UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA

TESIS:

"EL TEOREMA DE WEDDERBURN Y EL TEOREMA DE ARTIN-ZORN"

PRESENTA:

LAZO VILLATORO, BESSY YANIRA

MONTOYA NOLASCO, INGRID SUYAPA

MORENO MELÉNDEZ, MINDY SARAHI

PARA OPTAR AL TÍTULO DE:

LICENCIADA EN MATEMÁTICA

MARZO DE 2013

SAN MIGUEL, EL SALVADOR, CENTROAMÉRICA.

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA

TEMA:

“EL TEOREMA DE WEDDERBURN Y EL TEOREMA DE ARTIN-ZORN”

PRESENTA:

LAZO VILLATORO, BESSY YANIRA

MONTOYA NOLASCO, INGRID SUYAPA

MORENO MELÉNDEZ, MINDY SARAHI

PARA OPTAR AL TÍTULO DE:

LICENCIADA EN MATEMÁTICA

ASESOR DIRECTOR:

MSC. MARCELINO MEJÍA GONZÁLES

ASESOR METODOLÓGICO:

LIC. PEDRO FLÓRES SÁNCHEZ

CIUDAD UNIVERSITARIA DE ORIENTE, 18 DE MARZO DE 2013.

UNIVERSIDAD DE EL SALVADOR

ING. MARIO ROBERTO NIETO LOVO

RECTOR

MSC. ANA MARÍA GLOWER DE ALVARADO

VICERRECTORA ACADÉMICA

DRA. ANA LETICIA ZAVALETA DE AMAYA

SECRETARIA GENERAL

FACULTAD MULTIDISCIPLINARIA

ORIENTAL

LIC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ

DECANO

LIC. JORGE ALBERTO ORTEZ HERNÁNDEZ

SECRETARIO

LIC. EDWIND JEOVANNY TREJOS CABRERA

ADMINISTRADOR ACADÉMICO

DEPARTAMENTO DE CIENCIAS

NATURALES Y MATEMÁTICA

M.EST. JOSÉ ENRY GARCÍA

JEFE DEL DEPARTAMENTO

SECCIÓN DE MATEMÁTICA

ING. DOLORES BENEDICTO SARAVIA

COORDINADOR

TRABAJO DE GRADUACIÓN

APROBADO POR:

LIC. ULISES LIZAMA VIGIL

COORDINADOR DE PROCESOS DE GRADUACIÓN

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

MSC. MARCELINO MEJÍA GONZÁLEZ

ASESOR DIRECTOR

LIC. PEDRO FLÓRES SÁNCHEZ

ASESOR METODOLÓGICO

AGRADECIMIENTOS

A Dios, por haberme dado la sabiduría y el entendimiento para poder llegar al final de mi carrera y por estar conmigo en cada paso que doy.

A mis padres, mil gracias por haberme apoyado en todo momento, por su confianza, por sus consejos, por sus sacrificios para darme el estudio, pero más que nada por su amor.

A mis hermanas, por su apoyo, por su cariño y por su amistad.

A los asesores del trabajo de graduación, MSc. Marcelino Mejía y Lic. Pedro Flores, por su disposición, por su apoyo y motivación para la culminación de este trabajo de graduación.

A mis compañeras de tesis, por su amistad y por haber logrado juntas este triunfo.

Bessy Yanira Lazo Villatoro.

AGRADECIMIENTOS

A Dios, por haberme dado entendimiento para poder llegar al final de mi carrera, por proveerme de todo lo necesario para salir adelante y por todo lo que me ha dado.

A mis padres, por el apoyo incondicional que me brindaron por todos los sacrificios que hicieron a lo largo de mi carrera, así como su comprensión y paciencia en momentos difíciles que tuvimos.

A mis hermanos y hermanas, ya que estuvieron apoyándome a lo largo de mi carrera y dándome fuerzas para seguir.

A toda mi familia, por todo el apoyo brindado en especial a mi tía porque siempre estuvo a mi lado para ayudarme y apoyarme en todo momento.

A los asesores del trabajo de graduación, MSc. Marcelino Mejía y Lic. Pedro Flores, por la orientación y ayuda que me brindaron por su valioso tiempo que me dedicaron para la realización de este trabajo.

A mis compañeras de tesis, porque a pesar de todos los momentos difíciles que tuvimos pudimos salir adelante con nuestro trabajo, por su amistad y compresión.

Ingrid Suyapa Montoya Nolasco.

AGRADECIMIENTOS

En primer lugar a Dios, por darme la vida y una familia maravillosa, por darme la alegría de cosechar las semillas que planté, por estar presente y darme fuerzas en todas esas horas de estudio y momentos difíciles a lo largo de mi carrera.

A mis padres, por su amor, confianza y apoyo incondicional en todos los aspectos, y estar conmigo en todo momento.

A mis hermanos/as, por su amor y apoyo incondicional y darme esas palabras de ánimo cuando perdía las fuerzas para seguir y porque a pesar de la distancia siempre estuvieron y están conmigo; y especialmente a mi hermano Alex por ser la persona más especial en mi vida, por su cariño y por acompañarme en muchas noches de desvelo.

A mi familia, a mis sobrinos/as, cuñados/as, primos/as, a mis tías por el cariño, apoyo y motivación para seguir adelante.

A mis asesores, al MSc. Marcelino Mejía por sus enseñanzas a lo largo de mi carrera y por la disposición, orientación y ayuda que me brindó para la realización de esta tesis. Al Lic. Pedro Flores por sus enseñanzas, disposición y ayuda en este trabajo.

A los docentes de la sección de Matemáticas que fueron parte de mi formación profesional, de manera especial al Lic. Pedro Flores por el cariño, apoyo, motivación y amistad brindada, a la Lic. Sonia Martínez por sus enseñanzas, cariño y amistad que siempre me brindó.

A mis compañeras de tesis, por su compañerismo y amistad, y porque a pesar de los obstáculos logramos salir adelante con este trabajo.

A mi novio, por brindarme su amor, comprensión, ayuda y darme ánimos cuando más lo necesitaba y ser parte de mi vida.

A mis amigos/as, que siempre estuvieron y están a mi lado para ayudarme, escucharme, aconsejarme y compartir conmigo momentos de alegría y de tristeza.

Mindy Sarahi Moreno Meléndez

ÍNDICE GENERAL

INTRODUCCIÓN

En este trabajo de graduación se proyecta estudiar dos teoremas de gran importancia en Álgebra Abstracta y a la vez uno de ellos, que es una generalización del otro, interrelaciona esta área con la Geometría Proyectiva.

Desde hace siglos hasta nuestros días mediante la abstracción y el uso de la lógica en el razonamiento, las matemáticas han evolucionado y se han dividido en distintas ramas. Por ejemplo, el estudio de la estructura comienza al considerar las diferentes propiedades de los números inicialmente los números naturales, las reglas que dirigen las operaciones aritméticas se estudian en el Álgebra Elemental, la investigación de métodos para resolver ecuaciones lleva al campo del Álgebra Abstracta y el estudio del espacio origina la Geometría.

Estas ramas de las matemáticas están muy interrelacionadas, en este trabajo se mostrará la interrelación que hay entre dos ramas muy importantes, el Álgebra Abstracta y la Geometría Proyectiva, estudiando el Teorema de Wedderburn y el Teorema de Artin-Zorn; en donde la Teoría de Grupos, Teoría de Anillos y Teoría de Campos es necesaria para la demostración del Teorema de Wedderburn y relacionando ésta teoría con la Teoría de Anillos Alternativos se demuestra el teorema de Artin-Zorn, que es una generalización del teorema anterior.

En el Capítulo I, se enunciarán definiciones y algunos teoremas básicos de la Teoría de Grupos, Teoría de Anillos y Teoría de Campos que serán referidos en el desarrollo de los capítulos posteriores, permitiendo de esta forma al lector familiarizarse con los términos y la notación que será utilizada, sobre todo en la demostración del primer teorema (Teorema de Wedderburn).

En el Capítulo II, se desarrollara la teoría correspondiente a Planos Proyectivos y Anillos Alternativos. Cabe señalar que este capítulo es base para la demostración del segundo teorema (Teorema de Artin-Zorn).

Finalmente el Capítulo III, se centrará en las demostraciones de El Teorema de Wedderburn y El Teorema de Artin-Zorn. Es importante señalar que los teoremas no tienen demostraciones únicas, y por tanto las que se consideran en este trabajo son unas de las diversas pruebas dadas.

NOTAS HISTÓRICAS

Álgebra Abstracta

Uno de los campos más desarrollados en el siglo XIX fue el Álgebra Abstracta, y una de las grandes creaciones del álgebra fue la Teoría de Grupos, donde la figura principal es la del francés Evariste Galois (1811-1832).

Otro aporte de Galois, fue el descubrimiento de los campos finitos, campos con un número finito de elementos, en honor a él, el campo finito con p^r elementos es con frecuencia llamado el campo de Galois y es denotado por $GF(p^r)$.

Geometría Proyectiva

Un campo de la geometría que también posee importancia es el estudio de las propiedades proyectivas de las figuras, lo que se suele llamar como la Geometría Proyectiva.

Algebra y Geometría

Uno de los primeros matemáticos en descubrir el hecho que relaciona el Álgebra Abstracta con la Geometría Proyectiva, fue Klein quien responde a la pregunta ¿Qué es la Geometría?, introduciendo en la Geometría un nuevo concepto de carácter algebraico: el concepto de grupo.

Cabe mencionar que, dado que, la mayoría de personas está familiarizada con las operaciones numéricas, les resulta difícil imaginar que puedan operarse puntos, rectas, etc.

Joseph MacLagan Wedderburn y El Teorema de Wedderburn

Uno de los algebristas más importantes de la historia es el matemático escocés Joseph Henry MacLagan Wedderburn (2 de febrero de 1882 - 9 de octubre de 1948). Publicó alrededor de 40 libros y artículos, haciendo importantes avances en la teoría de anillos, álgebras y teoría matricial.

Entre sus principales resultados están una parte del conocido "Teorema de Wedderburn-Artin" acerca de álgebras semi-simples, el "Teorema principal de Wedderburn" que nos dice que si R es una k–álgebra de dimensión finita con k un campo perfecto entonces $R \cong S \oplus rad(R)$ como S – S – bimódulos y S una k–álgebra semisimple, y "El Teorema de Wedderburn" en anillos de división, el cual también puede ser encontrado con el nombre de "Teorema Pequeño de Wedderburn". El Teorema de Wedderburn de 1905, establece que todo anillo de división finito es un campo finito; a primera vista es curioso que la finitud y la posibilidad de dividir por elementos distintos de cero impliquen que la multiplicación del anillo sea conmutativa.

En el famoso artículo de Wedderburn "un teorema en álgebra finita" del año 1905, Wedderburn primero estableció su teorema, ahora considerado un clásico que cualquier anillo de división finito es conmutativo, esto es, un campo finito.

El teorema interrelaciona dos cosas aparentemente no relacionadas, a saber: el número de elementos en unos ciertos sistemas algebraicos y la multiplicación de esos sistemas. Wedderburn dio tres pruebas diferentes de este bonito teorema que ha sido aprobado por muchas personas usando variedad de diferentes ideas. Más pruebas fueron dadas más tarde por Emil Artin, Hans Zassenhaus, Nicolas Bourbaki y muchos otros.

Ernest Witt en 1931 dio la mejor prueba, la cual es de hecho una versión simplificada de la primera prueba ofrecida por Wedderburn. En su prueba Witt usa Teoría de Grupo, números complejos y alguna teoría básica de número.

En el libro Topics in Algebra de Herstein, se presentan dos pruebas: una se sigue esencialmente de la prueba de Witt mientras que la segunda es de una naturaleza mucho más algebraica y viene a ser técnicamente más compleja. Existen, por supuesto, numerosas otras pruebas disponibles en la literatura. Algunas, obtenidas del teorema por una aplicación de teoría de algebra simple y el famoso teorema de Skolem-Noether entre otros basados casi en la Teoría de Grupo.

Aparte de su belleza intrínseca el resultado ha sido muy importante y útil ya que surge en muchos contextos. Para los algebristas el Teorema de Wedderburn ha servido como un punto de partida para una larga área de investigación, en 1940 y 1950 se interesaron por los anillos de conmutatividad.

Emil Artin y sus aportes al Álgebra Abstracta

Emil Artin (3 de marzo de 1898 - 20 de diciembre de 1962), fue un matemático austriaco nacido en Viena que inició su carrera en Alemania, en la Universidad de Gotinga y en 1923 se mudó a la universidad de Hamburgo.

Fue uno de los mejores algebristas del siglo, con una influencia más importante de lo que podemos creer. Trabajó en la teoría de números, contribuyó a la teoría algebraica de los anillos asociativos y los números hipercomplejos.

Su actividad científica se centró de forma particular en la aritmética analítica y teórica de los campos de números cuadráticos. En 1944 descubrió anillos de condiciones mínimas para ideales, los llamados en su honor anillos de Artin. Sus aportaciones matemáticas se hallan expresadas en sus obras **Theorie der Gammafunktion** (1931), **Galois Theory** (1942), **Geometric Álgebra** (1957) y **The Collected Papers** (1965).

Emil Artin falleció en 1962, en Hamburgo, Alemania.

Max August Zorn

Max August Zorn nació el 6 de junio de 1906 en Krefeld, Alemania; murió el 9 de marzo de 1993 en Bloomington, Indiana, EE.UU. Fue un matemático alemán nacionalizado estadounidense. Trabajo en los campos de álgebra abstracta, teoría de grupos, teoría de números, lógica, análisis funcional y análisis numérico.

El Teorema de Artin-Zorn

El Teorema de Artin-Zorn es una generalización de El Teorema de Wedderburn, nombrado así después que Emil Artin y Max Zorn establecen que cualquier anillo de división alternativo finito es necesariamente un campo finito. Fue publicado primero por Zorn pero su publicación fue acreditada a Artin.

Como una consecuencia geométrica de El Teorema de Artin-Zorn, todo plano de Moufang finito es el clásico plano proyectivo sobre un campo finito. El plano de Moufang es un plano de traslación para toda recta.

Por el famoso teorema de Wedderburn que cualquier anillo de división finito es un campo finito, la prueba del Teorema de Artin-Zorn se reduce a demostrar las leyes asociativas.

SIMBOLOGÍA

$GF(p^r)$: Campo de Galois con una potencia de r elementos.

G: Grupo.

H: Subgrupo.

$|G|$: Orden de un grupo.

$\langle a \rangle$: Subgrupo generado por a.

$\langle G, \cdot \rangle$: Grupo con una operación binaria definida en él.

N_a: Normalizador de un elemento en el grupo.

C_a: Número de elementos conjugados de un elemento en el grupo.

C: Centro de un grupo.

S_n: Grupo simétrico.

$sig(\alpha)$: Signatura de una permutación.

$Alt(n)$: Grupo alternado.

R: Anillo.

$\langle R, +, \cdot \rangle$: Anillo con dos operaciones definidas en él.

R^*: Anillo de división.

$Z(R)$: Centro de un anillo.

N_x: Normalizador de un elemento en el anillo.

F: Campo.

E: Subcampo.

V: Espacio vectorial.

$\langle V, + \rangle$: Espacio vectorial con una operación escalar.

$[F:E]$: Extensión del campo F sobre E.

$ch(F)$: Característica de un campo F.

$\deg(p)$: Grado de un polinomio.

$F[x]$: Anillo de polinomio.

$\Phi_n(x)$: n-ésimo polinomio ciclotómico.

$\mathbb{Z}_p$: Conjunto de los enteros módulo p.

$(\cdot, \circ)$: Operación ternaria.

CAPÍTULO I

TEORÍA DE GRUPOS, TEORÍA DE ANILLOS Y TEORÍA DE CAMPOS

En este primer capítulo se introducen conceptos y terminología fundamentales, para el estudio de este trabajo de graduación. El objetivo principal es tener las herramientas necesarias para el desarrollo de El Teorema de Wedderburn y El Teorema de Artin-Zorn.

1.1. TEORÍA DE GRUPOS

Este apartado está dedicado a las definiciones preliminares de teoría de grupos necesarios en este trabajo; se presenta la definición de grupo y sus propiedades.

En primer lugar introducimos el concepto de mapeo o aplicación; un **mapeo** α de un conjunto S en un conjunto T es una regla que asigna a cada x del conjunto S una única y del conjunto T. Simbólicamente escribiremos esto empleando cualquiera de las notaciones: $\alpha: x \longrightarrow y$ ó $y = \alpha(x)$.

Y también el concepto de operación binaria que será útil en el desarrollo de este capítulo; sea S un conjunto y sea $S \times S$ el conjunto que denota todos los pares (s, t) con $s \in S,\ t \in S$. Entonces una aplicación de $S \times S$ sobre S será llamada una **operación binaria en S**.

Definición 1.1.1. Grupo

Un conjunto no vacío de elementos G, se dice que forma un grupo si en él está definida una operación binaria, llamada producto y denotada por $(\cdot)$ tal que se cumplen:

1. *Ley de cerradura*.

   Para todo par de elementos $\boldsymbol{a}, b$ de G, el producto $\boldsymbol{a} \cdot b = c$ existe y es un elemento único de G.

2. *Ley asociativa*.

   $\boldsymbol{a} \cdot (b \cdot c) = (\boldsymbol{a} \cdot b) \cdot c$, para todo $\boldsymbol{a}, b, c$ de G.

3. *Existencia de unidad*.

   Existe un elemento $\boldsymbol{e} \in G$ tal que $\boldsymbol{a} \cdot \boldsymbol{e} = \boldsymbol{e} \cdot \boldsymbol{a} = \boldsymbol{a}$ para toda $\boldsymbol{a}$ de G.

4. *Existencia de inverso.*

   Para toda $\boldsymbol{a}$ de G existe un elemento $\boldsymbol{a}^{-1}$ de G tal que $\boldsymbol{a} \cdot \boldsymbol{a}^{-1} = \boldsymbol{a}^{-1} \cdot \boldsymbol{a} = \boldsymbol{e}$

En el desarrollo de este trabajo se usara $\boldsymbol{a}b$ en lugar de $\boldsymbol{a} \cdot b$.

Notación. Escribimos $\langle G, \cdot \rangle$ para denotar un grupo G con una operación binaria definida en él.

Definición 1.1.2. Grupo abeliano

Un grupo G que satisface la ley conmutativa $\boldsymbol{a} \cdot b = b \cdot \boldsymbol{a}$, para todo par de elementos $\boldsymbol{a}, b$ de G se dice que es un grupo abeliano o conmutativo.

El nombre de “abeliano” se debe al matemático noruego Niels H. Abel (1802 – 1829) que contribuyo de manera decisiva a la unificación de la teoría de grupos.

Definición 1.1.3. Cuasi grupo

Un cuasi grupo Q, es un conjunto de elementos en el que está definida una operación binaria de producto $\boldsymbol{a}b$ tal que, en $\boldsymbol{a}b = c$ para cualesquiera dos de $\boldsymbol{a}, b, c$ determina en forma única el tercero como elemento de Q.

Definición 1.1.4. Lazo

Un lazo es un cuasi grupo Q con una unidad 1 tal que $1 \cdot \boldsymbol{a} = \boldsymbol{a} \cdot 1 = \boldsymbol{a}$, para todo elemento $\boldsymbol{a}$ de Q.

Definición 1.1.5. Grupo finito

Un grupo finito es un grupo G que tiene un número de elementos finito.

Definición 1.1.6. Orden de un grupo

El orden de un grupo G es su cardinal, es decir, el número de sus elementos. El orden de G es denotado por $|G|$.

Definición 1.1.7. Subgrupo

Un subconjunto no vacío H de un grupo G, se dice que es un subgrupo de G, si H es un grupo bajo las mismas operaciones en G.

Si G es un grupo, los subgrupos G y $\{\boldsymbol{e}\}$ se llaman los subgrupos triviales de G.

Lema 1.1.1. Un subconjunto no vacío H del grupo G es un subgrupo de G si y solo si

1) $\boldsymbol{a}, b \in H$ implica que $\boldsymbol{a}b \in H$
2) $\boldsymbol{a} \in H$ implica que $\boldsymbol{a}^{-1} \in H$

Prueba:

" $\Rightarrow$ "

Si H es un subgrupo de G, entonces (1) y (2) se verifican, porque un subgrupo cumple las mismas propiedades de un grupo y dentro de las propiedades de grupo estas dos leyes están dadas.

" $\Leftarrow$ "

Supongamos, recíprocamente, que H es un subconjunto de G para el que se verifican (1) y (2). Para confirmar que H es un subgrupo todo lo que se necesita verificar es que $\boldsymbol{e} \in H$ y que la ley asociativa se verifica para los elementos de H. Como la ley asociativa es válida para G, es claro que también es válida para H que es un subconjunto de G. Si $\boldsymbol{a} \in H$, según (2) $\boldsymbol{a}^{-1} \in H$, luego de acuerdo con (1) se tiene $\boldsymbol{e} = \boldsymbol{a}\boldsymbol{a}^{-1} \in H$.

Por tanto, se completa la prueba.

Definición 1.1.8. Grupo cíclico

Un grupo formado por todas las potencias de un mismo elemento $\boldsymbol{a}$ es llamado grupo cíclico, es decir, $\langle \boldsymbol{a} \rangle = G$, en este caso $\boldsymbol{a}$ se denomina un generador de G.

$\langle \boldsymbol{a} \rangle = \{\boldsymbol{a}^n : n \in \mathrm{Z}\}$ denota el subgrupo generado por $\boldsymbol{a}$.

Lema 1.1.2. Sea G un grupo abeliano finito con la propiedad de que la relación $x^n = \boldsymbol{e}$ se satisface por, a lo más, n elementos de G, para todo entero n. Entonces G es un grupo cíclico.

Prueba:

Sea G un grupo abeliano finito con la propiedad de que $x^n = \boldsymbol{e}$ se satisface por, a lo más, n elementos de G, para todo entero n.

Si el orden de G es una potencia de algún número primo q entonces el resultado es muy sencillo. Supongamos, en efecto, que $\boldsymbol{a} \in G$ es un elemento cuyo orden es todo lo grande que sea posible; su orden debe ser q^r para algún entero r. Los elementos $\boldsymbol{e}, \boldsymbol{a}, \boldsymbol{a}^2, \dots, \boldsymbol{a}^{q^{r-1}}$ nos dan q^r soluciones distintas de la ecuación $x^{q^r} = \boldsymbol{e}$ que, por hipótesis, implica que estas son todas las soluciones de la ecuación. Luego, si $b \in G$, su orden es q^s donde $s \leq r$, de donde $b^{q^r} = \left(b^{q^s}\right)q^{r-s} = \boldsymbol{e}$. Por la observación anteriormente hecha, esto obliga a que $b = \boldsymbol{a}^i$ para algún i, y por lo tanto G es cíclico.

Teorema 1.1.1. Teorema de Lagrange

Si G es un grupo finito y H es un subgrupo de G, entonces el orden de H es un divisor del orden de G.

Prueba:

Suponemos que G es un grupo finito y que H es un subgrupo de él.

Si $H = \{\boldsymbol{e}\}$ ó $H = G$ no hay nada que probar.

Suponemos entonces que $H \neq \{\boldsymbol{e}\}$ y $H \neq G$. Sea $H = \{h_1, \dots, h_r\}$ donde $r = |H|$.

Luego existe un elemento $\boldsymbol{a} \in G$, tal que $\boldsymbol{a} \notin H$. Entonces tenemos los siguientes elementos en G:

$$h_{1,}h_2, \dots h_r$$

$$h_1\boldsymbol{a}, h_2\boldsymbol{a}, \dots, h_r\boldsymbol{a}$$

Afirmamos que todos los elementos del segundo renglón son diferentes uno de otro y también diferente de cualesquiera de los elementos del primer renglón, es decir, hay $2r$ elementos distintos.

i. Si dos cualesquiera del segundo renglón fueran iguales, entonces $h_i\boldsymbol{a} = h_j\boldsymbol{a}$ con $i \neq j$, pero de acuerdo con la ley de cancelación, esto nos llevaría a que $h_i = h_j$, que es una contradicción.

ii. Si un elemento del segundo renglón fuera igual a uno del primero, entonces $h_i\boldsymbol{a} = h_j$, entonces multiplicando por ${h_i}^{-1}$ a la derecha nos da $\boldsymbol{a} = {h_i}^{-1}h_j \in H$ ya que H es un subgrupo de G; luego $\boldsymbol{a} \in H$, pero esto contradice que $\boldsymbol{a} \notin H$.

