal{N})$.

La demostración de los resultados anteriores se pueden consultar en cualquiera de las referencias [4], [5], [6], [9] ó [10].

LOS GRUPOS ALTERNANTES An, SON SIMPLES NO ABELIANOS SI n ≥ 5.

DEFINICION. Una PERMUTACION σ sobre un conjunto finito C, es una función biyectiva $\sigma : C \longrightarrow C$.

DEFINICION. EL GRUPO SIMETRICO de orden n, es el grupo de permutaciones sobre un conjunto de n elementos, con la operación de composición.

DEFINICION. Un CICLO de longitud k, es una permutación σ, de un conjunto finito C, si existen $c_1, c_2, \ldots, c_k \in C$ tal que

$$\sigma(c_1) = c_2, \quad \sigma(c_2) = c_3, \ldots, \sigma(c_k) = c_1 \quad y$$

$\sigma(c) = c \ \forall c \in C - \{c_1, c_2, \ldots, c_k\}$.

Se escribirá $\sigma = (c_1, c_2, \ldots, c_k)$.

Cada permutación es un producto de ciclos ajenos.

DEFINICION. Una TRANSPOSICION, es un ciclo de longitud 2.

Cada ciclo es un producto de transposiciones.
Cada permutación es un producto de transposiciones.

DEFINICION. Una PERMUTACION ES PAR, si se puede expresar como el producto de un número par de transposiciones.

DEFINICION. El GRUPO ALTERNANTE An, es el grupo formado por las permutaciones pares sobre un conjunto de n elementos.

Ahora observando los primeros valores de n, se tiene : A_2, es el grupo formado por la identidad; A_3, es el grupo cíclico de orden primo 3, por tanto simple.
A_4 no es un grupo simple, contiene un subgrupo $\mathbb{N} \triangleleft A_4$, de orden 4,

$$\mathbb{N} = \{ e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \} .$$

La demostración de que A_n, es simple para $n \geq 5$ se desarrolla por inducción, primero se demuestra que A_5 es simple, después que A_n lo es para $n > 5$.

TEOREMA. A_5 es simple.

DEMOSTRACION. Supóngase que existe $\mathbb{N} \triangleleft A_5$, con

$$\mathbb{N} \neq A_5, \quad y \quad \mathbb{N} \neq \langle e \rangle$$

como $|A_5| = 60 = 2^2(3)(5)$,
los posibles órdenes para $\mathbb{N}$ son :
$|\mathbb{N}| = 30, 5, 10, 15, 20, 3, 6, 12, 2, ó\ 4.$

CASO 1. Considérese $\mathbb{N} \triangleleft A_5$, con $|\mathbb{N}| = 30$.

sea $\mathbb{B} = \{ \sigma \in A_5 \mid \sigma(x_i) = x_i \} < A_5$,

$\mathbb{B}$ es el grupo de permutaciones pares sobre un conjunto de cuatro elementos.
por la proposición 1, $\mathbb{N} \cap \mathbb{B} \triangleleft \mathbb{B}$
por el segundo teorema de isomorfismo,

$$\frac{\mathbb{B}}{\mathbb{B} \cap \mathbb{N}} \cong \frac{\mathbb{B}\mathbb{N}}{\mathbb{N}} \subset \frac{A_5}{\mathbb{N}} , \quad \text{como} \quad \left|\frac{A_5}{\mathbb{N}}\right| = 2,$$

entonces $|\mathbb{B} / (\mathbb{B} \cap \mathbb{N})| \leq 2$, es decir $\mathbb{N} = \mathbb{B}$ ó $|\mathbb{B} \cap \mathbb{N}| = 6$

ya que $\mathcal{N} \neq \mathbb{B}$, entonces $\mathbb{B} \cap \mathcal{N}$ es un subgrupo de orden 6 de $\mathbb{B}$, pero $\mathbb{B} \cong A_4$ y A_4 no tiene subgrupos de orden 6,

$\therefore \quad |\mathcal{N}| \neq 30$.

CASO 2. Si $|\mathcal{N}| = 5, 10, 15$ ó 20, entonces $5 \mid |\mathcal{N}|$,
Por el primer teorema de Sylow $\mathcal{N}$ contiene un subgrupo p_5 de orden 5 $\quad p_5 \subset \mathcal{N} \subset A_5$

sea $a \in A_5$, $\quad a^{-1}p_5a \subset a^{-1}\mathcal{N}a = \mathcal{N}$
como todos los p-subgrupos de Sylow son conjugados, $\mathcal{N}$ contiene todos los 5-subgrupos de Sylow de A_5, en particular $\mathcal{N}$ debe contener todos los ciclos de orden 5 de A_5, pero éstos son 24, es decir $|\mathcal{N}| \geq 24$
contradiciendo que $|\mathcal{N}| = 5, 10, 15$ ó 20
por lo tanto $|\mathcal{N}| \neq 5, 10, 15$ y 20.

CASO 3. Si $|\mathcal{N}| = 3, 6$ ó 12, entonces $3 \mid |\mathcal{N}|$,
Por el primer teorema de Sylow $\mathcal{N}$ tiene un subgrupo p_3 de orden 3

$$p_3 \subset \mathcal{N} \subset A_5$$

sea $a \in A_5$, $\quad a^{-1}p_3a \subset a^{-1}\mathcal{N}a = \mathcal{N}$
$\mathcal{N}$ contiene a todos los 3-subgrupos de Sylow de A_5, ya que son conjugados.
$\mathcal{N}$ contiene todos los ciclos de longitud 3, que son 20, es decir $|\mathcal{N}| \geq 21$, contradicción.
$\therefore \quad |\mathcal{N}| \neq 3, 6$ y 12.

CASO 4. $|\mathcal{N}| = 4$

$\mathcal{V} = \{ e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}$ es un subgrupo de A_5 de orden 4.
$\mathcal{V}$ no es normal en A_5, porque si $\sigma = (1,5,2) \in A_5$

$$(1,5,2)(1,2)(3,4)(1,2,5) = (2,5)(3,4) \notin \mathcal{V}$$

por el segundo teorema de Sylow todos los subgrupos de orden 4 de A_5 son isomorfos a $\mathcal{V}$ y por consiguiente ninguno de ellos es normal en A_5.

$\therefore \quad |\mathcal{N}| \neq 4$.

CASO 5. $|H| = 2$

Si H es un subgrupo de orden 2, H debe estar formado por la identidad y por una permutación equivalente a (1,2)(3,4), pero (1,5,2)(1,2)(3,4)(1,2,5) = (2,5)(3,4) lo que implica que H no es normal en A_5.

Por tanto A_5 no contiene subgrupos normales de orden dos.

Se sigue que A_5 es simple. ∎

NOTACION. $\langle G, S \rangle$, denota el subgrupo generado por $G \cup S$.

PROPOSICION 2. Si $G, S \leq S_n$, $\quad [\, G : G \cap S \,] \leq [\, \langle G, S \rangle : S \,]$.

DEMOSTRACION. Sea $G \cap S = J$, es subgrupo de G,

sea $G = Je \cup Jx_2 \cup \dots \cup Jx_r$, con $J, Jx_2, \dots, Jx_r$

las diferentes clases laterales de J en G,

entonces las clases laterales $Je, Jx_2, \dots, Jx_r$ son diferentes clases laterales de J en $\langle G, J \rangle$.

Pues si $Jx_i = Jx_j$ $j \neq i$, entonces $x_i = kx_j$ con $k \in J$

pero $x_i, x_j \in G$, por lo que $k \in G$, y $k \in G \cap S = J$

luego Jx_i, Jx_j tienen un elemento en común $x_i = kx_j$,

contradiciendo el hecho de que Jx_i, Jx_j son ajenas.

Por lo tanto, existen al menos tantas clases laterales diferentes de J en $\langle S, G \rangle$ como las hay de $G \cap S$ en G, esto es,

$$[\, \langle G, J \rangle : J \,] \geq [\, G : G \cap S \,] \quad ∎$$

TEOREMA. A_n es simple, para $n > 5$.

DEMOSTRACION. Sea $H \lhd A_n$, $\quad \langle e \rangle \neq H \neq A_n$

sea i, $\quad 1 \leq i \leq n$.

considérese $\quad A_{n-1} = \{ \sigma \in A_n \mid \sigma(i) = i \} \leq A_n$

A_{n-1} es el grupo de permutaciones pares sobre el conjunto $\{ 1, 2, \dots, i-1, i+1, \dots, n \}$ con $n-1$ objetos.

$5 \leq (n-1) < n$ y por hipótesis de inducción $A_{n-1}^{(1)}$ es simple.

por la proposición 1, $\mathfrak{N} \cap A_{n-1}^{(1)} \triangleleft A_{n-1}^{(1)}$

por lo tanto $\mathfrak{N} \cap A_{n-1}^{(1)} = A_{n-1}^{(1)}$ ó $\mathfrak{N} \cap A_{n-1}^{(1)} = \langle e \rangle$.

CASO 1. Si $A_{n-1}^{(1)} = \mathfrak{N} \cap A_{n-1}^{(1)} \subset \mathfrak{N}$

sea $i \neq 1$, $\psi \in A_n$ tal que

$\psi(1) = i$, entonces $\psi^{-1} A_{n-1}^{(1)} \psi = A_{n-1}^{(i)}$

luego $A_{n-1}^{(i)} = \psi^{-1} A_{n-1}^{(1)} \psi \subset \psi^{-1} \mathfrak{N} \psi = \mathfrak{N}$ para todo $i \neq 1$

por lo tanto

$$\langle A_{n-1}^{(1)}, A_{n-1}^{(1)} \rangle \subset \mathfrak{N} \quad \Rightarrow$$

$$\frac{\langle A_{n-1}^{(i)}, A_{n-1}^{(i)} \rangle}{A_{n-1}^{(i)}} \subset \frac{\mathfrak{N}}{A_{n-1}^{(i)}}$$

de aquí $\left[\langle A_{n-1}^{(i)}, A_{n-1}^{(i)} \rangle : A_{n-1}^{(i)} \right] \leq \left[\mathfrak{N} : A_{n-1}^{(i)} \right]$

por otra parte $A_{n-1}^{(i)} \cap A_{n-1}^{(1)} = A_{n-2}^{(1,i)}$ es el grupo de permutaciones pares de n-2 elementos,
y el orden de los grupos alternantes es :

$$\left| A_{n-2}^{(1,i)} \right| = \tfrac{1}{2} (n-2)! \qquad \left| A_{n-1}^{(i)} \right| = \tfrac{1}{2} (n-1)!$$

que al considerar el índice

$$\left[A_{n-1}^{(i)} : A_{n-1}^{(1)} \cap A_{n-1}^{(i)} \right] = \left[A_{n-1}^{(i)} : A_{n-2}^{(1,i)} \right] = \frac{\frac{1}{2}(n-1)!}{\frac{1}{2}(n-2)!} = n-1$$

y aplicando la proposición 2 a $A_{n-1}^{(i)}$, $A_{n-1}^{(j)}$, se tiene :

$$\left[A_{n-1}^{(i)} : A_{n-1}^{(i)} \cap A_{n-1}^{(j)}\right] \leq \left[\langle A_{n-1}^{(i)}, A_{n-1}^{(j)}\rangle : A_{n-1}^{(j)}\right] \leq \left[\mathbb{N} : A_{n-1}^{(j)}\right]$$

$$n-1 \leq \left[\mathbb{N} : A_{n-1}^{(j)}\right]$$

como $A_{n-1}^{(i)} \subset \mathbb{N} \subset A_n$, $\quad n = \left[A_n : A_{n-1}^{(i)}\right] = \left[A_n : \mathbb{N}\right]\left[\mathbb{N} : A_{n-1}^{(i)}\right]$

se sigue que $\left[\mathbb{N} : A_{n-1}^{(i)}\right] | n$, $\quad \therefore \quad \left[\mathbb{N} : A_{n-1}^{(i)}\right] \leq n$

$$\left[\mathbb{N} : A_{n-1}^{(i)}\right] = n$$

entonces $[A_n : \mathbb{N}] = 1$ por consiguiente, $\mathbb{N} = A_n$.
Contradicción.
Es decir, no puede suceder que $A_{n-1}^{(i)} \cap \mathbb{N} = A_{n-1}^{(i)}$.

CASO 2. Supóngase $\mathbb{N} \cap A_{n-1}^{(i)} = \langle e\rangle$
(esto es, si $e \neq \sigma \in \mathbb{N}$, entonces $\sigma(i) \neq i$)
sea $\psi \in A_n$, tal que $\psi(i) = j$, $\quad i \neq j$

$\langle e\rangle = \psi(\mathbb{N} \cap A_{n-1}^{(i)})\psi^{-1} = \langle \psi\, \mathbb{N}\, \psi^{-1}\rangle \cap \langle \psi A_{n-1}^{(i)} \psi^{-1}\rangle = \mathbb{N} \cap A_{n-1}^{(j)}$
es decir, si $\sigma \in \mathbb{N}$, $\sigma \neq e$, entonces σ no fija ningún elemento.
Supóngase $\mathbb{N} \neq \langle e\rangle$, sea $e \neq \varphi \in \mathbb{N}$, con
$\varphi(i) = j \quad j \neq i$
$\varphi(h) = k \quad h \neq i, \quad h \neq j$
sean $l, m \neq i, j, h, k$, tales elementos existen porque $n \geq 6$
$\psi = (h, l, m) = (h, l)(h, m) \in A_n$ y

se tiene que $\psi \varphi \psi^{-1}(i) = \psi \varphi(i) = \psi(j) = j$
$\psi \varphi \psi^{-1}(l) = \psi \varphi(h) = \psi(k) = k$

además $(\varphi^{-1})(\psi \varphi \psi^{-1}) \in \mathbb{N}$ porque $\mathbb{N} \triangleleft A_n$

y $\quad \varphi^{-1}\psi\ \varphi\ \psi^{-1}(1) = \varphi^{-1}\psi\ \varphi(1) = \varphi^{-1}\psi(j) = \varphi^{-1}(j) = i$

$\varphi^{-1}\psi\ \varphi\ \psi^{-1}(1) = \varphi^{-1}\psi\ \varphi(h) = \varphi^{-1}\psi(k) = \varphi^{-1}(k) = h$

es decir, $\varphi^{-1}\psi\ \varphi\ \psi^{-1}$ es un elemento que deja fijo a un elemento i, e $\varphi^{-1}\psi\ \varphi\ \psi^{-1}$ es diferente de la identidad por enviar 1 en h.

Contradiciendo $\langle e \rangle \neq \mathbb{N} \cap A_{n-1}^{(1)}$

Por lo tanto $\mathbb{N} = \langle e \rangle$ y A_n es simple. ∎

LOS GRUPOS LINEALES ESPECIALES PROYECTIVOS PSL(n,F).

INTRODUCCION

Sea F un campo, V un F-espacio vectorial de dimensión n, GL(n,F) es el grupo de transformaciones lineales invertibles de V en V, denominado GRUPO LINEAL GENERAL DE ORDEN n sobre F, es decir GL(n,F) es el grupo de automorfismos de V en V, con la operación de composición.

La función Det : $GL(n,F) \longmapsto F^* = F-\{0\}$ es un epimorfismo y por el primer teorema de isomorfismo se tiene que

$$\frac{GL(n,F)}{N(Det)} \cong F^*, \qquad \text{con } N(Det) = \text{Núcleo de Det.}$$

El núcleo N de la función determinante son las transformaciones lineales de V en V cuyo determinante es 1 y se le denomina el GRUPO LINEAL ESPECIAL SL(n,F).

DEFINICION. Sea G un grupo, el CENTRO Z de G, está definido como el subgrupo $Z = \{ z \in G \mid zx = xz \quad \forall x \in G \}$.

Ahora se hará ver que el centro del grupo lineal general está formado por las matrices escalares, esto es por las matrices de la forma aE, con $a \in F^*$ y E la matriz identidad de n x n.

TEOREMA 1. El centro del grupo lineal general $GL(n,F)$, $Z = Z(GL(n,F))$, está formado por las matrices escalares.

DEMOSTRACION. Sea $T = \{ aE \mid a \in F^{\circ} \}$, es inmediato que $T \subset Z$, se demostrará que $Z \subset T$.
Sea $\{ v_1, v_2, \ldots, v_n \}$ base de V,

$X \in Z$ tal que $X(v_i) = \sum_{k=1}^{n} c_{ki} v_{ki}$ $\quad 1 \leq i \leq n$,

y $A \in SL(n,F)$ tal que
$A(v_j) = v_i + v_j$, $i \neq j$,
$A(v_k) = v_k$ si $k \neq j$,
si $i \neq j$ $XA(v_i) = X(v_i)$ y

$$AX(v_i) = A\left(\sum_{k=1}^{n} c_{ki} v_{ki}\right) = \sum_{k=1}^{n} c_{ki} A(v_k)$$

$$= \sum_{k=1}^{n} c_{ki} v_k + c_{ji} v_i = X(v_i) + c_{ji} v_i$$

como $XA = AX$, entonces $c_{ji} = 0$, si $j \neq i$,
$\therefore$ X es diagonal, $X(v_i) = c_{ii} v_i$.
Además $XA(v_j) = X(v_i + v_j) = X(v_i) + X(v_j) = c_{ii} v_i + c_{jj} v_j$,
$AX(v_j) = A(c_{jj} v_j) = c_{jj} A(v_j) = c_{jj}(v_i + v_j)$
$\therefore$ $c_{ii} = c_{jj}$.
Por lo tanto si X conmuta con la transversión A, implica que X es escalar. ■

TEOREMA 2. El centro del grupo lineal especial es $Z \cap SL(n,F)$.

DEMOSTRACION. Inmediato del anterior.

DEFINICION. Al grupo cociente $SL(n,F) / Z \cap SL(n,F)$, se le denomina el GRUPO LINEAL ESPECIAL PROYECTIVO, y se denota por $PSL(n,F)$.

$$PSL(n,F) = \frac{SL(n,F)}{Z \cap SL(n,F)}$$

Si F es un campo finito con $q = p^n$ elementos (p primo), se escribirá GL(n,q), SL(n,q), PSL(n,q), en cada caso respectivamente .

TEOREMA 3. Si $|F| = q = p^n$, entonces

i) $|GL(n,q)| = (q^n-1)(q^n-q) \dots (q^n-q^{n-2})(q^n-q^{n-1})$

ii) $|SL(n,q)| = (q^n-1)(q^n-q) \dots (q^n-q^{n-2})q^{n-1}$

iii) $|PSL(n,q)| = (1/d)|SL(n,q)|$, $d = (n,q-1)$.

DEMOSTRACION.

i) Sea $\alpha = \{ \alpha_1, \alpha_2, \dots, \alpha_n \}$ una base ordenada de V. sea $A \in GL(n,q)$, $\rightarrow$ $\{ A\alpha_1, A\alpha_2, \dots, A\alpha_n \}$ es base ordenada de V, es decir a cada $A \in GL(n,q)$ se le asocia una base $(A(\alpha))$. Inversamente si $\beta = \{\beta_1, \beta_2, \dots, \beta_n\}$ es una base ordenada de V, existe una única $A \in GL(n,q)$ tal que $A(\alpha_i) = \beta_i$.
Esto muestra que hay una biyección de GL(n,q) en el conjunto de bases ordenadas de V .

$\therefore$ $|GL(n,q)|$ = número de base ordenadas de V.
= número de bases ordenadas de $F^n \cong V$.

$|F| = q$, implica que existen q^n vectores distintos en V.
Así para seleccionar β_1 hay q^n-1 formas. Una vez seleccionado β_1, para escoger β_2, no debe estar en el subespacio generado por β_1, y se puede escoger de q^n-q formas.
De esta forma teniendo seleccionados a $\{ \beta_1, \dots, \beta_i \}$, la restricción para β_{i+1} es que no esté en el subespacio generado por $\{ \beta_1, \dots, \beta_i \}$, entonces hay q^n-q^i formas de escoger β_{i+1}.
En consecuencia se tienen $(q^n-1)(q^n-q) \dots (q^n-q^{n-1})$ bases ordenadas de V y

$$|GL(n,q)| = (q^n-1)(q^n-q) \dots (q^n-q^{n-1}) .$$

ii) $$\frac{GL(n,q)}{N(\det)} \cong F^* ,$$

$$\frac{|GL(n,q)|}{|SL(n,q)|} = |F^*| = q - 1$$

Porque el grupo multiplicativo de un campo de q elementos, es el grupo cíclico de q-1 elementos.

$$\therefore \quad |SL(n,q)| = \frac{|GL(n,q)|}{q - 1}$$

y por i), $|SL(n,q)| = (1/q-1)(q^n-1)(q^n-q) \dots (q^n-q^{n-2})(q^n-q^{n-1})$
$= (q^n-1)(q^n-q) \dots (q^n-q^{n-2})q^{n-1}$

iii) $Z(SL(n,q)) = \{ G \mid G \in Z(GL(n,q)) \text{ y } \det G = 1 \}$,
de donde se sigue que el orden de $Z(SL(n,q))$ es el número de soluciones de la ecuación $\alpha^n = 1$ en F^*.
Por otro lado los elementos de F^* forman un grupo cíclico de orden q-1, y todos ellos satisfacen $x^{q-1} = 1$
Sea $d = (n, q-1)$, existen enteros r, s tales que $d = nr + (q-1)s$,

$$\alpha^d = \alpha^{nr+(q-1)s} = (\alpha^{nr})(\alpha^{(q-1)s}) = \alpha^{nr} = (\alpha^n)^r$$

$$\therefore \quad \alpha^d = 1 \iff \alpha^r = 1 \qquad \text{porque } n = dt,\ t \in \mathbb{Z}.$$

por lo tanto basta encontrar el número de soluciones de la ecuación $\alpha^d = 1$, con $d = (n, q-1)$.
Como $x^{q-1}-1$ tiene q-1 raíces diferentes en F, a saber todos los elementos de F^*, $x^{q-1}-1$ se descompone en q-1 factores lineales diferentes.
El polinomio x^d-1 divide a $x^{q-1}-1$, lo que implica que x^d-1 se descompone en d diferentes factores lineales, lo que quiere decir que el orden de $Z(SL(n,q))$ es d.
Así,

$$|PSL(n,q)| = \frac{|SL(n,q)|}{|Z(SL(n,q)|} = \frac{|SL(n,q)|}{d} \qquad \text{con } d = (n, q-1)$$

∎

En lo subsecuente se considera la simplicidad de PSL(n,q), con (n,q) ≠ (2,2) y (n,q) ≠ (2,3), para lo cual se introducen los elementos necesarios.

Sea V un espacio vectorial de dimensión n, sobre el campo finito F. Un HIPERPLANO H de V, es un subespacio de V, de dimensión n-1.

DEFINICION. Una TRANSVERSION de V según el hiperplano H, es una función lineal $T : V \longmapsto V$ tal que
i) $T(v) = v$ para todo $v \in H$
ii) $T(v)-v \in H$ para todo $v \in V$.

DEFINICION. Sea V un F-espacio vectorial, el ESPACIO DUAL V^* de V es el espacio vectorial de la transformaciones lineales, $\mu : V \longmapsto F$, llamadas funcionales .

LEMA 1. Sea T una transversión diferente de la identidad E, según el hiperplano H y sea $\mu \in V^*$ una funcional lineal de V, con H = Núcleo de μ, entonces existe $0 \neq a \in H$ tal que
$T(v) = v-\mu(v)a$, para todo $v \in V$.
Inversamente, si $\mu \in V^*$, $\mu \neq 0$ con $0 \neq a \in V$ y $\mu(a) = 0$, entonces existe una transversión $T : V \longmapsto V$ según H = Núc μ tal que $T(v) = v-\mu(v)a$.

DEMOSTRACION.
$\Rightarrow$) $V = H \oplus \langle w \rangle$ con $\mu(w) = 1$ para algún $w \in V$
sea $a = w-T(w)$, $a \in H$ por def. de transversión
$a \neq 0$, ya que si $a = 0$ $T(w) = w$ $\Rightarrow$ $T = E$ contradicción.
sea $v \in V$, $\Rightarrow$ $v = h + cw$ con $h \in H = Núc\ \mu$.
$\mu(v) = \mu(h) + c\mu(w) = 0 + c.1 = c$
así, $T(v) = T(h) + cT(w) = h + \mu(v)T(w)$
$= h + \mu(v)(w-a)$
$= h + \mu(v)w - \mu(v)a$
$= h + cw - \mu(v)a = v - \mu(v)a$.

