TESIS UNA - PUNO

Universidad Nacional del Altiplano

UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO

FACULTAD DE INGENIERIA CIVIL Y ARQUITECTURA

ESCUELA PROFESIONAL DE CIENCIAS FÍSICO MATEMÁTICAS

UNA CLASIFICACIÓN COMPLETA DE LOS CAMPOS FINITOS

TESIS

PRESENTADO POR:

ELOY NINA AROHUATA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

LICENCIADO EN CIENCIAS FÍSICO MATEMÁTICAS

PUNO – PERÚ

2017

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO
FACULTAD DE INGENIERIA CIVIL Y ARQUITECTURA
ESCUELA PROFESIONAL DE CIENCIAS FÍSICO MATEMÁTICAS

"UNA CLASIFICACIÓN COMPLETA DE LOS CAMPOS FINITOS"

TESIS PRESENTADO POR EL BACHILLER

ELOY NINA AROHUATA

UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO - Facultad de Ingeniería Civil y Arquitectura - DIRECCIÓN DE UNIDAD DE INVESTIGACIÓN

PARA OPTAR EL TITULO PROFESIONAL DE:

LICENCIADO EN CIENCIAS FÍSICO MATEMÁTICAS

APROBADO POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE: Lic. Mario Félix Quispe Atamari

PRIMER MIEMBRO: Lic. Verónica Alicia Ibañez Ulloa

SEGUNDO MIEMBRO: M.Sc. Martin Condori Concha

DIRECTOR: Mg. Julio César Villalta Pacori

ASESOR: M.Sc. Juan Carlos Benavides Huanca

Tema : Una clasificación completa de los campos finitos
Área : Matemática.
Línea de Investigación: Matemática Pura

Fecha de sustentación: 18 de enero del 2017

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

DEDICATORIA

A mi amada madre María aruata y ala memoria de mi padre Felipe nina, a quienes debo todo lo que soy y lo que seré.

A mis hermanas Melania y Aneida y como no a mi hermanito menor Aldo, quienes son la fuente de motivación e inspiración de mi existencia, mi lucha y gloria.

A mis alumnas y alumnos, quienes representan la energía que necesita el mundo para alcanzar su desarrollo y progreso.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

AGRADECIMIENTOS

Primero agradezco a Dios por darme fuerzas para seguir adelante, crecer cada dia más como persona y nunca desampararme.

Segundo, quiero agradecer de forma muy especial al director de esta tesis Mg. Julio César Villalta Pacori, por su esfuerzo y dedicación a la hora de sacar adelante esta tesis. Sin el conocimiento y el tiempo que amablemente ha dedicado a orientarme y animarme, este trabajo difícilmente hubiera sido concluido satisfactoriamente.

Agradezco también a mi asesor de tesis MSc Juan Carlos Benavides Huanca y alos miembros del jurado por la revisión de esta tesis y por las correcciones pertinentes.

A todos mis amigos, familiares y compañeros de pre – grado, quienes sin esperar nada a cambio compartieron conocimientos, alegrías y tristezas.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

ÍNDICE GENERAL

Contenido

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

RESUMEN

La presente investigación titulada "Una Clasificación Completa de los Campos Finitos" tiene como principal objetivo determinar la estructura de todos los campos finitos. Se demuestra en primer lugar que todo campo finito tiene p^n elementos, donde p es la característica del campo y n cierto número natural, más aún todo elemento de dicho campo es una raíz del polinomio $x^{p^n} - x$. Después se demuestra que para cada natural n y cada primo p existe un único campo (salvo isomorfismos) con p^n elementos. Equivalentemente, dos campos cualesquiera con p^n elementos son isomorfos. A este campo se le llama el campo de Galois de orden p^n y se le representa por $GF(p^n)$. Finalmente se demuestra que el grupo de elementos distintos de cero del campo de Galois $GF(p^n)$ es cíclico; es decir, generado por un elemento que se denomina elemento primitivo. Para obtener estos resultados será necesario introducir ciertos conceptos de grupos, anillos, campos y polinomios, así como algunas propiedades que serán utilizadas en resultados posteriores. Entre estas propiedades se encuentra que todo campo finito, tiene característica un número primo. Esta propiedad pese a su aparente sencillez resulta clave en la teoría de campos finitos.

También será necesario introducir la teoría de extensión de campos y otros conceptos relacionados, como el grado de la extensión o campo intermedio. Se verá que toda extensión de campos $[L:K]$ puede ser vista como un espacio vectorial sobre K. Tras ello se continuará con la introducción de extensiones algebraicas y simples, así como campos factorizantes.

Una vez realizada esta introducción a las extensiones de campos y campos factorizantes será el momento de profundizar en la teoría de campos finitos.

Palabras Clave: Campos, Clasificación, Campos finitos.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

ABSTRACT

The present titled investigation ``A Complete Clasificación of the Finite Fields'' it has like main objective to determine the structure of all the finite fields. It is proven that in the first place every finite field has p^n elements, where p it is the characteristic of the field and

n certain natural number, furthermore every element of the aforementioned field is a root of the polynomial $x^{p^n} - x$. After it is demonstrated than for each native n and each cousin p there is an only field (except isomorphisms) with p^n elements. Equivalently, two fields anyone with p^n elements are isomorphic. This field is called the Galois field of order p^n and it represents to him for $GF(p^n)$. Finally it is demonstrated that the group of different elements of zero of the Galois field $GF(p^n)$ it is cyclic; that is, generated for an element that primitive element names itself. In order to obtain these results it will be necessary to introduce certain concepts of groups, rings, fields and polynomials, as well as some properties that will be used in later results. Between these properties he meets that every finite field, a prime number has characteristic. This property in spite of its apparent simplicity proves to be key in the theory of finite fields.

It will also be necessary to introduce the spanning theory of fields and other concepts related, like the degree of the extension or intermediate field. It will be seen that every extension of fields $[L:K]$ puede ser vista como un espacio vectorial sobre K. Behind it he will go on with the introduction of algebraic and simple extensions, as well as fields factorizantes.

A realized time this introduction to the extensions of fields and fields factorizantes will be the moment of delving deeply into the theory of finite fields.

Keywords:. Fields, Clasificación, Finite Fields.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

INTRODUCCIÓN

La disciplina matemática del álgebra incluye la teoría de los campos finitos, cuyo desarrollo se remonta a principios del siglo *XIX* cuando Carl Friedrich Gauss (1777-1855) y Evariste Galois (1811-1832) trabajaron en la teoría general de los campos finitos.

En su trabajo Evariste Galois resolviendo congruencias módulo un número primo p, quizá sin percibirlo de esa manera, introdujo lo que actualmente se conoce como el campo de enteros modulo p, uno de los campos finitos con p elementos mas importantes, ya que a partir de éste se construye otros campos arbitrarios con p^n elementos para cualquier entero $n>1$. El estudio de los campos finitos o campos de Galois no tuvo grandes avances por mucho tiempo, pero en las últimas décadas debido a las aplicaciones que tienen en diferentes áreas de la matemática así como en otras de gran relevancia en nuestros días como son las comunicaciones digitales y seguridad informática, ha habido un gran desarrollo y estudio sobre diversos aspectos de los campos finitos. Presentar en forma detallada dónde y cómo se usan actualmente los campos finitos sería interesante, pero también una gran tarea.

La presente investigación está destinado a obtener una clasificación completa de todos los campos finitos. Un conocimiento básico de álgebra abstracta (grupos, anillos, campos, polinomios, extensión de campos y campos factorizantes) y álgebra lineal será deseable para alcanzar el objetivo de este trabajo de investigación.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

CAPITULO I

1. PLANTEAMIENTO DEL PROPBLEMA, ANTECEDENTES Y OBJETIVOS DE LA INVESTIGACIÓN

1.1. Planteamiento del problema.

En la versión general en la que actualmente se presenta la teoría de Galois, la noción de campo ocupa un lugar central, en donde uno de los intereses es determinar la naturaleza de los campos que tienen solo un número finito de elementos. Tales campos se llaman *campos finitos*. Es claro que existen campos finitos, por ejemplo $\mathbb{Z}_p$, donde p es un número primo, es un campo finito.

Para un campo finito K, su característica es un número primo p y este campo K tiene un subcampo minimal, conocido como subcampo primo, que resulta ser:

$$\{0_K, 1_K, 2(1_K), \ldots, (p-1)(1_K)\}$$

Este subcampo primo es isomorfo a $\mathbb{Z}_p$, el campo de los enteros modulo p.

Usando la teoría desarrollada para la teoría de campos en general que devienen en la teoría de extensión de campos, la investigación propone obtener una descripción completa de todo los campos finitos y las propiedades importantes que poseen. Por lo tanto el problema se reduce a:

¿Es posible dar una clasificación completa de los campos finitos?