Si esos $2r$ elementos son todos elementos de G, entonces $|G| = 2r = 2|H|$ y entonces $|H|$ divide al orden de G.

Si por el contrario, hay más de $2r$ elementos en G, continuamos el proceso y tendremos que existe un elemento $b \in G$, que no aparece en ninguno de los dos renglones. Consideremos la nueva lista de elementos en G

$$h_{1,}h_2, \dots h_r$$

$$h_1\boldsymbol{a}, h_2\boldsymbol{a}, \dots, h_r\boldsymbol{a}$$

$$h_1b, h_2b, \dots, h_rb$$

Como antes, poco más o menos, podríamos mostrar que no hay en el tercer renglón dos elementos iguales y que ningún elemento del tercer renglón aparece en ninguno de los dos primeros. Tenemos, pues, en nuestra lista $3|H|$ elementos. Continuando en esta forma, cada nuevo elemento introducido da lugar a $|H|$ nuevos elementos. Como G es un grupo finito, terminaremos por agotar todos los elementos de G. Pero si terminamos usando k renglones para enumerar todos los elementos del grupo, habremos enumerado $k|H|$ elementos distintos, de donde $|G| = k|H|$, por lo tanto el orden de H divide al orden de G.

Definición 1.1.9. Orden de un elemento

Sea G un grupo, $\boldsymbol{a} \in G$, llamaremos orden del elemento $\boldsymbol{a}$, al menor entero n positivo tal que $\boldsymbol{a}^n = \boldsymbol{e}$, donde $\boldsymbol{e}$ es el elemento identidad de G.

Usamos la notación $|\boldsymbol{a}|$ para indicar el orden de $\boldsymbol{a}$. Si ese entero no existe, diremos que $\boldsymbol{a}$ tiene orden infinito.

Corolario. 1.1.1. Si G es un grupo finito y $\boldsymbol{a} \in G$, entonces el orden de $\boldsymbol{a}$ divide al orden de G.

Prueba:

Sea $\boldsymbol{a} \in G$ y consideremos el subgrupo cíclico generado por $\boldsymbol{a}$, $H = \langle \boldsymbol{a} \rangle$ el cual consiste en los elementos $\boldsymbol{a}^0 = \boldsymbol{e}, \boldsymbol{a}, \boldsymbol{a}^2, \dots, \boldsymbol{a}^{n-1}$, donde $\boldsymbol{a}^n = \boldsymbol{e}$.

Es claro entonces que $n = |H|$ y además $n = |\boldsymbol{a}|$.

De acuerdo al Teorema 1.1.1, tendremos que el orden de H divide al orden de G.

Luego, $|\boldsymbol{a}|$ divide a $|G|$.

Corolario 1.1.2. Si G es un grupo finito y $\boldsymbol{a} \in G$, entonces $\boldsymbol{a}^{|G|} = \boldsymbol{e}$.

Prueba:

De acuerdo con el corolario 1.1.1, $|\boldsymbol{a}|$ divide a $|G|$; luego $|G| = |\boldsymbol{a}|m$ para algún $m \in$ Z.

Por tanto,

$$\boldsymbol{a}^{|G|} = \boldsymbol{a}^{|\boldsymbol{a}|m}$$

$$= \left(\boldsymbol{a}^{|\boldsymbol{a}|}\right)^{m}$$

$$= \boldsymbol{e}^{m}$$

$$= \boldsymbol{e}.$$

Corolario 1.1.3. Si G es un grupo finito de orden primo p, entonces G es cíclico.

Prueba:

Sea $\boldsymbol{a} \in G$, $\boldsymbol{a} \neq \boldsymbol{e}$. Entonces $H = \langle \boldsymbol{a} \rangle$ el subgrupo cíclico generado por $\boldsymbol{a}$ tiene orden un divisor de p. Luego hay dos posibilidades:

i. $|H| = p$, lo cual implica $H = G$ y G es cíclico generado por $\boldsymbol{a}$

ii. $|H| = 1$, y por lo tanto se tendría $\boldsymbol{a} = \boldsymbol{e}$, lo cual es imposible.

Luego G es un grupo cíclico.

Definición 1.1.10. Clases laterales

Sea H un subgrupo de G. Una clase lateral izquierda de H en G es un subconjunto de G cuyos elementos pueden ser expresados como:

$$\boldsymbol{a}H = \{\boldsymbol{a}h : h \in H\}.$$

Similarmente, una clase lateral derecha de H en G es un subconjunto que puede ser expresado como:

$$Hb = \{hb : h \in H\}.$$

Definición 1.1.11. Subgrupo generado por $\boldsymbol{S}$

Sea $S \subseteq G$, con $S \neq \emptyset$, G un grupo. Al más pequeño de los subgrupo de G que contiene a S lo llamamos el subgrupo generado por S y lo notamos por $\langle S \rangle$.

Decimos que un grupo G es finitamente generado si $G = \langle S \rangle$ para algún $S \subset G$ finito.

Definición 1.1.12. Conjugado

Si $\boldsymbol{a}, b \in G$, entonces b se dice que es un conjugado de $\boldsymbol{a}$ en G si existe un elemento $c \in G$ tal que $b = c^{-1}\boldsymbol{a}c$.

Definición 1.1.13. Centro de un grupo

Sea G un grupo, el centro de G se define como:

$$Z(G) = \{\boldsymbol{a} \in G | \boldsymbol{a}x = x\boldsymbol{a} \text{ para todo } x \in G\}.$$

Definición 1.1.14. Normalizador

Si $\boldsymbol{a} \in G$, el normalizador de $\boldsymbol{a}$ en G, es el conjunto:

$$N_{\boldsymbol{a}} = \{x \in G | \ x\boldsymbol{a} = \boldsymbol{a}x\}.$$

Proposición 1.1.1. Si G es un grupo, entonces el normalizador $N_{\boldsymbol{a}}$ es un subgrupo de G.

Prueba:

En este resultado el orden de G, sea este finito o infinito, carece de importancia, por lo que no ponemos restricciones alguna sobre cuál sea ese orden.

Supongamos que $x, y \in N_{\boldsymbol{a}}$. Tenemos pues, $x\boldsymbol{a} = \boldsymbol{a}x$ y $y\boldsymbol{a} = \boldsymbol{a}y$.

Por tanto $(xy)\boldsymbol{a} = x(y\boldsymbol{a}) = x(\boldsymbol{a}y) = (x\boldsymbol{a})y = (\boldsymbol{a}x)y = \boldsymbol{a}(xy)$ luego $xy \in N_{\boldsymbol{a}}$. De $\boldsymbol{a}x = x\boldsymbol{a}$ se sigue que $x^{-1}\boldsymbol{a} = x^{-1}(\boldsymbol{a}x)x^{-1} = x^{-1}(x\boldsymbol{a})x^{-1} = \boldsymbol{a}x^{-1}$ luego x^{-1} está también en $N_{\boldsymbol{a}}$, por lema 1.1.1.

Así, hemos demostrado que $N_{\boldsymbol{a}}$ es un subgrupo de G.

Teorema 1.1.2. Si G es un grupo finito, entonces $c_{\boldsymbol{a}} = \frac{|G|}{|N_{\boldsymbol{a}}|}$; en otras palabras, el número de elementos conjugados $\boldsymbol{a}$ en G es el índice del normalizador de $\boldsymbol{a}$ en G.

Prueba:

Para comenzar, la clase de conjugados de $\boldsymbol{a}$ en G, $c_{(\boldsymbol{a})}$, consiste exactamente en todos los elementos $x^{-1}\boldsymbol{a}x$ cuando x recorre G, $c_{\boldsymbol{a}}$ mide el número de los distintos $x^{-1}\boldsymbol{a}x$. Nuestro método de prueba será mostrar que dos elementos en la misma clase lateral derecha de $N_{\boldsymbol{a}}$ en G da lugar a un mismo conjugado de $\boldsymbol{a}$, mientras que dos elementos en diferentes clases laterares derechas de $N_{\boldsymbol{a}}$ en G da lugar a diferentes conjugados de $\boldsymbol{a}$. De esta forma tendremos una correspondencia biyectiva entre conjugados de $\boldsymbol{a}$ y clases laterares derechas de $N_{\boldsymbol{a}}$ en G.

Supongamos que $x, y \in G$ están en una misma clase lateral derecha de $N_{\boldsymbol{a}}$ en G. Entonces $y = nx$ donde $n \in N_{\boldsymbol{a}}$ y entonces $n\boldsymbol{a} = \boldsymbol{a}n$. Por lo tanto como

$$y^{-1} = (nx)^{-1} = x^{-1}n^{-1},\ y^{-1}\boldsymbol{a}y = x^{-1}n^{-1}\boldsymbol{a}nx = x^{-1}n^{-1}n\boldsymbol{a}x = x^{-1}\boldsymbol{a}x\ ,$$

Es decir, x y y dan lugar a un mismo conjugado de $\boldsymbol{a}$.

Si, por otra parte, x y y están en clases laterales derechas distintas de $N_{\boldsymbol{a}}$ en G, afirmamos que $x^{-1}\boldsymbol{a}x \neq y^{-1}\boldsymbol{a}y$. Si no fuera este el caso, de $x^{-1}\boldsymbol{a}x = y^{-1}\boldsymbol{a}y$ deduciríamos que $yx^{-1} = \boldsymbol{a}yx^{-1}$; esto a su vez, implicaría que $yx^{-1} \in N_{\boldsymbol{a}}$. Pero esto nos dice que x y y están en la misma clase lateral derecha de $N_{\boldsymbol{a}}$ en G, lo que contradice el hecho de que están en diferentes clases laterales. Por tanto, se completa la prueba.

Corolario 1.1.4. $|G| = \sum \frac{|G|}{|N_{\boldsymbol{a}}|}$ donde esta suma se efectúa tomando un elemento $\boldsymbol{a}$ en cada clase de conjugado.

Prueba:

Como $|G| = \sum c_{\boldsymbol{a}}$, usando el Teorema 1.1.2, se deduce el corolario.

A la ecuación en este corolario se suele llamar ecuación de clase de G.

Lema 1.1.3. $\boldsymbol{a} \in Z(G)$ si y solo si $N_{\boldsymbol{a}} = G$. Si G es finito, $\boldsymbol{a} \in Z(G)$ si y solo si $|N_{\boldsymbol{a}}| = |G|$.

Prueba:

Si $\boldsymbol{a} \in Z(G)$, $x\boldsymbol{a} = \boldsymbol{a}x$ para todo $x \in G$, de donde $N_{\boldsymbol{a}} = G$.

Si recíprocamente, $N_{\boldsymbol{a}} = G$, $x\boldsymbol{a} = \boldsymbol{a}x$ para toda $x \in G$, de modo que $\boldsymbol{a} \in Z(G)$.

Si G es finito, $|N_{\boldsymbol{a}}| = |G|$ es equivalente a $N_{\boldsymbol{a}} = G$.

Definición 1.1.15. Subgrupo Normal

Un subgrupo H de G, se dice que es un subgrupo normal de G si para toda $\boldsymbol{a} \in G$ y toda $h \in H$, se cumple $\boldsymbol{a}h\boldsymbol{a}^{-1} \in H$.

Definición 1.1.16. Homomorfismo de grupo

Un homomorfismo es una función φ de un grupo G_1 sobre un grupo G_2 tal que cumple la condición:

$$\varphi(\boldsymbol{a}\cdot b) = \varphi(\boldsymbol{a})\cdot\varphi(b), \text{ para todo } \boldsymbol{a}, b \text{ de } G_1.$$

Definición 1.1.17. Isomorfismo de Grupo

Dos subgrupos G_1 y G_2 se dice que son isomorfos si existe una función uno a uno φ de G_1 sobre G_2, tal que para todo par de elementos $\boldsymbol{a}, b$ de G_1, se cumple:

$$\varphi(\boldsymbol{a}\cdot b) = \varphi(\boldsymbol{a})\cdot\varphi(b).$$

Definición 1.1.18. Automorfismo de Grupo

Por automorfismo de un grupo G, entenderemos un isomorfismo de G sobre sí mismo.

1.1.1. GRUPOS DE PERMUTACIONES

Definición 1.1.1.1. Permutación de un grupo

A un mapeo uno a uno de un conjunto $\{1, \dots, n\}$ sobre sí mismo le llamamos una permutación.

Cuando el conjunto dado es finito, una permutación puede escribirse poniendo en la primera fila todos los elementos del conjunto y debajo de cada elemento su imagen. La notación es la siguiente:

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

Ejemplo 1.1.1.1. Sea $\{1, 2, 3\}$ un conjunto. Entonces las permutaciones del conjunto son las siguientes:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Definición 1.1.1.2. Grupo simétrico

Grupo simétrico es el grupo de todas las permutaciones sobre un conjunto S. El grupo simétrico sobre n elementos es a menudo representado por S_n.

Se define el conjunto $S_n = \{\alpha: (1, \dots, n) \to (1, \dots, n) \mid \alpha \text{ es una permutación}\}$

Definición 1.1.1.3. Orden de un grupo simétrico

El orden del grupo simétrico S_n es $n!$. Se denota $|S_n| = n!$.

Definición 1.1.1.4. Multiplicación de permutaciones

Se define la multiplicación de dos permutaciones $\alpha, \beta \in S_n$ mediante $\alpha\beta = \alpha \circ \beta$, donde $\circ$ es composición usual de aplicaciones.

Ejemplo 1.1.1.2. Sea $\{1, 2, 3\}$ un conjunto y consideremos dos permutaciones encontradas en el ejemplo 1.1.1.1.

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Calcular $\alpha_2 \circ \alpha_6$.

Solución:

Usaremos la notación $\alpha_2\alpha_6$ para denotar la aplicación $\alpha_2 \circ \alpha_6$, esto quiere decir, primero se aplica α_6 y luego se aplica α_2.

$$\alpha_2 \circ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Definición 1.1.1.5. Ciclo de una permutación

Un ciclo de una permutación es la permutación α que envía a_1 en $\boldsymbol{a_2}$, $\boldsymbol{a_2}$ en $\boldsymbol{a_3}$,…,$\boldsymbol{a_{m+1}}$ en $\boldsymbol{a_m}$ y $\boldsymbol{a_m}$ en $\boldsymbol{a_1}$, y deja sin modificación todos los otros elementos.

Al ciclo α lo denotaremos por $(\boldsymbol{a_1}\, \boldsymbol{a_2}\, \ldots\, \boldsymbol{a_m})$ y al numero m lo llamaremos longitud del ciclo α.

Definición 1.1.1.6. Ciclos disjuntos

Dos ciclos $(\boldsymbol{a_1}\, \boldsymbol{a_2}\, \ldots\, \boldsymbol{a_m})$ y $(b_1\, b_2\, \ldots\, b_r)$ de S_n son disjuntos si para todos $i, j,\ 1 \leq i \leq m,\quad 1 \leq j \leq r,\quad \boldsymbol{a_i} \neq b_j$.

Ejemplo 1.1.1.3. Sea $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ un conjunto, encontrar los ciclos de la siguiente permutación $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}$.

Solución.

Veamos que la permutación α lleva $1 \to 3,\ 3 \to 4,\ 4 \to 2,\ 2 \to 6,\ 6 \to 1$

por definición de ciclo se tiene el ciclo $(1, 3, 4, 2, 6)$ y por la misma definición para los demás elementos de S_α lleva $5 \to 5,\ 7 \to 7,\ 8 \to 8,\ 9 \to 9$

y por tanto se dejan sin modificación.

Por lo que los ciclos de α son: $(1, 3, 4, 2, 6), (5), (7), (8), (9)$.

Lema 1.1.1.1. Toda permutación es el producto de sus ciclos.

Prueba:

Sea α la permutación. Entonces sus ciclos son de la forma $(s, s\alpha, \dots, s\alpha^{t-1})$.

De acuerdo con la multiplicación de ciclos, según lo definimos anteriormente, y como los ciclos de α son ajenos, la imagen de $s' \in S$ bajo α, que es $s'\alpha$, es la misma que la imagen de s' bajo el producto, ψ, de todos los ciclos distintos de α.

Luego α y ψ tienen el mismo efecto sobre cada uno de los elementos de S , de donde $\alpha = \psi$, que es lo que queríamos probar.

Ejemplo 1.1.1.4. En el ejemplo 1.1.1.2 se puede representar la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}$$

como el producto de los ciclos encontrados en dicho ejemplo, así

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix} = (1,3,4,2,6)(5)(7)(8)(9)$$

Definición 1.1.1.7. Descomposición de ciclos de orden k en ciclos de orden 2.

Un ciclo de orden k $(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \boldsymbol{a}_3, \dots, \boldsymbol{a}_{k-1},\ \boldsymbol{a}_k)$ en S_n puede ser descompuesto en ciclos de orden 2 de la siguiente forma:

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \dots, \boldsymbol{a}_{k-1}, \boldsymbol{a}_k) = (\boldsymbol{a}_1, \boldsymbol{a}_2)(\boldsymbol{a}_1, \boldsymbol{a}_3) \dots (\boldsymbol{a}_1, \boldsymbol{a}_{k-1})(\boldsymbol{a}_1, \boldsymbol{a}_k).$$

Lema 1.1.1.2. Toda permutación es un producto de ciclos de orden 2.

Prueba:

Primero note que la identidad $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ puede ser expresada como $(1,2)(1,2)$, y así este es el producto de ciclos de orden 2 (esto es porque necesitamos $n > 1$). Ahora consideremos cualquier permutación $\alpha \in S_n$.

Ya sabemos que podemos escribir α como un producto disjunto de ciclos de orden 2:

$\alpha = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_r)(b_1, b_2, \dots, b_s) \dots (c_1, c_2, \dots, c_t)$

y cada ciclo puede ser descompuesto sobre ciclos de orden 2 como sigue:

$\alpha = (\boldsymbol{a}_1, \boldsymbol{a}_2)(\boldsymbol{a}_1, \boldsymbol{a}_3) \dots (\boldsymbol{a}_1, \boldsymbol{a}_r)(b_1, b_2)(b_1, b_3) \dots (b_1, b_s) \dots (c_1, c_2)(c_1, c_3) \dots (c_1, c_t)$.

Esto completa la prueba.

Definición 1.1.1.8. Transposición

A los ciclos de orden 2 les llamaremos transposiciones.

Definición 1.1.1.9. Permutación par

Una permutación α, se dice que es una permutación par si puede representarse como un producto de un número par de transposiciones.

Definición 1.1.1.10. Permutación impar

Una permutación α que puede descomponerse en un número impar de trasposiciones recibe el nombre de permutación impar.

Definición 1.1.1.11. Signatura de una permutación

La signatura de una permutación de S_n se define mediante $sig\,(\alpha)$, como $sig\,(\alpha) = (-1)^m$ donde m es el número de transposiciones en que se ha descompuesto la permutación α.

Definición 1.1.1.12. Grupo alternado

Un subgrupo normal de S_n que está formado por todas aquellas permutaciones α tales que $sig(\alpha) = 1$, es decir las permutaciones pares, se denomina grupo alternado de n elementos. Se simboliza por $Alt(n)$

1.2. TEORÍA DE ANILLOS

Continuando con el estudio de las estructuras algebraicas, en este apartado estudiaremos los Anillos, proporcionando conceptos algebraicos que ayuden a la comprensión de esta estructura.

Definición 1.2.1. Anillo

Un conjunto no vacío R se dice que es un anillo si en R están definidas dos operaciones, denotadas por "+" y "·" respectivamente tales que para cualesquiera $\boldsymbol{a}, b, c$ de R se cumplen:

1) *Ley de cerradura para la suma*.

   La suma está bien definida. Esto significa que, para todo par de elementos $\boldsymbol{a}, b$ de R, $\boldsymbol{a} + b = c$ existe y es un elemento único de R.

2) *Ley asociativa para la suma*.

   $(\boldsymbol{a} + b) + c = \boldsymbol{a} + (b + c)$.

3) *Ley conmutativa para la suma*.

   $b + \boldsymbol{a} = \boldsymbol{a} + b$

4) *Elemento neutro para la suma*.

   Existe un 0 tal que $0 + \boldsymbol{a} = \boldsymbol{a} + 0 = \boldsymbol{a}$, para toda $\boldsymbol{a}$ de R.

5) *Elemento inverso para la suma*.

   Para toda $\boldsymbol{a}$ existe una $-\boldsymbol{a}$ tal que $(-\boldsymbol{a}) + \boldsymbol{a} = \boldsymbol{a} + (-\boldsymbol{a}) = 0$

6) *Ley de cerradura para la multiplicación*.

   La multiplicación está bien definida $\boldsymbol{a} \cdot b = d$ existe y es un elemento único de R.

7) *Ley asociativa para la multiplicación*.

   $(\boldsymbol{a} \cdot b) \cdot c = \boldsymbol{a} \cdot (b \cdot c)$

8) *Leyes distributivas*.

   $\boldsymbol{a} \cdot (b + c) = \boldsymbol{a} \cdot b + \boldsymbol{a} \cdot c$

   $(b + c) \cdot \boldsymbol{a} = b \cdot \boldsymbol{a} + c \cdot \boldsymbol{a}$

Notación. Escribimos $\langle R, +, \cdot \rangle$ para denotar un anillo R con dos operaciones definidas en él.

Definición 1.2.2. Anillo con unidad

Un anillo con unidad, es un anillo con unidad multiplicativa, usualmente denotado por 1, que satisface la propiedad $\boldsymbol{a} \cdot 1 = 1 \cdot \boldsymbol{a} = \boldsymbol{a}$ para todo $\boldsymbol{a}, b$ de R.

Definición 1.2.3. Anillo conmutativo

Si la multiplicación de R es tal que $\boldsymbol{a} \cdot b = b \cdot \boldsymbol{a}$ para todo $\boldsymbol{a}b$ de R, entonces llamamos a R anillo conmutativo.

Definición 1.2.4. Divisor de cero

Si R es un anillo, un elemento $\boldsymbol{a}$ de R, con $\boldsymbol{a} \neq 0$, se dice que es un divisor de cero si existe un elemento b de R, $b \neq 0$, tal que $\boldsymbol{a} \cdot b = 0$ ó $b \cdot \boldsymbol{a} = 0$.

Definición 1.2.5. Anillo de división

Es un anillo R en el cual los elementos diferentes de cero $R^* = R - \{0\}$ forman un grupo bajo la multiplicación.

Definición1.2.6. Subanillo

Un subconjunto S de un anillo $\langle R, +, \cdot \rangle$, se dice que es un subanillo de R si $\langle S, + \rangle$ es un subgrupo de $\langle R, + \rangle$ y el producto restringido a S es cerrado; de forma equivalente, la suma y el producto son operaciones cerradas sobre S y $\langle S, +, \cdot \rangle$ es un anillo.

Definición 1.2.7. Ideal

Sea R un anillo. Un subconjunto no vacío I de R se llama ideal de R si:

a) I es un subgrupo aditivo de R.

b) Dados $r \in R$, $\boldsymbol{a} \in I$, entonces $\boldsymbol{a}r \in I$ y $r\boldsymbol{a} \in I$.

Definición 1.2.8. Centro de un anillo

Sea R un anillo, el centro de un anillo, que denotaremos por $Z(R)$, es por definición el conjunto:

$$Z(R) = \{z \in R | zx = xz \text{ para todo } x \in R\}.$$

Nota. Denotaremos $Z(R) = Z$.

Definición 1.2.9. Normalizador de un anillo

Sea $x \in R$, el normalizador de x en R, es el conjunto:

$$N_x = \{\boldsymbol{a} \in R | \ \boldsymbol{a}x = x\boldsymbol{a}\}.$$

Proposición.1.2.1. El centro de un anillo R es un subanillo conmutativo de R.

Prueba:

Debemos mostrar que $Z(R)$ es no vacío, es cerrado bajo la suma y la multiplicación y contiene inversos aditivo.

Dado que $0 \cdot r = 0 = r \cdot 0$ para todo $r \in R$ la identidad aditiva $0 \in Z$, y por tanto Z es no vacio.

Si $z, w \in Z$ y $x \in R$, entonces

$(z + w)x = zx + wx = xz + xw = x(z + w)$

donde la segunda igualdad se sigue de que $z, w \in Z$. Por tanto $z + w$ está en Z.

Similarmente, para cualquier $x \in R$ tenemos:

$$(zw)x = z(wx) = z(xw) = (zx)w = (xz)w = x(zw)$$

Por tanto, $zw \in Z$.

Finalmente, para cualquier $x \in R$ tenemos:

$$(-z)x = -(zx) = -(xz) = x(-z)$$

Por tanto, $-z \in Z$.

Así, hemos demostrado que el centro e un anillo es un subanillo de R.