⇒) Sea $T : V \longrightarrow V$ tal que $T(v) = v - \mu(v)a$
como $\mu \in V^*$, $\mu \neq 0$ y $0 \neq a \in H = \text{Núc } \mu$, T es lineal .
Si $v \in H = \text{Núc } \mu$, entonces $T(v) = v$,
además $T(v) - v = \mu(v)a \in H$, $\forall\, v \in V$,
por lo tanto T es transversión de V según el hiperplano H . ∎

Si T es una transversión según el hiperplano H y $\mu \in V^*$ con $H = \text{Núc } \mu$ y $0 \neq a \in H$, se escribirá $T = (\mu, a)$.

LEMA 2. Sea H un hiperplano de V y $0 \neq \mu \in V^*$ tal que $\text{Núc } \mu = H$. Si μ' es otra funcional lineal de V con $\text{Núc } \mu' = H$, entonces $\mu' = \sigma\mu$, $\sigma \in F$.

DEMOSTRACION. Sea $V = H \oplus \langle w \rangle$, $w \in V$, tal que $\mu(w) \neq 0$, entonces si $\alpha = \mu'(w)/\mu(w)$, sea $h = \mu' - \alpha\mu$, la funcional lineal sobre V,
Si $v \in \text{Núc } \mu$, $h(v) = \mu'(v) - \alpha\mu(v) = 0$, porque $H = \text{Núc } \mu'$,
además $h(w) = \mu'(w) - \alpha\mu(w) = 0$
es decir h es cero en $V = H \oplus \langle w \rangle$
$\therefore \quad h = 0$
$\therefore \quad \mu' = \alpha\mu$. ∎

LEMA 3. Sea H un hiperplano de V y $T(\mu, a) \neq E$ una transversión de V según H, si $T = T(\mu' , a')$, entonces $\mu' = \alpha\mu$ y $a' = \alpha^{-1}a$.

DEMOSTRACION.
$T(v) = v - \mu'(v)a'$, $\quad T(v) = v - \mu(v)a$
entonces, $\mu'(v)a' = \mu(v)a$
y por el lema anterior $\alpha\mu(v)a' = \mu(v)a$
luego $\mu(v)(\alpha a' - a) = 0 \quad \Rightarrow \quad a = \alpha a'$ ∎

LEMA 4. Sea H un hiperplano de V, $\mu, \mu' \in V^*$ tales que

Núc μ = Núc μ' = H,

Si $\mathcal{T} = \{T(\mu, a) \mid a \in H\}$ y $\mathcal{T}' = \{T(\mu', a) \mid a \in H\}$

entonces $\mathcal{T} = \mathcal{T}'$

DEMOSTRACION. Sea $T(\mu, a) \in \mathcal{T}$

como $\mu' = \alpha\mu$ para algún $\alpha \in F$, $\Rightarrow T(\mu, a) = T(\mu', \alpha^{-1}a) \in \mathcal{T}'$.

Inversamente, $T(\mu', a) = T(\mu, \alpha a) \in \mathcal{T}$

$\therefore \quad \mathcal{T} = \mathcal{T}'$. ∎

LEMA 5.

i) $T(\mu, a_2)\cdot T(\mu, a_1) = T(\mu, a_1+a_2)$, $\qquad a_1, a_2 \in H$.

ii) $T(\mu, a)\cdot T(\mu, -a) = T(\mu, 0) = E$.

DEMOSTRACION.

i) $[T(\mu, a_2)\cdot T(\mu, a_1)](v) = T(\mu, a_2)(v-\mu(v)a_1)$

$= v-\mu(v)a_1 - \mu(v - \mu(v)a_1)a_2$

$= v-\mu(v)a_1 - (\mu(v) - \mu(v)\mu(a_1))a_2$

$= v-\mu(v)a_1 - \mu(v)a_2$, $\qquad \mu(a_1) = 0$

$= v-\mu(v)(a_1+a_2)$

$= T(\mu, a_1+a_2)$.

ii) $T(\mu, a)\cdot T(\mu, -a) = T(\mu, a-a) = T(\mu, 0)$. ∎

Si H es un hiperplano de V y $\mu \in V^*$ tal que H = Núc μ, entonces

$$\mathcal{T}(H) = \{ T(\mu, a) \mid a \in H \}$$

es el conjunto de todas las transversiones de V según H .

Del resultado anterior se desprende que $\mathcal{T}(H)$ es un grupo abeliano, además isomorfo a H, en efecto :

Sea $\varphi : H \longrightarrow \mathcal{T}$ tal que $\varphi(a) = T(\mu, a)$, se tiene

$\varphi(a_1+a_2) = T(\mu, a_1+a_2) = T(\mu, a_1)\cdot T(\mu, a_2) = \varphi(a_1)\varphi(a_2)$

luego φ es homomorfismo.

Sea T una transversión de V según H, por el lema 1, existe
$a \in \text{Núc } \mu = H$ con $\mu \in V^{\circ}$ tal que $T(v) = v - \mu(v)a \quad \forall a$
es decir φ es sobre.
Sea $a \in \text{Núc } \varphi$, $\Rightarrow \quad \varphi(a) = E = T(\mu, a)$
$T(u, a)(v) = v$ para todo $v \in V$
$= v - \mu(v)a$, de donde se tiene que
$\mu(v)a = 0$ para todo $v \in V$, $\therefore \quad a = 0$
así, φ es inyectiva,
de donde se sigue que φ es un isomorfismo de H a $\tilde{z}$.

LEMA 6. Sea $a \in V$, $\mu_1, \mu_2 \in V^{*}$ con $a \in \text{Núc } \mu_1 \cap \text{Núc } \mu_2$, entonces $T(\mu_1, a) \cdot T(\mu_2, a) = T(\mu_1 + \mu_2, a)$.

DEMOSTRACION.

$$
\begin{aligned}
[T(\mu_1, a) \cdot T(\mu_2, a)](v) &= [T(\mu_1, a)](v - \mu_2(v)a) \\
&= v - \mu_2(v)a - \mu_1(v - \mu_2(v)a)a \\
&= v - \mu_2(v)a - (\mu_1(v) - \mu_2(v)\mu_1(a))a \\
&= v - \mu_2(v)a - \mu_1(v)a \quad \text{porque } \mu_1(a) = 0 \\
&= v - (\mu_2(v) + \mu_1(v))a \\
&= v - (\mu_2 + \mu_1)(v)a = T(\mu_2 + \mu_1, a). \quad \blacksquare
\end{aligned}
$$

Considérese $\mathcal{T}_a = \{ T(\mu, a) \mid \mu \in V^{*} \text{ y } \mu(a) = 0 \}$, por el lema 6, dado $T(\mu, a)$ su inverso es $T(-\mu, a)$ y el elemento neutro es $T(\mu_{\phi}, a)$ donde μ_{ϕ} es la funcional nula, así se tiene :

LEMA 7. $\mathcal{T}_a$ es un subgrupo de GL(n,q).

LEMA 8. Si T es una transversión, entonces $T \in SL(n,q)$.

DEMOSTRACION. Sea T una transversión,
y $\beta = \{ \beta_1, \beta_2, \ldots, \beta_{n-1} \}$ una base de H .
si $w \in H$, $\beta' = \{ \beta_1, \beta_2, \ldots, \beta_{n-1}, w \}$ es base de V
$T(\beta_i) = \beta_i$ para $1 \leq i \leq n-1$

$T(w)-w \in H \quad \Rightarrow$

$$T(w)-w = \sum_{i=1}^{n-1} a_i\beta_i, \qquad T(w) = w + \sum_{i=1}^{n-1} a_i\beta_i$$

$$[T]_\beta = \begin{bmatrix} 1\,0 \dots a_1 \\ 0\,1 \dots a_2 \\ \dots\dots\dots \\ 0\,0 \dots 1 \end{bmatrix} \qquad \text{y} \qquad \det [T]_\beta = 1$$

por lo tanto $T \in SL(n,q)$. ■

LEMA 9. Sea $\mathcal{T}$ el subgrupo de $SL(n,q)$ generado por las transversiones, entonces $\mathcal{T}$ es normal en $GL(n,q)$.

DEMOSTRACION. Sea T una transversión de V según H y $G \in GL(n,q)$

$$\begin{aligned} (GTG^{-1})(v) &= (GT)(G^{-1}(v)) \\ &= G[\,G^{-1}(v) - \mu(G^{-1}(v))a\,] \qquad \text{con } H = \text{Núc } \mu,\ a \in H \\ &= v-\mu(G^{-1}(v))G(a) \\ &= v-(\mu G^{-1})(v)G(a) \end{aligned}$$

$GTG^{-1} = T'(\mu G^{-1}, G(a))$ es transversión según Núc μG^{-1}, basta ver que $G(a) \in$ Núc μG^{-1},

pero $\mu G^{-1}(G(a)) = \mu(a) = 0$. ■

TEOREMA 4. Las transversiones generan a $SL(n,q)$.

DEMOSTRACION. La demostración se hará por inducción sobre n .

Primero se demostrará que para todo $G \in SL(n,q)$,
existe $X \in \mathcal{T}G$ tal que $X(v_1) = v_1$ con $0 \neq v_1 \in V$.
sea $0 \neq v \in V$ y sea $v' = G(v)$, $v' \neq 0$

Caso 1. Supóngase que v, v' son linealmente independientes
entonces v', v'-v también lo son.
sea $\mu \in V^*$ tal que $\mu(v') = 1$, $\mu(v'-v) = 0$
considérese $T = T(\mu, v'-v)$, así
$(TG)(v) = T(v') = v'-\mu(v')(v'-v) = v'-(v'-v) = v$

es decir $TG = X \in \mathcal{T}G$ y $X(v) = v$.

Caso 2. Supóngase que v, $v'-v$ son linealmente dependientes
entonces v, v' lo son , $G(v) = v' = cv$.
sea $w \in V$ con $w \notin \langle v \rangle$ y
sea $\mu' \in V^*$ con $\mu'(v) = 1$, $\mu'(w) = 0$
considérese $T' = T(\mu', w)$, se tiene que
$GT'(v) = G(v - \mu'(v)w) = G(v-w)$
v, $v-w$ linealmente independientes, G inyectiva, implican que $G(v)$ y $G(v-w)$ son linealmente independientes.
Es decir, $GT'(v) = G(v-w) \notin \langle v \rangle$, lo cual lleva al primer caso, por lo tanto existe $X \in \mathcal{T}GT'$ tal que $X(v) = v$ para algún $0 \neq v \in V$.
luego $X \in \mathcal{T}GT' = \mathcal{T}T''G$ para algún T'' pues $\mathcal{T} \triangleleft GL(n,F)$
$\therefore \quad X \in \mathcal{T}\,T''G = \mathcal{T}G$

Ahora considerando $\overline{V} = V/\langle v_1 \rangle$, donde $X(v_1) = v_1$, X induce una transformación lineal $\overline{X} : \overline{V} \longmapsto \overline{V}$ definida por

$$\overline{X}(\, v + \langle v_1 \rangle \,) = X(v) + \langle v_1 \rangle$$

sea $\beta = \{ v_1, v_2, \ldots, v_n \}$ una base de V ,
entonces $\{ v_2 + \langle v_1 \rangle, v_3 + \langle v_1 \rangle, \ldots, v_n + \langle v_1 \rangle \}$ es base de $V/\langle v_1 \rangle$

y $\dim V/\langle v_1 \rangle = n-1$

$$[X]_\beta = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ 0 & a_{n2} & \vdots & a_{nn} \end{bmatrix}$$

$1 = \det X = 1.\det \overline{X}$ y $\overline{X} \in SL(n-1,q)$.

Si $n = 2$, $\dim \overline{V} = 1$ y $\overline{X} = \overline{E}$ ya que $\det \overline{X} = 1$

además $\overline{X}(v + \langle v_1 \rangle) = X(v) + \langle v_1 \rangle = v + \langle v_1 \rangle$

$\Rightarrow \quad X(v) - v \in \langle v_1 \rangle$

es decir, X es transversión según el hiperplano $\langle v_1 \rangle$

como $X \in \mathcal{T}G$, $X = (\prod_i T)G$, $T_i \in \mathcal{T}$
luego, como X es transversión, entonces G es producto de transversiones.

Sea $n > 2$, $\bar{X} \in SL(n-1, q)$ y supóngase que

$$\bar{X} = \prod_{i=1}^{k} \bar{T}(\bar{\mu}_i, \bar{w}_i) \qquad \text{con } \bar{\mu}_i \in \bar{V}^* \text{ y } \bar{\mu}_i(\bar{w}_i) = 0$$

sea $\Pi : V \longrightarrow \bar{V}$, $\Pi(v) = v + \langle v_1 \rangle$ el homomorfismo canónico.

y sea $w_i \in V$ tal que $\Pi(w_i) = \bar{w}_i$
definiendo $\mu_i \in V^*$ tal que

$$\mu_i(v_1) = 0, \quad \mu_i(v_j) = \bar{\mu}_i(\bar{v}_j) \quad j = 2, 3, \ldots, n \quad i = 1, 2, \ldots, n$$

si $v \in V$,

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \qquad \bar{v} = \alpha_2 \bar{v}_2 + \alpha_3 \bar{v}_3 + \ldots + \alpha_n \bar{v}_n$$

$$\mu_i(v) = \alpha_1 \mu_i(v_1) + \alpha_2 \mu_i(v_2) + \ldots + \alpha_n \mu_i(v_n)$$

$$= 0 + \alpha_2 \bar{\mu}_i(\bar{v}_2) + \ldots + \alpha_n \bar{\mu}_i(\bar{v}_n)$$

$$= \bar{\mu}_i(\alpha_2 \bar{v}_2 + \ldots + \alpha_n \bar{v}_n) = \bar{\mu}_i(\bar{v})$$

esto es, para todo $v \in V$ se tiene que $\mu_i(v) = \bar{\mu}_i(\bar{v})$
y $\mu_i(w_i) = \bar{\mu}_i(\bar{w}_i) = 0$,
$\therefore$ μ_i, w_i, definen una transversión $T(\mu_i, w_i)$.

sea $K = \left(\prod_i T(\mu_i, w_i) \right)^{-1} X$, como

$T(\mu_i, w_i)(v_i) = v_i - \mu_i(v_i)w_i = v_i + 0 = v_i$ para todo i.

y $X(v_i) = v_i$
se tiene $K(v_i) = \left(\prod_i T(\mu_i, w_i) \right)^{-1} X(v_i) = v_i$ (*)
ahora

$$\bar{T}(\bar{\mu}_i, \bar{w}_i)(\bar{v}) = \bar{v} - \bar{\mu}_i(\bar{v})\bar{w}_i$$

$$= \bar{v} - \mu_i(v)\bar{w}_i = \overline{v - \mu_i(v)w_i}$$

$$= \overline{T(\mu_i, w_i)v}$$

por lo tanto $\prod_i \overline{T}(\overline{\mu}_i, \overline{w}_i)(\overline{v}) = \prod_i \overline{T(\mu_i, w_i)(v)}$

es decir $\overline{X}(\overline{v}) = \prod_i \overline{T(\mu_i, w_i)(v)} = \prod_i T(\mu_i, w_i)(v) + \langle v_1 \rangle$

por definición de $\overline{X}$, $X(v) + \langle v_1 \rangle = \overline{X}(\overline{v}) = \prod_i \overline{T}(\overline{\mu}_i, \overline{w}_i)(\overline{v})$,

entonces $X(v) + \langle v_1 \rangle = \prod_i T(\mu_i, w_i)(v) + \langle v_1 \rangle$

$\therefore$ $X(v) - \prod_i T(\mu_i, w_i)(v) \in \langle v_1 \rangle$

ó $X(v) = \prod_i T(\mu_i, w_i)(v) + cv_1$ para algún $c \in F$,

de modo que

$$K(v) = \left(\prod_i T(\mu_i, w_i) \right)^{-1} X(v)$$

$$= \left(\prod_i T(\mu_i, w_i) \right)^{-1} \left(\prod_i T(\mu_i, w_i)(v) + cv_1 \right)$$

$$= \left(\prod_i T(\mu_i, w_i) \right)^{-1} \left(\prod_i T(\mu_i, w_i) \right)(v) + \left(\prod_i T^{-1}(\mu_i, w_i) \right)(cv_1)$$

$$= v + cv_1$$

de aquí $K(v) - v \in \langle v_1 \rangle$

$\beta = \{v_1, v_2, \ldots, v_n\}$ es base de V, y $X(v_1) = v_1$

y por lo anterior $K(v_1) = v_1 - a_1 v_1$ y $K(v_1) = v_1$

considerando ahora, una base dual de β,

$$\beta^* = \{\rho_1, \rho_2, \ldots, \rho_n\}$$

$$\rho_i(v_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

$T(\rho_j, a_j v_1)(v_i) = v_i - \rho_j(v_i) a_j v_1 = v_i - \delta_{ij} a_j v_1$ donde $\delta_{ij} = 0,1.$

$$\prod_{j=2}^{n} T(\rho_j, a_j v_1)(v_i) = \left(\prod_{j>i} T(\rho_j, a_j v_1)\right) T(\rho_i, a_i v_1) \left(\prod_{j<i} T(\rho_j, a_j v_1)\right)(v_i)$$

$$= \prod_{j>i} T(\rho_j, a_j v_1) T(\rho_i, a_i v_1)(v_i)$$

$$= \left(\prod_{j>i} T(\rho_j, a_j v_1)\right)(v_i - \rho_i(v_i) a_i v_1)$$

$$= \Big(\prod_{j>i} T(\mu_j, a_j v_i) \Big)(v_i - a_i v_i)$$

y como para cada $j > i$

$(T(\mu_j, a_j v_i))(v_i - a_i v_i) = v_i - a_i v_i - \mu_j(v_i - a_i v_i)a_j v_i$

$$= v_i - a_i v_i = K(v_i)$$

por lo tanto $\quad K = \prod_{j=2}^{n} T(\mu_j, a_j v_i)$,

es decir K es producto de transversiones
ya que $K = \Big(\prod_i T(\mu_i, w_i) \Big)^{-1} X$. se tiene $X = \prod_i T(\mu_i, w_i)\, K$
y como $X \in \mathcal{T}G$, $X = T'G$, con $T' \in \mathcal{T}$
entonces $T'G = \prod_i T(\mu_i, w_i)\, K$

$$G = (T')^{-1} \prod_i T(\mu_i, w_i)\, K$$

es decir, las transversiones generan a SL(n, q). ∎

LEMA 10. Sean H, H' hiperplanos de un F-espacio vectorial V de dimensión n, y sean $0 \neq a \in H$, $b \notin H$, $0 \neq a' \in H'$, $b' \notin H'$. Entonces existe $A \in GL(n,q)$ tal que $A(H) = H'$, $A(a) = a'$, y $A(b) = b'$.
Si $n \geq 3$, A se puede escoger en SL(n,q).

DEMOSTRACION.
Sean $\{ a_1 = a, a_2, \ldots, a_{n-1} \}$ y $\{ b_1 = a', b_2, \ldots, b_{n-1} \}$
bases de H y H' respectivamente y
$\{ a_1, a_2, \ldots, a_{n-1}, a_n = b \}$ y $\{ b_1, b_2, \ldots, b_{n-1}, b_n = b' \}$
bases de V
Sea $A : V \longrightarrow V$ la transformación lineal tal que
$A(a_i) = b_i$, $\quad i = 1, 2, \ldots, n$.
es inmediato que $A \in GL(n,q)$, además $A(a) = a'$, $A(b) = b'$.

Si $n \geq 3$ sea $C : V \longrightarrow V$ definida por

$$C(a_i) = \begin{cases} a_i & i \neq 2 \\ (\det A)^{-1} a_2 & i = 2 \end{cases}$$

$C \in GL(n,q)$, luego $A' = AC \in GL(n,q)$

$A'(a) = AC(a) = A(a) = a'$

$A'(b) = AC(b) = A(b) = b'$

$A'(H) = H'$

y $\det A' = \det (AC) = \det A \det C = \det A (\det A)^{-1} = 1$

$\therefore \quad A' \in SL(n,q)$. ∎

LEMA 11. Todas las transversiones de V, son conjugadas en $GL(n,q)$ y si $n \geq 3$, también son conjugadas en $SL(n,q)$.
Si $n = 2$, los grupos $Z(H)$ son conjugados.

DEMOSTRACION.

Sean las transversiones $T = T(\varphi, a)$ y $T' = T'(\varphi', a')$
con $H = Núc\ \varphi$, $H' = Núc\ \varphi'$ y considérense $b \in V$, $\varphi(b) = 1$,
$b' \in V$, $\varphi'(b') = 1$ entonces $b \in H$, $b' \in H'$,
así por el lema anterior, existe $G \in GL(n,q)$
(y si $n \geq 3$, $G \in SL(n,q)$) tal que $G(H) = H'$, $G(a) = a'$ y
$G(b) = b'$
considerando $V = H' \oplus \langle b' \rangle$, se tiene que demostrar

$$GTG^{-1}\big|_{H'} = T'\big|_{H'}$$

como $G(H) = H'$, si $x' \in H'$, existe $x \in H$, tal que $G(x) = x'$
ó $x = G^{-1}(x')$,
$(GTG^{-1})(x') = GT(G^{-1}(x')) = GT(x) = G(x-\varphi(x)a) = G(x)$
y $T'(x') = x'$ puesto que $x' \in H'$, y T' es transversión según H'.
$\therefore \quad (GTG^{-1})(x') = G(x) = x' = T'(x')$

ahora $(GTG^{-1})(b') = (GT)(b) = G(b-\varphi(b)a) = G(b)-G(a) = b'-a'$
y $T'(b') = b'-\varphi'(b')a' = b'-a'$
de donde $(GTG^{-1})(b') = T'(b')$
por lo tanto $GTG^{-1} = T'$

para $n = 2$

$$Z(H) = \{\ T(\varphi, \lambda a) \mid 0 \neq a \in H,\ \lambda = F\}$$
$$Z(H') = \{\ T(\varphi', \lambda a') \mid 0 \neq a' \in H',\ \lambda = F\}$$

sean $b \in H$ con $\varphi(b) = 1$ y $b' \in H'$ con $\varphi'(b') = 1$

entonces existe $G \in SL(n,q)$ tal que $G(a) = ca'$, $G(b) = b'$
se tiene que

$$(GT(\varphi, \lambda a)G^{-1})(a') = [GT(\varphi, \lambda a)](c^{-1}a) = G(c^{-1}a - \varphi(c^{-1}a)\lambda a)$$
$$= G(c^{-1}a) = c^{-1}G(a) = a'$$

y $T(\varphi', \lambda ca')(a') = a' - \varphi'(a')\lambda ca' = a'$

así que $(GT(\varphi, \lambda a)G^{-1})(a') = T(\varphi', \lambda ca')(a')$

de la misma forma

$$(GT(\varphi, \lambda a)G^{-1})(b') = [GT(\varphi, \lambda a)](b) = G(b - \varphi(b)\lambda a) = G(b)-\lambda G(a)$$
$$= b'-\lambda ca'$$

y $T(\varphi', \lambda ca')(b') = b' - \varphi'(b')\lambda ca' = b'-\lambda ca'$

entonces $(GT(\varphi, \lambda a)G^{-1})(b') = T(\varphi', \lambda ca')(b')$

$\therefore \quad GT(\varphi, \lambda a)G^{-1} = T(\varphi', \lambda ca')$

es decir, $G\tilde{z}(H)G^{-1} = \tilde{z}(H')$. ∎

Antes de continuar con nuestros resultados, se recuerdan otros conceptos.

DEFINICION. Sean $a, b \in \mathbb{G}$, con $\mathbb{G}$ un grupo, $c = [a,b] = a^{-1}b^{-1}ab$, es el conmutador de a y b.

DEFINICION. El subgrupo $\mathbb{G}'$ de $\mathbb{G}$, generado por los conmutadores de $\mathbb{G}$, se denomina SUBGRUPO CONMUTADOR o SUBGRUPO DERIVADO de $\mathbb{G}$.

DEFINICION. El segundo derivado de $\mathbb{G}$, $\mathbb{G}^{2)}$ es $(\mathbb{G}')'$ y en forma inductiva se puede definir el n-ésimo derivado de $\mathbb{G}$, como $(\mathbb{G}^{(n-1)})'$.

TEOREMA 5. Sea $\mathbb{G}$ un grupo y $\mathbb{H} < \mathbb{G}$, entonces las siguientes condiciones i) y ii) son equivalentes :

i) $\mathbb{G}' \subseteq \mathbb{H}$

ii) $\mathbb{H} \triangleleft \mathbb{G}$ y $\mathbb{G}/\mathbb{H}$ es abeliano.

