MTMD333/2025-B

ESTRUCTURAS Algebraicas

1º Bimestre: Deber (10 ejercicios, se entrega el día del examen)

2º Bimestre: Exposición (se puede escoger tema hasta la semana 9)
- Introducción, cuerpo, conclusión y bibliografía
- LaTeX

ESCUELA POLITECNICA NACIONAL
CONSEJO DE DOCENCIA

EPN-GD-MSP-03-03-PRD-05-FRM-02

SILABO

Versión 2

UNIDAD ACADÉMICA:	CIENCIAS			
CARRERA:	(RRA20) MATEMÁTICA			
PERIODO ACADÉMICO:	2025-B	SEPTIEMBRE 2025 - FEBRERO 2026	**TIPO:**	ORDINARIO

DETALLE DE ASIGNATURA:

NOMBRE:	ESTRUCTURAS ALGEBRAICAS	**PARALELO:**	A
CÓDIGO:	MTMD333	**PENSUM:**	MTM.20.30.01
CRÉDITOS:	3.00	**MODALIDAD**	PRESENCIAL
		(TIPO)	OBLIGATORIAS

COMPONENTES DE ORGANIZACIÓN DE LOS APRENDIZAJES	HORAS POR SEMANA	HORAS POR PERIODO ACADEMICO
Aprendizaje en Contacto con el Docente (AC)	4.00	64
Aprendizaje Práctico Experimental (AP)	2.00	32
Aprendizaje Autónomo (AA)	3.0	48
TOTAL	9.00	144

REQUISITOS DE LA ASIGNATURA

CO-REQUISITOS	
NOMBRE	**CÓDIGO**

PRE-REQUISITOS	
NOMBRE	**CÓDIGO**
ALGEBRA AFIN	MTMD212

HORARIO DE LA ASIGNATURA:

COMPONENTE DE APRENDIZAJES	HORARIO
AC	MTMD333 - ESTRUCTURAS ALGEBRAICAS - A - MiÃ©rcoles: 14-16 Jueves: 9-11 Viernes: 14-16

DESCRIPCIÓN DE LA ASIGNATURA:

EN ESTA ASIGNATURA, CONOCIDA TAMBIÉN COMO ÁLGEBRA ABSTRACTA, SE ESTUDIA LOS CONCEPTOS Y LAS PROPIEDADES ASOCIADAS A GRUPOS, ANILLOS Y CAMPOS.

INFORMACIÓN DE PROFESOR(ES) A CARGO:

NOMBRE	CORREO	FORMACIÓN ACADÉMICA	PARALELO	COMPONENTE DE APRENDIZAJE	DOCENTE PRINCIPAL
SERRANO DE LA TORRE SINTYA ESMERALDA	sintya.serrano@epn.edu.ec	Magister en Ciencias Matemática Aplicada	A	AC	X

OBJETIVOS DE CARRERA QUE APORTA LA ASIGNATURA: ESTRUCTURAS ALGEBRAICAS

CARRERA	OBJETIVO
(RRA20) MATEMÁTICA	NO APLICA

RESULTADOS DEL APRENDIZAJE DE LA ASIGNATURA:

TIPO DE RESULTADO	DESCRIPCIÓN DEL RESULTADO	FORMA DE EVIDENCIAR EL CUMPLIMIENTO**
Conocimientos	1.1 DESCRIBIR LAS ESTRUCTURAS DE GRUPO, ANILLO Y CAMPO. 1.2 DAR EJEMPLOS CONCRETOS DE GRUPOS, ANILLOS Y CAMPOS. 1.3 EXPLICAR EL CONCEPTO DE SUBGRUPO. 1.4 IDENTIFICAR CIERTAS ESTRUCTURAS ALGEBRAICAS CLÁSICAS COMO EL GRUPO DE KLEIN, EL GRUPO DE LOS CUATERNIONES, ANILLO DE LOS CUATERNIONES. 1.5 RELACIONAR LAS ESTRUCTURAS BÁSICAS CON CONCEPTOS PREVIAMENTE CONOCIDOS COMO SON LOS ENTEROS Y LOS POLINOMIOS. 1.6 EXPLICAR LA NOCIÓN DE HOMOMORFISMOS, ISOMORFISMOS Y AUTOMORFISMOS ENTRE ESTAS ESTRUCTURAS.	El estudiante debe resolver ejercicios prácticos, además debe conocer la teoría y demostraciones
Destrezas	2.1 DETERMINAR SI UNA ESTRUCTURA DADA ES UN GRUPO, ANILLO O CAMPO. 2.2 DEMOSTRAR PROPIEDADES INTERNAS ASOCIADAS A ESTAS ESTRUCTURAS. 2.3 DETERMINAR SI UNA ESTRUCTURA DADA ES UN SUBGRUPO O UN SUBANILLO. 2.4 DEMOSTRAR PROPIEDADES DE HOMOMORFISMOS E ISOMORFISMOS ASOCIADOS A ESTAS ESTRUCTURAS. 2.5 IDENTIFICAR ESTRUCTURAS ALGEBRAICAS ISOMORFAS ENTRE SÍ. 2.6 APLICAR LOS CONCEPTOS DEL ÁLGEBRA ABSTRACTA PARA DETERMINAR PROPIEDADES DE LOS POLINOMIOS. 2.7 IMPLEMENTAR CONCEPTOS ALGEBRAICOS EN COMPUTADORA.	El estudiante debe resolver ejercicios prácticos, además debe conocer la teoría y demostraciones
Valores y actitudes	3.1 DISCRIMINAR ENTRE PROCESOS MECÁNICOS PARA LA SOLUCIÓN DE CIERTOS PROBLEMAS Y PROCESOS SUSTENTADOS Y EXPLICADOS POR UNA TEORÍA. 3.2 ADOPTAR COMO UNA ÉTICA MATEMÁTICA: LA NO ACEPTACIÓN DE ASEVERACIONES SIN LA CORRESPONDIENTE DEMOSTRACIÓN, Y LA REFLEXIÓN SOBRE EL SIGNIFICADO DE LAS MENCIONADAS ASEVERACIONES. 3.3 DEMOSTRAR CAPACIDAD DE ESTUDIO Y TRABAJO EN EQUIPO. 3.4 DESARROLLAR EL SENTIDO DE RESPONSABILIDAD EN EL CUMPLIMIENTO DE LAS TAREAS, COMPROMISOS Y OBLIGACIONES. 3.5 DESARROLLAR LA CAPACIDAD DE AUTONOMÍA, EN PARTICULAR EN EL APRENDIZAJE, A FIN DE AMPLIAR Y PROFUNDIZAR LOS CONOCIMIENTOS MATEMÁTICOS.	Actividades en clase

** Descripciones específicas, medibles y demostrables de lo que el estudiante deberá hacer para el logro de los resultados del aprendizaje.

CONTENIDOS Y ACTIVIDADES DE APRENDIZAJE DE LA ASIGNATURA

DOCENTE: SERRANO DE LA TORRE SINTYA ESMERALDA, PARALELO: A, COMPONENTE : AC

N°	SEMANA	CONTENIDO	COMPONENTE DE APRENDIZAJE	HORAS	ACTIVIDADES DE APRENDIZAJE
1	SEMANA1	Repaso de conjuntos, funciones y operaciones binarias. Introducción a la teoría de números.	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de funciones, clases de equivalencia y conjuntos

			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
2	SEMANA2	Números enteros, algoritmo de la división, MCD, mcm e infinidad de números primos	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de números enteros
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
3	SEMANA3	Congruencias y aritmética modular. Prueba	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de aritmética modular
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
4	SEMANA4	Teorema de Fermat, teorema chino del resto, función Phi de Euler y solución de sistemas de congruencias.	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de teoremas de números enteros y sistemas de congruencias
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
5	SEMANA5	Teoría de grupos	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase. Evaluación
			AP	2.0	Ejercicios de grupos
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
6	SEMANA6	Subgrupos, Grupos cíclicos, subgrupos normales. Prueba	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de subgrupos normales y cíclicos.
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
7	SEMANA7	Grupos cocientes y Homomorfismo	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de grupos cocientes y homomorfismo
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
8	SEMANA8	Examen y Homomorfismos	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase. Evaluación
			AP	2.0	Ejercicios para el examen bimestral
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
9	SEMANA9	Teoremas de isomorfismos, automorfismos y monomorfismos	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de automorfismos
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
10	SEMANA10	Grupos de Klein, cuaterniones, grupos diédricos y producto de grupos	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de grupos de Klein, grupos diédricos y producto de grupos
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
11	SEMANA11	Grupos de permutaciones, teorema de Cayley. Prueba	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de permutaciones
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
12	SEMANA12	Grupos simples, ejemplos y aplicaciones	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de grupos simples

			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
13	SEMANA13	Teoremas de Sylow, Prueba	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios y aplicaciones de los grupos de Sylow
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
14	SEMANA14	Anillos, subanillos e ideales	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de anillos
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
15	SEMANA15	Anillo cociente, dominios, ideales y anillos de división	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios de dominio, cuerpos y anillos de división
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información
16	SEMANA16	Anillos de polinomios y examen	AC	4.0	Exposición oral (clase magistral), ejercicios dentro de clase, lecturas dentro de clase
			AP	2.0	Ejercicios para el examen
			AA	3.0	Ejercicios fuera de clase, lecturas fuera de clase, búsqueda de información

BIBLIOGRAFÍA BÁSICA OBLIGATORIA:

1.-Armstrong, M. , 1988. Groups and Symmetry. Lugar de publicación: . EditorialSpringer-Verlag
1.-Birkhoff, G., & Mac Lane, S. , 2010. A Survey of Modern Algebra. Lugar de publicación: . EditorialCRC Press
1.-Herstein, I. N. , 1964. Topics in algebra. Lugar de publicación: . EditorialBlaisdell
1.-Herstein, I. , 1996. Abstract Algebra. Lugar de publicación: USA. EditorialPrentice-Hall

BIBLIOGRAFÍA COMPLEMENTARIA ADICIONAL:

-Stephen Lovett , 2016. Abstract Algebra. Lugar de publicación: USA. EditorialCRC Press
-Ayres, F., Jaisingh, L. , 2004. Theory and Problems of Abstract Algebra. Lugar de publicación: USA. EditorialMcGraw-Hill
-Goodman, F. , 2006. Algebra. Abstract and Concrete. Lugar de publicación: -. EditorialSemisimple Press
-Rotman, J. , 2005. A first course in abstract algebra with applications. Lugar de publicación: USA. EditorialPrentice Hall
-GEORGE E. ANDREWS , 1994. Number theory . Lugar de publicación: New York . EditorialDOVER PUBLICATIONS, INC.
-Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery , 1991. An Introduction to the Theory of Numbers. Lugar de publicación: John Wiley & Sons, Inc.. EditorialUSA
-Fraleigh, John B., author. Katz, Victor J. , 2021. A First Course in Abstract Algebra. Lugar de publicación: New Jersey. EditorialPearson Education, Inc

METODOLOGÍA DE APRENDIZAJE DE LA ASIGNATURA

DOCENTE: SERRANO DE LA TORRE SINTYA ESMERALDA, PARALELO: A, COMPONENTE : AC

Método de aprendizaje	Recursos de aprendizaje	Escenarios de aprendizaje
Clase magistral	Exposiciones, lecturas, trabajos en grupo	Aula de clase

USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

a.- Ámbito de aplicación de la inteligencia artificial por parte del profesor

b.- Ámbito de aplicación de la inteligencia artificial por parte del estudiante

Apoyo al estudio y aprendizaje autónomo	Facilitar la comprensión de contenidos, resolver dudas, buscar información, elaborar esquemas y resúmenes, entre otros.

EVALUACIÓN

IMPORTANTE: De acuerdo al Art. 80 del RRA la contribución de cada componente de evaluación no podrá exceder el 35% de la calificación del aporte

ACTIVIDAD DE EVALUACIÓN	TIPO	APORTE 1 (%)		APORTE 2 (%)	
Examen	Sumativa	35.0	35.00	35.0	30.00
Prueba	Sumativa	30.0	25.00	25.0	30.00
Prueba	Sumativa	30.0	25.00	25.0	———
Taller/deber	Formativa	5.0	10.00	0.0	40.00
Exposición	Formativa	0.0	———	15.0	20.00 : 10.00 → Trabajo, 10.00 → Exposición
		100.0		100.0	

HORARIO Y MECANISMOS DE TUTORÍAS:

La exposición es puramente aplicada. En el trabajo si pueden ir demostraciones

mín. 4 pág. Trabajo Escrito → Introducción, Cuerpo, Conclusiones, Recomendaciones, Bibliografía

DOCENTE: SERRANO DE LA TORRE SINTYA ESMERALDA, PARALELO: A, COMPONENTE: AC

Horario (s) de tutorías	Ubicación / mecanismo / herramienta de contacto
Martes 11-12	Edificio 3, piso 5. Departamento de matemática

POLÍTICAS DE DESARROLLO DE LA ASIGNATURA

DOCENTE: SERRANO DE LA TORRE SINTYA ESMERALDA, PARALELO: A, COMPONENTE: AC

CÓDIGO DE ÉTICA EPN La tradición y el prestigio de la Politécnica exigen que el comportamiento de sus miembros se encuadre en el respeto mutuo, la honestidad, el apego a la verdad y el compromiso con la institución. Con tal antecedente, el presente Código de Ética define la norma de conducta de los miembros de la Escuela Politécnica Nacional:
RESPETO HACIA SÍ MISMO Y HACIA LOS DEMÁS Fomentar la solidaridad entre los miembros de la comunidad. Comportarse de manera recta, que afirme la autoestima y contribuya al prestigio institucional, que sea ejemplo y referente para los demás. Respetar a los demás y en particular la honra ajena y rechazar todo tipo de acusaciones o denuncias infundadas Respetar el pensamiento, visión y criterio ajenos. Excluir toda forma de violencia y actitudes discriminatorias. Apoyar un ambiente pluralista y respetuoso de las diferencias. Convertir la puntualidad en norma de conducta Evitar el consumo de bebidas alcohólicas, tabaco, substancias psicotrópicas o estupefacientes.
HONESTIDAD Hacer de la honestidad el principio básico de comportamiento en todos los actos. Actuar con justicia, probidad y diligencia. Actuar de acuerdo a la conciencia, sin que presiones o aspiraciones particulares vulneren los intereses institucionales. Velar por el cumplimiento de las garantías, derechos y deberes de los miembros de la Comunidad Politécnica Tomar oportunamente las medidas correctivas necesarias para superar las irregularidades que pudieren ocurrir.
VERDAD Hacer una mística de la prosecución de la verdad, tanto en la actividad académica como en lo cotidiano. Informar con transparencia y en forma completa. Emitir mensajes con autenticidad, que no distorsionen eventos ni realidades
COMPROMISO CON LA INSTITUCIÓN Hacer una mística de la prosecución de la verdad, tanto en la actividad académica como en lo cotidiano. Informar con transparencia y en forma completa. Emitir mensajes con autenticidad, que no distorsionen eventos ni realidades

ADAPTACIONES CURRICULARES PARA ATENDER A ESTUDIANTES CON NECESIDADES EDUCATIVAS ESPECIALES:

Metodologías de enseñanza-aprendizaje:
Ambientes de enseñanza-aprendizaje:

Métodos e instrumentos de evaluación:

UBICACIÓN:

Espacio:E39-PB/E019

02/10/2025

Teoría de Números

Los enteros salen de las clases de equivalencia entre naturales.

- $[(0,0)] = \{(0,0); (1,1); \ldots\}$
- $[(3,0)] =$
- $[(0,3)] =$

Principio del buen orden: Todo conjunto de enteros positivos tiene un elemento minimal.

Definición 1 (a divide b): Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, diremos que a divide b si existe $c \in \mathbb{Z}$ tal que

$$b = ac$$

Vamos a escribir $a \mid b$.
Si a no divide a b, se escribe $a \nmid b$

Sea $d \in \mathbb{Z}$, $d \neq 0$, a, b
$d \mid a$ y $d \mid b$
$\Rightarrow d \mid sa + tb$

Lema 1: Dados $a, b, c \in \mathbb{Z}$

1. $1 \mid a$
2. $b \mid b$ con $b \neq 0$
3. $c \mid 0$
4. Si $a \neq 0$, $a \mid b$ y $a \mid c$
5. Si $a \neq 0$ y $a \mid b$ y $a \mid c$, entonces $a \mid bc$
6. Si $a \neq 0$, $b \neq 0$ y $a \mid b$ y $b \mid a$, entonces $a = b$ ó $a = -b$
7. Sea $K \in \mathbb{Z}$, $K \neq 0$, $a \neq 0$. Si $a \mid b$, entonces $Ka \mid Kb$
8. Sean $a \neq 0$, $b \neq 0$. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$

Demostración:

1- Sabemos que

$$1 \cdot a = a$$

Por lo tanto,

$$1 \mid a,$$

2- Sabemos que

$$b = 1 \cdot b$$

Entonces,

$$b \mid b,$$

3- Sabemos que

$$0 = c \cdot 0$$

Entonces,

$$c \mid 0,$$

4.- Sean $k_1 \wedge k_2 \in \mathbb{Z}$, tales que

$$b = a \cdot k_1 \quad y \quad c = a \cdot k_2$$

Entonces,

$$b + c = a(k_1 + k_2)$$

Así,

$$a \mid b + c \quad //$$

5.- Sean $k_1 \wedge k_2 \in \mathbb{Z}$, tales que

$$b = a k_1 \quad y \quad c = a k_2$$

Entonces,

$$bc = a(k_1 k_2)$$

Así,

$$a \mid bc \quad //$$

6.- Tenemos que

$$a = k b \quad (1)$$
$$b = k_1 a \quad (2)$$

Reemplazando (1) en (2)

$$a = k k_1 a$$
$$k k_1 = 1$$

Entonces,

si $k = k_1 = 1$, $a = b$
si $k = k_1 = -1$, $a = -b$

7.- Sean $k, k_1 \in \mathbb{Z}$, tenemos que

$$b = a k_1$$
$$kb = k a k_1$$

Así,

$$ka \mid kb$$

8.- Sean $k_1, k_2 \in \mathbb{Z}$, tales que

$$b = a k_1 \quad (1)$$
$$c = b k_2 \quad (2)$$

Reemplazando (1) en (2)

$$c = a k_1 k_2$$

Así,

$$a \mid c$$

Proposición

↳ Algoritmo de Euclides: Sean $a, b \in \mathbb{Z}$ con $a \neq 0$, existen $q, r \in \mathbb{Z}$ tales que

$$b = aq + r \qquad 0 \leq r < |a|$$

donde q es el cociente y r el residuo.

Demostración:

Definamos el conjunto

$$S = \{b - ak \in \mathbb{N} : k \in \mathbb{Z}\}$$

Por el principio del buen orden, S posee un elemento minimal, que vamos a definir como

$$r = b - aq \quad \text{donde } q \in \mathbb{Z}$$

Ahara, supongamos que $r \geq a$

$$r - a \geq 0$$
$$b - aq - a \geq 0$$
$$b - a(q+1) \geq 0$$

Y sabemos que

$$b - a(q+1) \in S$$
$$\Rightarrow r - a < r$$

lo que contradice que r es el elemento minimal de S.

Por lo tanto, $r < a$

Definición 2

Máximo común divisor: Sean $a, b \in \mathbb{Z}^+$, $(a,b) \neq (0,0)$. El máximo común divisor de a y b es el entero d tal que

1.- $d \mid a$ y $d \mid b$ (común divisor)
2.- $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$

Se escribe $d = MCD(a,b)$

03/10/2025

Proposición

Aplicación!