Proposición.1.2.2. Sean R un anillo de división y $\boldsymbol{a} \in R$. Entonces

$N_x = \{\boldsymbol{a} \in R | \ \boldsymbol{a}x = x\boldsymbol{a}\}$ es un subanillo de división de R. Además $Z(R) \subseteq N_x \subseteq R$.

Prueba:

Si $\boldsymbol{a} \in Z$, entonces $\boldsymbol{a}r = r\boldsymbol{a}$ para toda $r \in R$, en particular $\boldsymbol{a}x = x\boldsymbol{a}$, luego $\boldsymbol{a} \in N_x$; se sigue que $Z \in N_x$.

Sean $\boldsymbol{a}, b \in N_x$, entonces $(\boldsymbol{a}+b)x = \boldsymbol{a}x + bx = x\boldsymbol{a} + xb = x(\boldsymbol{a}+b)$ por lo cual $\boldsymbol{a}+b \in N_x$. Por otro lado $(\boldsymbol{a}b)x = \boldsymbol{a}(bx) = \boldsymbol{a}(xb) = (\boldsymbol{a}x)b = (x\boldsymbol{a})b = x(\boldsymbol{a}b)$ luego $\boldsymbol{a}b \in N_x$.

Sea $\boldsymbol{a} \in N_x$ con $x \neq 0$, como $\boldsymbol{a}x = x\boldsymbol{a}$ entonces $x = \boldsymbol{a}^{-1}x\boldsymbol{a}$, por lo cual $x\boldsymbol{a}^{-1} = \boldsymbol{a}^{-1}x$, esto es, $\boldsymbol{a}^{-1} \in N_x$.

Por Lema 1.1.1, se concluye que $Z(R) \subseteq N_x$.

1.3. TEORÍA DE CAMPOS

Continuando con el estudio de las estructuras algebraicas, este apartado está dedicado a la teoría de Campos donde se proporciona el concepto y algunas propiedades.

Definición 1.3.1. Campo

Un conjunto no vacío F se dice que es un campo si en F están definidas dos operaciones, denotadas por "$+$" y "$\cdot$" respectivamente tales que para cualesquiera $\boldsymbol{a}, b, c$ de F se cumplen:

1) *Ley de cerradura para la suma*. La suma está bien definida. Esto significa que, para todo par ordenado de elementos $\boldsymbol{a}, b$ de F, $a + b = c$ existe y es un elemento único de F.
2) *Ley asociativa para la suma*. $(\boldsymbol{a} + b) + c = \boldsymbol{a} + (b + c)$
3) *Ley conmutativa para la suma*. $b + \boldsymbol{a} = \boldsymbol{a} + b$.
4) *Elemento neutro para la suma*. Existe un 0 tal que $0 + \boldsymbol{a} = \boldsymbol{a} + 0 = \boldsymbol{a}$, para toda $\boldsymbol{a}$ de F.
5) *Elemento inverso para la suma*. Para toda a existe una $-\boldsymbol{a}$ tal que $(-\boldsymbol{a}) + \boldsymbol{a} = \boldsymbol{a} + (-\boldsymbol{a}) = 0$.
6) *Ley de cerradura para la multiplicación*. La multiplicación está bien definida $ab = d$ existe y es un elemento único de F.
7) *Ley asociativa para la multiplicación*. $(\boldsymbol{a} \cdot b) \cdot c = \boldsymbol{a} \cdot (b \cdot c)$.

8) *Leyes distributivas.*

$$\boldsymbol{a} \cdot (b + c) = \boldsymbol{a} \cdot b + \boldsymbol{a} \cdot c,$$

$$(b + c) \cdot \boldsymbol{a} = b \cdot \boldsymbol{a} + c \cdot \boldsymbol{a}.$$

9) *Ley conmutativa para la multiplicación*. $b \cdot \boldsymbol{a} = \boldsymbol{a} \cdot b$.

10) *Elemento identidad en la multiplicación*. Existe un 1 tal que

$1 \cdot \boldsymbol{a} = \boldsymbol{a} \cdot 1 = 1$, para toda $\boldsymbol{a}$ de F.

11) *Elemento inverso para la multiplicación*. Para toda $\boldsymbol{a} \neq 0$, existe un $\boldsymbol{a}^{-1}$ tal que

$(\boldsymbol{a}^{-1}) \cdot \boldsymbol{a} = \boldsymbol{a} \cdot (\boldsymbol{a}^{-1}) = 1$.

Nota. Cuando el anillo de división R es conmutativo se dice que R es un campo.

Definición 1.3.2. Subcampo

Un subcampo E de F es un subconjunto de F que es campo para las mismas operaciones.

Definición 1.3.3. Espacio vectorial sobre un campo

Un espacio vectorial sobre un campo F es un grupo abeliano $\langle V, + \rangle$ junto con una operación escalar, que es, una función de $F \times V$ sobre V, la cual puede ser denotada por yuxtaposición y llamada multiplicación escalar.

Esto significa que para todo $\boldsymbol{a}$ de F y todo v de V, $\boldsymbol{a}v$ de V. Decimos que $\boldsymbol{a}v$ es un múltiplo escalar de V. Si se cumplen los siguientes axiomas:

1. *La multiplicación escalar se distribuye sobre la suma en F.*

   Para todo $\boldsymbol{a}, b$ de F y v de V, $(\boldsymbol{a}+b)v = \boldsymbol{a}v + bv$.

2. *La multiplicación escalar es distributiva sobre la suma en V.*

   Para todo $\boldsymbol{a}$ de F y v, w de V, $\boldsymbol{a}(v+w) = \boldsymbol{a}v + \boldsymbol{a}w$.

3. *La multiplicación escalar es asociativa sobre la multiplicación en F.*

   Para toda $\boldsymbol{a}, b$ de F y v de V, $(\boldsymbol{a}b)v = \boldsymbol{a}(b(v))$.

4. *La identidad de F es una identidad para la multiplicación escalar.*

   Para todo v de V, $1v = v$.

Definición 1.3.4. Dependencia e independencia de un conjunto de vectores

Un conjunto no vacío de vectores S en un espacio vectorial V sobre un campo F se dice que es linealmente dependiente sobre F si existe un subconjunto finito de S, es decir $s_1, \dots, s_n$, y escalares $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ no todos ceros tal que $\boldsymbol{a}_1 s_1 + \cdots + \boldsymbol{a}_n s_n = 0$.

Un conjunto no vacío es llamado independiente si no es dependiente.

Definición 1.3.5. Base

Una base para un espacio vectorial sobre F es un conjunto de vectores que extiende V sobre F y son independientes sobre F.

Así si B es una base para V sobre F y toda $v \in V$ puede ser expresada en una y solo una forma como una suma finita de múltiples escalares de los elementos en la base. Esto es, dado $v \in V$ existen vectores $b_1, \dots, b_n$ en B y escalares $v_1, \dots, v_n$ en F tal que

$$v = v_1 b_1 + \cdots + v_n b_n.$$

Definición 1.3.6. Extensión de un campo

Si E es un subcampo de F, se dice que F es un campo de extensión (o una extensión) de E. Se denota por F/E.

En particular, todo campo E es una extensión de su subcampo primo. El campo E es llamado a veces el campo base de una extensión.

La notación F/E para una extensión de un campo es una abreviatura de "F sobre E" y no es el cociente de F por E.

Si F/E es cualquier extensión de campos, entonces la multiplicación definida en F hace a F un espacio vectorial sobre E. En particular todo campo E puede ser considerado como un espacio vectorial sobre su campo primo.

Definición 1.3.7. Grado de una extensión de un campo

El grado de una extensión de un campo F/E, denotada $[F:E]$, es la dimensión de F como un espacio vectorial sobre E, es decir, $[F:E] = \dim_E F$.

La extensión se dice que es finita si $[F:E]$ es finita y se dice que es infinita de otra forma.

Definición 1.3.8. Grupo multiplicativo de un campo

Los elementos diferentes de cero de un campo que forman un grupo bajo la multiplicación $\{F - \{0\}, \cdot\}$ se denominan grupo multiplicativo.

Definición 1.3.9. Característica de un campo

La característica de un campo F, denotada por $ch(F)$, es definida como el entero positivo más pequeño p tal que $p.x = \underbrace{x + x + x + \cdots + x}_{p\ veces} = 0$ para algún $x \neq 0$ en F.

Proposición 1.3.1. La característica de un campo F, $ch(F)$, es 0 ó un número primo p. Si $ch(F) = p$ entonces para cualquier $x \in F$, $p.x = \underbrace{x + x + x + \cdots + x}_{p\ veces} = 0$.

Prueba:

Supongamos que $ch(F) = n$, $n \neq 0$, si $n = \boldsymbol{a}b$ es un número compuesto, con $n \cdot 1_F = 0$, entonces $\boldsymbol{a}b \cdot 1_F = (\boldsymbol{a} \cdot 1_F)(b \cdot 1_F) = 0$ y dado que F es un campo, $\boldsymbol{a} \cdot 1_F$ ó $b \cdot 1_F$ es 0, por lo que el menor entero es necesariamente un número primo.

Se ha probado así la primer parte de la proposición.

Sea $ch(F) = p$, y dado que F es un campo, se tiene la siguiente igualdad:

$$px = p(1_F \cdot x)$$

$$= (p \cdot 1_F)x$$

$$= (0)x$$

$$= 0$$

Quedando así probada la segunda parte de la proposición.

Definición 1.3.10. Campos primos

A los campos que no tienen ningún subcampo distinto de si mismo se les llama campos primos.

Todo campo es subcampo de sí mismo.

El subcampo primo de un campo F es el subgrupo de F generado por la identidad multiplicativa 1 de F. Es (isomorfo a) $\mathbb{Q}$ (si $ch(F) = 0$) o F_p(si $ch(F) = p$).

$\mathrm{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ el conjunto de los enteros módulo p.

Definición 1.3.11. Polinomio

Para $\boldsymbol{a}_0, \dots, \boldsymbol{a}_n$ constantes en algún campo F, un polinomio $p(x)$, de grado n en la variable x es de la forma: $p(x) = \boldsymbol{a}_n x^n + \boldsymbol{a}_{n-1} x^{n-1} + \cdots + \boldsymbol{a}_1 x^1 + \boldsymbol{a}_0 x^0$

Definición 1.3.12. Grado de un polinomio

Si $p(x) = \boldsymbol{a}_n x^n + \boldsymbol{a}_{n-1} x^{n-1} + \cdots + \boldsymbol{a}_1 x + \boldsymbol{a}_0 \neq 0$ y $\boldsymbol{a}_n \neq 0$, entonces el grado de $p(x)$, escrito $degp(x)$, es n.

Definición 1.3.13. Polinomio mónico.

Sea $\boldsymbol{a}_n x^n$ el término principal del polinomio

$$p(x) = \boldsymbol{a}_n x^n + \boldsymbol{a}_{n-1} x^{n-1} + \cdots + \boldsymbol{a}_1 x + \boldsymbol{a}_0$$

y $\boldsymbol{a}_n$ el coeficiente principal. Si $\boldsymbol{a}_n = 1$, entonces el polinomio es mónico.

Definición 1.3.14. Anillo de polinomios

Sea F un campo, el anillo de polinomio escrito como $F[x]$ es el conjunto de todos los símbolos $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \cdots + \boldsymbol{a}_n x^n$ donde n puede ser cualquier entero no negativo y donde los coeficientes $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ están todos en F.

Definición 1.3.15. Raíz de un polinomio

Si $p(x) \in F[x]$, entonces un elemento $\boldsymbol{a}$ que se encuentra en algún campo de extensión de F, se llama raíz de $p(x)$ si $p(\boldsymbol{a}) = 0$.

Definición 1.3.16. Campo de descomposición

La extensión del campo E de F, es llamada un campo de descomposición para el polinomio $f(x) \in F[x]$ si $f(x)$ se descompone completamente en factores lineales en $F[x]$.

Definición 1.3.17. Polinomio irreducible

Es un polinomio $p(x)$ tal que los únicos divisores son la unidad y el mismo $p(x)$.

Definición 1.3.18. Raíces de unidad

Sea F cualquier campo. Sea n un entero positivo. Una n-ésima raíz de unidad es un elemento $\zeta \in F$ tal que $\zeta^n = 1$ para algún entero positivo n.

Definición 1.3.19. Raíz primitiva de unidad

Un generador del grupo de las *n*-ésimas raíces de unidad es llamado una *n*-ésimas raíz primitiva de unidad.

Definición 1.3.20. El *n*-ésimo polinomio ciclotómico

El *n*-ésimo polinomio ciclotómico $\Phi_n(x)$ como el polinomio cuyas raíces son las *n*-ésimas raíces primitivas de la unidad:

$$\Phi_n(x) = \prod_{mcd(n,m)=1} (x - \zeta^m)$$

1.4. CAMPOS FINITOS

Es esencial para el desarrollo del teorema de Wedderburn investigar previamente sobre los campos que tienen un número finito de elementos y sus propiedades.

Definición 1.4.1. Campo finito

Es un campo que solo tiene un numero finito de elementos.

El ejemplo más pequeño en el que se puede pensar debe tener por lo menos dos elementos: el cero y el uno (para poder definir la operación binaria). Sea $A = \{0, 1\}$.

El anillo $\mathbb{Z}_p$ es una de las estructuras más importantes en teoría de números. La manera conveniente de construir esta estructura es por medio de la definición de congruencia.

La relación de congruencia se define como:

$\boldsymbol{a} \equiv b$ si y solo si $n|\boldsymbol{a} - b$. Si los enteros $\boldsymbol{a}, b$ están relacionados diremos que $\boldsymbol{a}$ es congruente con b modulo p.

El conjunto $\mathbb{Z}_p$ se conoce con el nombre de anillos de residuos módulo p y se denotan por $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$ pero se puede escribir simplemente como

$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

En el anillo de residuos modulo p se introduce una suma y un producto:

$$[\boldsymbol{a}] + [b] = [\boldsymbol{a} + b], \quad [\boldsymbol{a}][b] = [\boldsymbol{a}b].$$

Teorema 1.4.1. $\mathbb{Z}_p$ es un campo si y solo si p es un primo.

Prueba:

" $\Rightarrow$ "

Supongamos que si $\mathbb{Z}_p$ es un campo implica que p es un número primo.

Haremos un razonamiento por contradicción. Supongamos que p no es un número primo con $\boldsymbol{a}$ y b estrictamente menores que p, donde $p = \boldsymbol{a}b$. En $\mathbb{Z}_p$, tenemos que $[\boldsymbol{a}][b] = [\boldsymbol{a}b] = [p] = [0]$. Si $\mathbb{Z}_p$ es un campo, necesariamente $[\boldsymbol{a}] = 0$ o bien $[b] = 0$. Lo que contradice la hipótesis.

Entonces p es un número primo.

" $\Leftarrow$ "

Supongamos que si p es un número primo implica que $\mathbb{Z}_p$ es un campo.

Como $\mathbb{Z}_p$ es un anillo, asi que solo resta demostrar que todo elemento de $\mathbb{Z}_p$ tiene inverso multiplicativo. En efecto, consideremos $[m] \in \mathbb{Z}_p$ con $m < p$. Por ser p primo tenemos que m y p son primos entre si y por tanto existen enteros tales que

$1 = \boldsymbol{a}m + bp,$ de donde $[1] = [\boldsymbol{a}][m] + [b][p],\ [b][p] = [b][0] = [0]$.

Luego $[1] = [\boldsymbol{a}][m]$ y el inverso multiplicativo de $[m]$ es $[\boldsymbol{a}]$.

Entonces $\mathbb{Z}_p$ es un campo.

A los campos finitos se les llama campos de Galois en honor al matemático francés Evariste Galois (1811 - 1832). Al resolver el problema de encontrar cuales ecuaciones polinomiales tienen solución en radicales y cuáles no, Galois invento la Teoría de Grupos. El campo de Galois o también llamado campo finito es denotado por $GF(p^r)$.

1.5. PROPIEDADES DE LOS CAMPOS FINITOS

Propiedad 1.5.1. El número de elementos en un campo finito es una potencia de un primo.

Prueba:

Sea F un campo finito y sea q el número de elementos en él.

La característica de F no puede ser cero, para este caso el campo primo E en F ya tendría un número infinito de elementos.

Sea p la característica de F. Entonces el campo primo E es isomorfo con el anillo de clases residuales modulo p, y tiene p elementos.

Dado que solo existe un numero finito de elementos en F, existe en F un conjunto maximal de elementos linealmente independientes $\alpha_1, \dots, \alpha_n$ con respecto a E. De aquí, que n es el grado del campo $[F:E]$, y todo elemento de F es de la forma $c_1\alpha_1 + \cdots + c_n\alpha_n$ con coeficientes únicamente determinados en E.

Para todo coeficiente c_i, p valores son posibles, así existe estrictamente p^n expresiones de la forma $c_1\alpha_1 + \cdots + c_n\alpha_n$. Ya que ellos expresan la totalidad de los elementos en el campo, se sigue que $q = p^n$.

Así, hemos probado que el número de elementos en un campo finito es una potencia de p (p es la característica de F y el exponente es el grado del campo $[F:E]$).

Notación: Usaremos F_q para denotar al campo finito con $q = p^n$ elementos.

Propiedad 1.5.2. Para cada potencia de un primo p^r hay un campo finito $GF(p^r)$ con p^r elementos, y es único salvo isomorfismo.

Prueba:

Sea F un campo finito con $q = p^r$ elementos.

Sin el elemento cero todo anillo de división es un grupo multiplicativo. En el caso de un campo finito, el grupo es abeliano de orden $q - 1$. El orden de un elemento arbitrario α debe ser un divisor de $q - 1$ por Teorema 1.1.1 , de aquí se sigue que, $\alpha^{q-1} = 1$, para todo $\alpha \neq 0$. Multiplicando esta ecuación por α, obtenemos otra ecuación $\alpha^q - \alpha = 0$, la cual también es válida para $\alpha = 0$. De aquí que todos los elementos del campo son raíces del polinomio $x^q - x$. Si $\alpha_1, \dots, \alpha_q$ son los elementos del campo, $x^q - x$ debe ser divisible por $\prod_1^q (x - \alpha_i)$ dado que los grados son iguales y por Lema 1.4.1 , tenemos

$$x^q - x = \prod_1^q (x - \alpha_i)$$

Así, F va de E adjuntando todas las raíces del polinomio $x^q - x$. De aquí F es

únicamente determinado por un isomorfismo.

Así veamos lo siguiente para p y n dados todos los campos conmutativos con p^n elementos son isomorfos.

Se debe mostrar que para todo $n > 0$ y todo p existe actualmente un campo con $q = p^n$ elementos. Empecemos con el campo primo E de característica p, y forman un campo sobre E el cual $x^q - x$ se descompone en factores lineales. En este caso consideremos el conjunto de las raíces de $x^q - x$. Este conjunto es un campo, $x^{p^n} = x$ y $y^{p^n} = y$ implican $(x - y)^{p^n} = x^{p^n} - y^{p^n}$ y tomando $y \neq 0$ $\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}}$ de acuerdo con esto la diferencia y el cociente de dos raíces son nuevamente raíces. El polinomio $x^q - x$ tiene solo raíces simples, su derivada es $qx^{q-1} = -1$ dado que $q \equiv 0(p)$, y -1 nunca será cero. Asi el conjunto de sus raíces es un campo con q elementos. Así hemos probado que: Para toda potencia de un primo $q = p^n (n > 0)$ existe uno, y excepto para un solo isomorfismo, campo finito con precisamente q elementos, los elementos son las raíces del polinomio $x^q - x$.

Propiedad 1.5.3. Todo elemento x de $GF(p^r)$ satisface la relación $x^{p^r} = x$.

Prueba:

Si $x = 0$, el supuesto es verdadero. (Sustituyendo $0^{p^r} = 0$)

Si $x \neq 0$, entonces $x \in F^* = F - \{0\}$, y como F^* es un grupo con la multiplicación de F de orden $p^r - 1$, asi por Corolario 1.1.2 se tiene $x^{p^r-1} = 1$ para todo $x \neq 0$ en F.

Multiplicando esta relación $x^{p^r-1} = 1$ por x se obtiene que $x^{p^r} = x$.

Por tanto, hemos probado que todo elemento de un campo finito satisface la relación $x^{p^r} = x$.

Propiedad 1.5.4. El grupo multiplicativo $F^*(p^r)$ de los $p^r - 1$ elementos de $GF(p^r)$ distintos de cero, es cíclico. Un generador de este grupo cíclico se llama una raíz primitiva.

Prueba:

Sea F un campo finito. Sea G un grupo multiplicativo de los $p^r - 1$ elementos de F distintos de cero.

Dado que F es un campo finito, cualquier polinomio de grado n en $F[x]$ tiene a lo sumo n raíces en F. Así en particular, para cualquier entero n, el polinomio $x^n - 1$ tiene a lo sumo n raíces en F, y así todos los demás tienen a lo sumo n raíces en G.

La hipótesis del Lema 1.1.2 se satisface, dado que el grupo multiplicativo es un grupo Abeliano, y tiene la propiedad de que $x^n = 1$ que se satisface para lo sumo *n* elementos.

Por lo tanto G es un grupo cíclico.

Propiedad 1.5.5. Los automorfismos de $GF(p^r)$ son un grupo cíclico de orden r generado por el automorfismo $z \to \alpha(z) = z^p$.

Prueba:

Ya hemos visto que σ es un automorfismo de $GF(p^r)$. Además tenemos para $1 \leq k \leq m$ que $\alpha^k(z) = z^{p^k}$ y es la identidad si y solo si la ecuación $x^{p^r} = x$ tiene p^r soluciones, de aquí que si y solo si $k = r$. Por lo tanto hay al menos r automorfismos de $GF(p^r)$. Por otro lado sea ω que genera el grupo multiplicativo de $GF(p^r)$. Sea $q(x)$ el polinomio irreducible de grado r en $\mathbb{Z}_p[x]$ del cual ω es un cero. Cualquier automorfismo α de $GF(p^r)$ fijando 1 y de aquí que el subcampo primo $\mathbb{Z}_p$ entonces α también fijara $q(x)$. La imagen de ω es también un cero de $q(x)$. Esto significa que hay a lo sumo $r = \deg(q)$ posibilidades para la imagen $\alpha(\omega)$. Pero como $\mathbb{Z}_p(\omega) = GF(p^r)$ se deduce que una vez $\alpha(\omega)$ es determinado, cualquier imagen de $GF(p^r)$ bajo α es determinado. Por lo tanto puede haber a lo sumo tantos automorfismos como hay posibilidades para $\alpha(\omega)$, esto es, existe a lo sumo r automorfismos de $GF(p^r)$.

Combinando los argumentos de los dos últimos párrafos vemos que el grupo de automorfismos de $GF(p^r)$ es un grupo cíclico de orden r y generado por el automorfismo definido en $z \to \alpha(z) = z^p$.

Propiedad 1.5.6. Si F es un campo finito con q elementos y E es un subcampo de F, entonces el polinomio $x^q - x$ en $E[x]$ se factora en $F[x]$ como

$$x^q - x = \prod_{1}^{q} (x - \alpha_i)$$

y F es un campo de descomposición de $x^q - x$ sobre E.

Prueba:

El polinomio $x^q - 1$ de grado q tiene a lo mas q raíces en F. Por la propiedad 1.5.3 sabemos que existen q raíces nombradas, todo los elementos de F. Así el polinomio dado se descompone en F en la forma indicada, y no puede descomponerse en cualquier campo más pequeño.

CAPÍTULO II

PLANOS PROYECTIVOS Y TEORÍA DE ANILLOS ALTERNATIVOS

En este segundo capítulo se introducen conceptos fundamentales, para el estudio y el desarrollo de uno de los teoremas de este trabajo de graduación el cual es El Teorema de Artin-Zorn.

2.1. PLANOS PROYECTIVOS

En esta sección se da a conocer algunos conceptos geométricos como lo es punto, recta, plano; antes de entrar en detalle sobre los Planos Proyectivos.

Un punto es una figura geométrica adimensional: no tiene longitud, ni área y ni volumen, es decir la marca más pequeña que se pueda dibujar.

Una recta o **línea recta** es la que se extiende en una misma dirección y contiene infinitos puntos.

Un plano es la superficie geométrica que no posee volumen (es decir, que es solo bidimensional) y que posee un número infinito de rectas y puntos que lo cruzan de un lado al otro.

Definición 2.1.1. Plano proyectivo

Un plano proyectivo es un conjunto de puntos con ciertos subconjuntos distinguidos de él llamados rectas, que satisfacen los siguientes axiomas:

P1. Dos puntos distintos cualesquiera están contenidos en una y solo una recta.

