UNIVERSIDAD DE PANAMA
VICERRECTORIA DE INVESTIGACIÓN Y POSTGRADO
PROGRAMA CENTROAMERICANO DE MAESTRÍA EN MATEMÁTICA

PROPUESTA DIDÁCTICA PARA LA ENSEÑANZA DE ALGUNOS CONCEPTOS BÁSICOS DE LA TEORÍA DE GRUPOS

Félix Alberto Rangel Guerrero

Tesis presentada como uno de los requisito para optar al grado de Maestro en Ciencias con Especialización en Matemática Educativa.

Panamá, República de Panamá
1999

T. M

- 9 FEB 2000

Obsequio del Autor

APROBADO POR:

PROF.JOSUE ORTIZ G. M.Sc. .
PRESIDENTE

PROF. ANALIDA ARDILA M.Sc.
MIEMBRO

PROF. EGBERT AGARD M Sc.
MIEMBRO

REPRESENTANTE DE LA VICERRECTORIA
DE INVESTIGACION Y POSTGRADO

FECHA: 30-XI-99

3221573

AGRADECIMIENTO

Quiero agradecer de manera muy especial a Dios Todopoderoso y a la Santísima Virgen María porque gracias a su amor infinito he podido culminar este trabajo

Igualmente, mi agradecimiento al Profesor **Josué Ortíz** por su cooperación e interés en la realización del mismo; y a los Profesores **Guadalupe Castillo**, **Analida Ardila** y **Egbert Agard** por sus valiosas sugerencias

DEDICATORIA

A mis padres, **Juan** y **Fanny**, por su constante apoyo moral.

ÍNDICE

		Páginas
RESUMEN		**1**
INTRODUCCIÓN		**3**
CAPITULO I		**10**
EL CONSTRUCTIVISMO EN EL QUEHACER EDUCATIVO		
1.1	El Constructivismo	**13**
1.2	Etapas del Desarrollo Intelectual	**17**
1 3	Reflexiones Desde el Punto de Vista del Constructivismo para el Proceso de Enseñanza-Aprendizaje	**29**
CAPITULO II		**33**
TEORÍA DE GRUPOS		
2.1	Generalidades de Grupos	**35**
2.2	Subgrupos	**61**
2.3	Homomorfismos	**78**

CAPITULO III

PROPUESTA DIDÁCTICA PARA INTRODUCIR LA TEORÍA DE GRUPOS **108**

CONCLUSIONES **140**

RECOMENDACIONES **141**

BIBLIOGRAFÍA **142**

RESUMEN

En el presente trabajo abordamos el problema de la enseñanza de los conceptos fundamentales de la Teoría de Grupos El énfasis, sin embargo, está puesto en aquellos tópicos que podrían ser incluidos en el curriculum de la educación media. Lo hacemos convencidos de que en los cursos introductorios del álgebra elemental y la geometría puede motivarse al estudiante hacia la adquisición de tales conceptos en una forma natural y sencilla El enfoque que presenta el constructivismo sobre cómo se da el aprendizaje, en el que el estudiante construye el conocimiento y verifica por sí mismo los resultados encontrados, es el utilizado en la propuesta didáctica para introducir la teoría de grupos que se presenta en este trabajo

SUMMARY

Throughout this work we deal with the problem of teaching the fundamental concepts of The Theory of Groups. Nevertheless, we make special emphasis on those topics which could be included within the contents of high school curriculum. We do so convinced that the introductory courses of elemental algebra and geometry may motive students to acquire such concepts in a simple and natural way. We follow the constructivistic point of view, regarding the way people discover and gain knowledge making the learning

process a meaningful experience, to give a proposal about teaching the introductory concepts of group theory.

INTRODUCCIÓN

Al inicio de una carrera universitaria en el área de las ciencias exactas y tecnología los estudiantes se encuentran ante una encrucijada, ya que sus experiencias previas en la escuela secundaria no les han proporcionado la preparación académica requerida, ni les ha permitido lograr el desarrollo de las estructuras de pensamiento necesarias para asimilar los contenidos propuestos en los cursos a nivel superior En otras palabras, en general, los estudiantes de primer ingreso de nuestras universidades no poseen el lenguaje matemático ni han llegado al nivel del pensamiento formal, por lo cual es tan difícil para ellos seguir con éxito el desarrollo de cursos como "Fundamentos de la matemática", "Geometría métrica" y otros que son eminentemente de carácter axiomático. Por todo lo anterior, no es extraño que un gran porcentaje de estos estudiantes se desempeñe pobremente en sus carreras, y peor aún que abandonen las mismas debido a los fracasos. Otro grupo minúsculo, a pesar de estas deficiencias iniciales logrará sobrevivir y terminar la carrera.

El carácter fundamental de la concepción contemporánea de las matemáticas modernas es el de las estructuras algebraicas, por lo cual debería introducirse un poco del espíritu del álgebra moderna desde temprano, es decir en la aritmética y en el álgebra elemental, pero sin recurrir a las teorías

abstractas, sino más bien a través de ejemplos que estén al alcance de los estudiantes, deduciendo las nociones fundamentales De esta manera los alumnos se familiarizarían con las principales estructuras algebraicas, evitando en cierta medida las deficiencias antes mencionadas.

Actualmente en los cursos de aritmética se estudian algunas de estas nociones en forma superficial y mecánica El docente se limita a enseñar lo que presenta el texto; trabaja con el conjunto de los números enteros o con cualquier otro conjunto de números, definiendo las leyes o propiedades que en dicho conjunto se verifican (o se cumplen) de acuerdo a una operación dada.

Lo peor es que los alumnos estudian estas nociones en su primer año de bachillerato por primera y última vez, provocando que al ingresar a la universidad hayan olvidado lo poco que les enseñaron. Pero si dichas nociones las volvieran a ver durante los años subsiguientes en sus cursos de álgebra elemental el resultado sería distinto.

El estudio del álgebra moderna comienza con la noción de ley de composición interna en un conjunto, la cual a dos elementos X y Y del conjunto, hace corresponder un tercero que será designado de una manera

completamente arbitraria. Dicha ley puede ser o no asociativa, conmutativa, admitir un elemento neutro. Este elemento neutro tiene la propiedad de que al componerlo (u operarlo) con cualquier elemento x, a derecha o a izquierda, da otra vez el mismo elemento x, y el mismo suele designarse por la letra e.

Dentro del álgebra hay varias nociones fundamentales, de las cuales la primera es la noción de grupo Esencialmente un grupo es un conjunto en el cual está definida una ley de composición interna. Esta ley debe satisfacer tres propiedades: asociatividad, debe existir un elemento neutro y debe existir un elemento inverso para cada elemento del conjunto, o sea que debe ser posible hacer corresponder, a cada elemento x, un elemento x^{-1}; tal que al componerlo con x, a derecha o a izquierda, de como resultado el elemento neutro Ejemplos de este tipo de estructura algebraica hay muchos; tanto de leyes de composición interna como también de grupos. Aunque lo más probable es que los alumnos nunca se hayan dado cuenta de esta realidad. Un ejemplo no matemático sería pensar en el conjunto de los seres humanos (en condiciones normales), luego tomar del mismo una mujer y un hombre cualesquiera. Entonces, si estos se aparean el resultado será otro ser humano También podemos pensar que la mezcla de dos pinturas de diferentes colores es ley de composición interna en el conjunto que tiene por elementos todos los posibles colores de pintura

Trabajando de esta manera los alumnos avanzarán mejor. Pero, si empezamos por definir conceptos, proponer y demostrar teoremas y dar los ejemplos clásicos, sin dar oportunidad a la creatividad del alumno, lo único que cosecharemos será un alto índice de fracasos y alumnos con lagunas respecto al tema

A cuántos alumnos les pasará por la mente que y^x sea ley de composición interna en el conjunto de los números racionales, donde obviamente X y Y son racionales; que en el mismo conjunto, la media aritmética $\frac{x+y}{2}$, también lo sea. Cuántos percibirán que el conjunto de los polinomios con la adición usual como ley de composición interna constituya un grupo? Casos como estos podrán ser discutidos, obviamente, bajo la supervisión del profesor

La labor del profesor debe estar encaminada a desarrollar cierta destreza de abstracción reflexiva en el alumno, de tal manera que él mismo sea capaz de construir modelos similares. A partir de esto el alumno le encontrará sentido o significado al tema de estudio, provocando una sensación de satisfacción y, el conocimiento adquirido será más duradero. El profesor debe tener presente que su papel no es el de transmitir el conocimiento, sino el de proporcionar los instrumentos para que los alumnos lo construyan a partir de lo que ya saben.

Este trabajo, el cual consta de tres capítulos, lo hemos realizado con el fin de ayudar al docente a introducir las nociones básicas de las estructuras algebraicas en el último año del bachillerato, a través de una propuesta didáctica.

Para dicho propósito nos basamos en la Teoría Constructivista, puesto que la misma hace posible que el alumno construya el conocimiento en forma activa, ayuda al mismo a comparar sus experiencias nuevas con lo que ya conoce, y también, a resolver las diferencias entre lo conocido y lo nuevo. Además, porque crea en el sujeto la abstracción reflexiva, acción que hace posible que su conocimiento se materialice.

Del constructivismo nos ocupamos en el primer capítulo. En el segundo tratamos las nociones básicas necesarias de la Teoría de Grupos. En el último capítulo, el tercero, presentamos la propuesta didáctica sobre grupos, obviamente, a la luz del constructivismo.

Es nuestro anhelo, que este trabajo contribuya a mejorar la calidad de la enseñanza de la matemática en nuestro país y que al mismo tiempo motive a otros a investigar y preparar propuestas cuyo objetivo sea enfocar la enseñanza de aspectos fundamentales de la matemática de difícil comprensión cuando los mismos son impartidos en la forma tradicional expositiva, en la que el docente es el centro del proceso enseñanza-aprendizaje.

CAPITULO I

EL CONSTRUCTIVISMO EN EL QUEHACER EDUCATIVO

El ser humano no ha mostrado únicamente el deseo de aprender, sino que además, ha hecho todo lo posible por averiguar cómo se aprende. Desde tiempos remotos, cierto número de miembros de cada sociedad civilizada ha desarrollado y probado, hasta cierto punto, ideas acerca de la naturaleza del proceso de aprendizaje

A partir del siglo XVII, han surgido teorías más o menos sistemáticas del aprendizaje, en oposición a las ya existentes. Sin embargo, cuando una nueva teoría afecta las normas escolares, únicamente compite con ellas Entonces, las nuevas teorías que se incorporan, son agregadas a las antiguas, y la escena educativa se hace cada vez más confusa Lo más probable es que los docentes en su mayoría, de vez en cuando, hayan adoptado características en conflicto de diversas teorías del aprendizaje, sin percatarse de que son fundamentalmente de naturaleza contradictoria y no pueden armonizar entre sí.

En la didáctica han tenido gran vigencia y arraigo dos corrientes. **la escuela libresca y la doctrina de las facultades.** En la primera el aprendizaje era fundamentado en el contenido y el primer lugar lo ocupaba la **memoria**, es decir el **almacenaje de información**.

En la segunda, la base del método era la **disciplina formal**, el **adiestramiento o entrenamiento**, sin importar el contenido, sino únicamente la forma, con el peligro de trocar operaciones lógicas en meros mecanismos.

Para las teorías contemporáneas del activismo experimental el acto de aprender se considera un hecho activo, un proceso en el cual la conducta es parte fundamental.

Las teorías contemporáneas del aprendizaje podemos reducirlas a tres:

1 **Teorías conexionistas,** las cuales consideran el aprendizaje como el resultado de conexiones entre **estímulos y respuestas**, denominados **respuestas condicionadas** Dentro de estas teorías tenemos el **Conductismo**, el cual analiza la motivación en función de los instintos.

2. **Concepciones cognitivas**, las cuales hacen referencia a las **cogniciones**: percepciones, actitudes, creencias; que posee el sujeto en relación con su entorno, y tratan de fundamentar cómo esas cogniciones dan origen a conductas Entre éstas tenemos la **Gestal o Teoría de las formas**, la cual sostiene que el individuo que aprende recepta una situación planteada por comprensión de las relaciones lógicas de las conexiones entre medios y fines, a lo cual denomina **insigth:** visión o invisión hacia adentro; o comprensión profunda.

3. **La Constructivista**, la cual partiendo de la teoría piagetiana del aprendizaje hace uso de una metodología construida sobre la lógica. Es una teoría del activismo que se basa en el concepto de **operación**: acciones intensas asociativas y reversibles; además, identifica el pensamiento con la acción misma y define la inteligencia como un sistema de operaciones vivientes y actuantes

Las teorías contemporáneas, de una manera u otra, han reencontrado la verdad: la educación es un proceso interior y personal, por lo cual centran su atención en el aprendizaje como cambio o modificación de la conducta.

Existe una diferencia fundamental entre la teoría genética piagetiana y las otras que hemos mencionado. Puesto que éstas resaltan el **producto o resultado** del aprendizaje; mientras que el constructivismo se interesa por el proceso que interiormente vive el individuo que aprende y por los conflictos que se derivan de dicho proceso.

Adherido a corrientes pragmáticas, racionalistas e idealistas, y con un punto de vista tecnisista y mecanisista en la explicación de los fenómenos psíquicos, Piaget, es el fundador de una gran escuela, la cual nos ha legado un

grandioso trabajo de investigación, un minucioso análisis explicativo sobre la génesis del pensamiento como mecanismo de evolución.

1.1. EL CONSTRUCTIVISMO.

Hacia la década de los ochenta comenzó a precisarse, en la investigación de la psicología educativa la llamada segunda revolución cognitiva, es decir, la del constructivismo. De ésta podemos decir que es como un énfasis reciente, que poco a poco ha caracterizado una buena parte de las investigaciones en psicología cognitiva, y que además, tiene implicaciones bastante importantes en la psicología educativa y en los planteamientos de la didáctica sobre cómo se aprende, cómo se adquiere el conocimiento, cómo facitlitar o propiciar en el alumno el aprendizaje y la adquisición del conocimiento, etc.

Los orígenes del constructivismo están ligados con la teoría de los sistemas y de los modelos (que se construyen de la realidad), y con ciertas corrientes del pensamiento psicológico. Pero, el constructivismo más radical supone una epistemología determinada, que postula que no podemos referirnos a la realidad en sí misma, sino a la construcción que a partir de nuestra interacción con el mundo, hemos realizado de ella. No obstante, los antecedentes del constructivismo, en el campo de la psicología, se encuentran en la teoría piagetiana, no tanto en el aspecto más superfluo de la definición y periodización de unas de las fases del desarrollo mental, sino en su visión más profunda de las estructuras mentales que se van integrando paulatinamente en estructuras más complejas, gracias a la actividad cognitiva del sujeto.

El constructivismo es un punto de vista sobre el conocimiento, sobre cómo se adquiere éste y sus relaciones con el desarrollo general de la persona. Habla de una elaboración progresiva del pensamiento, en la cual nunca se llega a un conocimiento absoluto, pues siempre se evoluciona hacia conocimientos más elaborados. El conocimiento es el resultado de una construcción mental producto de la asimilación de estímulos y vivencias del aprendizaje a sus estructuras mentales (Méndez, 1993).

El enfoque del constructivismo es relativista, lo que conocemos no depende solamente de nuestra madurez física y neurológica, sino también del ambiente social y cultural del que procedemos, así como del momento histórico que nos toque vivir. Por ello, la esencia misma del proceso de aprendizaje en el constructivismo reside en el significado que para el alumno tiene un contenido propuesto, el comparar las nuevas experiencias con lo ya conocido y el poder resolver las diferencias entre lo conocido y lo nuevo (Méndez, 1993).

El conocimiento no se debe recibir en forma pasiva, sino que debe construirse activamente por los mismos estudiantes. La actividad mental del sujeto, entendida particularmente como la capacidad de establecer relaciones entre sucesos, ideas o acciones efectuadas previamente por la persona, está a la base del edificio del conocimiento. Piaget (1896-1980) ha llamado a esta acción abstracción reflexiva, la cual está al origen del pensamiento lógico-

matemático; y según la misma, el conocimiento es posible únicamente cuando el sujeto toma consciencia de sus acciones y es capaz de reflexionar sobre ellas.

Por lo tanto, una de las tareas esenciales en la educación es la búsqueda de significado. Las acciones que se toman en el proceso enseñanza-aprendizaje, tanto para el profesor como para el educando, deben tener un sentido, estar insertas en un contexto que corresponda a los antecedentes socio-culturales, motivacionales e intelectuales de unos y otros. La búsqueda de significado es un trabajo que se elabora mentalmente, puesto que debemos construirlos por nosotros mismos, y no transmitirlos como generalmente ocurre.

El constructivismo presenta una teoría psicopedagógica, la cual orienta el proceso de enseñanza-aprendizaje y a la vez impide que haya desperdicio de esfuerzos, que frecuentemente tanto los educadores como los estudiantes experimentan a lo largo de la educación formal. Partiendo del hecho de que el conocimiento se construye y es, además, evolutivo, crea un ambiente de reflexión y de investigación permanente que ha enriquecido el acto educativo.

Entonces, si el sujeto construye el conocimiento, ¿Cuál será el papel del profesor?

En primer lugar debe hacer un esfuerzo por relacionar el desarrollo psicogenético del alumno con el contenido de lo que se va ha enseñar. Además, debe saber qué, cuándo y cómo enseñar un determinado contenido.

Así, por ejemplo, en el álgebra elemental debe tomarse en cuenta la necesidad de que el estudiante conozca las operaciones fundamentales de la aritmética elemental, ya que sin esto las operaciones con expresiones algebraicas no tienen sentido

El profesor debe tener presente, dentro de una concepción constructivista, que el alumno elabora sus conocimientos en una interacción dinámica con el ambiente que lo rodea. En la escuela esto significa que es necesario ir más allá de las ayudas audio-visuales o de la práctica de ejercicios manuales (Piaget, 1971)

Las operaciones mentales derivan de la acción y no de las imágenes Por lo cual, reducir la actividad del educando a la motricidad o a una enseñanza basada en la imagen no es suficiente. Lo fundamental es que el alumno oriente su desarrollo de acuerdo con la evolución de sus estructuras cognoscitivas, mediante el ejercicio de sus mecanismos mentales. Esto es posible sólo cuando se le exige experimentar, resolver problemas o participar en discusiones que hagan posible la reflexión. Por lo tanto, el educador no puede limitarse a planear sus lecciones o clases en función del programa de estudios elaborado por el ministerio de educación Es necesario un conocimiento más amplio de la psicología genética, de los variados niveles estructurales que pueden prevalecer en sus alumnos, una búsqueda constante de situaciones de aprendizaje que promuevan la acción mental del educando. También, debe

convertirse en un permanente investigador, relacionarse con las metodologías de las ciencias sociales y aplicarlas en su tarea pedagógica.

Trabajando de esta forma, tendrá menos problemas de indisciplina, ya que sus alumnos estarán interesados de verdad en las actividades que él les proponga, sin tener que recurrir a las motivaciones externas

El constructivismo promueve una pedagogía integral, en la cual los aspectos intelectuales y socio-afectivos son de igual importancia. Por tal motivo, el profesor seguirá desempeñando una labor importante en el salón de clases, como el creador de un ambiente favorable a un aprendizaje creativo, en el que debe existir una mutua colaboración entre sus alumnos, y que poco a poco se logre el desarrollo total de la autonomía, la inventiva y el potencial intelectual del escolar.

1.2. ETAPAS DEL DESARROLLO INTELECTUAL.

Jean Piaget postula un modelo del desarrollo mental que explica ciertos postulados constructivistas en psicología cognitiva, como por ejemplo: la interacción para la adaptación mental; la construcción permanente y variada de estructuras simbólicas o de significado.

Le interesa el estudio de la elaboración progresiva de las estructuras intelectuales del sujeto, la cual finaliza en el pensamiento formal o hipotético deductivo, alrededor de los 16 años de edad. En todas las etapas del desarrollo del niño, las estructuras intelectuales son distintas; al principio son más concretas, más ligadas a la psicomotrocidad. En su fase final se desligan de lo concreto y alcanzan una síntesis entre el pensamiento, el lenguaje y la capacidad de formalización del adolescente.

El nivel estructural que haya logrado elaborar un individuo, determinará la capacidad adaptiva del mismo Pedagógicamente es importante comprender esto, dado que una misma situación de enseñanza será comprendida y asimilada de distinta manera, de acuerdo con esa variable aptitud.

Es por eso que plasmaremos el desarrollo intelectual del ser humano, según Piaget·

Las estructuras de la inteligencia son el resultado del intercambio activo que el infante realiza con todo lo que le rodea. A partir de estructuras hereditarias muy simples (reflejos neurológicos) el individuo elabora gradualmente: los esquemas de acción, el objeto permanente, las operaciones mentales concretas y luego, las operaciones mentales abstractas. Dicha interacción se realiza de acuerdo a una motivación interior de supervivencia y adaptación, sin necesidad de motivaciones externas.

Algo muy importante son los órganos de los sentidos, pues sin ellos sería imposible ese intercambio del individuo con su ambiente; sin embargo, Piaget asegura que las reacciones de un individuo a un estímulo dado no siempre son las mismas, puesto que éstas dependen de su nivel de desarrollo, de sus experiencias previas y de sus motivaciones

Según Piaget, en el ser humano, el desarrollo intelectual se divide en cuatro etapas sucesivas: la sensomotriz, la preoperatoria, la de las operaciones concretas y la de las operaciones formales.