Algoritmo de Euclides: Sean $a, b \in \mathbb{Z}$, $a \geq b$

$r_0 = a \qquad r_1 = b$

(1) $r_0 = q_1 r_1 + r_2$ para $0 \leq r_2 < r_1$

(2) $r_1 = q_2 r_2 + r_3$ para $0 \leq r_3 < r_2$

$\vdots$

(n-1) $r_{n-2} = q_{n-1} r_{n-1} + r_n$ para $0 \leq r_n < r_{n-1}$

(n) $r_{n-1} = q_n r_n + 0$

Ejemplos:

- $a = 234 \quad b = 84$

$234 = 2 \cdot 84 + 66$
$84 = 1 \cdot 66 + 18$
$66 = 3 \cdot 18 + 12$
$18 = 1 \cdot 12 + 6$
$12 = 2 \cdot 6 + 0$
$MCD(a,b) = 6$

- $a = 5241 \quad b = 872$

$5241 = 6 \cdot 872 + 9$
$872 = 96 \cdot 9 + 8$
$9 = 1 \cdot 8 + 1$
$8 = 8 \cdot 1 + 0$

Teorema 1.- Dado $MCD(a,b) = d$ y un K entero

a) $MCD(a, b+Ka) = MCD(a,b)$

b) $MCD(aK, bK) = |K| \, MCD(a,b)$ con $K \neq 0$

Demostración:

a) Definimos

$$s = MCD(a, b+Ka)$$

PD: $s = d$

Sabemos que:

(1) $s \mid a$ y $s \mid b+Ka$

(2) $d \mid a$ y $d \mid b$

Tenemos que

$s \mid Ka$, entonces

$s \mid (b+Ka) - Ka$

$s \mid b \quad (3)$

$s \mid d \quad (4)$

Por (2), $d \mid ka$ y

$$d \mid b + ka$$

$$d \mid s \quad (5)$$

Por (4) y (5),

$$d = s_{//}$$

b) Sea $n = MCD(ak, bk)$

P. D: $n = |k| d$

Sabemos que

(1) $d \mid a$ y $d \mid b$

(2) $kd \mid ak$ y $kd \mid bk$

Entonces,

$$kd \mid n \quad (3)$$

Así, sea $m \in \mathbb{Z}$,

$$n = kdm$$

Por lo tanto,

$$MCD(ak, bk) = kdm \quad (4)$$

- Asumiendo $k > 0$. P. D. $m = 1$

$$dkm \mid ak \text{ y } dkm \mid bk$$

$$dm \mid a \text{ y } dm \mid b$$

$$dm \mid d$$

Así, $m = 1$

- Asumiendo $k < 0$. P. D. $m = -1$

también se les conoce como coprimos

Definición 3 (Primo relativo): Se dice que a y b son primos relativos si y solo si $MCD(a,b)=1$.

Teorema 2.- Sean a,b enteros no ambos cero. Entonces K, ℓ enteros tale que

$$a = K\,MCD(a,b)$$
$$b = \ell\,MCD(a,b)$$

entonces, K y ℓ son primos relativos

Demostración: sea $n = MCD(K,\ell)$ P.D.: $n=1$

Sea $d = MCD(a,b)$, $q_1, q_2 \in \mathbb{Z}$ tales que

(1) $K = q_1 n$ y $\ell = q_2 n$

$$a = q_1 n\, MCD(a,b)$$
$$b = q_2 n\, MCD(a,b)$$

Así,

$$n\,MCD(a,b) \mid a \quad y \quad n\,MCD(a,b) \mid b$$

Entonces,

$$n\,MCD(a,b) \mid MCD(a,b)$$

Así, $c = 1$ //

Proposición

Caracterización de MCD: Dados $a,b \in \mathbb{Z}^*$, definimos un conjunto

$$S_{ab} = \{ sa + tb : s,t \in \mathbb{Z} \}$$

Proposición 3.- $S_{a,b}$ es el conjunto de los múltiplos de $MCD(a,b)$ y $MCD(a,b)$ es la más pequeña de las combinaciones positivas de a y b.

Demostración:

Sea M el conjunto de los múltiplos de $MCD(a,b)$

P.D: $S_{a,b} = M$

Llamaremos $MCD(a,b) = d$

- P.D: $S_{a,b} \subseteq M$

  Sea $x \in S_{a,b}$ P.D: $x = q\,MCD(a,b)$

  $x = sq + tb$ con $s,t \in \mathbb{Z}$

  Existen k y $l \in \mathbb{Z}$ tales que

  $a = kd$ y $b = ld$

  Así,

  $x = skd + tld$

  $x = (sk + tl)d$

  Por tanto, $x \in M$

- P.D: $M \subseteq S_{a,b}$

  Sea $x \in M$ P.D: existen $s,t \in \mathbb{Z}$ tq $x = as + bt$

  Podemos escribir

  $x = \alpha\, d$ (1) con $\alpha \in \mathbb{Z}$

  Por otro lado, sabemos que

08/10/2025

- $MCD(234, 84) = 6$ Encontrar s y t tales que $6 = s \cdot 234 + 84t$

(1) $234 = 2 \cdot 84 + 66$
(2) $84 = 1 \cdot 66 + 18$
(3) $66 = 3 \cdot 18 + 12$
(4) $18 = 1 \cdot 12 + 6$
(5) $12 = 2 \cdot 6 + 0$

$6 = 18 - 1 \cdot 12$
$= 18 - 1(66 - 3 \cdot 18)$
$= 18 + 3 \cdot 18 - 66$
$= 4 \cdot 18 - 66$
$= 4(84 - 66) - 66$
$= 4 \cdot 84 - 5 \cdot 66$
$= 4 \cdot 84 - 5(234 - 2 \cdot 84)$
$6 = 14 \cdot 84 - 5 \cdot 234$

→ Algoritmo de Euclides extendido

- $a = 1010101$ $b = 1221$

$1 = s\,1010101 + 1221t$
$1 = 11 - 2 \cdot 5$

$1010101 = 827 \cdot 1221 + 334$
$1221 = 3 \cdot 334 + 219$
$334 = 1 \cdot 219 + 115$
$219 = 1 \cdot 115 + 104$
$115 = 1 \cdot 104 + 11$
$104 = 9 \cdot 11 + 5$
$11 = 2 \cdot 5 + 1$
$5 = 5 \cdot 1 + 0$

$\Rightarrow MCD(a, b) = 1$

Definición 5 (Algoritmo de Euclides extendido): Dado $a, b \in \mathbb{Z}$, no ambos cero, el algoritmo de Euclides extendido encuentra enteros s, t tales que

$$MCD(a, b) = sa + tb$$

Teorema 4

- Dados a, b enteros distintos y primos relativos y c entero. Si $a \mid bc$, entonces $a \mid c$.

Demostración:

$bc = Ka$ (1) $\quad K \in \mathbb{Z}$
$MCD(a, b) = 1$

Sabemos que

$1 = sa + tb$ (2)

Si multiplicamos a (1) por t

$tbc = tKa$
$(1 - sa)c = tKa$ por (2)
$c = tKa + sac$

Entonces, $a \mid c$ //

Definición 6

mcm(a,b)

Mínimo común múltiplo: Sean a,b enteros, el mínimo común múltiplo de a y b es un entero m positivo tal que

1.- $a|m$ y $b|m$

2.- Si $a|m'$ y $b|m'$, entonces $m|m'$

♥ Dados a,b enteros positivos, probar que $ab = MCD(a,b)\,mcm(a,b)$ → Teorema 5

Llamaremos $MCD(a,b) = d$

Sabemos que para $l, k \in \mathbb{Z}$,

$$a = ld \quad y \quad b = kd$$

Igualmente, sabemos que l y k son primos relativos, por lo que

$$MCD(l,k) = 1$$

Entonces,

$$ab = (lkd)d$$

donde llamaremos $M = lkd$

$$\Rightarrow ab = Md$$

Así, $a|M$ y $b|M$

♥ Sea m' tal que $a|m'$ y $b|m'$

P.D: $m|m'$

Sean $q_1, q_2 \in \mathbb{Z}$, entonces

$$m' = aq_1 \quad y \quad m' = bq_2$$

Entonces,

$$aq_1 = bq_2 \quad (3)$$

$$ldq_1 = kdq_2$$

$$lq_1 = kq_2$$

$$k \mid q_1$$

Así, $q_1 = kc$ con $c \in \mathbb{Z}$

Entonces,

$$m' = akc$$
$$= (ld)c$$
$$m' = M\alpha$$

Por lo tanto, $M|m'$

Definición 7

Números primos: Un elemento $p \in \mathbb{Z}$ se dice primo si $p > 1$ y sus únicos divisores son 1 y el mismo p.

Definición (8): Si $n > 1$ y no es primo, n se dice compuesto.

Teorema 6 - Todo número entero positivo mayor que 1 es divisible por un primo.

Demostración:

- Si m es primo. Por definición de primo, el teorema se cumple

- Si m es compuesto.

  Sea S el conjunto de los compuestos que no son divisibles por un primo

  - Supongamos que $S \neq \phi$. Por el principio del buen orden, existe $m \in S$, elemento mínimal, que al ser compuesto, entonces

    $$m = a \cdot b \quad (1)$$

    Donde $a \neq 1$ y $b \neq 1$, por definición de S, a es compuesto,

    $$a = a_1 \cdot b_1 \quad (2)$$

    Entonces, $a \notin S$, pues

    $$a < m$$

  Sea p un primo tal que

  $$p \mid a \text{ y } a \mid m$$

  entonces,

  $$p \mid m$$

  Por lo tanto, $S = \phi$ //

Teorema 7

Teorema de Euclides para números primos (300 a.c.)

El conjunto de los números primos es infinito.

La idea de Euclides fue algo así:

Sea $N > 1$,

$$N! = 1 \cdot 2 \cdot 3 \ldots N$$

$$\Rightarrow N! + 1 \text{ es primo}$$

Si hay infinitos enteros, hay infinitos primos.

Demostración:

Supongamos que existen finitos primos, tal que

$$P = \{p_1, p_2, \ldots, p_n\}$$

Donde P es el conjunto de primos.

Sea Q un entero tal que

$$Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

Donde Q es un entero positivo mayor que 1

Diremos que Q es divisible por un primo p_j, es decir,

$$p_j \mid Q,$$

entonces $1 = Q - p_1 p_2 \ldots p_n$ por el algoritmo de Euclides extendido.

Así, $p_j \mid 1$, es decir,

$$p_j = 1 \text{ ó } p_j = -1$$

lo que contradice la definición de primo, pues 1 y -1 no son primos.

Así, el conjunto de los primos es infinito ■

Si n es compuesto, los divisores d de n están en $0 < d \leq \sqrt{n}$

↳ Lema 2

Proposición (Lema de Euclides): Si $p > 1$, entonces p es primo si para todo $a, b \in \mathbb{Z}$, $p \mid ab$ implica que $p \mid a$ ó $p \mid b$.

Demostración: Suponemos que $p \mid ab$

- Caso 1: $p \mid a$
- Caso 2: $p \nmid a$

  p y a son primos relativos, es decir, $MCD(p, a) = 1$.
  Así, por el teorema 3, $p \mid b$ ■

Teorema 8.- Si n es compuesto, los divisores de n: $0 < d \leq \sqrt{n}$.

Teorema de Euclides generalizado

Teorema 9.- Si p es primo y
$$p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_n$$
entonces, $p \mid a_i$ con $1 \leq i \leq n$

Teorema 10 (Teorema Fundamental de la Aritmética).- Si $n \in \mathbb{Z}$ y $n > 1$, entonces existe una factorización única en primos.
$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

15/10/2025

Definición (9): Función de orden primo
$$Ord_p: \mathbb{N}^* \longrightarrow \mathbb{N}$$
$$n \longmapsto K$$
$Ord_p(n) = K$ si y solo si $p^K \mid n$ y $p^{K+1} \nmid n$

Ejemplo: 1728
$1728 = 2 \cdot 864$
$= 2^2 \cdot 432$
$= 2^3 \cdot 216$
$= 2^4 \cdot 108$
$= 2^5 \cdot 54$
$= 2^6 \cdot 27$
$= 2^6 \cdot 3^3$

- $Ord_2(1728) = 6$
- $Ord_3(1728) = 3$
- $Ord_p(1728) = 0$ $\quad p \neq 3$ y $p \neq 2$

Definición 10
Función ϕ - Euler: Es la función $\phi: \mathbb{N}^* \longrightarrow \mathbb{N}$ el número de enteros positivos menores que n que son primos relativos de n.
$$\phi(n) = |\{a \in \mathbb{N}^* : MCD(n, a) = 1 \wedge 1 \leq a < n\}|$$

Ejemplos:
- $\phi(10) = 4$
- $\phi(20) = 8$
- $\phi(243) = \phi(3^5) = 162$
- $\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40$

Proposición: Si n entero positivo con descomposición
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$
$$\Rightarrow \phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n})$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \ldots \cdot (p_n^{\alpha_n} - p_n^{\alpha_n - 1})$$

Teorema 11.- Sea p un primo y a un entero positivo, entonces

$$\phi(p^a) = p^a - p^{a-1}$$

Si enumeramos todos los elementos menores a p^a, tenemos el listado $0, 1, 2, \ldots, p^a - 1$, que contiene p^a elementos. Los únicos no primos relativos de p^a son $0, p, 2p, \ldots$ Así,

$$\frac{p^a}{p} = p^{a-1}$$

son los múltiplos de p.
Por lo tanto, $\phi(p^a) = p^a - p^{a-1}$.

Teorema 12.- Sean n, m primos relativos y enteros positivos, entonces

$$\phi(n \cdot m) = \phi(n)\,\phi(m)$$

Demostración:

Sean $n = m = 1$ $\quad \phi(n \cdot m) = \phi(n)\,\phi(m)$

- Sea $1 < x < n \cdot m$ tal que

$$MCD(x, nm) = 1$$
$$MCD(x, n) = 1$$
$$MCD(x, m) = 1$$

$$x = q_1 m + r_1 \qquad 0 < r_1 < m$$
$$x = q_2 n + r_2 \qquad 0 < r_2 < n$$

$$MCD(m, r_1) = 1$$
$$MCD(n, r_2) = 1$$

$$\phi(mn) \leq \phi(m)\,\phi(n)$$

* Revisar la otra cota en el libro de Stark

Definición (11): Congruencia

Sean a, b enteros y n entero positivo si $n \mid a-b$ decimos que a y b son congruentes módulo n.

$$a \equiv b \mod n$$

Ejemplos:

- $23 \equiv 11 \mod 12$
- $1 \equiv -1 \mod 2$
- $-1 \equiv 1 \mod 2$
- $54 \equiv 36 \mod 3$
- $128 \equiv 11 \mod 13$
- $170 \equiv 10 \mod 4$
- $17 \equiv 1 \mod 4$
- $17 \not\equiv 10 \mod 4$

a) Todo entero a, b cumple
$$a \equiv b \mod 1.$$

b) Si $d \mid n$ y $a \equiv b \mod n$, entonces
$$a \equiv b \mod d.$$

c) Si $n \mid a$, entonces
$$a \equiv 0 \mod n$$

Teorema 13.- Sean a, b enteros, son congruentes módulo n si y solo si tienen el mismo residuo.

Demostración:

- Si $a \equiv b \mod n$

  Sabemos que para $k_1, k_2 \in \mathbb{Z}$

  (1) $a = k_1 n + r_1$ $\quad 0 \leq r_1 < n$

  (2) $b = k_2 n + r_2$ $\quad 0 \leq r_2 < n$

  Por hipótesis,
  $$n \mid a-b$$
  Entonces,

  (3) $a - b = kn$ con $k \in \mathbb{Z}$

  Reemplazando (2) en (3)
  $$a = (k + k_2) n + r_2$$
  Así, a y b tienen el mismo residuo.

- Si a y b tienen el mismo residuo,
  $$a = k_1 n + r \quad 0 \leq r < n$$
  $$b = k_2 n + r$$
  Así,
  $$a - b = (k_1 - k_2) n$$
  y por tanto,
  $$n \mid a-b$$
  $$a \equiv b \mod n \quad \blacksquare$$

La congruencia módulo n, es una relación de equivalencia en $\mathbb{Z}$.

Teorema 14.- Si $a \equiv b \mod n$ y $c \equiv d \mod n$, entonces:
Para todo par de enteros r, s

1.- $ar + cs \equiv br + ds \mod n$
2.- $a + c \equiv b + d \mod n$
3.- $a - c \equiv b - d \mod n$
4.- $ac \equiv bd \mod n$
5.- Para todo k entero, $a + k \equiv b + k \mod n$
6.- Para todo s entero positivo, $a^s \equiv b^s \mod n$

Demostración:

1.- Sabemos que

$$n \mid a - b \quad y \quad n \mid c - d$$

Por lo tanto,

$$n \mid r(a-b) \quad y \quad n \mid s(c-d)$$

Entonces,

$$n \mid r(a-b) + s(c-d)$$
$$n \mid ra + sc - (rb + sd)$$

Así,

$$ra + sc \equiv rb + sd \mod n.$$

2.- Por 1, si $r = s = 1$, se cumple.

3.- Por 1, si $r = 1$ y $s = -1$, se cumple.

4.- Tenemos que

$$ac - bd = c(a-b) + b(c-d)$$

Y por hipótesis,

$$n \mid a - b \quad y \quad n \mid c - d$$

Por lo tanto,

$$n \mid c(a-b) + b(c-d)$$
$$n \mid ac - bd$$

Así,

$$ac \equiv bd \mod n$$

5.- Tenemos que

$$n \mid a - b$$
$$n \mid a - b + k - k$$
$$n \mid a + k - (b + k)$$

Así,

$$a + k \equiv b + k \mod n$$

6.- Base de inducción: $n=1$

(1) $a \equiv b \mod n$

Hipótesis de inducción:

(2) $a^n \equiv b^n \mod n$

P.D: $a^{k+1} \equiv b^{k+1} \mod n$

(Polinomios)

Corolario 1.- Si $a \equiv b \mod n$, $P(x)$ polinomio entero (coeficiente entero), entonces

$$P(a) \equiv P(b) \mod n$$

16/10/2025

Ejercicios:

♥ Hallar el residuo de dividir 7^{135} entre 8.

$$7^{135} \equiv a \mod 8$$

$7 \equiv 7 \mod 8$

$7^2 \equiv 49 \mod 8$

$7^2 \equiv 1 \mod 8$

$7^{135} \equiv 7^{134} \cdot 7 \mod 8$

$7^{134} \cdot 7 \equiv (7^2)^{67} \cdot 7 \mod 8$

$7^{135} \equiv (1)^{67} \cdot 7 \mod 8$

$7^{135} \equiv 7 \mod 8$ residuo: 7

Ejercicio: Sean a, b enteros y p primo

P.D:

$$(a+b)^p = a^p + b^p \mod p$$

El binomio de Newton se define como

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

Donde

$$\binom{p}{k} = \frac{p(p-1)\cdots 1}{1 \cdot 2 \cdots (p-k)} = \frac{p!}{k!(p-k)!} = tp \quad \text{con } t \in \mathbb{Z} \text{ y } k \neq 0$$

Teorema 15.- Sea p primo. Para cualesquiera a, b enteros se tiene que

$$(a+b)^p \equiv a^p + b^p \mod p$$

Además:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

- Si $ac \equiv bc \mod n$, entonces $a \equiv b \mod n$

Contraejemplo:

$24 \equiv 12 \mod 6$

$4 \cdot 6 \equiv 3 \cdot 6 \mod 6$

$3 \equiv 4 \mod 6$ ↘↙

Teorema 16 - Si $ac \equiv bc \mod n$ y $d = MCD(c, n)$, entonces $a \equiv b \mod n/d$

Demostración:

Por hipótesis,

$$n \mid ac - bc$$

y tenemos que

$$d = MCD(c, n)$$

Así,

$c = dc_1$ (1) y $n = dn_1$ (2)

por lo tanto,

$$MCD(c_1, n_1) = 1 \quad (3)$$

Ahora,

$$kn = (ac - bc)$$

Por (1) y (2)

$$kdn_1 = c(a-b)$$
$$kdn_1 = dc_1(a-b)$$

Entonces,

$$kn_1 = c_1(a-b)$$

y tenemos que

$$n_1 \mid c_1(a-b)$$

Por (3),

$$n_1 \mid a-b$$

Así,

$$n/d \mid a-b$$

$$a \equiv b \mod n/d$$ ▨

- Un número escrito en forma decimal es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.

$$n = a_n a_{n-1} \dots a_0 \qquad (\dot{1}\dot{2}\dot{3}\dot{4}\dot{5})$$

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n$$

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

$$10 \equiv 1 \mod 3$$

Por el corolario 1:

$$P(10) \equiv P(1) \mod 3$$

Así,

$$n \equiv a_0 + a_1 + \dots + a_n \mod 3$$ ■

- Un número entero escrito de forma decimal es divisible por 4 si y solo si el número formado por sus dos últimas cifras es divisible por 4.