1.1.1. Justificación del problema.

Los campos finitos o campos de Galois son muy importantes en diversas áreas de las matemáticas, como la teoría de números o la geometría algebraica, y tienen numerosas aplicaciones en diferentes campos de indudable interés para el mundo industrial y financiero, como son la criptografía, la transmisión de datos, los códigos correctores de errores, el procesamiento digital de señales y la grabación de discos compactos entre otros.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Dada la diversidad de aplicaciones de los campos finitos, con la investigación obtenida se pretende contribuir con el material bibliográfico de álgebra sobre la descripción completa de los campos finitos. Así, el informe final de trabajo de investigación servirá como material de consulta a quienes se interesen y se planteen problemas con objeto de aplicación de los campos finitos o campos de Galois, ya sea por motivos de adquisición de mayor conocimiento o aplicación a otras áreas del conocimiento.

1.2. Antecedentes.

HERNÁNDEZ ABASCAL, José Gustavo (2010) *Extensiones de Galois.*
En este trabajo se estudia una parte de la teoría de Galois muy importante e interesante, dada una ecuación particular en un campo en donde no tiene solución, se puede construir una extensión de ese campo en donde si tiene solución y esa extensión es nuevamente un campo, con todas las operaciones inducidas por el campo inicial.

VELAZCO J. Armando (2013) *Construcción de campos finitos mediante extensiones.* En este paper se propone la construcción de campos finitos a partir de un campo finito dado mediante extensiones algebraicas los cuales son extensiones que permiten hallar la raíz de un polinomio irreducible.

TAPIA RECILLAS, Horacio (2011) *Sobre algunas aplicaciones de los campos de Galois*. En este artículo se introduce el concepto de campo de Galois o campo finito, el cual se motiva a partir de un caso concreto y se da su construcción en forma general. Asimismo se menciona a grandes rasgos algunas áreas donde los campos finitos se ponen de manifiesto, sin proporcionar detalles sobre la misma área o aplicación.

Los antecedentes presentados orientan al trabajo de investigación en la clasificación completa de los campos finitos o campos de Galois.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

1.3. Objetivos.

1.3.1. Objetivo general.

- Determinar una clasificación completa de los campos finitos con el análisis de la teoría de campos.

1.3.2. Objetivos específicos.

- Analizar cuándo las raíces de un polinomio $f(x) \in K[x]$ son distintos sobre un campo factorizante L.

- Analizar una condición suficiente para que un grupo abeliano finito sea cíclico.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO
Universidad Nacional del Altiplano

CAPITULO II

2. MARCO TEORICO

2.1. Grupos

Definición 2.1.1. (semigrupo).

Sea G un conjunto no vacío y $*$ una ley de composición interna en G. Si $*$ es asociativa entonces se dice que $(G,*)$ es **semigrupo** y si además $*$ tiene neutro entonces $(G,*)$ es **semigrupo con neutro**.

Definición 2.1.2. (grupo).

Un grupo es un par $(G,*)$, donde G es un conjunto y $*$ es una ley de composición interna en G que cumple las condiciones siguientes.

G_1. Asociatividad.

$$\forall a,b,c \in G \Rightarrow (a*b)*c = a*(b*c)$$

G_2. Existencia del elemento neutro o identidad.

$$\exists\, e \in G \,/ \forall a \in G \Rightarrow a*e = e*a = a$$

G_3. Existencia de inversos.

$$\forall a \in G, \exists\, a' \in G \,/\, a*a' = a'*a = e$$

Definición 2.1.3. (grupo abeliano). Un grupo $(G,*)$ es llamado un grupo abeliano si satisface la siguiente propiedad de *conmutatividad.*

$$\forall a,b \in G \Rightarrow a*b = b*a$$

Notación: En general, a $(G,*)$, la denotaremos simplemente G, excepto cuando se deba especificar para evitar confusiones. Para denotar la operación binaria * se usará la notación convencional de la adición y multiplicación usuales que es llamado

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

operación adición o multiplicación. Así, en lugar de la notación $a * b$ se usará ya sea $a + b$ que se lee suma de a y b o *ab* que se lee producto de a y b.

Definición 2.1.4 (grupo finito). Se dice que un grupo G es finito, si consta de un número finito de elementos. El número de elementos de G se llama orden de G y se denota por $|G|$.

2.1.1. Subgrupos

Definición 2.1.5 (subgrupo). Un subconjunto no vacío H de un grupo G, es un subgrupo de G, si H es un grupo bajo la operación de G. En tal caso se escribe $H \leq G$.

Teorema 2.1.1. *Un subconjunto no vacío H de un grupo G es un subgrupo de G si y solo si $ab^{-1} \in H$ para todo $a, b \in H$.*

Demostración.

($\Rightarrow$) Por hipótesis H es un subgrupo de G. Sean $a, b \in H$, entonces debemos demostrar que $ab^{-1} \in H$.

En efecto, como H es un subgrupo de G, por G_3 para $b \in H$ existe $b^{-1} \in H$.

Así para $a \in H$ y $b^{-1} \in H$ deducimos que $ab^{-1} \in H$, ya que H es cerrado bajo la operación binaria de G.

($\Leftarrow$) En este sentido la demostración lo haremos utilizando la definición de subgrupo. Es decir para que H sea un subgrupo de G debe satisfacer los axiomas del grupo siguientes:

- La asociatividad de la operación en H se verifica por ser $H \subset G$.
- Como $H \neq \varnothing$, existe $a \in H$. Por hipótesis, para $a = a$, $b = a$ tenemos que $ab^{-1} = aa^{-1} = e \in H$
- Sea $b \in H$, para $a = e$, $b = b$ por hipótesis tenemos que $ab^{-1} = eb^{-1} = b^{-1} \in H$.

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

- Sean $a,b \in H$, para $a = a$, $b = b^{-1}$ por hipótesis tenemos que $ab = a(b^{-1})^{-1} \in H$, con esto H es cerrado bajo la operación binaria de G.

Por lo tanto, según la definición de subgrupo concluimos que H es un subgrupo de G ■

Observaciones.

1. Según el teorema anterior para que un subconjunto H de un grupo G sea subgrupo debemos demostrar
   - $H \neq \varnothing$
   - $ab^{-1} \in H$, $\forall a,b \in H$.
2. Si G es un grupo, entonces G y $\{e\}$ son, claramente subgrupos de G, llamados los subgrupos triviales de G; a otros subgrupos se les llama no triviales o propios.

2.1.2. Grupos cíclicos

Una clase particularmente simple e importante de grupos está constituida por los grupos que poseen un sistema generador formado por un único elemento, es decir los grupos cíclicos.

Definición 2.1.6. Sea G un grupo y sea a un elemento cualquiera de G. El conjunto

$\langle a \rangle = \{a^m \ / m \in \mathbb{Z}\}$

es un subgrupo del grupo G, llamado el *subgrupo cíclico* de G generado por el elemento a.

Definición 2.1.7 (grupo cíclico). Un grupo G es *cíclico* si está generado por uno de sus elementos, es decir existe $a \in G$ de modo que $G = \langle a \rangle$.

Teorema 2.1.2. *Todo grupo cíclico es abeliano.*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Demostración. Sea G un grupo ciclíco. Para que G sea abeliano debemos demostrar que $\forall g_1, g_2 \in G : g_1 g_2 = g_2 g_1$.

En efecto, sea a un generador de G, entonces $G = \langle a \rangle = \{a^n \ / \ n \in \mathbb{Z}\}$.

Si, g_1 y g_2 son elementos cualesquiera de G, entonces existen enteros r y s tales que $g_1 = a^r$, $g_2 = a^s$, de manera que:

$$\begin{aligned} g_1 g_2 = \ a^r a^s &= a^{r+s}, && \text{por propiedad de potenciación} \\ &= a^{s+r}, && \text{la suma de enteros es conmutativa} \\ &= a^s a^r, && \text{por propiedad de potenciación} \\ &= g_2 g_1, && \text{hipótesis} \end{aligned}$$

Por lo tanto, el grupo cíclico G es abeliano ■

Definición 2.1.8. Sea G un grupo finito y $a \in G$. El menor entero positivo m tal que $a^m = e$ es llamado el orden de a y se escribe $|\, a \,| = m$. Si no existe tal entero m, se dice que el orden de a es infinito y se escribe $|\, a \,| = \infty$ para denotar el orden de a.