La etapa **sensomotriz** o de la **inteligencia sensomotriz** se lleva a cabo dentro de los 18 primeros meses de vida y coincide con la evolución psicomotora. Durante la misma el niño se apodera de todo el universo práctico que tiene a su alrededor, valiéndose únicamente de las percepciones y los movimientos. Va adquiriendo una coordinación cada vez más sincronizada entre sus percepciones y sus movimientos corporales, al mismo tiempo supera progresivamente su visión del mundo exterior.

Al término de esta etapa, el niño es capaz de construir la permanencia del objeto, el espacio y el tiempo, como esquemas motores de la acción del propio cuerpo; además, realiza sus primeras experiencias prácticas de causalidad; pero sin representaciones mentales de estos esquemas, es decir que se mantiene a nivel sensomotor.

Durante la segunda etapa, la de la **inteligencia preoperatoria**, el niño adquiere la capacidad de representación mental y, se hace presente la función simbólica: representar unas cosas con otras. Las primeras simbolizaciones se dan en el uso del lenguaje, en los juegos, en la imitación de algo en ausencia del modelo (imitación diferida), y en la explicación de sus sueños. De estas adquisiciones la más importante es el lenguaje, puesto que ésta influirá en las conductas del niño, tanto en lo cognitivo como en lo afectivo.

La etapa preoperatoria se divide en dos periodos: el primero que abarca desde los 18 meses hasta los 4 años, más o menos, **llamado período simbólico o preconceptual,** y el otro, desde los 4 años hasta los 7 años, llamado **período intuitivo.** El periodo preconceptual se caracteriza por la presencia de los preconceptos que se dan en el lenguaje del niño, y por un tipo de razonamiento que va de lo particular a lo particular, llamado **transcuctivo.**

Los preconceptos son esquemas que no tienen ni la generalización del concepto ni la particularidad de los elementos que lo conforman, sino que se colocan entre lo general y lo particular. En cuanto a su manera de asimilación, se sitúa entre el esquema sensomotor y el concepto; y en cuanto a estructura representativa, es semejante al símbolo imaginado. Apreciamos un ejemplo de preconcepto cuando el niño utiliza el término río para referirse a un lago, a una

quebrada, o al mar. También, cuando, después de haber visto pasar un avión, ve otro, el niño dice que es el mismo que vio por vez primera. En este segundo ejemplo se observa la dificultad para distinguir entre un elemento cualquiera de una colección y uno particular, en consecuencia utiliza inadecuadamente los artículos gramaticales **un** y **el**.

El razonamiento transductivo es ni deductivo ni inductivo. El niño no generaliza y su pensamiento no tiene rigor lógico. Por ejemplo, se da el caso del niño que identifica la vida con la autopropulción; es decir que para él la está viva porque se mueve, mientras que una carretilla no lo está por el hecho de que hay que empujarla. Sin embargo, niega que el viento tenga vida, puesto que éste no habla.

El período intuitivo se caracteriza por una coordinación gradual de las relaciones representativas, la cual hace posible que el niño logre alcanzar el umbral de las operaciones. Durante este período tiene lugar un esquematismo prelógico, hay centraciones y descentraciones. Por ejemplo, tenemos el caso del niño que prefiere dos monedas de cinco centésimos a una de diez, debido que centra su atención en el diámetro y no en el valor cuantitativo de las monedas. Pero, si dicho niño, se dirige a la tienda con la moneda de diez y sólo puede comprar seis pastillas de menta, y luego, le ocurre lo mismo al ir con las dos monedas de cinco, entonces empezará a centrar su atención en el valor cuantitativo, antes descuidado. La posibilidad que posee un niño para realizar

varias contracciones, anuncia ya la operación, aunque el sujeto considera las relaciones alternativamente, en vez de multiplicarlas lógicamente, como ha de suceder cuando aparezca la operación.

El pensamiento intuitivo va más allá del pensamiento preconceptual, ya que es una especie de acción ejecutada en pensamiento: ordenar, seriar, desplazar, etc y, además, porque se trata de configuraciones de conjunto y no de simples colecciones sincréticas simbolizadas por ejemplares. El sujeto no alcanza la reversibilidad mental, es decir que, aún no es capaz de volver al punto de partida, de anular una transformación, de percatarse de que mientras no se añade ni se agrega algo no hay modificación de una cantidad, etc. Por ejemplo, siendo B una colección real de bolitas de madera, A una parte de B formada por 10 bolitas oscuras y A' otra parte formada por 3 bolitas claras; al preguntarle a un niño menor de siete años si el todo es más o menos numeroso que la parte A, responderá que A supera a B; puesto que al disociar el todo B en partes, éste todo ya no existe como tal, y lo que quede de B no es más que la otra parte A'.

Este tipo de pensamiento carece de equilibrio ente la asimilación de las cosas a los esquemas mentales y la acomodación de estos esquemas a la realidad. Esta carencia de equilibrio se debe a que el pensamiento intuitivo limita los contornos de lo real sin corregirlo, y además, porque es egocéntrico:

está concentrado, constantemente, en función de la acción que el sujeto realiza en el momento. Por lo tanto para que sea operatorio, el pensamiento , deberá superar el egocentrismo, lo cual se logra gradualmente mediante una consideración cada vez mayor, por parte del sujeto, de los puntos de vista sus semejantes. Así como de otros ángulos de las experiencias vividas. El **fenomenismo perceptual** (imitación de los contornos de lo real sin corregirlo) va cediendo en forma progresiva a una visión más amplia y objetiva del mundo que rodea al sujeto.

Aproximadamente, a partir de los 7 años de edad, las primeras operaciones **lógico-aritméticas** y **espacio-temporales**, comienzan a manifestarse en las reacciones del niño. Es capaz de manejar una estructura de pensamiento, caracterizada por un equilibrio móvil, que gradualmente le permite superar el egocéntrismo y la dependencia perceptual observados en el pensamiento preoperatorio. Esta primera forma de equilibrio dinámico se logra gracias a la **reversibilidad** de las operaciones mentales que, por primera vez, aparecen.

Las **operaciones concretas,** que van desde los 7 años hasta los 12 años, se organizan en sistemas definidos, por Piaget, como **Agrupamientos Operatorios.** Dichas estructuras operatorias de conjunto aparecen en las operaciones lógicas de clasificación y de seriación, cuya construcción

simultánea hace posible la aparición del sistema numérico. Además, en esta etapa se construyen las operaciones espacio-temporales, a través de las cuales el niño logra alcanzar una comprensión adecuada del espacio y el tiempo.

Los agrupamientos operatorios presentan las siguientes condiciones:

C_1. La posibilidad de coordinación de las operaciones. En otras palabras, la coordinación de dos esquemas de acción constituye un nuevo esquema que se añade a los anteriores. En el pensamiento matemático, dos elementos cualesquiera de un grupo se pueden componer entre sí y dar como resultado un elemento del mismo grupo.

C_2 Una coordinación puede realizarse o suprimirse. Es decir que, una acción inteligente (operación) puede desarrollarse en los dos sentidos. En el pensamiento matemático, cada operación directa de un grupo, implica una operación inversa

C_3. Una operación combinada con su inversa se anula, es decir que, el retorno al punto de partida permite volver a encontrar éste sin cambio. Por ejemplo, +5-5=0.

C_4. Se puede alcanzar el mismo punto de llegada por diferentes caminos sin que dicho punto cambie, sin importar el camino elegido. El pensamiento es libre de hacer rodeos y un resultado obtenido por dos caminos diferentes es el mismo. Es como sumar tres números de dos maneras diferentes, (1+2)+3 = 1 + (2+3) = 6.

La aparición de las estructuras operatorias concretas favorece la adaptación social y la superación intelectual del niño; sin embargo, los agrupamientos propios de esta etapa, aun no constituyen una lógica formal que pueda aplicarse a todas las nociones y a todos los razonamientos. Estas estructuras del pensamiento operatorio tienen ciertas limitaciones:

L_1. Limitación en la reversibilidad, la cual es motivada por la característica de separación operatoria que presentan las agrupaciones elementales de clases y relaciones Las clases tienen una forma de reversibilidad denominada **inversión o negación** y las relaciones otra llamada **recíprociproca**, sin embargo, no hay una estructura que las incluya Lo cual implica una menor capacidad para superar la contradicción, estableciendo transformaciones compensadoras.

L_2. Las estructuras del pensamiento operatorio concreto, fuera de las fronteras de lo concreto, son inoperantes. En ellas, lo posible se reduce a una simple prolongación de las acciones aplicadas a un contenido particular.

L_3. Van de dominio en dominio con un desfase temporal, tal como ocurre con la conservación de la materia, peso y volumen, en la que existe un desfase de dos años entre la aparición de una y otra. Es un pensamiento que no es generalizable inmediatamente a todos los contenidos.

L_4. Hay dificultad en el sujeto al momento de formular una hipótesis de trabajo que lo oriente en la búsqueda de la solución de un problema Por lo general, el niño, se lanza de inmediato a la acción y a resolver el problema por tanteos, mediante ensayo y error.

Si se desea adaptar la enseñanza a los resultados de la psicología del desarrollo por oposición al logicismo de la escuela tradicional, hay un punto importante que resaltar, tanto para la teoría de la inteligencia como para las aplicaciones pedagógicas· Los mismos niños que llegan a las operaciones ya descritas, por lo general se muestran incapaces en cuanto dejan de manipular los objetos y se les convida a razonar por medio de simples proposiciones verbales.

Las operaciones tratadas aquí son, en efecto, operaciones concretas y no formales: están constantemente ligadas a la acción, la cual queda estructurada lógicamente por esas operaciones, comprendidas las palabras que la acompañan; sin embargo, no implican, en modo alguno, que sea posible construir un discurso lógico independientemente de la acción.

Durante la última etapa, la de las **operaciones formales,** que se inicia, aproximadamente, a los 12 años y finaliza alrededor de los 16 años, el sujeto ya no está obligado a razonar directamente sobre los objetos concretos, sino que es capaz de hacer deducciones en forma operacional a partir de simples

hipótesis enunciadas verbalmente, lo que se conoce como la **lógica de las proposiciones.**

La combinatoria y el **grupo de las dos reversibilidades** (entre la operación idéntica y negativa, y entre la recíproca y correlativa) son los principales rasgos característicos de las operaciones formales

La combinatoria de las operaciones formales se da de dos maneras complementarias entre sí: combinar objetos o combinar juicios. En cuanto a objetos, dicha combinatoria se observa en la capacidad del sujeto para combinar sistemáticamente y de cualquier manera posible, tarjetas de colores o con números, etc. En lo referente a juicios, la combinatoria se expresa por medio de las operaciones proposicionales; por ejemplo, la implicación, la disyunción, la conjunción, etc. El grupo de las dos reversibilidades se observa en la capacidad del adolescente para relacionar las operaciones de inversión o negación con la recíproca. Así, cada operación posee una inversa y una recíproca. Por ejemplo, si vertimos agua en un cuba vacío, y luego, colocamos dentro cierta cantidad de ladrillos, el adolescente podrá anticipar y coordinar la acción del peso que hace subir el nivel del agua (operación idéntica I), la acción inversa consiste en retirar los ladrillos (operación de negación **N**) con la operación recíproca R (resistencia del líquido, en caso de que el agua se sustituya por otro más denso).

El razonamiento que el adolescente pude hacer es el siguiente:

1º Operación idéntica I. El peso de los ladrillos hace subir el nivel del agua

2º Operación inversa o negativa **N**. Al retirar los ladrillos el nivel del agua baja

3º Operación recíproca **R.** Con un líquido más denso, y con el peso de un ladrillo, el nivel del liquido baja tanto que no podrá alcanzar el que tenía en el agua.

4º Operación correlativa **C.** Con un líquido menos denso que el agua y con el peso de los ladrillos, el nivel subirá mucho más que el que tenía con el agua

La síntesis final de los sistemas parciales o agrupamientos construidos en el estadio de las operaciones concretas es el grupo de las cuatro transformaciones **INRC,** puesto que reúne en una misma organización total las inversiones y las reciprocidades separadas hasta ese momento.

En conclusión, Piaget, llama al pensamiento del adolescente **pensamiento hipotético-deductivo,** puesto que el individuo está en capacidad de razonar sobre simples suposiciones, sin necesidad de una relación con la realidad o con las creencias del sujeto, confiado en la necesidad del razonamiento, por oposición a la concordancia de las conclusiones con las experiencias. Explica que el adolescente razona sobre los mismo scontenidos operatorios: el problema radica en clasificar, seriar, enumerar, medir, situar o

desplazar en el tiempo o en el espacio. Pero estas acciones no se podrán agrupar por las operaciones formales. lo serán las posiciones que expresan esas operaciones (Méndez, 1993).

1.3. REFLEXIONES DESDE EL PUNTO DE VISTA DEL CONSTRUCTIVISMO PARA EL PROCESO DE ENSEÑANZA-APRENDIZAJE.

Las investigaciones sobre, cómo los niños construyen la lengua oral y la lengua escrita, con intervenciones de los maestros contrarios a las propuestas convencionales, constituyen una vía constructivista interesante que todavía está en elaboración . En ese punto son muy prometedoras las investigaciones que se están realizando actualmente. Sin embargo, no podemos olvidar que no toda propuesta cognitiva es constructivista. Por otro lado, aunque no es posible dar normas o reglas estrictas y mucho menos pasos sucesivos para la enseñanza constructivista, sí es posible establecer algunos principios o recomendaciones que se están promoviendo con cierta flexibilidad al investigar en áreas como la enseñanza de las matemáticas, la enseñanza de la física y, en un grado menor en la enseñanza de la historia.

Es peligroso llegar demasiado rápido a proponer pasos exactos y secuencias precisas que acabarían por completo con el espíritu de la enseñanza constructivista Pero, también se corre el peligro de que el constructivismo sea considerado como una simple teoría que no es capaz de

hacer propuestas prácticas. Por estas razones exponemos ciertas reflexiones desde el punto de vista del constructivismo para guiar y no para repetir durante un proceso de enseñanza aprendizaje (Torres, 1992):

1. Guiar a los escolares para que reflexionen sobre su propio entorno y puedan crear modelos (o ejemplos) que les funcionen. Por ejemplo, en el caso del concepto de grupo, ayudarlos a que reflexionen sobre lo que ya conocen, y puedan entonces construir colectivamente nuevos ejemplos.
2. Es muy probable que al reflexionar sobre su propio entorno, los estudiantes construyan modelos que según el docente no son los más correctos, entonces lo más acertado es convencerlos, sin argumentaciones, encontrando un caso donde el modelo no funcione (falsación), es decir dar un contra-ejemplo. Luego, dejarlos que vuelvan a elaborar modelos y así sucesivamente. Entonces los alumnos verán los modelos de los libros y los proporcionados por el profesor como propuestas que deben ser sometidas al mismo procedimiento: intentar falsearlos
3. No cometer el error de querer diagnosticar la etapa de desarrollo intelectual de los alumnos o suponer en qué etapa deberían estar y luego proponer experiencias de aprendizaje en función de la etapa de desarrollo. Lo que debemos hacer es utilizar el método de entrevista por medio de actividades concretas, con lo cual se demuestra que los

alumnos construyen explicaciones (o modelos) al paso que se les va entrevistando sobre los fenómenos físicos, sociales, biológicos o psicosociales. Lo importante radica en que al entrevistar, únicamente, no estamos detectando, sino construyendo o ayudando a construir nuevas estructuras. Es decir que, las entrevistas, las encuestas o cualquier forma de diálogo no sólo son para observar, sino sobre todo para participar o contribuir en la construcción de nuevas estructuras de asimilación. Todo el que investiga construye lo que está investigando en función de sus técnicas, de sus preguntas y sus interpretaciones. Por lo tanto, no hay observación objetiva, sino participación en la naturaleza del objeto estudiado.

4. Fomentar la autonomía moral y cognitiva entre los alunamos; enseñar a partir de problemas que tengan significado o sentido para los escolares.

   Utilizar una pedagogía del error en cuanto el mismo no debe corregirse como algo indebido, sino tratado como etapas normales en las construcciones que realizan los alumnos.

   Promover en los alumnos la realización de proyectos vitales de carácter colectivo en su entorno; sumergir a los alumnos desde un principio en un ambiente donde los conocimientos que deben enseñarse sean requeribles para él

   Diagnosticar los problemas, las necesidades, intereses y recursos del entorno donde se va a enseñar, revisar y emplear con fines didácticos y

de análisis la historia del tema para ver su construcción colectiva en diferentes situaciones y momentos del desarrollo científico o tecnológico.

Presentar a los alumnos las teorías o explicaciones únicamente después que hayan elaborado algunas alternativas y vean las de las ciencias como otras opciones que tienen los mismos procedimientos de falsación.

Hacer hincapié en que los alumnos y los científicos no descubren verdades, sino que lo que hacen es construir modelos y conjeturas.

Reiterar que construir no es crear de la nada, sino elaborar a partir de los contenidos proporcionados, incluyendo los ya elaborados, los cuales deben ser vistos como materia para volver a construir.

5. Un docente constructivista debe tener una actitud particular ante la ciencia y ante las construcciones espontáneas de sus alumnos; debe pensar que los conocimientos elaborados por la humanidad son propios de una época determinada y que al alumno le sucede lo mismo.

CAPITULO II

TEORÍA DE GRUPOS

Los pilares fundamentales, sobre los cuales descanza el edificio matemático, son las estructuras algebráicas, cuyo prototipo es el grupo. El mismo es un sistema algebráico en el que esta definida una sola operación; la cual debe ser ley de composición interna y asociativa, debe incluir la posibilidad de dejar invariante cualquier elemento al combinarlo con cierto elemento de efecto nulo, y por último, debe ser reversible, es decir que, garantice la existencia del inverso de cada elemento.

Las primeras nociones expuestas sobre la Teoría de Grupos son fruto del genio matemático francés Evariste Galois (1811-1832), quien escribió sus valiosas ideas a la edad de 18 años. Pero, no fue sino tres años más tarde, la noche antes de su muerte, cuando su ferviente amor a la matemática se desborda y transcribe en breves líneas sus ideas fundamentales (sin demostraciones) insistiendo que poseía la demostración de todo. Su trabajo permitió generalizar la resolución de ecuaciones algebraicas Sin embargo, fue necesario que transcurrieran varias décadas para que sus ideas fueran reconocidas.

A mediados del siglo XIX esta teoría fue desarrollada por grandes matemáticos, entre ellos cabe mencionar a Augustin Luis Cauhy (1789-1857), Sir Arthur Cayley (1821-1895), Camille Jordan (1838-1922), Ludwing Sylow (1832-1918), y Marius Sophus Lie (1842-1899). Es notorio el hecho de que,

gracias a esta teoría, se ha logrado una unificación muy marcada en la matemática entre partes del Algebra y la Geometría, las cuales se consideraron por mucho tiempo diferente y no relacionadas. En el próximo capítulo veremos como es posible desarrollar la Teoría de Grupos utilizando la Geometría.

2.1. GENERALIDADES DE GRUPOS.

Definición 2.1:

Sea G un conjunto no vacio. Llamaremos ley de composición interna (u operación binaria) en G a aquella ley que aplicada a dos elementos cualesquiera de G da como resultado otro elemento del mismo conjunto.

Dicho formalmente, una ley de composición interna en G es una función definida por.

$$* : G \times G \rightarrow G$$

$$(x, y) \rightarrow x * y.$$

Ejemplo 2 1.

Tomemos el conjunto $Z^+ = \{ n \in Z \ / \ n > o \}$ Entonces, si $a, b \in Z^+$ implica que $a > 0$ y $b > 0$.