DEMOSTRACION.

i) ⇒ ii) Sean $h \in H \subset G$, $g \in G$

entonces $(h,g) = h^{-1}g^{-1}hg \in G' \subset H$

luego $h(h^{-1}g^{-1}hg) = g^{-1}hg \in H$, es decir $H \lhd G$

por otra parte sean $g, k \in G \Rightarrow$

$[g,k] = g^{-1}k^{-1}gk \in G' \subset H$

de donde $g^{-1}k^{-1}gkH = H$

$gkH = kgH$

y $gHkH = kHgH$

es decir G/H es abeliano.

ii) ⇒ i) Sean $g, k \in G$

$gkH = gHkH = kHgH = kgH$

$gkH = kgH$ y $g^{-1}k^{-1}gkH = H$

$\Rightarrow g^{-1}k^{-1}gk \in H$

$\therefore G' \subset H$. ∎

Ahora se define lo que es un grupo soluble.

DEFINICION. Un grupo G es SOLUBLE, si existen subgrupos $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_r = \langle e \rangle$ tales que $H_i \lhd H_{i-1}$ y H_{i-1}/H_i es abeliano.

TEOREMA 6. Un grupo G es soluble, si y sólo si $G^{(k)} = \langle e \rangle$ para algún $k \geq 1$.

DEMOSTRACION.

⇒) Si G es soluble, existen subgrupos $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_r = \langle e \rangle$ donde cada $H_i \lhd H_{i-1}$ y H_{i-1}/H_i es abeliano

por el teorema 5, $H_{i-1}' \subseteq H_i$, esto es

H_0/H_1 abeliano $\Rightarrow H_0' = G' \subset H_1$ y $G^{(2)} \subset H_1'$

$\mathbb{N}_1 / \mathbb{N}_2$ abeliano $\Rightarrow$ $\mathbb{N}_1' \subset \mathbb{N}_2$, $\mathbb{G}^{(2)} \subset \mathbb{N}_1' \subset \mathbb{N}_2$ y $\mathbb{G}^{(3)} \subset \mathbb{N}_2'$

$\mathbb{N}_2 / \mathbb{N}_3$ abeliano $\Rightarrow$ $\mathbb{N}_2' \subset \mathbb{N}_3$, $\mathbb{G}^{(3)} \subset \mathbb{N}_2' \subset \mathbb{N}_3$ $\therefore$ $\mathbb{G}^{(4)} \subset \mathbb{N}_3'$

sucesivamente

$\mathbb{G}^{(k)} \subset \mathbb{N}_k = \langle e \rangle$, de aquí que $\mathbb{G}^{(k)} = \langle e \rangle$

$\Leftarrow$) Si $\mathbb{G}^{(k)} = \langle e \rangle$ para algún k,
sea $\mathbb{N}_0 = \mathbb{G}$, $\mathbb{N}_1 = \mathbb{G}'$, ..., $\mathbb{N}_k = \mathbb{G}^{(k)} = \langle e \rangle$

entonces, $\mathbb{G} = \mathbb{N}_0 \supset \mathbb{N}_1 \supset \mathbb{N}_2 \supset \ldots \supset \mathbb{N}_k = \langle e \rangle$

por el teorema 5, $\mathbb{N}_i \lhd \mathbb{N}_{i-1}$
luego
$\mathbb{N}_{i-1} / \mathbb{N}_i = \mathbb{G}^{(i-1)} / \mathbb{G}^{(i)} = \mathbb{G}^{(i-1)} / (\mathbb{G}^{(i-1)})'$
por lo que $\mathbb{N}_{i-1} / \mathbb{N}_i$ es abeliano
por lo tanto $\mathbb{G}$ es soluble. ■

El siguiente resultado muestra qué es el subgrupo derivado de GL(n,q) y de SL(n,q) para (n,q) ≠ (2,2) y (n,q) ≠ (2,3), posteriormente se analizarán estos casos.

TEOREMA 7. Para n ≥ 3 y (n = 2, q > 3), se tiene que
$$(GL(n,q))' = SL(n,q) = (SL(n,q))'.$$

DEMOSTRACION. Como $GL(n,q)/SL(n,q) \cong F^*$ y este último es abeliano, por el teorema 5, se tiene que $(GL(n,q))' \subseteq SL(n,q)$.
Ahora, si $(SL(n,q))' = SL(n,q)$,
como $(SL(n,q))' \subset (GL(n,q))'$, entonces se tendrá
$$(GL(n,q))' \subset SL(n,q) = (SL(n,q))' \subset (GL(n,q))'$$
y $\therefore$ $SL(n,q) = (GL(n,q))' = (SL(n,q))'$.
Por lo tanto basta demostrar que $(SL(n,q))' = SL(n,q)$

Caso 1. Sea n ≥ 3
sean T y T' dos transversiones, por el lema 11, existe $G \in SL(n,q)$

tal que $GTG^{-1} = T'$, $\Rightarrow$ $GTG^{-1}T^{-1} = T'T^{-1} \in (SL(n,q))' \subset SL(n,q)$
T, T' están en la misma clase lateral derecha de $(SL(n,q))'$ en $SL(n,q)$, entonces todas las transversiones están en la misma clase lateral derecha.
Sea H un hiperplano de V y $T(\mu, a_1)$, $T(\mu, a_2)$ transversiones según H, como $n \geq 3$, dim $H = n-1 \geq 2$,
sean $a_1, a_2 \in H$, tales que $a_2 \neq 0$, $0 \neq a_2 \neq -a_1$
así $T(\mu, a_2) \circ T(\mu, a_1) = T(\mu, a_1+a_2) \neq E$ puesto que $a_1 + a_2 \neq 0$

luego $T^{-1}(\mu, a_1) \circ (T(\mu, a_1+a_2)) = T(\mu, a_2) \in (SL(n,q))'$

es decir en $(SL(n,q))'$ existe al menos una transversión diferente de E, como todas las transversiones son conjugadas en $SL(n,q)$ por el lema II, si T' es otra transversión, existe $G \in SL(n,q)$ tal que $G^{-1}TG = T'$
y $T' = GTG \in (SL(n,q))'$ porque $(SL(n,q))' \triangleleft SL(n,q)$
Por lo tanto todas las transversiones están en $(SL(n,q))'$

$$\therefore \quad SL(n,q) \subset (SL(n,q))'$$
$$\text{y} \quad SL(n,q) = (SL(n,q))' .$$

Caso 2. $q > 3$, $n = 2$,
considérese $V = \langle v_1, v_2 \rangle$, sea T una transversión
con $T(v_1) = v_1$ $T(v_2) = v_1 + v_2$, T es invertible
es decir $T \in GL(2,q)$
$q > 3 \Rightarrow$ existe $d \in F$, con $0 \neq d^2 \neq 1$
porque F^* es un grupo cíclico de orden $(q-1)$.
ahora sea $G \in GL(2,q)$ con $G(v_1) = dv_1$ y $G(v_2) = d^{-1}v_2$
$G \in SL(2,q)$
se tiene $GTG^{-1}(v_1) = GT(d^{-1}v_1) = G(d^{-1}v_1) = v_1$

$$GTG^{-1}(v_2) = GT(dv_2) = G(dv_1 + dv_2) = d^2v_1 + v_2$$

y

$$T^{-1}GTG^{-1}(v_1) = T^{-1}(v_1) = v_1$$

$$T^{-1}GTG^{-1}(v_2) = T^{-1}(d^2v_1 + v_2) = d^2v_1 + v_2 - T^{-1}(v_1)$$

$$= d^2v_1 + v_2 - v_1 = v_2 - v_1(1-d^2) \qquad 1-d^2 \neq 0$$

es decir,

$$T^{-1}GTG^{-1}(v_2) - v_2 = -v_1(1-d^2) \in \langle v_1 \rangle$$

por lo tanto $T^{-1}GTG^{-1}$ es una transversión diferente de E, según $U = \langle v_1 \rangle$, y $T^{-1}GTG^{-1} \in (SL(n,q))' = E$.

Como todas las transversiones de V son conjugadas en GL(n,q), por el lema 11, y $(SL(n,q))' \lhd GL(n,q)$, entonces SL(n,q) contiene a todo el grupo generado por ellas, que es SL(n,q), según el teorema 4.

Por lo tanto $SL(n,q) \subset (SL(n,q))'$ y $(SL(n,q))' = SL(n,q)$. ■

Para el caso (n,q) = (2,2) :

$|GL(2,2)| = (2^2-1)(2^2-2) = (3)(2) = 6$
$|SL(2,2)| = (2^2-1)2^{2-1} = (3)(2) = 6$

Sean $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL(2,2)$

pero $AB \neq BA$, por tanto GL(2,2) no es abeliano y
$GL(2,2) \cong SL(2,2) \cong S_3$.
$(GL(2,2))' = (SL(2,2))' = A_3$, en efecto:
Sea $H = \langle\langle 1, 2, 3 \rangle\rangle$
se observa que $H \lhd S_3$ y S_3/H es abeliano,
entonces $S_3' < H$
$S_3' \neq 1$, porque S_3 no es abeliano,
$\therefore \quad (GL(2,2))' = (SL(2,2))' \cong A_3 \subset S_3 \cong SL(2,2)$.

En el caso (n,q) = (2,3) :

$|GL(2,3)| = (3^2-1)(3^2-3) = 48$
$|SL(2,3)| = (3^2-1)(3) = 24$
Se mostrará que $(GL(2,3))' = SL(2,3)$.

$\frac{GL(2,3)}{SL(2,3)} \cong \{1, 2\}$ = grupo multiplicativo de F $\qquad (|F| = 3)$

$\therefore \quad (GL(2,3))' \subset SL(2,3)$

como $\dfrac{GL(2,3)}{(GL(2,3))'} \Big/ \dfrac{SL(2,3)}{(GL(2,3))'} \cong \dfrac{GL(2,3)}{SL(2,3)} \cong \{1, 2\}$

$$GL(2,3) \xrightarrow{\Pi} \frac{GL(2,3)}{(GL(2,3))'} \xrightarrow{\varphi} \{1, 2\}$$

Sean T_1, T_2 transversiones, entonces

$T_2 = S^{-1}T_1S$ para algún $S \in GL(2,3)$

$\therefore \quad \Pi(T_2) = \Pi(T_1)$ porque $\dfrac{GL(2,3)}{(GL(2,3))'}$ es abeliano

y $\varphi(\Pi(T_2)) = \varphi(\Pi(T_1)) = d$

Sea $T = T(\mu, a) \neq E$, $a \in Núc\ \mu$,

$T(\mu, a) \cdot T(\mu, a) = T(\mu, 2a) \neq E$ porque $2a \neq 0$, car $F = 3$.

$\therefore \quad (\varphi\Pi)(T(\mu, a))(\varphi\Pi)(T(\mu, a)) = \varphi\Pi(T(\mu, 2a))$

y $d^2 = d \quad \rightarrow \quad d = 1$

$\therefore \quad \Pi(T) \in (GL(2,3))' \quad \rightarrow \quad T \in (GL(2,3))'$

y como las transversiones generan a SL(n,q), entonces

$SL(2,3) \subset (GL(2,3))' \quad \therefore \quad (GL(2,3))' = SL(2,3)$.

Ahora se hará ver que $(SL(2,3))' \neq SL(2,3)$. Sea

$$K = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}2&0\\0&2\end{bmatrix}, \begin{bmatrix}1&1\\1&2\end{bmatrix}, \begin{bmatrix}2&2\\2&1\end{bmatrix}, \begin{bmatrix}2&1\\1&1\end{bmatrix}, \begin{bmatrix}1&2\\2&2\end{bmatrix}, \begin{bmatrix}0&2\\1&0\end{bmatrix}, \begin{bmatrix}0&1\\2&0\end{bmatrix} \right\}$$

$K \subset (SL(2,3))'$:

$$a = \begin{bmatrix}1&1\\1&2\end{bmatrix} \quad b = \begin{bmatrix}2&1\\1&1\end{bmatrix} \quad a^{-1}b^{-1}ab = \begin{bmatrix}2&0\\0&2\end{bmatrix}$$

$$a = \begin{bmatrix}1&0\\2&1\end{bmatrix} \quad b = \begin{bmatrix}0&2\\1&0\end{bmatrix} \quad a^{-1}b^{-1}ab = \begin{bmatrix}1&1\\1&2\end{bmatrix}$$

$$a = \begin{bmatrix}1&0\\1&1\end{bmatrix} \quad b = \begin{bmatrix}1&2\\0&1\end{bmatrix} \quad a^{-1}b^{-1}ab = \begin{bmatrix}2&2\\2&1\end{bmatrix}$$

$$a = \begin{bmatrix}2&0\\1&2\end{bmatrix} \quad b = \begin{bmatrix}1&1\\0&1\end{bmatrix} \quad a^{-1}b^{-1}ab = \begin{bmatrix}2&1\\1&1\end{bmatrix}$$

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \quad a^{-1}b^{-1}ab = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$a = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad a^{-1}b^{-1}ab = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$a = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \quad a^{-1}b^{-1}ab = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

Se verifica que K es un subgrupo de orden 8 y es el único 2-subgrupo de Sylow de SL(2,3), puesto que los elementos de SL(2,3) - K son de orden 3, como :

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

o bién de orden 6, como :

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

$\therefore$ $K \triangleleft SL(2,3)$ y como $|SL(2,3) / K| = 3$,
$SL(2,3) / K$ es abeliano

$\therefore$ $(SL(2,3))' \leq K$, $\therefore$ $(SL(2,3))' = K$

y $(SL(2,3))' \neq SL(2,3)$.

DEFINICION. Si Ω es un conjunto y $\mathbb{G}$ un grupo, entonces Ω es un $\mathbb{G}$-CONJUNTO, si existe una función

$\cdot : \mathbb{G} \times \Omega \longmapsto \Omega$ denotada por $\cdot (g, x) \longmapsto gx$, tal que

i) $1x = x$, $1 \in \mathbb{G}$

ii) $g(hx) = (gh)x$

para todo $x \in \Omega$ y todo $g, h \in \mathbb{G}$.

Si Ω es un $\mathbb{G}$-conjunto , se dice que $\mathbb{G}$ actúa sobre Ω.

DEFINICION. Sea V un espacio vectorial (n+1)-dimensional sobre un campo F, cualesquiera dos vectores v, w de V^{n+1} son EQUIVALENTEMENTE PROYECTIVOS si existe un escalar $r \neq 0$ con $w = rv$.

De esta manera se tiene definida una relación de equivalencia en V^{n+1}.

El vector nulo forma una clase de equivalencia por sí mismo.

La clase de equivalencia que contiene al vector v, será denotada por [v] y evidéntemente [v] = [rv] para todo $r \neq 0$.

DEFINICION. Cada clase diferente de [0], es llamada un PUNTO PROYECTIVO.

DEFINICION. El conjunto de todos los puntos proyectivos en V^{n+1}, es el ESPACIO PROYECTIVO DE DIMENSION n, sobre F, denotado por $\mathbb{P}^n(F)$.

Ahora, considerando el grupo PSL(n,q) y el espacio proyectivo $\mathbb{P}^{n-1}(F)$, se tiene que $\cdot : PSL(n,q) \times \mathbb{P}^{n-1}(F) \longmapsto \mathbb{P}^{n-1}(F)$ dada por $(gZ(SLn,q), a) = \langle g(v)\rangle$, con $g \in SL(n,q)$ y $a = \langle v\rangle$, es una función.
En efecto si
$(gZ, \langle v\rangle) = (g_1Z, \langle u\rangle) \Rightarrow (gZ = g_1Z \text{ y } \langle v\rangle = \langle u\rangle)$,
entonces $g^{-1}g_1 \in Z$ y $u = rv$, $r \neq 0$
$(g_1Z)\langle u\rangle = \langle g_1u\rangle = \langle g_1(rv)\rangle = \langle rg_1v\rangle = \langle g_1v\rangle = \langle gh(v)\rangle$ para algún $h \in Z$.
pero $Z = \{\alpha E \mid \alpha \in F^*\}$
$(g_1Z)\langle u\rangle = \langle g\alpha v\rangle = \langle \alpha gv\rangle = \langle g(v)\rangle = \langle gZ\rangle\langle v\rangle$

De hecho cada gZ es una permutación sobre $\mathbb{P}^{n-1}(F)$.
Sean $a = \langle v\rangle$, $b = \langle u\rangle \in \mathbb{P}^{n-1}(F)$ tales que $(gZ)(a) = (gZ)(b)$,
entonces $\langle g(v)\rangle = \langle g(u)\rangle$
$\Rightarrow g(u) = \alpha g(v)$ y $g^{-1}(g(u)) = g^{-1}(\alpha g(v))$
$\Rightarrow u = \alpha v$ y $\langle v\rangle = \langle u\rangle$, $\therefore a = b$.
Sea $b = \langle u\rangle \in \mathbb{P}^{n-1}(F)$, $u \in V$, existe $v \in V$ tal que $g(v) = u$,

entonces $(gZ)\langle v\rangle = \langle u\rangle$,
por lo tanto gZ es una permutación sobre $\mathbb{P}^{n-1}(F)$.

DEFINICION. Sea $\mathbb{G}$ un grupo de permutaciones sobre un conjunto Ω. $\mathbb{G}$ es TRANSITIVO sobre Ω, si dados $x, y \in \Omega$, existe $\alpha \in \mathbb{G}$ con $\alpha(x) = y$.

DEFINICION. Sea $\mathbb{G}$ un grupo de permutaciones sobre un conjunto Ω. $\mathbb{G}$ es k-TRANSITIVO sobre Ω si, dados $(x_1, x_2, \ldots, x_k)$ y $(y_1, y_2, \ldots, y_k) \in \Omega^k$ con $x_i \neq x_j$, $y_i \neq y_j$ para $i \neq j \in \{1, 2, \ldots, k\}$, existe $\alpha \in \mathbb{G}$, tal que $\alpha(x_i) = y_i$, para $i = 1, 2, \ldots, k$.

TEOREMA 8. PSL(n,q) es 2-transitivo sobre $\mathbb{P}^{n-1}(F)$.

DEMOSTRACION.
Sean (a_1, a_2) y $(a_1', a_2') \in \mathbb{P}^{n-1}(F) \times \mathbb{P}^{n-1}(F)$

con $a_1 \neq a_2$ y $a_1' \neq a_2'$
tales que $a_1 = \langle v_1\rangle$ $a_2 = \langle v_2\rangle$ $a_1' = \langle v_1'\rangle$ $a_2' = \langle v_2'\rangle$

con $v_1, v_1', v_2, v_2' \in V$
$\{v_1, v_2\}$, $\{v_1', v_2'\}$ son conjuntos linealmente independientes porque $a_1 \neq a_2$ $a_1' \neq a_2'$
Sean $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ $\mathcal{B}' = \{v_1', v_2', \ldots, v_n'\}$ bases de V

se construye $g \in SL(n,q)$ tal que $g(v_1) = v_1'$ $g(v_2) = cv_2'$, $c \in F^*$

por ejemplo si $A \in GL(n,q)$ tal que $A(v_i) = v_i'$ y

$B \in GL(n,q)$ tal que $B(v_i) = \begin{cases} v_i' & \text{si } i \neq 2 \\ (\det A)^{-1} v_2' & \text{si } i = 2 \end{cases}$

entonces $g = B \cdot A$ cumple con las condiciones necesarias porque

$g(v_1) = B(A(v_1)) = B(v_1') = v_1'$

$g(v_2) = B(A(v_2)) = B(v_2') = (\det A)^{-1} v_2'$

$g(v_j) = B(A(v_j)) = B(v_j') = v_j'$, si $j \geq 3$

$\det g = \det(B \circ A) = \det B \det A$ pero $\det B = (\det A)^{-1}$

$\therefore \quad g \in SL(n,q)$

y $g(v_1) = v_1'$, $g(v_2) = cv_2'$ con $c \in F^*$

(si $n \geq 3$ se puede tomar $c = 1$) .

$(gZ)a_1 = \langle gv_1 \rangle = \langle v_1' \rangle = a_1'$

$(gZ)a_2 = \langle gv_2 \rangle = \langle cv_2' \rangle = \langle v_2' \rangle = a_2'$.

gZ induce en $\mathbb{P}^{n-1}(F)$ una permutación que lleva a_1 en a_1' y a_2 en a_2' por lo tanto PSL(n,q) es 2-transitivo sobre $\mathbb{P}^{n-1}(F)$. ■

Existe un monomorfismo ψ de PSL(n,q) en $S_{\mathbb{P}^{n-1}(F)}$ donde $\psi(gZ)$ es la permutación inducida por gZ en $\mathbb{P}^{n-1}(F)$, por lo tanto PSL(n,q) es de hecho un subgrupo de $S_{\mathbb{P}^{n-1}(F)}$.

DEFINICION. Un **BLOQUE** de un $\mathbb{G}$-conjunto X, es un subconjunto $B \subset X$, tal que si $g \in \mathbb{G}$, entonces $gB = B$ o $gB \cap B = \emptyset$.

Ejemplo : $B = \emptyset$, $B = X$, son bloques llamados bloques triviales.

DEFINICION. Sea $\mathbb{G}$ un grupo de permutaciones de X tal que $\mathbb{G}$ es transitivo sobre X, se dice que $\mathbb{G}$ es **PRIMITIVO**, si y sólo si X contiene únicamente bloques triviales.

DEFINICION. Un grupo $\mathbb{G}$ de permutaciones de X es **IMPRIMITIVO**, si no es primitivo.

Ejemplo : Sea $X = \{1, 2, 3, 4\}$ los vértices de un cuadrado sobre el plano y $G = D_4$ el grupo de simetrías del cuadrado, entonces D_4 es imprimitivo :

sea $s = (1, 2, 3, 4)$ y $t = (2,4)$,

$D_4 = \langle s,t \rangle$ donde $s^4 = 1$, $t^2 = 1$, $ts = s^3t$.

Sea $B = \{1, 3\} \subset X$ entonces,

$sB = \{2, 4\}$	$stB = \{2, 4\}$
$s^2B = \{3, 1\}$	$s^2tB = \{3, 1\}$
$s^3B = \{2, 4\}$	$s^3tB = \{2, 4\}$
$tB = \{1, 3\}$	$s^4B = \{1, 3\}$

$B \neq \emptyset$, $B \neq X$ y para cada $g \in D_4$, $gB = B$ ó $gB \cap B = \emptyset$, por lo tanto B es un bloque no trivial de X, del mismo modo se puede verificar que $C = \{2, 4\}$ es bloque no trivial de X, además, éstos son los únicos, por lo tanto D_4 es imprimitivo.

LEMA 12. Supóngase que $\mathbb{G}$ es imprimitivo sobre Ω ($|\Omega| > 1$). Sea Δ un bloque no trivial, sean g_1, $g_2 \in \mathbb{G}$, entonces $g_1\Delta = g_2\Delta$ ó $g_1\Delta \cap g_2\Delta = \emptyset$.

DEMOSTRACION. $g_2^{-1}g_1 \in \mathbb{G} \Rightarrow g_2^{-1}g_1\Delta = \Delta$ ó $(g_2^{-1}g_1\Delta) \cap \Delta = \emptyset$

si $g_2\Delta \cap g_1\Delta \neq \emptyset \Rightarrow$

existe $x \in g_1\Delta \cap g_2\Delta$

$x = g_1y = g_2t$ $y, t \in \Delta$

$g_2^{-1}g_1y = t \in \Delta$ y $(g_2^{-1}g_1\Delta) \cap \Delta \neq \emptyset$

$\therefore$ $g_2^{-1}g_1\Delta = \Delta$ y $g_1\Delta = g_2\Delta$. ■

LEMA 13. Sea $\mathbb{G}$ imprimitivo sobre Ω y Δ un bloque no trivial. Las imágenes de Δ mediante las permutaciones de $\mathbb{G}$, forman una partición de Ω.

DEMOSTRACION. Si $y \in \Omega$, $x \in \Delta$, existe $g \in \mathbb{G}$ con $y = gx$,

puesto que $\mathbb{G}$ es transitivo sobre Ω, es decir $y \in g\Delta$
$\Omega = \bigcup_{g\in\mathbb{G}} g\Delta$ y como $g_1\Delta = g_2\Delta$ ó $g_1\Delta \cap g_2\Delta = 0$

y $g\Delta \neq 0$ para todo $g \in \mathbb{G}$
por lo tanto $\{ g\Delta \}_{g\in\mathbb{G}}$ forman una partición de Ω. ■

Se observa que si Δ es un bloque, $g\Delta$ también lo es y además si Ω es finito, $|\Omega| = \Sigma_{g\in\mathbb{G}}|g\Delta|$ y $|g\Delta| = |\Delta|$ implica que $|\Omega| = m|\Delta|$, donde m es el número de clases de equivalencia.

DEFINICION. Al conjunto de tranformados de Δ mediante las permutaciones de $\mathbb{G}$, se le llama el SISTEMA DE IMPRIMITIVIDAD generado por Δ.