La única recta k que contiene dos puntos distintos A y B se llamara la recta que une A y B.

P2. Dos rectas distintas contienen uno y solo un punto.

El punto único P contenido en dos rectas distintas k y t se llamara la intersección de k y t.

P3. Existen cuatro puntos tales que no hay tres de ellos que estén contenidos en una misma recta. (Ver Figura 2.1.1)

Sean A_1, A_2, A_3, A_4 cuatro puntos, ninguno de tres puntos esta sobre una misma recta. Su existencia está dada por P3. Hay entonces seis rectas distintas que unen los diferentes pares:

$L_1: A_1A_2B_1$

$L_2: A_1A_3B_2$

$L_3: A_1A_4B_3$

$L_4: A_2A_3B_3$

$L_5: A_2A_4B_2$

$L_6: A_3A_4B_1$

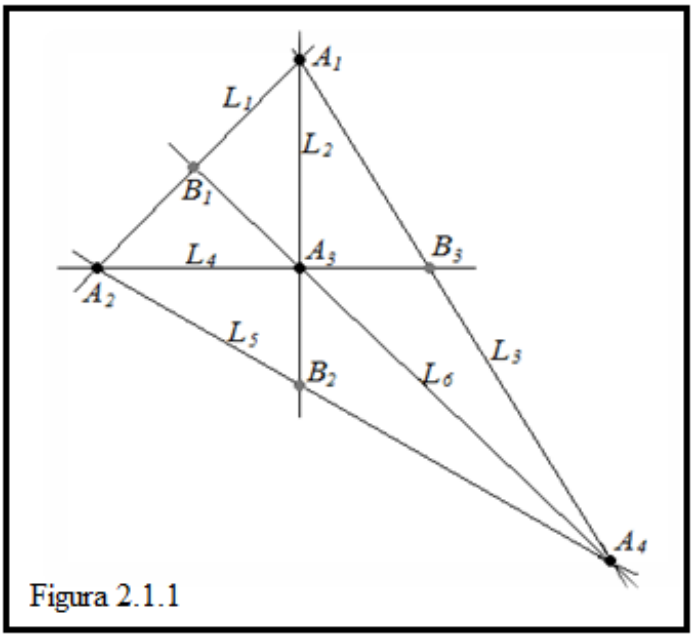


Figura 2.1.1

Aquí los puntos B_1, B_2, B_3 son las intersecciones de estas rectas, y por ser todas ellas distintas los B son distintos de los A y también distintos entre sí.

Ejemplo 2.1.1. Comprobar si el siguiente esquema del teorema de Desargues es un plano proyectivo.

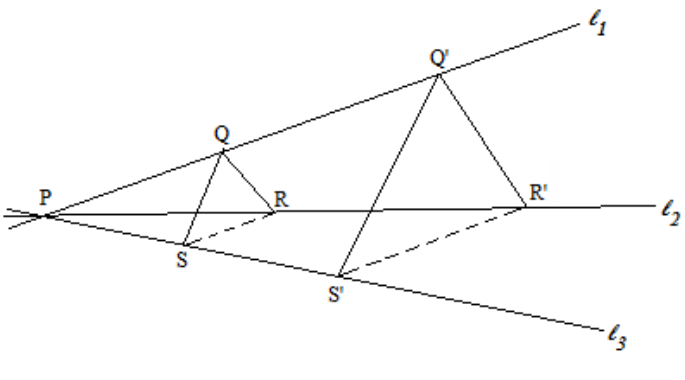


Figura 2.1.2

Solución:

Verificar si cumple las tres propiedades anteriores:

P1. Dos puntos distintos cualesquiera están contenidos en una y solo una recta.

Esta propiedad se cumple porque para cualesquiera dos puntos en la Figura 2.1.2 *solo existe una recta entre ellos dos. Por ejemplo, entre los puntos Q y S existe una y solo una recta entre ambos puntos.*

P2. Dos rectas distintas contienen uno y solo un punto.

Se cumple para todas las rectas de la Figura 2.1.2 *que en todos los casos es el punto de intersección. Por ejemplo, para la recta ℓ_1 y ℓ_2 contienen uno y solo un punto que en este caso es el punto P.*

P3. Existen cuatro puntos tales que no hay tres de ellos que estén contenidos en una misma recta.

Esta propiedad también se cumple. Por ejemplo, los puntos P, Q, Q' y R' no existen tres puntos que estén contenidos en la misma recta, ya que el punto Q esta contenido en la recta ℓ_1 y en la recta que va de Q a R.

Por lo tanto, el esquema del teorema de Desargues es un plano proyectivo.

Definición 2.1.2. Rectas concurrentes

Rectas concurrentes son tres o más rectas que tienen un punto en común.

(Ver Figura 2.1.3).

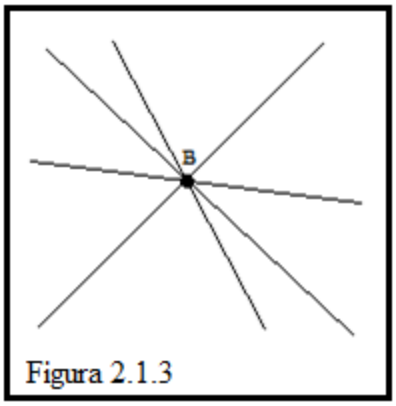


Figura 2.1.3

Definición 2.1.3. Isomorfismo de Planos

Un plano π_1 se dice que es isomorfo a un plano π_2 si hay una correspondencia uno a uno $P_1 \rightleftarrows P_2 = \alpha(P_1)$ entre los puntos $\{P_1\}$ de π_1 y los puntos $\{P_2\}$ de π_2 y una correspondencia uno a uno $k_1 \rightleftarrows k_2 = \beta(k_1)$ entre las rectas $\{k_1\}$ de π_1 y las rectas $\{k_2\}$ de π_2, tal que si $P_1 \in k_1$, entonces $\alpha(P_1) \in \beta(k_1)$.

Es claro que cada una de las correspondencias α y β determina a la otra, y una correspondencia uno a uno de puntos $P_1 \rightleftarrows \alpha(P_1)$ determinara un isomorfismo si cualesquiera tres puntos P_1, Q_1, R_1 de π_1 que estén sobre una misma recta, tienen siempre imágenes $\alpha(P_1), \alpha(Q_1)$ y $\alpha\,(R_1)$ que están también sobre una misma recta. Análogamente una correspondencia uno a uno β de rectas determinara un isomorfismo si todo conjunto de tres rectas concurrentes están mapeados sobre un conjunto de rectas concurrentes.

Definición 2.1.4. Colineación

Una colineación es un isomorfismo α de un plano π sobre sí mismo.

Las colineaciones de un plano forman un grupo.

Definición 2.1.5. Eje de la colineación

Sea α una colineación. La recta L, cuyos todos los puntos son fijados por α, se llama el eje de la colineación. (ver Figura 2.1.4).

Definición 2.1.6. Centro de la colineación

Sea α una colineación. El punto O, a través del cual toda recta permanece fija, se llama el centro de la colineación. (ver Figura 2.1.4)

Definición 2.1.7. Elación y homología

Sea α una colineación. Si deseamos hacer una distinción entre el eje de la colineación y el centro de la colineación, entonces si el centro O se encuentra sobre el eje L, llamamos a la colineación una elación. Si O no se encuentra en L, la colineación se llama una homología. (ver Figura 2.1.4)

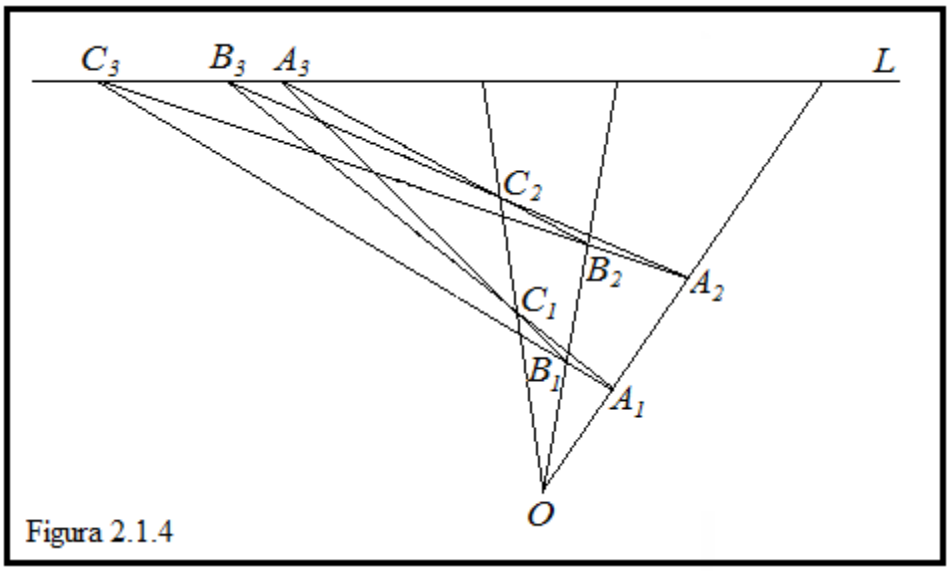


Figura 2.1.4

Definición 2.1.8. Operación ternaria

Sea ℓ una recta. Sean M y C coordenadas, donde $M = \ell \cap XY$ y $C = \ell \cap OY$, respectivamente. Sea $P = (x, y)$ un punto de ℓ que satisface la ecuación $x \cdot m \circ c = y$ donde $(\cdot,\circ)$ es una operación ternaria. (Ver Figura 2.1.5).

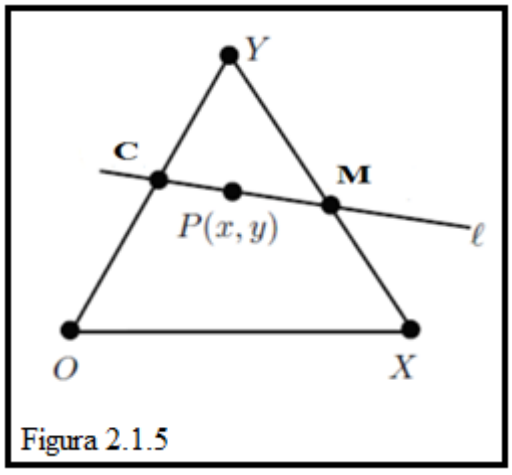


Figura 2.1.5

Definición 2.1.9. Anillo ternario

Sea R un anillo con dos elementos distintos 0 y 1, y con una operación ternaria $(\cdot,\circ)$ en R. Denotamos un anillo ternario si:

1. $\boldsymbol{a}\cdot 0\circ b = 0\cdot \boldsymbol{a}\circ b = b$, para cualquier $\boldsymbol{a}, b$ de R.

2. $1\cdot \boldsymbol{a}\circ 0 = \boldsymbol{a}\cdot 1\circ 0 = \boldsymbol{a}$, para cualquier $\boldsymbol{a}$ de R.

3. Dados $\boldsymbol{a}, b, c, d$ de R con $\boldsymbol{a}\neq c$, la ecuación $x\cdot \boldsymbol{a}\circ b = x\cdot c\circ d$ tiene una solución única para x de R.

4. Dados $\boldsymbol{a}, b, c$ de R la ecuación $\boldsymbol{a}\cdot b\circ x = c$ tiene una solución única para x de R.

5. Dados $\boldsymbol{a}, b, c, d$ de R, con $\boldsymbol{a}\neq c$, el sistema de ecuaciones

$$\begin{cases} \boldsymbol{a}\cdot x\circ y = b \\ c\cdot x\circ y = d \end{cases}$$

tiene una solución única para (x, y) de R.

2.1.1. INTRODUCCIÓN DE COORDENADAS

Sea π un plano proyectivo cualquiera y escojamos cuatro puntos X, Y, O, I tales que ninguno de tres de ellos se halle sobre una misma recta.

Llamaremos a XY la **recta del infinito L_∞.** Llamaremos a la recta OI, la recta $y = x$.

Sobre la recta OI demos coordenadas $(0,0)$ a O, $(1,1)$ a I y la sola coordenada (1) al punto C que es la intersección de OI y XY. Para otros puntos de OI asignamos coordenadas (b,b) tomando diferentes símbolos b para diferentes puntos. Para un punto P que no está sobre L_∞ sea (b,b) la intersección de XP con OI, y (a,a) la intersección de YP con OI. Asignemos entonces las coordenadas (a,b) a P. Esta regla reasigna las mismas coordenadas a los puntos de OI. Sea M el punto de intersección de la recta L_∞ con la que une los puntos $(0,0)$ y $(1,m)$. Asignemos a M la **coordenada simple** $(\boldsymbol{m})$ que podemos considerar intuitivamente como una pendiente. Tenemos ahora asignadas coordenadas a todos los puntos excepto Y, y a este le asignamos arbitrariamente una coordenada simple (∞).

Usaremos las rectas de nuestro plano para definir operaciones algebraicas sobre el sistema de coordenadas. Este sistema de coordenadas algebraico será un **anillo ternario**, y toda recta π excepto L_∞, tendrá una ecuación expresable en términos de las operaciones del anillo ternario. Si (x,y) es un punto finito de OI, tendremos $y = x$, y por tanto, tomamos $y = x$ como la ecuación para OI.

Una recta que pasa por Y distintas de L_∞ tendrá la propiedad de que todos sus puntos finitos (x, y) tienen la misma coordenadas x, digamos $x = c$, y esta igualdad es lo que tomaremos como su ecuación.

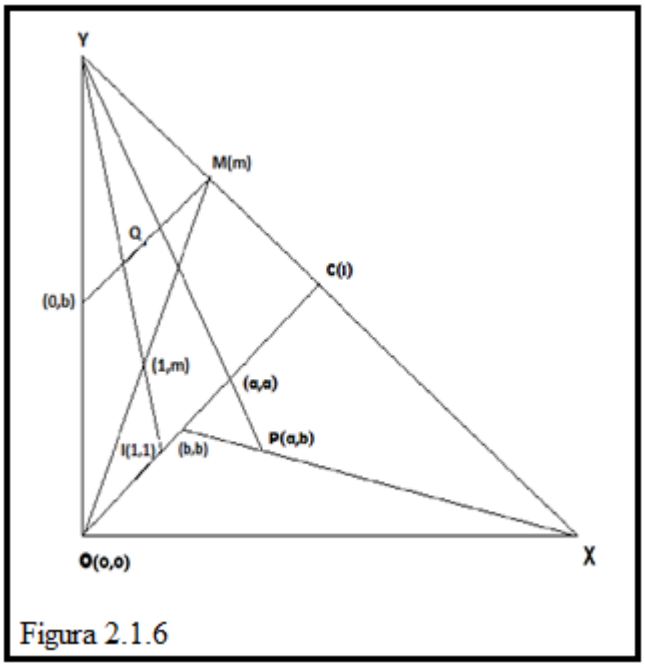


Figura 2.1.6

Si (x, y) es un punto finito de la recta que une $C = (1)$ y $(0, b)$ definimos una operación binaria de adición poniendo

$y = x + b$,

y tomamos esto como la ecuación de la recta. Si (x, y) es un punto finito de la recta que une $O = (0, 0)$ y (m), definimos una operación binaria de multiplicación, poniendo

$y = xm$,

y tomando esto como ecuación de la recta. En general, cualquier recta que no pase por Y intersectara L_∞ en algún punto (m) y OY en algún punto $(0, b)$. Si $Q = (x, y)$ es un punto de esta recta, definimos una operación ternaria

$y = x \cdot m \cdot b,$

y tomamos esto como la ecuación de la recta. Así pues, tanto la adición como la multiplicación son casos especiales de la operación ternaria, y vemos que

$$x + b = x \cdot 1 \circ b$$

$$xm = x \cdot m \circ 0$$

Los elementos 0 y 1 tienen propiedades familiares

$$0 + a = a + 0 = a$$

$$0m = m0 = 0$$

$$1m = m1 = m.$$

Definición 2.1.1.1. $C - L$ Transitivo

Un plano se dice que es $C - L$ transitivo si, para todas las líneas $L' \neq L$, a travez de C, el grupo de $C - L$ colineaciones actúa transitivamente en los puntos de L'.

Teorema 2.1.1.1. Si para dos diferentes centros C_1 y C_2 sobre un eje L los grupos de elaciones $G(C_1, L)$ y $G(C_2, L)$ son diferentes de la identidad, entonces el grupo total de traslaciones $G(L)$ es abeliano.

Además todo elemento diferente de 1 de $G(1)$ es:

1. de orden infinito.
2. del mismo orden primo p.

Prueba:

Supongamos $\alpha_1 \neq 1 \in G(C_1, L)$ y $\alpha_2 \neq 1 \in G(C_2, L)$. Sea P un punto cualquiera no sobre L. Tenemos entonces las siguientes rectas:

$$L_1 : C_1, P, P\alpha_1, \qquad L_2 : C_2, P, P\alpha_2.$$

$$L_1\alpha_2 : C_1, P\alpha_2, P(\alpha_1\alpha_2), \qquad L_2\alpha_1 : C_2, P\alpha_1, P(\alpha_2\alpha_1),$$

Pero $C_2, P\alpha_1$ y $(P\alpha_1)\alpha_2 = P(\alpha_1\alpha_2)$ están sobre una recta, y $C_1, P\alpha_2$ y $(P\alpha_2)\alpha_1 = P(\alpha_2\alpha_1)$ están sobre una recta. De aquí que la intersección de las rectas distintas $C_2P\alpha_1$ y $C_1P\alpha_2$ es $P(\alpha_1\alpha_2)$ y también $P(\alpha_2\alpha_1)$.

De aquí que $P(\alpha_1\alpha_2) = P(\alpha_2\alpha_1)$ para todo $P \notin L$. Luego $\alpha_1\alpha_2 = \alpha_2\alpha_1$. De aquí que un elemento $\alpha_1 \in G(C_1, L)$ permuta con todo elemento α_2 de cualquier $G(C_2, L)$ con $C_2 \neq C_1$. Supongamos que $\beta_1 \neq 1$ es otro elemento de $G(C_1, L)$. Entonces $\beta_1\alpha_2$ es una elación con centro C_3 no igual ni a C_1 ni a C_2.

Luego α_1 permuta con $\beta_1\alpha_2$, y como α_1 permuta con α_2, α_1 permuta también con β_1. De aquí que un $\alpha_1 \neq 1 \in G(C_1, L)$ permuta con todo elemento de $G(L)$, y por tanto $G(L)$ es abeliano. Existen ejemplos mostrando que $G(C_1, L)$ no es necesariamente abeliano si cualquier otro $G(C_i, L) = 1$ con $C_i \in L$.

Si todo elemento de $G(L)$ es de orden infinito, entonces (1) se verifica.

Si $G(L)$ contiene elementos de orden finito, entonces hay un elemento de orden primo, digamos, $\alpha_1 \in G(C_1, L)$, ${\alpha_1}^p = 1$. Ahora con $\alpha_2 \neq 1 \in G(C_2, L)$ $C_2 \neq C_1$, tenemos $\alpha_1\alpha_2 = \alpha_3 \in G(C_3, L)$, $C_3 \neq C_1, C_2$. Aquí $(\alpha_1\alpha_2)^p = {\alpha_2}^p = {\alpha_3}^p$ es un elemento común a $G(C_2, L)$ y $G(C_3, L)$, de donde es la identidad. Así pues, ${\alpha_2}^p = 1$. Análogamente, de ${\alpha_2}^p = 1$ se sigue que ${\beta_1}^p = 1$, para todo $\beta_1 \in G(C_1, L)$.

De aquí que todos los elementos de $G(L)$, excepto la identidad, son de orden p.

Teorema 2.1.1.2. Si un plano π es $C_1 - L$ transitivo y $C_2 - L$ transitivo para dos centros $C_1 \neq C_2$ sobre L, entonces π es $C - L$ transitivo para todo $C \in L$.

Prueba:

Tomemos una recta $M \neq L$ que pase por $C \neq C_1, C_2$ y sean P y Q cualesquiera dos puntos de M diferentes de C. Sea S la intersección de PC_1 y QC_2. Sean $\alpha_1 \in G(C_1, L)$ tal que $P\alpha_1 = S$ y $\alpha_2 \in G(C_2, L)$ tal que $S\alpha_2 = Q$.

Por la transitividad $C_1 - L$ y la $C_2 - L$ existen α_1 y α_2. Aquí $\alpha_1\alpha_2 = \alpha_3$ es una elación con eje L, y P, $P\alpha_3 = Q$ y C están sobre una recta. De aquí que $\alpha_3 \in G(C, L)$ y π es $C - L$ transitivo.

Definición 2.1.1.2. Plano de Traslación

Un plano proyectivo es un plano de traslación con respecto a la línea L esto es si $C - L$ transitivo para cada $C \in L$.

Teorema 2.1.1.3. Un plano es $Y - L_\infty$ transitivo si y solo si en el anillo ternario coordinizante R correspondiente tenemos:

1. $\boldsymbol{a} \cdot m \circ b = \boldsymbol{a}m + b$.
2. La adición es un grupo.

Prueba:

Supongamos que π es $Y - L_\infty$ transitivo. Tomemos en la Figura 2.1.7 YQV como $x = 0$, $V = (0, 0)$, $Q = (0, b)$, $X = (0)$, $T = (1)$, $M = (m)$.

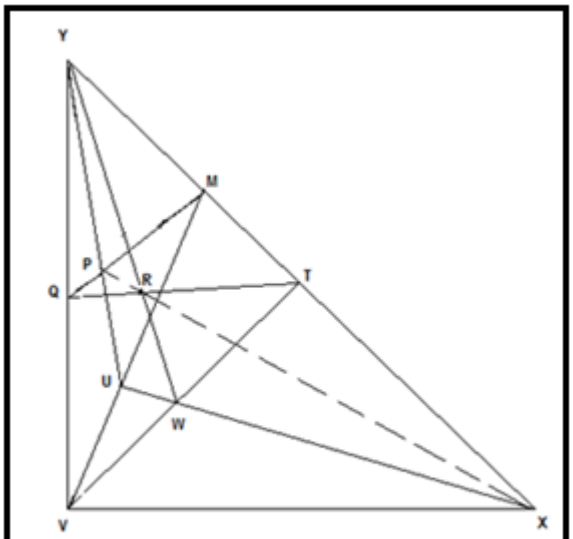


Figura 2.1.7

Aquí MQ es $y = x \cdot m \circ b$. Tomemos P sobre MQ como $P = (a, a \cdot m \circ b)$. Tracemos VM que es $y = xm$, TQ que es $y = x + b$, y YP que es $x = a$.

Entonces U, la intersección de YP y VM es $U = (a, am)$. Tracemos entonces UX que es $y = \boldsymbol{a}m$. UX intercepta VT que es $y = x$ en $W = (\boldsymbol{a}m, \boldsymbol{a}m)$. Entonces, YM que es $x = \boldsymbol{a}m$ intercepta QT que es $y = x + b$, en $R = (\boldsymbol{a}m, \boldsymbol{a}m + b)$. Ahora, si es cierto que PRX se encuentra sobre una recta, como RX es $y = \boldsymbol{a}m + b$, tendremos de $P = (\boldsymbol{a}, \boldsymbol{a} \cdot m \circ b)$, $\boldsymbol{a} \cdot m \circ b = \boldsymbol{a}m + b$. De aquí que hayamos de mostrar que PRX se encuentra sobre una recta. Por hipótesis π es $Y - L_\infty$ transitivo. Sea β la $Y - L_\infty$ colineación que fija todos los puntos de L_∞, todas las rectas que pasan por Y y sobre $x = 0$ a través de Y tal que $V\beta = Q$ o $(0,0)\beta = (0, b)$. Entonces β fija las rectas YPU, $(x = \boldsymbol{a})$, YRW, $(x = \boldsymbol{a}m)$. Además, $(VM)\beta = QM$, $(VT)\beta = QT$. De aquí que $U\beta = P$, $W\beta = R$, y desde luego, $X\beta = X$.

Pero UWX estaban sobre la recta $y = \boldsymbol{a}m$. De aquí que $U\beta, W\beta, X\beta, o\ PRX$ están sobre la recta $y = \boldsymbol{a}m + b$. De donde P es $(\boldsymbol{a}, \boldsymbol{a}m + b)$ y $\boldsymbol{a} \cdot m \circ b = \boldsymbol{a}m + b$, la primera parte de nuestro teorema.