Sumando estas desigualdades, miembro a miembro, obtenemos que $a + b > 0$. Es decir que, $(a+b) \in Z^+$

Por lo tanto, al definir la función

$$+ : Z^+ \times Z^+ \rightarrow Z^+$$

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

obtenemos una ley de composición interna en Z^+

En general, la adición es ley de composición interna en los conjuntos Z, Q, R, C. En cambio la división no es ley de composición interna en Z^+, ya que el cociente $1 \div 2$ no tiene solución en Z^+

Ahora consideremos el conjunto A = { 1,2,3 } y definamos sobre él las funciones I, ϕ y ψ de la manera siguiente:

$I(1) = 1$	$\phi(1) = 2$	$\psi(1) = 2$
$I(2) = 2$	$\phi(2) = 1$	$\psi(2) = 3$
$I(3) = 3$	$\phi(3) = 3$	$\psi(3) = 1$

y calculemos $\phi \circ \psi$, $\psi \circ \phi$ y ψ^2 donde **o** es la compuesta usual de funciones:

$(\phi \circ \psi)(1) = 1$ $(\psi \circ \phi)(1) = 3$ $(\psi \circ \psi)(1) = 3$

$(\phi \circ \psi)(2) = 3$ $(\psi \circ \phi)(2) = 2$ $(\psi \circ \psi)(2) = 1$

$(\phi \circ \psi)(3) = 2$ $(\psi \circ \phi)(3) = 1$ $(\psi \circ \psi)(3) = 2$

Llamaremos S_3 al conjunto cuyos elementos son $I, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2$

Es decir que,

$$S_3 = \{I, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$$

Comprobemos que **o** es ley de composición interna en S_3:

$I \circ I = I$ $I \circ (\phi \circ \psi) = \phi \circ \psi$

$I \circ \phi = \phi$ $I \circ (\psi \circ \phi) = \psi \circ \phi$

$I \circ \psi = \psi$ $I \circ \psi^2 = \psi^2$

$\phi \circ I = \phi$ $\phi \circ (\phi \circ \psi) = \psi$

$\phi \circ \phi = I \ . \ \phi^2 = I$ $\phi \circ (\psi \circ \phi) = \psi^2$

$\phi \circ \psi = \phi \circ \psi$ $\phi \circ \psi^2 = \psi \circ \phi$

$\psi \circ I = \psi$ $\psi \circ (\phi \circ \psi) = \phi$

$\psi \circ \phi = \psi \circ \phi$ $\psi \circ (\psi \circ \phi) = \phi \circ \psi$

$\psi \circ \psi = \psi^2$ $\psi \circ \psi^2 = I \ldots \psi^3 = I$

- $(\phi \circ \psi) \circ I = \phi \circ \psi$ $\quad (\phi \circ \psi) \circ (\phi \circ \psi) = I$.. $(\phi \circ \psi)^2 = I$

  $(\phi \circ \psi) \circ \phi = \psi^2$ $\quad (\phi \circ \psi) \circ (\psi \circ \phi) = \psi$

  $(\phi \circ \psi) \circ \psi = \psi \circ \phi$ $\quad (\phi \circ \psi) \circ \psi^2 = \phi$

- $(\psi \circ \phi) \circ I = \psi \circ \phi$ $\quad (\psi \circ \phi) \circ (\phi \circ \psi) = \psi^2$

  $(\psi \circ \phi) \circ \phi = \psi$ $\quad (\psi \circ \phi) \circ (\psi \circ \phi) = I$ $\quad (\psi \circ \phi)^2 = I$

  $(\psi \circ \phi) \circ \psi = \phi$ $\quad (\psi \circ \phi) \circ \psi^2 = \phi \circ \psi$

- $\psi^2 \circ I = \psi^2$ $\quad \psi^2 \circ (\phi \circ \psi) = \psi \circ \phi$

  $\psi^2 \circ \phi = \phi \circ \psi$ $\quad \psi^2 \circ (\psi \circ \phi) = \phi$

  $\psi^2 \circ \psi = I$ $\quad \psi^2 \circ \psi^2 = \psi$

Por lo tanto,

$$\circ : S_3 \times S_3 \to S_3$$

$$(x, y) \to x \circ y$$

es ley de composición interna en S_3

A continuación confeccionaremos una tabla en base a los resultados que acabamos de obtener, la cual nos será útil más adelante:

o	I	ϕ	ψ	$\phi \circ \psi$	$\psi \circ \phi$	ψ^2
I	I	ϕ	ψ	$\phi \circ \psi$	$\psi \circ \phi$	ψ^2
ϕ	ϕ	I	$\phi \circ \psi$	ψ	ψ^2	$\psi \circ \phi$
ψ	ψ	$\psi \circ \phi$	ψ^2	ϕ	$\phi \circ \psi$	I
$\phi \circ \psi$	$\phi \circ \psi$	ψ^2	$\psi \circ \phi$	I	ψ	ϕ
$\psi \circ \phi$	$\psi \circ \phi$	ψ	ϕ	ψ^2	I	$\phi \circ \psi$
ψ^2	ψ^2	$\phi \circ \psi$	I	$\psi \circ \phi$	ϕ	ψ

Tabla 2 1

Definición 2.2

Llamaremos grupoide a un conjunto no-vacio G provisto de una ley de composición interna $*$, el cual denotaremos por el par $(G, *)$

Ejemplo 2 2

$(Z^+, +)$ es un grupoide, puesto que + es ley de composición interna en Z^+. Otros grupoides son $(S_3, \circ)$, $(Z, +)$, $(R, \bullet)$, etc.

Definición 2 3

Si en un grupoide $(G, *)$ se cumple que para cualesquiera $x, y, z \in G$

$$(1)\ (x * y) * z = x * (y * z),$$

entonces diremos que $*$ es asociativa, y a $(G, *)$ lo llamaremos semigrupo.

Ejemplo 2 3

Tenemos que $(-5 + 3) + 4 = -5 + (3 + 4)$

$$-2 + 4 = -5 + 7$$

$$2 = 2.$$

Más aun, se puede demostrar que en general la igualdad (1) se cumple para cualquier elección de números enteros x, y, z. Es decir que, en (Z,+) la ley + es asociativa. Lo mismo ocurre en $\mathbb{Q}$, $\mathbb{R}$ y C.

Luego, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(C, +)$ son semigrupos.

Es fácil verificar que (S_3, o) y $(R, \bullet)$ son semigrupos, lo cual dejaremos al lector como ejercicio.

Por otro lado, en (S_3, o) el elemento I deja invariante a todos los elementos de S_3, bien sea operando a izquierda o a derecha (ver Tabla 2.1). Es decir que,

$$I \circ I = I$$

$$I \circ \phi = \phi = \phi \circ I$$

$$I \circ \psi = \psi = \psi \circ I$$

$$I \circ (\phi \circ \psi) = \phi \circ \psi = (\phi \circ \psi) \circ I$$

$$I \circ (\psi \circ \phi) = \psi \circ \phi = (\psi \circ \phi) \circ I$$

$$I \circ \psi^2 = \psi^2 = \psi^2 \circ I$$

Este hecho nos sirve para definir lo siguiente.

Definición 2.4:

Sea (G, $*$) un semigrupo y $e \in G$. Llamaremos a e elemento neutro o elemento identidad si para todo $x \in G$ se tiene que

$$e * x = x = x * e \quad (2).$$

Definición 2.5·

Llamaremos monoide a todo semigrupo que posea elemento neutro. En otras palabras, un monoide (G, $*$) es un semigrupo en el cual existe $e \in G$ que verifica la igualdad (2).

Ejemplo 2.5:

Son monoides los semigrupos (S_3 , o) , ($\mathbb{R}$, +) y ($\mathbb{R}$, •) cuyos elementos neutros son I, 0 y 1, respectivamente

En $(Z^{+}, +)$ no hay elemento neutro, puesto que el único número que deja invariantes a los números enteros (con la adición) es el cero; es decir que, para cualquier $x \in Z$, $0 + x = x = x + 0$, pero $0 \notin Z^{+}$

Luego, $(Z^{+}, +)$ no es monoide

Proposición 2.1:

En todo monoide el elemento neutro es único

Demostración:

Sea $(G, *)$ un monoide y $e \in G$ el elemento neutro. Supongamos que en G existe otro elemento neutro e_1.

Luego, como e es el neutro, $e * e_1 = e_1$ (I)

Además, puesto que e_1 es neutro, $e * e_1 = e$ (II)

Entonces, igualando (I) y (II), $e_1 = e$.

Por lo tanto, el elemento neutro es único.

Por otra parte, según la Tabla 2.1 correspondiente al monoide (S_3, o), podemos comprobar que:

$$I \circ I = I^2 = I$$

$$\phi \circ \phi = \phi^2 = I$$

$$(\phi \circ \psi) \circ (\phi \circ \psi) = (\phi \circ \psi)^2 = I$$

$$(\psi \circ \phi) \circ (\psi \circ \phi) = (\psi \circ \phi)^2 = I$$

$$\psi \circ \psi^2 = \psi^2 \circ \psi = I.$$

Observamos que a cada elemento de S_3 se puede asociar, de manera única, un elemento de modo que la composición de los dos, en cualquier oreden, produzca el elemento ıdentidad. Cuando ésto ocurre decimos que los elementos son inversos entre sí: ψ es el inverso de ψ^2 y viceversa; mientras que $I, \phi, \phi \circ \psi$ y $\psi \circ \phi$ son sus propios inversos, respectivamente.

Definición 2.6:

Sea $(G, *)$ un monoide y $x \in G$. Llamaremos a $x^{-1} \in G$ inverso de x si y sólo sı $x * x^{-1} = e = x^{-1} * x$ (3).

Definıción 2 7:

Llamaremos grupo al monoide $(G, *)$, en el cual para cada $x \in G$ existe su inverso $x^{-1} \in G$

Ejemplo 2.7:

En (S_3, o) tenemos que

$$I^{-1} = I$$

$$\phi^{-1} = \phi$$

$$\psi^{-1} = \psi^2$$

$$(\phi \circ \psi)^{-1} = \phi \circ \psi$$

$$(\psi \circ \phi)^{-1} = \psi \circ \phi$$

$$(\psi^2)^{-1} = \psi$$

Luego, concluimos que (S_3, o) es un grupo. El mismo es conocido comunmente como el grupo de permutaciones de orden 6.

En éste grupo es fácil verificar que $\phi \circ \psi = \psi^{-1} \circ \phi$ (I).

En efecto,

$\psi^{-1} \circ \phi = \psi^2 \circ \phi$, $\psi^{-1} = \psi^2$

$= (\psi \circ \psi) \circ \phi$, Tabla 2.1.

$= \psi \circ (\psi \circ \phi)$, asociando

$= \phi \circ \psi$, por la Tabla 2.1.

Utilizando éste resultado verifiquemos que $\psi \circ (\phi \circ \psi) = \phi$.

$\psi \circ (\phi \circ \psi) = \psi \circ (\psi^{-1} \circ \phi)$, por lo anterior (i).

$= (\psi \circ \psi^{-1}) \circ \phi$, asociando.

$= I \circ \phi$, propiedad de los inversos

$= \phi$, propiedad del neutro.

También es interesante el siguiente resultado:

$(\phi \circ \psi) \circ (\psi \circ \phi) = \phi \circ [\psi \circ (\psi \circ \phi)]$, asociando

$= \phi \circ [(\psi \circ \psi) \circ \phi)]$, asociando

$= \phi \circ (\psi^2 \circ \phi)$, Tabla 2.1.

$= \phi \circ (\psi^{-1} \circ \phi)$, $\psi^{-1} = \psi^2$

$= \phi \circ (\phi \circ \psi)$, por (i).

$= (\phi \circ \phi) \circ \psi$, asociando

$= \phi^2 \circ \psi$, Tabla 2 1.

$= I \circ \psi$, Tabla 2.1.

$= \psi$, propiedad del neutro

Por otro lado, como el número cero no posee inverso respecto a la multiplicación usual en Q, entonces $(Q, \bullet)$ no es grupo. Es decir que, no existe $x \in Q$ tal que $o \bullet x = 1 = x \bullet o$.

Pero, si tomamos el conjunto $Q^* = Q - \{o\}$, entonces $(Q^*, \bullet)$ sí es grupo. Puesto que, para cualquier $a/b \in Q^*$, existe $b/a \in Q^*$ tal que

$a/b \bullet b/a = 1 = b/a \bullet a/b$.

Proposición 2.2:

En todo grupo el inverso de un elemento es único.

Demostración:

Sea $(G, *)$ un grupo y $x \in G$.

Luego, existe $x^{-1} \in G$ tal que $x * x^{-1} = e = x^{-1} * x$.

Supongamos que $b \in G$ también es inverso de x

Entonces, $b = b * e$, por propiedad del neutro.

$= b * (x * x^{-1})$, propiedad de los inversos.

$= (b * x) * x^{-1}$, asociando.

$= e * x^{-1}$, propiedad de los inversos.

$= x^{-1}$, propiedad del neutro

Luego, $b = x^{-1}$.

Por lo tanto, el inverso de cada elemento es único.□

Otro ejemplo de grupo es $(Z, +)$, puesto que:

- La adición de dos números enteros a y b, da como resultado otro número entero. Es decir que, si $a, b \in Z$, entonces $(a + b) \in Z$.
- La adición es asociativa.
- Existe el número $0 \in Z$, tal que $0 + a = a = a + 0$, para cualquier $a \in Z$. En otras palabras, existe el neutro.

Finalmente, para cualquier $a \in Z$, existe $-a \in Z$, tal que:

$a + (-a) = 0 = -a + a$. En el caso de la adición se habla de elemento simétrico en vez de elemento inverso, puesto que el concepto de inverso es propio de la multiplicación.

Lema 2.1.

Si $(G, *)$ es un grupo, entonces

i) Para cada $a \in G$, $(a^{-1})^{-1} = a$.

ii) Para cualesquiera $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.

iii) Si $a, b, x \in G$ se cumple que:

(1) $a * x = b * x \Rightarrow a = b$

(2) $x * a = x * b \Rightarrow a = b$

iv) Si $a, b, x \in G$, entonces las ecuaciones

(3) $a * x = b$

(4) $x * a = b$

tienen una única solución x en G.

Demostración.

Sea $(G, *)$ un grupo y $a, b, x \in G$.

i) Como $a \in G$, entonces existe $a^{-1} \in G$ tal que $a^{-1} * a = e$.

Además, como $a^{-1} \in G$, existe $(a^{-1})^{-1} \in G$, inverso de a^{-1}.

Luego, $(a^{-1})^{-1} * a^{-1} = e$, por propiedad de los inversos.

$[(a^{-1})^{-1} * a^{-1}] * a = e * a$, operando con a a derecha

$(a^{-1})^{-1} * (a^{-1} * a) = e * a$, asociando

$(a^{-1})^{-1} * e = e * a$, por propiedad de los inversos.

$(a^{-1})^{-1} = a$, por propiedad del neutro.

Por lo tanto, $(a^{-1})^{-1} = a$ para cada $a \in G$.

ii) Como $a,b \in G$, entonces existen $a^{-1}, b^{-1} \in G$.

Además, dado que el inverso de $a * b$ es $(a * b)^{-1}$, entonces nos queda por probar que $b^{-1} * a^{-1}$ es inverso de $a * b$.

En efecto,

$(a*b) * (b^{-1} * a^{-1}) = a * (b*b^{-1}) * a^{-1}$, asociando.

$= a * e * a^{-1}$, por propiedad de los inversos

$= (a * e) * a^{-1}$, asociando

$= a * a^{-1}$, por propiedad del neutro.

$= e$, por propiedad de los inversos.

Ahora,

$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$, asociando

$= b^{-1} * e * b$, por propiedad de los inversos.

$= b^{-1} * e$, por propiedad del neutro

$= e$ por propiedad de los inversos

Por lo tanto, $(a * b)^{-1} = b^{-1} * a^{-1}$ para cualesquiera $a,b \in G$.

iii) Como $x \in G$, , existe su inverso $x^{-1} \in G$.

(1) Si $a * x = b * x$, entonces

$(a * x) * x^{-1} = (b * x) * x^{-1}$, operando a derecha con x^{-1}.

$a * (x * x^{-1}) = b * (x * x^{-1})$, asociando.

$a * e = b * e$, por propiedad de los inversos.

$a = b$, por propiedad del neutro.

Ahora, si $x * a = x * b$, entonces

$x^{-1} * (x * a) = x^{-1} * (x * b)$, operando a izquierda con x^{-1}.

$(x^{-1} * x) * a = (x^{-1} * x) * b$,asociando.

$e * a = e * b$,por propiedad de los inversos.

$a = b$,pro propiedad del neutro.

Ambos resultados conforman lo que se conoce como ley cancelativa.

Finalmente,

iv) Dado que $a \in G$, existe su inverso $a^{-1} \in G$.

En (3) tenemos que $a * x = b$.

$a^{-1} * (a * x) = a^{-1} * b$,operando a izquierda con a^{-1}.

$(a^{-1} * a) * x = a^{-1} * b$,asociando

$e * x = a^{-1} * b$,por propiedad de los inversos

$x = a^{-1} * b$,por propiedad del neutro

Luego, la solución de (3) es $x = a^{-1} * b$

Unicamente nos resta probar su unicidad

En efecto, supongamos que $x_1 \in G$ es solución de (3), entonces $a * x_1 = b$

Igualando éste último resultado con (3) obtenemos que

$a * x_1 = a * x$, y por la ley cancelativa, $x_1 = x$

Por lo tanto, la solución de (3) es única

La solución de (4) es similar, la dejamos al lector cómo ejercicio

Definición 2 8

Si (G, *) es un grupo tal que $a * b = b * a$, para cualesquiera $a,b \in G$ Entonces, llamaremos a (G, *) grupo conmutativo o grupo abeliano

Ejemplo 2.8

Los grupos (R , +) y (R*, •) son abelianos, puesto que tanto la adición como la multiplicación usuales son conmutativas.

Sin embargo, (S_3, o) no es abeliano, dado que $\phi \circ \psi \neq \psi \circ \phi$

Definición 2.9.

Si (G, *) es un grupo compuesto de un número finito de elementos, lo llamaremos grupo finito, y al número de sus elementos, orden del grupo, el cual denotaremos por o (G).

Ejemplo 2 9

El grupo (S_3, o) se compone de seis elementos, por tanto es finito, y su orden es o (S_3) = 6

Definición 2 10

Si (G, *) es un grupo y $n \in Z$, entonces las potencias de $a \in G$ quedan definidas así

$$a^n = \begin{cases} e & ,si \quad n = 0 \quad (i) \\ a & ,si \quad n = 1 \quad (ii) \\ a^{n-1} * a & ,si \quad n > 0 \quad (iii) \\ (a^{-1})^{-n} . & ,si \quad n < 0 \quad (iv) \end{cases}$$

Proposición 2.3:

Si $(G, *)$ es un grupo, $a \in G$ y $n \in Z$. Entonces $a^n = (a^{-1})^{-n}$.

Demostración:

Sean $(G, *)$ un grupo, $a \in G$ y $n \in Z$

- Por la defínción 2.10, $a^n = (a^{-1})^{-n}$ para $n < 0$.
- Ahora, si $n = 0$, entonces, por la definición 2 10, tenemos que

$a^0 = e$ y $(a^{-1})^0 = e$

Así, para $n = 0$, $a^n = (a^{-1})^{-n} = e$.

- Finalmente, si $n > 0$, entonces $-n < 0$.

Luego, $(a^{-1})^{-n} = [(a^{-1})^{-1}]^{-(-n)}$,por definición 2 10, (iv)

$= a^n$,por el Lema 2 1

Así, $a^n = (a^{-1})^{-n}$ para $n > 0$

Por lo tanto, concluimos que $a^n = (a^{-1})^{-n}$ para $n \in Z$.□

Proposición 2.4:

Si $(G,*)$ es un grupo, $a \in G$ y $n \in Z$. Entonces $a^{n+1} = a^n * a$

Demostración

Sean $(G, *)$ es un grupo, $a \in G$ y $n \in Z$.

- Iniciemos con $n = 0$

Entonces, $a^{n+1} = a^{0+1}$

$= a^1$,propiedad del neutro en (Z , +).

$= a$,por definición 2.10, (ii).

$= e * a$,por propiedad del neutro en G.

$= a^0 * a$, por definición 2.10 (i).

Así, $a^{n+1} = a^n * a$ para $n = 0$

– Ahora continuemos con $n > 0$.

Si $n > 0$, entonces $n + 1 > 0$.

Luego, $a^{n+1} = a^{(n+1)-1} * a$,por definición 2.10, (iii)

$= a^{n+(1-1)} * a$,asociando

$= a^{n+0} * a$,propiedad de inversos en (Z , +)

$= a^n * a$,propiedad del neutro en (Z , +).

Así, $a^{n+1} = a^n * a$ para $n > 0$.

Por último, consideremos $n < 0$

– Si $n = -1$, $a^{n+1} = a^{-1+1}$

$= a^0$,por propiedad de los inversos en (Z , +)

$= e$,por definición 2 10, (i).

$= a^{-1} * a$,por propiedad de los inversos en G

$= a^n * a$,$n = -1$

Así, $a^{n+1} = a^n * a$ para $n = -1$.

– Finalicemos con $n < -1$

Entonces, $n < -1$ implica que $-n > 1 > 0$ y $n + 1 < 0$.

Luego, $a^{n+1} = (a^{-1})^{-(n+1)}$,por definición 2 10, (iv).

$= (a^{-1})^{-(n+1)} * e$,por propiedad del neutro en G

$= (a^{-1})^{-(n+1)} * (a^{-1} * a)$,por propiedad de los inversos en G.

$= [\ (a^{-1})^{-(n+1)} * (a^{-1})\ ] * a$,por asociatividad en G.

$= (a^{-1})^{-(n+1)+1} * a$,por definición 2.10, (iii).

$= (a^{-1})^{-n+(-1+1)} * a$,por asociatividad en (Z , +)

$= (a^{-1})^{-n+0} * a$,por propiedad de los inversos en (Z , +)

$= (a^{-1})^{-n} * a$,por propiedad de neutro en (Z , +)

$= a^n * a$,por la proposición 2.3

Así, $a^{n+1} = a^n * a$ para $n < -1$.

Por lo tanto, concluimos que $a^{n+1} = a^n * a$ para $n \in Z$.□

Proposición 2.5:

Si (G, *) es un grupo, $a \in G$ y n,m, $\in$ Z . Entonces $a^{n+m} = a^n * a^m$.

Demostración.

Sea (G, *) un grupo, $a \in G$ y n,m, $\in$ Z.

– Empecemos con $n = m = 0$.

Entonces, $a^n * a^m = a^0 * a^0$

$= e * e$, por definición 2.10, (i).

$= e$, propiedad del neutro en G.