Definición (13): Aritmética módulo n

Para cada entero a y n entero positivo, definimos la clase de equivalencia

$$\bar{a} = \{x \in \mathbb{Z} : x \equiv a \mod n\}$$
$$= \{x \in \mathbb{Z} : x, a \text{ tienen el mismo residuo}\}$$

Estas clases de equivalencias se dicen clases residuales y son particiones de $\mathbb{Z}$.

Definición (14): El conjunto $\mathbb{Z}_n$ se define como:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$$

y contiene todas las clases de equivalencia módulo n.

Definición (15): Suma y producto $\mathbb{Z}_n$

Sean $\bar{a}$ y $\bar{b} \in \mathbb{Z}_n$, ♥ $\bar{a} + \bar{b} = \overline{a+b}$ ♥ $\bar{a} \cdot \bar{b} = \overline{ab}$

17/10/2025

Teorema 17. Para $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, se cumplen las siguientes propiedades:

Propiedades de la suma:

1. **Conmutativa:** $\bar{a} + \bar{b} = \bar{b} + \bar{a}$
2. **Asociativa:** $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$
3. **Elemento neutro:** $\bar{a} + \bar{0} = \bar{a}$
4. **Inverso aditivo:** Para todo $\bar{a}$ existe $\overline{-a}$ tal que $\bar{a} + \overline{-a} = \bar{0}$
5. **Resta:**
$$\bar{a} + \overline{-b} = \bar{a} - \bar{b}$$

Propiedades del producto:

1. **Conmutativa:** $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$
2. **Asociativa:** $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$
3. **Elemento neutro:** $\bar{a} \cdot \bar{1} = \bar{a}$
4. **Elemento nulo:** $\bar{a} \cdot \bar{0} = \bar{0}$
5. **Propiedad distributiva:** $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$
6. Si $MCD(a, n) = 1$, entonces existe $\bar{a}^{-1}$ tal que $\bar{a} \cdot \bar{a}^{-1} = \bar{1}$

Definición 16 (Unidad). Un elemento $\bar{a} \in \mathbb{Z}_n$ se dice **unidad** si existe $\bar{b} \in \mathbb{Z}_n$ tal que:

$$\bar{a} \cdot \bar{b} = \bar{1}$$

Es decir, si $\bar{a}$ tiene inverso multiplicativo en $\mathbb{Z}_n$.

Definición 17. El conjunto de todas las **unidades** de $\mathbb{Z}_n$ se denota por:

$$U(n) = \{\bar{a} \in \mathbb{Z}_n \mid \exists \bar{b} \in \mathbb{Z}_n \wedge \bar{a} \cdot \bar{b} = \bar{1}\}$$

Ejercicio: Hallar el inverso de $\bar{73}$ en $\mathbb{Z}_{23}$

$$123 = 1 \cdot 73 + 50$$
$$73 = 1 \cdot 50 + 23$$
$$50 = 2 \cdot 23 + 4$$
$$23 = 5 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$

$$1 = 4 - 1 \cdot 3$$
$$= 4 - (23 - 5 \cdot 4)$$
$$= 6 \cdot 4 - 1 \cdot 23$$
$$= 6(50 - 2 \cdot 23) - 1 \cdot 23$$
$$= 6 \cdot 50 - 12 \cdot 23 - 1 \cdot 23$$
$$= 6 \cdot 50 - 13 \cdot 23$$
$$= 6 \cdot 50 - 13(73 - 1 \cdot 50)$$
$$= 6 \cdot 50 - 13 \cdot 73 + 13 \cdot 50$$
$$= 19 \cdot 50 - 13 \cdot 73$$
$$= 19(123 - 1 \cdot 73) - 13 \cdot 73$$
$$= 19 \cdot 123 - 19 \cdot 73 - 13 \cdot 73$$
$$1 = 19 \cdot 123 - 32 \cdot 73$$

Así, $-\overline{32} = \overline{73^{-1}}$

$\Rightarrow \overline{73^{-1}} = \overline{91}$

Ejercicio: Calcular $\overline{3^{-1}}\,(\bar{6}-\overline{11})$ en $\mathbb{Z}_{13}$

- $13 = 4\cdot 3 + 1$
  $3 = 3\cdot 1 + 0$

- $1 = 13 - 4\cdot 3$
  $\Rightarrow \overline{3^{-1}} = \overline{-4}$
  $\overline{3^{-1}} = \bar{9}$

$\Rightarrow \bar{9}\,(\bar{6}-\overline{11}) = \bar{9}\,(-\bar{5})$
$= \bar{9}(\bar{8})$
$= \bar{7}$

→ Solución de una ecuación

Teorema 18.- Dada

$$ax \equiv b \mod n$$

tiene solución si y solo si

$$MCD(a,n) \mid b$$

Demostración:

⇒) Sea x_0 solución de
$ax \equiv b \mod n$
P.D: $d = MCD(a,n) \mid b$
Tenemos que
$ax_0 = b + nK$ con $K \in \mathbb{Z}$
$ax_0 - nK = b$
Sabemos que
$d \mid a$ y $d \mid n$
Así,
$d \mid b$

⇐) Si $d = MCD(a,b) \mid b$
P.D: $ax \equiv b \mod n$ tiene solución
Tenemos que
$b = Kd$ con $K \in \mathbb{Z}$
Existen s,t tales que
$d = sa + tn$
$Kd = K(sa + tn)$
$b = Ksa + tnK$
$-Ksa + b = tnK$
Entonces,
$Ksa \equiv b \mod n$
Así,
$x_0 = Ks$ ■

Stark: Pág 66-67 hasta el fin de la demostración

Ejercicio: $5x \equiv 52 \mod 3$

$2x \equiv 1 \mod 3$

$x \equiv 2 \mod 3$

Ejercicio: $14x \equiv 13 \mod 21$ Por el teorema 11, no tiene solución

Ejercicio: $3x \equiv 5 \mod 7$

23/10/2025

Definición (18): Sistema reducido de residuos módulo n.
Un subconjunto R de enteros se dice sistema reducido de residuos módulo n si cumple que

1.- R tiene $\phi(n)$ elementos.
2.- Para $r \in R$ se tiene $MCD(r,n) = 1$
3.- Los elementos $r \in R$ son incongruentes dos a dos.

Si $n = 8$

Si p es primo

Teorema 19.- Si $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ un sistema reducido de residuos módulo n y $MCD(K,n) = 1$, entonces
$\{Kr_1, Kr_2, \ldots, Kr_{\phi(n)}\}$
es un sistema reducido de residuos módulo n.

Demostración:

1.- Tiene $\phi(n)$ elementos

2.- $MCD(r_i, n) = 1$
$MCD(K,n) = 1$
$MCD(Kr_i; n) = 1$ (*)

3.-

Teorema 20 (Teorema de Euler).- Si $MCD(a,n)=1$, entonces

$$a^{\phi(n)} \equiv 1 \mod n$$

Demostración:

Sea $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ un sistema reducido de residuos, por el teorema anterior,

$$\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$$

es un sistema reducido de residuos.

Entonces,

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(n)} \mod n.$$

Dado que

$$MCD(r_i, n) = 1$$

Entonces,

$$1 \equiv a^{\phi(n)} \mod n \quad \blacksquare$$

Corolario 2 (Pequeño Teorema de Fermat).- Si p es primo, $MCD(a,p)=1$, entonces

$$a^{p-1} \equiv 1 \mod p$$

Teorema 21.- Si p es primo,

$$a^p \equiv a \mod p \quad \text{para } a \in \mathbb{Z}$$

Demostración:

- Caso 1: $p \nmid a$, $MCD(p,a)=1$

$$a^{p-1} \equiv 1 \mod p$$

Así,

$$a^p \equiv a \mod p$$

- Caso 2: $p \mid a$

$$a \equiv 0 \mod p$$
$$a^p \equiv a \mod p \quad \blacksquare$$

Teorema 22.- Dada (1) $ax \equiv b \mod n$.
Si $MCD(a,n)=1$, entonces la solución de (1) es

$$x \equiv a^{\phi(n)-1} b$$

Ejercicio: Hallar las dos últimas cifras de 27^{123}

$$\phi(100) = \phi(2^2 \cdot 5^2)$$
$$= (2^2 - 2)(5^2 - 5)$$
$$= 40 \qquad (123 = 3 \cdot 40 + 3)$$

$$27^{123} \equiv (27^{40})^3 \cdot 27^3 \mod 100$$

$$27^{40} \equiv 1 \mod 100$$

$$(27^{40})^3 \cdot 27^3 \equiv 27^3 \mod 100$$
$$\equiv 83 \mod 100$$

Ejercicio: Sean p y q primos. Probar que

$$p^{q-1} + q^{p-1} \equiv 1 \mod pq$$

Por el pequeño teorema de Fermat,

$$p^{q-1} \equiv 1 \mod q \quad \text{y} \quad q^{p-1} \equiv 1 \mod p$$

Igualmente,

$$q^{p-1} \equiv 0 \mod q \quad \text{y} \quad p^{q-1} \equiv 0 \mod p$$

Así,

(1) $p^{q-1} + q^{p-1} \equiv 1 \mod q$ y (2) $p^{q-1} + q^{p-1} \equiv 1 \mod p$

Dado que (1) y (2) son divisibles tanto para p como para q, entonces

$$p^{q-1} + q^{p+1} \equiv \mod pq \blacksquare$$

Ejercicio: Un comerciante compra lápices y borradores. Cada lápiz cuesta 53 centavos y cada borrador cuesta 26 centavos. El comerciante tiene 149 dólares, ¿cuál es la cantidad de lápices y borradores puede comprar?

$$53\ell + 26b = 14900 \qquad MCD(53,26) = 1$$

$$\ell = 2 + 26K > 0 \; ; \; b = 569 - 53K > 0$$

$$K > -\frac{1}{13} \qquad K < \frac{569}{53}$$

24/10/2025

Teorema 23.- $p^{q-1} + q^{p-1} \equiv 1 \mod pq$

Definición (19): Ecuaciones diofánticas lineales.

Una ecuación de la forma

$$ax + by \equiv c$$

se dice ecuación diofántica lineal, con $a, b, c \in \mathbb{Z}$.

Definición (20): Un sistema lineal de congruencias en dos incógnitas es un sistema de la forma:

$$\begin{cases} ax + by \equiv e \mod m \\ cx + dy \equiv f \mod m \end{cases}$$

con $a, b, c, d, e, f, m \in \mathbb{Z}$. Sea $D \in \mathbb{Z}$ tal que

$$D = ae - bd$$

El sistema tiene solución única en módulo m si $MCD(D, m) = 1$. Si esto se cumple, entonces la solución se expresa como:

$$\begin{cases} x \equiv (de - bf)D^{-1} \mod m \\ y \equiv (af - ce)D^{-1} \mod m \end{cases}$$

Definición (21): Teorema Chino del Resto

Sean $m_1, m_2, \ldots, m_r$ enteros positivos que son primos relativos dos a dos y $a_1, a_2, \ldots, a_r$ enteros arbitrarios, el sistema de congruencias

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_3 \mod m_r \end{cases}$$

tiene una única solución módulo $M = m_1 m_2 \cdots m_r$.

Para su solución, definimos

$$M_i = \frac{M}{m_i} \quad \text{con } i = 1, 2, \ldots, r$$

y sea y_i el inverso de M_i módulo m_i, es decir,

$$M_i y_i \equiv 1 \mod m_i$$

Entonces, la solución se puede escribir como

$$x_0 \equiv \sum_{i \le r} a_i M_i y_i \mod M$$

Teoría de Grupos

31/10/2025

Definición (22): Un grupo $(G, *)$ donde G es un conjunto no vacío y $*$ es una operación binaria de G, que satisface:

1.- Clausura bajo $*$: Si $a, b \in G$,
$$a * b \in G$$

2.- Asociativa: Dados $a, b, c \in G$
$$(a * b) * c = a * (b * c)$$

3.- Identidad: Existe $e \in G$ tal que para todo $x \in G$
$$x * e = x$$
$$e * x = x$$

4.- Inverso: Para todo $a \in G$, existe $b \in G$ tal que
$$b * a = a * b = e$$

Proposición.- Sea $(G, *)$ un grupo y $a \in G$, existe un único inverso de a.

Demostración:

Suponemos que existen $b_1, b_2 \in G$ inversos de a

P.D: $b_1 = b_2$

$$b_1 = b_1 * e$$
$$b_1 * e = b_1 * (a * b_2)$$
$$b_1 * (a * b_2) = (b_1 * a) * b_2$$
$$(b_1 * a) * b_2 = e * b_2$$
$$e * b_2 = b_2$$
$$b_1 = b_2 \blacksquare$$

El símbolo para el inverso de a, a^{-1}

Ejemplos de grupos:

1.- $(\mathbb{Z}, +)$
2.- $(\mathbb{Q}, +)$
3.- $(\mathbb{R}^{n \times n}, +)$
4.- $(\mathbb{R}, +)$
5.- $(\mathbb{C}, +)$
6.- $(\mathbb{Q}^*, \times)$
7.- $(\mathbb{R}^+, \times)$
8.- $(\mathbb{Z}_n, +)$
9.- $(U_n, \times)$
10.- $E_n = \{\theta_n^i : \theta_n^i$ complejo$\}$ raíces de la unidad

$\theta_n = \cos(2\pi/n) + i \operatorname{sen}(2\pi/n)$

$\theta_n^i * \theta_n^k = \theta_n^{i+k}$

$\theta_n^n = 1$

Definición (23): Grupo finito

Un grupo de G se dice finito si tiene finitos elementos
El número de elementos de G, se dice de orden G, $|G|$.

Ejemplo: $|E_n| = n$

Definición (24): Grupo Abeliano

Un grupo G se dice abeliano si y solo si para todo $a, b \in G$

$$a * b = b * a$$

Sea G un conjunto de funciones definidas como

$$T_{ab}: \mathbb{R} \to \mathbb{R}$$
$$r \mapsto ar + b \quad \text{con } a \neq 0,\ b \in \mathbb{R}$$

Sea $S = \{(x, y) : x, y \in \mathbb{R}\} \to$ plano $\mathbb{R}^2$

- Consideramos f, g funciones de S

$$f: S \to S \qquad g: S \to S$$
$$(x, y) \mapsto (-x, y) \qquad (x, y) \mapsto (-y, x)$$

- f: reflexión
- g: rotación $\frac{\pi}{2}$ contra las manecillas del reloj

$G = \{f^i g^j : i, j = 0, 1, 2, 3\}$ con composición de funciones

Este grupo no es abeliano.
Es un grupo diedral orden 8 $\to$ # elementos

- **Notación:**
  - S: G grupo
  - $a^0 = e$
  - $a^k = \underbrace{a * a * a * \dots * a}_{\hookrightarrow k \text{ veces}} \quad k \in \mathbb{Z}^+$
  - $a^{-k} = (a^{-1})^k$
  - Dado G grupo:
    - $x^n * x^m = x^{n+m}$
    - $(x^n)^m = x^{nm}$

↳ Definición 25

Ejercicio: Pruebe que si G es abeliano y $a, b \in G$, entonces
$(a * b)^n = a^n * b^n$ para todo $n \in \mathbb{Z}$

* Para n positivo:

Proposición: Dado G un grupo y $x \in G$. Para todo $n, m \in \mathbb{Z}$ se cumple que:

- $x^m \cdot x^n = x^{m+n}$
- $(x^m)^n = x^{mn}$

Lema 3.- Si G es un grupo, entonces:

1. La identidad es única
2. Todo $a \in G$, tiene un único inverso $a^{-1} \in G$
3. Si $a \in G$, se cumple que $(a^{-1})^{-1} = a$
4. Para $a, b \in G$, se cumple $(ab)^{-1} = b^{-1}a^{-1}$

Demostración:

① Sean $e_1, e_2 \in G$ tales que e_1 y e_2 son identidad en G

P.D: $e_1 = e_2$

Sea a^{-1} inverso de a,

$$e_1 = a * b$$

Por hipótesis,

$$e_1 = (e_2 * a) * a^{-1}$$
$$e_1 = e_2 * (a * a^{-1}) \quad \text{(prop. asociativa)}$$
$$e_1 = e_2 * e_1$$

Y dado que e_1 es identidad

$$e_1 = e_2$$

Así, la identidad es única ■

② P.D: $(a^{-1})^{-1} = a$

Sabemos que

Lema 4.- Si G es un grupo
a) Si $a*b = a*c$, entonces $b = c$
b) Si $b*a = c*a$, entonces $b = c$

Ejercicio: Si G es un grupo finito con orden par, pruebe que al menos existe un elemento $a \neq 0$ tal que $a = a^{-1}$.

Tenemos que $|G| = 2n$

P.D. $\exists a \in G$ tq $a = a^{-1}$

Sea X un conjunto no vacío. 05/11/2025

$$S(X) = \{ f : f: X \to X,\ 1\text{-}1 \text{ y sobreyectivas} \}$$

- $(S(X), \circ)$ es un grupo?
  - Si X es finito de orden n
    $S(X) = S_n$
    * Tomando $n=3$:
      $X = \{x_1, x_2, x_3\}$
      - $i: X \to X$, $x \mapsto x$
      - $h: X \to X$, $x_1 \mapsto x_2$, $x_2 \mapsto x_3$, $x_3 \mapsto x_1$

$$i = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix} \qquad h = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$$

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$j = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad k = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$l = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad m = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Grupos generales lineales de orden n

- $GL_n(\mathbb{R})$ ($\mathbb{C}$, $\mathbb{Z}_p$): matrices $n \times n$ con coeficientes reales invertibles.

Definición (26): Subgrupo
Sea $H \subseteq G$ no vacío, se dice subgrupo de G si H es un grupo.

Teorema 24 (Teorema de caracterización de subgrupos).-
Sea $H \subseteq G$, H no vacío y G grupo. H se dice subgrupo ssi:

(SG1) Sean $x, y \in H$, entonces $x * y \in H$.
(SG2) Si $x \in H$, entonces $x^{-1} \in H$

Para las demostraciones se puede usar el teorema o el corolario, no ambos.

Corolario 3:- Si G es un grupo, $H \subseteq G$ no vacío, H es subgrupo de G si y solo si
(SG3) Si $x, y \in H$, entonces $x * y^{-1} \in H$

- $GL_2(\mathbb{R})$

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - cb = 1 \right\}$$

$H \subseteq GL_2(\mathbb{R})$
H subgrupo de $GL_2(\mathbb{R})$ → En algunos libros se denota como: $H \leq GL_2(\mathbb{R})$

(SG1) Sean A, B en H.
P.D: $AB \in H$
$|AB| = |A||B| = 1$ Así, $AB \in H$

(SG2) Si $A \in H$,
P.D: $A^{-1} \in H$
$|A^{-1}| = \frac{1}{|A|} = 1$ Así, $A^{-1} \in H$

Corolario 4:- Dado G un grupo y H subgrupo de G. $K \subseteq H$ es subgrupo de G si y solo si K es subgrupo de H.

- $GL_2(\mathbb{Z}_2)$: $|GL_2(\mathbb{Z}_2)| = 6$
- $GL_2(\mathbb{Z}_5)$: $|GL_2(\mathbb{Z}_5)| = 480$

★ Sea G un grupo, $a \in G$,

$$C(a) = \{ g \in G : ga = ag \} \mapsto C(a): \text{centralizado de } a \text{ en } G$$

$C(a)$ es subgrupo de G → demostración en el cuaderno.
Demostrar si es o no abeliano

★ Sea G grupo (↑ Mostrar que es subgrupo)

$$Z(G) = \{ z \in G : xz = zx \ \forall x \in G \} \mapsto Z(G): \text{centro de } G$$

★ Sea G grupo y $a \in G$, H subgrupo de G.

$$aHa^{-1} = \{ aha^{-1} : h \in H \}$$

Definición (27): Subgrupo cíclico
Sea G un grupo y $a \in G$, generado por a.
$\langle a \rangle = \{ a^j : j \in \mathbb{Z} \}$ es un subgrupo cíclico

Demostración:
SG3: Sean $b_1, b_2 \in \langle a \rangle$, $b_2 = a^{s_2}$

$b_1 * b^{-1} \in \langle a \rangle$
$a^{s_1} * (a^{s_2})^{-1} = a^{s_1} * a^{-s_2} = a^{s_1 - s_2}$ $s_1 - s_2 \in \mathbb{Z}$

Definición (28): Grupo cíclico

Un grupo G se dice cíclico si existe $a \in G$ tal que

$$G = \langle a \rangle$$

a se dice generador de G.