DEFINICION. Sea $\mathbb{G}$ un grupo y Ω un $\mathbb{G}$-conjunto, $a \in \Omega$. El ESTABILIZADOR de a en $\mathbb{G}$, es el subgrupo $S_{\mathbb{G}}(a)$ de $\mathbb{G}$, definido por
$$S_{\mathbb{G}}(a) = \{ g \in \mathbb{G} \mid ga = a \}.$$

TEOREMA 9. Si $\mathbb{G}$ es un grupo de permutaciones transitivo sobre Ω, entonces $\mathbb{G}$ es primitivo, si y sólo si, para todo $a \in \Omega$, $S_{\mathbb{G}}(a) <_{max} \mathbb{G}$.

DEMOSTRACION.
$\Rightarrow$) Supóngase que existe $a \in \Omega$, tal que existe $\mathbb{H} < \mathbb{G}$ con
$S_{\mathbb{G}}(a) < \mathbb{H} < \mathbb{G}$,
considérese $\Delta = \mathbb{H}a = \{ ha \mid h \in \mathbb{H} \}$
supóngase $g\Delta \cap \Delta \neq 0$, $\Rightarrow$ $gh'a = ha$, $h, h' \in \mathbb{H}$

así que $h^{-1}gh'a = a$ $\Leftrightarrow$ $h^{-1}gh' \in S_{\mathbb{G}}(a) \subset \mathbb{H}$
$\Rightarrow$ $g \in \mathbb{H}$ y $g\Delta = g\mathbb{H}a = \mathbb{H}a = \Delta$

luego $\Delta = \mathbb{H}a \neq 0$ puesto que $a \in \Delta$,
Además, si $\Delta = \mathbb{H}a = \Omega$, se escoge $g \in \mathbb{G}-\mathbb{H}$ y $ga \in \Omega$

es decir $ga = ha$ para algún $h \in \mathbb{H}$, $\Rightarrow$

$h^{-1}ga = a$, $h^{-1}g \in S_\Omega(a) \subset \mathbb{H}$ $\Rightarrow$ $g \in \mathbb{H}$

contradicción con $g \in \mathbb{G}-\mathbb{H}$

$\therefore$ $\Delta = \mathbb{H}a \neq \Omega$

Finalmente $\Delta = \mathbb{H}a$ no es singular, puesto que $S_\Omega(a) < \mathbb{H}$, es decir, existe $h \in \mathbb{H}$ tal que $ha \neq a$.

En resumen Δ es un bloque no trivial, lo que implica que $\mathbb{G}$ es imprimitivo (contradicción).

$\Leftarrow$) Supóngase que $\mathbb{G}$ es imprimitivo y sea Δ un bloque no trivial, si $a \in \Delta$ se mostrará que $S_\Omega(a) = A$ no es maximal.

Sea $\mathbb{H} = \{g \in \mathbb{G} \mid g\Delta = \Delta\}$, $\mathbb{H}$ es un subgrupo de $\mathbb{G}$ y es transitivo sobre Δ.

En efecto si $a_1, a_2 \in \Delta$,

existe $k \in \mathbb{G}$ tal que $ka_1 = a_2 \in k\Delta$

$a_2 \in \Delta \cap k\Delta$ $\Rightarrow$ $\Delta = k\Delta$ ya que Δ es un bloque

así que $k \in \mathbb{H}$, $\therefore$ $\mathbb{H}$ es transitivo sobre Δ.

Por otra parte, si $g \in A = S_\Omega(a)$, $g(a) = a$ así que $\Delta \cap g\Delta \neq \emptyset$

$\Rightarrow$ $\Delta = g\Delta$ y $g \in \mathbb{H}$

pero $\mathbb{H} \neq A$ porque $\mathbb{H}$ es transitivo sobre Δ, mientras que A no lo es.

$\mathbb{H} \neq \mathbb{G}$ porque $\mathbb{G}$ es transitivo sobre Ω, mientras que $\mathbb{H}$ lleva a $\Delta \subsetneq \Omega$ en Δ, por lo tanto $A < \mathbb{H} < \mathbb{G}$.

Contradiciendo el hecho de que $A = S_\Omega(a)$ es maximal. ■

Si $\mathbb{G}$ es transitivo sobre Ω y $\mathbb{H} \triangleleft \mathbb{G}$, en general $\mathbb{H}$ no es transitivo sobre Ω.

Ejemplo :

$V^{\vec{}} = V-\{0\}$, V un F-espacio vectorial, $GL(V)$ es transitivo sobre $V^{\vec{}}$, si $\mathbb{H} = Z(GL(V))$ es fácil verificar que $\mathbb{H}$ no es transitivo sobre $V^{\vec{}}$.

TEOREMA 10. Sea $\mathbb{G}$ transitivo sobre Ω, $|\Omega| > 1$ y $E \neq \mathbb{N} \lhd \mathbb{G}$, $\mathbb{N}$ no transitivo sobre Ω, entonces las órbitas de $\mathbb{N}$ son bloques de Ω con respecto a $\mathbb{G}$ y forman un sistema de imprimitividad para $\mathbb{G}$, es decir $\mathbb{G}$ es imprimitivo y cada órbita de $\mathbb{N}$ es un bloque no trivial. Además todas las órbitas tienen la misma longitud.

DEMOSTRACION. Sea T una órbita de $\mathbb{N}$, con $|T| > 1$.
Existe una tal T porque $\mathbb{N} \neq E$.
Si $g \in \mathbb{G}$, $n \in \mathbb{N}$ se tiene que $g^{-1}ng = n' \in \mathbb{N}$ y
por lo tanto $ngT = gn'T = gT$
se sigue que $n(gT) = gT$ para cada $n \in \mathbb{N}$
sean $g_i, g_j \in gT$, $(i, j \in T)$;
existe $n \in \mathbb{N}$ tal que $ni = j$,
de donde se sigue que $g_j = gni$
y $(gng^{-1})gi = gj$, $\therefore$ $gi, gj \in gT$ son $\mathbb{N}$-equivalentes
$\therefore$ gT es una órbita de $\mathbb{N}$ lo que implica que
$gT = T$ ó $gT \cap T = 0$ por lo tanto T es un bloque no trivial
ya que $T \neq \Omega$ por que $\mathbb{N}$ no es transitivo sobre Ω,
$\therefore$ $\mathbb{G}$ es imprimitivo .
Cada órbita de $\mathbb{N}$ es de la forma gT para algún $g \in \mathbb{G}$, en efecto si
Y es una órbita de $\mathbb{N}$
si $y \in Y$, $x \in T$, existe $g \in \mathbb{G}$ tal que $gx = y$
$\therefore$ $y \in gT$ y $gT \cap Y \neq 0$ $\therefore$ $gT = Y$
$\therefore$ las órbitas de $\mathbb{N}$ forman un sistema de imprimitividad ■

COROLARIO 10. Todo subgrupo normal propio de un grupo primitivo es transitivo.

TEOREMA 11. Un grupo $\mathbb{G}$ de permutaciones 2-transitivo sobre Ω, es primitivo.

DEMOSTRACION.
Supóngase que $\mathbb{G}$ es imprimitivo, sea Δ un bloque no trivial, es decir $|\Delta| > 1$ $\Delta \neq \Omega$,

sean $a, b \in \Delta$ con $a \neq b$ y $c \in \Delta$

como $\mathbb{G}$ es 2-transitivo, existe $g \in \mathbb{G}$ tal que $g(a, b) = (a, c)$,

$\Rightarrow$ $g\Delta \neq \Delta$, $\Delta \cap g\Delta \neq \emptyset$ lo que es un absurdo

Por lo tanto $\mathbb{G}$ es primitivo. ∎

Obsérvese que si un grupo es k-transitivo, también es (k-1)-transitivo.

COROLARIO 11. Un grupo de permutaciones k-transitivo, $k \geq 2$, es primitivo.

LEMA 14. Sean $\mathbb{N} \triangleleft \mathbb{G}$, $\mathbb{R} < \mathbb{G}$, entonces $(\mathbb{NR})^{(r)} \subset \mathbb{NR}^{(r)}$.

DEMOSTRACION. Por inducción.

$r = 1$ $\quad \mathbb{R}' \triangleleft \mathbb{R} \Rightarrow \mathbb{NR}' \triangleleft \mathbb{NR}$

como $\mathbb{NR} = (\mathbb{NR}')\mathbb{R}$

así $\dfrac{\mathbb{NR}}{\mathbb{NR}'} = \dfrac{(\mathbb{NR}')\mathbb{R}}{\mathbb{NR}'} \cong \dfrac{\mathbb{R}}{\mathbb{NR}' \cap \mathbb{R}}$ 2do. teo. de isomorfismo

como $\mathbb{R}' \subset \mathbb{NR}' \cap \mathbb{R}$, por el teorema 5,

$\dfrac{\mathbb{R}}{\mathbb{NR}' \cap \mathbb{R}}$ es abeliano

luego $\dfrac{\mathbb{NR}}{\mathbb{NR}'}$ es abeliano

y por el teorema 5, también, $(\mathbb{NR})' \subset \mathbb{NR}'$

hipótesis de inducción : $(\mathbb{NR})^{(r)} \subset \mathbb{NR}^{(r)}$,

P. D. $(\mathbb{NR})^{(r+1)} \subset \mathbb{NR}^{(r+1)}$

$$(\mathbb{NR})^{(r+1)} = \left(\mathbb{NR}^{(r)}\right)' \subset \left(\mathbb{NR}^{(r)}\right)' \subset \mathbb{N}\left(\mathbb{R}^{(r)}\right)' = \mathbb{NR}^{(r+1)} \ . \quad \blacksquare$$

LEMA 15. Sea $\mathbb{G}$ primitivo sobre Ω tal que

i) $\mathbb{G}' = \mathbb{G}$

ii) Existe $a \in \Omega$ tal que $S_\alpha(a)$, contiene un subgrupo $\mathbb{P} \lhd S_\alpha(a)$ con $\mathbb{P}$ soluble y tal que los elementos conjugados de $\mathbb{P}$ en $\mathbb{G}$ generan a $\mathbb{G}$.

Entonces $\mathbb{G}$ es simple.

DEMOSTRACION. Sea $\mathbb{N} \lhd \mathbb{G}$, $\mathbb{N} \neq E$. P. D. $\mathbb{N} = \mathbb{G}$

Como $\mathbb{G}$ es primitivo por el corolario 10, $\mathbb{N}$ es transitivo, y si $a \in \mathbb{G}$, $S_\alpha(a)$ es maximal, según el teorema 9.

$\mathbb{N} \not\subset S_\alpha(a)$ puesto que $\mathbb{N}$ es transitivo sobre Ω y $S_\alpha(a)$ no lo es

$\mathbb{N}S_\alpha(a) = \mathbb{G}$ porque $S_\alpha(a)$ es un subgrupo maximal de $\mathbb{G}$

$\mathbb{R} \lhd \mathbb{G}$ porque $\mathbb{R} \lhd S_\alpha(a)$, en efecto

$g^{-1}rg = (ns)^{-1}rns = s^{-1}n^{-1}rns = s^{-1}n^{-1}nr_1s = s^{-1}r_1s \in \mathbb{P}$,

y como $\mathbb{N} \lhd \mathbb{G}$ entonces $\mathbb{N}\mathbb{R} \lhd \mathbb{G}$

$\forall\, g \in \mathbb{G}$, si $r \in \mathbb{R} \subset \mathbb{N}\mathbb{P}$, implica $g^{-1}rg \in \mathbb{N}\mathbb{P}$,

además como los conjugados de $\mathbb{P}$ en $\mathbb{G}$ generan $\mathbb{G}$ (por hipótesis) se tiene que $\mathbb{G} \subset \mathbb{N}\mathbb{R}$ $\therefore$ $\mathbb{N}\mathbb{R} = \mathbb{G}$.

Como $\mathbb{R}$ es soluble, existe un entero $k \geq 1$ tal que $\mathbb{R}^{(k)} = \langle e \rangle$ y por el lema 14 se tiene que

$\mathbb{G}^{(k)} = (\mathbb{N}\mathbb{R})^{(k)} \subset \mathbb{N}\mathbb{P}^{(k)} = \mathbb{N}e = \mathbb{N}$

y como $\mathbb{G}' = \mathbb{G}$, entonces $\mathbb{G} = \mathbb{G}^{(k)} \subset \mathbb{N}$

$\therefore$ $\mathbb{G} = \mathbb{N}$ y $\mathbb{G}$ es simple. ∎

LEMA 16. Sean $\mathbb{N} \lhd \mathbb{G}$, $\mathbb{A} < \mathbb{G}$, entonces

$$\left(\frac{\mathbb{A}\mathbb{N}}{\mathbb{N}}\right)' = \frac{\mathbb{A}' \mathbb{N}}{\mathbb{N}}$$

DEMOSTRACION. $\mathbb{A}\mathbb{N}$ es subgrupo de $\mathbb{G}$

considerando el homomórfismo canónico $\Pi : \mathbb{A}\mathbb{N} \longrightarrow \mathbb{A}\mathbb{N}/\mathbb{N}$

$\Pi(\langle \mathbb{A}\mathbb{N} \rangle') \subset (\mathbb{A}\mathbb{N}/\mathbb{N})'$ en efecto :

$\langle \mathbb{A}\mathbb{N} \rangle' < \mathbb{A}\mathbb{N}$

si $[a,b] \in (\mathbb{A}\mathbb{N})'$

$\Pi[a,b] = \Pi(a^{-1}b^{-1}ab) = (\Pi a)^{-1}(\Pi b)^{-1}(\Pi a)(\Pi b) = [\Pi a, \Pi b] \in \left[\frac{\mathbb{A}\mathbb{N}}{\mathbb{N}}\right]'$

pero $\pi((A\partial N)') = \frac{(A\partial N)'\partial N}{\partial N}$

$\therefore \quad \frac{(A\partial N)'\partial N}{\partial N} \subset \left(\frac{A\partial N}{\partial N}\right)'$

como $\quad A \subset A\partial N, \quad A' \subset (A\partial N)' \quad$ y $\quad A'\partial N \subset (A\partial N)'\partial N$

$\therefore \quad \frac{A'\partial N}{\partial N} \subset \frac{(A\partial N)'\partial N}{\partial N} \subset \left(\frac{A\partial N}{\partial N}\right)'$

es decir $\quad \frac{A'\partial N}{\partial N} \subset \left(\frac{A\partial N}{\partial N}\right)'$

inversamente $\quad \frac{A\partial N/\partial I}{A'\partial N/\partial I} \cong \frac{A\partial I}{A'\partial I} = \frac{A(A'\partial I)}{A'\partial I} \cong \frac{A}{A \cap A'\partial I}$

$A' \subset A, \quad A' \subset A'\partial I \quad \Rightarrow \quad \frac{A}{A \cap A'\partial I}$ es abeliano

así $\quad \frac{A\partial N/\partial N}{A'\partial N/\partial N}$ es abeliano y $\left(\frac{A\partial N}{\partial I}\right)' \subset \frac{A'\partial I}{\partial N}$. ■

TEOREMA. PSL(n,q) es simple si $n \geq 3$, o si $n = 2$ y $q > 3$.

DEMOSTRACION.

i) Por el Teorema 8, PSL(n,q) es 2-transitivo sobre $\mathbb{P}^{n-1}(F)$ y por el Teorema 11, PSL(n,q) es primitivo.

ii) $(PSL(n,q))' = PSL(n,q)$, en efecto :

$$PSL(n,q) = \frac{SL(n,q)}{SL(n,q) \cap Z} \cong \frac{SL(n,q)Z}{Z}$$

$$(PSL(n,q))' = \left(\frac{SL(n,q)Z}{Z}\right)'$$

$$= \frac{(SL(n,q))'Z}{Z} \qquad \text{por el lema 16}$$

$$= \frac{(SL(n,q))Z}{Z} \qquad \text{por el teorema 7}$$

$$\cong \frac{SL(n,q)}{SL(n,q) \cap Z} = PSL(n,q)$$

iii) Sea $w \in V$, $w \neq 0$ y
sea $\mathcal{T}_w = \{ T \mid T(v) = v - \mu(v)w,\ 0 \neq \mu \in V^* \text{ y } \mu(w) = 0 \}$
por el lema 6, $\mathcal{T}_w$ es abeliano y por lo tanto soluble.
ahora se demuestra que
$\langle g\mathcal{T}_w g^{-1} \mid g \in SL(n,q) \rangle = \langle \mathcal{T}_{gw} \mid g \in SL(n,q) \rangle = SL(n,q)$

a) Sea $T \in \mathcal{T}_w$, es decir $T(v) = v - \mu(v)w$ con $\mu(w) = 0$
entonces

$$gTg^{-1}(v) = (gT)(g^{-1}v) = g(g^{-1}v - \mu(g^{-1}v)w)$$
$$= v - (\mu g^{-1})(v)g(w)$$

como $(\mu g^{-1})(gw) = \mu(w) = 0$ $\quad gTg^{-1} = T'(\mu g^{-1}, g(w)) \in \mathcal{T}_{gw}$
así $\quad g\mathcal{T}_w g^{-1} \subset \mathcal{T}_{gw}$

b) sea $T \in \mathcal{T}_{gw}$, es decir $T(v) = v - \mu(v)gw$ con $\mu(gw) = 0$
entonces

$$g^{-1}Tg(v) = (g^{-1}T)(gv) = g^{-1}(gv - \mu(gv)gw)$$
$$= v - (\mu g)(v)w$$

y como $(\mu g)(w) = \mu(gw) = 0$ $\quad g^{-1}Tg = T'(\mu g, w) \in \mathcal{T}_w$

así $\quad g^{-1}\mathcal{T}_{gw}g \subset \mathcal{T}_w$
por lo tanto

$$\mathcal{T}_{gw} = gg^{-1}\mathcal{T}_{gw}gg^{-1} \subset g\mathcal{T}_w g^{-1} \subset \mathcal{T}_{gw}$$

por tanto

$$\mathcal{T}_{gw} = g\mathcal{T}_w g^{-1}$$

c) Sea T una transversión, $T(v) = v - \mu(v)w'$ con $\mu(w') = 0$
así $T \in \mathcal{T}_{w'}$
como $SL(n,q)$ es transitivo sobre V, existe $g \in SL(n,q)$ tal que

$g(w) = w'$, $\Rightarrow$ $T \in \mathcal{T}_{gv}$

es decir toda transversión está contenida en un subgrupo $\mathcal{T}_{gv} = g\mathcal{T}_v g^{-1}$ con w fijo y g conveniente y como las transversiones generan a SL(n,q)

$\langle g\mathcal{T}_v g^{-1} \mid g \in SL(n,q)\rangle = \langle \mathcal{T}_{gv} \mid g \in SL(n,q)\rangle = SL(n,q)$.

como $\mathcal{T}_v \subset SL(n,q)$, por el teorema de la correspondencia, y el homomorfismo canónico

$$\Pi : SL(n,q) \longmapsto \frac{SL(n,q)}{Z(SL(n,q))}$$

define una correspondencia uno a uno entre el conjunto de subgrupos de SL(n,q) que contienen a Z(SL(n,q)) y el conjunto de todos los subgrupos de

$$\frac{SL(n,q)}{Z(SL(n,q))} = PSL(n,q),$$

de modo que $\mathcal{T}w \longmapsto K = \dfrac{\mathcal{T}_v\, Z(SL(n,q))}{Z(SL(n,q))}$

y como los conjugados de $\mathcal{T}_v$ en SL(n,q) generan a SL(n,q), los conjugados de K en PSL(n,q) generan a PSL(n,q).

Considérese $a = \langle w\rangle \in \mathbb{P}^{n-1}(F)$

$$S(a) = \{\, g \in PSL(n,q) \mid g(a) = a \,\}$$
$$PSL(n,q)$$

como $K = \dfrac{\mathcal{T}_v\, Z(SL(n,q))}{Z(SL(n,q))} \cong \dfrac{\mathcal{T}_v}{\mathcal{T}_v \cap Z(SL(n,q))}$,

$K \subset S(a)$, puesto que si $\bar{T} \in K$, se tiene
$PSL(n,q)$

$\bar{T}(a) = \bar{T}\langle w\rangle = \langle Tw\rangle = \langle w - \mu(w)w\rangle = \langle w\rangle = a$

es decir, $\bar{T} \in S(a)$
$PSL(n,q)$

además $\mathcal{T}_v$ es abeliano y $Z \cap SL(n,q)$ es el centro de SL(n,q), entonces K también es abeliano, por lo tanto soluble.

y $K \triangleleft S(a)$
$PSL(n,q)$

Hasta aquí se demostró que PSL(n,q) cumple con todas las condiciones del lema 15, y se puede concluir que PSL(n,q) es simple si $n \geq 3$ o $n = 2$ y $q > 3$. ∎

Ahora analizando a PSL(2,2) y PSL(2,3), se tiene :

$|PSL(2,2)| = 2(2^2-1) = (2)(3) = 6$
por lo tanto $PSL(2,2) \cong SL(2,2) \cong S_3$, como se vio anteriormente, así que PSL(2,2) no es simple.

$|PSL(2,3)| = \frac{1}{2}\, 3(3^2-1) = 12$
PSL(2,3) es un grupo de permutaciones 2-transitivo sobre el espacio proyectivo $\mathbb{P}(1,3)$ de cuatro elementos, y como PSL(2,3) tiene 12 elementos, por lo tanto PSL(2,3) es isomorfo a un subgrupo de S_4, de orden 12, pero el único subgrupo de orden 12 de S_4 es A_4. por lo tanto $PSL(2,3) \cong A_4$.
y PSL(2,3) no es simple.

C A P I T U L O II

CASOS EN QUE GRUPOS LINEALES ESPECIALES PROYECTIVOS DIFERENTES PSL(n,q) Y PSL(n_1,q_1) TIENEN LA MISMA CARDINALIDAD.

Como se planteo en un principio, esta parte del trabajo demuestra que sólo hay tres casos en que grupos lineales especiales proyectivos diferentes tienen la misma cardinalidad, en dos de estos casos los grupos correspondientes resultan isomorfos y en el otro caso no existe isomorfismo alguno entre los grupos. Así, se tiene :

$$|PSL(2,4)| = |PSL(2,5)| \quad y \quad PSL(2,4) \cong PSL(2,5)$$

$$|PSL(2,7)| = |PSL(3,2)| \quad y \quad PSL(2,7) \cong PSL(3,2)$$

$$|PSL(3,4)| = |PSL(4,2)| \quad y \quad PSL(3,4) \ncong PSL(4,2)$$

Sea N = N(n, q) el orden del grupo lineal especial proyectivo de un espacio vectorial V de dimensión n ≥ 2, sobre un campo F con $q = p^r$ elementos, p primo, y sea d = (n, q-1), por el teorema 3 del capítulo I.

$$\begin{aligned} N = N(n, q) &= (1/d)(q^n-1)(q^n-q) \dots (q^n-q^{n-2})(q^{n-1}) \\ &= (1/d)(q^n-1)q(q^{n-1}-1) \dots q^{n-2}(q-1)(q^{n-1}) \\ &= (1/d)\, q^{n(n-1)/2}\, (q^n-1) \dots (q^2-1) \end{aligned}$$

Si PSL(n_1, q_1) es otro grupo lineal especial proyectivo con $q_1 = p_1^{r_1}$ se intenta reconocer aquellos casos en que

$$(*) \qquad N = (1/d)q^{n(n-1)/2}\,(q^r-1) \dots (q^2-1)$$

$$= (1/d_1)q_1^{n_1(n_1-1)/2}\,(q_1^{r_1}-1)\dots(q_1^2-1)$$

Se usarán resultados expuestos en el apéndice en el siguiente

procedimiento que consiste en recorrer todos los posibles valores de los números n, p, r, n_1, p_1, r_1 .

El siguiente esquema considera los correspondientes subcasos :

Caso I	$p_1 = p$
	1.1 $r_1 n_1 = rn$
	1.2 $2 \le rn < r_1 n_1$, $r_1 n_1 = 6$ $p = 2$
	1.3 $2 \le rn < r_1 n_1$, $r_1 n_1 = 6$ $p = 2$
	a) $n = 3$
	b) $n = 4$ PSL(3,4), PSL(4,2)
	c) $n = 5$
Caso II	$p_1 = p$ $n = 2$
	a) $q \ge 13$
	$n_1 = 3$ $q_1 = 2$ PSL(3,2), PSL(2,7)
	$n_1 = 3$ $q_1 \ge 3$
	b) $q \ge 16$ $n_1 \ge 3$
	c) $n_1 = 2$
	q q_1 impares
	q_1 impar q par
	$q_1 = q + 1$ PSL(2,4), PSL(2,5)
	$q_1 < q - 1$
Caso III	$p_1 = p$ $n = 3$ $n_1 \ge 3$
	$q < 7$
	$q \ge 7$
Caso IV	$p_1 = p$ $\min(n_1, n) \ge 4$ p_1 impar
	a) $q \ge 5$
	b) $q = 4$
	c) $q = 3$
	d) $q = 2$

CASO I

Supóngase que $p_1 = p$

como d_1 y d son primos a p, se tiene

$$r_1 n_1(n_1-1) = rn(n-1) \qquad (1)$$

I.1 Supóngase $r_1 n_1 = rn$, por (1), $n_1-1 = n-1$, $n_1 = n$

al sustituir en $r_1 n_1 = rn$, $r_1 = r$. que resulta el caso trivial en que todos : p, n, r son iguales para los dos grupos.