$= a^0$, por definición 2.10, (i)

$= a^{0+0}$, propiedad del neutro en $(Z , +)$

$= a^{n+m}$, $n = m = 0$

Así, $a^{n+m} = a^n * a^m$ para $n = m = o$

– Consideremos $n \in Z$ y $m \in Z^+$

$m = 1$, $a^{n+m} = a^{n+1}$

$= a^n * a$, por la proposición 2 4

$= a^n * a^1$, por definición 2.10, (ii)

$= a^n * a^m$, $m = 1$

Así, $a^{n+m} = a^n * a^m$ para $n \in Z$ y $m = 1$

Supongamos que para $m = k > 0$, $a^n * a^k = a^{n+k}$, $k \in Z$

Ahora veamos si se verifica para $m = k+1$

En efecto,

$a^n * a^m = a^n * a^{k+1}$

$= a^n * (a^k * a)$, por la proposición 2 4.

$= (a^n * a^k) * a$, asociando

$= a^{n+k} * a$, por hipótesis de inducción.

$= a^{(n+k)+1}$, por la proposición 2.4

$= a^{n+(k+1)}$, asociatividad en $(Z , +)$

$= a^{n+m}$, $m = k + 1$

Así, $a^{n+m} = a^n * a^m$ para $n \in Z$ y $m \in Z^+$.

Los demás casos los dejamos al lector como ejercicio.□

Proposición 2.6:

Si $(G, *)$ es un grupo, $a \in G$ y $n,m \in Z$. Entonces $(a^n)^m = a^{nm}$.

Demostración:

Sean $(G, *)$ un grupo, $a \in G$ y $n, m \in Z$.

- Si $m = 0$, $(a^n)^0 = e$, por definición 2.10, (i).

$= a^0$, por definición 2.10, (i).

$= a^{n \bullet 0}$, para todo $x \in Z$, $x \bullet 0 = 0$.

$= a^{nm}$, $m = 0$.

Así, $(a^n)^m = a^{nm}$ para $n \in Z$ y $m = 0$.

- Consideremos $m = 1$.

Luego, $(a^n)^m = (a^n)^1$

$= a^n$, por definición 2.10, (ii).

$= a^{n \bullet 1}$, propiedad del neutro en $(Z , \bullet)$.

$= a^{nm}$, $m = 1$.

Así, $(a^n)^m = a^{nm}$ para $n \in Z$, $m = 1$.

- Supongamos que para $m = k > 0$, $(a^n)^k = a^{nk}$, $k \in Z$.

Ahora veamos si se verifica para $m = k + 1$.

En efecto,

$(a^n) = (a^n)^{k+1}$

$= (a^n)^k * a^n$, proposición 2.4.

$= a^{nk} + a^n$, por hipótesis de inclución.

$= a^{nk+n}$, proposición 2 4.

$= a^{n(k+1)}$, distributividad en Z.

$= a^{nm}$, $m = k + 1$

Así, $(a^n)^m = a^{nm}$ para $m > 1$.

Hasta aquí hemos demostrado que $(a^n)^m = a^{nm}$ para $n \in Z$ y $m \geq 0$. Los casos restantes los dejamos al lector.□

Proposición 2.7:

Si $(G,*)$ es un grupo abeliano, $a, b \in G$ y $n \in Z$. Entonces $(a * b)^n = a^n * b^n$.

Demostración.

Sean $(G,*)$ un grupo, $a, b \in G$ y $n \in Z$.

– Si $n = 0$, $(a * b)^n = (a * b)^0$

$= e$, por definición 2.10, (i)

$= e * e$, propiedad del neutro.

$= a^0 * b^0$, por definición 2.10. (i).

$= a^n * b^n$, $n = 0$

Así, $(a * b)^n = a^n * b^n$ para $n = 0$

– Consideremos $n = 1$.

Entonces, $(a * b)^n = (a * b)^1$

$= a * b$, por definición 2.10, (ii).

$= a^1 * b^1$, por definición 2.10, (ii).

$= a^n * b^n$, $n = 1$

Así, $(a * b)^n = a^n * b^n$ para $n = 1$

– Ahora supongamos que para $n = k > 0$, $(a * b)^k = a^k * b^k$, $k \in Z$

Averigüemos si se verifica para $n = k + 1$

En efecto,

$(a * b)^n = (a * b)^{k+1}$

$= (a * b)^k * (a * b)$, por proposición 2.4

$= (a^k * b^k) * (a * b)$, por hipótesis de inducción.

$= a^k * (b^k * a) * b$, por asociatividad.

$= a^k * (a * b^k) * b$, por conmutatividad.

$= (a^k * a) * (b^k * b)$, por asociatividad.

$= a^n * b^n$, $n = k + 1$.

Así, $(a * b)^n = a^n * b^n$ para $n > 1$

Por lo tanto, $(a * b)^n = a^n * b^n$ para $n \geq 0$

El caso donde $n < 0$ lo dejamos al lector como ejercicio.□

Definición 2.11

Sea (G, $*$) un grupo. Si G se compone de las potencias de uno de sus elementos, entonces lo llamaremos grupo cíclico. Es decir que , G se dice cíclico si cada uno de sus elementos es una potencia de $a \in G$ El elemento a se denomina generador del grupo.

Para indicar que (G, $*$) es generado por a escribimos $G = < a >$. La forma general de un grupo cíclico (G, $*$), de orden infinito, es

$$G = \{..., a^{-2}, a^{-1}, e, a^{1}, a^{2},...\};$$

y de orden finito es $G = \{ e, a^{1}, a^{2}, ...a^{n-1}\}$, donde n es el menor entero positivo que verifica la igualdad $a^{n} = e$.

Ejemplo 2.11·

El grupo (Z , +) es generado por el número uno. Es decir que, $Z = < 1 >$.

Luego, $Z = \{ .., -3\cdot1, -2\cdot1, -1\cdot1, 0\cdot1, 2\cdot1, 3\cdot1,...\} = <1>$.

Dejamos al lector, como ejercicio, verificar que $Z = <-1>$, y que (S_3, o) no es cíclico.

Proposición 2.8:

Todo grupo cíclico es abeliano.

Demostración:

Sea (G, *) un grupo cíclico.

Entonces, existe $a \in G$ tal que $G = \langle a \rangle$.

Sean $x,y \in G$, entonces $x = a^n$ y $y = a^m$; $m,n \in Z$

Luego, $x * y = a^n * a^m$

$= a^{n+m}$, proposición 2.5.

$= a^{m+n}$, conmutatividad en (Z , +)

$= a^m * a^n$, proposición 2.5.

$= y * x$

Así, (G, *) es abeliano

Por lo tanto, todo grupo cíclico es abeliano. □

Ahora consideremos el grupo abeliano (R, +) y supongamos que $x \in R$ es un generador de este grupo

Luego, existen $n, m \in Z$ tales que : $mx = 2$ $(m \neq 0)$ y $nx = \sqrt{2}$.

Entonces, $x = \frac{2}{m}$ Es decir que, x es racional

Pero, si x es racional, entonces nx es racional, puesto que es el producto de la multiplicación de los números racionales n y x. Luego, $\sqrt{2}$ sería racional, dado $nx = \sqrt{2}$, lo cual es una contradicción. Así, (R ,+) no es cíclico.

Por lo tanto, concluimos que no todo grupo abeliano es cíclico.

2 2 **SUBGRUPOS**

Definición 2 12.

Sea $(G, *)$ un grupo y $H \subseteq G$. Entonces, llamaremos a H subgrupo G sí y sólo si $(H, *)$ es grupo Esto lo denotaremos por $H_{sg}G$.

Ejemplo 2 12

Sabemos que $(R, +)$ es un grupo y que $Z \subseteq R$. Además, $(Z ,+)$ es un grupo Por lo tanto, Z_{sg} R Es decir que, Z es un subgrupo de R

Los subgrupos de (S_3,o) son $H_1 = \{I\}$, $H_2 = \{I, \phi\}$, $H_3 = \{I, \phi\circ\psi\}$, $H_4 = \{I, \psi \circ \phi\}$, $H_5 = \{I, \psi \circ \psi^2\}$ y S_3 De éstos, los cinco primeros son grupos cíclicos generados por I, ϕ, ψ, $\phi \circ \psi$, $\phi \circ \psi$ y ψ^2 respectivamente. Es decir que,

$H_1 = < I >$, $H_2 = < \phi >$, $H_3 = < \phi\circ\psi >$, $H_4 = < \psi \circ \phi >$, $H_5 = < \psi >$.

El grupo (S_3, o) a pesar de no ser cíclico, posee subgrupos cíclicos como acabamos de ver. Sin embargo, existen dos elementos de S_3 que combinados entre sí generan al grupo. Nos referimos a ϕ y ψ. En efecto.

$$I = \phi^2 \circ \psi^3$$

$$\phi = \phi \circ \psi^3$$

$$\psi = \phi^2 \circ \psi$$

$$\phi \circ \psi = \psi^{-1} \circ \phi$$

$$\psi \circ \phi = \phi \circ \psi^2$$

$$\psi^2 = \phi^2 \circ \psi^{-1}$$

(que el lector verifique esto utilizando la Tabla 2 1)

Luego, la presentación de (S_3,o) será

$$S_3 = \{\phi^j \circ \psi^k / j,k, \in Z, \ \phi \circ \psi = \psi^{-1} \circ \phi\}$$

La presentación de grupos es un tema interesante, pero, como no forma parte de nuestro objetivo, lo dejaremos hasta aquí.

Proposición 2.9:

Sean $(G, *)$ un grupo y $H \subseteq G$. Entonces, H_{sg} G sí y sólo si

i) $H \neq \phi$

ii) $x,y \in H$, entonces $x * y^{-1} \in H$.

Demostración:

($\Rightarrow$) Sean $(G, *)$ un grupo y H_{sg} G

– Como H_{sg} G, entonces $e \in H$.

Luego, $H \neq \phi$

– Si $y \in H$, entonces $y^{-1} \in H$, pues $H_{sg}\, G$

Luego, si $x,y \in H$, entonces $x * y^{-1} \in H$.

($\Leftarrow$) Sean $(G, *)$ un grupo y $H \subseteq G$ tal que

i) $H \neq \phi$

ii) $x, y \in H$, entonces $x * y^{-1} \in H$

– Como $H \neq \phi$, existe por lo menos un elemento $x \in H$.

Además, por hipótesis (ii), $x * x^{-1} \in H$

Así , $e \in H$

– Sea $y \in H$, entonces por (ii), $e * y^{-1} = y \in H$.

– Sean $x, y \in H$, entonces $x^{-1} \in H$ y $y^{-1} \in H$.

Luego, $x * (y^{-1})^{-1} \in H$, por (ii)

Así, por el lema 2 1, $x * y \in H$. Es decir que, $*$ es ley de composición interna en H.

Por lo tanto, $H_{sg}G$.□

Proposición 2.10:

Si $(G, *)$ es un grupo, $H_1 {}_{sg}\, G$ y $H_2 {}_{sg}\, G$. Entonces $H_1 \cap H_2 {}_{sg}\, G$.

Demostración.

– Por hipótesis $e \in H_1$ y $e \in H_2$. Entonces $e \in H_1 \cap H_2$.

Luego, $H_1 \cap H_2 \neq \phi$.

– Sean $x, y \in H_1 \cap H_2$. Entonces $x, y \in H_1$ y $x, y \in H_2$.

Luego, por la proposición 2.9, $x * y^{-1} \in H$, y $x * y^{-1} \in H_2$.

Así, $x * y^{-1} \in H_1 \cap H_2$

Por lo tanto, en virtud de la proposición 2.9, $H_1 \cap H_2$ sg G □

Proposición 2.11:

Si (G, *) es un grupo y $a \in G$ Entonces $\langle a \rangle = \{a^n / n \in Z\}$ es subgrupo de G

Demostración:

– Como $a \in G$, entonces $a^0 = e$

Luego, $e \in \langle a \rangle$

Así, $\langle a \rangle \neq \phi$

– Finalmente, sean $x, y \in \langle a \rangle$, entonces existen $m,n \in Z$ tales que $x = a^m$ y $y = a^n$.

Por otro lado, como $-n \in Z$, entonces $a^{-n} \in \langle a \rangle$ y $a^n * a^{-n} \in \langle a \rangle$

Además, $e = a^0 = a^{-n+n}$, propiedad de los inversos en (Z , +).

$= a^{-n} * a^n$, por la proposición 2 5

$= a^{-n} * y$, $y = a^n$

Luego, $y^{-1} = a^{-n}$ En consecuencia $x * y^{-1} = a^m * a^{-n} \in \langle a \rangle$

Por la proposición 2 9, concluimos que $\langle a \rangle$ sg G.□

Proposición 2.12.

Si (G,∗) es un grupo cíclico y $H \leq_{sg} G$, entonces H es cíclico

Demostración:

Sean (G,∗) un grupo cíclico y $H \leq_{sg} G$.

Sea $a \in G$ tal que $G = \langle a \rangle$, y supongamos que m es el menor entero positivo tal que $a^m \in H$.

Luego, como todo elemento $x \in H$ pertenece a G, entonces $x = a^k$, $k \in Z$.

Además, como $k = mq + r$; $0 \leq r < m$ y $q, r \in Z$, entonces $a^k = a^{mq+r}$.

Luego, $a^k = a^{mq} * a^r$, por la proposición 2.5.

$= (a^m)^q * a^r$, por la proposición 2.6.

Ahora, operando a izquierda con $(a^m)^{-q}$ obtenemos que

$(a^m)^{-q} * a^k = (a^m)^{-q} * [\,(a^m)^q * a^r\,]$

$= [(a^m)^{-q} * (a^m)^q] * a^r$, asociando.

$= e * a^r$, propiedad de los inversos.

$= a^r$, propiedad del neutro.

Entonces $a^r \in H$, puesto que $a^m, a^k \in H$. Pero, como $r < m$, entonces $r = 0$

Así, $k = mq$. Luego, los elementos de H son de la forma $(a^m)^q$. Es decir que $H = \langle a^m \rangle$.

Por lo tanto, H es cíclico.□

Definición 2.13.

Sean (G, *) un grupo, $H_{sg}G$ y a,b $\in$ G. Diremos que a es congruente con b módulo H si $a * b^{-1} \in H$ Lo cual simbolizaremos $a \equiv b \bmod H$

Ejemplo 2 13

Consideremos (S_3,o) y $H_5 = \{I, \psi, \psi^2\}$.

Entonces, $\psi \equiv \psi^2 \bmod H_5$. En cambio es falso que $\phi \equiv \psi \bmod H_5$, puesto que $\phi * \psi^{-1} \notin H_5$

Definición 2 14

Sean (G, *) un grupo, $a \in G$ y $H_{sg}G$. Definiremos $\bar{a}$ como el conjunto de los $x \in G$ tal que $a \equiv x \bmod H$. Es decir que,

$$\bar{a} = \{x \in G / a \equiv x \bmod H\}.$$

Ejemplo 2 14

Consideremos (Z , +) y (3 Z , +), donde 3 Z $_{sg}$ Z.

Entonces $\bar{5} = \{x \in Z / 5 \equiv x \bmod 3Z\}$

$= \{x \in Z / (5 - x) \in 3Z\}$

$= \{\ , -4, -1, 2, 5, 8, ..\}$

Definición 2.15.

Sean (G, $*$) un grupo, $a \in G$ y $H_{sg}G$. Llamaremos clase lateral derecha de H al conjunto $H_a = \{x * a / x \in H\}$.

Ejemplo 2.15

Tomemos $H_2 = \{I, \phi\}$, el cual es subgrupo de (S_3, o)

Entonces, $H_2\phi = \{I \circ \phi, \phi \circ \phi\} = \{\phi, I\} = H_2$.

Proposición 2.13

Si (G, $*$) en un grupo, $a \in G$ y $H_{sg}G$ Entonces $Ha = \bar{a}$.

Demostración

- Si $p \in Ha$, entonces existe $x \in H$ tal que $p = x * a$.

Luego, $a * p^{-1} = a * (x * a)^{-1}$

$= a * (a^{-1} * x^{-1})$, por el Lema 2 1.

$= (a * a^{-1}) * x^{-1}$, asociando

$= e * x^{-1}$, propiedad de los inversos

$= x^{-1}$, propiedad del neutro

En consecuencia, $a * p^{-1} \in H$, puesto que $x^{-1} \in H$.

Así, por la definición 2.14, $p \in \bar{a}$. Luego, $H a \subseteq \bar{a}$.

– Finalmente, si $p \in \bar{a}$, entonces $a \equiv p \mod H$

Luego, por la definición 2.13, $a * p^{-1} \in H$. Entonces, existe $x \in H$ tal que $a * p^{-1} = x$ De donde $a = x * p$, por el Lema 2 1

Ahora, operando a izquierda con x^{-1}, obtenemos que

$$x^{-1} * a = x^{-1} * (x * p)$$

$$= (x^{-1} * x) * p \quad \text{, por asociatividad.}$$

$$= e * p \quad \text{, propiedad de los inversos}$$

$$= p \quad \text{, propiedad del neutro}$$

Como $x^{-1} * a \in Ha$, entonces $p \in Ha$ Luego, $\bar{a} \subset Ha$.

Por lo tanto, concluimos que $Ha = \bar{a}$ □

Proposición 2.14:

Si (G, *) es un grupo y $H_{sg}G$. Entonces existe una correspondencia biyectiva entre dos clases laterales derechas de H en G.

Demostración

Sean (G, *) un grupo, a,b ∈ G y $H_{sg}G$

Sea f : Ha → Hb tal que f(x * a) = x * b, para todo x ∈ H.

– Sean x_1 , x_2 ∈ H

Si $f(x_1 * a) = f(x_2 * a)$, entonces $x_1 * b = x_2 * b$, por definición de f.

Luego, $x_1 = x_2$, por el Lema 2.1.

Así, f es inyectiva.

– Finalmente, por construcción de f tenemos que f(Ha) = Hb.

Luego, f es suryectiva

Por lo tanto, f es biyectiva.□

Esta proposición es importantísima cuando H es un grupo finito, puesto que lo que afirma es que dos clases laterales derechas de H tienen el mismo orden.

Además, He = H, luego cualquier clase lateral derecha de H en G tienen el mismo orden de H. Es decir que, o(Ha) = o(H), a $\in$ G.

Proposición 2.15:

Si (G, $*$) es un grupo finito y $H_{sg}G$. Entonces Ha = Hb $\Leftrightarrow$ Ha $\cap$ Hb = ϕ,

para cualesquiera a,b $\in$ G

Demostración.

Supongamos que Ha $\cap$ Hb $\neq \phi$, y demostremos que Ha = Hb.

En efecto:

Si Ha $\cap$ Hb $\neq \phi$, entonces existe g $\in$ Ha $\cap$ Hb.

Luego, $g = h_1 * a$ y $g = h_2 * b$, donde $h_1, h_2 \in H$.

Entonces, $h_1 * a = h_2 * b$.

Así, $a = h_1^{-1} * h_2 * b$ y $b = h_2^{-1} * h_1 * a$ (1).

– Ahora, probaremos que $Ha \subseteq Hb$.

Sea $x \in Ha$, entonces existe h e H tal que $x = h * a$.

Luego, $x = h * (h_1^{-1} * h_2 * b)$, por (1).

$= (h * h_1^{-1} * h_2) * b$, por asociatividad.

Entonces, $x \in Hb$, puesto que $h * h_1^{-1} * h_2 \in H$.

Así, $Ha \subseteq Hb$

– Por último probemos que $Hb \subseteq Ha$.

Sea $y \in Hb$, entonces existe $h \in H$ tal que $y = h * b$.

Luego, $y = h * (h_2^{-1} * h_1 * a)$, por (1).

$= (h * h_2^{-1} * h_1) * a$, por asociatividad.

Entonces, como $h * h_2^{-1} * h_1 \in H$, $y \in Hb$

Así, $Hb \subseteq Ha$

Por lo tanto, $Ha = Hb$.

Concluimos, entonces que dos clases laterales derechas de H en G o son idénticas o son disjuntas.□

Teorema (de Lagrange) 2.1:

Si (G, *) es un grupo finito y $H_{sg}G$. Entonces $o(H)$ es un divisor de $o(G)$.

Demostración.

Sean (G, *) un grupo y $H_{sg}G$.

Supongamos que n es el número de clases laterales derechas distintas de H en G

Luego, tenemos que

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_n,$$

donde $Ha_i \cap Ha_j = \phi$, $i \neq j$.

Entonces, $o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_n)$

$o(G) = o(H) + o(H) + \ldots + o(H)$, pues $o(Ha_i) = o(H)$.

$o(G) = n \cdot o(H)$.

Por lo tanto , $o(H)$ es un divisor de $o(G)$.□

Para ilustrar este teorema consideremos el grupo finito (S_3, o), el cual tiene por subgrupo a

$H_5 = \{I, \psi, \psi^2\}$.

Sabemos que $o(S_3) = 6$ y $o(H_5) = 3$.

Luego, como 3 es divisor de 6, entonces $o(H_5)$ es divisor de $o(S_3)$.

Definición 2.16:

Sean $(G,*)$ un grupo y $a \in G$. Llamaremos orden del elemento a al menor entero positivo m tal que $a^m = e$, y lo denotaremos por $o(a)$. De no existir tal entero diremos que a es de orden infinito

Ejemplo 2.16

En el grupo (S_3, o) tenemos que:

$o(I) = 1$ $\quad o(\phi) = 2$ $\quad o(\psi) = 3$

$o(\phi \circ \psi) = 2$ $\quad o(\psi \circ \phi) = 2$ $\quad o(\psi^2) = 3$.

Proposición 2.16:

Si $(G, *)$ es un grupo finito y $a \in G$ de orden m. Entonces m es divisor de $o(G)$.