Ejemplos de grupos cíclicos:

- $\mathbb{Z}_n = \langle 1 \rangle$
- $E_n \rightarrow$ raíces de la unidad

06/11/2025

☆ Sea G grupo, $a \in G$,

$$\langle a \rangle = \{a^s : s \in \mathbb{Z}\}$$

i) Si $a^n \neq a^m$ para todo $n \neq m$, el orden $\langle a \rangle$ es infinito.

ii) Si existen m, n distintos, con $n > m$ tales que $a^n = a^m$, entonces

$$a^n = a^m$$
$$a^n a^{-m} = e$$
$$a^{n-m} = e$$

Si definimos el conjunto no vacío

$$S = \{k \in \mathbb{N} : a^k = e\}$$

S tiene un elemento minimal t tal que

$$a^t = e$$

Para cualquier entero n,

$$n = qt + r \qquad 0 \leq r < t$$

Así,

$$a^n = a^{qt+r} \qquad 0 \leq r < t$$
$$= (a^t)^q \cdot a^r \qquad 0 \leq r < t$$
$$a^n = a^r \qquad 0 \leq r < t$$

Por tanto,

$$a^0 = e, a^1, a^2, \ldots, a^{t-1} \text{ son diferentes}$$

$$\langle a \rangle = \{a^s : 0 \leq s < t\}$$

Definición (29): Orden de un elemento

Dado G un grupo y $x \in G$, el orden de un elemento x es el menor de los positivos t (si existe), tal que $x^t = e$. En este caso, se dice que x tiene orden finito t. Si no existe t para x, se dice que x tiene orden infinito. El orden de x se denota $|x|$.

Proposición: Dado G grupo y H subgrupo de G. Si $x \in H$, entonces $\langle x \rangle \subseteq H$.

Teorema 25.- Si G es grupo cíclico, $G = \langle g \rangle$. Si H es subgrupo de G, entonces H es cíclico.

- Todo grupo cíclico es abeliano. → demostraciones en el cuaderno

Definición (30): Clase lateral

Sea G grupo, H subgrupo de G, $a \in G$

- $aH = \{ah : h \in H\}$ se llama clase lateral izquierda de H en G
- $Ha = \{ha : h \in H\}$ se llama clase lateral derecha de H en G

Proposición: Sea G grupo, $H \subseteq G$ subgrupo, $a \in G$. Si $b \in aH$, entonces $aH = bH$

Demostración:

Tenemos que $b \in aH$, entonces $b = ah_1$

P.D: $aH = bH$

- P.D: $bH \subseteq aH$

  Sea $c \in bH$ P.D: $c \in aH$

  $c = bh_2$

  $c = ah_1h_2$

  Tomamos $h_1h_2 = h$, entonces

  $c = ah \in aH$

- P.D: $aH \subseteq bH$

  Sea $d \in aH$ P.D: $d \in bH$

  $d = ah_3$

  $d = bh_1h_i^{-1}h_3$

  $d \in bH$

  $a = ae = ah_1h_i^{-1}$

  $= bh_1^{-1}$

Teorema 26 (Teorema de Lagrange).- Si G es un grupo finito y H subgrupo de G, entonces el orden de H divide al orden de G.

Demostración:

Dados $a, b \in G$, $a \sim b$ si y solo si $ab^{-1} \in H$ (1)

$ab^{-1} = h$

$a = hb$

Así mismo, $a \sim b$ si y solo si $a \in Hb$

$[b] = Hb$

Dado K el número de clases laterales distintas.

$$Ha_1, Ha_2, \ldots, Ha_K$$

$$G = \bigcup_{1 \le i \le K} Ha_i$$

$$Ha_i \cap Ha_k = \emptyset \quad o \quad Ha_i = Ha_k$$

Sea la función f_i definida como:

$$f_i : H \to Ha_i$$
$$h \mapsto ha_i$$

Donde f_i es una función 1-1 y sobre Ha_i.

Sea $|H|$ orden de H

$$|G| = |\bigcup_{1 \le i \le K} Ha_i| = K|H|$$ ∎

Definición (31): Índice de un subgrupo finito

El número de clases laterales (izquierdas o derechas) de G. (grupo finito)

$$i(H) = |G|/|H| = K$$

Teorema 27.- Si G es de orden primo, entonces G es cíclico. → Hacer demostración

Teorema 28.- Si G es grupo, $a \in G$, entonces (→ finito) orden de a $o(a) \mid |G|$

Demostración:

$o(a) = |\langle a \rangle|$ por teorema de Lagrange

$\Rightarrow |\langle a \rangle| \mid |G|$

Cuando un grupo es de orden primo, solo pueden haber 2 subgrupos cíclicos generados:
$H = \langle e \rangle$
$H = G$

Teorema 29.- Si G es un grupo finito de orden n, $a \in G$, entonces $a^n = e$

Definición 32 (Homomorfismo). Dados G, G' dos grupos, entonces la función $\varphi : G \to G'$ es un homomorfismo si

$$\varphi(ab) = \varphi(a)\varphi(b),$$

para todo $a, b \in G$.

Definición 33 (Monomorfismo, isomorfismo y automorfismo). Dados G, G' dos grupos y un homomorfismo $\varphi : G \to G'$ un homomorfismo se dice **monomorfismo** si φ es biyectiva. Un monomorfismo es sobre G' se dice **isomorfismo** y un isomorfismo de G en G se dice **automorfismo**.

Definición 34 (Grupos isomorfos). Dos grupos G y G' se dicen isomorfos, si existe un isomorfismo de G en G'. Se escribe $G \simeq G'$.

Teorema 30 (Teorema de Cayley).- Todo grupo G es isomorfo a un subgrupo de funciones $A(S)$, con S apropiado. $A(S)$ es el conjunto de las funciones 1-1 de S en S.

Demostración del Teorema de Euler usando grupos

Dado $(\mathcal{U}_n, \cdot)$ un grupo

$|\mathcal{U}_n| = \phi(n)$

$\bar{a}^{\phi(n)} = e$ por el teorema anterior

$\bar{a}^{\phi(n)} = \bar{1}$

Tenemos que $n \mid a^{\phi(n)} - 1$

$\Rightarrow a^{\phi(n)} \equiv 1 \mod n$ ▨

En $\mathbb{Z}_n$, n entero positivo

$\mathcal{U}_n = \{\bar{a} : MCD(a,n) = 1\}$

$(\mathcal{U}_n, \cdot)$ ↪ en $\mathbb{Z}_n$

$|\mathcal{U}_n| = \phi n$

Lema 5. Si ϕ es un homomorfismo de G en G', entonces:

a. $\phi(e) = e'$ (elemento unidad en G')

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

c. $\phi(a^n) = \phi(a)^n$

Definición 35 (Imagen). La imagen de ϕ, $\phi(G)$ es

$$\phi(G) = \{\phi(a) : a \in G\}$$

Lema 6. Si ϕ es homomorfismo de G en G', entonces la imagen de ϕ es un subgrupo de G'

Definición 36 (Núcleo). Si ϕ es homomorfismo de G en G', entonces el núcleo de ϕ está definido por:

$$nu(\phi) = \{a \in G : \phi(a) = e'\}$$

Lema 7. Si $w' \in G'$ es de la forma $\phi(x) = w'$, entonces

$$\{y \in G : \phi(y) = w'\} = (ker\phi)x$$

Teorema 31. Si ϕ es homomorfismo de G en G, entonces:

a. $nu(\phi)$ es un subgrupo de G

b. Dado $a \in G$, $a^{-1}(nu\phi)a \subseteq nu\phi$

Corolario 5. Si ϕ es un homomorfismo de G en G' entonces ϕ es un monomorfismo si y solo si $nu(\phi) = \langle e \rangle$

07/11/2025

Definición (37): Subgrupo normal

Un subgrupo N de G grupo se dice normal si para todo $a \in G$.

$$aNa^{-1} \subseteq N$$

Y se denota

$$N \triangleleft G$$

Teorema 32.- $N \triangleleft G$ si y solo si toda clase lateral izquierda de N en G es clase lateral derecha de N en G.

Teorema 33 (Teorema de caracterización de subgrupos normales).-
Si G es grupo y N es subgrupo de G, las siguientes proposiciones son equivalentes.

a) N es subgrupo normal.
b) Si $a \in G$, entonces $aNa^{-1} \subset N$
c) Si $a \in G$, entonces $aNa^{-1} = N$
d) Si $a \in G$, entonces $aN = Na$
e) Si $a \in G$, entonces existe $b \in G$ tal que $aN = Nb$

Demostración: a y b se derivan de la definición.

Si N es subgrupo normal,

- P.D: $aNa^{-1} = N$ a) $\Rightarrow$ c)

  P.D: $N \subseteq aNa^{-1}$

  Sea $n \in N$ P.D: $n \in aNa^{-1}$

  $n = ene$

  $= aa^{-1}naa^{-1}$

  $= a(a^{-1}na)a^{-1}$ $a^{-1}na \in N$ por def. de grupo normal

  $n = an_1a^{-1}$

  Así, $n \in aNa^{-1}$

  P.D: $aNa^{-1} \subseteq N$: es análoga

- P.D: $aN = Na$ a) ⇒ d)

  P.D: $aN \subseteq Na$

  Sea $an_1 \in aN$ P.D: $an_1 \in Na$

  $an_1 = aa^{-1}na$

  $= na \in Na$

  P.D: $Na \subseteq aN$: es análoga

- P.D: N es normal d) ⇒ a)

  Sea $x \in aNa^{-1}$ P.D: $x \in N$

  $x = an_1a^{-1} \in a^{-1}Na$

  $xa = an_1$

  $xa \in Na$

  $x \in N$ ■

Si G es grupo abeliano, entonces todo subgrupo de G es normal? Si

$aNa^{-1} \subset N$

$ana^{-1} = aa^{-1}n \in N$

♥ Grupo de cuaterniones

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

$a(1) + bi + cj + dk.$

$i^2 = j^2 = k^2 = ijk = -1$

•	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	-k	k	j	-j
-i	-i	i	1	-1	k	-k	-j	j
j	j	-j	k	-k	-1	1	-i	i
-j	-j	j	-k	k	1	-1	i	-i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Todos son normales

$N_1 = \langle 1 \rangle$

$N_2 = \{1, -1\}$

$N_3 = \{1, -1, i, -i\}$

$N_4 = \{1, -1, j, -j\}$

$N_5 = \{1, -1, k, -k\}$

$N_6 = \{1, -1, i, -i, j, -j, k, -k\}$

si todo subgrupo de G es normal, entonces G es abeliano? Falso

Proposición: Si G es un grupo, A familia de subgrupos normales de G, entonces $\cap A$ es subgrupo normal de G.

Demostración:

- $\cap A$ es subgrupo por SG3.
- Para probar que es normal, tomamos $x \in a \cap A a^{-1}$

P.D: $x \in \cap A$

Sea $h \in \cap A$, $x = aha^{-1}$

♥ $GL_n(\mathbb{R})$ ↷ determinantes

$SL_n(\mathbb{R}) = \{A : |A| = 1\}$ P.D: $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$

Sea $B \in GL_n(\mathbb{R})$, P.D: $B\,SL_n(\mathbb{R})\,B^{-1} \subseteq SL_n(\mathbb{R})$

Sea $x \in B\,SL_n(\mathbb{R})\,B^{-1}$

$x = BAB^{-1}$ con $A \in SL_n(\mathbb{R})$

$|BAB^{-1}| = |B|\,|A|\,\frac{1}{|B|}$

$= 1$ ■

♥ Centro de G: $Z(G)$

12/11/2025

Para un grupo G y N subgrupo de G, $N \triangleleft G$. Para un subgrupo H, establecemos $a \sim b$ si $ab^{-1} \in H$. Dado

$[a] = \{x \in G : x \sim a\}$ (♥)

así,

$a \in Nb = \{nb : n \in N\}$

pero por (♥),

$[a] = Na$

Teorema 34.- Si $N \triangleleft G$ y $G/N = \{[a] : a \in G\} = \{Na : a \in G\}$ entonces, G/N es un grupo con la operación $[a][b] = [ab]$

Demostración: $[e]$ es la identidad de G/N

$[aa^{-1}] = [e]$

$[a][a^{-1}] = [e]$,

$[a^{-1}] = [a]^{-1}$

13/11/2025

Dado G un grupo $N \triangleleft G$,

$$G/N = \{[a] : a \in G\}$$
$$= \{Na : a \in G\}$$

G/N se dice G módulo N.

Teorema 35.- Si $N \triangleleft G$, entonces existe un homomorfismo Ψ de G en G/N tal que $\underset{\text{núcleo}}{\underline{nu\,\Psi}}$ es N.

$$\Psi : G \to G/N$$
$$a \mapsto Na$$

Demostración:

a) Ψ es homomorfismo

b) $nu\,\Psi = N$ ($nu\,\Psi \subseteq N$ y $N \subseteq nu\,\Psi$)

$$nu\,\Psi = \{a \in G : \Psi(a) = [e]\}$$
$$[e] = Ne = N$$
$$\Psi(a) = Na = N$$

- Sea $a \in nu\,\Psi$ P.D: $a \in N$

$$\Psi(a) = \underline{Na = N} \hookrightarrow \text{si esto pasa, } a \in N$$
$$a \in N$$

- Sea $n \in N$ P.D: $n \in nu\,\Psi$

$$\Psi(n) = Nn = N = [e]$$

Así, $n \in nu\,\Psi$

Al igual que en álgebra lineal, para probar un homomorfismo basta con probar que es inyectiva.

Si G es grupo finito, $N \triangleleft G$, entonces

$$|G/N| = \frac{|G|}{|N|}$$

Teorema 37 (Teorema de Cauchy).- Si G es grupo abeliano finito, de orden $|G|$ y p es un primo que divide al orden G, entonces existe un elemento en G de orden p.

Demostración: Inducción sobre el orden de G.

- Basa de inducción: $n = 1$

  $|G| = 1$

  No hay p primo que divida al orden de G.

- Hipótesis de inducción:

  Inducción fuerte: supongamos que el teorema se cumple para todo grupo con menos elementos que $n = |G|$

Supongamos un subgrupo $N \neq \langle e \rangle$ y $N \neq G$

- Caso 1: $p \mid |N|$ y $|N| < |G|$

  Existe un elemento en N tal que tiene orden p.

- Caso 2: $p \nmid |N|$, además, $N \lhd G$

  Sea G/N grupo cociente, por el teorema anterior,

  $$|G/N| = \frac{|G|}{|N|}$$

  y $p \nmid |N|$, $p \mid |G|$, por lo tanto,

  $p \mid |G/N|$ → demostrar que G es abeliano

  por hipótesis de inducción, existe un elemento $[e] \neq [a] \in G/N$ que tiene orden p

  $$[a]^p = [e]$$
  $$[a^p] = [e]$$
  $$a^p \in N$$

  y dado que $[a] \neq [e]$, entonces $a \notin N$

  Sea $|N| = m$

  $$(a^p)^m = e$$
  $$(a^m)^p = e$$
  $$\boxed{b = a^m}$$

  Así, va a haber un elemento de orden p.

♥ $G = \{ T_{a,b} : a, b \in \mathbb{R} \wedge a \neq 0 \}$ G' reales con la multiplicación

$$\varphi : G \to G'$$
$$T_{a,b} \mapsto a$$

$$\ker \varphi = \{ T_{a,b} : \varphi(T_{a,b}) = 1 \}$$
$$\ker \varphi = \{ T_{1,b} : b \in \mathbb{R} \}$$
$$G/\ker \varphi = \{ [T_{1,b}]\, T_{c,d} : T_{c,d} \in G \}$$
$$= \{ \ker \varphi\, T_{c,d} : T_{c,d} \in G \} \quad \ker \varphi = K$$
$$= \{ K\, T_{c,d} : T_{c,d} \in G \}$$

$$K\, T_{c,d} = \{ T_{1,b} \cdot T_{c,d} \}$$
$$= \{ T_{c,b+d} : \overset{c \neq 0}{b+d \in \mathbb{R}} \}$$
$$K\, T_{c,d} = K\, T_{c,0}$$

$$\Psi : G/N \to G'$$
$$K\, T_{c,0} \mapsto c$$

- ✡ Ψ es monomorfismo?
- ✡ Ψ es isomosfismo?

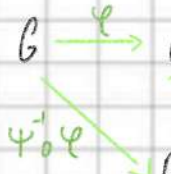
19/11/2025

Teorema (Primer Teorema de homomorfismos).- Sea φ un homomorfismo de G sobre G' con $\ker\varphi = K$, entonces

$$G/K \simeq G'$$

y el isomorfismo de G/K en G' es:

$$\begin{aligned} \Psi : G/K &\longrightarrow G' \\ Ka &\longmapsto \varphi(a) \end{aligned}$$



¿Ψ está bien definida?

Sean $Ka = Kb$ P.D: $\varphi a = \varphi b$

$$\Psi(Ka) = \varphi(a)$$
$$\Psi(Kb) = \varphi(b)$$

y φ está bien definida, es decir,

$$\varphi(a) = \varphi(b)$$

y así, Ψ es una función

¿φ es homomorfismo?

$$\begin{aligned} \Psi(Ka) &= \Psi(Kb) \\ \Psi(KaKb) &= \Psi(Kab) \\ &= \varphi(ab) \\ &= \varphi(a)\,\varphi(b) \\ &= \Psi(Ka)\,\Psi(Kb) \end{aligned}$$

Sea $x \in G'$, P.D: existe $Ka \in G/K$ tal que $\Psi(Ka) = x$

Dado que φ es sobre G', se tiene que existe $a \in G$ tal que

$$\varphi(a) = x$$

por definición de Ψ

$$\Psi(Ka) = \varphi(a) = x$$

¿Ψ es inyectiva?

Supongamos que $\Psi(Ka) = \Psi(Kb)$ P.D: $Ka = Kb$

Por hipótesis,

$$\varphi(a) = \varphi(b)$$
$$\varphi(a)\,\varphi(b^{-1}) = e$$
$$\varphi(ab^{-1}) = e$$
$$ab^{-1} \in K$$

Así, $Ka = Kb$

Teorema (Teorema de correspondencia).- Sea φ homomorfismo de G sobre G' con $\nu\varphi = K$. Si H' subgrupo de G' y

$$H = \{a \in G : \varphi(a) \in H'\}$$

Entonces, H es subgrupo de G y $K \subset H$ y $H/K \simeq H'$.
Además, si $H' \triangleleft G'$, entonces $H \triangleleft G$.

Demostración:

- Sean $a, b \in H$ P.D. $ab^{-1} \in H$

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

Por hipótesis,

$$\varphi(a) \in H' \text{ y } \varphi(b)^{-1} \in H'$$

Por tanto,

$$\varphi(a)\,\varphi(b)' \in H' \text{ pues } H' \text{ es subgrupo}$$

Así,

$$ab^{-1} \in H$$

- $K \subset H$

Sea $k \in K$

$$\varphi(k) = e' \in H'$$

Dado que H' es subgrupo,

$$k \in H$$

$$\varphi|_H : H \longrightarrow H'$$

$\varphi|_H$ es sobreyectiva porque una restricción de una función sobreyectiva es sobreyectiva.