I.2 Supóngase $2 \leq rn < r_1 n_1$
y si $r_1 n_1 \neq 6$, $p \neq 2$
aplicando el teorema 2 del apéndice con $a = p \neq 2$,
$k = r_1 n_1 \neq 6$
$k = r_1 n_1 > 2$ por hipótesis,
entonces existe un primo p_2 tal que
$p_2 | p^{r_1 n_1} - 1 = q_1^{r_1} - 1$ y $p_2 \nmid p^i - 1$ con $i < r_1 n_1$
es decir $p_2 \nmid q_1 - 1$ y por tanto $p_2 \nmid d_1$
reescribiendo (*)
$d_1 q_1^{r_1(n_1-1)/2} (q_1^{r_1}-1) \cdots (q_1^2-1) = d q_1^{n_1(r_1-1)/2} (q_1^{r_1}-1) \cdots (q_1^2-1)$
se observa que p_2 divide al lado derecho de esta igualdad pero p_2 no divide al lado izquierdo, lo cual no puede ser posible.
En otras palabras este caso de valores no es factible.

I.3 Si $2 \leq rn < r_1 n_1$
y $r_1 n_1 = 6$, $p = 2$
entonces $rn < 6$, si $n_1 - 1 \geq n-1$
$(n-1)(rn) \leq (n_1-1)(rn)$
$< (n_1-1)(r_1 n_1)$ que contradice a (1)
$\therefore \quad n_1 - 1 < n-1 \quad$ y $\quad n_1 < n$
así $\quad 2 \leq n_1 < n \leq rn \leq 5$

Subcaso a)
Si $n = 3$, $rn \leq 5$
$\Rightarrow \quad r = 1$
$n_1 < n \quad \Rightarrow \quad n_1 = 2$
por (1) $\quad r_1(2) = 3(3-1) = 6 \quad \Rightarrow \quad r_1 = 3$
y al sustituir estos valores en (*), se obtiene :

$$q = 2^1 = 2 \qquad d(3, 2-1) = 1$$

$$\therefore \quad 2^{3\cdot 2/2}(2^3-1)(2^2-1) = (8)(7)(3) = 168$$

mientras que

$$q_1 = 2^3 = 8 \qquad d_1(2, 8-1) = 1$$

$\therefore \quad 8^{2(1/2)}(8^2-1) = (8)(63) = 504$

es decir, este caso tampoco es posible.

Subcaso b)

Si $n = 4$, $rn \leq 5$

$\Rightarrow \quad r = 1$

por (1) $\quad 4(3) = 12 = r_1 n_1 (n_1-1) = 6(n_1-1)$

$n_1-1 = 2$ y $n_1 = 3 \quad \therefore \quad r_1 = 2$

al sustituir estos valores en (*), se obtiene :

$q = 2^1 = 2 \qquad d(4, 2-1) = 1$

$\therefore \quad 2^{4\cdot\frac{3}{2}}(2^4-1)(2^3-1)(2^2-1) = 2^6\ (15)(7)(3) = 20160$ y

$q_1 = 2^2 = 4 \qquad d_1(3, 4-1) = 3$

$\therefore \quad \frac{1}{3}\ 4^{3(2/2)}(4^3-1)(4^2-1) = (64)(63)(5) = 20160$

Este es uno de los casos contemplados en que dos grupos PSL(3, 4) y PSL(4, 2) tienen la misma cardinalidad.

Subcaso c)

Si $n = 5$

$\Rightarrow \quad r = 1$

por (1), $\quad 6(n_1-1) = 5(5-1) = 20$

aquí 6 divide el lado izquierdo mientras que al lado derecho no lo divide, por lo tanto este caso de valores queda excluído.

CASO II.

Supóngase $\qquad p_1 \neq p \quad$ y $\quad n = 2$

Subcaso a). $\quad q \leq 13$

$n = 2 \quad \Rightarrow \quad (1/d)q(q^2-1) = (1/d)q(q+1)(q-1)$

$= (1/d_1)q_1^{n_1(n_1-1)/2}(q_1^{n_1} - 1) \ldots (q_1^2 - 1) \qquad (2)$

y $\quad q \leq 13 \quad \Rightarrow$

$(1/d)q(q+1)(q-1) \leq (1/d)(13)(14)(12) = (1/d)(2^3)(3)(7)(13)$

que no es divisible por la sexta potencia de algún primo, de aquí que $n_1 \geq 3$

si $n_1 = 3$ y $q_1 = 2$, sustituyendo los valores en el lado derecho de (2) se obtiene

$$N = 2^{3\,2\cdot 2}(2^3-1)(2^2-1) = 2^9(7)(3) = 168$$

como $n = 2$, entonces $q = 7$
que resulta ser el segundo caso excepcional entre PSL(3, 2) y PSL(2, 7).

Si $n_1 = 3$ y $q_1 \geq 3$
$d_1(n_1, q_1-1) = d_1(3, q_1-1) \Rightarrow d_1 < 3$ y $1/d_1 \geq \frac{1}{3}$
así que

$$N = (1/d_1)q_1^{3(2\cdot 2)}(q_1^3-1)(q_1^2-1)$$

$$\geq \tfrac{1}{3}\, 3^3(3^3-1)(3^2-1)$$

$$= 3^2(13)(2^1) = 1872$$

mientras que el valor mayor para $q \leq 13$ es

$$q(q-1)(q+1) \leq (13)(12)(14) = 2184$$
$$N = \tfrac{1}{2}\, q(q-1)(q+1) \leq 1092, \quad (d \leq 2)$$

por tanto este caso es desechado.

Subcaso b). $q \geq 16$, $n_1 \geq 3$

$$N = (1/d_1)q_1^{n_1(n_1-1)\cdots 2}(q_1^{n_1}-1)\cdots(q_1^2-1)$$

$$< q_1^{n_1(n_1-1)\cdots 2}\, q_1^{n_1}\, q_1^{(n_1-1)}\cdots q_1^2 = q_1^{n_1^2-1} \qquad (3)$$

y de (2) $\quad (1/d)q(q-1)(q+1) < q_1^{n_1^2-1}$

$n = 2 \Rightarrow$

$$\tfrac{1}{2}\, q^3(1-1/q)(1+1/q) = \tfrac{1}{2}\, q(q-1)(q+1)$$
$$\leq (1/d)q(q-1)(q+1) < q_1^{n_1^2-1}$$

Si p_1 es impar $(d_1, p_1) = 1$ ya que $d_1 \mid p_1^{r_1}-1$

$q_1^{n_1(n_1-1)/2}$ debe dividir a $q-1$ ó $q+1$

Si $p_1 = 2$, entonces p es impar y d = 2, en cualquier caso

$$q_1^{n_1(n_1-1)/2} \quad \text{divide a} \quad q-1 \text{ ó } q+1$$

$$\therefore \quad q_1^{n_1(n_1-1)/2} \leq q+1 \qquad (4)$$

por otra parte, como $n_1 \geq 3$, $\quad 2n_1 \geq 6$

$$8n_1 \geq 6n_1 + 6 = 6(n_1+1)$$
$$\tfrac{4}{3}\, 8n_1 \geq 2(n_1+1)$$
$$\tfrac{4}{3}\, 8 \geq 2(n_1+1)/n_1 \qquad (5)$$

elevando (4) a la potencia $2(n_1+1)/n_1 \leq 8/3$

$$\left(q_1^{n_1(n_1-1)/2}\right)^{2(n_1+1)/n_1} \leq (q+1)^{8/3}$$

$$q_1^{n_1^2-1} \leq (q+1)^{8/3}$$

por transitividad

$$\tfrac{1}{2}\, q^3(1 - 1/q)(1 + 1/q) < (q+1)^{8/3}$$
$$= q^{8/3}\left(\frac{q+1}{q}\right)^{8/3}$$
$$= q^{8/3}(1 + 1/q)^{8/3}$$

dividiendo esta desigualdad por $q^{8/3}$ y multiplicando por 2,

$$q^{1/3}(1 - 1/q)(1 + 1/q) < 2(1 + 1/q)^{8/3}$$

así $$q^{1/3} < \frac{2(1 + 1/q)^{8/3}}{1 - 1/q}$$

como $q \geq 16$, $\quad \Rightarrow \quad 1 + 1/q \leq 1 + 1/16$, $\quad 1 - 1/q \geq 1 - 1/16$

y $$\frac{1}{1 - 1/q} \leq \frac{1}{1 - 1/16}$$

$$\therefore \quad q^{1/3} < \frac{2(1 + 1/q)^{5/3}}{1 - 1/q} \leq \frac{2(1 + 1/16)^{5/3}}{1 - 1/16} = \frac{2(17/16)^{5/3}}{15/16}$$

$$q^{1/3} < \frac{2(17)^{5/3}}{15(16)^{2/3}}$$

elevando al cubo,

$$q < \frac{2^3 17^5}{15^3 16^2} = \frac{2^3 17^5}{2^8 15^3} = \frac{17^5}{2^5 15^3} = 13.15 < 14$$

que es una contradicción a $q \geq 16$,
por lo tanto este caso no es posible.

Subcaso c) $n_1 = 2$
ahora se tiene $(1/d_1)\, q_1(q_1 + 1)(q_1 - 1) = (1/d)q(q + 1)(q - 1)$

Si q y q_1 son impares, entonces $d = d_1 = 2$

como q_1 no puede dividir a q+1 ó q-1 porque son pares,
por lo tanto $q_1 | q$, $\therefore \quad q_1 = q$

Si q_1 es impar y q es par entonces $d_1 = 2$ y $d = 1$, por lo tanto

$$q_1(q_1 + 1)(q_1 - 1) = 2q(q + 1)(q - 1)$$

Si $q \geq q_1$, entonces $q(q+1)(q-1) \geq q_1(q_1+1)(q_1-1)$
contradicción.
por tanto $q < q_1$

además q_1 divide a $q + 1$ ó $q - 1$.

Si es igual a algún factor, sólo puede ser a $q + 1$
entonces $q_1 + 1 = q + 2$ $\qquad q_1 - 1 = q$

y $\qquad (q + 1)(q + 2)q = 2q(q + 1)(q - 1) \rightarrow$

$q + 2 = 2q - 2, \quad \rightarrow \quad q = 4 \quad$ y $\quad q_1 = 5$

que resulta el otro caso especial entre los grupos PSL(2, 4) y PSL(2, 5).

Si q_1 es divisor propio de $q + 1$, como $q_1 > 0$ y $q + 1 > 0$

$q + 1 = tq_1$ para algún $t > 0$

$t = 1$ $q + 1 = q_1$, ya considerado

$\therefore$ $t \geq 2$, y $q + 1 = tq_1 \geq 2q_1$

$\therefore$ $q_1 \leq \frac{1}{2}(q + 1)$ así que $q < q_1 < \frac{1}{2}(q + 1)$

entonces $q < 1$, que no es posible.

CASO III.

Suponer $p_1 \neq p$ $n = 3$ $n_1 \geq 3$

ahora se tiene

$$(1/d_1)q_1^{n_1(n_1-1)/2}(q_1^{n_1} - 1) \ldots (q_1^2 - 1) = (1/d)q^3(q^3-1)(q^2-1) \quad (6)$$

$$= (1/d)q^3(q^2+q+1)(q+1)(q-1)^2$$

luego $d(3, q-1) \leq 3$ y $1/d \geq \frac{1}{3}$, así

$$\tfrac{1}{3}\, q^3(q^2+q+1)(q+1)(q-1)^2 \leq (1/d)q^3(q^2+q+1)(q+1)(q-1)^2$$

$$= (1/d)q^6(1 + 1/q + 1/q^2)(1 + 1/q)(1 - 1/q)^2 \quad (7)$$

por transitividad de (7), (6) y (3), se tiene

$$\tfrac{1}{3}\, q^6(1 + 1/q + 1/q^2)(1 + 1/q)(1 - 1/q)^2 \leq N \leq q_1^{n_1^2-1}$$

además $$\tfrac{1}{3}\, q^6(1 - 1/q)^2 < q_1^{n_1^2-1} \quad (8),$$

porque $1 < (1 + 1/q + 1/q^2)(1 + 1/q)$.

observándose los primeros valores para q :

$q = 2$ $d(3, 1) = 1$, $N = 2^3(2^3-1)(2^2-1) = 2^3(7)(3)$

$q = 3$ $d(3, 2) = 1$, $N = 3^3(3^3-1)(3^2-1) = 2^4 3^3(13)$

$q = 4$ $d(3, 3) = 3$, $N = \frac{1}{3}4^3(4^3-1)(4^2-1) = 2^6 3^2(5)(7)$

$q = 5$ $d(3, 4) = 1$, $N = 5^3(5^3-1)(5^2-1) = 2^5(3)5^3(31)$

como $p_1^{n_1 n_1(n_1-1)/2}$ debe ser la contribución exacta de P_1 a N, el exponente de p_1 debe ser divisible por

$$\tfrac{1}{2}\, n_1(n_1-1) = 3, 6, 10, 15, 21, 28. \ldots$$

que en cada caso se tiene lo siguiente :

$q = 2$ $p_1 = 2, 7$ ó 3 y el exponente de p_1 debe ser divisible

por 3, 6, 10, ... $\therefore \quad p_1 = 2 = p^1 = q$

$q = 3$ con el mismo argumento $p_1 = 3 = p$

y sucesivamente para los casos $q = 4, 5$ se llega a $p_1 = p$

contrario a la hipótesis : $p_1 \neq p$.

Así estos casos quedan excluídos.

$\therefore \quad q \geq 7$.

Sea f el orden de q en $\mathbb{Z}_{p_1}^*$, es decir el mínimo valor de n tal que $q^n \equiv 1 \pmod{p_1}$

en otras palabras $p_1 | q^f - 1$ y $p_1 \nmid q^n - 1$ si $n < f$

como

$q_1^{p_1(p_1-1)/2} \equiv p_1^{r_1 p_1(p_1-1)/2}$ divide el lado derecho de (6)

entonces $f \leq 3$, así se tiene,

si $f = 3 \Rightarrow p_1 | q^3 - 1 = (q^2 + q + 1)(q - 1)$

y como $p_1 \nmid q-1 \Rightarrow p_1 | q^2+q+1$ y $p_1 \leq q^2+q+1$

si $f = 2$, $p_1 | q^2-1 = (q+1)(q-1)$ y $p_1 | q+1$ ya que $p_1 \nmid q-1$

si $f = 1$ y $p_1 = 3 \Rightarrow p_1 | q-1$ y $3 | 3(q-1)^2$

si $f = 1$ y $p_1 = 2 \Rightarrow p_1 | q-1$ y $2 | 2(q-1)^2$

además $p_1 | q-1 = q+1-2$, $p_1 | q+1$

$\therefore \quad p_1 | 4(q+1)$

si $f = 1$, $p_1 \neq 2, 3 \Rightarrow p_1 | (q-1)^2$

claramente el término $3(q-1)^2$ es mayor o igual a los otros casos, pues si $q \geq 7$

$q^2 \geq 7q$

$q^2+1 > q^2$ y $2(q^2+1) > q^2+1$

así que $2(q^2+1) > 7q$

$2q^2 + 2 - 7q > 0$

$3q^2 - 6q + 3 - q^2 - q - 1 > 0$

$3q^2 - 6q + 3 > q^2 + q + 1$

$3(q^2 - 2q + 1) > q^2 + q + 1$

$$3(q-1)^2 > q^2 + q + 1$$

y para el otro término

$q \geq 7,$

$$3q \geq 21$$
$$3q - 10 \geq 11$$
$$q(3q - 10) \geq 77 > 1$$
$$3q^2 - 10q > 1$$
$$3q^2 - 10q - 1 > 0$$
$$3q^2 - 6q - 4q + 3 - 4 > 0$$
$$3q^2 - 6q + 3 > 4q + 4$$
$$3(q^2 - 2q + 1) > 4(q + 1)$$
$$3(q-1)^2 > 4(q + 1)$$

por lo tanto $q_1^{n_1(n_1-1)/2} \leq 3(q - 1)^2$ (9)

además $n_1 \geq 3 \quad \Rightarrow \quad 2n_1 \geq 6$

$$2n_1 + 6n_1 \geq 6n_1 + 6$$
$$8n_1 \geq 6(n_1 + 1)$$
$$8/3 \geq 2(n_1 + 1)/n_1$$

así que elevando (9) a la potencia $2(n_1 + 1)/n_1 \leq 3/3$ se tiene

$$\left[q_1^{n_1(n_1-1)/2}\right]^{2(n_1+1)/n_1} \leq \left(3(q-1)^2\right)^{8/3}$$

$$q_1^{n_1^2-1} \leq 3^{8/3}(q-1)^{16/3}$$

aplicando transitivamente (8) y esta última desigualdad

$$\frac{1}{5}\, q^8(1 - 1/q)^2 < q_1^{n_1^2-1} \leq 3^{8/3}(1 - 1/q)^{16/3} q^{16/3}$$

multiplicando por 3

$$q^8(1 - 1/q)^2 < 3^{11/3}(1 - 1/q)^{16/3}\, q^{16/3}$$

dividiendo por $(1 - 1/q)^2$

$$q^8 < 3^{11/3}(1 - 1/q)^{10/3} q^{16/3}$$

dividiendo por $q^{16/3}$

$$q^{8/3} < 3^{11/3}(1 - 1/q)^{10/3}$$

como $(1 - 1/q)^{10/9} < 1$, $\Rightarrow$ $q^{10/9} < 3^{11/9}$

y $q^{9} < 3^{11}$, $q < 3^{11/9} < 3^{12/9} = 3^{3/2} = \sqrt{27} < 6$

contrario al hecho de que $q \geq 7$,

así que estos casos son desechados.

CASO IV.

Suponer $p_1 \neq p$, $\min(n_1, n) \geq 4$ y sea p_1 impar.

N es dividido exactamente por $p_1^{r_1 n_1 (n_1-1)/2}$ y este número debe

por lo tanto dividir a $(q^n-1)(q^{n-1}-1) \cdots (q^2-1)(q-1)$

sea f el orden de q en $\mathbb{Z}_{p_1}^*$

es decir, $q^f \equiv 1 \pmod{p_1}$ ó $p_1 | q^f-1$ y a ninguna otra potencia menor que f.

Por la proposición 3 del apéndice ,

$$p_1 | q^n-1 \quad \Leftrightarrow \quad f | n$$

luego, si $p_1 | q^k-1$ con $n \geq k > f$

entonces $f | k$ y $k = fi$ para algún i.

si $i \leq n/f$, $k = fi \leq n$ $\therefore$ $i \leq \lfloor n/f \rfloor$, el máximo entero menor o igual que n/f.

Es decir puede haber a lo más $\lfloor n/f \rfloor$ números k tales que $p_1 | q^k-1$,

Por el lema 1, t.e) del apéndice,

$\text{ord}(q^k-1) = \text{ord}(q^{fi}-1) = \text{ord}(q^f-1) + \text{ord}\, i$

puesto que $\text{ord}\, k = \text{ord}(fi) = \text{ord}\, f + \text{ord}\, i = 0 + \text{ord}\, i$

sea $\text{ord}(q^f-1) = \alpha$, esto es, α es el máximo exponente de p_1 tal

que $p_1^{\alpha} | q^f-1$

sea $p_1^{\alpha} = x$ ó equivalentemente $\log_{p_1} x = \alpha = \ln x / \ln p_1$

sustituyendo se tiene $\text{ord}(q^f-1) = \ln x / \ln p_1$

y $\ln x = \ln p_i^{\alpha} < \ln q^f$ puesto que $p_i^{\alpha} \leq q^f - 1 < q^f$

por lo tanto $\dfrac{\ln x}{\ln p_i} < \dfrac{\ln q^f}{\ln p_i}$ $(\ln p_i > 0)$

y $\lceil n/f \rceil \text{ord}\ (q^f-1) < \dfrac{n \ln q^f}{f \ln p_i}$

además

$$\frac{n \ln q^f}{f \ln p_i} = \frac{\ln (q^f)^n}{f \ln p_i} = \frac{\ln (q^n)^f}{f \ln p_i} = \frac{f \ln q^n}{f \ln p_i} = \frac{\ln q^n}{\ln p_i}$$

$$\therefore \quad \lceil n/f \rceil \text{ord}\ (q^f-1) < \frac{\ln q^n}{\ln p_i}$$

por otra parte el orden de i, con $i = 1, \ldots, \lceil n/f \rceil$, es menor o igual a e, donde e es el mayor exponente [cf. 3] tal que

$$p_i^{e} \mid \lceil n/f \rceil !$$

$$e = \sum_{i=1}^{\infty} \left[\frac{n/f}{p_i^i} \right] = \sum_{i=1}^{\infty} \left[\frac{n}{f p_i^i} \right] < \sum_{i=1}^{\infty} \frac{n}{f p_i^i} = \frac{n}{f} \sum_{i=1}^{\infty} \frac{1}{p_i^i}$$

como

$$\sum_{i=0}^{\infty} \frac{1}{p_i^i} = \frac{p_i}{p_i - 1} = 1 + \sum_{i=1}^{\infty} \frac{1}{p_i^i}$$

se tiene $$\sum_{i=1}^{\infty} \frac{1}{p_i^i} = \frac{p_i}{p_i - 1} - 1 = \frac{1}{p_i - 1}$$

entonces $e < \dfrac{n}{f}\left(\dfrac{1}{p_i - 1}\right) \leq \dfrac{n}{p_i - 1}$ ya que $1 \leq f$,

por lo tanto la potencia de p_i que divide a $(q^n-1)(q^{n-1}-1) \ldots (q-1)$, es menor que

$$p_i^{\ln q^n / \ln p_i \; p_i^{n/p_i - 1}}$$

aplicando la proposición 8 del apéndice con $x = p_1 \geq 2$

$$3^{1+3-1} \geq p_1^{1+p_1-1}$$

que elevando a la n_1 $\quad 3^{n_1+2} \geq p_1^{n_1(p_1+1)}$

y además como $\quad \ln q^n / \ln p_1 = \log_{p_1} q^n$

si $z = \log_{p_1} q^n$ es decir $p_1^z = q^n$, entonces

$$p_1^{(n_1+3)^{n_1}} \cdot p_1^{n_1(p_1-1)} = p_1^{z+n_1} p_1^{z-n_1} = p_1^{2z} = q^{2n}$$

de modo que $\quad p_1^{(n_1+3)^{n_1}} \cdot p_1^{n_1(p_1-1)} \leq q^{2n} 3^{n_1+2}$

por lo tanto $\quad q_1^{n_1(n_1-1)/2} < q^n 3^{n_1+2}$ $\qquad$ (10)

ahora, como $\quad 4 \leq n_1$

$$4 + 4n_1 \leq n_1 + 4n_1$$

$$4(1 + n_1) \leq 5n_1$$

$$2(1 + n_1) \leq 5/2\ (n_1)$$

$$2(1 + n_1)/n_1 \leq 5/2$$

y elevando (10) a la potencia $2(1 + n_1)/n_1 \leq 5/2$, se tiene

$$\left(q_1^{n_1(n_1-1)/2}\right)^{2(n_1+1)/n_1} < \left(q^n 3^{n_1+2}\right)^{5/2}$$

$$q_1^{n_1^2-1} < q^{5n/2} 3^{5n/4}$$

puesto que $3^5 < 4^4$ $\quad (243 < 256)$, se tiene

$$N < q_1^{n_1^2-1} < q^{5n/2} 4^n \qquad (11)$$

ya que

$$N = (1/d)q^{n(n+1)/2}(q^n-1)(q^{n-1}-1) \ldots (q^2-1)$$

$$= (1/d)q^{n(n+1)/2}(1 - 1/q^n)q^n(1 - 1/q^{n-1})q^{n-1} \ldots (1 - 1/q^2)q^2$$

$$= (1/d)q^{n(n+1)/2} q^{n(n+1)/2 - 1}(1 - 1/q^n) \ldots (1 - 1/q^2)$$

$$= (1/d)q^{n^2-1}(1 - 1/q^2) \ldots (1 - 1/q^n)$$

luego $\sum_{i=2}^{\infty} \frac{1}{q^i} > \sum_{i=2}^{n} \frac{1}{q^i} \quad \rightarrow \quad 1 - \sum_{i=2}^{\infty} \frac{1}{q^i} < 1 - \sum_{i=2}^{n} \frac{1}{q^i}$

como $0 \leq 1/q^i \leq 1$, por la proposición 9 del apéndice

$$1 - \sum_{i=2}^{n} \frac{1}{q^i} \leq \prod_{i=2}^{n} (1 - 1/q^i)$$

transitivamente $\quad 1 - \sum_{i=2}^{\infty} \frac{1}{q^i} < \prod_{i=2}^{n} (1 - 1/q^i)$

que al sustituir en N,

$$N = (1/d)q^{n^2-1} \prod_{i=2}^{n} (1 - 1/q^i) > (1/d)q^{n^2-1}(1 - \sum_{i=2}^{\infty} \frac{1}{q^i}) \qquad (12)$$

se sabe que $\quad \sum_{i=0}^{\infty} \frac{1}{q^i} = \frac{1}{1 - 1/q} = \frac{q}{q-1} = 1 + \frac{1}{q} + \sum_{i=2}^{\infty} \frac{1}{q^i}$

de aquí $\quad \sum_{i=2}^{\infty} \frac{1}{q^i} = \frac{q}{q-1} - \frac{q+1}{q} = \frac{1}{q(q-1)}$

y $\quad 1 - \sum_{i=2}^{\infty} \frac{1}{q^i} = 1 - \frac{1}{q(q-1)} \qquad (13)$

por (11),(12) y (13)

$$(1/d)q^{n^2-1}(1 - 1/q(q-1)) < q^{5n/2} 4^n$$

multiplicando por q

$$(1/d)q^{n^2}(1 - 1/q(q-1)) < q^{5n/2+1} 4^n$$

multiplicando por d y dividiendo por $1 - 1/q(q-1)$

$$(q^n)^n = q^{n^2} < \frac{d}{1 - 1/q(q-1)} \; q^{5n/2+1} 4^n$$

extrayendo raiz n-ésima

$$q^n < 4\left(\frac{d}{1 - 1/q(q-1)}\right)^{1/n} q^{3/2 + 1/n}$$

puesto que $n \geq 4$, se sustituye 4 por n en la derecha

$$q^n < 4\left(\frac{d}{1 - 1/q(q-1)}\right)^{\frac{1}{4}} q^{3/2 + \frac{1}{4}} = 4\left(\frac{d}{1 - 1/q(q-1)}\right)^{\frac{1}{4}} q^{3-\frac{1}{4}}$$

esta última relación se analizará para los diferentes valores de q.