¿Cuál es el efecto de la colineación β determinada por $(0,0)\beta = (0, b)$ sobre un punto general $(\boldsymbol{a}, c)$? Fácilmente encontramos esto en unos cuantos pasos. Pues

$$y = x \rightarrow y = x + b,$$

$$x = c \rightarrow x = c,$$

$$(c, c) \rightarrow (c, c + b),$$

$$y = c \rightarrow y = c + b,$$

$$x = \boldsymbol{a} \rightarrow x = \boldsymbol{a},$$

$$(a, c) \rightarrow (a, c + b).$$

De aquí que si $(0,0)\beta = (0, b)$, entonces

$$(\boldsymbol{a}, c)\beta = (\boldsymbol{a}, c + b).$$

Ahora, si δ es la $Y - L_\infty$ colineación determinada por

$$(0,0)\delta = (0, d),$$

encontramos en general que $(u, v)\delta = (u, v + d)$.

Para la $\beta\delta$ encontramos

$$(0,0)(\beta\delta) = [(0,0)\beta]\delta = (0,b)\delta = (0,b+d).$$

De aquí que $(\boldsymbol{a},c)(\beta\delta) = [\boldsymbol{a},c+(b+d)]$.

Pero $[(\boldsymbol{a},c)\beta]\delta = (\boldsymbol{a},c+b)\delta = [\boldsymbol{a},(c+b)+d]$. De aquí que la adición satisface la ley asociativa $c+(b+d) = (c+b)+d$.

Como la adición en un plano siempre tiene un cero y es un lazo, se sigue de ello que la adición será un grupo. De donde hemos probado (2).

Recíprocamente, supongamos que un anillo ternario R de π satisface:

1. $\boldsymbol{a}\cdot m \circ b = \boldsymbol{a}m + b$.
2. La adición es un grupo.

Para cualquier $b \in R$ definamos un mapeo $\beta = \beta(b)$ para puntos:

$$(\infty) \to (\infty),$$

$$(m) \to (m),$$

$$(\boldsymbol{a},c) \to (\boldsymbol{a},c+b).$$

Para rectas:

$$L_\infty \to L_\infty,$$

$$x = \boldsymbol{a} \to x = \boldsymbol{a},$$

$$y = xm + t \rightarrow y = xm + (t + b).$$

Esto es una colineación, ya que si $(\boldsymbol{a}, c)$ esta sobre $y = xm + t$, entonces $c = \boldsymbol{a}m + t$, de donde

$$c + b = (\boldsymbol{a}m + t) + b = \boldsymbol{a}m + (t + b)$$

y por tanto $(\boldsymbol{a}, c + b)$ esta sobre $y = xm + (t + b)$, y el resto de las comprobaciones necesarias para mostrar que β es una colineación es inmediato. Pero esta es una $Y - L_\infty$ colineación que lleva $(0, 0)$ en $(0, b)$. Pero como b era arbitrario, π es $Y - L_\infty$ transitiva.

Teorema 2.1.1.4. Un plano π es un plano de traslación con respecto al eje L_α si y solo si el anillo ternario correspondiente es un sistema Veblen-Wedderburn, lo que quiere decir:

1. La adición es un grupo abeliano.
2. La multiplicación (excluyendo 0) es un lazo.
3. $(\boldsymbol{a} + b)m = am + bm.$
4. Si $r \neq s, xr = xs + t$ tiene una solución única x.
5. $\boldsymbol{a} \cdot m \circ b = \boldsymbol{a}m + b.$

Prueba:

Por el teorema 2.1.1.2 π será un plano de traslación con eje L_α si es $Y - L_\alpha$ transitivo y además $X - L_\alpha$ transitivo. Por el teorema 2.1.1.3, sabemos (5), $\boldsymbol{a} \cdot m \circ b = \boldsymbol{a}m + b$ y que la adición es un grupo. En la prueba del teorema 2.1.1.3 mostramos la existencia de

una elación $\beta(b)$ para cada $b \in R$ que mapea un $(\boldsymbol{a}, c)$ arbitrario en $(\boldsymbol{a}, c + b)$. Por el teorema 2.1.1.1 el grupo de traslación en su totalidad es abeliano, de donde

$$\beta(b)\beta(d) = \beta(d)\beta(b),$$

Y por tanto, $(\boldsymbol{a}, c + b + d) = (\boldsymbol{a}, c + d + b)$, de donde $b + d = d + b$, y la adición en R es abeliana, probando (1).

Sea b un elemento arbitrario de R y consideremos la elación con centro X que lleva $(0,0)$ en $(b, 0)$. Tenemos, sucesivamente,

$$(0,0) \to (b, c),$$

$$y = x \to y = x - b,$$

$$y = \boldsymbol{a} \to y = \boldsymbol{a},$$

$$(\boldsymbol{a}, \boldsymbol{a}) \to (\boldsymbol{a} + b, \boldsymbol{a}),$$

$$x = \boldsymbol{a} \to x = \boldsymbol{a} + b,$$

$$y = \boldsymbol{a}m \to y = \boldsymbol{a}m,$$

$$(\boldsymbol{a}, \boldsymbol{a}m) \to (\boldsymbol{a} + b, \boldsymbol{a}m).$$

Además, como $(0,0) \to (b, c)$,

$$y = xm \to y = xm - bm.$$

Pero entonces, como $(\boldsymbol{a}, \boldsymbol{a}m)$ esta sobre $y = xm$, tenemos $(\boldsymbol{a} + b, am)$ sobre

$y = xm - bm$, de donde

$$\boldsymbol{a}m = (\boldsymbol{a} + b)m - bm,$$

y por tanto, $\boldsymbol{a}m + bm = (\boldsymbol{a} + b)m$. Esto prueba la ley distributiva (3).

En un plano la multiplicación es siempre un lazo, y la condición (4) dice que si $r \neq s$, las rectas $y = xr$ y $y = xs + t$ se intersectan en un punto finito único.

Un sistema de elementos con operaciones binarias de adición y multiplicación que satisfacen las condiciones $(1), (2), (3), (4)$ se llama un sistema de Veblen-Wedderburn.

Mostraremos ahora que, recíprocamente, todo sistema de Veblen-Wedderburn R puede usarse como el sistema de coordenadas de un plano de traslación con eje L_α. Tomamos como nuestros puntos:

1. Los puntos finitos $(\boldsymbol{a}, b)$ con $\boldsymbol{a}, b$ elementos arbitrarios de R.
2. Los puntos infinitos (m) con $m \in R$.
3. El punto $Y = (\infty)$.

Nuestras rectas serán:

1. L_α con puntos (∞) y (m).
2. Rectas $x = c$ conteniendo a (∞) y todos los puntos (c, d).
3. Rectas $y = xm + b$ conteniendo los puntos (m) y $(\boldsymbol{a}, \boldsymbol{a}m + b)$ para todo $\boldsymbol{a} \in R$.

Es sencillo ahora verificar que hay una sola recta que une dos puntos distintos, un punto único que se encuentra en dos rectas distintas, y que de los cuatro puntos $(0,0),(1,1),(\infty)$ y (0) no hay tres que se encuentren en una misma recta. Esta verificación implica varios casos y necesitamos la condición (4) para mostrar que las rectas $y = xr + b$ y $y = xs + c$ con $r \neq s$ se intersectan en un punto único que es finito.

Para un plano de Veblen-Wedderburn se verifica fácilmente que el mapeo de puntos finitos $(x,y) \rightarrow (x + r, y + s)$ es una colineación para cualesquiera r y s, que fija todos los puntos de L_∞ y para rectas finitas mapea

$x = c \rightarrow x = r + c,\ y = xm + b \rightarrow y = xm - rm + s + b$. Si $s = rt$ esta colineación es una elación con eje L_∞ y centro (t). De aquí que un plano de Veblen-Wedderburn es un plano de traslación con eje L_∞.

Teorema 2.1.1.5. Si π es un plano de traslación con respecto a tres rectas que no tienen un punto en común, entonces es un plano de traslación para toda recta.

Prueba:

Para el Teorema, notemos que una familia de rectas que con dos rectas contienen el haz de recta que pasan por su intersección, es necesariamente la familia de todas las rectas del plano si contienen tres rectas que no pasan por un mismo punto.

Supongamos que L_1 y L_2 son dos rectas que se intersectan en un punto Y y que π es un plano de traslación con respecto a ambas L_1 y L_2. Sea L_3 una tercera recta que pasa por Y y sea C cualquier punto de L_3 distinto de Y. Sea RCS una recta cualquiera que pasa por C diferente de L_3 que intersecta L_1 en R y a L_2 en S. Entonces hay una elación α con eje L_1 y centro R que lleva S en C y L_2 en L_3. Como π tiene todas las elaciones con eje L_2 y centro S, entonces la configuración del Teorema de linealidad es válida para todos los casos con S como centro y L_2 como eje. La colineación α lleva a todas estas configuraciones en todas las configuraciones del Teorema de linealidad con centro C y eje L_3. Por tanto en π existen todas las elaciones posibles con centro C y eje L_3. Como este argumento es válido para todo punto de L_3 diferente de Y, entonces por teorema 2.1.1.2, π es un plano de traslación con eje L_3.

Teorema 2.1.1.6. U n plano π es un plano de traslación para toda recta que pasa por el punto $y = (\infty)$ si y solo si,

1) sus rectas finitas están dadas por ecuaciones lineales $x = c$ y $y = xm + b$,

2) las coordenadas satisfacen las siguientes leyes:

2.1) La adición es un grupo abeliano.

2.2) $(\boldsymbol{a} + b)m = (\boldsymbol{a}m + bm)$

2.3) $\boldsymbol{a}(s + t) = \boldsymbol{a}s + \boldsymbol{a}t$

2.4) Todo $\boldsymbol{a} \neq 0$ tiene un inverso $\boldsymbol{a}^{-1}$ que satisface $\boldsymbol{a}^{-1}\boldsymbol{a} = \boldsymbol{a}\boldsymbol{a}^{-1} = 1$

2.5) $\boldsymbol{a}^{-1}(\boldsymbol{a}b) = b$

Prueba:

Supongamos que π es un plano de traslación para toda recta que pase por $y = (\infty)$. Esto incluye L_∞, y también por el teorema 2.1.1.4 sabemos que las condiciones de linealidad (1) se satisfacen y que las coordenadas son un sistema de Veblen-Wedderburn. Esto nos da las condiciones (2.1) y (2.2) del teorema. Hemos de probar las restante tres condiciones.

Consideremos la elación con $Y = (\infty)$ como centro, $x = 0$ como eje, que mapea el punto (0) sobre el punto (m).

Aquí todos los puntos $(0, b)$ son fijos y las rectas L_∞ y $x = c$ son fijas.

Encontramos, sucesivamente

$$(0) \rightarrow (m)$$

$$(0, b) \rightarrow (0, b)$$

$$y = b \rightarrow y = xm + b$$

$$x = \boldsymbol{a} \rightarrow x = \boldsymbol{a}$$

$$(\boldsymbol{a}, b) \rightarrow (\boldsymbol{a}, \boldsymbol{a}m + b)$$

Esto nos da el mapeo para un punto finito arbitrario.

En particular

$$(1, t) \rightarrow (1, m + t)$$

$$(0,0) \rightarrow (0,0)$$

de donde

$$y = xt \rightarrow y = (m + t).$$

Pero

$$(\boldsymbol{a}, \boldsymbol{a}t) \rightarrow (\boldsymbol{a}, \boldsymbol{a}m + t)$$

y como $(\boldsymbol{a}, \boldsymbol{a}t)$ esta sobre $y = xt$, tenemos $(\boldsymbol{a}, \boldsymbol{a}m + t)$ sobre $y = x(m + t)$ de donde

$$\boldsymbol{a}m + t = \boldsymbol{a}(m + t)$$

la ley distributiva (2.3)

Consideremos ahora la elación con centro (0, 0) y eje $x = 0$ que lleva (0) a $(-1 - \boldsymbol{a}, 0)$.

Aquí

$$(0) \rightarrow (-1, -\boldsymbol{a}, 0)$$

$$(0,1 + \boldsymbol{a}) \rightarrow (0,1 + \boldsymbol{a})$$

de donde $y = 1 + \boldsymbol{a} \rightarrow y = x + 1 + \boldsymbol{a}$

$$(0) \rightarrow (-1, -\boldsymbol{a}, 0)$$

$$(0, b + \boldsymbol{a}b) \rightarrow (0, b + \boldsymbol{a}b)$$

de donde $y = b + \boldsymbol{a}b \rightarrow y = xb + b + \boldsymbol{a}$

$$y = 1 + \boldsymbol{a} \rightarrow y = x + 1 + \boldsymbol{a}$$

$$y = x(1 + \boldsymbol{a}) \rightarrow y = x(1 + \boldsymbol{a}),$$

de donde

$(1, 1 + \boldsymbol{a}) \rightarrow (d, d + 1 + \boldsymbol{a})$ si $\boldsymbol{a} \neq 0$

donde

$$d(1 + \boldsymbol{a}) = d + 1 + \boldsymbol{a}.$$

Además

$$(\infty) \rightarrow (\infty),$$

$$(1, 1 + \boldsymbol{a}) \rightarrow (d, d + 1 + \boldsymbol{a}),$$

de donde $x = 1 \rightarrow x = d$.

Ahora

$$y = x(b + \boldsymbol{a}b) \rightarrow y = x(b + \boldsymbol{a})b,$$

$$y = b + \boldsymbol{a}b \rightarrow y = xb + b + \boldsymbol{a}b,$$

y por tanto $(1, b + \boldsymbol{a}b) \rightarrow (d, d[b + \boldsymbol{a}b])$,

donde también $d(b + \boldsymbol{a}b) = db + b + \boldsymbol{a}b$.

Aquí suponemos no solamente $\boldsymbol{a} \neq 0$, si no también $(-1 - \boldsymbol{a}, 0) \neq (0,0)$, es decir, $\boldsymbol{a} \neq -1$. Para tal $\boldsymbol{a}$ existe un d tal que $d(1 + \boldsymbol{a}) = d + 1 + \boldsymbol{a}$, y para toda b, $d(b + \boldsymbol{a}b) = db + b + \boldsymbol{a}b$. Si ponemos $d = u + 1$ y usamos las leyes distributivas, encontramos

$u\boldsymbol{a} = 1,$

$u(\boldsymbol{a}b) = b.$

Por las leyes distributivas encontramos directamente que incluso para $\boldsymbol{a} = -1$, estas relaciones se verifican para $u = -1$. Como para $u \neq 0$ hay un v con

$vu = 1,$

$v(u\boldsymbol{a}) = \boldsymbol{a},$

tenemos $v = \boldsymbol{a}$. De aquí escribimos $u = \boldsymbol{a}^{-1}$ y tenemos las leyes (2.4)

$\boldsymbol{a}\boldsymbol{a}^{-1} = \boldsymbol{a}^{-1}\boldsymbol{a} = 1,$ y (2.5) $\boldsymbol{a}^{-1}(\boldsymbol{a}b) = b.$

Recíprocamente, supongamos que las condiciones (1) y (2) se verifican para las coordenadas de un plano π. Por el Teorema 2.1.1.4 sabemos que π es un plano de traslación con respecto a L_∞. Usando el Teorema 2.1.1.5 será suficiente mostrar que π tiene una colineación que mapea L_∞ sobre alguna otra recta que pase por $Y = (\infty)$.

El siguiente mapeo es dicha colineación:

$(\infty) \to (\infty)$,

$(m) \to (1, m)$,

$(-1, m) \to (-m)$,

$(0, b) \to (0, b)$,

$(c, d) \to [(1 + c^{-1})^{-1} d], c \neq 0, -1.$

$(L_\infty) \to x = 1$,

$x = -1 \to L_\infty$,

$x = 0 \to x = 0$,

$x = c \to x = (1 + c^{-1})^{-1}, c \neq 0, -1.$

$y = xm + b \to y = x(m - b) + b.$

Para demostrar esto debemos probar que las incidencias se preservan por el mapeo; en particular que si (c, d) esta sobre $y = xm + b$, entonces el punto imagen esta sobre la recta imagen. Se reduce esto a mostrar que

$$(1 + c^{-1})(cm + b) = (1 + c^{-1})^{-1}(m - b) + b$$

es una identidad. Se sigue esto de las leyes del Teorema, ya que las dos siguientes son identidades:

$$(1+c)^{-1}(cm) = (1+c^{-1})^{-1}m,$$

$$(1+c)^{-1}b = (1+c^{-1})^{-1}(-b) + b.$$

Probaremos una identidad más basada en las leyes arriba enunciadas.

Escribamos:

$$[y^{-1} - (y+z^{-1})^{-1}][y(zy)+y] = t,$$

donde excluimos solamente los valores $y = 0$, $y = -z^{-1}$. Entonces, multiplicando por $y + z^{-1}$ tenemos

$$(y+z^{-1})t = (y+z^{-1})\big[zy + 1 - (y+z^{-1})^{-1}\big(y(zy)\big) - (y+z^{-1})^{-1}y\big]$$

$$= y(zy) + y + y + z^{-1} - y(zy) - y$$

$$= y + z^{-1}$$

De aquí que $t = 1$ y $y^{-1} - (y+z^{-1})^{-1}$, y $y(zy)+y$ son inversos. Luego para cualquier x,

$$[y^{-1} - (y+z^{-1})^{-1}]\big[\big(y(zy)\big)x + yx\big] = x.$$

Escribamos ahora

$$[y^{-1} - (y+z^{-1})^{-1}][y(z(yx)) + yx] = w.$$

Y encontramos

$$(y+z^{-1})w = (y+z^{-1})[z(yx)+x] - y[z(yx)] - yx$$

$$= yx + z^{-1}x = (y + z^{-1})x.$$

De aquí que $w = x$. Comparando ahora las expresiones para w y x vemos que debemos tener

$$[y(zy)]x = y[z(yx)]$$

la identidad de Moufang.

Esta identidad es claramente válida para los valores excluidos $y = 0$, $y = z^{-1}$, y por tanto se verifican sin excepción. En particular, la identidad de Moufang con $z = 1$ se reduce la ley alternativa izquierda: $(yy)x = y(yx)$

Definición 2.1.1.3. Plano de Moufang

Si un plano es un plano de traslación para toda recta, se le llama un plano de Moufang.

Teorema 2.1.1.4. Teorema de planos Moufang

Un plano es un plano de Moufang, si y solo si todo anillo ternario es

1) Lineal

2) Un anillo de división alternativo, es decir, satisface las siguientes leyes:

2.1) La adición es un grupo abeliano.

2.2) $(\boldsymbol{a}+b)m=\boldsymbol{a}m+bm$

2.3) $\boldsymbol{a}(s+t)=\boldsymbol{a}s+\boldsymbol{a}t$

2.4) Todo $\boldsymbol{a}\neq 0$ tiene un inverso $\boldsymbol{a}^{-1}$ que satisface $\boldsymbol{a}^{-1}\boldsymbol{a}=\boldsymbol{a}\boldsymbol{a}^{-1}=1$

2.5) $\boldsymbol{a}^{-1}(\boldsymbol{a}b)=b.$

2.6) $(b\boldsymbol{a})\boldsymbol{a}^{-1}=b.$

Además las leyes alternativas son válidas:

2.7) $\boldsymbol{a}(\boldsymbol{a}b)=(\boldsymbol{a}\boldsymbol{a})b,\qquad (b\boldsymbol{a})\boldsymbol{a}=b(\boldsymbol{a}\boldsymbol{a}).$

Prueba:

Por el teorema 2.1.1.6 tenemos 1) y también 2.1), 2.2), 2.3), 2.4), 2.5) debemos probar 2.6) ya que claramente la ley alternativa derecha $(b\boldsymbol{a})\boldsymbol{a}=b(\boldsymbol{a}\boldsymbol{a})$ se sigue de 2.6) exactamente en la misma forma que la ley alternativa izquierda se sigue 2.5).

Consideramos la elación con eje $y=0$ y centro (0, 0) tal que $Y=(\infty)$ se mapea sobre $(0,-1)$. Tenemos, sucesivamente:

$$(\infty)\rightarrow(0,-1).$$

$$(1,0)\ \rightarrow(1,0).$$

de donde $x=I\rightarrow y=x-1$

$$(\infty)\rightarrow(0,-1).$$

$$(\boldsymbol{a},0)\ \rightarrow(\boldsymbol{a},0)$$

de donde

$$x = \boldsymbol{a} \rightarrow y = x\boldsymbol{a}^{-1} - 1$$

$$x = 1 \rightarrow y = x - 1$$

$$y = x(1 - \boldsymbol{a}b) \rightarrow y = x(1 - \boldsymbol{a}b)$$

Por tanto

$$(1, 1 - \boldsymbol{a}b) \rightarrow [(\boldsymbol{a}b)^{-1}, (\boldsymbol{a}b)^{-1} - 1]$$

Además

$$(0) \rightarrow (0),$$

de donde

$$y = 1 - \boldsymbol{a}b \rightarrow y = (\boldsymbol{a}b)^{-1} - 1$$

$$x = \boldsymbol{a} \rightarrow y = x\boldsymbol{a}^{-1} - 1$$

$$y = x(\boldsymbol{a}^{-1} - b) \rightarrow x(\boldsymbol{a}^{-1} - b)$$

de donde

$$(\boldsymbol{a}, 1 - \boldsymbol{a}b) \rightarrow (b^{-1}, b^{-1}\boldsymbol{a}^{-1} - 1)$$

Como

$$(0) \rightarrow (0)$$

tenemos

$$y = 1 - \boldsymbol{a}b \;\rightarrow y = b^{-1}\boldsymbol{a}^{-1} - 1$$

Comparando imágenes de $y = 1 - \boldsymbol{a}b$ debemos tener

$$(\boldsymbol{a}b)^{-1} = b^{-1}\boldsymbol{a}^{-1}.$$

Usando esto como una ley, encontramos, como $b^{-1} = \boldsymbol{a}(\boldsymbol{a}^{-1}b^{-1})$

$$b = (b^{-1})^{-1} = [\boldsymbol{a}(\boldsymbol{a}^{-1}b^{-1})]^{-1}$$

$$= (\boldsymbol{a}^{-1}b^{-1})^{-1}\boldsymbol{a}^{-1}$$

$$= (b\boldsymbol{a})\,\boldsymbol{a}^{-1}$$

Esto prueba 2.6).

Hemos demostrado que en un plano de Moufang las coordenadas satisfacen las leyes enumeradas anteriormente para un anillo de división alternativo. Recíprocamente, supongamos que tenemos un anillo de división alternativo. Si construimos un plano con estas coordenadas, por el teorema 2.1.1.6 el plano es un plano de traslación para toda recta que pase por $Y = (\infty)$ .De aquí que, por el teorema 2.1.1.5 se seguirá que el plano es un plano de traslación para toda recta si podemos encontrar una colineación que cambie $Y = (\infty)$. La siguiente reflexión es válida:

$$(\boldsymbol{a}, b) \leftrightarrows (b, \boldsymbol{a})$$

$$(0) \leftrightarrows (\infty)$$

$$(m) \leftrightarrows (m^{-1}), \quad m \neq 0$$

$$x = c \leftrightarrows y = c,$$

$$y = xm + b \leftrightarrows xm^{-1} - bm^{-1}, \quad m \neq 0$$

Esto completa la prueba del teorema.

Nota. La teoría de anillos de división alternativos se abordará en el siguiente capítulo.

2.2. ANILLOS ALTERNATIVOS

En este apartado hablaremos de una estructura algebraica, llamada anillo alternativo similar a la estructura de anillo a diferencia que esta nueva estructura cumple con otras propiedades.

Previamente necesitamos mencionar la definición de **función antisimétrica**: Una función $h(x_1, \dots, x_n)$ en un anillo se dice que es antisimetrica si

1. Es lineal en cada uno de sus argumentos.
2. Se anula siempre que cualquiera dos de sus argumentos son iguales.

Definición 2.2.1. Anillo de división alternativo

Un anillo alternativo $\boldsymbol{R}$ en un sistema con una adición binaria y una multiplicación en el que se satisfacen las siguientes leyes:

1. La adición es un grupo abeliano.
2. $(x + y)m = xm + ym.$
3. $x(s + t) = xs + xt.$
4. Todo $x \neq 0$ tiene un inverso x^{-1} que satisface $x^{-1}x = xx^{-1} = 1.$
5. $x^{-1}(xy) = y.$
6. $(yx)x^{-1} = y.$

7. La multiplicación satisface las dos leyes asociativas débiles,

$$(xx)y = x(xy), \quad y(xx) = (yx)x. \qquad (\mathbf{2.2.1})$$

En un plano de Moufang teníamos las leyes multiplicativas:

$$\boldsymbol{a}\boldsymbol{a}^{-1} = \boldsymbol{a}^{-1}\boldsymbol{a} = 1, \quad \boldsymbol{a}^{-1}(\boldsymbol{a}b) = b = (b\boldsymbol{a})\boldsymbol{a}^{-1} \qquad (\mathbf{2.2.2})$$

Y en anillos alternativos tenemos las leyes multiplicativas

$$(xx)y = x(xy), \quad y(xx) = (yx)x.$$

Definiremos dos cantidades para todo anillo en el que las leyes distributivas se verifiquen, el asociador (x, y, z) y el conmutador (x, y). Las definimos por las siguientes reglas:

$$(x, y, z) = (xy)z - x(yz), \qquad (x, y) = xy - yx \qquad (\mathbf{2.2.3})$$

El asociador $(x, y, z) = (xy)z - x(yz)$ mide la distancia en que x, y, z se están asociando, ya que eso es solo la diferencia entre las dos formas $(xy)z$ y $x(yz)$ de asociar x, y, z en el orden dado.