Existe

$$\Psi|_H : H/K \to H'$$
$$Kh \longmapsto \varphi|_H(h)$$

es isomorfismo y

$$H/K \simeq H'$$

♥ Sea $H' \triangleleft G'$ P.D: $H \triangleleft G$
Sea $a \in H$ P.D: $aHa^{-1} \subseteq G$

P.D: $\varphi(aha^{-1}) \in H'$

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

Teorema (Segundo Teorema de homomorfismos).- Sea H subgrupo de G, $N \triangleleft G$, entonces

$$HN = \{hn : h \in H \wedge n \in N\}$$

es un subgrupo de G, $H \cap N \triangleleft H$

$$H/(H \cap N) \cong (HN)/N$$

Demostración:

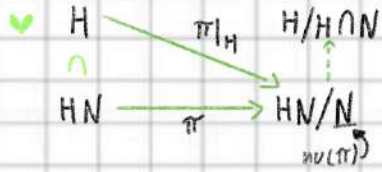
♥ P.D: $H \cap N \triangleleft H$
Sea $a \in H$ tal que P.D: $a(H \cap N)a^{-1} \subseteq H \cap N$
Sea $x \in H \cap N$,

$axa^{-1} \in H$
$axa^{-1} \in N$ ↦ pues x pertenece a la intersección ☺

♥ P.D: HN es subgrupo de G.
Sean $a_1, a_2 \in HN$ PD: $a_1 a_2^{-1} \in HN$

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1}$$
$$= h_1 h_2^{-1} (h_2 n_1 n_2^{-1} h_2^{-1}) \in HN$$
$$= h_1 h_2^{-1} (h_2 n_3 h_2^{-1}) \in HN \quad \text{con } n_3 = n_1 n_2^{-1}$$

♥ P.D: $N \subseteq HN$ y $N \triangleleft HN$

♥


$\pi : HN \to HN/N$, $a \mapsto Na$

$f = \pi|_H : H \to HN/N$, $a \mapsto Na$

f es sobre HN/N.
$\ker f = \{a \in H : Na = N\} = H \cap N$

Entonces,

$$H/H \cap N \cong HN/N$$

Teorema (Tercer Teorema de Homomorfismos).- Sea φ un homomorfismo de G sobre G' con $\ker \varphi = K$, entonces si $N' \trianglelefteq G'$

$$N = \{a \in G : \varphi(a) \in N'\}$$

se tiene que

$$G/N \simeq G'/N'$$

o lo mismo

$$G/N \simeq (G/K)/(N/K)$$

Demostración:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ & \searrow^{\Psi} & \uparrow \\ G/N & & G'/N' \end{array} \qquad \begin{aligned} \Psi : G &\longrightarrow G'/N' \\ a &\longmapsto N'\varphi(a) \end{aligned}$$

Sea $N'x' \in G'/N'$

Dado φ es sobreyectiva

$$x' = \varphi(x) \quad \text{para } x \in G$$

Tenemos que Ψ es un homomorfismo

26/11/2025

Sea S conjunto no vacío y $A(S)$ grupo simétrico de S. Si S es finito, $S_n = A(S)$
↳ grupo simétrico

$f: S \to S$ sobre y 1-1

S conjunto no vacío y $f \in A(S)$ define una relación en S.
Sean $s, t \in S$

$s \sim t$ si y solo si $t = f^i(s)$ con $i \in \mathbb{Z}$
↑ relación de equivalencia en S

- $s \sim s$ $\quad s = f^0(s)$
- Si $s \sim t$, entonces $t \sim s$ $\quad t = f^i(s)$, $s = f^{-i}(t)$
- $s \sim t$, $t \sim r$ $\quad t = f^i(s)$, $r = f^j(t)$, $r = f^{i+j}(s)$

La clase de equivalencia de s, $[s]$ se denomina **órbita de s bajo f.**

Lema.- Si $f \in A(S)$ de orden p, p es primo, entonces toda órbita de S tiene 1 o p elementos.

$$[s] = \{t : t = f^i(s)\}$$

Dado $s \in S$.

- Caso 1: $s = f(s)$
  La órbita de $[s] = \{s\}$
- Caso 2: $s \neq f(s)$
  $[s] = \{f^0(s), f(s), \dots, f^{p-1}(s)\}$
  Si no son distintos,
  $$f^i(s) = f^j(s) \quad \text{con } 0 \le i < j \le p-1$$
  $$f^{j-i}(s) = s$$
  y $0 \le m = j - i \le p-1$
  $$f^m(s) = s$$
  $f^p(s) = s$ y $m \nmid p$ entonces $ap + mb = 1$
  $$f^1(s) = f^{ap+mb}(s) = f^{ap}(f^{mb}(s))$$
  $$= f^{ap}(s)$$
  $$= s$$
  Así, la órbita de s.
  $$s, f(s), f^2(s), \dots, f^{p-1}(s)$$

Teorema de Cauchy.- Si p es un primo y p divide al orden de G, entonces G tiene un elemento de orden p.

Demostración: Demostración por inducción:

- Si $p=2$, entonces el orden de G es par, existe un elemento en G, ate tal que

$$aa = e \qquad a^2 = e$$

- Si $p \neq 2$, sea S el conjunto de las p-uplas, $(a_1, a_2, \ldots, a_p)$ donde $a_1, \ldots, a_p \in G$ y $a \cdot a \cdot \ldots \cdot a_p = e$ (1)

Sea $|G|=n$, S tiene n^{p-1} elementos.

Sean $g_1, g_2, \ldots, g_{p-1} \in G$, arbitrario >

$$g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$$

$$(g_1 g_2 \ldots) g_p = e$$

$$g_p (g_1 g_2 \ldots g_{p-1}) = e$$

$$f: S \longrightarrow S$$

$$(a_1, a_2, \ldots, a_p) \mapsto (a_p, a_1, a_2, \ldots, a_{p-1})$$

$$f \in A(S)$$

$$f = I \qquad f^p = I$$

f tiene orden p

Si $s \in S$, con órbita $[s]$ con 1 elemento, entonces $f(s)=S$ para todos los $a_i = a \in G$.

$$S = (a_1, \ldots, a_p)$$

$$S = (a_p, a, \ldots, a)$$

$$S = (a, a, \ldots, a)$$

$$a^p = e \qquad a \neq e$$

Dado que $n = |G|$, $p \mid n$. Así, $n = kp$

$$n^{p-1} = m + m_1 = m + k_1 p$$

Si $f(s) \neq s$, las órbitas tienen 1 o p elementos

$$S = \{(a, a, \ldots), (e, e, \ldots), \ldots\}$$

$$p \mid n^{p-1} \quad \text{y} \quad p \mid k_1 p$$

$$p \mid m \text{ entonces, necesariamente } m > 1$$

Lema: Dado G un grupo de orden pq, donde p, q son primos y $p>q$. Si $a \in G$ de orden p, y A es subgrupo de G generado por a, entonces

$$A \triangleleft G$$

Demostración:

Vamos a probar que A es el único subgrupo de G de orden p.

- Sea B subgrupo de orden p

P.D: $|AB| = p^2$

Sabemos que A es de orden p primo, entonces $A \cap B = \{e\}$

Si $xv = yw$, donde $x, y \in A$ y $v, w \in B$

$$x = yw v^{-1}$$

$$\underbrace{y^{-1}x}_{\in A} = wv^{-1} \Rightarrow \in B$$

Entonces pertenecen a la intersección, donde

$$x = y \quad \text{y} \quad w = v$$

Así, tenemos que $pq < p^2$ pues $p > q$.
Pero, un subgrupo no puede tener orden mayor al grupo, por lo tanto, es una contradicción.

Así, A es el único subgrupo de G de orden p.

- Sea $x \in G$

$$xAx^{-1} \text{ es de orden } p$$
$$xAx^{-1} = A$$

28/11/2025

- Sea A, B subgrupos de G, de orden m y n respectivamente.
PD: $\frac{|A||B|}{|A \cap B|} = |AB|$

$AB = \{a_i b_j : a_i \in A \text{ y } b_j \in B \text{ con } i \leq m \text{ y } j \leq n\}$
Tenemos que AB es subgrupo de G y
$A \subseteq AB$ y $B \subseteq AB$
Así mismo, tomamos $d \in A \cap B$, es decir,
$d \in A$ y $d \in B$
Sea $g \in AB$ tal que
$g = g_1 g_2 = (g_1 d)(d^{-1} g_2)$
Si $a_1 b_1 = a_2 b_2$, entonces
$d = a_i' a_1 = b_2 b_i^{-1}$

Corolario :- Si G es grupo de orden pq y $a \in G$ es de orden p y A es generado por a,

$$A \triangleleft G$$

y si $x \in G$,

$$x^{-1} a x = a^i$$

para algún $0 < i < p$
Demostración: $xAx^{-1} = A$
Sea a elemento de A,
$$xax^{-1} \in A$$
tiene que escribirse
$$xax^{-1} = a^i$$

Lema :- Si $a \in G$ es de orden m y $b \in G$ de orde n, m y n son primos relativos y $ab = ba$, entonces $c = ab$ es de orden mn.

Demostración:
Sea A subgrupo generado por a y B subgrupo generado por b. Así,
$|A| = m$ y $|B| = n$

Y dado que (♥) $MCD(m,n)=1$, entonces

$$A \cap B = \{e\}$$

Entonces,

$$|A \cap B| \mid n \quad y \quad |A \cap B| \mid m$$

por teorema de Lagrange.
Entonces tenemos que

$$(c)^i = (ab)^i = e$$
$$(ab)^i = a^i b^i = e$$
$$a^i = b^i$$

Así,

$$a^i = e \quad y \quad b^i = e$$

Donde

$$m \mid i \quad y \quad n \mid i$$

Además, por (♥),

$$mn \mid i \qquad i \geq mn$$

Así,

$$(ab)^{mn} = a^{mn} b^{mn} = e \blacksquare$$

♥ G tiene orden 15

$a \in G$ tiene orden 5 y $b \in G$ tiene orden 3 por Cauchy.
Entonces,

$$b^{-1}ab = a^i \qquad \text{para algún } 0 < i < 5$$
$$b^{-1}b^{-1}abb = b^{-1}a^i b$$
$$b^{-2}ab^2 = (b^{-1}ab)^i$$
$$b^{-2}ab^2 = (a^i)^i$$
$$b^{-3}ab^3 = a^{i^3}$$
$$a = a^{i^3}$$
$$a^{i^3-1} = e$$

Sabemos que el orden de a es 5, entonces,

$$i^3 - 1 \equiv 0 \mod 5$$
(1) $$i^3 \equiv 1 \mod 5$$

Por Fermat

(2) $$i^4 \equiv 1 \mod 5$$

Así,

$$i = 1$$

Y

$$b^{-1}ab = a$$
$$ab = ba$$

Así,

$c = ab$ orden 15

Y

$\langle c \rangle = G$ y G es cíclico $\blacksquare$

Teorema 2.8.5 → Stark

10/12/2025

Producto Directo

Sean G_1 y G_2 grupos:

- $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \wedge g_2 \in G_2\}$
  - ↳ $(g_1, g_2) * (g_3, g_4) = (g_1 * g_3, g_2 * g_4)$

Definición ( ): Producto directo

Sean $G_1, G_2, \ldots, G_n$ grupos, el producto directo es:

$$G_1 \times G_2 \times \ldots \times G_n = G$$

con elementos n-úplas.

$$(a_1, a_2, \ldots, a_n) \quad \text{donde} \quad a_i \in G_i$$

y la operación es componente a componente:

$$(a_1, a_2, a_3, \ldots, a_n) * (b_1, b_2, b_3, \ldots, b_n) = (a_1 b_1, a_2 b_2, a_3 b_3, \ldots, a_n b_n)$$

Tomamos un subgrupo de G definido como:

$$\overline{G_i} \leq G$$

$$\overline{G_i} = \{(e_1, e_2, \ldots, a_i, e_{i+1}, \ldots, e_n) : a_i \in G_i\}$$

$\overline{G_i}$ isomorfo G_i

P.D: $\overline{G_i} \triangleleft G$

Sea $b \in G$ tal que $b = (b_1, b_2, \ldots, b_n)$ P.D: $b\,\overline{G_i}\,b^{-1} \leq \overline{G_i}$

Sea $a \in \overline{G_i}$ P.D: $bab^{-1} \in \overline{G_i}$

$$\begin{aligned} bab^{-1} &= (b_1, b_2, \ldots, b_i, \ldots, b_n) * (e_1, e_2, \ldots, a_i, \ldots, e_n) * (b_1^{-1}, b_2^{-1}, \ldots, b_i^{-1}, \ldots, b_n^{-1}) \\ &= (b_1 e_1 b_1^{-1}, b_2 e_2 b_2^{-1}, \ldots, b_i a_i b_i^{-1}, \ldots, b_n e_n b_n^{-1}) \\ &= (b_1 b_1^{-1}, b_2 b_2^{-1}, \ldots, b_i a_i b_i^{-1}, \ldots, b_n b_n^{-1}) \\ &= (e_1, e_2, \ldots, b_i a_i b_i^{-1}, \ldots, e_n) \end{aligned}$$

y $b_i a_i b_i^{-1} \in G_i$

Así, $bab^{-1} \in \overline{G_i}$ y $b\,\overline{G_i}\,b^{-1} \leq \overline{G_i}$

Por tanto, se cumple que

$$\overline{G_i} \triangleleft G. \blacksquare$$

Definición ( ): G se dice que es un grupo con producto directo interno si es producto de los subgrupos normales $N_1, N_2, \ldots, N_n$ si para todo $a \in G$, tiene como representación única como producto de elementos $n_1 \in N_1, n_2 \in N_2, \ldots, n_n \in N_n$.

$$a = n_1 n_2 \ldots n_n$$

Lema :- Si $G = G_1 \times G_2 \times \ldots \times G_n$ es producto externo de $G_1, G_2, \ldots, G_n$, entonces G es producto interno de $\overline{G_1}, \overline{G_2}, \ldots, \overline{G_n}$

Lema :- Si G es grupo, M y N normales de G tales que $M \cap N = \{e\}$. Entonces, $m \in M$ y $n \in N$,

$$mn = nm$$

Lema :- Si G es producto directo interno de subgrupos normales $N_1, N_2, \dots, N_n$, entonces

$$N_i \cap N_j = \{e\} \quad \text{con } i \neq j$$

Teorema :- Dado G grupo con subgrupos normales $N_1, N_2, \dots, N_n$. Entonces

$$\Psi(a_1, a_2, \dots, a_n) = a_1 a_2 \dots a_n$$

es un isomorfismo de $N_1 \times N_2 \times \dots \times N_n$ sobre G si y solo si G es producto interno de $N_1, N_2, \dots, N_n$.

Demostración:

- Si G es producto interno de $N_1, \dots, N_n$

  P.D: $\Psi : N_1 \times N_2 \times \dots \times N_n \to G$ es isomorfo

  - P.D: Ψ es homomorfismo

    Sean $a, b \in N_1 \times \dots \times N_n$ P.D: $\Psi(ab) = \Psi(a)\Psi(b)$

    $$\begin{aligned}\Psi(ab) &= \Psi(a_1 b_1, a_2 b_2, \dots, a_n b_n) \\ &= a_1 b_1 a_2 b_2 \dots a_n b_n \\ &= a_1 a_2 \dots a_n b_1 b_2 \dots b_n \\ &= \Psi(a)\Psi(b)\end{aligned}$$

  - P.D: Ψ es inyectiva

    Sea $\Psi(a_1, a_2, \dots, a_n) = \Psi(b_1, b_2, \dots, b_n)$ P.D: $(a_1, a_2, \dots a_n) = (b_1, b_2, \dots b_n)$

    $$a_1 a_2 \dots a_n = b_1 b_2 \dots b_n$$

    $$a_i = b_i \quad \text{con } 1 \leq i \leq n$$

11/12/2025

Grupo de Permutaciones

Teorema (Teorema de Cayley).- Todo grupo G es isomorfo a un subgrupo $A(S)$ para S adecuado.

Demostración:

Sean G un grupo finito que es S, conjunto finito.
Tomamos S_n (suponiendo que S tiene n elementos).

$$\phi : G \to S_n$$

Sean $x, y \in G$ (demostrar que ϕ es homomorfismo)

$$\phi(xy) = \phi(x)\,\phi(y) \quad (\star)$$

Para cada $x \in G$

$$\lambda_x : G \to G$$
$$g \mapsto xg$$

P.D: $\lambda_x \in S_n$

- λ_x es inyectiva

  Sea $\lambda_x(a) = \lambda_x(b)$ P.D: $a = b$

  $$xa = xb$$
  $$a = b$$

- λ_x es sobreyectiva

  Sea $c \in G$ P.D: existe $g \in G$

  $$\lambda_x(g) = c$$
  $$\lambda_x(g) = xg = c$$
  $$g = x^{-1}c$$

  Si tomamos g como $x^{-1}c$, entonces

  $$\lambda_x(g) = \lambda_x(x^{-1}c)$$
  $$= x x^{-1} c$$
  $$= c$$

Así, en $(\star)$ tenemos que $\phi(x) = \lambda_x$ y $\phi(y) = \lambda_y$, entonces

$$\lambda_{xy} = \lambda_x \lambda_y$$

Sea $g \in G$ P.D: $\lambda_{xy}(g) = \lambda_x \lambda_y(g)$

$$\lambda_{xy}(g) = xyg$$
$$xyg = x(yg)$$
$$= x(\lambda_y(g))$$
$$= \lambda_x(\lambda_y(g))$$
$$= \lambda_x \lambda_y(g)$$

Entonces, ϕ es homomorfismo

$$\phi : G \longrightarrow S_n$$
$$x \longmapsto \lambda_x$$

- ϕ es 1-1

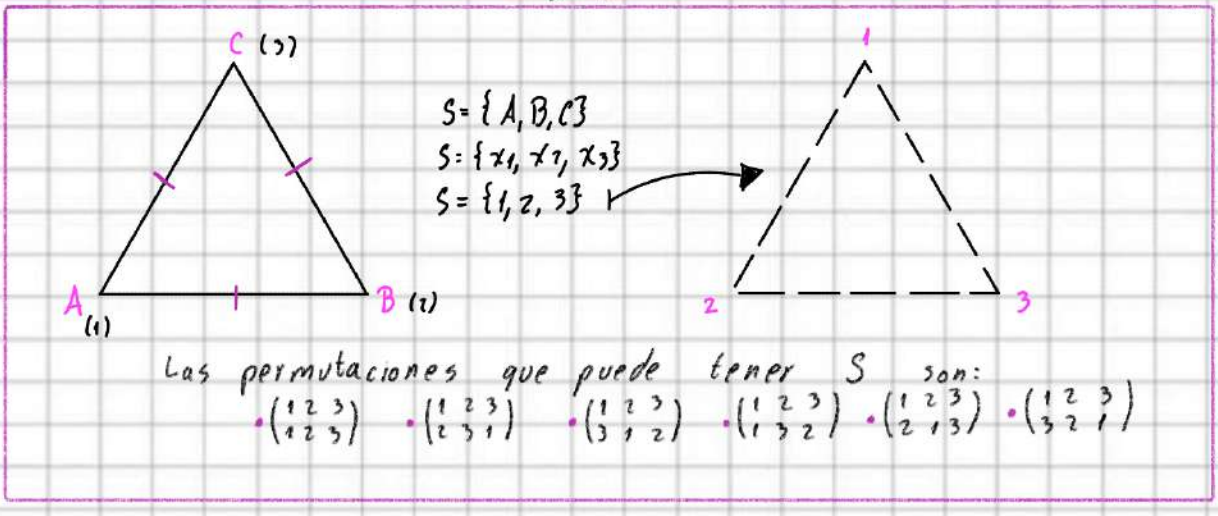
  Sea $\phi(x) = \phi(y)$, P.D: $x = y$

  Por def. de ϕ,

  $$\lambda x = \lambda y$$

  En particular,

  $$\lambda x(e) = \lambda y(e)$$
  $$xe = ye$$
  $$x = e$$



Las permutaciones que puede tener S son:

$\cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

12/12/2025

Si trabajamos en S_7:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 3 & 2 & 5 & 4 & 6 & 7 \\ 7 & 3 & 2 & 6 & 1 & 5 & 4 \end{pmatrix}$$

$\sigma \in S_7$: $\sigma(5) = 6$
$\sigma(1) = 7$
$\sigma(2) = 2$

$$\sigma^{-1} = \begin{pmatrix} 7 & 2 & 3 & 1 & 6 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 7 & 6 & 5 & 1 \end{pmatrix} \quad \sigma(\sigma^{-1}) = e$$

Ciclos de descomposición

Deficición( ): K-ciclo

Dados $i_1, i_2, \dots, i_k$ distintos en $S = \{1, 2, \dots, n\}$. El símbolo

$$(i_1, i_2, i_3, \dots, i_k)$$

representa la permutación $\sigma \in S_n$.