2.1.3. Clases laterales y teorema de Lagrange

Definición 2.1.9. Sea H un subgrupo de un grupo G y $a, b \in G$. Diremos que a es *congruente derecha* con b módulo H, denotado $a \equiv_r b \bmod H$, si $ab^{-1} \in H$, y a es *congruente izquierda* con b módulo H, denotado $a \equiv_l b \bmod H$, si $a^{-1}b \in H$.

Teorema 2.1.3. *Sea H un subgrupo de un grupo G. Entonces*

1. *La congruencia derecha (izquierda) módulo H es una relación de equivalencia en G.*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2. *La clase de equivalencia de* $a \in G$, *bajo la congruencia derecha (izquierda) módulo* H *es el conjunto* $Ha = \{ha / h \in H\}$ $\left(aH = \{ah / h \in H\}\right)$.
3. $| Ha | = | H | = | aH |$, *para todo* $a \in G$.

Demostración. Demostraremos el enunciado para la congruencia derecha. Las demostraciones para la congruencia izquierda son análogas.

1. La congruencia derecha módulo H es una relación de equivalencia.

   Reflexividad: $a \equiv_r a \bmod H$ si $aa^{-1} = e \in H$.

   Simetría: $a \equiv_r b \bmod H$, entonces $b \equiv_r a \bmod H$.

   En efecto, $a \equiv_r b \bmod H$ implica que $ab^{-1} \in H$. Como $H \leq G$, $ab^{-1}{}^{-1} = ba^{-1} \in H$, de donde por definición $b \equiv_r a \bmod H$.

   Transitividad: $a \equiv_r b \bmod H$ y $b \equiv_r c \bmod H$, entonces $a \equiv_r c \bmod H$.

   En efecto,

   $$a \equiv_r b \bmod H \Rightarrow ab^{-1} \in H$$

   $$b \equiv_r c \bmod H \Rightarrow bc^{-1} \in H$$

   Como, $H \leq G \Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in H$, de donde por definición $a \equiv_r c \bmod H$.

   Por lo tanto, $\equiv_r$ es una relación de equivalencia en G.

2. La clase de equivalencia $\overline{a}$ o $[a]$ que contiene a $a \in G$ se obtiene como sigue:

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

$$\begin{aligned}[a] = \{x \in G \,/\, x \equiv_r a \bmod H\} &= \{x \in G \,/\, xa^{-1} \in H\} \\ &= \{x \in G \,/\, xa^{-1} = h,\ h \in H\} \\ &= \{x \in G \,/\, x = ha,\ h \in H\} \\ &= \{ha \,/\, h \in H\} = Ha\end{aligned}$$

Por lo tanto, $[a] = Ha = \{ha \,/\, h \in H\}$.

3. $|\, Ha \,| = |\, H \,|$, para ello definamos una función $\varphi : H \to Ha$ por $\varphi(h) = ha$, $h \in H$ y debemos demostrar que φ es biyectiva.

   En efecto,

   Para probar la *inyectividad*, vemos que si $\varphi(h_1) = \varphi(h_2)$; $h_1, h_2 \in H$, entonces $h_1 a = h_2 a$, por la propiedad cancelativa del grupo G, se deduce que $h_1 = h_2$.

   Ahora, para probar la *sobreyectividad*, notemos que por la definición de φ, podemos ver que $\varphi(h) = ha$ y así todo elemento de Ha es imagen de un elemento $h \in H$.

Luego, dado que φ es biyectiva, todos los conjuntos Ha tienen el mismo número de elementos, y por lo tanto H también. ■

Definición 2.1.10 (clases laterales**).** Sea H un subgrupo de un grupo G y $a \in G$. El conjunto Ha es llamado clase lateral derecho en G y aH es llamado clase lateral izquierdo de H en G.

Observación. En general no es el caso que una clase lateral derecha sea también una clase lateral izquierda.

Teorema 2.1.4 (teorema de Lagrange**).** *Si G es un grupo finito y H es un subgrupo de G, entonces el orden de H divide al orden de G, es decir* $|\, H \,| \,\big|\, |\, G \,|$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Demostración. Supongamos que G tiene n elementos y H m elementos. Consideremos la colección de las clases laterales derechas de H en G, Por el teorema 2.1.3, estas clases laterales son disjuntas, tienen el mismo número m de elementos como H y todo elemento de G está en alguna clase lateral derecha. Entonces, si hay r clases laterales derechas, debemos tener $n = rm$, de modo que m divide a n. ■

Corolario 2.1.1. *Si G es un grupo finito de orden un número primo p, entonces G es un grupo cíclico.*

Demostración. Sea $a \in G - \{e\}$. Entonces el subgrupo cíclico $H = \langle a \rangle$ de G generado por a tiene al menos dos elementos, a y e. Pero por el teorema de Lagrange, el orden $m > 1$ de $\langle a \rangle$ debe dividir al primo p, puesto que p es primo, entonces sus únicos divisores son 1 y p. Así debemos tener que $m = p$ y $\langle a \rangle = G$, de modo que G es cíclico. ■

Corolario 2.1.2. *Si G es un grupo finito y $a \in G$, entonces $|a|$ es un divisor de $|G|$.*

Demostración. Sabemos que $|a|$ es el orden del subgrupo cíclico $\langle a \rangle$ de G generado por el elemento a, luego por el teorema de Lagrange se tiene que $|a|$ divide a $|G|$. ■

Definición 2.1.11. El exponente $e = e(G)$ de un grupo G es el menor entero positivo $e = e(G)$ con la propiedad de que $a^e = 1$ para todo a en G.

Observación. El exponente siempre existe (en un grupo finito): es el MCM de los órdenes de los elementos de G.

Teorema 2.1.5. *Sea G un grupo abeliano finito con exponente e. Entonces existe un elemento a en G tal que $|a| = e$.*

Demostración. Ver [1]. ■

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Corolario 2.2.3. *Si* G *es un grupo abeliano finito tal que* $e(G) = |G|$, *entonces* G *es ciclíco.*

2.1.4. Subgrupos normales y grupos cocientes.

Definición 2.1.12 (subgrupo normal**).** Un subgrupo H de un grupo G es un *subgrupo normal* de G lo cual escribiremos $H \trianglelefteq G$, si $gH = Hg$, para todo $g \in G$. Es decir, un subgrupo normal de un grupo G es precisamente aquel en el cual las clases laterales izquierdas y derechas son las mismas.

Observación. Decir que $gH = Hg$ es lo mismo que

$$H = g^{-1}Hg = \{g^{-1}hg \,/\, h \in H\}$$

Proposición 2.1.1. *Si* H *es un subgrupo de un grupo* G *tal que* $g^{-1}Hg \subseteq H$ *para todo* $g \in G$, *entonces* $g^{-1}Hg = H, \forall g \in G$. *Es decir* H *es un subgrupo normal de* G.

Demostración. Para $g \in G$, existe $g^{-1} \in G$, de modo que

$$gHg^{-1} = (g^{-1})^{-1}Hg^{-1} \subseteq H$$

Luego, para $h \in H$ se tiene que $ghg^{-1} \in H$, de donde $ghg^{-1} = h_1$, para algún $h_1 \in H$. Así $h = g^{-1}h_1g \in g^{-1}Hg$, lo que implica que $H \subseteq g^{-1}Hg$, $\forall g \in G$.

Por lo tanto $g^{-1}Hg = H$, $\forall g \in G$. Es decir H es un subgrupo normal de G. ■

Observación. Según la proposición, un criterio para demostrar que un subgrupo H de un grupo G es un subgrupo normal, es suficiente verificar que $g^{-1}Hg \subseteq H$, $\forall g \in G$.

Teorema 2.1.6. *Todo subgrupo de un grupo abeliano es un subgrupo normal.*

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Demostración. Sea H un subgrupo de un grupo abeliano G. Como G es conmutativo, para $h \in H$ y $g \in G$ se tiene que

$$g^{-1}hg = g^{-1}gh = eh = h \in H.$$

Así $g^{-1}hg \subseteq H$ para todo $g \in G$, por la observación anterior concluimos que H es un subgrupo normal de G. ■

Definición 2.2.13 (grupo cociente**).** Sea N un subgrupo normal de un grupo G. El conjunto de las clases laterales izquierdas de N en G es un grupo bajo la operación $(aN)(bN) = abN$. Este grupo es llamado el *grupo cociente* de G por N y se denota por G / N. Las clases laterales izquierdas son las clases residuales de G módulo N.

Teorema 2.1.7. *Si G es un grupo cíclico y N un subgrupo normal de G, entonces G / N es un grupo cíclico.*

Demostración. Sea a un generador de G y definamos

$$G / N = \ a^r \in a^r N / \langle a \rangle = G, r \in \mathbb{Z} \ = a^r N$$

Como $\langle aN \rangle$ es un subgrupo cíclico de G / N generado por aN, deducimos que

$$\langle aN \rangle \subseteq G / N \qquad (2.1)$$

Debemos verificar que $G / N \subseteq \langle aN \rangle$.