a) $q \geq 5$

$d \leq q-1 \quad \Rightarrow \quad 1/q \leq 1/5, \quad q-1 \leq 4, \quad 1/q-1 \geq 1/4$

$$\frac{1}{q}\left(\frac{1}{q-1}\right) \leq \frac{1}{5}\left(\frac{1}{4}\right) = \frac{1}{20} \quad \Rightarrow \quad -\frac{1}{q(q-1)} \geq -\frac{1}{20}$$

$$\frac{1}{1 - 1/q(q-1)} \leq \frac{1}{1 - 1/20}$$

como $\frac{1}{20} < \frac{1}{5}$, $\Rightarrow$ $\frac{1}{1 - 1/20} < \frac{1}{1 - 1/5}$

por lo tanto $\frac{1}{1 - 1/q(q-1)} < \frac{1}{1 - 1/5} = \frac{1}{4/5} = \frac{5}{4}$

luego $q^n < 4(5d/4)^{\frac{1}{n}} q^{3-\frac{1}{n}} < 4(5/4)^{\frac{1}{4}} q^{\frac{1}{4}} q^{3-\frac{1}{4}} \qquad (d \leq q-1 < q)$

$$q^n < 4(5/4)^{1/4} q^3 = (4^3(5))^{1/4} q^3$$

$$= \sqrt[4]{320}\; q^3 = (4.23)q^3 < 5q^3 \leq qq^3 = q^4$$

por lo tanto $n < 4$. Contradicción ($n \geq 4$).
Este caso no es factible.

b) Si $q = 4$, $d \leq 3$,

$$\frac{1}{q} = \frac{1}{4} \quad \Rightarrow \quad \frac{1}{q}\left(\frac{1}{q-1}\right) = \frac{1}{12}$$

$$\frac{1}{12} < \frac{1}{4} \quad \Rightarrow \quad \frac{1}{1 - 1/12} < \frac{1}{1 - 1/4}$$

$$\therefore \quad \frac{1}{1 - 1/q(q-1)} < \frac{1}{1 - 1/4} = \frac{1}{3/4} = \frac{4}{3}$$

luego $4^n = q^n < 4(3(4/3))^{\frac{1}{4}} 4^{3-\frac{1}{4}} = 4(4^{\frac{1}{4}}) 4^{3-\frac{1}{4}} = 4^4$
asi que $n < 4$. Contradicción.

c) Si $q = 3$, $P_1 \geq 5$ puesto que P_1 es impar diferente de P.
Si se intercambian los papeles de q con q_1 en el caso a).

$q_1 \geq 5$ y $q_1^{n_1} < q_1^4$ $\Rightarrow$ $n_1 < 4$, contradicción.

d) Si $q = 2$, $d = 1$

$$\frac{d}{1 - 1/q(q-1)} = 2$$

y $q^n = 2^n < 4(2^{\frac{1}{4}})(2^{3-\frac{1}{4}}) = 4(2^3) = 2^5$

$\Rightarrow$ $n < 5$, $n = 4$

pero $N = 2^{4(3/2)}(2^4-1)(2^3-1)(2^2-1)$

$= 2^6(3)(5)(7)(3) = 2^6(3^2)(5)(7)$

ningún primo impar p_1 tiene potencia $n_1 \geq 1$
por tanto, no es posible este caso.
De esta forma se han recorrido todos los posibles valores para p, p_1, n, n_1, r, r_1, lo cual demostró que sólo hay tres casos posibles en que grupos diferentes PSL(n,q) tienen la misma cardinalidad.

Ahora se procede a estudiar si existen o no isomorfismos entre los grupos PSL(n,q) que tienen la misma cardinalidad.

TEOREMA. Sea G un grupo simple de orden 60, entonces $G \cong A_5$.

DEMOSTRACION.

Primero se probará que G contiene un subgrupo H de índice 5.
$|G| = 2^2(3)(5)$, sea $\Pi = \{2, 3, 5\}$
si $p \in \Pi$ sea N_p el número de p-subgrupos de Sylow de G.

entonces $N_p \equiv 1 \pmod p$ $\quad N_p = [G : N_G(B)]$,
donde B es un p-subgrupo de sylow de G y
$N_G(B) = \{g \in G \mid g^{-1}Bg = B\}$ es el estabilizador de B en G.

Ahora se demuestra que $[G : N_G(B)] = 5$ para algún p-subgrupo de sylow B.
Supóngase $k = [G : N_G(B)] < 5$ para algún p-subgrupo de Sylow B,
Si X es el conjunto de clases laterales derechas de $N_G(B)$ en G,
el grupo $S_k = S_X$, con $k < 5$,
según Caley existe un homomorfismo $\varphi : G \rightarrowtail S_k$,
como $|S_k| = k!$ y $k! < 60$, $(|G| = 60)$
entonces φ no es inyectivo,
por lo tanto $\langle e\rangle \neq Núc\ \varphi \lhd G$
entonces G no es simple (contradicción).

De aquí que $N_p \geq 5$
Ahora supóngase que $k = [G : N_G(B)] > 5$ para todo B,
con B un p-subgrupo de Sylow.
Analizando los valores de N_p :
$N_5 = 5t + 1$, $N_5 | 2^2(3)(5) \rightarrow t = 1$ y $N_5 = 6$

$N_3 = 3t + 1$, $t = 1$ ó $t = 3$ entonces $N_3 = 4$ ó 10
$N_3 = 4$ no puede suceder por lo expuesto anteriormente
$\therefore N_3 = 10$

$N_2 = 2t + 1$, $t = 1, 2$ ó 7 entonces $N_2 = 3, 5$ ó 15
$N_2 = 3$ ó 5 no están contemplados en la hipótesis $N_p > 5$
$\therefore N_2 = 15$.

Ahora sean B_1, B_2 dos 2-subgrupos de Sylow, $B_1 \neq B_2$
Si $B_1 \cap B_2 = B \neq \langle e\rangle$, como B es abeliano $i = 1, 2$,

$B \lhd \langle B_1, B_2\rangle = T \neq G$, porque G es simple

$\therefore \quad 4 < |T| < 60, \qquad y \qquad |T| = 12 \quad ó \quad 20$

entonces $[G : N_G(T)] = 5$ (contradicción) ó

$[G : N_G(T)] = 3$ (contradicción),

$\therefore \quad B_1 \cap B_2 = \langle e \rangle$, así que $N_2 = 15$.

Por lo tanto en G existen :

$N_2(4-1) = 45$ elementos de orden una potencia de 2,

$N_3(3-1) = 20$ elementos de orden 3 y

$N_5(5-1) = 24$ elementos de orden 5,

contradicción, $|G| = 60$.

Por lo tanto G tiene un subgrupo H de índice 5, el cual es el normalizador de un p-subgrupo de Sylow de G.

Sea pues $H < G$ de índice 5,

y $X = \{H, Hx_1, Hx_2, Hx_3, Hx_4\}$, entonces $S_X = S_5$

existe un homomorfismo inyectivo $\varphi : G \rightarrowtail S_5$

$\varphi(G) < S_5$ y $|\varphi(G)| = 60$, $\therefore \quad \varphi(G) \cong A_5$.

en efecto :

Si $K < S_5$, $|K| = 60$, entonces $K \cong A_5$,

$[S_5 : K] = 2$, entonces $K \lhd S_5$

si $K \neq A_5$, entonces $KA_5 = S_5$

$$120 = |KA_5| = \frac{|K||A_5|}{|K \cap A_5|} \quad \Rightarrow \quad 2 = \frac{|A_5|}{|K \cap A_5|}$$

entonces $K \cap A_5 \lhd A_5$ (contradicción).

$\therefore \quad G \cong \varphi(G) \cong A_5$ ∎

COROLARIO. PSL(2,4) y PSL(2,5) son isomorfos a A_5.

TEOREMA. $PSL(2,7) \cong PSL(3,2)$.

DEMOSTRACION.

$PSL(2,7)$ es simple de orden $168 = 2^3(3)(7) = \frac{1}{2}\, 7(7^2-1)$,

si s_7 el número de 7-subgrupos de Sylow de $PSL(2,7)$, entonces

$s_7 \equiv 1 \pmod 7$ y $s_7 \mid 2^3(3)(7)$ $\therefore$ $s_7 = 1$ ó 8.
como PSL(2,7) es simple, entonces $s_7 = 8$.
PSL(2,7) es un grupo de permutaciones sobre los 8 conjugados de un 7-subgrupo de Sylow B .
Por un teorema de Frobenius PSL(2,7) es el único grupo simple de orden $\frac{1}{2}\,7(7^2-1)$.
Por lo tanto, como PSL(3,2) es simple de orden $\frac{1}{2}\,7(7^2-1)$, implica PSL(3,2) $\cong$ PSL(2,7) ∎

Ahora corresponde observar que PSL(4,2) y PSL(3,4) son grupos no isomorfos, así se tienen dos grupos simples con la misma cardinalidad, 20160, los cuales no son isomorfos.

TEOREMA. PSL(4,2) $\not\cong$ PSL(3,4).

DEMOSTRACION. Se observa que F_4^* es un grupo cíclico de orden 3,
se sigue que si $g \in Z(GL(3,4))$, entonces $g^3 = 1$
sea $\overline{\sigma} \in PSL(3,4)$ tal que $\overline{\sigma}^{\,2} = 1$,
sea $\sigma \in SL(3,4)$ tal que $\sigma \in \overline{\sigma}$
$\overline{\sigma}^{\,2} = 1 = Z(SL(3,4))$ significa que $\sigma^2 \in Z(SL(3,4))$
$\therefore$ $\sigma^3 = 1$
el elemento σ^3 cae en la clase $\overline{\sigma}^{\,3} = \overline{\sigma}$
se considerará σ^3 en lugar de σ, por lo tanto $\sigma^2 = 1$.
Tomando la transformación lineal $\mathfrak{T}(x) = x + \sigma x$, $x \in V$.
Sea H = Núc $\mathfrak{T}$, entonces $V/H \cong \mathfrak{T}(V)$,
de aquí que $3 = \dim V = \dim H + \dim \mathfrak{T}(V)$.

Si $\dim H = 3$, entonces $\mathfrak{T}(V) = 0$ y $x + \sigma x = 0$ $\forall\, x \in V$,
$\sigma x = x$ (caracteriztica 2), por lo tanto $\sigma = 1$,
contrario a lo supuesto, orden $\sigma = 2$.
Se sigue que $\dim H \leq 2$.

Para $x \in H$, $\mathfrak{T}(x) = 0 = x + \sigma x$, $\Rightarrow$ $\sigma x = x$, esto es H consiste de los elementos fijos por la izquierda por σ.

Los elementos en $I(V)$ son fijos por la izquierda por σ, puesto que $\sigma(x + \sigma x) = \sigma x + \sigma^2 x = \sigma x + x$, entonces $I(V) \subset H$

$\therefore$ dim $I(V) \leq$ dim H.

Esto deja dim H = 2 como única posibilidad, es decir, H es un hiperplano.

$x \in H$ si y sólo si, $\sigma x = x$

si $x \in V$, $T(\sigma(x) - x) = \sigma(x) - x + \sigma(\sigma(x) - x)$

$= \sigma(x) - x + \sigma^2(x) - \sigma(x)$

$= \sigma(x) - x + x - \sigma(x) = 0$

es decir $\sigma(x) - x \in H$

$\therefore$ σ es una transversión según H, $\sigma \neq E$.

Puesto que n = 3, cualesquiera dos transversiones diferentes de la identidad son conjugadas, de aquí que los elementos de orden 2 en PSL(3,4) forman un único conjunto de elementos conjugados.

Se observa que $GL(4,2) \cong SL(4,2) \cong PSL(4,2)$.

sea $\{v_1, v_2, v_3, v_4\}$ una base de V

Entre los elementos de orden 2 tenemos primero :

$T : V \rightarrowtail V$ tal que

$T(v_1) = v_1$, $T(v_2) = v_1 + v_2$, $T(v_3) = v_3$, $T(v_4) = v_4$

T es transversión, $T \neq E$ y $T^2 = E$, la cual forma una clase de elementos conjugados.

ahora si $T_2 : V \rightarrowtail V$ es la función lineal

$T_2(v_1) = v_1$, $T_2(v_2) = v_1 + v_2$, $T_2(v_3) = v_3$, $T_2(v_4) = v_3 + v_4$,

se tiene que $T_2^2 = E$ pero T_2 no es transversión.

Por lo tanto los elementos de orden 2 forman al menos dos conjuntos de elementos conjugados.

$\therefore$ $PSL(3,4) \ncong PSL(4,2)$. ■

CASOS EN QUE GRUPOS LINEALES ESPECIALES PROYECTIVOS PSL(n,q) TIENEN LA MISMA CARDINALIDAD DE ALGUN GRUPO ALTERNANTE A_m

1) $n = 2 \quad q = 3 \quad N = \frac{1}{2}\,4!$
2) $n = 2 \quad q = 4 \quad N = \frac{1}{2}\,5!$
3) $n = 2 \quad q = 5 \quad N = \frac{1}{2}\,5!$
4) $n = 2 \quad q = 9 \quad N = \frac{1}{2}\,6!$
5) $n = 3 \quad q = 4 \quad N = \frac{1}{2}\,8!$
6) $n = 4 \quad q = 2 \quad N = \frac{1}{2}\,8!$

Se demostrará que son los únicos casos.

Sea $N = (1/d)q^{n(n-1)/2}(q^n-1)\ \ldots\ (q^2-1) = \frac{1}{2}\,m!$

$q^{n(n-1)/2} = p^{\ell n(n-1)/2}$

es la potencia exacta de p que divide a N,

como se mencionó anteriormente, si p es primo y n es un entero positivo, el mayor exponente θ tal que $p^{\theta} \mid n!$ está dado por

$$\theta = \sum_{i=1}^{\infty} \lfloor n/p^i \rfloor$$

de aquí que $p^{\ell n(n-1)/2} = p^{\theta} \mid m!$ es tal que

$$\theta = \tfrac{1}{2}\,\ell n(n-1) = \sum_{i=1}^{\infty} \lfloor m/p^i \rfloor = \lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \ldots$$

si $p \neq 2$, $p^{\theta} \mid \frac{1}{2}\,m!$.

para $p = 2$ $\quad 2^{\theta} \mid m! \qquad \theta = \lfloor m/2 \rfloor + \lfloor m/2^2 \rfloor + \ldots$

$m! = k2^{\theta} = k2^{1+(\theta-1)}$ p. a. k entero

$m! = k2(2^{\theta-1})$

$\therefore \quad \frac{1}{2}\,m! = k2^{\theta-1}$

es decir la máxima potencia de 2 que divide a $\frac{1}{2}\,m!$ es

$$\tfrac{1}{2}\,\ell n(n-1) = \theta - 1$$

ó $\qquad 1 + \tfrac{1}{2}\,\ell n(n-1) = \theta = \lfloor m/2 \rfloor + \lfloor m/2^2 \rfloor + \ldots$

como $\quad \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor < \sum_{i=1}^{\infty} \frac{m}{p^i} = m \sum_{i=1}^{\infty} \frac{1}{p^i} = \frac{m}{p-1}$

$\tfrac{1}{2}\,\ell n(n-1) < m/p-1$

$$\therefore \quad p^{rn(n-1)/2} = q^{r(n-1)/2} < p^{m/p-1} \qquad (13)$$

luego como $n \geq 2$, $\quad 3n \geq 2n + 2$

$$3n \geq 2(n + 1)$$

$$3 \geq 2(n + 1)/n$$

elevando (13) a la potencia $3 \geq 2(n+1)/n$

$$(p^{rn(n-1)/2})^{2(n+1)/n} < (p^{m/p-1})^{3}$$

$$q^{r^2-1} < p^{3m/p-1}$$

puesto que $\frac{1}{2}\, m! = N < q^{r^2-1}$, entonces $\frac{1}{2}\, m! < p^{3m/p-1}$ (14)

Por la proposición 11 del apéndice $m^m e^{-m} < \frac{1}{2}\, m!$

$$\therefore \quad m^m e^{-m} < p^{3m/p-1}$$

extrayendo raíz m-ésima

$$(m^m e^{-m})^{1/m} < (p^{3m/p-1})^{1/m}$$

$$me^{-1} < p^{3/p-1}$$

$$m < e(p^{3/p-1}) \qquad (15)$$

usando esta desigualdad, se considerarán todos los posibles valores del número p primo, en forma decreciente, con los correspondientes subcasos que se muestran en la tabla 2

Caso a) $p \geq 7$.

se cumple que la función $x^{1/x-1}$ es decreciente

$p^{3/p-1} \leq 7^{3/6} = 7^{1/2}$, entonces por (15)

$$m < e(7^{1/2}) \leq 7$$

y $p \leq m \quad \Rightarrow \quad m = p = 7$

$\frac{1}{2}\, rn(n-1) = 1 + 0 + \ldots + \quad \Rightarrow \quad rn(n-1) = 2$

$\therefore \quad r = 1 \quad n = 2$

$N = \frac{1}{2}\, 7^{2/2}(7^2-1) = 7(24) = 168 \neq \frac{1}{2}\, 7! = 2520.$

es decir, este caso no es posible.

Caso a) $p \geq 7$
Caso b) $p = 5$ $PSL(2,5)$, A_5
Caso c) $p = 3$ $n \geq 3$ $n = 2$ $r = 4, 5$ $r = 1$ $PSL(2,3)$, A_4 $r = 2$ $PSL(2,9)$, A_6
Caso d) $p = 2$ $n > 6$ i) $5 \leq n \leq 6$ ii) $n \leq 4$ $m \geq 11$ iii) $n \leq 4$ $m \leq 5$ $PSL(2,4)$, A_5 $6 \leq m \leq 10$ $n = 4$ $r = 1$ $PSL(4,2)$, A_8 $n = 3$ $r = 1$ $n = 3$ $r = 2$ $PSL(3,4)$, A_{10} $n = 2$ $r = 3, 6, 7$

Tabla 2.

Caso b) $p = 5$, $p^{3/p-1} = 5^{3/4}$, $m < e(5^{3/4})$

$m \leq 9$ $\Rightarrow$ $\frac{1}{2} rn(n-1) = \lfloor 9/5 \rfloor + \lfloor 9/25 \rfloor + \ldots$

$= 1$

$\therefore$ $r = 1$, $n = 2$ que resulta ser el caso especial

$N = \frac{1}{2} 5(5^2-1) = \frac{1}{2} 5(24) = 60 = \frac{1}{2} 5!$

de $PSL(2,5)$ y A_5.

Caso c) $p = 3$, $p^{3/p-1} = 3^{3/2}$, $m < e(3^{3/2})$, $m \leq 14$

$m! \leq 14! = 1.2.3.4.5.6.7.8.9.10.11.12.13.14$

$\therefore$ 1, 2, 4, 5 son las potencias exactas de 3 que pueden dividir a $\frac{1}{2} m!$

si $n \geq 3$ $\frac{1}{2} n(n-1) = 3, 6, \ldots$ no es posible

$n = 2$ $\frac{1}{2} n(n-1) = 1$ y $r = 1, 2, 4, 5$

$N = \frac{1}{2} m! = \frac{1}{2} 3^r(3^{2r}-1) = \frac{1}{2} 3^r(3^r+1)(3^r-1)$

el hecho de que con $r = 4, 5$,

$3^4 + 1 = 82$, $3^5 + 1 = 244$

son divisibles por 41 y 61 respectivamente y $m!$ no lo

es, deja como únicas posibilidades a $r = 1, 2$ que vuelven a resultar dos casos especiales :

$2 = d = (q-1, n) = (3^r-1, 2)$

$N = \frac{1}{2}\, 3(3^2-1) = 12 = \frac{1}{2}\, 4!$

$N = \frac{1}{2}\, 3^2(3^4-1) = 360 = \frac{1}{2}\, 6!$

correspondientes a PSL(2,3) y A_4, PSL(2,9) y A_6.

Caso d) $p = 2$, $p^{3^{r-1}} = 2^3 = 8$, $m < e(3) < 21$

$1 + \frac{1}{2}\, n(n-1) \leq \lfloor 21/2 \rfloor + \lfloor 21/4 \rfloor + \lfloor 21/8 \rfloor + \lfloor 21/16 \rfloor + \ldots$

$= 10 + 5 + 2 + 1 = 18$

$\frac{1}{2}\, n(n-1) \leq 17$

si $n > 6$, $\Rightarrow$ $\frac{1}{2}\, n(n-1) > 21$ no es posible

$n \leq 6$

i) $n \geq 5$ $(P^r)^5 - 1 = q^5-1$ es un factor de

$N = (1/d)q^{n(n-1)/2}(q^n-1) \ldots (q^2-1)$

$\therefore$ $2^5-1 = 31 \mid \frac{1}{2}\, m!$ pero $m < 21$

otro caso imposible.

ii) $n \leq 4$, $m \geq 11$.

uno de los factores $q^s-1 = 2^{rs}-1$ es divisible por 11, pero 2 es una raiz primitiva módulo 11, esto es $2^{(p-1)} = 2^{10} \equiv 1 \pmod{11}$,

$\therefore$ $10 \mid rs$

entonces, $2^{rs}-1 = 2^{10t}-1$ para algún t

$= (2^{5t} + 1)(2^{5t} - 1)$

y $31 = 2^5-1 \mid (2^5)^t - 1^t = 2^{5t} - 1$

$\therefore$ $31 \mid 2^{rs} - 1$ $\therefore$ $31 \mid \frac{1}{2}\, m!$

imposible ($m < 21$).

iii) $n \geq 4$, $m \leq 10$.