Demostración:

Sean (G, *) un grupo finito y $a \in G$ tal que $o(a) = m$

Sea H = <a>. Entonces, por la proposición 2.11, $H_{sg}G$.

Luego, por la definición 2.11, $o(a) = o(H)$. Es decir que, $o(H) = m$.

Entonces, por el Teorema 2.1, $o(H)$ divide a $o(G)$.

Por lo tanto, m es divisor de $o(G)$.□

Proposición 2.17:

Si (G, *) es un grupo finito de orden n y $a \in G$. Entonces $a^n = e$.

Demostración.

Sean (G, *) un grupo finito de orden n y $a \in G$.

Supongamos que $o(a) = m$. Entonces, por la proposición 2.16, m es divisor de n. Es decir que, existe $k \in N$ tal que $n = km$.

Luego, $a^n = a^{km}$

$= a^{mk}$, por conmutatividad en (Z , •).

$= (a^m)^k$, por la proposición 2.6

$= e^k$, por la definición 2.16.

$= e$, por propiedad del neutro

Por lo tanto, concluimos que $a^n = e$ □

Para ilustrar esta proposición consideremos el grupo (S_3, o) tiene $o(S_3)=6$

Además, por el ejemplo 2.16, sabemos que $o(\psi) = 3$. Luego, como $6 = 2 \cdot 3$,

tenemos $o(\psi)$ es divisor de $o(S_3)$

Por otro lado, $\psi^6 = \psi^{3\cdot 2}$

$= (\psi^3)^2$, por la proposición 2.6.

$= (I)^2$, por la definición 2 16

$= I$, propiedad del neutro

Que el lector verifique que esto ocurre con los otros elementos de S_3

Definición 2 17.

Sean $(G, *)$ un grupo y $H_{sg}G$. Llamaremos a H subgrupo normal de G, sí y sólo sí para todo $g \in G$ y para todo $n \in H$, se tiene que $g * n * g^{-1} \in H$.

Nota: H subgrupo normal de G lo denotaremos, $H \trianglelefteq G$.

Ejemplo 2.17·

Consideremos el grupo (S_3, o) y $H_5 = \{I, \psi, \psi^2\}_{sg}$ G.

En efecto, utilizando la Tabla 2.1,

- si $n = I$, entonces $g \circ I \circ g^{-1} = g \circ g^{-1} = I \in H$, para todo $g \in G$.

- si $n = \psi$, entonces $1 \circ \psi \circ 1^{-1} = \psi \circ 1 = \psi \in H$

$$\psi \circ \psi \circ \psi^{-1} = \psi \circ \psi \circ \psi^2 = \psi \circ \psi^3 = \psi \circ 1 = \psi \in H$$

$$\phi \circ \psi \circ \phi^{-1} = (\phi \circ \psi) \circ \phi = \psi^2 \in H$$

$$(\phi \circ \psi) \circ \psi \circ (\phi \circ \psi)^{-1} = (\phi \circ \psi) \circ \psi \circ (\phi \circ \psi) = \psi^2 \in H.$$

$$(\psi \circ \phi) \circ \psi \circ (\psi \circ \phi)^{-1} = (\psi \circ \phi) \circ \psi \circ (\psi \circ \phi) = \psi^2 \in H$$

$$\psi^2 \circ \psi \circ (\psi^2)^{-1} = (\psi^2 \circ \psi) \circ \psi = \psi^3 \circ \psi = 1 \circ \psi = \psi = 1$$

- Finalmente, si $n = \psi^2$ tenemos que:

$$1 \circ \psi^2 \circ 1^{-1} = (1 \circ \psi^2) \circ 1 = \psi^2 \circ 1 = \psi^2 \in H$$

$$\phi \circ \psi^2 \circ \phi^{-1} = (\phi \circ \psi^2) \circ \phi = \psi \in H$$

$$\psi \circ \psi^2 \circ \psi^{-1} = (\psi \circ \psi^2) \circ \psi^2 = \psi^3 \circ \psi^2 = I \circ \psi^2 = \psi^2 \in H$$

$$(\phi \circ \psi) \circ \psi^2 \circ (\phi \circ \psi)^{-1} = (\phi \circ \psi) \circ \psi^2 \circ (\phi \circ \psi) = \psi \in H.$$

$$(\psi \circ \phi) \circ \psi^2 \circ (\psi \circ \phi)^{-1} = (\psi \circ \phi) \circ \psi^2 \circ (\psi \circ \phi) = \psi \in H.$$

$$\psi^2 \circ \psi^2 \circ (\psi^2)^{-1} = \psi^2 \circ (\psi^2 \circ \psi) = \psi^2 \circ 1 = \psi^2 \in H$$

Por lo tanto, $H_5 \trianglelefteq S_3$

Proposición 2.18:

Si $(G, *)$ es un grupo y $H \subseteq_{sg} G$. Entonces, $H \trianglelefteq G$ si y sólo si $g*H*g^{-1} = H$, para todo $g \in G$

Demostración:

Sean $(G, *)$ un grupo y $H_{sg}G$.

($\Rightarrow$) Si $H \trianglelefteq G$, entonces $g * H * g^{-1} = H$, para todo $g \in G$

1) Sean $g \in G$ y $x \in g * H * g^{-1}$, entonces existe $n \in H$ tal que

$x = g * n * g^{-1}$

Luego, $g * n * g^{-1} = x \in H$, puesto que $H \trianglelefteq G$.

Así, $g * H * g^{-1} \subseteq H$, para todo $g \in G$.

2) Sean $g \in G$ y $n \in H$, entonces

$n = e * n * e$, propiedad del neutro

$= (g * g^{-1}) * n * (g * g^{-1})$, propiedad de los inversos.

$= g * (g^{-1} * n * g) * g^{-1}$, por asociatividad.

Luego, como $g \in G$ y $H \trianglelefteq G$, entonces existe $x \in H$ tal que $x = g^{-1} * n * g$.

Entonces, $g * x * g^{-1} = n \in g * H * g^{-1}$

Así, $H \subseteq g * H * g^{-1}$, para todo $g \in G$.

Concluimos, por (1) y (2), que $g * H * g^{-1} = H$

($\Leftarrow$) Finalmente probaremos que, si $g * H * g^{-1} = H$ entonces $H \trianglelefteq G$.

En efecto,

Sean $n \in H$ y $g \in G$, entonces $g * n * g^{-1} \in g * H * g^{-1}$.

Luego, $g * n * g^{-1} \in H$

Por lo tanto, $H \trianglelefteq G$

Proposición 2.19:

Si (G, ∗) es un grupo y H_{sg} G. Entonces, $H \trianglelefteq G$ sí y sólo si toda clase lateral izquierda (C.L.I.) de H en G, es una clase lateral derecha (C.L.D.) de H en G.

Demostración

Sean (G, ∗) un grupo y $H_{sg}G$.

(⇒) Si $H \trianglelefteq G$, entonces toda CLI de H es una CLD de H en G.

En efecto,

Sea $g \in G$, entonces $g^{-1} \in G$. Por la proposición 2.18,

$g * H * g^{-1} = H$

Luego, $g * H = g * (g^{-1} * H * g)$

$= (g * g^{-1}) * H * g$, por asociatividad.

$= e * H * g$, por propiedad de los inversos

$= H * g$, por propiedad del neutro

Así, toda CLI es una CLD

Observación debemos tener presente que H ∗ g es lo mismo que Hg

(⇐) Ahora probaremos que, si toda CLI es una CLD de H en G, entonces

$H \trianglelefteq G$

Sea $g \in G$, entonces, por hipótesis, $g * H = H * g$.

Luego, $g * H * g^{-1} = H * g * g^{-1}$

$= H * e$, por propiedad de los inversos.

$= H$, por propiedad del neutro

Así, por la proposición 2.18, $H \trianglelefteq G$.□

2 3. HOMOMORFISMOS.

Definición 2.18.

Sean $(G, *)$ y $(G^1, _T)$ dos grupos, y $f : G \to G^1$ una aplicación. Llamaremos a g homomorfismos de grupo si $f(x * y) = f(x) \ _T f(y)$, para cualesquiera $x, y \in G$

Ejemplo 2 18:

Consideremos los grupos $(R , +)$ y $(R^*, \bullet)$, y definamos una aplicación $f : R \to R^*$ tal que $f(x) = 2^x$, par todo $x \in R$

Ahora, veremos si f es un homomorfismo.

En efecto, sean $a,b \in R$

Entonces, $f(a * b) = 2^{a+b}$, por definición de f.

$= 2^a \cdot 2^b$, por la proposición 2.5.

$= f(a) \cdot f(b)$, por definición de f

Por lo tanto, f es un homomorfismo.

Definición 2.19.

Sea (G, $*$) un grupo. Llamaremos endomorfismo de G, a todo homorfismo

$f . G \to G$.

Ejemplo 2.19.

Consideremos la aplicación $f . (G, *) \to (G, *)$ tal que $f(x) = x$, donde, obviamente, (G, $*$) es un grupo.

Ahora, si $a,b \in G$. Entonces $f(a * b) = a * b$, por definición de f.

$= f(a) * f(b)$, por definición de f.

Por lo tanto, f es un endomorfismo.

Definición 2.20:

Sean (G, $*$) y (G^1, τ) dos grupos y $f : G \to G^1$ un homomorfismo Llamaremos monomorfismo a f, si es f es inyectivo.

Ejemplo 2.20:

En el ejemplo 2.18 probamos que $f : (R , +) \to (R^* , \bullet)$ tal que $f(x) = 2^x$ es un homomorfismo. Veamos ahora si es inyectivo.

Sean $a,b \in R$. Por demostrar que $f(a) = f(b) \Rightarrow a = b$.

En efecto, $f(a) = f(b)$ implica que $2^a = 2^b$, por definición de f.

$a \bullet \log 2 = b \bullet \log 2$, propiedad de la función log.

$a = b$, dividiendo por log2.

Por lo tanto, f es inyectivo Así, pues, f es un monomorfismo.

Definición 2.21

Sean $(G, *)$ y $(G^1, _T)$ dos grupos y $f: G \rightarrow G^1$ un homomorfismo Si f es suryectivo, entonces lo llamaremos epimorfismo.

Ejemplo 2.21:

Consideremos el homomorfismo del ejemplo 2.18, y probemos que es suryectivo.

Sea $y \in R^*$. Por demostrar que existe $x \in R$ tal que $y = 2^x$.

En efecto,

Sea $x = \frac{\log y}{\log 2}$, $x \in R$.

entonces $x \bullet \log 2 = \log y$, multiplicando por log2.

luego $\log 2^x = \log y$, propiedad de la función log.

entonces $2^x = y$

Así, f es suryectivo, y por lo tanto es un epimorfismo.

Definición 2.22

Sean $(G, *)$ y (G^1, τ) dos grupos y $f \cdot G \to G^1$ un homomorfismo. Si f es biyectivo (inyectivo y suryectivo), entonces lo llamaremos isomorfismo

Ejemplo 2 22

Consideremos nuevamente el homomorfismo del ejemplo 2.18, puesto que el mismo es inyectivo y suryectivo, es decir, biyectivo como vimos en los ejemplos 2 20 y 2.21 respectivamente

Por lo tanto, $f \cdot R \to R^*$ tal que $f(x) = 2^x$ es un isomorfismo

Definición 2.23:

Sea $(G, *)$ un grupo y $f \quad G \to G$ un endomorfismo Si f es biyectivo, entonces lo llamaremos automorfismo

Ejemplo 2 23

Consideremos el endomorfismo $I : (G, *) \to (G, *)$ tal que $I(x) = x$, y probemos que es biyectivo

- Sean $x, y \in G$

Luego, si $I(x) = I(y)$, entonces $x = y$, por definición de I.

Así, I es inyectivo

- Ahora, sea $y \in G$

Luego, existe $x = y$ en G tal que $y = f(x)$, por definición de I.

Así, I es suryectivo

Por lo tanto, concluimos que I es biyectivo, y en consecuencia es un automorfismo.

Definición 2.24.

Sean $(G, *)$ y (G^1, T) dos grupos, y $f : G \to G^1$ un homomorfismo. Llamaremos núcleo de f al conjunto $Nf = \{x \in G / f(x) = e^1\}$, donde e^1 es el elemento neutro de G^1

Definición 2.25.

Llamaremos imagen de un homomorfismo $f : G \to G^1$ al conjunto $Imf = \{y \in G / \exists\, x \in G, f(x) = y\}$.

Ejemplo 2.25.

Hallaremos el núcleo y la imagen del isomorfismo $f (R,+)\to(R^*,\bullet)$ tal que $f(x) = 2^x$, para todo $x \in R$

- Tenemos que $Nf = \{x \in R / f(x) = 1\}$, por definción 2.24.

$= \{x \in R / 2^x = 1\}$,por definición de f

Luego, $Nf = \{0\}$, ya que la única solución de $2^x = 1$ es $x = 0$.

- Finalmente,

$Imf = \{y \in R^* / \exists\, x \in R , y = f(x)\} = R^*$, puesto que f es suryectivo.

Proposición 2.20:

Sean $(G, *)$ y (G^1, τ) dos grupos, e y e^1 sus respectivos elementos neutros. Si $f : G \to G^1$ es un homomorfismo, entonces

i) $f(e) = e^1$

ii) $f(x^{-1}) = [f(x)]^{-1}$

Demostración:

Sean $(G, *)$ y (G^1, τ) dos grupos.

i) Sea $x \in G$, entonces $f(x) \in G^1$.

Luego, $f(x) \tau e^1 = f(x)$, propiedad del neutro en G^1

$= f(x * e)$, propiedad del neutro en G.

$= f(x) \tau f(e)$, f es homomorfismo.

Entonces, $e^1 = [f(x)]^{-1} \tau f(x) \tau f(e)$, por el Lema 2.1.

$= e^1 \tau f(e)$, propiedad de los inversos en G^1.

$= f(e)$, propiedad del neutro en G^1.

Así, queda demostrado que $f(e) = e^1$.

ii) Para terminar, sea $x \in G$, entonces $f(x), f(x^{-1}) \in G^1$.

Luego, $f(x) \tau f(x^{-1}) = f(x * x^{-1})$, f es homomorfismo.

$= f(e)$, propiedad de los inversos.

$= e^1$, por (i).

$= f(x) \tau [f(x)]^{-1}$, propiedad de los inversos.

De donde $f(x^{-1}) = [f(x)]^{-1}$, por el Lema 2.1

Por lo tanto, hemos demostrado que, $f(x^{-1}) = [f(x)]^{-1}$. □

Proposición 2.21:

Si $(G, *)$ y $(G^1, _T)$ son dos grupos y $f: G \to G^1$ un homomorfismo

Entonces $Nf \,_{sg}\, G$

Demostración

Sean $(G, *)$ y $(G^1, _T)$ dos grupos y $f: G \to G^1$ un homomorfismo.

– Sean $x,y \in Nf$.

Entonces, $f(x) = e^1 = f(y)$, por definición de Nf.

Luego, $f(x * y) = f(x) \,_T\, f(y)$, f es homomorfismo.

$= e^1 \,_T\, e^1$, por lo anterior.

$= e^1$, por propiedad del neutro.

Así, $x * y \in Nf$. En consecuencia $*$ es ley de composición interna en Nf.

– Además, $f(e) = e^1$, por la proposición 2 20.

Luego, $e \in Nf$

– Finalmente, sea $x \in Nf$

Luego, $f(e) = f(x * x^{-1})$, propiedad de los inversos.

$= f(x) \,_T\, f(x^{-1})$, f es homomorfismo.

$= e^1 \,_T\, f(x^{-1})$, $x \in Nf$

$= f(x^{-1})$, propiedad del neutro.

Entonces $e^1 = f(x^{-1})$, puesto que $f(e) = e^1$.

Así, $x^{-1} \in Nf$, para todo $x \in Nf$.

Por lo tanto, (Nf, $*$) es un grupo, y en consecuencia $Nf \ _{sg} \ G$.□

Proposición 2.22.

Si (G, $*$) y (G^1, $_T$) son grupos, $H \ _{sg} \ G$ y $H^1 \ _{sg} \ G^1$, y f: $G \rightarrow G^1$ un homomorfismo.

Entonces

i) $f(H) \ _{sg} \ G^1$

ii) $f^{-1}(H^1) \ _{sg} \ G$.

Demostración:

Sean (G, $*$) y (G^1, $_T$) dos grupos, $H_{sg}G$, $H^1{}_{sg}G^1$ y f: $G \rightarrow G^1$ un homomorfismo.

i) Como $H_{sg}G$, entonces $e \in H$.

Luego, $f(e) = e^1$, por la proposición 2 20.

Entonces $e^1 \in f(H)$.

Así, $f(H) \neq \phi$

– Ahora, si $y \in f(H)$, entonces existe $x \in H$ tal que $f(x) = y$.

Además, como H es grupo, existe $x^{-1} \in H$ tal que $x * x^{-1} = e$.

Luego, $e^1 = f(e)$, por la proposición 2.20.

$= f(x * x^{-1})$, propiedad de los inversos.

$= f(x) \ _T \ f(x^{-1})$, f es homomorfismo.

$= f(x) \tau [f(x)]^{-1}$, por la proposición 2 20

$= y \tau y^{-1}$, sustituyendo f(x).

Así, $y^{-1} \in f(H)$.

Por lo tanto, en virtud de la proposición 2.9, $f(H)$ $_{sg}$ G^1.

ii) Finalmente, como H^1 es grupo, entonces $e^1 \in H^1$.

Además, por la proposición 2.20, $e^1 = f(e)$.

Luego, $f^{-1}(e^1) = e$. Entonces $e \in f^{-1}(H^1)$.

Así, $f^{-1}(H^1) \neq \phi$.

Sea $x \in f^{-1}(H^1)$, entonces existe $y \in H^1$ tal que $y = f(x)$.

Luego, como H^1 es grupo, existe $y^{-1} \in H$

Entones, $y^{-1} = [f(x)]^{-1}$,sustituyendo y.

$= f(x^{-1})$,por la proposición 2.20

Luego, $f(x^{-1}) \in (H^1)$.

Así, $x^{-1} \in f^{-1}(H^1)$

Por lo tanto, en virtud de la proposición 2.9 , $f^{-1}(H^1)$ $_{sg}$ G.□

Proposición 2.23:

Si $(G, *)$ y (G^1, τ) son grupos y $f : G \rightarrow G'$ es un homomorfismo. Entonces $Nf \trianglelefteq G$.

Demostración.

Sean $(G, *)$ y $(G^1,_T)$ dos grupos y $f : G \to G^1$ un homomorfismo, por la proposición 2.21, $Nf \,_{sg}\, G$

Luego, únicamente nos resta probar la normalidad de Nf

En efecto,

Sean $g \in G$ y $n \in Nf$. Entonces,

$f(g^{-1} * n * g) = f(g^{-1}) \,_T\, f(n) \,_T\, f(g)$, f es homomorfismo.

$= f(g^{-1}) \,_T\, e^1 \,_T\, f(g)$, $n \in Nf$.

$= f(g^{-1}) \,_T\, f(g)$, propiedad del neutro

$= f(g^{-1} * g)$, f es homomorfismo.

$= f(e)$, propiedad de los inversos.

$= e^1$, proposición 2.20

Luego, $g^{-1} * n * g \in Nf$.

Por lo tanto, $Nf \trianglelefteq G$.□

Definición 2 26.

Sean $(G, *)$ y $(G^1, _T)$ dos grupos , y $f : G \to G^1$ un homomorfismo.

Llamaremos a $g \in G$ imagen inversa de $g^1 \in G^1$ bajo f, si $f(g) = g^1$

Ejemplo 2 26

Consideremos el homomorfismo f . (Z, +) $\rightarrow$ (Z, +) tal que

f(x) = 2x

Entonces, el número 16 $\in$ Z es la imagen inversa de 32 $\in$ Z bajo f, puesto que f(16) = 2(16) = 32 Sin embargo, no siempre la imagen inversa de un elemento es única, ya que depende del homomorfismo Esto lo podemos verificar en el homomorfismo f^1 (R*,•) $\rightarrow$ (R*,•) tal que $f^1(x) = x^2$

En efecto, el elemento 2 $\in$ R* es imagen inversa 4$\in$ R*, pero -2$\in$ R* también lo es. Es decir que, $f^1(-2) = 4 = f^1(2)$.

Luego, la imagen inversa de 4 $\in$ R*, no es única, bajo f^1 Además, con este resultado hemos probado que f^1 no es inyectivo.

Por lo tanto, concluimos que, si un homomorfismo f no es inyectivo, entonces la imagen inversa de $g^1 \in G^1$ no es única.

Proposición 2.24:

Si $f : (G, *) \rightarrow (G^1, {}_T)$ es un homomorfismo. Entonces el conjunto de todas las imágenes inversas de $g^1 \in G^1$ bajo f en G, está dado por Nfx, donde x es una imagen inversa particular cualquiera de g^1 en G.

Demostración

Sean $f : (G, *) \rightarrow (G^1, {}_T)$ un homomorfismo, $g^1 \in G^1$, y $x \in G$ una imagen inversa particular de g^1.

Para empezar supongamos que $g^1 = e^1$ Entonces todas sus imágenes inversas serían los $g \in Nf$, puesto que para todo $g \in Nf$, $f(g) = e^1$ Es decir que, el conjunto de todas las imágenes inversas de e^1 es Nfx , donde $x = e$.

Ahora supongamos que $g^1 \neq e^1$

Si $n \in Nf$ y $g = n * x$, entonces $f(g) = f(n * x)$

$= f(n)_T f(x)$, f es homomorfismo.