En efecto, sea $gN \in G / N$, como $g \in G = \langle a \rangle$ existe $r \in \mathbb{Z}$ tal que $g = a^r$, de modo que $gN = a^r N = (aN)^r$, de donde $gN \in \langle aN \rangle$. Así

$$G / N \subseteq \langle aN \rangle \qquad (2.2)$$

De (2.1) y (2.2), concluimos que $G / N = \langle aN \rangle$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Por lo tanto G/N es cíclico si G es un grupo cíclico. ■

2.1.5. Homomorfismo de grupos.

Sea $f: G \to \bar{G}$ una aplicación entre dos grupos, si a y b son elementos de G, entonces $a \cdot b$ es un elemento de G. Por otra parte $f(a)$ y $f(b)$ son elementos de $\bar{G}$, luego $f(a) \cdot f(b)$ está en $\bar{G}$.

Definición 2.1.14. Sean G y $\bar{G}$ dos grupos. Una aplicación $\varphi: G \to \bar{G}$ es un *homomorfismo* si $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ para todos los elementos $a, b \in G$.

Teorema 2.1.8. *Si N es un subgrupo normal de un grupo G, entonces la aplicación canónica $\hat{\varphi}: G \to G/N$ dada por $\hat{\varphi}(a) = aN$ para $a \in G$, es un homomorfismo.*

Demostración. Para $a, b \in G$, se debe demostrar que $\hat{\varphi}(ab) = \hat{\varphi}(a)\hat{\varphi}(b)$.
En efecto,

$$\begin{aligned} \hat{\varphi}(ab) &= (ab)N, ab \in G \\ &= (aN)(bN), \text{ porque } H \trianglelefteq G \\ &= \hat{\varphi}(a)\hat{\varphi}(b) \blacksquare \end{aligned}$$

Definición 2.1.15. Sea $\varphi: G \to \bar{G}$ un homomorfismo de grupos y $\bar{e}$ es la identidad en $\bar{G}$, entonces el **Kernel** de φ, **o núcleo** es el conjunto

$$Ker\,\varphi = \{a \in G / \varphi(a) = \bar{e}\}$$

Teorema 2.1.9. *Sea $\varphi: G \to \bar{G}$ un homomorfismo de grupos, se tiene que:*

1. *si e es la identidad de G, entonces $\varphi(e)$ es la identidad de $\bar{G}$,*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2. $\varphi(a^{-1}) = \left[\varphi(a)\right]^{-1}$, *para todo* $a \in G$,
3. *si* H *es un subgrupo de* G, *entonces* $\varphi(H)$ *es un subgrupo de* $\bar{G}$,
4. *el núcleo de* φ *es un subgrupo normal de* G.

Demostración.

1. Como φ es un homomorfismo de G en $\bar{G}$, se sigue que

$$\varphi(a) = \varphi(ae) = \varphi(a)\varphi(e) = \varphi(a)\bar{e} \quad \text{y}$$

$$\varphi(a) = \varphi(ea) = \varphi(e)\varphi(a) = \bar{e}\,\varphi(a)$$

de donde por la propiedad cancelativa en $\bar{G}$, resulta que $\varphi(e)$ es la identidad $\bar{e}$ en $\bar{G}$.

2. Para todo $a \in G$, se tiene que

$$\varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) \quad \text{y}$$

$$\varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a)$$

como el inverso de $\varphi(a)$ en $\bar{G}$ es único, resulta que $\varphi(a^{-1}) = [\varphi(a)]^{-1}$.

3. Como $e \in H$ implica que $\varphi(e) = \bar{e} \in \varphi(H)$, de donde se tiene que $\varphi(H) \neq \varnothing$. Sean $a, b \in \varphi(H)$, entonces existen $h_1, h_2 \in H$ tales que

$$a = \varphi(h_1), \quad b = \varphi(h_2)$$

de donde $b^{-1} = [\varphi(h_2)]^{-1} = \varphi(h_2^{-1})$ con $h_2^{-1} \in H$, por que H es un subgrupo de G.

Así, $ab^{-1} = \varphi(h_1)\varphi(h_2^{-1}) = \varphi(h_1h_2^{-1}) \in \varphi(H)$, ya que φ es homomorfismo y $h_1h_2^{-1} \in H$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Por lo tanto, según el teorema 2.1.1 deducimos que $\varphi(H)$ es un subgrupo de $\bar{G}$.

.

4. Por definición, el núcleo de φ es el conjunto $Ker\,\varphi = \{a \in G \,/\, \varphi(a) = \bar{e}\}$. En primer lugar demostraremos que $Ker\,\varphi$ es un subgrupo de G.

   En efecto, como $\varphi(e) = \bar{e}$, tenemos que $\bar{e} \in Ker\,\varphi$, de donde $Ker\,\varphi \neq \varnothing$. Sean $a, b \in Ker\,\varphi$, entonces $\varphi(a) = \bar{e}$, $\varphi(b) = \bar{e}$ y

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)[\varphi(b)]^{-1} \\ &= \bar{e}(\bar{e})^{-1} = \bar{e}, \end{aligned}$$

   de donde $ab^{-1} \in Ker\varphi$. Por lo tanto $Ker\,\varphi$ es un subgrupo de G.

   Para demostrar la normalidad de $Ker\,\varphi$, sea $g \in G$ y $k \in Ker\,\varphi$, entonces debemos probar que $g^{-1}kg \in Ker\,\varphi$.

   En efecto, para $g \in G$ y $k \in Ker\,\varphi$, tenemos que

$$\begin{aligned} \varphi(g^{-1}kg) &= \varphi(g^{-1})\varphi(k)\varphi(g) \\ &= [\varphi(g)]^{-1}\bar{e}\,\varphi(g) \\ &= [\varphi(g)]^{-1}\varphi(g) = \bar{e} \end{aligned}$$

   de donde $g^{-1}kg \in Ker\,\varphi$. Por lo tanto $Ker\,\varphi$ es un subgrupo normal de G. ■

Definición 2.1.16 (isomorfismo**).** Un homomorfismo de grupos $\varphi : G \to \bar{G}$ se llama *isomorfismo* o también que G y $\bar{G}$ son grupos isomorfos, lo cual se denota por $G \cong \bar{G}$, si φ es una biyección.

Ejemplo 2.1.1. Demostrar que el grupo $\mathbb{R}$ bajo la adición es isomorfo al grupo $\mathbb{R}^+$ bajo la multiplicación.

Demostración.

- Definamos una aplicación $\varphi : \mathbb{R} \to \mathbb{R}^+$ por $\varphi(x) = e^x$, $\forall x \in \mathbb{R}$.

Repositorio Institucional UNA-PUNO

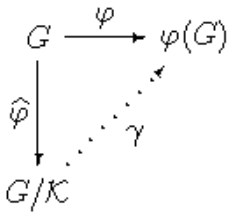
No olvide citar esta tesis

- Para todo $x, y \in \mathbb{R}$, obtenemos $\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$. Por lo tanto φ es un homomorfismo.
- Sean $x, y \in \mathbb{R}$ tales que $\varphi(x) = \varphi(y)$, entonces $x = y$.

  En efecto, como $e^x = e^y$, aplicando logaritmo natural se obtiene $x = y$. Por lo tanto φ es inyectiva.
- Si $r \in \mathbb{R}^+$, entonces existe $\ln r \in \mathbb{R}$ tal que $\varphi(\ln r) = e^{\ln r} = r$. Por lo tanto φ es sobre $\mathbb{R}^+$. ■

2.1.6. El teorema fundamental del homomorfismo.

Sea $\varphi : G \to \bar{G}$ un homomorfismo de grupos, con núcleo $\mathcal{K}$. Entonces $\varphi(G)$ es un grupo y existe un isomorfismo canónico (natural) $\gamma : G / \mathcal{K} \to \varphi(G)$ tal que conmuta el diagrama.



Demostración.

- Considerando $H = G$ en el teorema 2.1.8, deducimos que $\varphi(G)$ es un subgrupo de $\bar{G}$, luego $\varphi(G)$ es un grupo.

  Como $\mathcal{K} = Ker\,\varphi$ es un subgrupo normal de G, existe el grupo cociente $G / \mathcal{K}$ dado en la definición 2.1.12.

- El grupo cociente $G / \mathcal{K}$ es isomorfo al grupo $\varphi(G)$; es decir, $G / \mathcal{K} \cong \varphi(G)$.