$\sigma(i_1) = i_2$ $\quad \sigma(i_2) = i_3$

$\sigma(i_n) = i_5$ $\dots$ $\sigma(i_j) = i_{j+1}$

para $j < k$, $\quad \sigma(i_k) = i_1$

y para $s \notin \{i_1, i_2, \dots, i_k\}$, $\quad \sigma(s) = s$

♥ En S_7:

$\tau = (1, 3, 5, 4)$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 1 & 4 & 6 & 7 \end{pmatrix}$$

$\tau = (1\ 3\ 5\ 4)$

$\sigma = (1\ 2\ 4\ 5\ 7)$

$$\begin{aligned} \sigma\tau &= (1\ 2\ 4\ 5\ 7)(1\ 3\ 5\ 4) \\ &= (1\ 3\ 7)(2\ 4)(5)(6) \\ &= (1\ 3\ 7)(2\ 4) \end{aligned}$$

$$\begin{aligned} \tau\sigma &= (1\ 3\ 5\ 4)(1\ 2\ 4\ 5\ 7) \\ &= (1\ 2)(3\ 5\ 7)(4) \\ &= (3\ 5\ 7)(1\ 2) \end{aligned}$$

Sea $S = \{1, 2, \ldots, n\}$, $i_1, i_2 \in S$
$\tau = (i_1, i_2)$ transposición

Si K-ciclo y m-ciclo no tienen elementos en común, se dicen ciclos disjuntos.

Lema .- Si σ y τ son ciclos disjuntos en S_n, entonces $\sigma\tau = \tau\sigma$

Demostración:

P.D: Para todo $s \in S$, $\sigma\tau(s) = \tau\sigma(s)$

♥ Si $s \notin \sigma$ y $s \notin \tau$, entonces

$$\begin{aligned} \sigma\tau(s) &= \sigma(\tau(s)) \\ &= \sigma(s) \\ &= s \\ &= \tau(s) \\ &= \tau(\sigma(s)) \\ &= \tau\sigma(s) \end{aligned}$$

♥ Si $s \in \tau$

$$\sigma\tau(s) = \sigma(\tau(s))$$

♥ Sea $\tau(s) = i_s$

- $\sigma(\tau(s)) = \sigma(i_s)$
  $= i_s$ pues σ y τ son disjuntos
- $\tau(\sigma(s)) = \tau(s)$
  $= i_s$

Lema .- Toda permutación de S_n es producto de ciclos disjuntos.

↳ Deber

★ Todo K-ciclo tiene orden K. $\sigma = (i_1\ i_2\ \dots\ i_k)$

P.D: $\sigma^k = e$

Si tomamos i_1:

$\sigma(i_1) = i_2$

$\sigma(i_2) = i_3$

$\sigma^2(i_1) = \sigma(\sigma(i_1)) = \sigma(i_2) = i_3$

$\vdots$

Así, $\sigma = (i_1\ \sigma(i_1)\ \sigma^2(i_1)\ \dots\ \sigma^{k-1}(i_1))$

es la órbita de i_1 con respecto a σ

$\{i_1, \sigma(i_1), \dots, \sigma^{k-1}(i_1)\}$

Para $i \in \sigma$

$\{i, \sigma(i), \dots, \sigma^{k-1}(i)\}$

P.D: $\sigma^k = e$

$\sigma^k(i) = i$

Por tanto,

$\sigma^k = e$

★ Dada $\sigma \in S_n$, tiene descomposición en ciclos disjuntos de tamaño $m_1, m_2, \dots, m_k$. El orden de σ es el $mcm(m_1, m_2, \dots, m_k)$.

Demostración:

Sea $\sigma = \tau_1 \tau_2 \dots \tau_k$, donde τ_i es de tamaño m_i para $1 \le i \le k$.

Sea $M = mcm(m_1, m_2, \dots, m_k)$

σ tiene orden M ($\sigma^M = e$ y M es el más pequeño con esta propiedad)

$\sigma^M = (\tau_1\ \tau_2 \dots \tau_k)^M$

dado que τ_1, τ_2 son ciclos disjuntos. Por el lema anterior se cumple que $\tau_i \tau_j = \tau_j \tau_i$

$\sigma^M = \tau_1^M \tau_2^M \dots \tau_k^M$

y $m_i | N$, entonces $\tau_i^M = e$

Así,

$\sigma^M = e$

Por otro lado, sea $\sigma^N = e$ P.D: $M | N$

$\sigma^N = \tau_i^N \dots \tau_k^N$

$m_i | N$

Así,

$M | N$

Lema .- Toda permutación en S_n, es producto de transposiciones

17/12/2025

18/12/2025

Anillos

Dado un conjunto no vacío R, se definen dos operaciones. $+, \cdot, R$ se dice anillo si cumple:

a) Cerradura de la suma: Dados $a, b \in R$, entonces $a+b \in R$
b) Conmutativa de la suma: Para todo $a, b \in R$, entonces $a+b = b+a$
c) Asociativa de la suma: Dados $a, b, c \in R$, entonces $(a+b)+c = a+(b+c)$
d) Existencia del neutro: Existe un elemento $0 \in R$ tal que para todo $x \in R$, $0+x = x$
e) Existencia del inverso de la suma: Dado $a \in R$, existe un elemento b tal que $a+b=0$ y b se escribe $-a$.

R es grupo abeliano con respecto a $+$.

f) Cerradura del producto: Sean $a, b \in R$, entonces $a \cdot b \in R$
g) Asociativa del producto: Dados $a, b, c \in R$, entonces $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
h) Distributiva del producto con respecto a la suma: Sean $a, b, c \in R$, entonces $a(b+c) = ab + ac$ y $(b+c)a = ba + ca$

Anillo Con Unidad:
Dado un anillo R, si $1 \in R$ tal que $1 \neq 0$ y para todo $a \in R$.
$$a \cdot 1 = 1 \cdot a = a$$

Anillo Conmutativo:
Sea R un anillo, se dice conmutativo si para todo $a, b \in R$:
$$a \cdot b = b \cdot a$$

Definición ( ): Dominio integral
Un anillo conmutativo R es dominio integral si $a \cdot b = 0$ implica que $a = 0$ ∨ $b = 0$. Ej: $\mathbb{Z}$

Definición ( ): Anillo de división
Sea R un anillo con unidad, se dice que R es anillo de división si para todo $a \neq 0$, existe $b \in R$ tal que
$$ab = 1 \quad \text{y} \quad ba = 1$$
Así, b se denota a^{-1}.

Definición ( ): Cuerpo

Un anillo R se dice cuerpo si es anillo conmutativo de división.

✔ $\mathbb{Z}_p$ con p primo es cuerpo.

Sea $\bar{a} \in \mathbb{Z}_p$, $\bar{a} \neq 0$ P.D: existe $\bar{b} \in \mathbb{Z}_p$ tal que $\bar{a}\bar{b} = 1$

$MCD(a,p) = 1$ pues p es primo

$a^{p-1} \equiv 1 \mod p$

$a \cdot a^{p-2} \equiv 1 \mod p$

$\bar{a}\,\bar{a}^{p-2} = \bar{1}$

b es $\bar{a}^{p-2}$

Definición ( ): Cero divisor

Un elemento $a \neq 0$ en el anillo R se dice cero divisor si

$$ab = 0 \quad \text{y} \quad ba = 0$$

Para algún $b \neq 0$.

Sea $R \subseteq \mathbb{Q}$, $a \in \mathbb{Q}$ tal que $a = \frac{m}{n}$. Sea $R = \{a : a = \frac{m}{n}$; m, n primos relativos y m es impar$\}$

- R es anillo $+, \cdot$ en $\mathbb{Q}$.
- R es dominio integral, anillo de división, cuerpo
  - ✔ P.D: R es anillo
    - Cerradura de la suma: Sean $a, b \in R$ tales que

$$a = \frac{m_1}{n_1} \quad \text{y} \quad b = \frac{m_2}{n_2}$$

P.D: $a + b \in R$

$$a + b = \frac{m_1}{n_1} + \frac{m_2}{n_2}$$

Por def. de R: $MCD(m_1, n_1) = 1$ y $MCD(m_2, n_2) = 1$.

$$\Rightarrow a + b = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$$

P.D: $m_1 n_2 + m_2 n_1$ es impar

Por hipótesis, m_1 y m_2 se pueden escribir como:

$$m_1 = 2k_1 + 1 \quad \text{y} \quad m_2 = 2k_2 + 1$$

Así, $m_1 n_2 + m_2 n_1 = (2k_1 + 1)n_2 + (2k_2 + 1)n_1$

$$= 2k_1 n_2 + n_2 + 2k_2 n_1 + n_1$$

$$= 2(k_1 n_2 + k_2 n_1) + n_1 + n_2$$

- Contraejemplo: sean $a = \frac{1}{5}$ y $b = \frac{1}{3}$

$$a + b = \frac{1}{5} + \frac{1}{3} = \frac{8}{3} \quad \text{y } 8 \text{ es par}$$

$a + b \notin R$.

R no es anillo.

Sea $R \subseteq \mathbb{Q}$, $a \in \mathbb{Q}$ tal que $a = \frac{m}{n}$. Sea $R = \{a : a = \frac{m}{n}$; m, n primos relativos y n es impar$\}$

- R es anillo $+, \cdot$ en $\mathbb{Q}$.
- R es dominio integral, anillo de división, cuerpo

Definición ( ): Subanillo

H se dice subanillo de R anillo si $H \subseteq R$ no vacío y H es anillo.

Teorema (Teorema de caracterización de subanillos).- Sea R anillo y $H \subseteq R$ no vacío, H se dice subanillo de R si:

(SA_1) Para todo $a, b \in H$: $a + b \in H$
(SA_2) Sea $a \in H$, entonces $-a \in H$
(SA_3) Dados $a, b \in H$, entonces $ab \in H$

→ Se pueden usar estas 3

Para demostrar: ↕

(SA_4) Dados $a, b, c \in H$, entonces $ab - b \in H$ → O se puede usar este

Ejemplo: R conjunto de funciones continuas en $[0,1]$ para $x \in [0,1]$, $f, g \in R$

$(f+g)(x) = f(x) + g(x)$ $\quad$ $(f \cdot g)(x) = f(x) \cdot g(x)$

- P.D: R es dominio integral
  - Dado que hereda las propiedades de los reales, se cumple:
    - Cerradura de la suma
    - Conmutativa de la suma
    - Asociativa de la suma
    - Existencia del neutro: la función nula tq $h(x) = 0$ $\forall x \in [0,1]$
    - Existencia del inverso de la suma:
      Sean $f, g \in R$ tales que $f(x) + g(x) = 0$. Entonces, $g(x) = -g(x)$.
    - Cerradura del producto
    - Asociativa del producto
    - Distributiva del producto respecto a la suma
  - P.D: R es dominio integral
    - Contraejemplo:

19/12/2025

Lema .- Dado R un anillo. Sea $a, b \in R$

a) $a \cdot 0 = 0 \cdot a = 0$

b) $a(-b) = (-a)b = -(ab)$

c) Si $1 \in R$, entonces $-1(a) = -a$

Demostración:

a) Dado que R es un anillo, entonces existe $0 \in R$ tal que $b + 0 = b$ (1)

Si multiplicamos (1) por a, entonces,

$$ab + a0 = ab$$

Y dado que R es anillo, $ab \in R$ y existe su inverso aditivo. Así:

$$-ab + ab + a0 = -ab + ab$$

$$a0 = 0 \quad (2)$$

Multipliquemos a en (1) por el otro lado.

$$ba + 0a = ba$$

$$-ba + ba + 0a = -ba + ba$$

$$0a = 0 \quad (3)$$

Así, de (2) y (3), se cumple que

$$a0 = 0a = 0$$

Definición ( ): Anillo Booleano

Un anillo R se dice Booleano si para todo $x \in R$,

$$x^2 = x$$

Lema .- Todo elemento Booleano es conmutativo.

Demostración:

Sean $x, y \in R$. Si R es Booleano, P.D: $xy = yx$

Por hipótesis:

$$x^2 = x \quad \text{y} \quad y^2 = y$$

Así, tomamos $(x+y)^2 \in R$, es decir, $(x+y)^2 = x + y$ (♥)

$$(x+y)^2 = (x+y)(x+y)$$

$$= (x+y)x + (x+y)y$$

$$= x^2 + xy + yx + y^2$$

Por (♥) e hipótesis:

$$x + y = x + xy + yx + y^2$$

$$0 = xy + yx \quad (1)$$

$$0x = xyx + yx^2 \quad (2)$$

$$x0 = x^2y + xyx \quad (3)$$

$$xyx + yx^2 = xyx + x^2y$$

$$yx^2 = x^2y$$

$$yx = xy \quad \blacksquare$$

Definición ( ): Homomorfismo de anillo

Sean R y R' anillos, $\varphi: R \to R'$. φ se dice homomorfismo si para $a, b \in R$ se cumple que:

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$

♥ $nu(\varphi) = \{x \in R : \varphi(x) = 0\}$

P.D: $nu(\varphi)$ es subanillo de R.

Sean $a, b \in nu(\varphi)$, entonces

$$ab \in nu(\varphi)$$
$$\varphi(ab) = \varphi(a)\varphi(b) = 0$$

Si $a, b \in nu\,\varphi$, $a \pm b \in nu\,\varphi$

$$\varphi(a \pm b) = \varphi(a) \pm \varphi(b)$$
$$= 0 \pm 0$$
$$= 0$$

$\varphi(b + (-b)) = 0$
$\varphi(b) + \varphi(-b) = 0$
Por lo tanto
$-\varphi(b) = \varphi(-b)$

Sea $r \in R$

$$r(nu\,\varphi) = \{r \cdot n : n \in nu\,\varphi\}$$
$$rn \in nu\,\varphi$$
$$\varphi(rn) = \varphi(r)\varphi(n) = 0$$

Definición ( ): Ideal

Sea R un anillo, llamaremos ideal de R a un subconjunto I no vacío de R tal que

- I subgrupo aditivo
- Para todo $r \in R$ y $a \in I$: $ra \in I$ y $ar \in I$

Lema .- $\varphi: R \to R'$ homomorfismo, entonces $nu\,\varphi$ es un ideal de R.

♥ Sea R un anillo y K subgrupo aditivo de R,

$$R/K = \{a + K : a \in R\}$$

$$(a+K)(b+K) = ab + K$$
$$a + K = a' + K$$
$$b + K = b' + K$$
$$a - a' \in K \text{ ; llamaremos}$$
$$b - b' \in K$$

P.D: $(a+K)(b+K) = ab + K = a'b' + K$

P.D: $ab - a'b' \in K$

K tiene que ser ideal

$$(a - a')b \in K \quad \text{y} \quad a'(b - b') \in K$$
$$ab - a'b$$
$$a'b - a'b'$$
$$\Rightarrow ab - a'b' \in K$$

- R/K es anillo

  Sean $a, b \in R$

  $(a+K)+(b+K) = (a+b)+K$

  $(a+K)(b+K) = ab+K$

Teorema - Sea K un ideal de R anillo. El anillo cociente R/K como grupo aditivo con el producto

$$(a+K)(b+K) = ab+K$$

y

$$\varphi : R \to R/K$$
$$a \mapsto a+K$$

φ es homomorfismo de R en R/K

8. Let $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$ and let $\mathbb{C}$ be the field of complex numbers.

Define $\psi: R \to \mathbb{C}$ by $\psi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$. We leave it to the reader to verify that ψ is an isomorphism of R onto $\mathbb{C}$. So R is isomorphic to the field of complex numbers.

- $\Psi: R \longrightarrow \mathbb{C}$ P.D: Ψ es isomorfismo

  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a+bi$

- P.D: Ψ es inyectiva:

  Sean $X, Y \in R$ tales que:

  (♥) $X = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $Y = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

  Así, si $\Psi(X) = \Psi(Y)$ (1) P.D: $X = Y$

  De (1):

  $$a+bi = c+di$$
  $$(a+bi)-(c+di) = 0$$
  $$(a-c)+(b-d)i = 0$$

  Dado que $a, b, c, d \in \mathbb{R}$, entonces tenemos:

  $$a-c = 0 \quad y \quad (b-d)i = 0\,i$$

  Así, $a = c$ y $b = d$

  Por lo tanto, $X = Y$ y Ψ es isomorfismo.

- P.D: Ψ es sobreyectiva

  PD: $\mathbb{C} = rec(\Psi)$

  - P.D: $rec(\Psi) \subseteq \mathbb{C}$

    Sea X, definida en (♥) anteriormente, entonces

    $$\Psi(X) = a+bi$$

    donde $a, b \in \mathbb{R}$, las cuales pueden tomar cualquier valor. Por lo tanto, por def. de número complejo,

    $$\Psi(X) \in \mathbb{C}$$

- P.D: $\mathbb{C} \subseteq rec(\Psi)$

  Sean $a, b \in \mathbb{R}$,

  $a + bi \in \mathbb{R}$

  Por otro lado, $\Psi(x) = a + bi$

  Así, $a + bi \in rec(\Psi)$

Así, $\mathbb{C} = rec(\Psi)$ y Ψ es sobreyectiva.
Por lo tanto, Ψ es un isomorfismo de $\mathbb{R}$ en $\mathbb{C}$

- P.D: Ψ es un homomorfismo.

  P.D: Se preserva la suma y el producto

  - P.D: $\Psi(X+Y) = \Psi(X) + \Psi(Y)$, con $X \wedge Y \in R$ (*)

    Sean $X = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ y $Y = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, entonces

$$X + Y = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}$$

    Así, por def. de Ψ,

$$\begin{aligned} \Psi(X+Y) &= (a+c) + (b+d)i \\ &= a + c + bi + di \\ &= a + bi + c + di \quad \text{pues } a, b, c, d \in \mathbb{R} \\ &= (a+bi) + (c+di) \end{aligned}$$

$$\Psi(X+Y) = \Psi(X) + \Psi(Y)$$

    Por tanto, Ψ preserva la suma.

  - P.D: $\Psi(XY) = \Psi(X)\Psi(Y)$

    Consideramos $X \wedge Y \in R$, definidos en (*). Entonces,

$$XY = \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & -bd + ac \end{pmatrix}$$

    Así, $\Psi(XY) = (ac - bd) + (ad + bc)i$ i)

    Por otro lado, tenemos que

$$\begin{aligned} \Psi(X)\Psi(Y) &= (a+bi)(c+di) \\ &= ac + adi + bci - bd \\ &= ac - bd + adi + bci \end{aligned}$$

$$\Psi(X)\Psi(Y) = (ac - bd) + (ad + bc)i \quad ii)$$

    Por lo tanto, por i) y ii), Ψ preserva el producto, es decir,

$$\Psi(XY) = \Psi(X)\Psi(Y)$$

Dado que Ψ cumple con ser un isomorfismo de $\mathbb{R}$ en $\mathbb{C}$, entonces $\mathbb{R}$ y $\mathbb{C}$ son isomorfos entre sí ■

07/01/2025

- Dado el anillo de funciones reales en $[0,1]$ R,

$$f+g(x) = f(x)+g(x)$$
$$fg(x) = f(x)g(x)$$
$$I = \{f \in R : f(\tfrac{1}{2}) = 0\}$$

I es ideal de R?