$= e^1 {}_T g^1$, $n \in Nf$

$= g^1$, propiedad del neutro.

De esta manera, todos los elementos del conjunto Nfx son imágenes inversas de g^1, siempre que x lo sea.

Finalmente probaremos que, si $p \in G$ es imagen inversa de g^1, entonces $p \in Nfx$

En efecto, supongamos que $f(p) = g^1 = f(x)$

Luego, $f(p) = f(x)$

Entonces $f(p) \top [f(x)]^{-1} = f(x) \top [f(x)]^{-1}$

$= e^1$, propiedad de los inversos.

Así, por la proposición 2 20, $f(p) \top f(x^{-1}) = e^1$.

Luego, como f es homomorfismo, $f(p * x^{-1}) = e^1$

En consecuencia $p * x^{-1} \in Nf$, es decir que, $p \in Nfx$.

Por lo tanto, Nfx es el único que contiene todas las imágenes inversas de g^1, siempre que x sea una de esas imágenes.□

Para ilustrar esta proposición consideremos el ejemplo 2 26, en el cual verificamos que las imágenes inversas de $4 \in R^*$ bajo f^1 eran $-2, 2 \in R^*$

El $Nf^1 = \{ x \in R^* / f^1(x) = 1 \} = \{ x \in R^* / x^2 = 1\} = \{-1, 1\}$.

Luego, $Nf^1{}_2 = \{-2, 2\}$

Por lo tanto, $Nf^1{}_2$ contiene todas las imágenes inversas de 4, bajo f^1.

Proposición 2. 25:

Si f $(G, *) \rightarrow (G^1, \top)$ es un homomorfismo. Entonces, f es un monomorfismo si y sólo si $Nf = \{e\}$.

Demostración

Sean $(G, *)$ y (G^1, τ) dos grupos, y $f \quad G \to G^1$ un homomorfismo.

($\Rightarrow$) Si f es inyectivo, entonces $Nf = \{e\}$.

i) Sea $x \in Nf$, entonces $f(x) = e^1$, por la definición 2.24

Luego, por la proposición 2 20 , $f(x) = f(e)$

Entonces, como f es inyectivo, $x = e$

Así, $x \in \{ e \}$ Es decir que, $Nf \subseteq \{ e \}$

ii) Por la proposición 2.20 , $f(e) = e^1$

Entonces, por la definición 2.24, $e \in Nf$

Luego, $\{ e \} \subseteq Nf$.

Concluimos, por (i) y (ii), que $Nf = \{ e \}$.

($\Leftarrow$) Si $Nf = \{ e \}$, entonces f es inyectivo

En efecto,

Sean $x, y \in G$ tal que $f(x) = f(y)$.

Luego, $f(x) \tau [f(y)]^{-1} = f(y) \tau [f(y)]^{-1}$

$f(x) \tau [f(y)]^{-1} = e^1$, propiedad de los inversos

$f(x) \tau f(y^{-1}) = e^1$, por la proposición 2 20

$f(x * y^{-1}) = e^1$, f es homomorfismo.

Entonces, por la definición 2 24, $x * y^{-1} \in Nf$

Además, por hipótesis $Nf = \{ e \}$, por lo cual $x * y^{-1} = e$.

Luego, $(x * y^{-1}) * y = e * y$

$x * (y^{-1} * y) = e * y$, por asociatividad.

$x * e = e * y$, propiedad de los inversos

$x = y$, propiedad del neutro.

En consecuencia f es inyectivo, y por lo tanto es un monomorfismo.□

Para ilustración de esta proposición determinemos el núcleo del homomorfismo $f : (Z, +) \to (Z, +)$ tal que $f(x) = 2x$, y veamos después si es inyectivo o no.

En efecto,

$Nf = \{ x \in Z \ / \ f(x) = e \} = \{ x \in Z \ / \ 2x = 0 \} = \{ 0 \}$.

Ahora supongamos que $x, y \in Z$.

Luego, si $f(x) = f(y)$ entonces $2x = 2y$. Es decir que, $x = y$.

Por lo tanto, f es inyectivo.

Definición 2.27

Sean $(G, *)$ y $(G^1, _T)$ dos grupos. Diremos que G y G^1 son isomorfos si y sólo si se puede establecer entre ellos un homomorfismo biyectivo, es decir, un isomorfismo.

Ejemplo 2.27·

En el ejemplo 2.22, probamos que $f : (R, +) \rightarrow (R^*, \bullet)$ es un isomorfismo. Por lo tanto, (R, +) y (R^*, •) son isomorfos. Lo cual denotaremos por $R \cong R^*$.

Proposición 2.26:

Si (G, *) es un grupo cíclico de orden infinito. Entonces, (G, *) es isomorfo a (Z , +).

Demostración·

Sea (G, *) un grupo cíclico de orden infinito, y $x \in Z$ tal que $G = < x > = \{ x^n / n \in Z \}$.

Definamos una aplicación f , así :

$$f : G \rightarrow Z$$

$$a^n \rightarrow n$$

Por demostrar que f es un isomorfismo.

i) Primeramente probaremos que f es homomorfismo.

Sean $x, y \in G$, entonces existen $m,n \in Z$, tales que $x = a^m$, $y = a^n$.

Luego, $f(x * y) = f(a^m * a^n)$

$= f(a^{m+n})$, por la proposición 2.5

$= m + n$, por definición de f.

$= f(a^m) + f(a^n)$, por definición de f

$= f(x) + f(y)$, sustituyendo.

Así, hemos desmostrado que f es homomorfismo.

ii) Veamos ahora la inyectividad de f.

Sean $x, y \in G$, entonces existen $m, n \in Z$, tales que $x = a^m$, $y = a^n$

Luego, si $f(x) = f(y)$ entonces $f(a^m) = f(a^n)$.

Entonces, por definición de f, $m = n$.

Luego, $a^m = a^n$. En consecuencia, $x = y$.

Así, queda demostrado que, f es inyectivo.

iii) Finalmente probaremos que f es suryectivo.

Por la definición 2.25, la $Imf = \{ n \in Z \ / \exists x \in G, f(x) = n \}$.

Entonces, por la definición de f, tenemos que

$$Imf = \{ n \in Z \ / \exists a^n \in G, \ f(a^n) = n \}.$$

Luego, cada $n \in Z$ tiene una imagen inversa en G.

Así, hemos demostrado que, f es suryectivo

Por lo tanto, concluimos que f es un isomorfismo, y en consecuencia $G \cong Z$.□

Proposición 2.27:

Sean $(G, *)$ y (G^1, T) dos grupos, y $x \in G$ tal que $o(x) = n$

Si $f: G \to G^1$ es un homomorfismo, entonces $o(f(x)) = n$.

Demostración

Sean $f\ (G, *) \rightarrow (G^1, T)$ un homomorfismo, y $x \in G$ tal que $o(x) = n$.

Por la definición 2.16, $x^n = e$

Luego, $f(x^n) = f(e)$

Entonces, por la proposición 2.20, $f(x^n) = e^1$.

Ahora, probaremos que $f(x^n) = [f(x)]^n$, $n \in Z^+$.

- Si $n = 1$, entonces $f(x) = [f(x)]^1$.
- Supongamos que para $n = k > 1$, $k \in Z$, se cumple que

$$f(x^k) = [f(x)]^k \qquad (1).$$

- En lo que sigue veremos si se verifica para $n = k + 1$.

En efecto, $f(x^{k+1}) = f(x^k * x)$, por la proposición 2.4.

$= f(x^k)\ T\ f(x)$, f es homomorfismo

$= [f(x)]^k\ T\ f(x)$, por la hipótesis (1).

$= [f(x)]^{k+1}$, por la proposición 2.4

Luego, para todo $n \in Z^+$, $f(x^n) = [f(x)]^n$.

Como consecuencia de este resultado tenemos que

$$f(x^n) = [f(x)]^n = e^1$$

Por lo tanto, concluimos que $o(f(x)) = n$ □

Definición 2.28:

Sea $G \neq \phi$ un conjunto. Definiremos a B(G) como el conjunto de todas las aplicaciones biyectivas del conjunto G sobre si mismo. Es decir que,

$$B(G) = \{f: G \to G \,/\, f \text{ es biyectiva}\}.$$

Es fácil verificar que B(G) con la composición usual de funciones, como ley de composición interna, (B(G), o), es un grupo; lo cual dejaremos al lector como ejercicio.

Definición 2 29:

Sea (G, *) un grupo. Definiremos por $\mathcal{A}(G)$ al conjunto de todos los automorfismos de G, es decir que,

$\mathcal{A}(G) = \{f : G \to G \,/\, f \text{ es automorfismo}\}$.

Proposición 2.27:

Si (G, *) es un grupo, entonces ($\mathcal{A}(G)$, o) es un grupo.

Demostración:

Sea (G, *) un grupo.

Probaremos que $\mathcal{A}(G)$ sg B(G).

- Primeramente debemos probar que $\mathcal{A}(G) \subseteq B(G)$

Sea $h \in \mathcal{A}(G)$, entonces h es un automorfismo de G.

Luego, h es un isomorfismo, es decir, un homomorfismo biyectivo de G sobre si mismo. Así, $h \in B(G)$

En consecuencia $\mathcal{A}(G) \subseteq B(G)$.

- Ahora probaremos que $\mathcal{A}(G) \neq \phi$.

En el ejemplo 2.23, probamos que $I : G \to G$ tal que $I(x) = x$ es un automorfismo.

Luego, $I \in \mathcal{A}(G) \neq \phi$

Además, I es el elemento neutro de $\mathcal{A}(G)$.

- A continuación probaremos que, si $f_1, f_2 \in \mathcal{A}(G)$, entonces $(f_1 \circ f_2) \in \mathcal{A}(G)$.

Sean $f_1, f_2 \in \mathcal{A}(G)$ y $x, y \in G$.

Luego,

$(f_1 \circ f_2)(x * y) = f_1(f_2(x * y))$, por definición de la compuesta.

$= f_1 (f_2(x) * f_2(y))$, f_2 es un automorfismo.

$= f_1(f_2(x) * f_1 (f_2 (y))$, f_1 es un automorfismo.

$= (f_1 \circ f_2) (x) * (f_1 \circ f_2)(y)$, por definición de la compuesta

Así, $(f_1 \circ f_2) \in \mathcal{A}(G)$

- Finalmente probemos que, si $f \in \mathcal{A}(G)$, entonces $f^{-1} \in \mathcal{A}(G)$.

Sea $f \in \mathcal{A}(G)$, entonces $f \in B(G)$ Luego $f^{-1} \in B(G)$, puesto que B(G) es un grupo

Sean $x, y \in G$, entonces $f^{-1}(x), f^{-1}(y) \in G$.

Luego $f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x) * f(f^{-1}(y))$, f es homomorfismo.

$= (f \circ f^{-1})(x) * (f \circ f^{-1})(y)$, por definición de la compuesta.

$= I(x) * I(y)$, propiedad de los inversos

$= x * y$, definición de I.

Entonces $f^{-1}(x) * f^{-1}(y) = f^{-1}(x * y)$

Luego, $f^{-1} \in \mathcal{A}(G)$

Hemos demostrado, en virtud de la proposición 2 9, que $\mathcal{A}(G) \leq_{sg} B(G)$

Por lo tanto, $(\mathcal{A}(G), \circ)$ es un grupo.□

Definición 2 30

Sea (G, *) un grupo. Definiremos automorfismo interior correspondiente a $g \in G$, a la aplicación f_g. $G \to G$ tal que

$f_g(x) = g^{-1} * x * g$, para todo $x \in G$.

Proposición 2.28:

Si (G, *) es un grupo y $g \in G$, entonces $f_g \in \mathcal{A}(G)$

Demostración.

Sean (G, *) un grupo y $g \in G$

Por la definición 2 30, f_g: $G \to G$ tal que $f_g(x) = g^{-1} * x * g$, para todo $x \in G$ es un automorfismo interior de g.

- Primero debemos probar que f_g es un homomorfismo.

Sean $x,y \in G$ Entonces

$f_g(x * y) = g^{-1} * (x * y) * g$, por definición de f_g

$= g^{-1} * (x * e * y) * g$, por propiedad del neutro

$= g^{-1} *[x * (g * g^{-1}) * y] * g$, por propiedad de los inversos

$= (g^{-1} * x * g) *(g^{-1} * y * g)$, asociando

$= f_g(x) * f_g(y)$, por definición de f_g

Luego, f_g es un homorfismo

- Ahora probemos que f_g es inyectivo.

Sean $x, y \in G$

Si $f_g(x) = f_g(y)$, entonces $g^{-1} * x * g = g^{-1} * y * g$, por definición de f_g

Luego, por la ley cancelativa (Lema 2.1) , $x = y$

Así, f_g es inyectivo

- Finalmente probaremos la suryectividad.

Sea $y \in G$. Si $x = g * y * g^{-1}$, entonces

$f_g(x) = g^{-1} * (g * y * g^{-1}) * g$, por definición de f_g

$= (g^{-1} * g) * y * (g^{-1} * g)$, por asociatividad.

$= e * y * e$, por propiedad de los inversos

$= y$, por propiedad del neutro

Luego, f_g es suryectivo.

Por lo tanto, concluimos que, f_g es un automorfismo de G. Es decir que, $f_g \in \mathcal{A}(G)$ □

Proposición 2.29:

Si (G, *) es un grupo abeliano, entonces $f_g = I$, para $g \in G$.

Demostración

Sean (G, *) un grupo abeliano y $g \in G$

Si $x \in G$, entonces $f_g(x) = g^{-1} * x * g$, por definición de f_g

$= g^{-1} * g * x$, por conmutatividad.

$= e * x$, propiedad de los inversos.

$= x$, propiedad del neutro

$= I(x)$, por definición de I.

Por lo tanto, $f_g = I$.□

Pero, si (G, *) es no abeliano, existen $g,y \in G$ tales que $g * y \neq y * g$, luego $f_g(y) = g^{-1} * y * g \neq y$. Por lo tanto, $f_g \neq I$

Definición 2.31

Sea (G, *) un grupo. Definiremos por $A_i(G)$ al conjunto de los automorfismos interiores de G. Es decir que,

$A_i(G) = \{f_g \in \mathcal{A}(G) / g \in G\}$.

De esta definición deducimos que $A_i(G) \subseteq \mathcal{A}(G)$ Además, si $x \in G$, entonces

$I(x) = x$, por definición de I.

$= e * x * e.$, por propiedad del neutro

$= e^{-1} * x * e$, $e^{-1} = e$

$= I_e(x)$, por la definición 2.30.

Luego, $I = I_e \in A_i(G)$.

Proposición 2.30:

Si (G, *) es un grupo, entonces (A_χ(G), ∘) es un grupo.

Demostración.

Por demostrar que $A_\chi(G) \leq_{sg} a(G)$.

- Sabemos que $A_\chi(G) \subseteq a(G)$.

- Además, probamos que $I_e \in A_\chi(G)$. En consecuencia $A_\chi(G) \neq \phi$.

- Ahora, probaremos que, si $f_g, f_y \in A_\chi(G)$, entonces $(f_g \circ f_y) \in A_\chi(G)$.

Sean $g, y \in G$ y $f_g, f_y \in A_\chi(G)$. Luego, si $x \in G$, entonces

$(f_g \circ f_y)(x) = f_g(f_y(x))$, por definición de la compuesta.

$= f_g(y^{-1} * x * y)$, por la definición 2.30

$= g^{-1} * (y^{-1} * x * y) * g$, por la definición 2.30.

$= (g^{-1} * y^{-1}) * x * (y * g)$, por asociatividad

$= (y * g)^{-1} * x * (y * g)$, por el lema 2.1.

$= f_y * g(x)$, por la definición 2.30

Luego, $(f_g \circ f_y) \in Ad(G)$

- Finalmente vamos a probar que $f_g \in Ad(G)$ tiene inverso en $Ad(G)$

Sean g, x, $\in$ G Entonces,

$I(x) = I_e(x)$, resultado anterior a esta proposición

$= e^{-1} * x * e$, por la definición 2 30

$= f_e(x)$, por la definición 2.30.

$= f_{g-1} * g(x)$, por propiedad de los inversos

$= (f_g \circ f_{g-1})(x)$, por el resultado anterior

Luego, el inverso de f_g es f_{g-1}.

Así, por la proposición 2 9, $Ad(G)_{sg}\ a(G)$.

Por lo tanto, $(Ad(G), \circ)$ es un grupo.□

Teorema (de cayley) 2.2:

Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.

Demostración

Sean $(G, *)$ un grupo, y $g \in G$

Sea $T = \{t_g : G \to G \,/\, t_g(x) = g * x, \forall x \in G\}$ y $B(G) = S_n$.

Primero vamos a probar que $T \leq_{sg} B(G)$.

i) Sean $x, y \in G$. Luego, si $t_g(x) = t_g(y)$, entonces $g * x = g * y$, por definición de t_g. De donde $x = y$, por el Lema 2.1. Así, t_g es inyectivo.

ii) Sea $y \in G$. Entonces, $y = e * y$, por propiedad del neutro.

$= (g * g^{-1}) * y$, por propiedad de los inversos.

$= g * (g^{-1} * y)$, por asociatividad.

$= t_g (g^{-1} * y)$, por definición de t_g.

Luego, para cada $y \in G$, existe $x = (g^{-1} * y) \in G$ tal que $t_g(x) = y$.

Así, t_g es suryectivo.

En consecuencia t_g es biyectivo. Es decir que, $t_g \in B(G)$.

Por lo tanto, $T \subseteq B(G)$

iii) Como $e \in G$, entonces $t_e \in T$.

Es más, $t_e = I$, puesto que $t_e(x) = e * x = x$, para todo $x \in G$ (1).

Luego, existe el elemento neutro $t_e = I \in T$.

Así, $T \neq \phi$

IV) Si $t_g, t_j \in T$, entonces $(t_g \circ t_j) \in T$.

Sean x, j, $\in G$, entonces $t_{g*j}(x) = (g * j) * x$, por definición de T.

$= g * (j * x)$, por asociatividad.

$= g * (t_j(x))$, por definición de T

$= t_g(t_j(x))$, por definición de T

$= (t_g \circ t_j)(x)$, por definición de la compuesta.

Luego, $t_g \circ t_j = t_{g*j}$, para todo $x \in G$ (2).

Así, $(t_g \circ t_j) \in T$

V) Probemos que todo elemento de T tiene su inverso en T.

Sea $g \in G$, entonces $g^{-1} \in G$

Por (2), $t_g \circ t_{g-1} = t_{g*g-1}$

$= t_e$, por propiedad de los inversos.

$= I$, por (1).

Luego, si $t_g \in T$, entonces su inverso será $t_{g-1} \in T$.

Por los resultados (i), (ii), (iii), (iv) y (v), y en virtud de la proposición 2.9, queda demostrado que T_{sg} B(G)

Ahora únicamente, nos resta demostrar que $G \cong T$.

En efecto,

Sea $h: G \to T$ una aplicación tal que $h(g) = t_g$, para todo $g \in G$ Por demostrar que h es un isomorfismo

- Sean $g, y \in G$ Luego,

$h(g * y) = t_{g*y}$, por definición de h.

$= t_g \circ t_y$, por el resultado (2).

$= h(g) \circ h(y)$, por definición de h.

Así, h es un homomorfismo.

- Probemos la inyectividad de h.

Sea $g \in Nh$, entonces $h(g) = I$, por la definición 2.24

$t_g = I$, por definición de h.

$t_g(x) = I(x)$, $x \in G$

$g * x = x$, por definición de t_g y de I.

$g = e$, por propiedad del neutro.

Así, $Nh = \{e\}$. Luego, por la proposición 2.25, h es inyectivo

- Finalmente probaremos que h es suryectivo.

Sea $t_g \in T$, entonces existe $g \in G$ tal que $h(g) = t_g$

Luego, h es suryectivo.

Hemos demostrado que h es un isomorfismo

Por lo tanto, $G \cong T$, T_{sg} B(G).□

CAPITULO III

PROPUESTA DIDACTICA PARA INTRODUCIR LA TEORIA DE GRUPOS

Como requisito indispensable cada grupo de tres alumnos deberá tener (en el aula) una cartulina, un lápiz, una regla, unas tijeras, un transportador, una tabla 11" x 11" (no muy gruesa), un clavo y un martillo.

Con estos materiales a mano lo primero que harán, será dibujar, en la tabla, un plano cartesiano de tamaño considerable. Luego, en la cartulina, un triángulo equilátero de lado 5" y vértices A, B y C, el cual recortarán con las tijeras. Después, hallarán el baricentro de dicho triángulo, lo perforarán con el clavo para ubicarlo justamente sobre el centro del plano cartesiano, y posteriormente martillarán el clavo hasta dejarlo firme y en forma vertical, de manera tal que el vértice C quede sobre el eje x, como podemos apreciar en la Fig. 1.