De la misma forma, el conmutador $(x, y) = xy - yx$ mide la distancia en que x y y se están conmutando.

El asociador se desvanece, es decir, se hace cero cuando $(xy)z = x(yz)$, en cualquier anillo asociativo y el conmutador se desvanece, se hace cero cuando $xy = yx$, en cualquier anillo conmutativo.

La antisimetría implica la propiedad alternante y el asociador y el conmutador son simétricos en un anillo alternativo.

Tanto el asociador como el conmutador son lineales en cada argumento.

Las leyes $(xx)y = x(xy), \quad y(xx) = (yx)x$ pueden reescribirse de la siguiente forma:

$(xx)y = x(xy)$

$(xx)y - x(xy) = 0$

$(x, x, y) = 0$; por definición de asociador.

Y la segunda se reescribe así:

$y(xx) = (yx)x$

$(yx)x - y(xx) = 0$

$(y, x, x) = 0$; por definición de asociador.

Por tanto,

$(x, x, y) = 0, \qquad (y, x, x) = 0$ $\qquad (\mathbf{2.2.4})$

Estas leyes son llamadas: **ley alternativa izquierda** y **ley alternativa derecha**, respectivamente.

Por la linealidad del asociador, hacemos las siguientes combinaciones en los argumentos:

1. $(x,\ y+z,\ y+z)=0$ $(\mathbf{2.2.5})$
2. $(y+z,\ y+z,\ x)=0$
3. $(x+y,\ x+y,\ z)=0$
4. $(z,\ x+y,\ x+y)=0$
5. $(y,\ x+z,\ x+z)=0$
6. $(x+z,\ x+z,\ y)=0$

Haciendo uso de la definición de asociador, se tiene:

1. $(x,\ y+z,\ y+z)=0$

   $\big(x(y+z)\big)(y+z)-x\big((y+z)(y+z)\big)=0$

   $(xy+xz)(y+z)-[x(yy+yz+zy+zz)]=0$

   $(xy)y+(xy)z+(xz)y+(xz)z-x(yy)-x(yz)-x(zy)-x(zz)=0$

   $[(xy)y-x(yy)]+[(xy)z-x(yz)]+[(xz)y-(xz)y]+[(xz)z-x(zz)]=0$

   $(x,y,y)+(x,y,z)+(x,z,y)+(x,z,z)=0$

   $(x,y,z)+(x,z,y)=0$

   $(x,y,z)=-(x,z,y)$

2. $(y+z,\ y+z,\ x)=0$

$\big((y+z)(y+z)\big)x-(y+z)\big((y+z)x\big)=0$

$(yy+yz+zy+zz)x-(y+z)(yx+zx)=0$

$(yy)x+(yz)x+(zy)x+(zz)x-[y(yx)+y(zx)+z(yx)+z(zx)]=0$

$[(yy)x-y(yx)]+[(yz)x-y(zx)]+[(zy)x-z(yx)]+[(zz)x-z(zx)]=0$

$(y,y,x)+(y,z,x)+(z,y,x)+(z,z,x)=0$

$(y,z,x)+(z,y,x)=0$

$(y,z,x)=-(z,y,x)$

3. $(x+y,\ x+y,\ z)=0$

$\big((x+y)(x+y)\big)z-(x+y)\big((x+y)z\big)=0$

$(xx+xy+yx+yy)z-(x+y)(xz+yz)=0$

$(xx)z+(xy)z+(yx)z+(yy)z-[x(xz)+x(yz)+y(xz)+y(yz)]=0$

$[(xx)z-x(xz)]+[(xy)z-x(yz)]+[(yx)z-\ y(xz)]+[(yy)z-y(yz)]=0$

$(x,x,z)+(x,y,z)+(y,x,z)+(y,y,z)=0$

$(x,y,z)+(y,x,z)=0$

$(x,y,z)=-(y,x,z)$

4. $(z,\ x+y,\ x+y)=0$

   $(z(x+y))(x+y)-z\big((x+y)(x+y)\big)=0$

   $(zx+zy)(x+y)-z(xx+xy+yx+yy)=0$

   $[(zx)x+(zx)y+(zy)x+(zy)y]-z(xx)-z(xy)-z(yx)-z(yy)=0$

   $[(zx)x-z(xx)]+[(zx)y-z(xy)]+[(zy)x-z(yx)]+[(zy)y-z(yy)]=0$

   $(z,x,x)+(z,x,y)+(z,y,x)+(z,y,y)=0$

   $(z,x,y)+(z,y,x)=0$

   $(z,x,y)=-(z,y,x)$

5. $(y,\ x+z,\ x+z)=0$

   $(y(x+z))(x+z)-y\big((x+z)(x+z)\big)=0$

   $(yx+yz)(x+z)-y(xx+xz+zx+zz)=0$

   $[(yx)x+(yx)z+(yz)x+(yz)z]-y(xx)-y(xz)-y(zx)-y(zz)=0$

   $[(yx)x-y(xx)]+[(yx)z-y(xz)]+[(yz)x-y(zx)]+[(yz)z-y(zz)]=0$

   $(y,x,x)+(y,x,z)+(y,z,x)+(y,z,z)=0$

   $(y,x,z)+(y,z,x)=0$

   $(y,z,x)=-(y,x,z)$

6. $(x+z,\ x+z,\ y)=0$

$\big((x+z)(x+z)\big)y-(x+z)\big((x+z)y\big)=0$

$(xx+xz+zx+zz)y-(x+z)(xy+zy)=0$

$(xx)y+(xz)y+(zx)y+(zz)y-[x(xy)+x(zy)+z(xy)+z(zy)]=0$

$[(xx)y-\ x(xy)]+[(xz)y-x(zy)]+[(zx)y-z(xy)]+[(zz)y-\ z(zy)]=0$

$(x,x,y)+(x,z,y)+(z,x,y)+(z,z,y)=0$

$(x,z,y)+(z,x,y)=0$

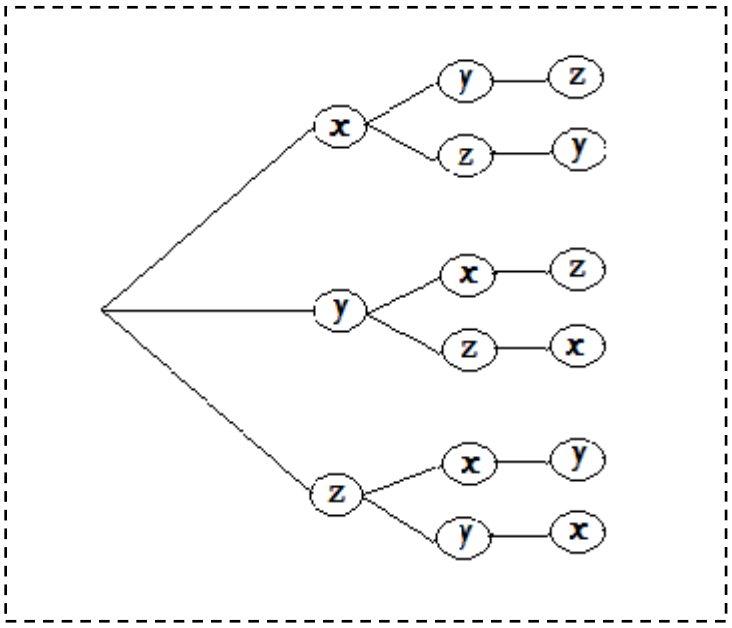
$(z,x,y)=-(x,z,y)$

De donde tenemos

$$(x,y,z)=-(x,z,y)=(z,x,y)=-(z,y,x)=(y,z,x)=-(y,x,z) \qquad (\mathbf{2.2.6})$$

Nos dice esto que (x,y,z) bajo las permutaciones del grupo simétrico sobre x,y,z no cambia por el grupo alterno y cambia de signo bajo las permutaciones impares. Es esta propiedad la que llevó a llamar ***alternativos*** a estos anillos.

Se puede obtener las permutaciones sobre x,y,z, como en teoría de grupos, y ver esta misma propiedad. Se procede como sigue:



Las permutaciones resultantes son:

$$\alpha_1 = \begin{pmatrix} x & y & z \\ x & y & z \end{pmatrix}$$

$$\alpha_2 = \begin{pmatrix} x & y & z \\ x & z & y \end{pmatrix}$$

$$\alpha_3 = \begin{pmatrix} x & y & z \\ y & x & z \end{pmatrix}$$

$$\alpha_4 = \begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix}$$

$$\alpha_5 = \begin{pmatrix} x & y & z \\ z & x & y \end{pmatrix}$$

$$\alpha_6 = \begin{pmatrix} x & y & z \\ z & y & x \end{pmatrix}$$

Y ahora encontramos el signo de cada permutación para conocer las permutaciones impares:

$$\alpha_1 = \begin{pmatrix} x\ y\ z \\ x\ y\ z \end{pmatrix} = (x)(y)(z) = (x\ \ y)(x\ \ z) \Rightarrow\ \ sig(\alpha_1) = (-1)^2 = 1$$

$$\alpha_2 = \begin{pmatrix} x\ y\ z \\ x\ z\ y \end{pmatrix} = (x)(y\ \ z) = (y\ \ z) \Rightarrow\ sig(\alpha_2) = (-1)^1 = -1$$

$$\alpha_3 = \begin{pmatrix} x\ y\ z \\ y\ x\ z \end{pmatrix} = (x\ \ y)(z) = (x\ \ y) \Rightarrow\ sig(\alpha_3) = (-1)^1 = -1$$

$$\alpha_4 = \begin{pmatrix} x\ y\ z \\ y\ z\ x \end{pmatrix} = (x\ \ y\ \ z) = (x\ \ y)(x\ \ z) \Rightarrow\ \ sig(\alpha_4) = (-1)^2 = 1$$

$$\alpha_5 = \begin{pmatrix} x\ y\ z \\ z\ x\ y \end{pmatrix} = (x\ \ z\ \ y) = (x\ \ z)(x\ \ y) \Rightarrow\ \ \ sig(\alpha_5) = (-1)^2 = 1$$

$$\alpha_6 = \begin{pmatrix} x\ y\ z \\ z\ y\ x \end{pmatrix} = (x\ \ z)(y) = (x\ \ z) \Rightarrow sig(\alpha_6) = (-1)^1 = -1$$

Entonces las permutaciones impares son:

$(x, z, y),$ $(y, x, z),$ (z, y, x)

Y son exactamente las que cambian de signo en la ecuación $(2.2.6)$.

Mediante el uso de la regla $(x, y, z) = -(x, z, y)$ se obtiene la ley reflexiva de la siguiente forma:

$(x, y, x) = -(x, x, y)$

y $(x, y, x) = -(x, x, y) = 0,$ por ecuación (2.2.4)

de donde,

$(x, y, x) = (xy)x - x(yx) = 0$ por definición del asociador

De aquí que,

$$(xy)x = x(yx) \qquad (\mathbf{2.2.7})$$

Esta ley se llama la ***ley reflexiva***.

La siguiente identidad puede verificarse que es válida en cualquier anillo con las leyes distributivas

$$(wx, y, z) - (w, xy, z) + (w, x, yz) = w(x, y, z) + (w, x, y)z \qquad (\mathbf{2.2.8})$$

Verificación

$(wx, y, z) - (w, xy, z) + (w, x, yz)$

$= \big[\big((wx)y\big)z - (wx)(yz)\big] - \big[\big(w(xy)\big)z - w\big((xy)z\big)\big] + \big[(wx)(yz) - w\big(x(yz)\big)\big]$

$= \big((wx)y\big)z - (wx)(yz) - \big(w(xy)\big)z + w\big((xy)z\big) + (wx)(yz) - w\big(x(yz)\big)$

$= w[(xy)z - x(yz)] + [(wx)y - w(xy)]z$

$= w(x, y, z) + (w, x, y)z$

Definimos la función $f(w, x, y, z)$ por la regla

$$f(w, x, y, z) = (wx, y, z) - x(w, y, z) - (x, y, z)w \qquad (\mathbf{2.2.9})$$

Lema 2.2.1. En todo anillo alternativo $\boldsymbol{R}$ la función

$f(w,x,y,z) = (wx,y,z) - x(w,y,z) - (x,y,z)w$ es antisimétrica y satisface las identidades

$$3f(w,x,y,z) = (w,(x,y,z)) - (x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y)) \quad (\mathbf{2.2.10})$$

$$f(w,x,y,z) = ((wx),y,z) + ((y,z),w,x) \quad (\mathbf{2.2.11})$$

Prueba:

Por (2.2.6) podemos escribir (2.2.8) en la forma

$$(wx,y,z) - (xy,z,w) + (yz,w,x) = w(x,y,z) + (w,x,y)z \quad (\mathbf{2.2.12})$$

Sustituyendo para (wx,y,z) su expresión en términos de f como la dada por (2.2.9) se tiene

$$f(w,x,y,z) = (wx,y,z) - x(w,y,z) - (x,y,z)w$$

de donde despejamos (wx,y,z)

$$(wx,y,z) = f(w,x,y,z) + x(w,y,z) + (x,y,z)w$$

y análogamente para los otros términos de la izquierda de (2.2.12) tenemos

$$(xy,z,w) = f(x,y,z,w) + y(x,z,w) + (y,z,w)x$$

$$(yz,w,x) = f(y,z,w,x) + z(y,w,x) + (z,w,x)y$$

Luego sustituyendo el lado derecho de estas ecuaciones en (2.2.12) se tiene:

$$[f(w,x,y,z) + x(w,y,z) + (x,y,z)w] - [f(x,y,z,w) + y(x,z,w) + (y,z,w)] +$$
$$[f(y,z,w,x) + z(y,w,x) + (z,w,x)y] = w(x,y,z) + (w,x,y)z$$

$$f(w,x,y,z) + x(w,y,z) + (x,y,z)w - f(x,y,z,w) - y(x,z,w) - (y,z,w)x +$$
$$f(y,z,w,x) + z(y,w,x) + (z,w,x)y = w(x,y,z) + (w,x,y)z$$

$$f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = w(x,y,z) + (w,x,y)z - x(w,y,z) -$$
$$(x,y,z)w + y(x,z,w) + (y,z,w)x - z(y,w,x) - (z,w,x)y$$

$$f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = w(x,y,z) - (x,y,z)w - x(w,y,z) +$$
$$(y,z,w)x + y(x,z,w) - (z,w,x)y - z(y,w,x) + (w,x,y)z$$

$$f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = [w(x,y,z) - (x,y,z)w] -$$
$$[x(w,y,z) - (y,z,w)x] + [y(x,z,w) - (z,w,x)y] - [z(y,w,x) - (w,x,y)z]$$

$$f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = (w,(x,y,z)) - (x,(y,z,w)) +$$
$$(y,(z,w,x)) - (z,(w,x,y))$$

$$f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = F(x,y,z,w) \qquad (\mathbf{2.2.13})$$

donde $F(x,y,z,w)$ es el segundo miembro de (2.2.10) y por tanto cambia de signo cuando sus argumentos son permutados cíclicamente. De aquí que por (2.2.13),

$$0 = F(w,x,y,z) + F(x,y,z,w) = f(w,x,y,z) + f(z,w,x,y).$$

Verificando $0 = F(w,x,y,z) + F(x,y,z,w)$.

Por ecuación $(2.2.13)$ se tiene,

$$F(x,y,z,w) = (w,(x,y,z)) - (\,x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))$$

$$F(w,x,y,z) = (z,(w,x,y)) - (w,(x,y,z) + (\,x,(y,z,w) - \,(y,(z,w,x))$$

Entonces,

$$F(w,x,y,z) + F(x,y,z,w) = \big[(z,(w,x,y)) - (w,(x,y,z)) + (\,x,(y,z,w)) -$$

$$\big(y,(z,w,x)\big)\big] + [(w,(x,y,z)) - (\,x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))]$$

$$F(w,x,y,z) + F(x,y,z,w) = (z,(w,x,y)) - (w,(x,y,z)) + (\,x,(y,z,w)) -$$

$$\big(y,(z,w,x)\big) + (w,(x,y,z)) - (\,x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))$$

$$F(w,x,y,z) + F(x,y,z,w) = 0$$

Luego, verificamos $f(w,x,y,z) + f(z,w,x,y) = 0$ ó $f(w,x,y,z) = -f(z,w,x,y)$

La identidad (2.2.8) la podemos reescribir como

$$(wx,y,z) - (w,xy,z) + (w,x,yz) - w(x,y,z) - (w,x,y)z = 0 = g(w,x,y,z)$$

$$f(z,w,x,y) = \,(zw,x,y) - w(z,x,y) - (w,x,y)z$$

Luego,

$$f(z,w,x,y) = f(z,w,x,y) - g(w,x,y,z)$$

$$= (zw,x,y) - w(z,x,y) - (w,x,y)z - (wx,y,z) + (w,xy,z) - (w,x,yz) + w(x,y,z) + (w,x,y)z$$

$$= (zw,x,y) - w(x,y,z) - (w,x,y)z - (wx,y,z) + (w,xy,z) - (w,x,yz) + w(x,y,z) + (w,x,y)z$$

$$= (zw,x,y) - (wx,y,z) + (xy,z,w) - (yz,w,x)$$

Entonces, aplicando este resultado a $f(w,x,y,z)$ tenemos:

$$f(w,x,y,z) = (wx,y,z) - (xy,z,w) + (yz,w,x) - (zw,x,y)$$

y podemos ver que

$$-f(z,w,x,y) = -[(zw,x,y) - (wx,y,z) + (xy,z,w) - (yz,w,x)]$$

$$= -(zw,x,y) + (wx,y,z) - (xy,z,w) + (yz,w,x)$$

$$= (wx,y,z) - (xy,z,w) + (yz,w,x) - (zw,x,y)$$

Por lo tanto,

$$f(w,x,y,z) = -f(z,w,x,y) \qquad (\mathbf{2.2.14})$$

De aquí que f cambia de signo cuando sus argumentos se permutan cíclicamente y, por (2.2.9), cuando sus dos últimos argumentos son intercambiados, y, por tanto, cuando cualquiera dos de ellos son intercambiados.

Aplicando la ecuación $(2.2.9)$ se tiene,

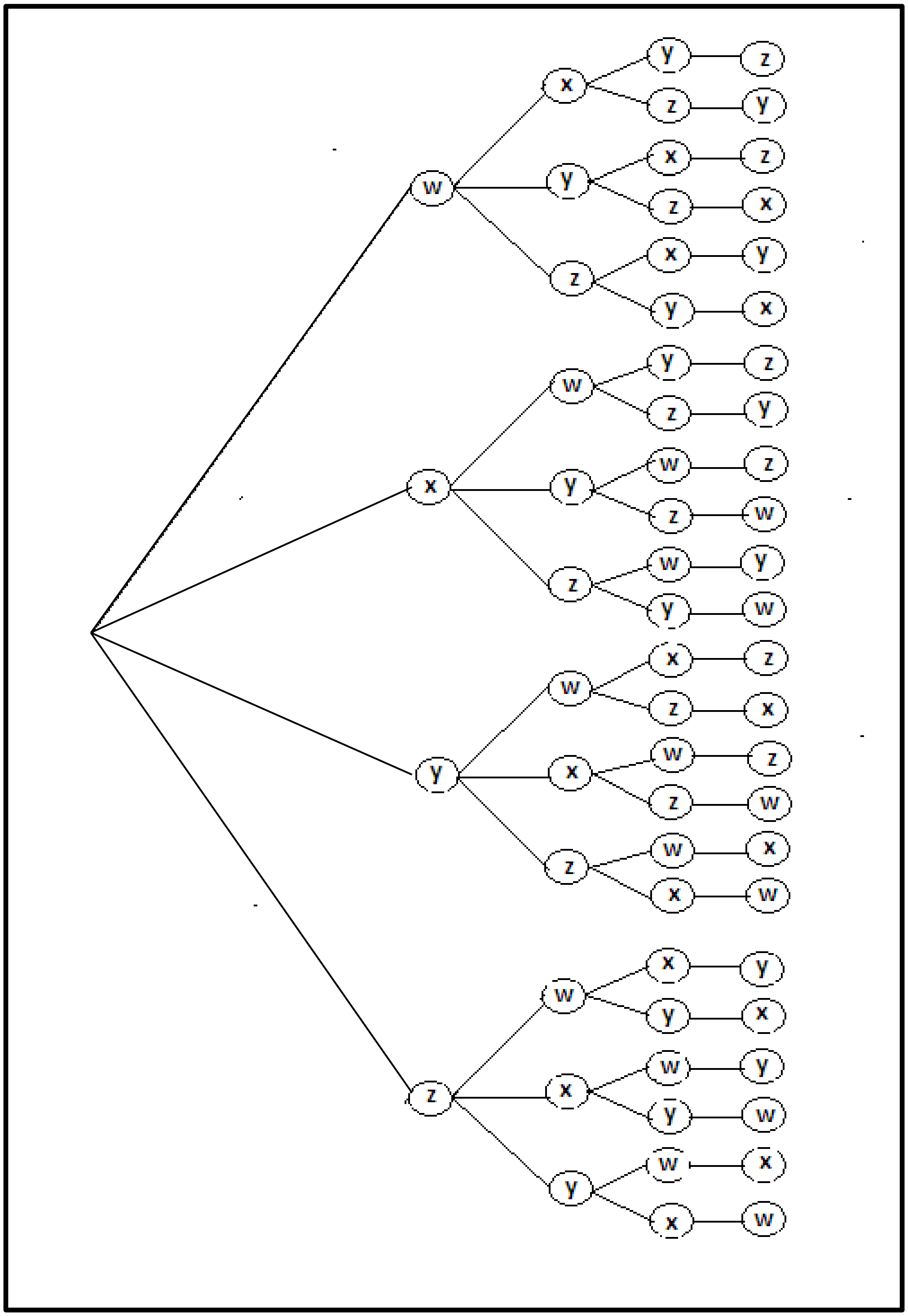
$$f(w,x,y,y) = (wx,y,y) - x(w,y,y) - (x,y,y)w$$

$$= 0 - x \cdot 0 - 0 \cdot w, \qquad \text{por ecuación } (2.2.4)$$

$$= 0$$

Por tanto, f es antisimétrica.