  En efecto, definamos la aplicación $\gamma : G / \mathcal{K} \to \varphi(G)$ por $\gamma(a\mathcal{K}) = \varphi(a)$, para todo $a\mathcal{K} \in G / \mathcal{K}$.

  1. γ está bien definida (como aplicación).

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Sean $a\mathcal{K}, b\mathcal{K} \in G\,/\,\mathcal{K}$ tales que $a\mathcal{K} = b\mathcal{K}$, entonces $\gamma(a\mathcal{K}) = \gamma(b\mathcal{K})$.

En efecto, tenemos $a\mathcal{K} = b\mathcal{K}$, implica que $b^{-1}a \in \mathcal{K}$, luego

$$\begin{aligned} \varphi(b^{-1}a) &= \overline{e} \\ \varphi(b^{-1})\varphi(a) &= \overline{e} \\ [\varphi(b)]^{-1}\varphi(a) &= \overline{e}, \quad \text{de donde } \varphi(a) = \varphi(b). \end{aligned}$$

Asi, por definición de γ : $\gamma(a\mathcal{K}) = \varphi(a) = \varphi(b) = \gamma(b\mathcal{K})$.

2. γ es homomorfismo.

Sean $a\mathcal{K}, b\mathcal{K} \in G\,/\,\mathcal{K}$, entonces $\gamma(a\mathcal{K}\,b\mathcal{K}) = \gamma(a\mathcal{K})\gamma(b\mathcal{K})$.

En efecto,

$$\begin{aligned} \gamma(a\mathcal{K}\,b\mathcal{K}) &= \gamma(ab\mathcal{K}), && \mathcal{K} \text{ es un subgrupo normal} \\ &= \varphi(ab), && \text{por definición de } \gamma \\ &= \varphi(a)\varphi(b), && \varphi \text{ es homomorfismo} \\ &= \gamma(a\mathcal{K})\gamma(b\mathcal{K}) \end{aligned}$$

3. γ es inyectiva.

Sean $a\mathcal{K}, b\mathcal{K} \in G\,/\,\mathcal{K}$ tales que $\gamma(a\mathcal{K}) = \gamma(b\mathcal{K})$, entonces $a\mathcal{K} = b\mathcal{K}$.

En efecto, de $\gamma(a\mathcal{K}) = \gamma(b\mathcal{K})$ se tiene $\varphi(a) = \varphi(b)$, luego

$$\begin{aligned} [\varphi(b)]^{-1}\varphi(a) &= \overline{e} \\ \varphi(b^{-1})\varphi(a) &= \overline{e} \\ \varphi(b^{-1}a) &= \overline{e}, \quad \text{de donde } b^{-1}a \in \mathcal{K}. \end{aligned}$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

esto implica que $a\mathcal{K} = b\mathcal{K}$.

4. γ es sobre $\varphi(G)$.

   En efecto, dado $\varphi(g) \in \varphi(G)$, por definición existe $g\mathcal{K} \in G/\mathcal{K}$ tal que $\gamma(g\mathcal{K}) = \varphi(g)$.

Luego, de 1), 2), 3) y 4) se tiene que $G/\mathcal{K} \cong \varphi(G)$.

El diagrama es claramente conmutativo, ya que para todo $a \in G$,

$$\begin{aligned} \gamma(\hat{\varphi}(a)) &= \gamma(a\mathcal{K}) \\ &= \varphi(a), \end{aligned}$$

de donde, $\gamma \circ \hat{\varphi} = \varphi$. ■

2.2. Anillos y campos

Desde un punto de vista aritmético, los anillos son las estructuras que recogen las operaciones de suma y producto, como las que tenemos en $\mathbb{Z}$.

Definición 2.2.1 (anillo**).** Sea R un conjunto no vacío, donde se definen las operaciones $(+)$ y $(\cdot)$ (suma y multiplicación). Se dice que la terna $(R, +, \cdot)$ es un *anillo*, si cumple lo siguientes:

1. $(R, +)$ es un grupo abeliano

2. La multiplicación en R es asociativa.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in R$$

3. Para todo a, b y c en R se cumple las leyes distributivas

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Notación: Habitualmente se usará R para designar el anillo $(R,+,\cdot)$.

Definición 2.2.2. Un anillo en que la multiplicación es conmutativa es un *anillo conmutativo*. Un anillo R con identidad multiplicativa 1 tal que $1\cdot a = a\cdot 1 = a$ para todo $a \in R$ es un *anillo con unitario*. Una identidad multiplicativa en un anillo es un *elemento unitario*.

2.2.1. Dominios enteros y campos.

Definición 2.2.3. Los elementos a y b distintos de cero de un anillo R se llaman *divisores de cero* si $a\cdot b = 0$. En particular, a es un divisor izquierdo de cero y b es un divisor derecho de cero.

Observación. En un anillo conmutativo, todo divisor izquierdo de cero es también un divisor derecho de cero.

Definición 2.2.4 (dominio entero**).** Un anillo conmutativo R con unitario es un *dominio entero o dominio de integridad*, si no tiene divisores de cero, es decir, si $a\cdot b = 0$ en R implica que $a = 0$ o bien $b = 0$.

***Ejemplo* 2.3.1.** $\mathbb{Z}$ y $\mathbb{Z}_p$ para cualquier primo p es un dominio entero.

Observación. En un domino entero se cumple la ley de cancelación, es decir, si en un dominio de integridad tenemos que $a\cdot b = a\cdot c$ y $a \neq 0$, entonces $b = c$, pues $a(b-c) = 0$, luego $b - c = 0$.

Definición 2.2.5 (anillo de división y campo**).** Sea R un anillo con unitario. Un elemento u en R es una **unidad** de R si tiene inverso multiplicativo en R. Si todo elemento distinto de cero en R es una unidad, entonces R es un *anillo de división*. Un **campo** es un anillo de división conmutativo.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Observación.

1. Un inverso multiplicativo de un elemento a en un anillo R con unitario 1, es un elemento $a^{-1} \in R$ tal que $a^{-1} \cdot a = a \cdot a^{-1} = 1$.
2. Según la definición un campo es un anillo conmutativo con unitario, en donde todos los elementos distintos de cero son invertibles.

Proposición 2.2.1. *Todo campo F es un dominio entero.*

Demostración. Todo campo es un anillo conmutativo con unitario. Si $ab = 0$ en F y $a \neq 0$ debemos probar que $b = 0$.

En efecto, como $a \in F - \{0\}$ es unidad, existe $a^{-1} = \dfrac{1}{a} \in F$ de modo que

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0.$$

Luego,

$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b.$$

Entonces, no existe divisores de cero en F. Por lo tanto F es dominio entero ■

Teorema 2.2.1. *Todo dominio entero finito es un campo.*

Demostración. Sean $0, 1, a_1, \ldots, a_n$ todos los elementos de un dominio entero finito D. Sea $a \in D - \{0\}$, entonces debemos demostrar que existe $b \in D$ tal que $ab = 1$. Considerando $a1, aa_1, \ldots, aa_n$, afirmamos que todos estos elementos de D son distintos, de lo contrario $aa_i = aa_j$ para $i \neq j$ nos da $a_i = a_j$ $(\rightarrow\leftarrow)$ pues D es un dominio entero. Así $a1, aa_1, \ldots, aa_n$ son los elementos $1, a_1, \ldots, a_n$ en algún orden, de manera que $a1 = 1$ de donde $a = 1$ ó $aa_i = 1$ para algún i, para $a \neq 1$.

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Por lo tanto, a tiene inverso multiplicativo en D, de modo que D es un campo ■

2.2.2. Subanillos e ideales.

Definición 2.2.6 (subanillo**).** Sea S un subconjunto no vacío de un anillo $(R,+,\cdot)$ Se dice que S es un *subanillo* de R si con las operaciones inducidas S posee estructura de anillo.

Proposición 2.2.2. *Un subconjunto S de un anillo R es un subanillo de R si y solo si se cumplen las tres condiciones siguientes:*

1. $0 \in S$,
2. $a-b \in S$ *para todo* $a,b \in S$,
3. $a \cdot b \in S$ *para todo* $a,b \in S$.

$\Rightarrow$] Si S es un subanillo de R, entonces por definición 2.2.6 S mismo es un anillo bajo las operaciones inducidas de R, luego $(S,+)$ es un grupo y S es cerrado bajo la multiplicación inducida de R. Así se tiene que:

- la identidad aditiva $0 \in S$,
- $a-b \in S$ para todo $a,b \in S$ porque S es un grupo bajo la adición,
- $ab \in S$ para todo $a,b \in S$ porque S es cerrado bajo la multiplicación inducida de R.