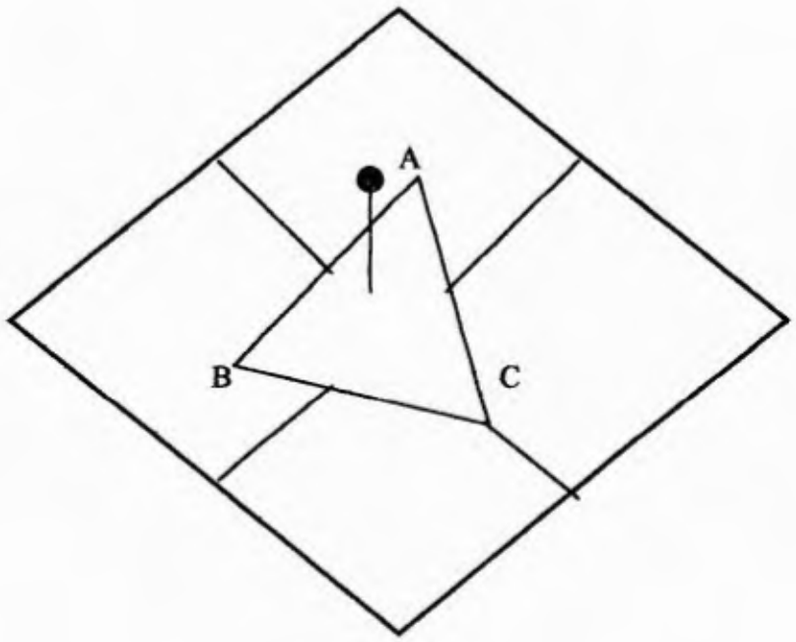

Fig 1

Ahora los alumnos harán rotar el triángulo 120°, en sentido antihorario, alrededor del clavo. Después escribirán lo que han observado.

En efecto, el resultado de esta rotación, o mejor dicho lo que debieron observar los alumnos es que; el vértice A tomo la posición del vértice B, éste la posición del vértice C, y éste último la posición del vértice A, como lo muestra la Fig. 2.

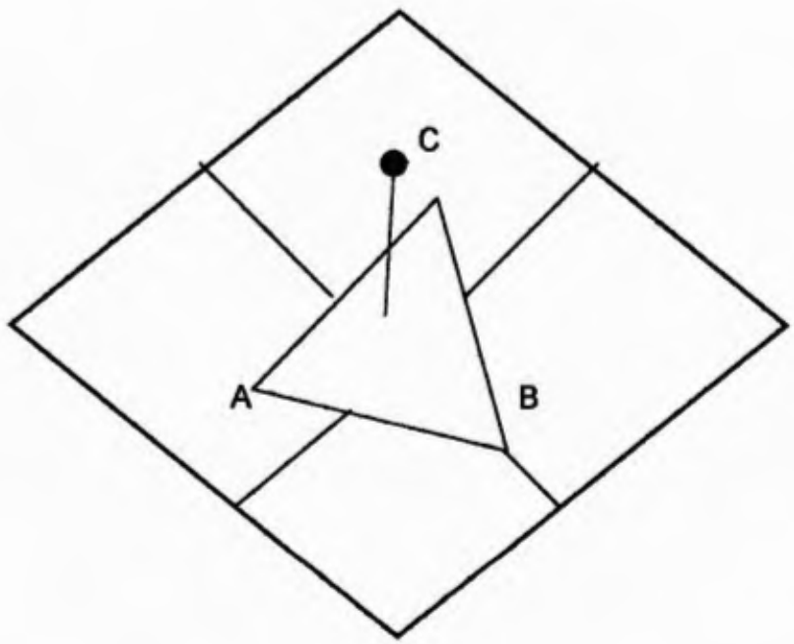

Fig. 2

Luego, en común acuerdo le podrán nombre a esta primera rotación. Siendo el más adecuado r_1.

Finalmente escribirán dicha rotación como un conjunto de pares ordenados, donde la abscisa será el vértice en su posición original y la ordenada la posición que ocupará dicho vértice después de la rotación. Entonces deberán escribir que

$$r_1 = \{(A, B), (B, C), (C, A)\}$$

Posteriormente deberán colocar el triángulo en su posición original, como en la Fig. 1.

Luego, harán lo mismo que en la fase anterior. Pero rotando el triángulo 240°.

En esta ocasión los alumnos deberán observar que: el vértice A pasó a ocupar la posición del vértice C, éste la posición del vértice B, y éste último la posición del vértice A, como podemos ver en la Fig. 3.

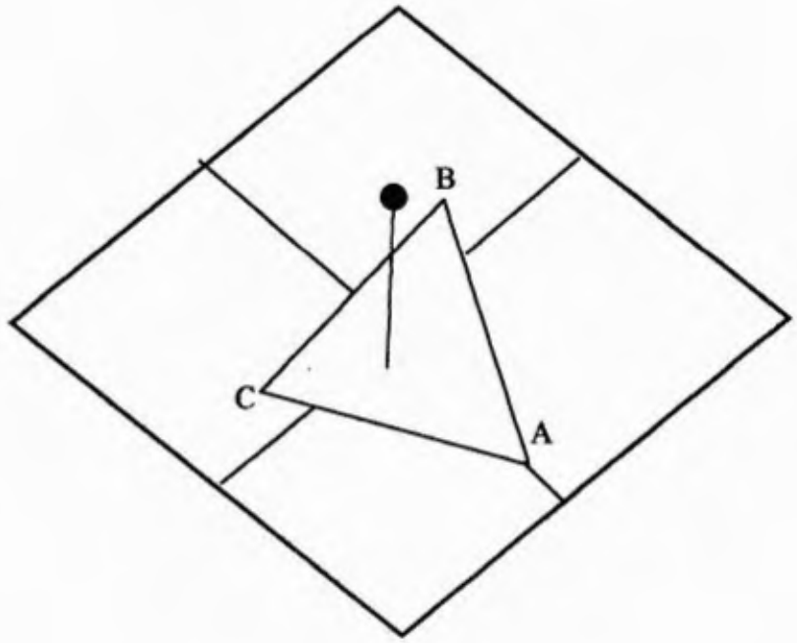

Fig 3

Además, tomando como referencia la primera rotación, a ésta la llamarán r_2, y la escribirán de la siguiente manera

$$r_2 = \{(A, C), (B, A), (C, B)\}$$

En una tercera fase colocarán nuevamente el triángulo en su posición original, Fig 1, y después lo rotarán 360° en sentido antihorario.

Luego de esta rotación, los alumnos, deben percatarse de que el triángulo se ha mantenido invariante

Llamando r_o a dicha rotación, la escribirán así

$$r_o = \{(A, A), (B, B), (C, C)\}$$

Por otro lado, una transformación, matemáticamente, es una operación por la cual se proyecta una figura geométrica formando otra. Entonces, podemos afirmar que r_o, r_1 y r_2 son transformaciones del triángulo ABC en sí mismo

Designemos, ahora por R al conjunto cuyos elementos son dichas transformaciones. Es decir que,

$$R = \{ r_o, r_1, r_2\}$$

Seguidamente preguntamos a los alumnos..

¿Qué sucedería si aplicamos dos transformaciones, en forma consecutiva, a cada uno de los vértices del triángulo ABC?

Expliquemos de que se trata...

Por ejemplo, primeramente le aplicamos al vértice A la transformación r_1 y al resultado de esto le aplicamos la transformación r_2

En efecto, los alumnos observarán que r_1 lleva a A sobre el vértice B, y que r_2, lleva a B sobre el vértice A. Luego, contestarán que el resultado de aplicar r_1 y r_2, consecutivamente, a A es el mismo vértice A.

Después de esto les enseñaremos el simbolismo matemático que se utiliza para representar estos cálculos. Entonces, para expresar que el resultado de aplicar r_1 al vértice A es igual a B, escribimos.

$$r_1 (A) = B$$

Similarmente, para expresar que el resultado de aplicar r_2 al vértice B es igual a A, escribimos.

$$r_2 (B) = A$$

Por lo tanto, escribimos

$$r_2 (r_1 (A)) = r_2 (B) = A,$$

para expresar que el resultado de aplicar las transformaciones r_1 y r_2, en forma consecutiva, al vértice A es igual a A.

Ahora vamos a definir una operación entre dos transformaciones cualesquiera del triángulo ABC, la cual denotaremos por o.

En efecto, llamaremos **composición** de dos transformaciones, r y s, a la operación s o r, que consiste en aplicar las dos transformaciones, consecutivamente, primero r y después s, a cada vértice del triángulo ABC.

Luego, la composición de r_1 y r_2 se escribe r_2 o r_1. Así, $(r_2 \text{ o } r_1)$ (A) expresa la aplicación consecutiva de r_1 y r_2 al vértice A.

Por lo tanto, $(r_2 \text{ o } r_1)(A) = r_2 (r_1 (A))$

$= r_2 (B)$

$= A.$

En lo que sigue los alumnos deberán aplicar r_0 o r_0, r_0 o r_1, r_0 o r_2, r_1 o r_0, r_1 o r_1, r_1 o r_2, r_2 o r_0, r_2 o r_1, y r_2 o r_2, a cada vértice y escribir los resultados como conjuntos de pares ordenados.

Los resultados que los estudiantes deben obtener son los siguientes.

1 $(r_0 \text{ o } r_0)$ (A) = $r_0 (r_0 (A)) = r_0 (A) = A$

$(r_0 \text{ o } r_0)$ (B) = $r_0 (r_0 (B)) = r_0 (B) = B$

$(r_0 \text{ o } r_0)$ (C) = $r_0 (r_0 (C)) = r_0 (C) = C$

Luego, $(r_0 \text{ o } r_0) = \{(A, A), (B, B), (C, C)\} = r_0$

2. $(r_0 \text{ o } r_1)$ (A) = $r_0 (r_1 (A)) = r_0 (B) = B$

$(r_0 \circ r_1)(C) = r_0(r_1(C)) = r_0(C) = C$

$(r_0 \circ r_1)(A) = r_0(r_1(A)) = r_0(A) = A$

Así, $(r_0 \circ r_1) = \{(A, B), (B, C), (C, A)\} = r_1$

3. $(r_0 \circ r_2)(A) = r_0(r_2(A)) = r_2(A) = A$

$(r_0 \circ r_2)(B) = r_0(r_2(B)) = r_2(B) = B$

$(r_0 \circ r_2)(C) = r_0(r_2(C)) = r_2(C) = C$

Entonces, $r_0 \circ r_2 = \{(A, C), (B, A), (C, B)\} = r_2$

4. $(r_1 \circ r_0)(A) = r_1(r_0(A)) = r_1(A) = B$

$(r_1 \circ r_0)(A) = r_1(r_0(B)) = r_1(B) = C$

$(r_1 \circ r_0)(C) = r_1(r_0(C)) = r_1(C) = A$

Luego, $r_1 \circ r_0 = \{(A,B),(B,C),(C,A)\} = r_1$

5. $(r_1 \circ r_1)(A) = r_1(r_1(A)) = r_1(B) = C$

$(r_1 \circ r_1)(B) = r_1(r_2(A)) = r_2(A) = A$

$(r_1 \circ r_1)(C) = r_1(r_1(C)) = r_1(A) = B$

Así, $r_1 \circ r_1 = \{(A,C), (B,A), (C,B)\} = r_2$

6. $(r_1 \circ r_2)(A) = r_1(r_2(A)) = r_1(C) = A$

$(r_1 \circ r_2)(B) = r_1(r_2(B)) = r_1(A) = B$

$(r_1 \circ r_2)(C) = r_1(r_2(C)) = r_1(B) = C$

Entonces, $r_1 \circ r_2 = \{(A,A), (B,B), (C,C)\} = r_0$

7. $(r_2 \circ r_0)(A) = r_2(r_0(A)) = r_2(A) = C$

$(r_2 \circ r_0)(B) = r_2(r_0(B)) = r_2(B) = A$

$(r_2 \circ r_0)(C) = r_2(r_0(C)) = r_2(C) = B$

Luego, $r_2 \circ r_0 = \{(A,C), (B,A), (B,A)\} = r_2$

8. $(r_2 \circ r_1)(A) = r_2(r_1(A)) = r_2(B) = A$

$(r_2 \circ r_1)(B) = r_2(r_1(B)) = r_2(C) = B$

$(r_2 \circ r_1)(C) = r_2(r_1(C)) = r_2(A) = C$

Así, $r_2 \circ r_1 = \{(A,A), (B,B), (C,C)\} = r_0$

Por último

9. $(r_2 \circ r_2)(A) = r_2(r_2(A)) = r_2(C) = B$

$(r_2 \circ r_2)(B) = r_2(r_2(B)) = r_2(A) = C$

$(r_2 \circ r_2)(C) = r_2(r_2(C)) = r_2(B) = A$

Luego $r_2 \circ r_2 = \{(A,B), (B,C), (C,A)\} = r_1$

Una vez obtienen estos resultados, reiteramos la pregunta anterior ¿Qué sucederá si aplicamos dos transformaciones, en forma consecutiva, a cada uno de los vértices del triángulo ABC? O mejor dicho ¿Cuál es el resultado de la composición de dos transformaciones del conjunto R?.

En efecto, deberán contestar que al aplicar dos transformaciones consecutivamente, a cualquier vértice del triángulo se obtendrá un vértice de dicho triángulo. Además deberán concluir que la composición de dos transformaciones del conjunto R da como resultado otra transformación del mismo conjunto.

Luego de estas conclusiones les definimos lo siguiente Llamamos ley de composición interna en un conjunto a aquella operación que aplicada a dos elementos del conjunto da como resultado otro elemento de dicho conjunto. Por lo tanto, la operación o es ley de composición interna en el conjunto R

Construyamos ahora la tabla de la operación o, según los resultados obtenidos, la cual nos será útil más adelante.

0	r_o	r_1	r_2
r_o	r_o	r_1	r_2
r_1	r_1	r_2	r_o
r_2	r_2	r_o	r_1

Tabla 3 1

Trabajando con dicha tabla resolverán el siguiente ejercicio

Ejercicio # 1

Calcular:

1. r_o o (r_1 o r_2) = ?
2. (r_o o r_1) o r_2 = ?
3. r_2 o (r_2 o r_2) = ?
4. (r_2 o r_2) o r_1 = ?
5. r_1 o (r_2 o r_1) = ?
6. (r_1 o r_2) o r_1 = ?

Los estudiantes deberán obtener lo siguiente.

1. r_o o (r_1 o r_2) = r_o o r_0 = r_o
2. (r_o o r_1) o r_2 = r_1 o r_2 = r_o

   Entonces, r_o o (r_1 o r_2) = (r_o o r_1) o r_2
3. r_2 o (r_2 o r_1) = (r_0 o r_1) o r_2
4. (r_2 o r_2) o r_1 = r_1 o r_1 = r_2

   Luego, r_2 o (r_2 o r_1) = (r_2 o r_2) o r_1
5. r_1 o (r_2 o r_1) = r_1 o r_0 = r_1
6. (r_1 o r_2) o r_1 = r_o o r_1 = r_1

   Así, r_1 o (r_2 o r_1) = (r_1 o r_2) o r_1

Finalizado el ejercicio debemos decirles que esta propiedad se conoce como asociatividad, y que por lo tanto la operación o es asociativa.

Ahora observarán con atención la Tabla 3.1. para ver si existe un elemento que tenga la propiedad de que al componerlo (u operarlo) con cualquier elemento r, a derecha o a izquierda, dé como resultado otra vez el mismo elemento r.

La respuesta deberá ser que si existe tal elemento, y que el mismo es r_0; puesto que

$r_0 \circ r_0 = r_0$

$r_0 \circ r_1 = r_1 \circ r_0 = r_1$

$r_0 \circ r_2 = r_2 \circ r_0 = r_2$

Seguidamente les decimos que un elemento con tal propiedad recibe el nombre de elemento neutro. Luego, el conjunto R, con la operación o, tiene elemento neutro.

Nuevamente fijarán su atención en la Tabla 3.1 para ver si existe, para cada elemento de R, otro elemento de manera tal que al operarlos dé como resultado el elemento neutro.

Efectivamente, los alumnos deberán observar que

$$r_0 \circ r_0 = r_0$$

$$r_1 \circ r_2 = r_1 \circ r_2 = r_0$$

Luego les diremos que cuando esto ocurre los elementos se dicen inversos entre sí. Entonces, r_1 es inverso de r_2, mientras que r_0 es inverso de sí mismo.

Por lo tanto, en el conjunto R, todo elemento tiene su inverso, respecto a la operación o.

En adelante denotaremos por x^{-1} al elemento inverso de x.

Entonces, para el conjunto R, tenemos que

$$r_0^{-1} = r_0; \quad r_1^{-1} = r_2 \quad y \quad r_2^{-1} = r_1$$

Con esto ya estamos en condiciones de definirles lo que conocemos como grupo.

En efecto, un conjunto no vacio con una operación que es ley de composición interna, asociativa, que tiene elemento neutro y un inverso para cada elemento se llama **grupo.** Así el conjunto R con la operación o es un grupo; y lo denotamos por (R, o).

Además, les diremos que como R es finito, entonces (R, o) se dice grupo finito, y que la cantidad de elementos del conjunto R la llamamos orden del grupo, luego el orden de (R, o) es tres, lo que denotamos por a (R) = 3.

Hay otras propiedades que veremos más adelante. Por, ahora, tomarán el triángulo ABC y trazarán sobre él los tres ejes de simetría AA', BB' y CC', con líneas de trazos, como podemos apreciar en la Fig. 4

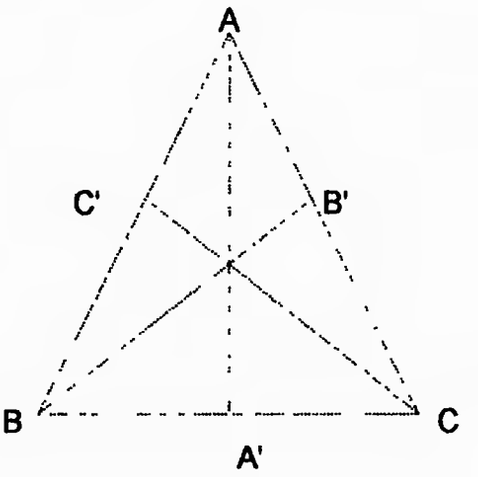

Fig. 4

Luego un estudiante de cada grupo mantendrá el triángulo suspendido en el aire en forma horizontal, y otro estudiante le colocará (al triángulo) un lápiz

justamente debajo del eje de simetría AA', tal como vemos a la Fig. 5. (visto desde arriba)

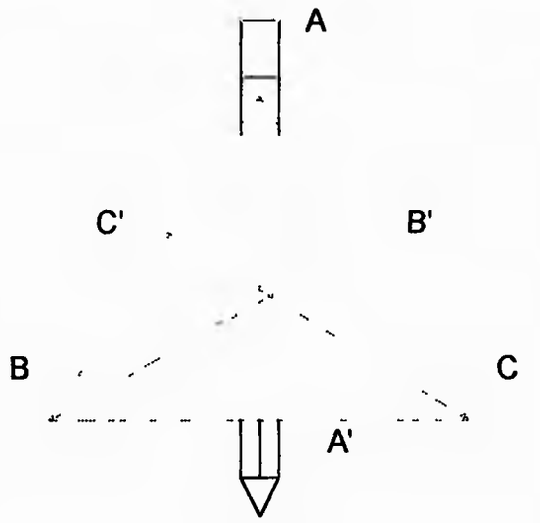

Fig. 5

Después, el estudiante que está sujetando el triángulo, lo hará rotar 180° en sentido anti-horario alrededor del lápiz y anotarán lo observado tal como hicieron con las tres rotaciones anteriores.

En efecto, los estudiantes deben haber observado que el vértice C pasó a ocupar la posición del vértice B y viceversa, mientras que el vértice A se mantiene invariante, como nos lo muestra la Fig 6

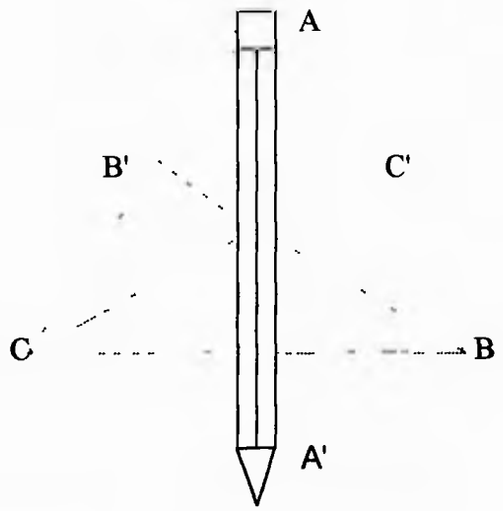

Fig. 6

Entonces, llamando s_1 a esta rotación, la escribirán así:

$$s_1 = \{(A, A), (B, C), (C, B)\}$$

A continuación los alumnos harán lo mismo, pero colocando el lápiz debajo del eje BB' y también, escribirán lo que han observado.

En esta ocasión los estudiantes deberán percatarse de que el vértice A ha tomado la posición del vértice C y viceversa, quedando invariante el vértice B este resultado lo podemos apreciar en la Fig. 7

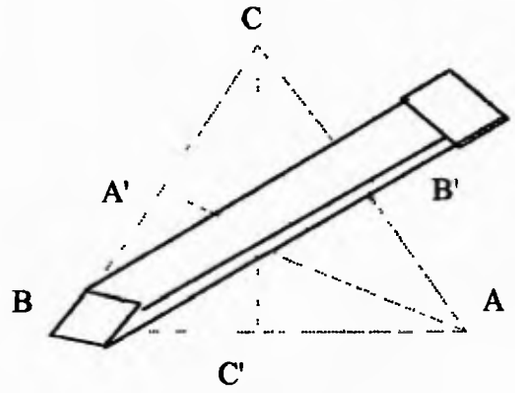

Fig. 7

Poniéndole por nombre s_2 a dicha rotación, la escribirán de la manera siguiente:

$$s_2 = \{(A, C), (B, B), (C, A)\}$$

Por último, colocarán el lápiz debajo del eje de simetría CC' y después harán rotar el triángulo 180° en sentido antihorario.