- P.D: $f-g \in I$

$$f-g(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2}) = 0$$

- P.D: $fg \in I$

$$fg(\tfrac{1}{2}) = f(\tfrac{1}{2})g(\tfrac{1}{2}) = 0$$

- Sea $h \in R$ y $f \in I$ ∘ P.D: $fh \in I$

$$fh(\tfrac{1}{2}) = f(\tfrac{1}{2})h(\tfrac{1}{2}) = 0$$

Qué es R/I?

$$R/I = \{r+I : r \in R\}$$
$$r(x) = \underbrace{r(x) - r(1/2)}_{h(x)} + r(1/2)$$
$$h(\tfrac{1}{2}) = r(\tfrac{1}{2}) - r(\tfrac{1}{2}) = 0$$

$$r(x)+I = h(x) + r(\tfrac{1}{2}) + I = r(\tfrac{1}{2}) + I$$

$$R/I = \{r(\tfrac{1}{2}) + I : r \in R\}$$
$$r(\tfrac{1}{2}) \in R$$
$$\varphi : \mathbb{R} \to R/I$$

$$\varphi : R/I \longrightarrow \mathbb{R}, \quad r(\tfrac{1}{2})+I \mapsto r(\tfrac{1}{2})$$

- $R = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}\right\}$

$$I = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R}\right\}$$

a) I ideal de R
b) R/I
c) $R/I \simeq$?

a) P.D: I es ideal de R

- P.D: Es subgrupo aditivo.

Sean $M, N \in I$, $x \in \mathbb{R}$

P.D: $M+N \in I$

$$M+N(x) = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x+x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2x \\ 0 & 0 \end{pmatrix} \quad : 2x \in \mathbb{R}$$

$$\Rightarrow M+N \in I$$

- Sea $H \in R$ P.D: $HN \in I$ y $NH \in I$
  - ☆ P.D: $HN \in I$

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix}$$

Dado que $a, b, c \in \mathbb{R}$, $ac \in \mathbb{R}$ y $HN \in I$

  - ☆ P.D: $NH \in I$

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & c \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$$

Así, $NH \in I$

♥ Dado R anillo conmutativo, con $1 \neq 0$, $a \in R$

$$\langle a \rangle = \{xa : x \in R\}$$

Entonces, $\langle a \rangle$ es ideal de R.

Sean $u \in \langle a \rangle$ y $v \in \langle a \rangle$

P.D: $u - v \in \langle a \rangle$

Si $u = xa$ y $v = ya$ $x, y \in R$

$u - v = xa - ya = (x-y)a \in \langle a \rangle$

Si $u \in \langle a \rangle$ y $r \in R$

$ru = (rx)a \in \langle a \rangle$

Proposición.- Sea R un anillo con $1 \neq 0$. Un ideal I es igual R si y solo si I contiene a 1.

i) Si $I = R$, entonces I contiene a 1.

ii) Si $1 \in I$, entonces $I = R$

Demostración:

⇐) Si $1 \in I$ P.D: $I = R$

P.D: $R \subseteq I$

Sea $r \in R$ P.D: $r \in I$

$r \cdot 1 \in I$
$1 \cdot r \in I$ } → I es ideal por eso se cumple

$r \cdot 1 = r$

entonces,

$r \in I$

Definición ( ): Suma, producto y potencia de ideales

Sea R anillo y I, J ideales.

Suma: $I+J=\{a+b: a\in I \wedge b\in I\}$

Producto: I y J son las sumas finitas de los elementos a_ib_i tal que $a_i\in I \wedge b_i\in J$.

$$IJ=\{a_1b_1+a_2b_2+\dots+a_nb_n: a_i\in I \wedge b_i\in J\}$$

Potencia: I^k es el producto iterativo de I y $I^0=R$

Proposición: Dados I, J ideales de R anillo. Entonces, $I+J, I\cdot J, I\cap J$ son ideales de R y además,

$$IJ \subseteq I\cap J \subseteq \begin{matrix} I \\ J \end{matrix} \subseteq I+J$$

Demostración:

- P.D: $I+J$ es ideal de R

  Sea $r\in R$ y $a+b\in I+J$

  $$r(a+b)=ra+rb\in I+J \quad (ra\in I,\ rb\in J)$$

- P.D: IJ es ideal de R

  $$a_1b_1+a_2b_2+\dots+a_nb_n\in IJ$$
  $$a_1'b_1'+a_2'b_2'+\dots+a_n'b_n'\in IJ$$

  $r\in R$

  $$\Rightarrow r(a_1b_1+\dots+a_nb_n)=ra_1b_1+\dots+ra_nb_n\in IJ$$

- P.D: $I\cap J$ es ideal de R

  }

- Por 2.20 de Pinter, se cumplen $I\cap J\subseteq I$ y $I\cap J\subseteq J$
- P.D: $IJ\subseteq I\cap J$

  Sean $a\in I$, $b\in J$

  $$ab\in I$$
  $$ab\in J$$
  $$\Rightarrow ab\in I\cap J$$

Definición ( ): Ideales comaximales

Sea R un anillo con $1\neq 0$ y dos ideales I, J tal que

$$I+J=R$$

Definición ( ): Suma directa

Sean R y S anillos, la suma directa

$$R\oplus S=\{(r,s): r\in R \wedge s\in S\}$$
$$(r,s)+(t,u)=(r+t,\ s+u)$$
$$(r,s)(t,u)=(rt,\ su)$$

Teorema (Teorema chino del resto para anillos).- Dado un anillo conmutativo con unidad $1 \neq 0$ y $A_1, A_2, \ldots, A_k$ ideales de R. La función:

$$\begin{aligned} \Psi : R &\longrightarrow R/A_1 \oplus R/A_2 \oplus \ldots \oplus R/A_k \\ r &\longmapsto (r+A_1, r+A_2, \ldots, r+A_k) \end{aligned}$$

es homomorfismo, con

$$\operatorname{nu}\Psi = A_1 \cap A_2 \cap \ldots \cap A_k$$

Si A_i son ideal comaximales 2 a 2, entonces

$$A_1 A_2 \ldots A_k = A_1 \cap A_2 \cap \ldots \cap A_k$$

y

$$R/A_1 \ldots A_k \simeq R/A_1 \oplus R/A_2 \oplus \ldots \oplus R/A_k$$

Demostración:

- P.D. Ψ es homomorfismo.

  ✓ Sean $a, b \in R$ P.D: $\Psi(a+b) = \Psi(a) + \Psi(b)$

  $$\begin{aligned} \Psi(a+b) &= ((a+b)+A_1, (a+b)+A_2, \ldots, (a+b)+A_k) \\ &= (a+b+A_1, a+b+A_2, \ldots, a+b+A_k) \\ &= ((a+A_1)+(b+A_1), (a+A_2)+(b+A_2), \ldots, (a+A_k)+(b+A_k)) \\ &= (a+A_1, a+A_2, \ldots, a+A_k) + (b+A_1, b+A_2, \ldots, b+A_k) \\ &= \Psi(a) + \Psi(b) \end{aligned}$$

  ✓ P.D: $\Psi(ab) = \Psi(a)\Psi(b)$

  $$\begin{aligned} \Psi(ab) &= (ab+A_1, ab+A_2, \ldots, ab+A_k) \\ &= ((a+A_1)(b+A_1), (a+A_2)(b+A_2), \ldots, (a+A_k)(b+A_k)) \\ &= (a+A_1, a+A_2, \ldots, a+A_k)(b+A_1, b+A_2, \ldots, b+A_k) \\ &= \Psi(a)\Psi(b) \end{aligned}$$

- P.D: $\operatorname{nu}\Psi = A_1 \cap A_2 \cap \ldots \cap A_k$

  Demostración por inducción:

  ✓ Para $k=2$,

  $$\begin{aligned} \Psi : R &\to R/A_1 \oplus R/A_2 \\ r &\mapsto (r+A_1, r+A_2) \end{aligned}$$

  P.D: $\operatorname{nu}\Psi = A_1 \cap A_2$

  $$\operatorname{nu}\Psi = \{r : \Psi(r) = (A_1, A_2)\}$$

  $$\Psi(r) = (r+A_1, r+A_2)$$

  $$r + A_1 = A_1$$

  $$\operatorname{nu}\Psi = \{r : r \in A_1 \wedge r \in A_2\} = A_1 \cap A_2$$

  } → Paso de inducción

- Supongamos que A_1, A_2 son comaximales P.D: $A_1 A_2 = A_1 \cap A_2$

  ✓ $A_1 A_2 \subseteq A_1 \cap A_2$ se cumple por prop anterior

✓ P.D: $A_1 \cap A_2 \subseteq A_1 A_2$

Sea $x \in A_1 \cap A_2$ P.D: $x \in A_1 A_2$

$x \in A_1$ y $x \in A_2$

dado que A_1 y A_2 son comaximales, entonces

$$A_1 + A_2 = R$$
$$1 \in A_1 + A_2$$
$$1 = a_1 + a_2$$

Sea $x \in R$ tal que

$$x = x \cdot 1$$
$$= xa_1 + xa_2$$
$$\Rightarrow x \in A_1 A_2$$

- P.D: Ψ es sobreyectiva

Sea $x \in R/A_1 \oplus R/A_2$ (v) P.D: existe r tal que $\Psi(y) = x$

Por (v), tenemos que x se puede escribir como

$$x = (r + A_1, s + A_2)$$

Tenemos que $a_1 + a_2 = 1$ y escribimos y como

$$y = r + s$$
$$y = ra_1 + sa_2$$

Así,

$$\Psi(y) = (ra_1 + sa_2 + A_1, ra_1 + sa_2 + A_2)$$
$$= (sa_2 + A_1, ra_1 + A_2)$$
$$= (s(1 - a_1) + A_1, r(1 - a_2) + A_2$$
$$= (s + A_1, r + A_2)$$

08/01/2025

- Si R es un anillo conmutativo con unidad con sus únicos ideales son $\langle 0 \rangle$ y R. R es cuerpo.
  - Demostrar que R es anillo de división

    Dado $a \in R$, $a \neq 0$. Entonces existe $b \in R$ tal que

    $$ab = 1$$

    Sea $\langle a \rangle = \{x \cdot a : x \in R\}$ es ideal, entonces

    $$\langle a \rangle = R$$

    $$1 \in \langle a \rangle$$

    Así, existe b tal que

    $$1 = a \cdot b$$

    Por tanto, R es cuerpo.
- Si R es cuerpo, todos los ideales de R son $\langle 0 \rangle$ y R.
  - Sea $I \neq \langle 0 \rangle$, ideal de R P.D: $I = R$
    - ✓ $R \subseteq I$:

      Sea $r \in R$ P.D: $r \in I$

      Sea $u \in I$, $u^{-1} \in R$. Entonces,

      $$1 = uu^{-1} \in I$$

Sea un homomorfismo $\varphi : R \longrightarrow R'$, donde R es cuerpo, por teorema de correspondencia, R' es cuerpo.

Definición ( ): Ideal Maximal

Un ideal propio (distinto a los triviales) M de R se dice ideal Maximal si los únicos ideales de R que contienen a M son M y R.

Teorema :- Si R anillo conmutativo con unidad y R' anillo. ϕ homomorfismo de R sobre R'. Entonces, $\phi(1)$ es la unidad de R'.

Demostración:

Sea $r' \in R'$ P.D: $r' \cdot \phi(1) = r'$

Dado que ϕ es sobreyectivo, existe $a \in R$ tal que $\phi(a) = r'$

$$\phi(a)\phi(1) = \phi(a \cdot 1)$$
$$= \phi(a)$$
$$= r' \blacksquare$$

Teorema :- Sea R anillo conmutativo con unidad $1 \neq 0$ y M ideal maximal de R. Entonces, R/M es cuerpo.

Demostración:

Sea φ sobreyectivo, tal que

$$\varphi : R \longrightarrow R/M$$
$$r \longmapsto r + M$$

Donde $1 + M$ es la unidad de R/M.

Así, R/M es anillo conmutativo con unidad $1 + M \neq M$.

Si I' es ideal de R/M, entonces

$I' = \langle 0 \rangle$ ✓ $I' = R/M$

↳ $I' = M$ ✗

Sea $I' \neq M$, existe $r + M \in I'$, con $r \notin M$.

$I' = \langle r + M \rangle$

Dado que $1 + M \in I'$, entonces $1 \notin M$ y por tanto, $R/M = I'$ ■

✔ Si R un anillo conmutativo con unidad tal que M es ideal de R y R/M es cuerpo. Entonces M es maximal de R.

Sea $\varphi : R \to R/M$ sobreyectiva. Dado que R/M es cuerpo, por teorema de correspondencia, R es cuerpo y por ende, M es ideal maximal de R.

Anillo de Polinomios

Dado $\mathbb{F}$ cuerpo. Un anillo de polinomios con x en $\mathbb{F}$, contiene a los elementos expresados de la siguiente forma:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \quad \text{con} \quad n \geq 0 \text{ y } a_i \in \mathbb{F}$$

Se denota $\mathbb{F}[x]$.

Igualdad: Sean $p(x), q(x) \in \mathbb{F}[x]$ tales que

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \wedge \quad b_0 + b_1 x + \ldots + b_m x^m$$

con $n \geq 0$ y $m \geq 0$.

Se dice que $p(x)$ es igual a $q(x)$ si para todo $i \geq 0$,

$$a_i = b_i$$

Si $n < m$, entonces:

$$b_{n+1} = \ldots = b_m = 0$$

Definición ( ): Suma en el anillo de polinomios

Sean $p(x), q(x) \in \mathbb{F}[x]$, tales que

$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a x^n$ y $q(x) = b_0 + b_1 x + \ldots + b_m x^m$

La suma se define como:

$$p(x) + q(x) = p(x) + q(x) = c_0 + c_1 x + \ldots + c_s x^s$$

donde $c_i = a_i + b_i$ y s es el mayor de los grados n y m.

Definición ( ): Producto en $\mathbb{F}[x]$

Sean $p(x), q(x) \in \mathbb{F}[x]$ tales que

$p(x) = a_0 + a_1 x + \ldots + a x^n$ y $q(x) = b_0 + b_1 x + \ldots + b_m x^n$

El producto se define como:

$$pq(x) = c_0 + c_1 x + \ldots + c_t x^t$$

donde $c_i = a_i b_0 + a_{i-1} b_1 + \ldots + a_0 b_i$

para todo $i \geq 0$.

Ejemplo: $p(x) = 1 + x - x^2 \qquad q(x) = 2 + x^2 + x^3$

$$pq(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + c_6 x^6 + \dots$$

- $c_0 = 2$
- $c_1 = 2$
- $c_2 = -1$
- $c_3 = 2$
- $c_4 = 0$
- $c_5 = -1$
- $c_6 = c_7 = c_8 = \dots = 0$

$$\Rightarrow pq(x) = 2 + 2x - x^2 + 2x^3 - x^5$$

♥ Verificar que $\mathbb{F}[x]$ es anillo conmutativo con unidad.

- Sean $p(x), q(x) \in \mathbb{F}[x]$. P.D: $p(x)\,q(x) = q(x)\,p(x)$

Tenemos que

$$p(x)\,q(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_t x^t$$

y

$$q(x)\,p(x) = d_0 + d_1 x + d_2 x^2 + \dots + d_r x^r$$

Tenemos que probar que estos son iguales.

Por def. de producto de polinomios,

$$c_i = a_i b_0 + a_{i-1} b_1 + \dots + a_0 b_i$$

y

$$d_i = b_i a_0 + d_{i-1} a_1 + \dots + b_0 a_i$$

P.D: $c_i = d_i$

Supongamos que son distintos, es decir, existe n tal que

$$c_i - d_i = n$$

$$a_i b_0 + a_{i-1} b_1 + \dots + a_0 b_i - (b_i a_0 + b_{i-1} a_1 + \dots + b_0 a_i) = n$$

$$(a_i b_0 - b_0 a_i) + (a_{i-1} b_1 - b_1 a_{i-1}) + \dots + (a_1 b_{i-1} - b_{i-1} a_1) + (a_0 b_i - b_i a_0) = n$$

Dado que están definidos sobre un cuerpo

09/01/2026

Definición ( ): Grado

Sea $p(x) \in \mathbb{F}[x]$. Si $p(x) = a_0 + a_1 x + \dots + a_n x^n$ con $a_n \neq 0 \in \mathbb{F}$, entonces el grado $p(x)$ es

$$grad(p(x)) = n$$

♥ Sean $p(x), g(x) \in \mathbb{F}[x]$

$$grad(pg(x)) = grad(p(x)) + grad(g(x))$$

Demostración:

Dados $p(x), g(x) \in \mathbb{F}[x]$, tales que

$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ y $q(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$

Es decir, $grad(p(x)) = n$ y $grad(g(x)) = m$

♥ El grado de la suma es: $grad(p+g(x)) = max(grad(p(x)), grad(g(x)))$

Demostración:

Por def. de suma, sea $n = grad(p(x))$ y $m = grad(g(x))$ tal que $n \leq m$,

$$p+g(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_k x^k$$

y k es el mayor de los exponentes, así, $k = m$ y m es el máximo entre n y m.

♥ $\mathbb{F}[x]$ es dominio integral

Demostración:

$\mathbb{F}[x]$ no es dominio integral, pues un polinomio únicamente es 0 si todos sus coeficientes son 0, pero esto es un caso particular.

Algoritmo de división

Sea $p(x), g(x) \in \mathbb{F}[x]$ y $g(x) \neq 0$, entonces

$$p(x) = q(x) g(x) + r(x)$$

con $q(x), r(x) \in \mathbb{F}[x]$ y $grad(r(x)) < grad(g(x))$ ∨ $r(x) = 0$

Demostración:

- Si $p(x) = 0$ o $grad(p(x)) < grad(g(x))$

$$p(x) = 0\, g(x) + p(x)$$

- Si $grad(p(x)) \geq grad(g(x))$

Sean $m \geq n$ tq $p(x) = a_0 + a_1 x + \dots + a_m x^m$ y $g(x) = b_0 + b_1 x + \dots + b_n x^n$

Sea $m-n \geq 0$, tenemos que existe

$$\frac{a_m}{b_n} x^{m-n} g(x) = \frac{a_m}{b_n} x^{m-n}(b_0 + b_1 x + \ldots + b_n x^n)$$
$$= \frac{a_m}{b_n} b_0 x^{m-n} + \ldots + a_m x^m$$

Dado que $a \neq 0$, entonces $\operatorname{grad}\left(\frac{a_m}{b_n} x^{m-n} g(x)\right) = m$.

Sea $h(x) \in \mathbb{F}[x]$ tal que

$$p(x) - \frac{a_n}{b_n} x^{m-n} g(x) = h(x)$$

donde

$$\operatorname{grad}(h(x)) < \operatorname{grad}(p(x))$$

Y tenemos 2 casos:

a) $\operatorname{grad}(h(x)) < \operatorname{grad}(g(x))$:

$$p(x) = \left(q_1(x) + \frac{a_m}{b_n} x^{m-n}\right) g(x) + r_1(x)$$
$$q(x) = q_1(x) + \frac{a_m}{b_n} x^{m-n}$$

con $\operatorname{grad}(r_1(x)) < \operatorname{grad}(g(x))$ o $r_1(x) = 0$

b) $\operatorname{grad}(h(x)) \geq \operatorname{grad}(g(x))$:

$$h(x) = q_1(x) g(x) + r_1(x)$$

donde:

$$\operatorname{grad}(r_1(x)) < \operatorname{grad}(g(x)) \quad \vee \quad r_1(x) = 0$$

Teorema - Sea $I \neq \langle 0 \rangle$ ideal de $\mathbb{F}[x]$, entonces $I = \{f(x) g(x) : f(x) \in \mathbb{F}[x]\}$ donde $g(x)$ es fijo $g(x) \in \mathbb{F}[x]$, I consiste en todos los múltiplos de $g(x)$.

Demostración:

Sea $I \neq \langle 0 \rangle$ ideal de $\mathbb{F}[x]$, sabemos que $g(x) \in I$, con $g(x) \neq 0$ tal que $g(x)$ tiene el menor grado en I si $t(x) \in I$, entonces

$$\operatorname{grad}(t(x)) \geq \operatorname{grad}(g(x)) \quad (1)$$

Sea $t(x) \in I$

$$t(x) = q(x) g(x) + r(x)$$

donde $\operatorname{grad}(r(x)) < \operatorname{grad}(g(x))$ o $r(x) = 0$.

Y dado que I es ideal, $q(x) g(x) \in I$ y

$$t(x) - q(x) g(x) \in I$$

Por lo tanto,

$$r(x) \in I$$

Si $\operatorname{grad}(r(x)) < \operatorname{grad}(g(x))$, existe una contradicción, por lo tanto,

$$r(x) = 0$$

Así,

$$I = \{q(x) g(x) : q(x) \in \mathbb{F}[x]\}$$

Definición ( ): Dominio Integral Principal

Un dominio integral R se dice principal si todos sus ideales se escriben de la forma

$$I = \{x \cdot a : x \in R\} \qquad a \in I$$

En $\mathbb{F}[x]$: $I = \{f(x)g(x) : f(x) \in \mathbb{F}[x]\} = \langle g(x) \rangle$???