$m! \leq 10! = 1.2.3.4.5.6.7.8.9.10$

dividiendo por 2 : $1.3.4.5.6.7.8.9.10$

$\frac{1}{2}\, n(n-1) = 2, 3, 6$ ó 7.

si $m \leq 5$ $\quad 2^2 \mid \frac{1}{2}\, m!$ $\quad \frac{1}{2}\, rn(n-1) = 2$ $\quad rn(n-1) = 4$

$n < 3 \quad r = 2, \quad n = 2$

obteniendose el otro caso especial con PSL(2,4) y A_5

$N = (2^{2\cdot 2})(4^2-1) = 60 = \frac{1}{2}\, 5!$

si $m \geq 6$ $\quad 1.2.3.4.5 \mid 6.7.8.9.10$

con las potencias

$\frac{1}{2}\, rn(n-1) = 3,\ 6$ ó 7 $\quad p$ puede dividir a $\frac{1}{2}\, m!$

algunos términos de $2^{rs}-1$ deben ser divisibles por 5,

entonces $4 \mid rs$

(2 es raíz primitiva módulo 5, $2^{rs} \equiv 1 (\text{mód } 5) \leftrightarrow \varphi(5) \mid rs$)

al analizar valores de $\frac{1}{2}\, rn(n-1)$ para $n \leq 4$

$n = 4 \quad \frac{1}{2}\, r(4)(3) = 6r = 6, \quad r = 1$

$n = 3 \quad \frac{1}{2}\, r(3)(2) = 3r = 3$ ó $6, \quad r = 1$ ó $2.$

$n = 2 \quad \frac{1}{2}\, r(2) = r = 3,\ 6$ ó $7\ .$

quedando excluídos los casos

$n = 3 \quad r = 1 \quad (2^3-1)(2^2-1)$

$n = 2 \quad r = 3 \quad (2^9)^2-1$

$n = 2 \quad r = 7 \quad (2^7)^2-1$

y observando

$n = 4 \quad r = 1$ da el caso PSL(4,2) y A_8

$N = 2^{4(3/2)}(2^4-1)(2^3-1)(2^2-1) = 20160 = \frac{1}{2}\, 8!$

$n = 3 \quad r = 2$ se obtiene el caso PSL(3,4) y A_8

$N = 4^{3(2/2)}(4^3-1)(4^2-1) = 20160 = \frac{1}{2}\, 8!$

$n = 2 \quad r = 6$ se obtiene un factor

$(2^6)^2-1 = 2^{12}-1 = (2^6-1)(2^6+1)$

pero $13 \mid 2^6+1$ $\quad$ y $\quad 13 \nmid \frac{1}{2}\, m!$ lo cual no es posible. ■

Ahora se verá si existen isomorfismos o no entre los grupos PSL(n,q) y A_m correspondientes :

1) PSL(2,3) $\cong$ A_4 no es grupo simple, como se analizó anteriormente.

2) Se ha demostrado que todo grupo simple de orden 60, es isomorfo a A_5, por lo tanto $A_5 \cong PSL(2,4) \cong PSL(2,5)$.

3) $PSL(2,9) \cong A_6$.

DEMOSTRACION.
$PSL(2,9)$ contiene un subgrupo B isomorfo a A_5, según 8.13 de [5].
B es de índice 6 : $|PSL(2,9) : B| = 360/60 = 6$.
Sea $X = \{B, Bx_1, Bx_2, Bx_3, Bx_4, Bx_5\}$ el conjunto de las clases laterales derechas de B en $PSL(2,9)$, entonces $S_X = S_6$.
Por Caley existe un homomorfismo $\varphi : PSL(2,9) \longrightarrow S_6$, si φ no es inyectivo, entonces Núc $\varphi \neq \langle e \rangle$, y Núc $\varphi \lhd PSL(2,9)$, lo cual contradice la simplicidad de $PSL(2,9)$,

$\therefore \varphi$ es inyectivo.

entonces $\varphi(PSL(2,9)) < S_6$ y $|\varphi(PSL(2,9))| = 360$.
Como el único subgrupo de S_6 de índice 2 es A_6, entonces
$PSL(2,9) \cong \varphi(PSL(2,9)) \cong A_6$.

4) $PSL(4,2) \cong A_8$.

DEMOSTRACION.

$|GL(4,2)| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3) = 20160 = \frac{1}{2}\,8!$

$\left|\frac{GL(4,2)}{SL(4,2)}\right| = |F^*| = 1, \quad \Rightarrow \quad GL(4,2) \cong SL(4,2)$

además $PSL(4,2) = \frac{SL(4,2)}{Z(SL(4,2))} \quad \Rightarrow \quad SL(4,2) \cong PSL(4,2)$

por lo tanto $PSL(4,2) \cong GL(4,2)$.
Ahora considerándose :

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \qquad G_3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$G_4 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \qquad G_5 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad G_6 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$G_i \in GL(4,2)$, $1 \leq i \leq 6$ y se pueden verificar las siguientes relaciones $G_i^3 = G_i^2 = E \quad (2 \leq i \leq 6)$

$$(G_i G_{i-1})^3 = E \quad (1 \leq i \leq 5)$$

$$(G_i G_j)^2 = E \quad (i + 1 < j)$$

entonces $G_1, \ldots, G_6$ generan A_8 según el teorema 19.8 [5].
Sea $G = \langle G_1, \ldots, G_6 \rangle$, entonces $G < GL(4,2)$,
esto es $A_8 < GL(4,2)$
$|GL(4,2)| = |A_8|$, implica que $A_8 = GL(4,2)$
$\therefore \quad A_8 \cong GL(4,2) \cong PSL(4,2)$.

5) Como $PSL(4,2) \ncong PSL(3,4)$ y por 4), entonces $PSL(3,4) \ncong A_8$.

A P E N D I C E

En esta parte del trabajo, se desarrollan los conceptos y resultados que se usaron en el capitulo II.
De aqui en adelante se considerarán enteros a, b tales que (a, b) = 1, $|a| \geq |b| > 1$, y p un número primo, a menos que se especifique otra cosa.

PROPOSICION 1. Si $p|a^n-b^n$ para algún n, entonces $p \nmid a$ y $p \nmid b$.

DEMOSTRACION. Suponer que p|a, es decir a = rp p. a. r entero
así que $-b^n = (a^n-b^n)-a^n = kp-rp$ p. a. k entero
$= p(k-r)$
ó $b^n = p(r-k)$, de aqui $p|b^n$ y p|b
contradicción, (a, b) = 1.
En forma análoga $p \nmid b$. ∎

PROPOSICION 2. $p|a^n-b^n$ si y sólo si $(a/b)^n \equiv 1 \pmod p$.

DEMOSTRACION. $a^n-b^n \equiv 0 \pmod p$
$\Leftrightarrow$ $a^n \equiv b^n \pmod p$, y por prop. 1 $p \nmid b$
$\Leftrightarrow$ $a^n/b^n = (a/b)^n \equiv 1 \pmod p$ ∎

DEFINICION. Sea f el orden de a/b en $\mathbb{Z}_p^*$, esto es, $(a/b)^f \equiv 1 \pmod p$ y si $(a/b)^n \equiv 1 \pmod p$, entonces $f \leq n$.

Si f es el orden de a/b en $\mathbb{Z}_p^*$ y puesto que $\mathbb{Z}_p^*$ es el grupo cíclico de orden p-1, entonces f|p-1 .

PROPOSICION 3. $P|a^n-b^n$ si y sólo si f|n .

DEMOSTRACION.

$\Rightarrow$) Si $p \mid a^n - b^n$ $\Rightarrow$ $(a/b)^n \equiv 1 \pmod p$ (prop. 2)

como f es el mínimo número tal que

$(a/b)^f \equiv 1 \pmod p$, $f \leq n$

luego $(a/b)^n = (a/b)^{qf+r} \equiv 1 \pmod p$, $0 \leq r < f$

$= (a/b)^{qf}(a/b)^r \equiv 1 \pmod p$

de aquí $(a/b)^r \equiv 1 \pmod p$ y $r = 0$

$\therefore$ $n = qf$ y $f \mid n$.

$\Leftarrow$) Si $f \mid n$, $n = qf$, p.a. q entero

por prop. 2 $p \mid a^f - b^f$, así

$a^n - b^n = a^{qf} - b^{qf} = ((a^f - b^f) + b^f)^q - (b^f)^q$

$= (a^f - b^f)\{(a^f - b^f)^{(q-1)} + q(a^f - b^f)^{(q-2)}b^f + \dots + qb^{f(q-1)}\}$

$\therefore$ $p \mid a^n - b^n$ ∎

DEFINICION. Sea φ_n el n-ésimo polinomio mónico en $\mathbb{C}[x]$ definido por $\varphi_n(x) = \prod(x-\alpha)$, $\alpha \in U_n$, donde U_n es el conjunto de todas las raices n-ésimas primitivas de la unidad. Este polinomio es el llamado n-ESIMO POLINOMIO CICLOTOMICO.

La correspondiente FORMA HOMOGENEA ASOCIADA al polinomio ciclotómico es:

$$\varphi_n(x,y) = y^{\varphi(n)}\varphi_n(x/y) ,$$

donde $\varphi(n)$ es la función de Euler aplicada a n .

PROPOSICION 4. Si n es un entero positivo, entonces

$$x^n - 1 = \prod_{d \mid n} \varphi_d(x) .$$

DEMOSTRACION. [cf. 3]. ∎

La proposición 4 permite calcular los polinomios ciclotómicos recursivamente por división :

$$x-1 = \Phi_1(x)$$
$$x^2-1 = \Phi_1(x)\Phi_2(x)$$

$$x^3-1 = \Phi_1(x)\Phi_3(x)$$
$$x^4-1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$$
$$x^5-1 = \Phi_1(x)\Phi_5(x)$$
$$x^6-1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$$

de modo que

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$

Por la proposición 4 se tiene que para n un entero positivo,

$$a^n-b^n = b^n\left((a/b)^n - 1\right) = b^n \prod_{d\mid n} \Phi_d(a/b) \qquad (1)$$

y si $r\mid n$,

$$\frac{a^n-b^n}{a^r-b^r} = \frac{b^n \prod_{d\mid n}\Phi_d(a/b)}{b^r \prod_{d\mid r}\Phi_d(a/b)} = b^{n-r} \prod_{d\mid n,\ d\nmid r} \Phi_d(a/b) \qquad (2)$$

PROPOSICION 5. Si $p\mid\Phi_n(a, b)$ entonces $p\mid a^n-b^n$.

DEMOSTRACION. $a^n-b^n = b^n \prod_{d\mid n} \Phi_d(a/b)$ por (1)

$$= b^{n-\varphi(n)}\, b^{\varphi(n)} \Phi_n(a/b) \prod_{d\mid n,\ d\neq n} \Phi_d(a/b)$$

$$= b^{n-\varphi(n)} \Phi_n(a, b) \prod_{d\mid n,\ d\neq n} \Phi_d(a/b)$$

$\therefore$ si $p\mid\Phi_n(a, b)$, $p\mid a^n-b^n$. ∎

COROLARIO 6. Si $p|\phi_n(a, b)$ entonces $f|n$.

DEMOSTRACION. Se sigue de las proposiciones 5 y 3 . ∎

DEFINICION. EL ORDEN de m, respecto al primo p, es el exponente de la máxima potencia de p que divide a m . Es decir $p^{\text{ord}_p m}|m$ y si $p^k|m$ para algún k, entonces $k \leq \text{ord}_p m$.

A partir de las ecuaciones (1) y (2) se obtienen respectivamente,

$$\phi_n(a/b)\,|\,a^n-b^n \qquad (3)$$

y si $r|n$,

$$\phi_n(a/b)\,|\,\frac{a^n-b^n}{a^r-b^r} \qquad (4)\ .$$

Como $\phi_n(a, b) = b^{\phi(n)}\phi_n(a/b)$ y $p\nmid b$, entonces

$$\text{ord}\ \phi_n(a, b) = \text{ord}\ \phi_n(a/b) \qquad (5).$$

PROPOSICION 7. Sea f el orden de a/b en $\mathbb{Z}_p^*$, si $\text{ord}\ \phi_n(a/b) \neq 0$ entonces $f|n$.

DEMOSTRACION. $\text{ord}\ \phi_n(a/b) \neq 0$,
$\Rightarrow$ $\text{ord}\ \phi_n(a, b) \neq 0$ por (5),
$\Rightarrow$ $p|\phi_n(a, b)$ y $f|n$ por cor. 6 . ∎

LEMA 1. Sea f el orden de a/b en $\mathbb{Z}_p^*$. Entonces se cumple lo siguiente :

1. Si p es impar,
   a) $\text{ord}\ \phi_f(a, b) > 0$.
   b) $\text{ord}\ \phi_{fp^i}(a, b) = 1, \qquad i \geq 1$.

c) ord $\Phi_n(a, b) = 0$, para cualquier otro $n \geq 1$.

d) ord $(a^n - b^n) = 0$, si $f \nmid n$.

e) ord $(a^n - b^n) =$ ord $(a^f - b^f)$ + ord n, si $f \mid n$.

2. a) ord $\Phi_2(a, b) = 1$, para $i \geq 2$.

b) Si $\Phi_1(a, b) = a - b \equiv 0 \pmod 4$, entonces ord $\Phi_2(a, b) = 1$.

c) Si $\Phi_2(a, b) = a + b \equiv 0 \pmod 4$, entonces ord $\Phi_1(a, b) = 1$.

d) ord $\Phi_n(a, b) = 0$, para $n = 2^i l$, $i \geq 0$, $l \geq 3$ impar.

DEMOSTRACION.

1. a) $(a/b)^f \equiv 1 \pmod p \quad \Rightarrow \quad$ ord $((a/b)^f - 1) > 0$.

Además, $(a/b)^f - 1 = \prod_{d \mid f} \Phi_d(a/b) = \Phi_f(a/b) \prod_{d \mid f,\ d \neq f} \Phi_d(a/b)$

si $d \mid f$ y $d \neq f$, entonces $d < f$ y $f \nmid d$, así,

ord $\Phi_d(a/b) = 0$ por la prop. 7

$\Rightarrow$ ord $((a/b)^f - 1) =$ ord $\Phi_f(a/b)$

$\therefore$ ord $\Phi_f(a/b) > 0$

y por (5), ord $\Phi_f(a, b) > 0$.

b) Sea $n = fp^i$, $r = fp^{i-1}$, $i \geq 1$.

$$\frac{a^n - b^n}{a^r - b^r} = \frac{(a^r)^p - (b^r)^p}{a^r - b^r} = \frac{\left((a^r - b^r) + b^r\right)^p - b^{rp}}{a^r - b^r} =$$

$$= (a^r - b^r)^{p-1} + p(a^r - b^r)^{p-2} b^r + \ldots + \binom{p}{2} (a^r - b^r) b^{r(p-2)} + p b^{r(p-1)}$$

como $f \mid p$, $\Rightarrow$ $p \mid a^r - b^r$ por prop. 3 así que

$$p \mid \frac{a^n - b^n}{a^r - b^r} \quad y \quad p \nmid b \quad \Rightarrow \quad p^2 \nmid \frac{a^n - b^n}{a^r - b^r},$$

$$\therefore \quad \text{ord} \ \frac{a^n - b^n}{a^r - b^r} = 1.$$

por otra parte $\dfrac{a^n-b^n}{a^r-b^r} = b^{n-r} \prod_{d\mid n,\ d\nmid r} \Phi_d(a/b)$ por (2),

entonces $\sum_{d\mid n,\ d\nmid r} \operatorname{ord} \Phi_d(a/b) = 1$.

Por lo tanto existe un divisor d de n tal que $d\nmid r$ y ord $\Phi_d(a/b) = 1$.

$\therefore$ ord $\Phi_d(a,b) = \operatorname{ord} \Phi_d(a/b) = 1$ por (5)

y por el corolario 6, $f\mid d$

entonces $d\mid n$, $d\nmid r$ y $n = fp^i$, $r = fp^{i-1}$ implica $d = n$

$\therefore$ ord $\Phi_d(a/b) = \operatorname{ord} \Phi_n(a/b) = \operatorname{ord} \Phi_n(a, b) = 1$.

c) Sea $n = fp^i l$, $i \geq 0$, $p\nmid l$, $l \geq 1$.

sea $r = fp^i$,

$$\frac{a^n-b^n}{a^r-b^r} = \frac{a^{rl}-b^{rl}}{a^r-b^r} = \frac{\left((a^r-b^r)+b^r\right)^l - b^{rl}}{a^r-b^r} =$$

$$= (a^r-b^r)^{l-1} + l(a^r-b^r)^{l-2}b^r + \cdots + \binom{l}{2}(a^r-b^r)b^{r(l-2)} + lb^{r(l-1)}$$

por lo tanto $p\nmid \dfrac{a^n-b^n}{a^r-b^r}$.

pero $\Phi_n(a/b)$ es divisor de $\dfrac{a^n-b^n}{a^r-b^r}$ por (4),

entonces ord $\Phi_n(a/b) = \operatorname{ord} \Phi_n(a, b) = 0$.

d) Si $f\nmid n$ entonces $p\nmid a^n-b^n$, prop. (3)

$\therefore$ ord $a^n-b^n = 0$.

e) Si $f\mid n$, $\dfrac{a^n-b^n}{a^f-b^f} = b^{n-f} \prod_{d\mid n,\ d\nmid f} \Phi_d(a/b)$ por (2)

de ésto y la prop. 7

$$\operatorname{ord}\ \frac{a^n-b^n}{a^f-b^f} = \sum_{i\mid n} \operatorname{ord}\ \Phi_{fp^i}(a/b)$$

$i > 0 \quad \Rightarrow \quad fp^i = d \neq f,$

$d = fp^i \quad \Rightarrow \quad \operatorname{ord}\ \Phi_d(a/b) \neq 0.$

Por la observación de que $f \mid p-1$, entonces $p \nmid f$.

Entonces los valores de i corren sobre todos los valores $1 \leq i \leq \operatorname{ord} n$ y por el inciso b),

$\operatorname{ord}\ (a^n-b^n) - \operatorname{ord}\ (a^f-b^f) = \operatorname{ord} n$.

2. Si $p = 2$. $f = 1$ y $a/b \equiv 1 \pmod 2$

a) $\Phi_{2^t}(a, b) = b^{\varphi(2^t)}\Phi_{2^t}(a/b)$

$$= b^{2^t-2^{t-1}} \frac{(a/b)^{2^t}-1}{\prod_{0 \leq k \leq t-1} \Phi_{2^k}(a/b)}$$

$$= b^{2^t-2^{t-1}} \frac{((a/b)^{2^{t-1}}-1)((a/b)^{2^{t-1}}+1)}{(a/b)^{2^{t-1}}-1}$$

$$= b^{2^t-2^{t-1}}((a/b)^{2^{t-1}}+1) = a^{2^{t-1}}+b^{2^{t-1}}$$

como $a/b \equiv 1 \pmod 2$,

$2 \mid a/b - 1$ y $2 \mid a/b - 1 + 2 = a/b + 1$

$\therefore \quad 4 \mid (a/b - 1)(a/b + 1) = (a/b)^2 - 1$

$\Rightarrow \quad 4 \mid (a/b)^{2^{t-1}} - 1$ para $t \geq 2$

y $(a/b)^{2^{t-1}} \equiv 1 \pmod 4$

$\therefore \quad (a/b)^{2^{t-1}} + 1 \equiv 2 \pmod 4,$

$\Rightarrow \quad a^{2^{t-1}} + b^{2^{t-1}} = \Phi_{2^t}(a, b) \equiv 2 \pmod 4$

$\Phi_{2^t}(a, b) - 2 = 4k, \qquad$ p.a. k entero

$\phi_2(a, b) = 4k + 2 = 2(2k + 1)$

$2 \mid \phi_2(a, b)$ pero $2^2 \nmid \phi_2(a, b)$

$\therefore$ ord $\phi_2(a, b) = 1$.

b) Si $\phi_1(a, b) = a - b \equiv 0 \pmod 4$

$\Rightarrow \quad 4 \mid a - b$,

luego $\phi_2(a, b) = a + b = a - b + 2b$

$= 4k + 2b$, p.a. k entero

$\therefore \quad 2 \mid \phi_2(a, b)$ pero $2^2 \nmid \phi_2(a, b)$ porque $2 \nmid b$

$\therefore$ ord $\phi_2(a, b) = 1$.

c) Si $\phi_2(a, b) = a + b \equiv 0 \pmod 4$

$4 \mid \phi_2(a, b) = a + b$

$\phi_1(a, b) = a-b = a + b -2b = 4k - 2b$, p.a. k entero

entonces $2 \mid \phi_1(a, b)$ y

$2^2 \nmid \phi_1(a, b)$ porque $2 \nmid b$

$\therefore$ ord $\phi_1(a, b) = 1$

d) Sea $n = 2^t l$, $t \geq 0$, l impar, $l \geq 3$.

como $\phi_n(a/b) \mid \dfrac{a^n - b^n}{a^{2^t} - b^{2^t}}$

$$\text{ord } \phi_n(a/b) \leq \text{ord } \frac{a^n - b^n}{a^{2^t} - b^{2^t}}$$

además

$$\frac{a^n - b^n}{a^{2^t} - b^{2^t}} = (a^{2^t} - b^{2^t})^{l-1} + l(a^{2^t} - b^{2^t})^{l-2} b^{2^t} + \dots +$$

$$+ \binom{l}{2}(a^{2^t} - b^{2^t})(b^{2^t})^{l-2} + l(b^{2^t})^{l-1}$$

$\therefore \quad 2 \nmid \dfrac{a^n - b^n}{a^{2^t} - b^{2^t}}$

y ord $\Phi_n(a/b) = \text{ord}\ \Phi_n(a, b) = 0$. ■

Ahora se procederá a encontrar una estimación de $|\Phi_n(a, b)|$ tomando a, b sobre todas las parejas de números complejos que satisfacen $|a| > |b| + 1 \geq 2$.

DEFINICION. Dado $n > 0$ un entero, sea

$$L(n) = \inf \{ |\Phi_n(a, b)| : a, b \in \mathbb{C} \}.$$

Antes de demostrar el siguiente resultado se obtienen unas propiedades útiles.

I. Si $p|n$, $L(np) \geq L(n)$ y $L(np) \geq (1 + p)^{\varphi(n)}$.

DEMOSTRACION.

$$\Phi_{np}(a, b) = b^{\varphi(np)} \frac{(a/b)^{np}-1}{\prod_{i|np,\ i\nmid n} \Phi_i(a/b)} = b^{\varphi(np)} \frac{(a/b)^{np}-1}{(a/b)^{k}-1}$$

por la proposición 4,
donde k es el mayor divisor de np tal que $k \neq np$, esto es, $k|np$, $k \neq np$ y si $k'|np$ tal que $k' \neq np$, entonces $k' \leq k$.
como

$$\Phi_n(a^p, b^p) = (b^p)^{\varphi(n)} \frac{\left(a^p/b^p\right)^{n}-1}{\prod_{i|n,\ i\nmid n} \Phi_i(a^p/b^p)} = b^{p\varphi(n)} \frac{(a/b)^{np}-1}{(a^p/b^p)^{m}-1}$$

donde m es el mayor divisor de n tal que $m \neq n$.
se tiene que

$\varphi(np) = \varphi(n)\varphi(p)(d/\varphi(d))$ donde $d = (n, p) = p$
$= \varphi(n)\varphi(p)(p/\varphi(p)) = p\varphi(n)$

$k = pm$, puesto que es el mayor divisor de np y $mp \neq np$
por lo tanto $\Phi_{np}(a, b) = \Phi_n(a^p, b^p)$ (21).

Ahora,

$$\{\,|\varphi_n(a^p, b^p)| : a, b \in \mathbb{C}\,\} \subseteq \{\,|\varphi_n(a, b)| : a, b \in \mathbb{C}\,\}$$

$$\inf\{\,|\varphi_n(a, b)| : a, b \in \mathbb{C}\,\} \leq \inf\{\,|\varphi_n(a^p, b^p)| : a, b \in \mathbb{C}\,\}$$

$$= \inf\{\,|\varphi_{np}(a, b)| : a, b \in \mathbb{C}\,\} \quad \text{por (21)}$$

así $L(n) \leq L(np)$ si $p|n$. (22).

Por otra parte

$$|\varphi_n(a, b)| = |b^{\varphi(n)}\varphi_n(a/b)| = |b^{L^{n-1}} \prod_{k,n=1} (a/b - \omega_n^k)|$$

$$= \prod_{k,n=1} |a - b\omega_n^k|$$

además $|a - b\omega_n^k| \geq ||a| - |b\omega_n^k|| = |\,|a|-|b|\,| = |a|-|b|$

por lo tanto

$$\prod_{k,n=1} |a - b\omega_n^k| \geq \prod_{k,n=1} (|a|-|b|) = (|a|-|b|)^{\varphi(n)}$$

$$\therefore \quad |\varphi_n(a, b)| \geq (|a|-|b|)^{\varphi(n)} \quad (23)$$

Luego como $|a| \geq |b| + 1$ y $|b| \geq 1$,

$$|a|^p-|b|^p = (|a|-|b| + |b|)^p - |b|^p$$

$$\geq (|a|-|b|)^p + p(|a|-|b|)^{p-1}\,|b|$$

$$\geq 1 + p$$

$$\therefore \quad (|a|^p-|b|^p)^{\varphi(n)} \geq (1 + p)^{\varphi(n)} \quad (24)$$

Así que $|\varphi_{np}(a, b)| = |\varphi_n(a^p, b^p)|$

$$\geq (\,|a^p|-|b^p|\,)^{\varphi(n)} \quad \text{por (23)}$$

$$\geq (1 + p)^{\varphi(n)} \quad \text{por (24)}$$

$\therefore \quad (1 + p)^{\varphi(n)} \leq L(np) = \inf\{|\varphi_{np}(a, b)| : a, b \in \mathbb{C}\}$, si $p|n$ ■

II. Si $p \geq 5$, $L(p) > 2p$.

DEMOSTRACION.