$\Leftarrow$] Supongamos que se cumplen las condiciones 1, 2 y 3, entonces S es un subanillo de R.

En efecto, como S es un subconjunto no vacío de R, tenemos que demostrar que S es un anillo bajo las operaciones inducidas de R. Es decir, debemos verificar los tres axiomas de la definición de anillos para S:

- $(S,+)$ es un grupo abeliano.

  Como se cumplen las condiciones 1 y 2 para S, vemos que S es un subconjunto no vacío de R y $a-b \in S$ para todo $a,b \in S$. Según el teorema

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

2.2.1, S es un subgrupo del grupo aditivo $(R,+)$. Como $(R,+)$ es abeliano, luego $(S,+)$ es un grupo abeliano.

- La multiplicación en S es asociativa.

  Sean $a,b,c \in S$, entonces $(ab)c = a(bc)$.

  En efecto, como $S \subseteq R$ y $a,b,c \in S$ se sigue que $a,b,c \in R$. Del hecho que en R la multiplicación es asociativa obtenemos que $(ab)c = a(bc)$.

- Se cumplen las leyes distributivas en S.

  Sean $a,b,c \in S$, entonces $a(b+c) = ab+ac$ y $(a+b)c = ac+bc$.

  En efecto, como $S \subseteq R$ y $a,b,c \in S$ implica que $a,b,c \in R$. Sabemos que en R se cumplen las leyes distributivas, de donde se obtiene que $a(b+c) = ab+ac$ y $(a+b)c = ac+bc$. ■

Definición 2.2.7 (ideal**).** Un *ideal* (o un ideal bilateral) en un anillo R es un subgrupo aditivo $(I,+)$ de R tal que si $r \in R$ y $a \in I$, entonces $ar \in I$, $ra \in I$; es decir, $rI \subseteq I$ y $Ir \subseteq I$ para todo $r \in R$.

Observaciones.

a) Todo anillo R tiene al menos dos ideales, el ideal *impropio* R y el ideal *trivial* $\{0\}$.

b) Sea I un ideal de un anillo R; se dice, que I es un ideal propio de R si $I \neq R$.

Definición 2.2.8. Sea R un anillo conmutativo con unitario, el conjunto

$$aR = \langle a \rangle = \{ar \,/\, r \in R\}$$

es un ideal de R llamado *ideal principal* generado por $a \in R$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2.2.3. Anillos cocientes y homomorfismos.

Sea I un ideal propio de un anillo R. Si consideramos R como un grupo abeliano con respecto a la operación de adición, entonces el ideal I es un subgrupo normal de R, y por consiguiente podemos definir el grupo cociente R/I, cuyos elementos son las clases laterales

$$[x] = x + I = \{x + a \,/\, a \in I\}, x \in R$$

Teorema 2.2.2. *Sea I un ideal propio de un anillo R. Si las operaciones de adición y multiplicación en R/I dadas por*

$$\begin{aligned} (x+I)+(y+I) &= (x+y)+I \\ (x+I)(y+I) &= (xy)+I, x, y \in R, \end{aligned}$$

están bien definidas, entonces bajo estas operaciones el grupo cociente R/I es un anillo (con neutro $0+I$ y identidad multiplicativa $1+I$).

Demostración.

- R/I es un grupo abeliano.

  Sean $x+I,\ y+I \in R/I$, entonces $(x+I)+(y+I) = (y+I)+(x+I)$.

  En efecto,

$$\begin{aligned} (x+I)+(y+I) &= (x+y)+I \\ &= (y+x)+I, \qquad (\mathrm{R},+)\,\text{es abeliano} \\ &= (y+I)+(x+I), \qquad I \trianglelefteq R \end{aligned}$$

- La multiplicación en R/I es asociativa.

  Si $x+I,\ y+I,\ z+I \in R/I \Rightarrow$

  $[(x+I)(y+I)](z+I) = (x+I)[(y+I)(z+I)]$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

En efecto, desarrollando:

$$\begin{aligned}
[(x+I)(y+I)](z+I) &= (xy+I)(z+I) \\
&= (xy)z+I \\
&= x(yz)+I, && R \text{ es un anillo} \\
&= (x+I)(yz+I), && I \trianglelefteq R \\
&= (x+I)[(y+I)(z+I)]
\end{aligned}$$

- En R/I se cumplen las leyes distributivas.

  a) $(x+I)[(y+I)+(z+I)] = (xy+I)+(xz+I)$

  b) $[(x+I)+(y+I)](z+I) = (xz+I)+(yz+I)$

  Verificando a):

$$\begin{aligned}
(x+I)[(y+I)+(z+I)] &= (x+I)[(y+z)+I] \\
&= x(y+z)+I \\
&= (xy+xz)+I \\
&= (xy+I)+(xz+I)
\end{aligned}$$

  Análogamente se verifica b).

Luego, se cumplen los tres axiomas de la definición de anillos, se concluye que R/I es un anillo ■

Definición 2.2.9 (homomorfismo**).** Sean R y $\bar{R}$ dos anillos. Una aplicación $\varphi : R \to \bar{R}$ es un *homomorfismo* si preserva las dos operaciones de los anillos; es decir, si cumple las dos condiciones siguientes:

- $\varphi(a+b) = \varphi(a)+\varphi(b)$
- $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$, para todo a,b en R.

Definición 2.2.10. Sea R y $\bar{R}$ dos anillos. Un homomorfismo $\varphi : R \to \bar{R}$ el cual es biyectivo se llama un *isomorfismo* de anillos.

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Dos anillos R y $\overline{R}$ son *isomorfos* (abreviadamente: $R \cong \overline{R}$) si existe un isomorfismo $\varphi : R \to \overline{R}$. Cuando dos anillos son isomorfos son algebraicamente indistinguibles, es decir, uno es conmutativo si y solo si lo es el otro, etc., por tanto podemos considerarlo el mismo anillo.

Definición 2.2.11. Sea $\varphi : R \to \overline{R}$ un homomorfismo de anillos, llamamos *imagen* y *núcleo* de φ, respectivamente, a los conjuntos.

$$\mathrm{Im}\varphi = \{\varphi(a) \,/\, a \in R\} \qquad \text{y} \qquad \mathrm{Ker}\varphi = \{a \in R \,/\, \varphi(a) = \overline{0}\},$$

donde $\overline{0}$ es la identidad aditiva de $\overline{R}$.

Observación. Conviene observar que, mientras que la imagen inversa de un ideal por un homomorfismo es un ideal, la imagen de un ideal no es en general un ideal (salvo que el homomorfismo sea suryectiva). Lo único que se puede afirmar es que la imagen de un subanillo es un subanillo.

Teorema 2.2.3. *Si I es un ideal de un anillo R, entonces la aplicación canónica $\hat{\varphi} : R \to R/I$ dada por $\hat{\varphi}(r) = r + I$ para todo $r \in R$ es un homomorfismo de anillos de R sobre R/I.*

Demostración. Por hipótesis I es un ideal de R, entonces según el teorema 2.2.2 la suma y multiplicación de clases laterales están bien definidas.

- Si $a, b \in R$, entonces $\hat{\varphi}(a+b) = \hat{\varphi}(a) + \hat{\varphi}(b)$.

En efecto,

$$\begin{aligned} \hat{\varphi}(a+b) &= (a+b) + I, \qquad \text{pues } a+b \in R \\ &= (a+I) + (b+I) \\ &= \hat{\varphi}(a) + \hat{\varphi}(b) \end{aligned}$$

- Si $a, b \in R$, entonces $\hat{\varphi}(ab) = \hat{\varphi}(a)\hat{\varphi}(b)$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

En efecto,

$$\begin{aligned} \hat{\varphi}(ab) &= ab + I, \quad \text{pues } ab \in R \\ &= (a+I)(b+I) \\ &= \hat{\varphi}(a)\hat{\varphi}(b) \end{aligned}$$

- $\hat{\varphi}$ es sobre R/I.

En efecto, dado $a + I \in R/I$, por definición de $\hat{\varphi}$ se ve que existe $a \in R$ tal que $\hat{\varphi}(a) = a + I$.

De a), b), c) se concluye que $\hat{\varphi} : R \to R/I$ es un homomorfismo de anillos de R sobre R/I. ■

Proposición 2.2.3. *El núcleo de un homomorfismo de anillos $\varphi : R \to \bar{R}$ es un ideal bilátero de R.*

Demostración.

1. Se demuestra que $Ker\varphi$ es un subgrupo aditivo del grupo abeliano $(R,+)$ con los items siguientes:

   - Como $Ker\varphi = \{r \in R / \varphi(r) = \bar{0}\}$, $0 \in R$ y $\varphi(0) = \bar{0}$, vemos que $0 \in Ker\varphi$. De donde, $Ker\varphi$ es un subconjunto no vacío del grupo $(R,+)$.
   - Sean $r_1, r_2 \in Ker\,\varphi$, entonces $r_1 - r_2 \in Ker\,\varphi$.