Esta vez escribirán, que observaron, que el vértice C se mantuvo invariante, mientras que los vértices A y B cambiaron de posición entre sí, como nos muestra la Fig. 8.

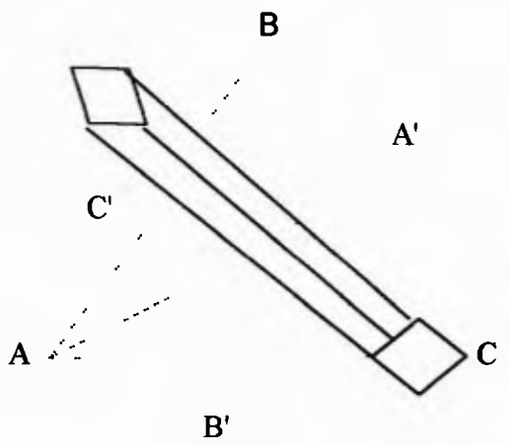

Fig 8

Luego, llamando s_3 a esta rotación, escribirán la misma así:

$$s_3 = \{(A, B), (B, A), (C, C)\}$$

Los alumnos han encontrado tres transformaciones más, del triángulo ABC. Denotemos por S al conjunto cuyos elementos son dichas transformaciones. Es decir

$$S = \{s_1, s_2, s_3\}$$

Seguidamente les preguntamos ... ¿Es (S, o) un grupo?

Es de esperar que empiecen por averiguar si la operación o es ley de composición interna en S Para lo cual obtendrán los siguientes resultados:

10. $(s_1 \text{ o } s_1)(A) = s_1(s_1(A)) = s_1(A) = A$

$(s_1 \text{ o } s_1)(B) = s_1(s_1(B)) = s_1(C) = B$

$(s_1 \circ s_1)(C) = s_1(s_1 C) = s_1(B) = C$

Luego, $s_1 \circ s_1 = \{(A, A), (B, B), (C, C)\} = r_0$

11. $(s_1 \circ s_2)(A) = s_1(s_2(A)) = s_1(C) = B$

$(s_1 \circ s_2)(B) = s_1(s_2(B)) = s_1(B) = C$

$(s_1 \circ s_2)(C) = s_1(s_2 C) = s_1(A) = A$

Entonces, $s_1 \circ s_2 \{(A, B), (B, C), (C, A)\} = r_1$

12. $(s_1 \circ s_3)(A) = s_1(s_3(A)) = s_1(B) = C$

$(s_1 \circ s_3)(B) = s_1(s_3(B)) = s_1(A) = A$

$(s_1 \circ s_3)(C) = s_1(s_3(C)) = s_1(C) = B$

Así, $s_1 \circ s_3 = \{(A, C), (B, A), (C, B)\} = r_2$

13. $(s_2 \circ s_1)(A) = s_2(s_1(A)) = s_2(A) = C$

$(s_2 \circ s_1)(B) = s_2(s_1(B)) = s_2(C) = A$

$(s_2 \circ s_1)(C) = s_2(s_1(C)) = s_2(B) = B$

Luego, $s_2 \circ s_1 \{(A, C), (B, A), (C, B)\} = r_2$

14. $(s_2 \circ s_2)(A) = s_2(s_2(A)) = s_2(A) = A$

$(s_2 \circ s_2)(B) = s_2(s_2(B)) = s_2(B) = B$

$(s_2 \circ s_2)(C) = s_2(s_2(C)) = s_2(C) = C$

Entonces, $s_2 \circ s_2 \{(A, A), (B, B), (C, C)\} = r_0$

15. $(s_2 \circ s_3)(A) = s_2(s_3(A)) = s_2(B) = B$

$(s_2 \circ s_3)(B) = s_2(s_3(B)) = s_2(A) = C$

$(s_2 \circ s_3)(C) = s_2(s_3(C)) = s_2(C) = A$

Así, $s_2 \circ s_3 = \{(A, B), (B, C), (C, A)\} = r_1$

16. $(s_3 \circ s_1)(A) = s_3(s_1(A)) = s_3(A) = B$

$(s_3 \circ s_1)(B) = s_3(s_1(B)) = s_3(C) = C$

$(s_3 \circ s_1)(C) = s_3(s_1(C)) = s_3(B) = A$

Luego, $s_3 \circ s_1 = \{(A, B), (B, C), (C, A)\} = r_1$

17. $(s_3 \circ s_2)(A) = s_3(s_2(A)) = s_3(C) = C$

$(s_3 \circ s_2)(B) = s_3(s_2(B)) = s_3(B) = A$

$(s_3 \circ s_2)(C) = s_3(s_2(C)) = s_3(A) = B$

Entonces, $s_3 \circ s_2 = \{(A, C), (B, A), (C, B)\} = r_2$

18. $(s_3 \circ s_3)(A) = s_3(s_3(C)) = s_3(B) = A$

$(s_3 \circ s_1)(B) = s_3(s_3(B)) = s_3(A) = B$

$(s_3 \circ s_1)(C) = s_3(s_1(C)) = s_3(B) = C$

Así, $s_3 \circ s_3 = \{(A, A), (B, B), (C, C)\} = r_0$

En efecto, los estudiantes deberán concluir que la operación **o** no es ley de composición interna en S, y que por lo tanto (S, o) no es grupo.

Después de haber visto esto, preguntamos a los estudiantes si la unión de los conjuntos R y S sería un grupo con la operación **o**.

Designamos por T a la unión de los conjuntos R y S. Entonces, $T = R \cup S$. Es decir.

$$T = \{r_0, r_1, r_2, s_1, s_2, s_3\}$$

Ahora los alumnos deberán verificar si (T, o) es un grupo o no. Obviamente los resultados (1), (2), ..., (18) son válidos para este ejercicio, por lo cual el mismo no será tan largo.

En forma similar a lo que ya han realizado hallarán que:

$r_0 \circ s_1 = \{(A, A), (B, C), (C, B)\} = s_1$

$r_0 \circ s_2 = \{(A, C), (B, B), (C, A)\} = s_2$

$r_0 \circ s_3 = \{(A, B), (B, A), (C, C)\} = s_3$

Además,

$r_1 \circ s_1 = \{(A, B), (B, A), (C, C)\} = s_3$

$r_1 \circ s_2 = \{(A, A), (B, C), (C, B)\} = s_1$

$r_1 \circ s_3 = \{(A, C), (B, B), (C, A)\} = s_2$

También,

$r_2 \circ s_1 = \{(A, C), (B, B), (C, A)\} = s_2$

$r_2 \circ s_2 = \{(A, B), (B, A), (C, C)\} = s_3$

$r_2 \circ s_3 = \{(A, A), (B, C), (C, B)\} = s_1$

Lo mismo que,

$s_1 \circ r_0 = \{(A, A), (B, C), (C, B)\} = s_1$

$s_1 \circ r_1 = \{(A, C), (B, B), (C, A)\} = s_2$

$s_1 \circ r_2 = \{(A, B), (B, A), (C, C)\} = s_3$

Además,

$s_2 \circ r_0 = \{(A, C), (B, B), (C, A)\} = s_2$

$s_2 \circ r_1 = \{(A, B), (B, A), (C, C)\} = s_3$

$s_2 \circ r_2 = \{(A, A), (B, C), (C, B)\} = s_1$

Por último,

$s_3 \circ r_0 = \{(A, B), (B, A), (C, C)\} = s_3$

$s_3 \circ r_1 = \{(A, A), (B, C), (C, B)\} = s_1$

$s_3 \circ r_2 = \{(A, C), (B, B), (C, A)\} = s_2$

Acerca de estos resultados (junto con los anteriores) deberán concluir que la operación o es ley de composición interna en T, que r_0 es el elemento neutro y que cada elemento tiene su inverso:

$$r_0^{-1} = r_0;\ r_1^{-1} = r_2;\ r_2^{-1} = r_1;\ s_1^{-1} = s_1;\ s_2^{-1} = s_2;\ s_3^{-1} = s_3$$

Finalmente verificarán que o es asociativa en T; y entonces concluirán que (T, o) es un grupo.

A continuación construirán una tabla similar a la Tabla 3.1, la cual deberá quedar así:

o	r_0	r_1	r_2	s_1	s_2	s_3
r_0	r_0	r_1	r_2	s_2	s_2	s_3
r_1	r_1	r_2	r_0	s_3	s_1	s_2
r_2	r_2	r_0	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	r_0	r_1	s_2
s_2	s_2	s_3	s_1	r_2	r_0	r_1
s_3	s_3	s_1	s_2	r_1	r_2	r_0

Tabla 3 2

Después resolverán el siguiente ejercicio utilizando los datos de la Tabla 3 2

Ejercicio #2

I. Parte. Calcular

i) $(r_2^{-1})^{-1} = ?$ ii) $(s_3^{-1})^{-1} = ?$

iii) $(r_1 \ o \ s_2)^{-1} = ?$ iv) $s_2^{-1} \ o \ r_1^{-1} = ?$

II. Parte. Probar que

i) Si r_1 o s_1 = x o s_1 entonces $x = r_1$

ii) Si s_1 o r_1 = s_1 ó x entonces $x = r_1$

III. Parte. Resolver las siguientes ecuaciones

i) r_1 o x = s_2

ii) x o r_1 = s_1

La solución de los estudiantes deberá ser la siguiente:

I Parte.

i) $(r_2^{-1})^{-1} = (r_1)^{-1} = r_2$

ii) $(s_3^{-1})^{-1} = (s_3)^{-1} = s_3$

iii) $(r_1 \circ s_2)^{-1} = (s_1)^{-1} = s_1$

iv) $s_2^{-1} \circ r_1^{-1} = s_2 \circ r_2 = s_1$

II Parte.

i) Operación s_1^{-1} a derecha con la igualdad $r_1 \circ s_1 = x \circ s_1$.

Es decir,

$$(r_1 \circ s_1) \circ s_1^{-1} = (x \circ s_1) \circ s_1^{-1}$$

Luego, asociando obtendrán que

$$r_1 \circ (s_1 \circ s_1^{-1}) = x \circ (s_1 \circ s_1^{-1})$$

Por propiedad de los inversos

$$r_1 \circ r_0 = x \circ r_0$$

Por propiedad del neutro

$$r_1 = x$$

ii) De manera similar, operarán s_1^{-1} a izquierda con a igualdad

$$s_1 \circ r_1 = s_1 \circ x$$

Es decir, s_1^{-1} o (s_1 o r_1 = s_1^{-1} o (s_1 o x)

Luego, asociando obtendrán

$$(s_1^{-1} \text{ o } s_1) \text{ o } r_1 = s_1^{-1} \text{ o } s_1) \text{o } x$$

Por propiedad de los inversos

$$r_0 \text{ o } r_1 = r_0 \text{ o } x$$

Por propiedad del neutro

$$r_1 = x$$

III. Parte

i) Operando r_1^{-1} a izquierda con la igualdad r_1 o x = s_2 obtendrán que

$$r_1^{-1} \text{ o } (r_1 \text{ o } x) = r_1^{-1} \text{ o } s_2$$

Asociando,

$$(r_1^{-1} \text{ o } r_1) \text{ o } x = r_1^{-1} \text{ o } s_2$$

Por propiedad de los inversos

$$r_0 \text{ o } x = r_1^{-1} \text{ o } s_2$$

Por propiedad del neutro

$$x = r_1^{-1} s_2$$

Con este resultado queda resuelta la ecuación r_1 o x = s_2

ii) Aquí deberán operar r_1^{-1} a derecha con la igualdad x o r_1 = s_2

Es decir, $(x \circ r_1) \circ r_1^{-1} = s_2 \circ r_1^{-1}$

Luego, asociando

$$x \circ (r_1 \circ r_1^{-1}) = s_2 \circ r_1^{-1}$$

Por propiedad de los inversos

$$x \circ r_0 = s_2 \circ r_1^{-1}$$

Por propiedad del neutro

$$x = s_2 \circ r_1^{-1}$$

Así, queda resulta la ecuación $x \circ r_1 = s_2$.

Una vez resuelto todo el ejercicio, los estudiantes deberán expresar lo que han descubierto a través del mismo. En su orden dirán que.

i) El inverso del inverso de un elemento es el mismo elemento. Es decir que, $(x^{-1})^{-1} = x$

ii) El inverso de la operación de dos elementos es igual a la operación de los inversos de dichos elementos, pero en orden contrario Esto es, $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

En cuanto a la segunda parte,

$$si \begin{cases} a \circ c = b \circ c, \text{ entonces } a = b \\ c \circ a = c \circ b, \text{ entonces } a = b \end{cases}$$

donde a, b y c pertenecen al mismo grupo.

Luego les haremos saber que esta propiedad es llamada Ley Cancelativa.

Por último, expresarán que las soluciones de las ecuaciones a o x = b y x o a = b, serán $x = a^{-1} \circ b$ y $x = b \circ a^{-1}$, respectivamente

Además, existen dos propiedades que los estudiantes ya deberían haber intuido u observado De no ser así, debemos ayudarles para que así sea Estos son: Primero que el elemento neutro es único Es decir que, en un grupo no pueden existir dos o más elementos neutros Y la otra es que, el elemento inverso de cada elemento, también, es único.

Hasta el momento hemos visto propiedades que se verifican en cualquier grupo, pero existen otras que no, como veremos

Comencemos con la siguiente pregunta... ¿Sería posible extraer subconjuntos de T que sean grupos con la misma operación **o**?

La respuesta deberá ser afirmativa, puesto que ellos saben que (R, o) es grupo, y que R es subconjunto de T.

Seguidamente les damos la siguiente definición:

Si (T, o) es un grupo cualquiera y R es subconjunto de T, y además (R, o) es un grupo, entonces R se dice subgrupo de T.

Ahora los alumnos deberán averiguar si T posee más subgrupos, para lo cual será indispensable el uso de la Tabla 3.2.

Los resultados deberán ser los siguientes:

1. Uno será $N = \{r_0\}$, puesto que

   Como $r_0 \circ r_0 = r_0$, entonces o es ley de composición interna en N.

   Además, $(r_0 \circ r_0) \circ r_0 = r_0 \circ (r_0 \circ r_0) = r_0$, o es asociativa.

   r_0 es elemento neutro.

   Existe el inverso, $r_0^{-1} = r_0$

2. Otro será $M = \{ r_0 , s_1\}$, dado que

   La operación o es ley de composición interna en M.

   $r_0 \circ r_0 = r_0$

   $r_0 \circ s_1 = s_1 \circ r_0 = s_1$

   $s_1 \circ s_1 = r_0$

   Además, o es asociativa.

   El elemento neutro es r_0 .

   Existen los inversos, $r_0^{-1} = r_0$ y $s_1^{-1} = s_1$

3. También P = {r_0, s_2), pues

   La operación **o** es ley de composición interna en P,

   r_0 o r_0 = r_0

   r_0 o s_2 = s_2 o r_0 = s_2

   s_2 o s_2 = r_0

   La operación **o** es asociativa.

   El elemento neutro es r_0.

   Existen los inversos $r_0^{-1} = r_0$ y $s_2^{-1} = s_2$

4. Además, Q = { r_0, s_3}, ya que

   La operación **o** es ley de composición interna Q.

   r_0 o r_0 = r_0

   r_0 o s_3 = s_3 o r_0 = s_3

   s_3 o s_3 = r_0

   La operación **o** es asociativa

   El elemento neutro es r_0.

   Existen los inversos, $r_0^{-1} = r_0$ y $s_2^{-1} = s_3$

5. Obviamente, el otro subgrupo es, el mismo T.

   Luego, (T, o) posee seis subgrupo N, M, P, Q, R, y T.

A continuación buscaremos la manera de introducir la conmutatividad diciéndoles que en nuestro diario vivir a veces realizamos, consecutivamente, dos acciones sin importar su orden y obtenemos el mismo resultado. Por

ejemplo, si en un cubo plástico vertemos cierta cantidad de pintura de color rojo, y después una cantidad igual de pintura de color amarillo obtendremos, de esta mezcla, pintura color anaranjado. Lo mismo ocurrirá si primero vertemos la pintura amarilla y después la roja.

Luego hacemos la pregunta ... ¿Ocurrirá lo mismo con las transformaciones del triángulo ABC?

Haciendo uso de la Tabla 3.2, los alumnos deberán responder que no siempre ocurre. Esto lo justificarán con ejemplos como $r_1 \circ s_1 \neq s_1 \circ r_1$. Puesto que

$$r_1 \circ s_1 = s_2 \text{ y } s_1 \circ r_1 = s_3$$

Seguidamente les preguntaremos que ... ¿En qué caso se cumple la propiedad en cuestión?

Ellos deberán contestar que en los siguientes casos:

$$r_0 \circ r_1 = r_1 \circ r_0 = r_1$$

$$r_0 \circ r_2 = r_2 \circ r_0 = r_2$$

$$r_1 \circ r_2 = r_2 \circ r_1 = r_0$$

$$r_0 \circ s_1 = s_1 \circ r_0 = s_1$$

$$r_0 \circ s_2 = s_2 \circ r_0 = s_2$$

$$r_0 \circ s_3 = s_3 \circ r_0 = s_3$$

Con esto basta para decirles que esta propiedad se llama conmutatividad; y que cuando ésta se verifica para dos elementos cualesquiera de un grupo, el mismo se llama grupo conmutativo o Abeliano.

Ahora preguntamos.. ¿Es T abeliano? ¿Algún subgrupo de T lo es?

Deberán responder que T no es abeliano, pero que N, M, P, R, y Q si lo son.

CONCLUSIONES

De este trabajo concluimos que:

1. Lo ideal hubiera sido llevar a la práctica nuestra propuesta didáctica, pero nos fue imposible. Sin embargo, haremos el intento en el futuro, pues ésta es la única manera de averiguar su efectividad, y además, porque nos permitirá corregir las posibles deficiencias de la misma.

2. El docente constructivista debe estar constantemente actualizado sobre su asignatura y su aplicación, porque puede ocurrir que los estudiantes presenten ejemplos que sean los menos indicados en el estudio de algún concepto. De manera que él pueda corregirlos correctamente con contra-ejemplos.

3. Esta propuesta sugiere que a partir de actividades concretas y conocimientos previos se demuestren las propiedades abstractas de la teoría de grupo, ayudando al alumno a lograr un aprendizaje más significativo.

4. En la propuesta didáctica no es indispensable el uso del triángulo equilátero, puede reemplazarse por otro polígono regular de n lados.

RECOMENDACIONES

1. Los pre-requisitos indispensables para poner en práctica la propuesta didáctica (que aquí presentamos), son los cursos de Teoría de Conjuntos, Trigonometría y Geometría Analítica, es decir que, los alumnos deben conocer los conceptos fundamentales de estas materias.

2. Si el docente que utiliza nuestra propuesta didáctica le parece que no avanza con la rapidez que él desea, no debe preocuparse; puesto que esta cimentando en el estudiante un aprendizaje significativo. Con lo cual el alumno comprenderá mejor el material siguiente.

3 En caso de que alguien desee utilizar otro polígono regular en vez del triángulo equilátero, le sugerimos utilizar el cuadrado, del cual se obtiene un grupo de ocho transformaciones Recomendamos el cuadrado porque entre más lados tenga el polígono el problema se hará más complejo, y viceversa, entre menos lados, menos dificultad

BIBLIOGRAFÍA

1. Bauslag, Benjamin and Chandler.: Bruce. Group Theory. McGraw Hill Book Company, N Y., 1968.

2. Birkoff, G. and Maclane, S.: A Survay of Modern Algebra. Macmillan, N.Y., 1977.

3. Gentile, Enzo.: Notas de Algebra. Ediciones Previas, Buenos Aires, 1976.

4. Herstein, I.N. · Topics in Álgebra, 2nd. de . Wiley, N.Y., N.Y., 1975.

5. Jacobson, Nathan.: Basic Álgebra I. W.H. Freeman and Company, N.Y., 1985.

6 Kurosh, A.G : Curso de Algebra Superior. Editorial Mir, Moscú, 1977.

7. Kurosh, A G.: Lectures on General Algebra. Chelsea, N Y., 1965

8. Lang, S. Algebra.: Addison-Wesley, Reading, Mass., 1967

9. Méndez, Zayra.: Aprendizaje y Cognición. Convenio BID - FOD - UNED, San José, 1993

10. Murnghan, Francis D.: The Theory of Group. Dover Publications, N.Y., 1963.

11. Orton, A.: Didáctica de las Matemáticas Editorial Morata, Madrid, 1990.

12. Piaget, Jean y otros.: La Enseñanza de las Matemáticas. Aguilar, Madrid, 1971

13. Pozo, J.A.: Teorías Cognitivas del Aprendizaje, 4ª de.. Editorial Morata, Madrid, 1996

14. Schenk-Danzinger, Lotte.: Psicología Pedagógica. Editorial Kapeluz, Buenos Aires, 1977

15. Silva Rehermann, César.: Matemática Básica Superior. Editorial Científico -Técnico, La Habana, 1985

16. Skemp, Richard R.: Psicología del Aprendizaje de las Matemáticas, 2ª de.. Editorial Morate, Madrid, 1993.

17. Torres C., Miriam N.: Constructivismo y Educación. University of New Mexico, U.S.A., 1992.