Se tiene que $|\varphi_p(a, b)| = \dfrac{|a^p-b^p|}{|a-b|}$ por prop. 4.

$0 \leq |a-b| \leq |a| + |b| \quad \Rightarrow \quad \dfrac{1}{|a-b|} \geq \dfrac{1}{|a| + |b|}$

$$\therefore \quad \frac{|a^p-b^p|}{|a-b|} \geq \frac{||a|^p-|b|^p|}{|a| + |b|} = \frac{|a|^p-|b|^p}{|a| + |b|}$$

y $$|\varphi_p(a, b)| \geq \frac{|a|^p-|b|^p}{|a| + |b|} = \frac{x^p- y^p}{x + y}$$

donde $x = |a|$, $y = |b|$

$x \geq y + 1 \geq 2$

$$(x^p-y^p)(1 + 2y) = x(1+y)(x^{p-1}-(1+y)^{p-1}) + y(x^p-(1+y)^p) + y^p(x-(1+y)) + (x+y)((1+y)^p - y^p) \geq (x+y)((1+y)^p-y^p)$$

$\therefore$

$$|\varphi_p(a,b)| \geq \frac{x^p-y^p}{x + y} = \frac{(x^p-y^p)(1+2y)}{(x+y)(1+2y)} \geq \frac{(x+y)((1+y)^p-y^p)}{(x+y)(1+2y)} = \frac{(1+y)^p-y^p}{1+2y}$$

como $y = |b| \geq 1$

$$(1+y)^p-2^p = \sum_0^p \binom{p}{k} y^k - \sum_0^p \binom{p}{k} = \sum_0^p \binom{p}{k}(y^k-1) \geq \binom{p}{p}(y^p-1) = y^p-1$$

y

$$(1+y)^p-2^p y = \sum_0^p \binom{p}{k} y^k - y\sum_0^p \binom{p}{k} = \sum_0^p \binom{p}{k}(y^k-y) \geq \binom{p}{p}(y^p-y) = y^p-y$$

además

$$((1+y)^p-2^p) + 2((1+y)^p-2^p y) = 3(1+y)^p - 2^p(1+2y)$$

$$\therefore \quad 3(1+y)^p - 2^p(1+2y) \geq y^p - 1 + 2(y^p-y) = 3y^p - (1+2y) \quad \Rightarrow$$

$$3(1+y)^p - 3y^p \geq 2^p(1+2y) - (1+2y) = (2^p - 1)(1+2y) \quad \Rightarrow$$

$(1+y)^p - y^p \geq \frac{1}{3}(2^p - 1)(1+2y)$

$$\therefore \quad |\Phi_p(a,b)| \geq \frac{(1+y)^p - y^p}{1+2y} \geq \frac{(2^p-1)(1+2y)}{3(1+2y)} = \frac{2^p-1}{3}$$

$\therefore \quad L(p) \geq \frac{1}{3}2^p - 1$

y para $p \geq 9$, $L(p) > 2p$. ■

III. Si $p \geq 5$, $L(2p) > 2p$.

DEMOSTRACION.

Primero se probará que
$\Phi_{2n}(x) = \Phi_n(-x)$, si n es impar y $n > 1$.
Se usará la igualdad : $x^{2n}-1 = -(x^n-1)((-x)^n-1)$, para n impar e inducción.

Sea $n = 3$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} \qquad \text{por prop. 4}$$

$$= -\frac{(x^3-1)((-x)^3-1)}{(x^3-1)(\Phi_2(x))}$$

$$= \frac{(-x)^3-1}{-(x+1)} = \frac{(-x)^3-1}{-x-1} = \frac{(-x)^3-1}{\Phi_1(-x)} = \Phi_3(-x)$$

hipótesis de inducción : si $n = 2l-1$ con $2 \leq l \leq k$

$$\Phi_{2n}(x) = \Phi_n(-x)$$

P.D. para $n = 2k+1$

$$\Phi_{2(2k+1)}(x) = \frac{x^{2(2k+1)}-1}{\prod_{d \mid 2(2k+1) \atop d \neq 2(2k+1)} \Phi_d(x)} = \frac{-(x^{2k+1}-1)((-x)^{2k+1}-1)}{\prod_{d \mid 2k+1} \Phi_d(x)\,\Phi_2(x) \prod_{d \mid 2(2k+1) \atop \text{múltiplos de dos}} \Phi_d(x)}$$

$$\Phi_{2(2k+1)}(x) = \frac{(-x)^{2k+1}-1}{-\Phi_2(x)\prod_d \Phi_d(x)} = \frac{(-x)^{2k+1}-1}{\Phi_1(-x)\prod_d \Phi_d(-x)} = \Phi_{2k+1}(-x)$$

$d \mid 2(2k+1)$, múltiplos de dos; $d \mid 2k+1$

$$\therefore \quad \varphi_{2n}(x) = \varphi_n(-x) \quad \text{si } n \text{ es impar} \quad \text{y} \quad n > 1 . \qquad (25)$$

Ahora,

$$\varphi_{2p}(a, b) = b^{\varphi(2p)}\phi_{2p}(a/b) = b^{\varphi(2)\varphi(p)}\varphi_p(-a/b) \qquad \text{por (25)}$$

$$= b^{\varphi(p)}\phi_p(-a/b) = \phi_p(a,-b)$$

$$\text{y} \qquad |\varphi_{2p}(a, b)| = |\phi_p(a,-b)| \qquad (26)$$

como

$$\{\ |\phi_p(a,-b)| : a, b \in \mathbb{C}\ \} \subset \{\ |\varphi_p(a, b)| : a, b \in \mathbb{C}\ \}$$

$$\inf\{\ |\phi_p(a, b)| : a, b \in \mathbb{C}\ \} \leq \inf\{\ |\varphi_p(a,-b)| : a, b \in \mathbb{C}\ \}$$

$$= \inf\{\ |\varphi_{2p}(a, b)| : a, b \in \mathbb{C}\ \} \quad \text{por (26)}$$

$$\therefore \qquad L(p) \leq L(2p) \qquad (27)$$

y por II, si $p \geq 5$, $2p < L(2p)$. ∎

IV. Si $p \nmid n$, entonces $L(np) \geq L(n)^{p-1}$.

DEMOSTRACION. Sea ε_p una raíz primitiva p-ésima de la unidad, entonces

$$\varepsilon^p \prod_{\varepsilon \neq 1} \phi_n(a, \varepsilon b) = \phi_n(a, \varepsilon_p b)\phi_n(a, \varepsilon_p^2 b) \cdots \phi_n(a, \varepsilon_p^{p-1} b)$$

$$= \prod_{(k,n)=1} (a - b\varepsilon_p \sigma_n^k) \prod_{(k,n)=1} (a - b\varepsilon_p^2 \sigma_n^k) \cdots \prod_{(k,n)=1} (a - b\varepsilon_p^{p-1} \sigma_n^k)$$

donde se tienen la relación : $1 = (\varepsilon_p)^p = (\sigma_n)^n = (\sigma_{np})^{np}$,

sea $\varepsilon_p = \sigma_{np}^n$, $\sigma_n = \sigma_{np}^p$

sustituyendo

$$\varepsilon^p \prod_{\varepsilon \neq 1} \varphi_n(a, \varepsilon b) = \prod_{(k,n)=1} (a - b\sigma_{np}^n \sigma_{np}^{pk}) \prod_{(k,n)=1} (a - b\sigma_{np}^{2n} \sigma_{np}^{pk}) \cdots$$

$$\cdots \prod_{(k,n)=1} (a - b\sigma_{np}^{(p-1)n} \sigma_{np}^{pk})$$

$$= \prod_{(k,n)=1} (a - b\varepsilon_{np}^{1+pk}) \prod_{(k,n)=1} (a - b\varepsilon_{np}^{2+pk}) \cdots \prod_{(k,n)=1} (a - b\varepsilon_{np}^{n(p-1)+pk})$$

cada factor tiene tantos términos como $\varphi(n)$ y son p-1 factores es decir son $\varphi(n)(p-1) = \varphi(n)\varphi(p) = \varphi(np)$, ya que $(n, p) = 1$ además $(in + pk, np) = 1$, puesto que si $d \neq 1$, tal que $d|in + pk$, y $d|np$, entonces $d|n$ $(d \nmid p)$ y $d|pk$ implica $d|k$, contradiciendo $(n, k) = 1$.

de aquí que $$\varphi_{np}(a, b) = \prod_{\varepsilon^p=1,\ \varepsilon\neq 1} \varphi_n(a, \varepsilon b)$$

por tanto, si $p \nmid n$ $$|\varphi_{np}(a, b)| = \prod_{\varepsilon^p=1,\ \varepsilon\neq 1} |\varphi_n(a, \varepsilon b)|$$

$$\{\ |\varphi_n(a, \varepsilon b)| : a, b \in \mathbb{C}\ \} \subset \{\ |\varphi_n(a, b)| : a, b \in \mathbb{C}\ \}$$

$$L(n) = \inf \{\ |\varphi_n(a, b)| : a, b \in \mathbb{C}\ \} \leq \inf \{\ |\varphi_n(a, \varepsilon b)| : a, b \in \mathbb{C}\ \}$$

considérese

$$\{\ \prod |\varphi_n(a, \varepsilon b)| : a, b \in \mathbb{C}\ \} \quad \varepsilon^p = 1, \quad \varepsilon \neq 1$$

$$\therefore \quad L(n)^{p-1} \leq \inf \{\ \prod |\varphi_n(a, \varepsilon b)| : a, b \in \mathbb{C}\ \} = L(np)\ . \quad \blacksquare$$

V. Si $x \geq 3$, $y \geq 3$, entonces $x^{y-1} \geq xy$.

DEMOSTRACION.

Sea $g(y) = x^{y-1} - xy = x(x^{y-2} - y)$, $x \neq 0$,

entonces $g'(y) = x(\log x(x^{y-2}) - 1)$

si $y \geq 3$, $y-2 \geq 1$ $\therefore$ $x^{y-2} \geq x \geq 3$

si $x \geq 3$, $\log x \geq \log 3 > 1$

$\therefore$ $\log x(x^{y-2}) > 3 > 1$

$\therefore$ $g'(y) > 0$, es decir g es creciente

luego $g(3) = x^2 - 3x$, como $x \geq 3$, $x^2 \geq 3x$, implica $g(3) \geq 0$,

si $y \geq 3$, $g(y) \geq g(3)$, esto es, $x^{y-1} - xy \geq x^2 - 3x \geq 0$

$\therefore \quad x^{(y-1)} \geq xy$. ■

VI. Si n es divisible por el cuadrado de un primo p, entonces $L(n) \geq L(n/p)$.

DEMOSTRACION. Se sigue de I. porque $p \mid \frac{n}{p}$. ■

LEMA 2. Para $n \neq 1, 2, 3$ y 6 se tiene que $L(n) > \prod_{p \mid n} p$.

DEMOSTRACION. (Por inducción)

i) Si n es divisible por el cuadrado de un primo p y $n/p = 1, 2, 3$ ó 6. $(n = p, 2p, 3p$ ó $6p)$

como $p \mid n/p$, las únicas posibilidades son : $n = 4, 9, 12$ ó 18 .

Pero por la segunda afirmación de I.

$L(4) = L(2.2) \geq (1 + 2)^{(2-2)} = 3 > 2$

$L(9) = L(3.3) \geq (1 + 3)^{(3-3)} = 4^2 = 16 > 3$

$L(12) = L(6.2) \geq (1 + 2)^{(6-6)} = 3^2 = 9 > 2(3)$

$L(18) = L(6.3) \geq (1 + 3)^{(6-6)} = 4^2 = 16 > 2(3)$

ahora, si $n \neq 4, 9, 12$ y 18, y $p^2 \mid n$

hipótesis de inducción : si $m < n$, $L(m) > \prod_{p \mid m} p$

P.D. para n.

sea $n = p_1^2 q$, q un entero positivo.

como $p_1 \mid \frac{n}{p_1} = p_1 q$ por I., $L(p_1^2 q) \geq L(p_1 q)$,

$p_1 q < n \quad \therefore \quad L(p_1 q) > \prod_{p \mid p_1 q} p' = \prod_{p \mid p_1 q} p$

es decir $L(n) > \prod_{p \mid n} p$.

ii) Supóngase que n es libre de cuadrado, esto es, n no es divisible por el cuadrado de algún primo p.

Sea p el número primo mayor divisor de n y sea $n = pm$.

por hipótesis $p \geq 5$,

Si $m = 1$, entonces por II. $L(p) > 2p > p$

y se cumple la afirmación.

Si $m = 2$, entonces por III. $L(2p) > 2p$.

Si $m = 3$, $n = 3p$ y $3 \nmid p$ por IV

$L(3p) \geq (L(p))^2 > 4p^2$ por II.

$> 3p$.

Si $m = 6$, $L(6p) = L(3(2p)) \geq (L(2p))^2$, porque $3 \nmid 2p$ por IV.

$(L(2p))^2 > 4p^2 > 6p$

$\therefore \quad L(6p) > 6p$.

hipótesis de inducción : si $m < n$, $L(m) > \prod_{p \mid m} p$.

P.D. para n.

sea $n = mp$,

n libre de cuadrado implica $p \nmid m$

entonces $L(mp) \geq L(m)^{p-1}$ por IV.

como $L(m) \geq 3$ y $p > 3$, aplicando V. con $x = L(m)$, $y = p$,

$L(m)^{p-1} \geq pL(m)$

$\therefore \quad L(mp) \geq pL(m) > p \prod_{p' \mid m} p'$

ó $L(n) > \prod_{p \mid n} p$. ■

TEOREMA 1. Si $n > 2$ y a, b son enteros tales que $(a, b) = 1$, $|a| \geq |b| + 1 \geq 2$, entonces existe p primo tal que $p \mid a^n - b^n$ y $p \nmid a^i - b^i$, si $0 < i < n$, a excepción de $n = 3$, $a = \pm 2$, $b = \mp 1$ ó $n = 6$, $a = \pm 2$, $b = \pm 1$.

Además $p \nmid n$ y $(a/b)^n \equiv 1 \pmod p$.

DEMOSTRACION.

Supóngase que para todo primo p tal que $p \mid a^n - b^n$, existe $0 < i < n$, tal que $p \mid a^i - b^i = b^i \prod_{d \mid i} \phi_d(a/b)$.

En particular si $p \mid \phi_n(a/b)$, como $a^n - b^n = b^n \prod_{d \mid n} \phi_d(a/b)$

entonces existe $d \leq i < n$ tal que

$p \mid \phi_d(a/b)$.

Sea f el orden de (a/b) módulo p .
Como ord $\varphi_n(a/b) > 0$, y ord $\varphi_j(a/b) > 0$.
Se sigue del primer lema que si $p > 2$, $n = fp^k$ y $d = fp^j$ donde
$0 \le j < k$, así que $p|n$,
también por el lema 1, ord $\varphi_n(a/b) = 1$.
Si $p = 2$ y ord $\varphi_n(a/b) > 0$, del lema 1, 2) $n = 2^k$ y si $n > 2$,
ord $\varphi_n(a/b) = 1$.
Por lo tanto, en cualquier caso si $n > 2$

$$|\varphi_n(a/b)| = \prod_{p|\varphi_n(a/b)} p^{\text{ord } \varphi_n(a/b)} \le \prod_{p|n} p$$

y $$|\varphi_n(a, b)| \le |\varphi_n(a/b)| \le \prod_{p|n} p$$

lo cual contradice el lema 2, si $n \neq 1, 2, 3, 6$.

ahora analizando los casos $n = 3$, $n = 6$
si $|a| \ge 3$,

$$\varphi_3(a, b) = a^2 + ab + b^2 = \tfrac{1}{4}a^2 + ab + b^2 + \tfrac{3}{4}a^2$$
$$= (\tfrac{1}{2}a + b)^2 + \tfrac{3}{4}a^2$$

y $|a| \ge 3 \quad \Rightarrow \quad a^2 \ge 9, \quad \tfrac{3}{4}a^2 \ge \tfrac{3}{4}(9) = 27/4,$

como $(\tfrac{1}{2}a + b)^2 \ge 0$

$\varphi_3(a, b) \ge 27/4 > 6$
con lo cual se tiene que

$$\prod_{p|3} p = 3 < 6 \le L(3) = \inf\{\ |\varphi_3(a,b)|\ \} \quad \text{si } |a| \ge 3$$

mientras que para $|a| = 2$
si $a = 2$, $b = -1$

$$\varphi_3(2, -1) = \tfrac{3}{4}(2)^2 + (\ \tfrac{1}{2}(2) + (-1)\ )^2 = 3 \not> 3, \quad \text{falla.}$$

si $a = 2$, $b = 1$

$$\varphi_3(2, 1) = \tfrac{3}{4}(2)^2 + (\ \tfrac{1}{2}(2) + 1\ )^2 = 3 + 4 = 7 > 3$$

si cumple el lema.

si a = -2, b = 1

$$\varphi_3(-2, -1) = \tfrac{1}{4}(-2)^3 + \left(\tfrac{1}{2}(-2) + 1\right)^2 = 3 \nmid 3, \quad \text{falla.}$$

si a = -2, b = -1

$$\varphi_3(-2, -1) = \tfrac{1}{4}(-2)^2 + \left(\tfrac{1}{2}(-2) - 1\right)^2 = 3 + 4 = 7 > 3$$

si cumple el lema.

además como $\varphi_3(a, b) = \varphi_3(a, -b)$ por (25)
el lema no se cumple para $\varphi_3(2, 1)$ y $\varphi_3(-2, -1)$
Por lo tanto salvo las excepciones de n = 3, a = ± 2, b = ∓ 1 ó n = 6, a = ± 2, b = ± 1, siempre se contradice al lema 2, por lo tanto existe p tal que $p \mid a^n - b^n$ y $p \nmid a^i - b^i$, si $0 < i < n$.
De esta forma n es el orden de a/b módulo p
y por tanto $n \mid p-1$ y $p \nmid n$. ■

TEOREMA 2. Si a > 1 es un entero y n > 2, entonces existe un primo p tal que $p \mid a^n - 1$ y $p \nmid a^i - 1$ si $i < n$, a menos que n = 6, a = 2.

DEMOSTRACION. Aplicar el TEOREMA 1 con b = 1. ■

OTROS RESULTADOS :

PROPOSICION 8. Si x > 1, la función $x^{1/x-1}$ es decreciente.

DEMOSTRACION.
Sea $f(x) = x^{1/x-1} = \exp(\ln x^{1/x-1}) = \exp\left(\frac{\ln x}{x-1}\right)$

$$f'(x) = \left(\frac{\ln x}{x-1}\right)' \exp\left(\frac{\ln x}{x-1}\right) = \frac{x-1/x - \ln x}{(x-1)^2}\left[\exp\left(\frac{\ln x}{x-1}\right)\right]$$

ahora sea $g(x) = \frac{x-1}{x} - \ln x$

$$g'(x) = \frac{x - (x-1)}{x^2} - \frac{1}{x} = \frac{1-x}{x^2}$$

si x > 1, 1-x < 0, ⇒ g'(x) < 0,
esto es , g es decreciente y como g(1) = 0, g(x) < 0,

$$\therefore \quad f'(x) = \frac{g(x)}{(x-1)^2}\left[\exp\left(\frac{\ln x}{x-1}\right)\right] < 0,$$

y $f(x)$ es decreciente. ■

PROPOSICION 9. Si $0 \le x_i \le 1$, entonces $\prod_{i=1}^{m}(1-x_i) \ge 1 - \sum_{i=1}^{m} x_i$.

DEMOSTRACION. Inducción sobre m.

$m = 1 \qquad \prod_{i=1}^{1}(1-x_i) = 1-x_1 = 1 - \sum_{i=1}^{1} x_i$

hipótesis de inducción : $m = k, \qquad \prod_{i=1}^{k}(1-x_i) \ge 1 - \sum_{i=1}^{k} x_i$.

P.D.

$m = k + 1 \qquad \prod_{i=1}^{k+1}(1-x_i) = \left(\prod_{i=1}^{k}(1-x_i)\right)(1-x_{k+1})$

$$\ge \left(1 - \sum_{i=1}^{k} x_i\right)(1-x_{k+1})$$

$$= 1 - \sum_{i=1}^{k} x_i - x_{k+1} + x_{k+1}\sum_{i=1}^{k} x_i$$

$$\ge 1 - \sum_{i=1}^{k+1} x_i$$

$x_{k+1}\sum_{i=1}^{k} x_i \ge 0 \qquad$ ya que $\qquad 0 \le x_i \le 1$. ■

PROPOSICION 10. Para todo entero positivo m, $(1 + 1/m)^m < e$.

DEMOSTRACION. $\ln x = \int_1^x \frac{du}{u}$

se tiene que $\ln(1 + 1/m) = \int_1^{1+1/m} \frac{du}{u}$

$f(u) = 1/u$ es continua en $[1, 1 + 1/m]$, por el teorema del valor

medio para integrales, existe $t \in (1, 1 + 1/m)$ tal que

$$\int_1^{1+1/m} \frac{du}{u} = 1/m(f(t)) = 1/m(1/t) = 1/mt$$

$$1 < t < 1 + 1/m \quad \Rightarrow \quad m < mt < m + 1$$

$$\therefore \quad \frac{1}{m+1} < \frac{1}{mt} < \frac{1}{m} \quad y \quad \ln(1 + 1/m) < \frac{1}{m}$$

entonces $m \ln(1 + 1/m) < 1$

aplicando la exponencial la cual es creciente

$$e^{m\ln(1+1/m)} < e$$

$$\therefore \quad (1 + 1/m)^m < e$$ ■

PROPOSICION 11. Para todo entero positivo m, $m^m e^{-m} < \frac{1}{2} m!$.

DEMOSTRACION. Por inducción.

$m = 1 \quad \Rightarrow \quad e^{-1} < \frac{1}{2} \qquad (e > 2)$

Hipótesis de inducción : $m^m e^{-m} < \frac{1}{2} m!$

P. D. para m + 1

como $(1 + 1/m)^m < e$ por la proposición 10

multiplicando por m+1 la desigualdad

$$\frac{(m+1)^{m+1}}{m^m} < e(m+1) \quad y \quad (m+1)^{m+1} m^{-m} e^{-1} < m + 1$$

multiplicando por la hipótesis de inducción

$$(m+1)^{m+1} m^{-m} e^{-1} (m^m e^{-m}) < (m+1)(\tfrac{1}{2} m!)$$

$$(m+1)^{m+1} e^{-(m+1)} < \tfrac{1}{2} (m+1)!$$ ■

B I B L I O G R A F I A

[1] Artin, E., *The orders of linear groups*, Communications on pure and Applied Mathematics, Vol. VIII, 355-366, 1955.

[2] Artzy, R., *Linear Geometry*, Addison-Wesley, 1965.

[3] Bastida, Julio R., *Field Extensions and Galois Theory*, Encyclopedia of Mathematics and its applications, Addison-Wesley, California, 1984.

[4] Fraleigh, John B., *Algebra Abstracta*, Addison-Wesley Iberoamericana, Tercera edición, versión en español, 1988.

[5] Huppert, B., *Endliche Gruppen* I. Springer-Verlag, Berlin Heidelberg New York, 1967.

[6] Herstein, I. N., *Topics in Algebra*, John Wiley & Sons, Inc. New York, Segunda edición, 1964.

[7] Konneth, I., *A classical Introduction to modern Number Theory*, Springer, New York, 1982.

[8] Niven y Zuckerman., *Introduccion a la teoria de los Numeros*, Limusa, 1969.

[9] Rotman, J., *An Introduction to The Theory of groups*, Ally and Bacon, Inc. Boston, Tercera edición, 1984.

[10] Zappa, Guido., *Fondamenti di Teoria dei gruppi*, Monografie Matematiche 13, Vol. I, Consiglio Nazionale Delle Ricenche, Edizione Cremonese Roma, 1965.

[11] Zappa, Guido., *fondamenti di Teoria dei gruppi*, Monografie Matematiche 18, Vol. II Consiglio Nazionale Delle Ricenche, Edizione Cremonese Roma, 1970.