Se pueden obtener las permutaciones del conjunto $(w \quad x \quad y \quad z)$, como en teoría de grupos y así verificar cuando f cambia de signo. Se procede como sigue:


w
x
y
z
y
z
x
z
x
y
w
y
z
w
z
w
y
w
x
z
w
z
w
x
w
x
y
w
x
y
x
y
z
y
z
x
z
x
y
x
y
z
y
z
w
z
w
y
w
z
x
z
w
z
w
x
w
y
x
y
w
y
w
x
w

Las permutaciones resultantes son:

$$\sigma_1 = \begin{pmatrix} w & x & y & z \\ w & x & y & z \end{pmatrix} \qquad \sigma_{13} = \begin{pmatrix} w & x & y & z \\ y & w & x & z \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} w & x & y & z \\ w & x & z & y \end{pmatrix} \qquad \sigma_{14} = \begin{pmatrix} w & x & y & z \\ y & w & z & x \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} w & x & y & z \\ w & y & x & z \end{pmatrix} \qquad \sigma_{15} = \begin{pmatrix} w & x & y & z \\ y & x & w & z \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} w & x & y & z \\ w & y & z & x \end{pmatrix} \qquad \sigma_{16} = \begin{pmatrix} w & x & y & z \\ y & x & z & w \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} w & x & y & z \\ w & z & x & y \end{pmatrix} \qquad \sigma_{17} = \begin{pmatrix} w & x & y & z \\ y & z & w & x \end{pmatrix}$$

$$\sigma_6 = \begin{pmatrix} w & x & y & z \\ w & z & y & x \end{pmatrix} \qquad \sigma_{18} = \begin{pmatrix} w & x & y & z \\ y & z & x & w \end{pmatrix}$$

$$\sigma_7 = \begin{pmatrix} w & x & y & z \\ x & w & y & z \end{pmatrix} \qquad \sigma_{19} = \begin{pmatrix} w & x & y & z \\ z & w & x & y \end{pmatrix}$$

$$\sigma_8 = \begin{pmatrix} w & x & y & z \\ x & w & z & y \end{pmatrix} \qquad \sigma_{20} = \begin{pmatrix} w & x & y & z \\ z & w & y & x \end{pmatrix}$$

$$\sigma_9 = \begin{pmatrix} w & x & y & z \\ x & y & w & z \end{pmatrix} \qquad \sigma_{21} = \begin{pmatrix} w & x & y & z \\ z & x & w & y \end{pmatrix}$$

$$\sigma_{10} = \begin{pmatrix} w & x & y & z \\ x & y & z & w \end{pmatrix} \qquad \sigma_{22} = \begin{pmatrix} w & x & y & z \\ z & x & y & w \end{pmatrix}$$

$$\sigma_{11} = \begin{pmatrix} w & x & y & z \\ x & z & w & y \end{pmatrix} \qquad \sigma_{23} = \begin{pmatrix} w & x & y & z \\ z & y & w & z \end{pmatrix}$$

$$\sigma_{12} = \begin{pmatrix} w & x & y & z \\ x & z & y & w \end{pmatrix} \qquad \sigma_{24} = \begin{pmatrix} w & x & y & z \\ z & y & x & w \end{pmatrix}$$

Luego encontramos el signo de cada permutación

$$\sigma_1 = \begin{pmatrix} w & x & y & z \\ w & x & y & z \end{pmatrix} = (w)(x)(y)(z) \Rightarrow sig(\sigma_1) = 1$$

$$\sigma_2 = \begin{pmatrix} w & x & y & z \\ w & x & z & y \end{pmatrix} = (w)(x)(y \quad z) \Rightarrow sig(\sigma_1) = (-1)^1 = -1$$

$$\sigma_3 = \begin{pmatrix} w & x & y & z \\ w & y & x & z \end{pmatrix} = (w)(x \quad y)(z) \Rightarrow sig(\sigma_2) = (-1)^1 = -1$$

$$\sigma_4 = \begin{pmatrix} w & x & y & z \\ w & y & z & x \end{pmatrix} = (w)(x \quad y \quad z) = (x \quad y)(x \quad z) \Rightarrow sig(\sigma_4) = (-1)^2 = 1$$

$$\sigma_5 = \begin{pmatrix} w & x & y & z \\ w & z & x & y \end{pmatrix} = (w)(x \quad z \quad y) = (x \quad z)(x \quad y) \Rightarrow sig(\sigma_5) = (-1)^2 = 1$$

$$\sigma_6 = \begin{pmatrix} w & x & y & z \\ w & z & y & x \end{pmatrix} = (w)(x \quad z)(y) \Rightarrow sig(\sigma_6) = (-1)^1 = -1$$

$$\sigma_7 = \begin{pmatrix} w & x & y & z \\ x & w & y & z \end{pmatrix} = (w \quad x)(y)(z) \Rightarrow sig(\sigma_7) = (-1)^1 = -1$$

$$\sigma_8 = \begin{pmatrix} w & x & y & z \\ x & w & z & y \end{pmatrix} = (w \quad x)(y \quad z) \Rightarrow sig(\sigma_8) = (-1)^2 = 1$$

$$\sigma_9 = \begin{pmatrix} w & x & y & z \\ x & y & w & z \end{pmatrix} = (w \quad x \quad y)(z) = (w \quad x)(w \quad y) \Rightarrow sig(\sigma_9) = (-1)^2 = 1$$

$$\sigma_{10} = \begin{pmatrix} w & x & y & z \\ x & y & z & w \end{pmatrix} = (w\ x\ y\ z) = (w\ x)(w\ y)(w\ z) \Rightarrow sig(\sigma_{10}) = (-1)^3 = -1$$

$$\sigma_{11} = \begin{pmatrix} w & x & y & z \\ x & z & w & y \end{pmatrix} = (w\ x\ z\ y) = (w\ x)(w\ z)(w\ y) \Rightarrow sig(\sigma_{11}) = (-1)^3 = -1$$

$$\sigma_{12} = \begin{pmatrix} w & x & y & z \\ x & z & y & w \end{pmatrix} = (w \quad x \quad z)(y) = (w \quad x)(w \quad z) \Rightarrow sig(\sigma_{12}) = (-1)^2 = 1$$

$$\sigma_{13} = \begin{pmatrix} w & x & y & z \\ y & w & x & z \end{pmatrix} = (w \quad y \quad x)(z) = (w \quad y)(w \quad x) \Rightarrow sig(\sigma_{13}) = (-1)^2 = 1$$

$$\sigma_{14} = \begin{pmatrix} w & x & y & z \\ y & w & z & x \end{pmatrix} = (w\ y\ z\ x) = (w\ y)(w\ z)(w\ x) \Rightarrow sig(\sigma_{14}) = (-1)^3 = -1$$

$$\sigma_{15} = \begin{pmatrix} w & x & y & z \\ y & x & w & z \end{pmatrix} = (w \quad y)(x)(z) \Rightarrow sig(\sigma_{15}) = (-1)^1 = -1$$

$$\sigma_{16} = \begin{pmatrix} w & x & y & z \\ y & x & z & w \end{pmatrix} = (w \quad y \quad z)(x) = (w \quad y)(w \quad z) \Rightarrow sig(\sigma_{16}) = (-1)^2 = 1$$

$$\sigma_{17} = \begin{pmatrix} w & x & y & z \\ y & z & w & x \end{pmatrix} = (w \quad y)(x \quad z) \Rightarrow sig(\sigma_{17}) = (-1)^2 = 1$$

$$\sigma_{18} = \begin{pmatrix} w & x & y & z \\ y & z & x & w \end{pmatrix} = (w\ y\ x\ z) = (w\ y)(w\ x)(w\ z) \Rightarrow sig(\sigma_{18}) = (-1)^3 = -1$$

$$\sigma_{19} = \begin{pmatrix} w & x & y & z \\ z & w & x & y \end{pmatrix} = (w\ z\ y\ x) = (w\ z)(w\ y)(w\ x) \Rightarrow sig(\sigma_{19}) = (-1)^3 = -1$$

$$\sigma_{20} = \begin{pmatrix} w & x & y & z \\ z & w & y & x \end{pmatrix} = (w \quad z \quad x)(y) = (w \quad z)(w \quad x) \Rightarrow sig(\sigma_{20}) = (-1)^2 = 1$$

$$\sigma_{21} = \begin{pmatrix} w & x & y & z \\ z & x & w & y \end{pmatrix} = (w \quad z \quad y)(x) = (w \quad z)(w \quad y) \Rightarrow sig(\sigma_{21}) = (-1)^2 = 1$$

$$\sigma_{22} = \begin{pmatrix} w & x & y & z \\ z & x & y & w \end{pmatrix} = (w \quad z)(x)(y) \Rightarrow sig(\sigma_{22}) = (-1)^1 = -1$$

$$\sigma_{23} = \begin{pmatrix} w & x & y & z \\ z & y & w & z \end{pmatrix} = (w\ z\ x\ y) = (w\ z)(w\ x)(w\ y) \Rightarrow sig(\sigma_{23}) = (-1)^3 = -1$$

$$\sigma_{24} = \begin{pmatrix} w & x & y & z \\ z & y & x & w \end{pmatrix} = (w \quad z)(x \quad y) \Rightarrow sig(\sigma_{24}) = (-1)^2 = 1$$

Así hemos obtenido las permutaciones impares del conjunto $(w \;\; x \;\; y \;\; z)$.

En (2.2.13) tenemos que $f(w,x,y,z) - f(x,y,z,w) + f(y,z,w,x) = F(x,y,z,w)$

Pero aplicando el intercambio de argumentos tenemos que:

$-f(x,y,z,w) = f(w,x,y,z)$

$f(y,z,w,x) = f(w,x,y,z)$

Entonces sustituyendo en (2.2.13) nos queda

$f(w,x,y,z) + f(w,x,y,z) + f(w,x,y,z) = F(x,y,z,w)$

$3f(w,x,y,z) = F(x,y,z,w)$

Luego, sustituyendo

$F(x,y,z,w) = (w,(x,y,z)) - (x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))$

resulta

$3f(w,x,y,z) = (w,(x,y,z)) - (x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))$ y así (2.2.13) se reduce a (2.2.10).

De $f(w,x,y,z) = (wx,y,z) - x(w,y,z) - (x,y,z)w$ despejamos (wx,y,z) y obtenemos $(wx,y,z) = x(w,y,z) + (x,y,z)w + f(w,x,y,z)$ intercambiando w y x en esta ecuación se tiene $(xw,y,z) = w(x,y,z) + (w,y,z)x + f(x,w,y,z)$.

Luego, a (wx, y, z) le restamos (xw, y, z) y obtenemos

$$(wx, y, z) - (xw, y, z) = x(w, y, z) + (x, y, z)w + f(w, x, y, z) - w(x, y, z) - (w, y, z)x - f(x, w, y, z)$$

$$= -[w(x, y, z) - (x, y, z)w] + [x(w, y, z) - (w, y, z)x] + f(w, x, y, z) + f(w, x, y, z)$$

$$= -\big(w, (x, y, z)\big) + \big(x, (w, y, z)\big) + 2f(w, x, y, z)$$

Y como

$$(wx, y, z) - (xw, y, z) = \big[\big((wx)y\big)z - (wx)(yz)\big] - \big[\big((xw)y\big)z - (xw)(yz)\big]$$

$$= \big((wx)y\big)z - \big((xw)y\big)z - (wx)(yz) + (xw)(yz)$$

$$= \big((wx)y - (xw)y\big)z - (wx)(yz) + (xw)(yz)$$

$$= \big((wx - xw)y\big)z - (wx - xw)(yz)$$

$$= \big((w, x)y\big)z - (w, x)(yz)$$

$$= \big((w, x), y, z\big)$$

Entonces

$$\big((w, x), y, z\big) = -\big(w, (x, y, z)\big) + \big(x, (w, y, z)\big) + 2f(w, x, y, z)$$

Hemos calculado así, el primer miembro del lado derecho de la ecuación (2.2.11).

Sustituyendo $\big((y,z),w,x\big)$ en términos de la ecuación anterior obtenemos

$$\big((y,z),w,x\big) = -\big(y,(z,w,x)\big) + \big(z,(y,w,x)\big) + 2f(y,z,w,x)$$

Utilizando la ecuación $(2.2.10)$ se calcula el segundo miembro del lado derecho de la ecuación $(2.2.11)$, de la siguiente forma

$$3f(w,x,y,z) = (w,(x,y,z)) - (\,x,(y,z,w)) + (y,(z,w,x)) - (z,(w,x,y))$$

$$\big(z,(w,x,y)\big) - \big(y,(z,w,x)\big) + 2f(w,x,y,z) = \big(w,(x,y,z)\big) - \big(\,x,(y,z,w)\big) - f(w,x,y,z)$$

$$\big(z,(y,w,x)\big) - \big(y,(z,w,x)\big) + 2f(w,x,y,z) = \big(w,(x,y,z)\big) - \big(\,x,(y,z,w)\big) - f(w,x,y,z)$$

$$\big((y,z),w,x\big) = \big(w,(x,y,z)\big) - \big(\,x,(y,z,w)\big) - \,f(w,x,y,z)$$

Luego sumamos los dos términos, $\big((y,z),w,x\big)$ y $\big((w,x),y,z\big)$ y se obtiene

$$\big((y,z),w,x\big) + \big((w,x),y,z\big) = -\big(w,(x,y,z)\big) + \big(x,(w,y,z)\big) + 2f(w,x,y,z) + \big(w,(x,y,z)\big) - \big(\,x,(y,z,w)\big) - \,f(w,x,y,z)$$

$$= f(w,x,y,z)$$

Por tanto se prueba la ecuación la ecuación $(2.2.11)$.

Lema 2.2.2. Para todo x, y, z de un anillo alternativo, tenemos:

$$(x^2, y, z) = x(x, y, z) + (x, y, z)x, \qquad (\mathbf{2.2.15})$$

$$(x, xy, z) = (x, y, xz) = (x, y, z)x, \qquad (\mathbf{2.2.16})$$

$$(x, yx, z) = (x, y, zx) = x(x, y, z), \qquad (\mathbf{2.2.17})$$

y las identidades de Moufang

$$(xy)(zx) = x\big((yz)x\big) = \big(x(yz)\big)x. \qquad (\mathbf{2.2.18})$$

$$x\big(y(xz)\big) = \big((xy)x\big)z, \quad \big((zx)y\big)x = z\big(x(yx)\big). \qquad (\mathbf{2.2.19})$$

Prueba:

Prueba de $(\mathbf{2.2.15})$. Obtenemos (2.2.15) de $f(x, x, y, z) = 0$.

$f(x, x, y, z) = (xx, y, z) - x(x, y, z) - (x, y, z)x = 0$, por ecuación. (2.2.9),

de donde

$$(xx, y, z) = x(x, y, z) + (x, y, z)x$$

$$(x^2, y, z) = x(x, y, z) + (x, y, z)x.$$

Prueba de $(\mathbf{2.2.16})$. Obtenemos las dos partes de (2.2.16) observando que $f(x, y, z, x) = 0$ y $f(x, z, x, y) = 0$, por antisimetría de $f(w, x, y, z)$.

Por definición de $f(w, x, y, z)$, $f(x, y, z, x) = (xy, z, x) - y(x, z, x) - (y, z, x)x = 0$

de donde

$(xy, z, x) = y(x, z, x) + (y, z, x)x$

$(x, xy, z) = y(x, x, z) + (x, y, z)x$

$(x, xy, z) = y(0) + (x, y, z)x$

$(x, xy, z) = (x, y, z)x$

Y $f(x, z, x, y) = (xz, x, y) - z(x, x, y) - (z, x, y)x = 0$

de donde

$(xz, x, y) = z(x, x, y) + (z, x, y)x$

$(x, y, xz) = z(0) + (x, y, z)x$

$(x, y, xz) = (x, y, z)x$

Por tanto,

$(x, xy, z) = (x, y, xz) = (x, y, z)x$

Prueba $(\mathbf{2.2.17})$. Obtenemos (2.2.17) de $f(y, x, x, z) = 0$ y $f(z, x, x, y) = 0$.

$f(y, x, x, z) = (yx, x, z) - x(y, x, z) - (x, x, z)y = 0$

de donde

$(yx, x, z) = x(y, x, z) + (x, x, z)y$

$(yx, x, z) = x(y, x, z) + (0)y$

$-(x, yx, z) = x\big(-(x, y, z)\big)$

$-(x, yx, z) = -x(x, y, z)$

$(x, yx, z) = x(x, y, z).$

Y $f(z, x, x, y) = (zx, x, y) - x(z, x, y) - (x, x, y)z = 0$

de donde

$(zx, x, y) = x(z, x, y) + (x, x, y)z$

$(zx, x, y) = x(z, x, y) + (0)z$

$(x, y, zx) = x(x, y, z).$

Por tanto,

$(x, yx, z) = (x, y, zx) = x(x, y, z).$

Prueba de $(2.2.18)$.

Para probar $(2.2.18)$ notamos que:

$(x, y, zx) = (xy)(zx) - x\big(y(zx)\big)$

de donde,

$(xy)(zx) = x\big(y(zx)\big) + (x, y, zx)$

$$= x\big(y(zx)\big) + x(x, y, z)$$

$$= x\big(y(zx)\big) + x(y, z, x)$$

$$= x[y(zx) + (y, z, x)]$$

$$= x[y(zx) + (yz)x - y(zx)]$$

$$= x\big((yz)x\big)$$

Por tanto,

$(xy)(zx) = x\big((yz)x\big)$.

Para probar que $(xy)(zx) = \big(x(yz)\big)x$ notamos que:

$$(x, y, z)x = [(xy)z - x(yz)]x = \big((xy)z\big)x - \big(x(yz)\big)x$$

de donde,

$$\big(x(yz)\big)x = \big((xy)z\big)x - (x, y, z)x$$

$$= (xy)(zx) + (xy, z, x) - (x, y, z)x \qquad [\text{ por } *\ ]$$

$$= (xy)(zx) + (x, xy, z) - (x, y, z)x$$

$$= (xy)(zx) + 0$$

$$= (xy)(zx)$$

Usando $(xy, z, x) = \big((xy)z\big)x - (xy)(zx)$

obtenemos

$*\quad \big((xy)z\big)x = (xy)(zx) + (xy, z, x)$

Por tanto,

$(xy)(zx) = x\big((yz)x\big) = \big(x(yz)\big)x.$

Prueba de $(2.2.19)$. La primera ecuación de $(2.2.19)$ se deriva como sigue:

$(xy, x, z) = \big((xy)x\big)z - (xy)(xz)$

de donde,

$\big((xy)x\big)z = (xy)(xz) + (xy, x, z)$

$= x\big(y(xz)\big) + (x, y, xz) - (x, xy, z)$ [por $**$]

$= x\big(y(xz)\big).$

Usando $(x, y, xz) = (xy)(xz) - x\big(y(xz)\big)$

obtenemos,

$**\quad (xy)(xz) = (x, y, xz) + x\big(y(xz)\big).$

La segunda ecuación de $(2.2.19)$ se deriva como sigue:

$$(z,x,yx) = (zx)(yx) - z\big(x(yx)\big)$$

de donde,

$$z\big(x(yx)\big) = (zx)(yx) - (z,x,yx)$$

$$= \big((zx)y\big)x - (zx,y,x) - (z,x,yx) \qquad [\text{ por } ***\ ]$$

$$= \big((zx)y\big)x - \big(-(x,y,zx)\big) - (x,yx,z)$$

$$= \big((zx)y\big)x + (x,y,zx) - (x,yx,z)$$

$$= \big((zx)y\big)x$$

Usando $(zx,y,x) = \big((zx)y\big)x - (zx)(yx)$

obtenemos,

$***\quad (zx)(yx) = \big((zx)y\big)x - (zx,y,x)$

Por tanto, se han demostrado las leyes $(2.2.19)$.

Las identidades $(2.2.16)$ y $(2.2.17)$ se pueden generalizar así: en cualquier asociador x, y, z con un factor x en y ó z, se puede sacar el factor x (dejando las otras x, y y z solas) a la izquierda si x es un factor derecho ó a la derecha si x es un factor izquierdo:

$(x, xy, z) = (x, y, z)x$

$(x, yx, z) = x(x, y, z)$

Las identidades de Moufang juegan un papel importante en la teoría de anillos alternativos. Observamos que las identidades de Moufang son generalizaciones de las leyes alternativas en el sentido de que si suponemos $z = 1$ en $(2.2.18)$ y $(2.2.19)$ obtenemos:

$(xy)x = x(yx) = (xy)x$ ley reflexiva

$x(yx) = (xy)x,\ (xy)x = x(yx)$ ley reflexiva

Si $y = 1$,

$x(zx) = x(zx)$

$x(xz) = (xx)z,\ (zx)x = z(xx)$.

Demostraremos que las leyes $(2.2.2)$ se siguen de las de $(2.2.1)$ en un anillo de división.

Dado un elemento $\boldsymbol{a} \neq 0$, hay entonces un u tal que $\boldsymbol{a}u = 1$.

Entonces $\boldsymbol{a} = (\boldsymbol{a}u)\boldsymbol{a} = \boldsymbol{a}(u\boldsymbol{a})$, de donde también $u\boldsymbol{a} = 1$, y podemos escribir $u = \boldsymbol{a}^{-1}$, donde $\boldsymbol{a}^{-1}\boldsymbol{a} = \boldsymbol{a}\boldsymbol{a}^{-1} = 1$.

Dados $\boldsymbol{a}, b$ distintos de cero, se determina c por la relación $b = \boldsymbol{a}^{-1}c$. Entonces,

$$\boldsymbol{a}^{-1}(\boldsymbol{a}b) = \boldsymbol{a}^{-1}\big(\boldsymbol{a}(\boldsymbol{a}^{-1}c)\big)$$

$$= \big((\boldsymbol{a}^{-1}\boldsymbol{a})\boldsymbol{a}^{-1}\big)c \text{ , por la primera ley de } (2.2.19)$$

$$= (1\boldsymbol{a}^{-1})c$$

$$= \boldsymbol{a}^{-1}c$$

$$= b$$

Análogamente,

$$(b\boldsymbol{a})\boldsymbol{a}^{-1} = \big((\boldsymbol{a}^{-1}c)\boldsymbol{a}\big)\boldsymbol{a}^{-1}$$

$$= \big((c\boldsymbol{a}^{-1})\boldsymbol{a}\big)\boldsymbol{a}^{-1} \text{ , por la segunda ley de } (2.2.19)$$

$$= c\big(\boldsymbol{a}^{-1}(\boldsymbol{a}\boldsymbol{a}^{-1})\big)$$

$$= c(\boldsymbol{a}^{-1}\ 1)$$

$$= c\boldsymbol{a}^{-1}$$

$$= \boldsymbol{a}^{-1}c$$

$$= b$$

Quedando así demostrado que las leyes (2.2.1) implican las leyes (2.2.2) en un anillo de división.

CAPÍTULO III

EL TEOREMA DE WEDDERBURN Y EL TEOREMA DE ARTIN-ZORN

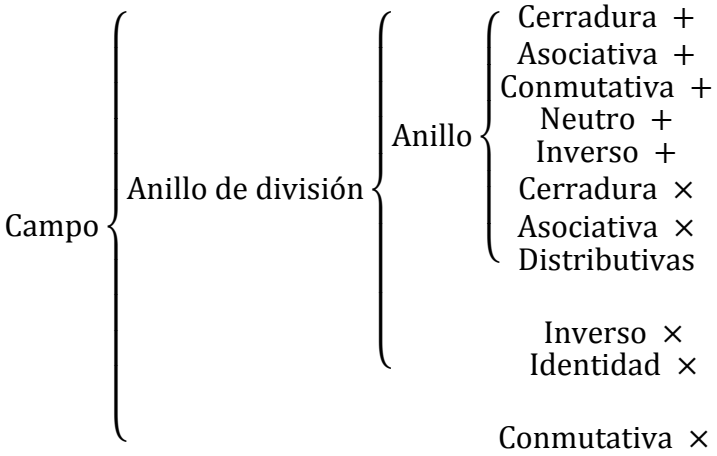
3.1. EL TEOREMA DE WEDDERBURN

Teorema 3.1.1. El Teorema de Wedderburn

Un anillo de división finito R es necesariamente conmutativo y por tanto un campo finito $GF(p^r)$.

Prueba:

Recordando que un anillo de división satisface todos los axiomas de un campo excepto que la conmutatividad de la multiplicación no es asumida. El Teorema de Wedderburn nos dice que si asumimos que el anillo de división es finito entonces la conmutatividad de la multiplicación se sigue de los otros axiomas de campo, como podemos observar en el siguiente gráfico:



Sea R un anillo de división finito, con unidad $1 \neq 0$.

Si se muestra que R es conmutativo entonces, por definición 1.3.2 R es un campo.

Sea $Z(R) = Z$, el centro de R, esto es: $\{z \in R: zx = xz \text{ para todo } x \in \mathrm{R}\}$.

Z es un anillo conmutativo de R, y por tanto un campo finito, por proposición 1.2.1.

Z es cerrado bajo la suma y la multiplicación, y la multiplicación es conmutativa dentro de Z por definición.

Como R es finito, la característica es positiva y necesariamente un número primo p, o de otra forma R podría tener divisores de cero, por proposición 1.3.1.

Supongamos R tiene una base de r elementos:

$x_1 = 1, x_2, \dots, x_r$ sobre F_p. Entonces R tiene exactamente p^r elementos, por ser R un espacio vectorial sobre el campo primo F_p.

Supongamos que Z tiene $q = p^s$ elementos, por propiedad 1.5.1 de campos finitos.

Ahora, la idea de la prueba es la siguiente:

Queremos probar que R es conmutativo.

Sabemos que Z es conmutativo, y si podemos mostrar que $R = Z$ habríamos terminado la prueba.

Ahora bien, si podemos mostrar que $|R| = |Z|$, es decir, que el orden o el número de elementos de R es igual al número de elementos de Z, entonces $R = Z$, y otra vez, habríamos terminado la prueba.

Luego, dado que R es finito cualquier subconjunto de R es cerrado bajo la multiplicación y la suma, y es un subanillo, de hecho un subanillo de división de R, por proposición 1.2.1.