Definición ( ): Polinomio mónico

Sea $p(x) \in \mathbb{F}[x]$, $p(x)$ es mónico si el coeficiente de su mayor exponente es 1.

$$p(x) = a_0 + a_1 x + a_1 x^2 + \ldots + x^n$$

Definición ( ): Divisor

Sean $f(x), g(x) \in \mathbb{F}[x]$ con $g(x) \neq 0$, $g(x)$ divide a $f(x)$ y se escribe $g(x) \mid f(x)$ si $f(x) = a(x)g(x)$, donde $a(x) \in \mathbb{F}[x]$ y $f(x) \in \langle g(x) \rangle$

♥ Si $g(x) \mid f(x)$ y $f(x) \neq 0$, entonces $\langle f(x) \rangle \subseteq \langle g(x) \rangle$

Demostración:

Sea $p(x) \in \langle f(x) \rangle$ P.D: $p(x) \in \langle g(x) \rangle$

$$p(x) = h(x)f(x)$$

por hipótesis, existe $a(x) \in \mathbb{F}[x]$ tal que

$$f(x) = a(x)g(x)$$
$$p(x) = h(x)a(x)g(x)$$

Donde $h(x)a(x) \in \mathbb{F}[x]$. Así,

$$p(x) \in \langle g(x) \rangle$$
$$\langle f(x) \rangle \subseteq \langle g(x) \rangle \blacksquare$$

Definición ( ): Máximo común divisor

Sean $f(x), g(x) \in \mathbb{F}[x]$ (no ambos 0), existe un polinomio $d(x) \in \mathbb{F}[x]$, $d(x)$ es mónico tal que

a) $d(x) \mid f(x)$ y $d(x) \mid g(x)$

b) Si $d'(x) \mid f(x) \wedge d'(x) \mid g(x)$, entonces $d'(x) \mid d(x)$

16/01/2026

22/01/2026

Teorema .- Si $f(x) \in \mathbb{F}[x]$, entonces $f(x)$ es irreducible o $f(x)$ es el producto de polinomios irreducibles

$$f(x) = a\, p_1^{m_1}(x) p_2^{m_2}(x) \cdots p_j^{m_j}(x)$$

donde $p_k(x)$ es $p_k(x)$ es polinomio irreducible y mónico, m_k son enteros positivos con factorización única.

Demostración:

Demostración por inducción sobre el grado de $f(x)$

- Base de inducción: $n = 1$.

$$\text{grad}(f(x)) = 1$$

$$f(x) = a + bx \; ; \; b \neq 0.$$

Por def. de irreducible, entonces $f(x) = a + bx$ es irreducible.

- Sea $f(x)$ un polinomio con $\text{grad}(f(x)) = k$. Para todo $g(x) \in \mathbb{F}[x]$ se cumple el teorema con $\text{grad}(g(x)) < k$.

Tenemos dos casos:

a) Si $f(x)$ es irreducible, entonces se cumple el teorema

b) Si $f(x)$ no es irreducible, entonces existen $h(x), g(x) \in \mathbb{F}[x]$ tales que

$$f(x) = h(x)\, g(x)$$

donde $0 < \text{grad}(h(x)) < k$ y $0 < \text{grad}(g(x)) < k$

Para $h(x)$ y $g(x)$ se cumple que son irreducibles o producto de irreducibles. Así,

$f(x)$ es producto de polinomios irreducibles

Mostremos que la factorización es única.

Sea $f(x) = a p_1^{m_1}(x) \cdots p_s^{m_s}(x)$ y $f(t) = b q_1^{r_1}(x) \cdots q_s^{r_s}(x)$

$$p_i(x) \mid f(x)$$

$$p_i(x) \mid b\, q_1^{r_1}(x) \cdots q_s^{r_s}(x)$$

entonces existe $q_k(x)$ tal que

$$p_i(x) \mid q_k(x)$$

pues $p_k(x)$ y $q_k(x)$ son irreducibles y mónicos. Así,

$$p_i(x) = q_k(x)$$

Polinomios sobre $\mathbb{Q}$

Definición ( ): Polinomio Primitivo

Un polinomio de la forma $f(x)=a_0+a_1x+\dots+a_nx^n$ se dice polinomio primitivo si el máximo común divisor de $a_0, a_1, \dots, a_n$ es 1.

Lema :- Si $f(x)$, $g(x)$ son primitivos, entonces $g(x)f(x)$ es primitivo.

Demostración:

$f(x)=a_0+a_1x+\dots+a_nx^n$ y $g(x)=b_0+b_1x+\dots+b_mx^m$

Tenemos que

$$f(x)g(x)=c_0+c_1x+\dots+c_{m+n}x^{m+n}$$

donde

$$c_j=a_0b_j+a_1b_{j-1}+\dots+a_jb_0$$

Supongamos que $f(x)g(x)$ no es primitivo.

Entonces, a $c_0, c_1, \dots, c_{m+n}$ les divide p primo, es decir,

$$p \mid c_j \;;\; p \mid a_0b_j+\dots+a_jb_0$$

Dado que $f(x)$ es primitivo, tomamos a_k, el cuál es el primer coeficiente de $f(x)$ tal que $p \nmid a_k$ (1)

Igualmente, tomamos b_s, el primer coeficiente de $g(x)$ tal que

$$p \nmid b_s \quad (2)$$

Sea el coeficiente de x^{k+s}

$$c_{k+s}=(a_0b_{k+s}+a_1b_{k+s-1}+\dots+a_{k-1}b_{s+1})+a_kb_s+(a_{k+1}b_{s-1}+\dots+a_{k+s}b_0)$$

Sabemos que, por la elección de a_k:

$$p \mid a_0, \dots, p \mid a_{k-1} \Rightarrow p \mid a_0b_{k+s}+\dots+a_{k-1}b_{s+1}$$

Por otro lado, por la elección de b_s:

$$p \mid b_0, \dots, p \mid b_{s-1} \Rightarrow p \mid a_{k+1}b_{s-1}+\dots+a_{k+s}b_0$$

Pero, por hipótesis,

$$p \mid c_{k+s}$$

Entonces

$$p \mid a_kb_s \Rightarrow p \mid a_k \vee p \mid b_s$$

Lo cuál es una contradicción de (1) y (2).

Por lo tanto, $f(x)g(x)$ debe ser primitivo ■

Definición ( ): Contenido de un polinomio

Sea $f(x)=a_0+a_1x+\dots+a_nx^n$ con $a_i \in \mathbb{Z}$. $MCD(a_1, \dots, a_n)$ es el contenido de $f(x)$.

Así, si el contenido de $f(x)$ es p, entonces.

$$f(x)=pg(x) \text{ con } g(x) \text{ primitivo}$$

Lema (Lema de Gauss).- Si $f(x)$ es primitivo, se puede factorar como producto de dos polinomios con coeficientes racionales, se puede factorar como producto de polinomios con coeficientes enteros.

Demostración:

Sea $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $f(x)$ es primitivo, es decir, $MCD(a_0, \dots, a_n) = 1$.

Sean $u(x) \in \mathbb{Q}[x]$ y $v(x) \in \mathbb{Q}[x]$ P.D: $f(x) = u(x)\,v(x)$ (1)

Sacamos factor común en (1), entonces

$$f(x) = \frac{a}{b}\, g(x)\, h(x)$$

$$b f(x) = a\, g(x)\, h(x)$$

Y dado que $f(x)$ es primitivo, entonces $g(x)h(x)$ es primitivo. Así,

$$b = a \Rightarrow \left(\frac{a}{b}\right) = 1$$

Criterio Eisenstein: Dado $f(x) = a_0 + a_1 x + \dots + a_n x^n$ un polinomio con coeficientes enteros tal que para un primo p,

$$p \nmid a_n,\ p \mid a_0,\ p \mid a_2, \dots, p \mid a_{n-1}$$

y $p^2 \nmid a_0$.

Entonces, $f(x)$ es irreducible en racionales.

Demostración:

Supongamos que $f(x)$ es reducible en $\mathbb{Q}[x]$ y dado que $f(x)$ es primitivo, por el lema de Gauss:

$$f(x) = (b_0 + b_1 x + \dots + b_r x^r)(c_0 + c_1 x + \dots + c_s x^s)$$

donde b_i y c_j son enteros y $r, s > 0$.

Tenemos que

$$a_0 = b_0 c_0$$

Así, $p \mid a_0$ y $p \mid b_0 c_0$.

Pero como $p^2 \nmid a_0$, entonces

$p \mid b_0$ o $p \mid c_0$ de manera exclusiva, es decir, no a ambos.

- Si $p \mid b_0$ y $p \nmid c_0$: (*)

No todos los elementos $b_0, \dots, b_r$ son divisibles por p, pues $p \nmid a_n$.

Tomemos b_k como el primer coeficiente b tal que

(1) $p \nmid b_k$ con $k < r$

Así,

$$p \mid b_{k-1} \dots p \mid b_0$$

Entonces,

$$a_k = b_0 c_k + b_1 c_{k-1} + \dots + b_{k-1} c_1 + b_k c_0$$

Y dado que $p \mid a_k$, entonces, $p \mid b_k c_0$ y por (1), $p \mid c_0$, lo cual contradice a (*).

Así, $f(x)$ es irreducible ■

23/01/2026

Principios de conteo

Dado G un grupo, H subgrupo de G, sea $a \in G$.

$$Ha = \{ha : h \in H\}$$

Si tomamos H y K subgrupos de G,

$$HK = \{hk : h \in H \wedge k \in K\}$$

- En S_3: H y K subgrupos de S_3 tales que:
  - $H = \{e, (1\ 2)\}$
  - $K = \{e, (2\ 3)\}$
  - $HK = \{e, (1\ 2), (2\ 3), (1\ 2\ 3)\}$
  - $KH = \{e, (1\ 2), (2\ 3), (1\ 3\ 2)\}$

Lema .- Sean H y K subgrupos de G. HK es subgrupo de G si y solo si $HK = KH$.

Demostración:

⇒) Si HK es subgrupo de G P.D: $HK = KH$

Sea $h \in H$ y $k \in K$ tales que $kh \in KH$ P.D: $kh \in HK$

Dado que H y K son subgrupos, entonces

$$h^{-1} \in H \text{ y } k^{-1} \in K$$

Entonces,

$$h^{-1}k^{-1} \in HK$$

Pero HK es subgrupo, por lo tanto,

$$(h^{-1}k^{-1})^{-1} \in HK$$

$$kh \in HK$$

Sea $hk \in HK$ P.D: $hk \in KH$

idem

⇐) Si $HK = KH$ P.D: HK es subgrupo de G

Sean $x \in HK$ y $y \in HK$ P.D: $xy \in HK$

Sean $x = hk$ y $y = h'k'$, entonces

$$xy = hkh'k'$$

$$= hh_1k_1k' \quad \text{donde } kh' = h_1k_1$$

($h \in H$, $h_1 \in H$, $k_1 \in K$, $k' \in K$)

Así, $xy \in HK$

Sea $x \in HK$ P.D: $x^{-1} \in HK$

$$x^{-1} = (hk)^{-1}$$

$$= k^{-1}h^{-1} \in KH$$

y $k^{-1}h^{-1} \in KH$

♥ Normalizador o centrado en a

$$N(a) = \{x \in G : xa = ax\}$$

♥ Centro de G

$$Z(G) = \{x : xg = gx \quad \forall g \in G\}$$

Definición ( ): Conjugado de a

Sean $a, b \in G$, entonces b se dice conjugado de a si existe $c \in G$ tal que

$$b = c^{-1}ac$$

$a \sim b$ si a y b están conjugados

Lema - La relación conjugar es relación de equivalencia

a) $a \sim a$

b) $a \sim b$ entonces $b \sim a$

c) $a \sim b$ y $b \sim c$ entonces $a \sim c$

Demostración:

a) $a = e^{-1}ae$

b) Si $a \sim b$, entonces

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

c) Si $a \sim b$, entonces

$$b = x^{-1}ax$$

Si $b \sim c$, entonces

$$c = y^{-1}by$$

Entonces:

$$c = y^{-1}x^{-1}axy$$
$$= (xy)^{-1}a\,xy$$

Así, $a \sim c$.

♥ Clase de equivalencia de a bajo la relación de conjugado

$$C(a) = \{x : a \sim x\}$$

- $|G| = \sum |C(a)|$ (sobre C_a)
- $S_3 = \{e, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
- $C(e) = \{e\}$
- $C(1\ 2) = \{(1\ 2), (1\ 3)^{-1}(1\ 2)(1\ 3), (2\ 3)^{-1}(1\ 2)(2\ 3), (1\ 2\ 3)^{-1}(1\ 2)(1\ 2\ 3), (1\ 3\ 2)^{-1}(1\ 2)(1\ 3\ 2)\}$
  $= \{(1\ 2), (2\ 3), (1\ 3)\}$
- $C(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2)\}$

Teorema - Si G es finito,

$$C_a = \frac{|G|}{|N(a)|}$$

el número de conjugados de a en G es índice del normalizador de a en G.

Demostración:

- Sean $x, y \in G$ tales que pertenecen a la misma clase lateral derecha.
  Dado $n \in N(a)$ (♥) tal que
  $$y = nx$$
  Entonces,
  $$y^{-1}ay = x^{-1}n^{-1}anx$$
  Por (♥), $an = na$, entonces
  $$y^{-1}ay = x^{-1}n^{-1}nax$$
  $$= x^{-1}ax$$
- Sean x, y tales que pertenecen a distintas clases laterales de $N(a)$ (♦)
  P.D: $x^{-1}ax \neq y^{-1}ay$
  Supongamos que
  $$x^{-1}ax = y^{-1}ay$$
  $$yx^{-1}ax = ay$$
  $$yx^{-1}a = ayx^{-1}$$
  Así, $yx^{-1} \in N(a)$, por lo tanto, $y \sim x$. Pero eso contradice a (♦) ■

- $|G| = \sum \frac{|G|}{|N(a)|}$

♥ $Z(G) = \{x : xy = yx \quad \forall y \in G\}$
Si $a \in Z(G)$, entonces
$$xa = ax$$
$$a = x^{-1}ax$$
Así, a solo tiene un solo conjugado

28/01/2026

Lema - $a \in Z(G)$ si y solo si $N(a) = G$

Demostración:

⇒) Si $a \in Z(G)$ P.D: $N(a) \subseteq G$ ∧ $G \subseteq N(a)$
Sea $x \in G$,
$$xa = ax$$
Se cumple que $a \in Z(G)$, por lo tanto
$$N(a) = G$$

⇐) Si $N(a) = G$ P.D: $a \in Z(G)$
Tenemos que $xa = ax$ para todo $x \in G$ ■

Teorema - Si $|G| = p^n$, donde p es primo, entonces $Z(G) \neq \langle e \rangle$

Demostración:

Tenemos que $|G| = \sum \frac{|G|}{|N(a)|}$.

Sea $a \in G$, entonces $N(a)$ subgrupo de G con $|N(a)| \mid |G|$. Así,

$$|N(a)| = p^{\alpha_a}$$

Si $a \in Z(G)$ y $N(a) = G$

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N(a)|}$$

$$p^n = |Z(G)| + \sum_{\substack{a \notin Z(G) \\ \alpha_a < n}} \frac{p^n}{p^{\alpha_a}}$$

$$p \mid \frac{p^n}{p^{\alpha_a}}$$

$$p \mid p^n$$

$$p \mid -\sum_{\alpha_a < n} \frac{p^n}{p^{\alpha_a}} + p^n$$

$p \mid |Z(G)|$ Así, $|Z(G)| > 1$ y entonces, $Z(G) \neq \langle e \rangle$ ■

Corolario - Si $|G| = p^2$ con p primo, entonces G es abeliano.

Demostración: P.D: $Z(G) = G$

Por el teorema anterior, $Z(G) \neq \langle e \rangle$. Así, por Lagrange $Z(G)$ es de orden p o p^2.

Si $|Z(G)| = p$, entonces $a \in G$ y $a \notin Z(G)$; $N(a)$ subgrupo de G.

$$Z(G) \subseteq N(a)$$

y $a \in N(a)$, $|N(a)| = p^2$. Entonces

$$|N(a)| = |G|$$

y así,

$$a \in Z(G)$$

Por lo tanto $|Z(G)| = p^2$. Así, $Z(G) = G$, por lo que G es abeliano ■

Definición ( ): Subgrupo p-Sylow

Si G un grupo, un subgrupo de G de orden p^α, pero $p^{\alpha+1} \nmid |G|$, entonces el subgrupo se dice p-Sylow.

→ Primera Parte

Teorema (Teorema de Sylow) - Si p es primo y $p^\alpha \mid |G|$, entonces G tiene subgrupo de orden p^α.

Demostración:

Demostración por inducción sobre el orden de G.

- Base de inducción: $|G| = 2$

  $2 \mid |G|$ y $2^2 \nmid |G|$

  Así, el teorema se cumple

- Hipótesis de inducción: Suponemos que el teorema se cumple para todo grupo de orden menor que $|G|$.

  Supongamos que p es primo

  $p^n \mid |G|$ y $p^{n+1} \nmid |G|$

Sea H subgrupo de G s. $p^m \mid |H|$, donde $H \neq G$. H tiene un subgrupo T de orden p^m.

Tenemos que T es subgrupo de G.

Si $p^m \nmid |H|$ con $H \neq G$, entonces

$|H| \mid |G|$

P.D: $|G| = \Sigma \frac{|G|}{|N(a)|}$

Sea $a \in G$

$N(a) = \{x : xa = ax\}$

Tenemos que $a \notin Z(G)$ si y solo si $N(a) \neq G$

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N(a)|}$$

y así, $p \mid |G|$ y $p^m \nmid |N(a)|$

$$p \mid \frac{|G|}{|N(a)|}$$

$$p \mid \sum_{a \in Z(G)} \frac{|G|}{|N(a)|} \text{ y } p \mid |G|$$

$$p \mid |Z(G)|$$

Por Cauchy, existe $b \in Z(G)$ tal que b es de orden p.

$B = \langle b \rangle$ con orden primo

Así, B es normal

$$\bar{G} = G/B$$

$$|\bar{G}| = \frac{|G|}{|B|}$$

$p^{m-1} \mid |\bar{G}|$ y $p^m \nmid |\bar{G}|$ y $|\bar{G}|$ es menor que $|G|$

Así, del teorema tenemos que $\bar{G}$ tiene un subgrupo $\bar{P}$ de orden p^{m-1} tal que

$$P = \{x \in G : xB \in \bar{P}\}$$

$$\bar{P} \simeq P/B$$

$$p^{m-1} = |P/B| = \frac{|P|}{p}$$

$$p^m = |P| \blacksquare$$

Teorema (2ª Parte del Teorema de Sylow):- Todos los p-Sylow subgrupos de G son conjugados entre sí.

P_1, P_2 p-Sylow, existe $g \in G$ tal que

$$P_1 = g^{-1} P_2 g$$

Teorema (3ª Parte del Teorema de Sylow):- Si n_p es el número de p-Sylow subgrupos de G, entonces n_p satisface que:

1) n_p es divisor de $|G|$
2) $n_p \equiv 1 \mod p$.

Ejercicio: Probar que un G grupo de orden 99 tiene subgrupos no triviales normales.

$|G| = 99 = 9 \cdot 11 = 3^2 \cdot 11$

Tenemos H 11-Sylow y H_2 3-Sylow

Sea n_{11} el número de 11 el número de 11-Sylow subgrupos de G.

n_{11}: 11 19 3 33 99 1

$11 \not\equiv 1 \mod 11$ $9 \not\equiv 1 \mod 11$ $3 \not\equiv 1 \mod 11$ $33 \not\equiv 1 \mod 11$ $99 \not\equiv 1 \mod 11$

Así,

$$n_{11} = 1$$

Entonces,

$$H = g^{-1} H g$$ ■