   En efecto,

   $r_1 \in Ker\varphi$ implica que $r_1 \in R$ y $\varphi(r_1) = \bar{0}$,

   $r_2 \in Ker\varphi$ implica que $r_2 \in R$ y $\varphi(r_2) = \bar{0}$;

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

de modo que $r_1 - r_2 \in R$ y $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) = \overline{0}$. De donde $r_1 - r_2 \in Ker\,\varphi$.

2. Si $r \in R$ y $a \in Ker\,\varphi$, entonces ra y $ar \in Ker\,\varphi$.

   En efecto, $a \in Ker\,\varphi$ implica que $\varphi(a) = \overline{0}$.

- Sabemos que $ra \in R$ y

$$\begin{aligned} \varphi(ra) &= \varphi(r)\varphi(a) \\ &= \varphi(r)\overline{0} \\ &= \overline{0} \end{aligned}$$

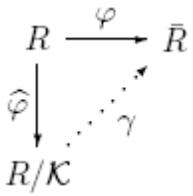
- También $ar \in R$ y

$$\begin{aligned} \varphi(ar) &= \varphi(a)\varphi(r) \\ &= \overline{0}\varphi(r) \\ &= \overline{0} \end{aligned}$$

  De las dos últimas deducciones obtenemos que ar y $ra \in Ker\,\varphi$

Luego, de 1) y 2) se sigue que $Ker\,\varphi$ es un ideal bilátero de R. ■

Teorema 2.2.4. *Sea* $\varphi : R \to \bar{R}$ *un homomorfismo sobreyectivo de anillos, con núcleo* $\mathcal{K}$. *Entonces existe un isomorfismo de anillos* $\gamma : R / \mathcal{K} \to \bar{R}$ *que hace conmutativo el diagrama.*



Demostración. Definamos la aplicación $\gamma : R / \mathcal{K} \to \bar{R}$ por $\gamma(a + \mathcal{K}) = \varphi(a)$, para todo $a + \mathcal{K} \in R / \mathcal{K}$.

1. γ está bien definida (como aplicación).

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Sean $a+\mathcal{K}, b+\mathcal{K} \in R/\mathcal{K}$ tales que $a+\mathcal{K}=b+\mathcal{K}$, entonces

$\gamma(a+\mathcal{K})=\gamma(b+\mathcal{K})$.

En efecto,

$$\begin{array}{rcll} \text{Si}, a+\mathcal{K} & = & b+\mathcal{K} & \Rightarrow \quad a-b\in\mathcal{K} \\ & & & \Rightarrow \quad \varphi(a-b)=\overline{0} \\ & & & \Rightarrow \quad \varphi(a)=\varphi(b) \\ & & & \Rightarrow \quad \gamma(a+\mathcal{K})=\gamma(b+\mathcal{K}) \end{array}$$

2. γ es un homomorfismo.

- Sean $a+\mathcal{K}, b\mathcal{K}\in R/\mathcal{K}$, entonces

  $\gamma[(a+\mathcal{K})+(b+\mathcal{K})]=\gamma(a+\mathcal{K})+\gamma(b+\mathcal{K})$.

  En efecto,

$$\begin{array}{rcll} \gamma[(a+\mathcal{K})+(b+\mathcal{K})] & = & \gamma[(a+b)+\mathcal{K}], & \mathcal{K}\,\text{es un ideal de}\,R \\ & = & \varphi(a+b), & \text{definición de}\,\gamma \\ & = & \varphi(a)+\varphi(b), & \varphi\,\text{es un homomorfismo} \\ & = & \gamma(a+\mathcal{K})+\gamma(b+\mathcal{K}) & \end{array}$$

- Sean $a+\mathcal{K}, b+\mathcal{K}\in R/\mathcal{K}$, entonces $\gamma[(a+\mathcal{K})(b+\mathcal{K})]=\gamma(a+\mathcal{K})\gamma(b+\mathcal{K})$

  .

  En efecto,

$$\begin{array}{rcll} \gamma[(a+\mathcal{K})(b+\mathcal{K})] & = & \gamma[ab+\mathcal{K}], & \mathcal{K}\,\text{es un ideal de}\,R \\ & = & \varphi(ab), & \text{definición de}\,\gamma \\ & = & \varphi(a)\varphi(b), & \varphi\,\text{es un homomorfismo} \\ & = & \gamma(a+\mathcal{K})\gamma(b+\mathcal{K}) & \end{array}$$

3. γ es inyectiva.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Sean $a+\mathcal{K}, b+\mathcal{K} \in R/\mathcal{K}$, tales que $\gamma(a+\mathcal{K}) = \gamma(b+\mathcal{K})$ entonces, $a+\mathcal{K} = b+\mathcal{K}$.

En efecto, de $\gamma(a+\mathcal{K}) = \gamma(b+\mathcal{K})$, se tiene $\varphi(a) = \varphi(b)$. De donde $\varphi(a-b) = \overline{0}$, implica que $a-b \in \mathcal{K}$, luego $a+\mathcal{K} = b+\mathcal{K}$.

4. γ es sobre $\overline{R}$.

Dado $c \in \overline{R}$, existe $a+\mathcal{K} \in R/\mathcal{K}$ tal que $\gamma(a+\mathcal{K}) = c$.

En efecto, del hecho que $c \in \overline{R}$ sabemos que existe $a \in R$ tal que $c = \varphi(a)$. Por definición de la aplicación γ, vemos que $\gamma(a+\mathcal{K}) = c$. Así existe $a+\mathcal{K} \in R/\mathcal{K}$ tal que $\gamma(a+\mathcal{K}) = c$.

Luego, de 1), 2), 3) y 4) deducimos que γ es un isomorfismo de $R/\mathcal{K}$ sobre $\overline{R}$. Esto indica que $R/\mathcal{K}$ es isomorfo a $\overline{R}$.

La conmutatividad del diagrama es claro, ya que para todo $a \in R$, se tiene

$$\gamma(\hat{\varphi}(a)) = \gamma(a+\mathcal{K}) = \varphi(a),$$

de donde, $\gamma \circ \hat{\varphi} = \varphi$. ■

2.2.4. Ideales maximales y primos.

Definición 2.2.12. Un ideal propio M de un anillo R es un *ideal maximal* si I es un ideal de R tal que $M \subset I \subset R$, entonces $M = I$ ó $I = R$.

Teorema 2.2.5. *Sea R un anillo conmutativo con unitario. Entonces, M es un ideal maximal de R si y solo si R/M es un campo.*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Demostración.

$\Rightarrow]$ Por hipótesis M es un ideal maximal. Demostraremos que R/M es un campo.

Como $M \neq R$ es un ideal de R, se demuestra que R/M es un anillo conmutativo con unitario. Sea $x+M$ un elemento distinto de cero de R/M; es decir, $x+M \neq M$, luego debemos demostrar que existe $y+M \in R/M$ tal que $(x+M)(y+M)=1+M$.

Como $x+M \in R/M-\{M\}$, se deduce que $x \notin M$, de modo que el ideal generado por M y x es R, de donde $1 \in R$ y podemos escribir como $1=xy+a$ para algunos $a \in M$ e $y \in R$, luego $(x+M)(y+M)=xy+M=1+M$, de modo que $x+M$ tiene como inverso multiplicativo a $y+M$, por lo tanto R/M es un campo.

$\Leftarrow]$ Supongamos que R/M es un campo, entonces vamos demostrar que M es un ideal maximal de R.

Sea N un ideal de R tal que $M \subseteq N \subseteq R$, tomando el homomorfismo $\gamma: R \to R/M$ se deduce que $M/M=\gamma(M) \subseteq \gamma(N) \subseteq \gamma(R)=R/M$, donde $\gamma(N)$ es un ideal de R/M. Como R/M es un campo, entonces debemos tener $M/M=\gamma(M)=N/M$ ó $N/M=\gamma(N)=R/M$. De esto se deduce que $M=N$ ó $N=R$, por consiguiente M es un ideal maximal de R. ■

Definición 2.2.13. Un ideal propio I de un anillo conmutativo R es un *ideal primo* si para todo $a,b \in R$ tales que $ab \in I$ se tiene que $a \in I$ o $b \in I$.

Teorema 2.2.6. *Sea R un anillo conmutativo con unitario y $I \neq R$ un ideal en R. Entonces R/I es un dominio de integridad si y solo si I es un ideal primo en R.*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Demostración.