En todo caso, R es un espacio vectorial sobre Z, donde la suma vectorial es suma en R y la multiplicación escalar es solo multiplicación en R para los elementos de Z.

Y si R tiene una base de t elementos sobre Z, entonces R tiene $q^t = (p^s)^t = p^{st} = p^r$ elementos en total, aquí si $t = 1$ entonces $|R| = |Z|$, y habríamos terminado la prueba.

Por lo tanto, quedaría por demostrar que $t = 1$.

Ahora bien, para empezar la prueba del teorema tenemos dos casos:

i. Si $t = 1$.

   Sustituyendo $t = 1$ en la siguiente ecuación $q^t = (p^s)^t = p^{st} = p^r$ que denota el número de elementos en total de R, se tiene:

$$q = p^s = p^r$$

   Y como Z tiene $q = p^s$ elementos, por lo tanto hemos mostrado que $Z = R$.

ii. Supongamos, por el contrario que $t > 1$.

Derivaremos una contradicción usando las propiedades del t-ésimo polinomio ciclotómico $\Phi_t(x)$.

Sea N_x el normalizador de un elemento x de R, $N_x = \{\boldsymbol{a} \in R \mid \boldsymbol{a}x = x\boldsymbol{a}\}$.

El normalizador N_x de R es un subanillo de división que contiene a Z, $N_x \supseteq Z$, por proposición 1.2.2.

De aquí que, N_x contiene q^d elementos para algún entero d, y como R es un espacio vectorial sobre N_x, tenemos necesariamente que $d|t$.

De aquí que en el grupo multiplicativo $R^* = R - \{0\}$ de los $p^r - 1 = q^t - 1$ elementos de R distintos de 0, un elemento x que no está en Z tiene un normalizador de orden $q^d - 1$, donde d es un divisor de t y $d < t$.

Como N_x es un subanillo de división de R se sigue que ${N_x}^* = N_x - \{0\}$ es un subgrupo centralizador de R^* que tiene $q^d - 1$ elementos.

Por el Teorema de Lagrange (Teorema 1.1.1), el orden de ${N_x}^*$ divide al orden de R^*, es decir, $(q^d - 1) \mid (q^t - 1)$, esto implica que $d|t,\ d < t$.

Para mostrar que $(q^d - 1) \mid (q^t - 1)$ implica que $d|t$, supongamos que $t = kd + m$, m residuo con $0 \leq m < d$, como

$$q^t - 1 = (q^d - 1)(q^{t-d} + q^{t-2d} + \cdots + q^{t-kd}) + (q^{t-kd} - 1),$$

y $(q^d - 1)|(q^t - 1)$, entonces $(q^d - 1) \mid (q^{t-kd} - 1)$, pero $m = t - kd < d$ así que $0 \leq q^m - 1 < q^d - 1$,

luego, la única forma de que $(q^d - 1) \mid (q^m - 1)$ es que $q^m = 1$;

por otro lado, como $0,1 \in Z$ entonces $q \geq 2$ por lo cual la igualdad $q^m = 1$ implica $m = 0$, luego $d|t$.

El centro de R^* es Z^*, el cual tiene orden $q - 1$. Para los $x \in R^*$, el normalizador de x en R^* es exactamente $N_x{}^*$.

En el grupo de elementos distintos de cero de R tenemos la relación de conjugación, x es conjugado de y si $x = \boldsymbol{a}^{-1}y\boldsymbol{a}$ para algún $\boldsymbol{a} \neq 0$ en R.

Según el Teorema 1.1.2 el número de elementos de R conjugados de x es el índice del normalizador de x en el grupo de elementos distintos de cero de R. Por tanto, el número de conjugados de x en R es $\frac{q^t-1}{q^d-1}$.

Note que si $x \in Z^*$ entonces x tiene un solo conjugado pues $\boldsymbol{a}x\boldsymbol{a}^{-1} = \boldsymbol{a}\boldsymbol{a}^{-1}x = \boldsymbol{a}$ para toda $\boldsymbol{a} \in R^*$, de aquí que $q^t - 1 = q^d - 1$ esto es $t = d$.

Recíprocamente, si $t = d$ entonces $R^* = N_x{}^*$ (pues $\frac{q^t-1}{q^d-1} = 1$), es decir, $x\boldsymbol{a} = \boldsymbol{a}x$ para toda $\boldsymbol{a} \in R^*$ luego $x \in Z^*$. Hemos probado que $t = d$ si y solo si $x \in Z^*$.

Por otro lado, si $d = 1$ entonces $Z^* = N_x{}^*$; esto implica $x \in Z^*$ por lo cual, si $x \notin Z^*$, entonces $d \neq 1$ y $d \neq t$.

Consideremos ahora la ecuación de clase (corolario 1.1.4) para el grupo R^*.

De aquí, una clase de conjugación en R^* que contiene más de un elemento tiene $(q^t - 1) \,/\, (q^d - 1)$ elementos, donde d es un divisor de t con $1 \leq d < t$. De aquí que la ecuación de clase será

$$q^t - 1 = q - 1 + \sum_{\substack{d|t \\ d\neq t \\ d\neq 1}} \frac{q^t-1}{q^d-1} \qquad (\mathbf{3.1.1.1})$$

donde $q - 1$ enumera los elementos del centro, y la suma efectuada sobre una x en cada clase conjugada para x que no está en el centro.

El problema ha sido reducido a probar que ninguna ecuación tal como $(3.1.1.1)$ puede cumplirse en los enteros.

La prueba de este hecho se basa a demostrar que existe un entero que divida a $(q^t - 1) \,/\, (q^d - 1)$ para todos los divisores d de t, excepto para $d = t$, pero que no divide a $q - 1$.

Una vez hecho esto, la ecuación $q^t - 1 = q - 1 + \sum (q^t - 1) \,/\, (q^d - 1)$ será imposible a menos que $t = 1$ y, con lo cual el teorema de Wedderburn será probado.

El medio que emplearemos con este propósito es la teoría de polinomios ciclotómicos.

Consideremos el polinomio $f(x) = x^t - 1$ como elementos de $\mathbb{C}[x]$ donde $\mathbb{C}$ es el campo de los números complejos.

En $\mathbb{C}[x]$ $x^t - 1 = \prod(x - w)$ donde el producto es tomado sobre todas las raíces t-ésimas de la unidad, esto es todas las $w \in \mathbb{C}$, tales que $w^t = 1$.

El conjunto de todas $w \in \mathbb{C}$ que satisfacen $w^t = 1$ forman un grupo bajo la multiplicación. Como todo subgrupo finito del grupo de los elementos distintos de cero de un campo es cíclico, por propiedad 1.5.4 de campos finitos, se sigue que el grupo de todas las t-ésimas raíces de la unidad es un grupo cíclico. Una raíz que es un generador del grupo mencionado es una t-ésima raíz primitiva de la unidad.

Sea $\Phi_t(x) = \prod_{mcd(j,t)=1}(x - w^j)$,

Donde w es una t-ésima raíz primitiva de la unidad, w^j para $j = 1, \dots, t$, $(j, t) = 1$, son todas las t-ésimas raíces primitivas de la unidad. Este polinomio se llama polinomio ciclotómico.

Enumeramos los primeros polinomios ciclotómicos:

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = \frac{(x - 1)(x + 1)}{(x - 1)} = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = \frac{(x - 1)(x^2 + x + 1)}{(x - 1)} = x^2 + x + 1$$

$$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = \frac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = \frac{(x-1)(x+1)(x^2+1)}{(x-1)(x+1)} = x^2 + 1$$

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = \frac{(x-1)(x^4 + x^3 + x^2 + x + 1)}{(x-1)} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)}$$

$$= \frac{(x^3-1)(x^3+1)}{(x-1)(x+1)(x^2 + x + 1)}$$

$$= \frac{(x-1)(x^2 + x + 1)(x+1)(x^2 - x + 1)}{(x-1)(x+1)(x^2 + x + 1)}$$

$$= x^2 - x + 1$$

Observe que todos esos polinomios son mónicos y con coeficientes enteros. Afirmamos que, en general, $\Phi_t(x)$ es un polinomio mónico con coeficientes enteros.

Si m es un divisor de t, cada factor $x - \theta$ de $\Phi_m(x)$ es un factor de $x^t - 1$ pues, como $\theta^m = 1$ tenemos que $\theta^t = (\theta^m)^{t/m} = 1$ y además $x - \theta$ aparece solo una vez en la factorización de $x^t - 1$ pues este último no tiene raíces repetidas. Recíprocamente sea $x - w$ un factor de $x^t - 1$ y sea m el orden de w en el grupo de las t-ésimas raíces de la unidad, de la definición de raíz primitiva w es una m-ésima raíz primitiva de la unidad por lo que $x - w$ es un factor de $\Phi_m(x)$ y $m|t$ por el Teorema de Lagrange. Con esto hemos probado que para cada divisor m de t los factores $\Phi_m(x)$ aparecen una vez en la

factorización de $x^t - 1$ y recíprocamente que cada factor de $x^t - 1$ es un factor de $\Phi_m(x)$ para algún m divisor de t, es decir,

$$x^t - 1 = \prod_{m|t} \Phi_m(x) \qquad (\mathbf{3.1.1.2})$$

Probaremos que $\Phi_t(x)$ es un polinomio mónico con coeficientes enteros, por inducción sobre t:

Para $t = 1$, hemos visto que $\Phi_t(x) = x - 1$.

Supongamos como hipótesis de inducción que $\Phi_m(x)$ es un polinomio mónico con coeficientes enteros para $m < t$.

Demostraremos el resultado para t. Por hipótesis de inducción se sigue que en particular $\Phi_m(x)$ es un polinomio mónico con coeficientes enteros para $m|t$ con $m < t$, luego por (3.1.1.2) se tiene: $x^t - 1 = \Phi_t(x)g(x)$ donde $g(x)$ es el producto de los polinomios $\Phi_m(x)$ donde $m|t$ con $m < t$ y como estos polinomios satisfacen la hipótesis de inducción, se sigue que $g(x)$ es mónico y con coeficientes enteros.

Como $g(x)$ es mónico existen polinomios $q(x)$, $r(x)$ únicos y con coeficientes enteros tales que

$x^t - 1 = q(x)g(x) + r(x)$ donde $r(x) = 0$ o $deg(r(x)) < deg(g(x))$, de esto se sigue que $g(x)\big(\Phi_t(x) - q(x)\big) = r(x)$: si $r(x) \neq 0$ entonces $\Phi_t(x) \neq q(x)$ por lo cual

$$deg\big(g(x)\big) \leq deg\big(g(x)\big) + deg\big(\Phi_t(x) - q(x)\big) = deg(r(x)) < deg(g(x))$$

lo cual es imposible, luego $r(x) = 0$ y, como $g(x) \neq 0$, se sigue que $\Phi_t(x) = q(x)$ de aquí $\Phi_t(x)$ es un polinomio con coeficientes enteros.

El hecho de que sea mónico se sigue de que el término principal de $x^t - 1$ es igual al producto del termino principal de $g(x)$, que es mónico, por el de $\Phi_t(x)$.

Sea m un divisor de t, entonces $x^m - 1 | x^t - 1$ este hecho se sigue de la identidad:

$x^t - 1 = (x^m - 1)\left(x^{t-m} + x^{t-2m} + \cdots + x^{t-(k-1)m} + 1\right)$, donde $t = km$, asi $(x^t - 1)/(x^m - 1)$ es un polinomio con coeficientes enteros. Ahora, afirmamos que para cualquier divisor m de t, con $m < t$,

$$\Phi_t(x) \left| \frac{x^t - 1}{x^m - 1} \right.$$

en el sentido de que el cociente es un polinomio con coeficientes enteros. Para ver esto, note que

$$x^m - 1 = \prod_{k|d} \Phi_k(x)$$

Puesto que cada divisor de m es un divisor de t, reagrupando los términos en (3.1.2) obtenemos $x^t - 1 = (x^m - 1)p(x)$ donde $p(x)$ es el producto de las $\Phi_k(x)$ tales que $k|t$ y $k \nmid m$. Como $m < t$ entonces $\Phi_t(x)$ no aparece en la expresión de $x^m - 1$ como producto de las $\Phi_k(x)$. Así (3.1.1.2) puede ser escrita como $x^t - 1 = \Phi_t(x)(x^m - 1)f(x)$ donde

$$f(x) = \prod_{\substack{k|t \\ k\nmid m \\ k\neq t}} \Phi_k(x)$$

es un polinomio con coeficientes enteros, así

$$\frac{x^t - 1}{x^m - 1} = \Phi_t(x) f(x)$$

luego

$$\Phi_t(x) \left| \frac{x^t - 1}{x^m - 1} \right.$$

en el sentido de que el cociente, que es $f(x)$, es un polinomio con coeficientes enteros, lo cual demuestra la afirmación.

Como $\Phi_t(x)$ es un polinomio con coeficiente enteros, tenemos para cualquier entero x, $\Phi_t(x)$ es un entero que divide a $(x^t - 1)/(x^m - 1)$ para cualquier divisor $m < t$ de hecho $(x^t - 1)/(x^m - 1) = \Phi_t(x) f(x)$ con $f(x)$ entero. En particular, retomando el contexto de la ecuación (3.1.1.1), se tiene que

$$\Phi_t(x) \left| \frac{x^t - 1}{x^d - 1} \right.$$

en el sentido de que el cociente, es un polinomio con coeficientes enteros.

Y por sustitución para $x = q$,

$\Phi_t(q) \left| \frac{q^t - 1}{q^d - 1} \right.$ y $\Phi_t(q) | (q^t - 1)$

De aquí concluimos de la clase de ecuación que $\Phi_t(q)|(q-1)$ al menos que $t=1$.

Pero ahora estimamos el valor absoluto de $\Phi_t(q)$ de su definición, considerando las t-ésima raíces de unidad como números complejos.

Así

$$|\Phi_t(q)| = \prod_{mcd(j,t)=1}|q - w^j| > q - 1$$

Porque $q \in \mathbb{Z}$, $q \geq 2$ y si $t > j > 1$, $|q - w^j| > q - 1$, ver figura 3.1.1.1.

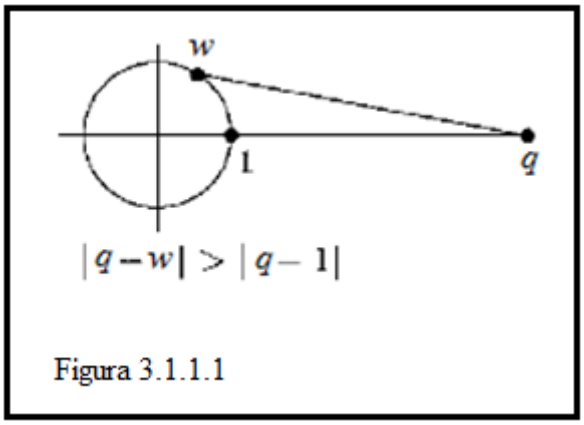


Figura 3.1.1.1

De aquí que si $t > 1$ concluimos que $|\Phi_t(q)| > q - 1$, entonces $\Phi_t(q)$ no puede dividir a $q - 1$, lo que nos lleva a una contradicción.

Por tanto, t debe ser igual a 1 y Z debe ser igual a R y R debe ser un campo finito.

3.2. EL TEOREMA DE ARTIN-ZORN

3.2.1. El Teorema de Artin-Zorn

Un anillo de división alternativo finito, es un campo finito $GF(P^r)$.

Prueba:

Sea $\boldsymbol{R}$ un anillo de división alternativo finito.

Consideremos $\boldsymbol{R_1}$ generado por b y c, donde $\boldsymbol{R_1}$ es un subsistema de $\boldsymbol{R}$ cerrado respecto a la adición y a la multiplicación. $\boldsymbol{R_1}$ es finito y no tiene divisores de cero.

Sean $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ los elementos de $\boldsymbol{R_1}$ distintos de cero.

Entonces para cualquier $x \in \boldsymbol{R_1}$, $x\boldsymbol{a}_1, \ldots, x\boldsymbol{a}_t$ son todos diferentes si $x \neq 0$, ya que $\boldsymbol{R_1}$ no contiene divisores de cero. De aquí que para algún elemento, digamos $\boldsymbol{a}_1$, tenemos $x\boldsymbol{a}_1 = x$ de donde $\boldsymbol{a}_1 = \frac{x}{x} = 1$ es la unidad de $\boldsymbol{R}$.

Además para algún $\boldsymbol{a}_i$ tenemos $x\boldsymbol{a}_i = 1$, de donde $\boldsymbol{a}_i = \frac{1}{x} = x^{-1}$.

Los elementos de $\boldsymbol{R_1}$ son sumas de monomios $(x_1 \ldots x_r)(x_{r+1} \ldots x_n)$, donde cada x_i es b ó c y los términos están asociados de cierto modo.

Como ambas leyes distributivas se verifican, la multiplicación será asociativa en $\boldsymbol{R}$, si y solo si la multiplicación de los monomios es asociativa.

Para mostrar esto, definimos monomios normales (o asociados con paréntesis) a la izquierda en forma recursiva por las reglas:

$$[x_1 x_2] = x_1 x_2$$

$$[x_1 \dots x_n] = [x_1 \dots x_{n-1}]x_n \qquad (\mathbf{3.2.1})$$

Debemos mostrar que toda asociación con paréntesis arbitraria es igual al monomio normal.

Para ello probaremos por inducción sobre la longitud del monomio que todo monomio es igual al monomio normal con iguales factores en igual orden.

Por ecuación (2.2.4) y (2.2.6) esto es cierto para monomios en b y c de longitud tres, ya que en tal caso debe haber un factor repetido, por tanto

$$x_1(x_2 x_3) = (x_1 x_2)x_3 = [x_1 x_2]x_3 \qquad (\mathbf{3.2.2})$$

Ahora debemos demostrar que:

$$[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s] \qquad (\mathbf{3.2.3})$$

Usando inducción sobre $n = r + s$ para un n fijo, primero usaremos inducción sobre s.

i. Para $s = 1$.

Para $s = 1$ se sigue que:

$[u_1 \dots u_r][v_1] = [u_1 \dots u_r v_1]$ por la ecuación (3.2.1).

Por lo tanto la ecuación (3.2.3) se verifica.

ii. Para $s > 1$.

Suponiendo $s > 1$ y $v_1 = v_s = b$ o $v_1 = v_s = c$, por ser $\boldsymbol{R_1}$ generado por

b y c.

Entonces, en la segunda identidad de (2.2.19), $z[x(yx)] = [(zx)y]x$, tomando

$z = [u_1 \dots u_r]$, $v_1 = v_s = x$ y $[v_2 \dots v_{s-1}] = y$.

Esto es

$$[u_1 \dots u_r][x v_2 \dots v_{s-1} x] = [u_1 \dots u_r v_1 v_2 \dots v_{s-1} v_s] \qquad (\mathbf{3.2.4})$$

Verificación.

$[u_1 \dots u_r][x v_2 \dots v_{s-1} x] = \{([u_1 \dots u_r]x)[v_2 \dots v_{s-1}]\}x$ por identidad (2.2.19)

$= \{([u_1 \dots u_r]v_1)[v_2 \dots v_{s-1}]\}v_s$ sustituyendo el valor x.

$= \{[u_1 \dots u_r v_1][v_2 \dots v_{s-1}]\}v_s$ utilizando segunda igualdad de (3.2.1)

$= [u_1 \dots u_r v_1 v_2 \dots v_{s-1}] v_s$ utilizando primera igualdad de (3.2.1)

$= [u_1 \dots u_r v_1 v_2 \dots v_{s-1} v_s]$ utilizando segunda igualdad de (3.2.1)

Por tanto, hemos probado $[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s]$ cuando $v_1 = v_s$.

Suponiendo $v_1 \neq v_s$ entonces $v_1 = b, v_s = c$.

Aquí u_r es ó b ó c por que $\boldsymbol{R_1}$ es generado por b y c. Suponiendo $u_r = b$.

Tomando $x = [u_1 \dots u_{r-1}], u_r = b,\ v_1 = b,\ y = [v_2 \dots v_s]$.

Ahora utilizando la función

$$f(w, x, y, z) = (wx, y, z) - x(w, y, z) - (x, y, z)w$$

La desarrollamos para $f(x, b, b, y)$ y obtenemos

$f(x, b, b, y) = (xb, b, y) - b(x, b, y) - (x, b, b)y = 0$ por ser una función antisimetrica.

Aquí $(x, b, b) = 0$, y por inducción en la longitud x, b y y se asocian, de donde $(x, b, y) = 0$. De aquí que $(xb, b, y) = 0$.

A esta igualdad le aplicamos el asociador y obtenemos:

$(xb, b, y) = 0$

$[(xb)b]y - (xb)(by) = 0$

$$(xb)(by) = [(xb)b]y \qquad (\mathbf{3.2.5})$$

Ahora utilizamos esta identidad y desarrollamos como sigue

$$[u_1 \dots u_{r-1}b][bv_2 \dots v_s] = [u_1 \dots u_{r-1}u_r v_1 v_2 \dots v_s] \qquad (\mathbf{3.2.6})$$

Verificación.

$[u_1 \dots u_{r-1}b][bv_2 \dots v_s] = ([u_1 \dots u_{r-1}b]b)[v_2 \dots v_s]$ por identidad (3.2.5)

$= ([u_1 \dots u_{r-1}u_r]v_1)[v_2 \dots v_s]$ sustituyendo b

$= [u_1 \dots u_{r-1}u_r v_1][v_2 \dots v_s]$ utilizando segunda igualdad de (3.2.1)

$= [u_1 \dots u_{r-1}u_r v_1 v_2 \dots v_s]$ utilizando primera igualdad de (3.2.1)

Por tanto, hemos probado $[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s]$ cuando $v_1 \neq v_s$ y $u_r = b$.

Análogamente, si $u_r = c$, escribimos $x = [u_1 \dots u_{r-1}]$, $u_r = c$,

$[v_1 \dots v_{s-1}] = z$, $v_s = c$.

Ahora utilizando la función

$$f(w,x,y,z) = (wx,y,z) - x(w,y,z) - (x,y,z)w$$

La desarrollamos para $f(x,c,z,c)$ y obtenemos

$f(x,c,z,c) = (xc,z,c) - c(x,z,c) - (c,z,c)x = 0$ por ser una función antisimetrica.

Aquí $(c,z,c) = 0$, y por inducción sobre la longitud $(x,z,c) = 0$, de donde $(xc,z,c) = 0$.

A esta última igualdad le aplicamos el asociador y obtenemos:

$(xc,z,c) = 0$

$[(xc)z]c - (xc)(zc) = 0$

$$(xc)(zc) = [(xc)z]c \qquad (\mathbf{3.2.7})$$

Ahora utilizamos esta identidad y desarrollamos como sigue:

$$[u_1 \dots u_{r-1}c][v_1 \dots v_{s-1}c] = [u_1 \dots u_{r-1}u_r v_1 \dots v_{s-1}v_s] \qquad (\mathbf{3.2.8})$$

Verificación.

$[u_1 \dots u_{r-1}c][v_1 \dots v_{s-1}c] = ([u_1 \dots u_{r-1}c][v_1 \dots v_{s-1}])c$ por identidad (3.2.7)

$= ([u_1 \dots u_{r-1}u_r][v_1 \dots v_{s-1}])v_s$ sustituyendo c

$= [u_1 \dots u_{r-1}u_r v_1 \dots v_{s-1}]v_s$ utilizando primera igualdad de (3.2.1)

$= [u_1 \dots u_{r-1}u_r v_1 \dots v_{s-1}v_s]$ utilizando segunda igualdad de (3.2.1).

Por tanto, hemos probado $[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s]$ cuando $v_1 \neq v_s$ y $u_r = c$.

De aquí que (3.2.4), (3.2.6) y (3.2.8) establecen $[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s]$ en todos los casos.

Nota. La inducción sobre r se desarrolla de la misma forma que la inducción sobre s.

Esto prueba la asociatividad de $\boldsymbol{R_1}$, y por tanto la de $\boldsymbol{R}$.

BIBLIOGRAFÍA

HALL, Marshall, JR. Teoría de los Grupos. México, 1973. Editorial Trillas.

DEAN, Richar A. Classical Abstract Algebra. New York, 1990. Editorial Harper & Row, Publishers.

HERSTEIN, I.N. Álgebra Moderna. México, 1980. Editorial Trillas.

PACHECO, Roger y PEREZ, Efrén. El Terorema de Wedderburn para anillos de división finitos. En: Abstraction and Application, Vol. 1, (2009), P. 59-71.