$\Rightarrow$] Sea R/I un dominio de integridad y $wz \in I$, entonces demostraremos que $w \in I$ ó $z \in I$.

En efecto, de $wz \in I$ deducimos que $(w+I)(z+I) = wz + I = I$. Por hipótesis $w + I = I$ ó $z + I = I$, por lo tanto $w \in I$ ó $z \in I$.

$\Leftarrow$] Sea I un ideal primo y $(x+I)(y+I) = I \in R/I$. Demostraremos que $x + I = I$ ó $y + I = I$ debido a que R/I es un anillo conmutativo con unitario.

En efecto, usando la igualdad

$$\begin{aligned} xy + I &= (x+I)(y+I) \\ &= I \end{aligned}$$

vemos que $xy \in I$. Como I es primo, se sigue que $x \in I$ ó $y \in I$, esto significa que $x + I = I$ ó $y + I = I$. ■

2.2.5. Campo de cocientes de un dominio entero.

Sea D un domino de integridad y

$$S = D \times (D - \{0\}) = \{(a,b) \,/\, a,b \in D, b \neq 0\}$$

el conjunto de todo los pares ordenados. Luego, se define en S la relación $(a,b) \equiv (c,d)$ si y solo si $ad = bc$. Se demuestra que esta relación es de equivalencia.

Sea F el conjunto de las clases de equivalencia, escribimos $[a,b]$ para la clase de equivalencia del elemento (a,b) en S. Así pues

$$F = \{[a,b] \,/\, (a,b) \in S\}$$

donde $[a,b] = \{(x,y) \in S \,/\, (x,y) \equiv (a,b)\}$.

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Definimos la suma y multiplicación en F por las reglas:

$$\begin{aligned}[a,b]+[c,d] &= [ad+bc,bd]\\ [a,b][c,d] &= [ac,bd]\end{aligned}$$

Se comprueba que estas reglas están bien definidas y de esta forma F se convierte en un anillo conmutativo, con identidades aditiva y multiplicativa $0=[0,1]$, $1=[1,1]$, respectivamente. En realidad F se convierte en un campo, el cual se denomina **campo de cocientes** de D, ya que para todo $[a,b]\in F-\{0\}$, existe $[b,a]\in F$ tal que $[a,b][b,a]=[ab,ba]=[1,1]=1$.

Lema 2.3.1. *La aplicación* $\varphi : D \to F$ *definida por*

$$\varphi(a)=[a,1],\ a\in D$$

es un homomorfismo inyectivo.

Demostración.

1. φ es un homomorfismo.

- Sean $a,b\in D$, entonces $\varphi(a+b)=\varphi(a)+\varphi(b)$.

En efecto,

$$\begin{aligned}\varphi(a+b) &= [a+b,1], \quad \text{definición de } \varphi\\ &= [a,1]+[b,1]\\ &= \varphi(a)+\varphi(b)\end{aligned}$$

- Sean $a,b\in D$, entonces $\varphi(ab)=\varphi(a)\varphi(b)$.

En efecto,

$$\begin{aligned}\varphi(ab) &= [ab,1], \quad \text{definición de } \varphi\\ &= [a,1][b,1]\\ &= \varphi(a)\varphi(b)\end{aligned}$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

2. φ es inyectiva.

Sean $a,b \in D$, tales que $\varphi(a)=\varphi(b)$ entonces, $a=b$.

En efecto,

$$\varphi(a)=\varphi(b) \Rightarrow [a,1]=[b,1] \Rightarrow a=b.\blacksquare$$

2.3. Dominios enteros y polinomios.

Definición 2.3.1. Sea R un dominio entero.

a) Sean $a,b \in R$, se dice que a *divide* a b (y se denota $a \mid b$) si existe un $c \in R$ tal que $b=ac$.

b) Se dice que dos elementos a y b de R son *asociados* en R (y se escribe $a \sim b$) si $b=au$, donde u es una unidad de R.

Definición 2.3.2. Un domino entero R es un *dominio de ideales principales* (DIP) si todo ideal I de R es un ideal principal, es decir

$$I=\langle a\rangle=\{ar \,/\, r \in R\},\ a \in I.$$

Teorema 2.3.1. *Sea R un dominio de integridad y $a,b \in R$. Entonces*

1. $a \mid b$ *si y solo si* $\langle b\rangle \subset \langle a\rangle$.

2. $a \sim b$ *si y solo si* $\langle b\rangle=\langle a\rangle$.

3. a *es una unidad en* R *si y solo si* $\langle a\rangle=R$.

Demostración.

1. Supongamos primero que $a \mid b$, entonces $b=za$; para algún $z \in R$, de donde

$$\langle b\rangle=Rb=Rza \subset Ra=\langle a\rangle.$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Recíprocamente, supongamos que $\langle b\rangle \subset \langle a\rangle$, entonces existe un $z \in R$, tal que $b = za$; de donde $a \mid b$.

2. Supongamos primero que $a \sim b$, entonces existe una unidad u de R tal que $a = ub$ y $b = u^{-1}a$. Así $b \mid a$ y $a \mid b$ de donde $\langle a\rangle = \langle b\rangle$.

   Recíprocamente, supongamos que $\langle a\rangle = \langle b\rangle$, entonces existen $u, v \in R$ tales que $a = ub$, $b = va$. Luego, $(uv)a = u(va) = ub = a = 1a$, tomando los extremos y por cancelación se tiene $uv = 1$. Así u y v son unidades, de donde $a \sim b$.

3. Es claro que $\langle 1\rangle = R$. Luego,

$$\langle a\rangle = R \Leftrightarrow a \sim 1 \Leftrightarrow a \text{ es una unidad. } \blacksquare$$

Definición 2.3.3 (domino euclidiano**).** Sea R un domino entero y $R^* = R - \{0\}$. Se dice que R es un {\em domino euclidiano} si existe una aplicación $\delta : R^* \to \mathbb{Z}^+$ tal que:

a) $\delta(a) \leq \delta(ab)$, para todo $a, b \in R^*$.

b) Dados $a, b \in R$, con $b \neq 0$, existen $q, r \in R$ tales que $a = bq + r$, en donde $\delta(r) < \delta(b)$ si $r \neq 0$.

Teorema 2.3.2. *Todo dominio euclidiano es un domino de ideales principales (DIP).*

Demostración. Sea D un dominio euclidiano. Entonces el ideal $\{0\}$ es principal. Sea $I \neq \langle 0\rangle$ un ideal de D y sea $b \neq 0$ el elemento de I para el que

$$\delta(b) = \min\{\delta(x) : x \in I - \{0\}\}.$$

Dado $a \in I$, por ser D un dominio euclidiano existe q, r tal que $a = qb + r$ con $r = 0$ (ya que $\delta(r) < \delta(b)$ es imposible porque $r = a - qb \in I$). Por lo tanto $a = qb \in \langle b\rangle$ y así $I = Db = \langle b\rangle$ es un ideal principal. $\blacksquare$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Definición 2.3.4. Sea R un dominio entero. El elemento $d \in R$ es llamado *máximo común divisor* (MCD) de los elementos a y b en R^*, si se cumple las siguientes propiedades:

a) $d \mid a$ y $d \mid b$;

b) si $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

2.3.1. Dominios de factorización única.

Definición 2.3.5. Sea R un dominio entero. Un elemento $p \in R$ distinto de cero que no sea unidad es un *irreducible* de R si no admite ninguna descomposición $p = ab$ con a y b elementos de R, salvo que uno de ellos sea una unidad.

Teorema 2.3.3. *Sea R un dominio de ideales principales y $p \in R$. Entonces las condiciones siguientes son equivalentes:*

1. *p es irreducible;*
2. *$\langle p \rangle$ es un ideal maximal de R;*
3. *$R / \langle p \rangle$ es un campo.*

Demostración.

$1) \Rightarrow 2)$.

Supongamos que p es irreducible, entonces p no es unidad y así $\langle p \rangle$ es un ideal maximal de R.

En efecto, supongamos por contradicción que existe un domino de ideal principal $\langle q \rangle$ tal que $\langle p \rangle \subset \langle q \rangle \subset R$, entonces $p \in \langle q \rangle$ y $p = aq$, para algún $a \in R$, esto contradice a que p sea irreducible, luego $\langle p \rangle$ es un ideal maximal de R.

$2) \Rightarrow 3)$.

Sea $a + \langle p \rangle$ un elemento no nulo de $R / \langle p \rangle$, entonces $a \notin \langle p \rangle$, y el ideal $\langle a \rangle + \langle p \rangle$ contiene a $\langle p \rangle$ y asumiendo que $\langle p \rangle$ es maximal se tiene

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

$$\langle a\rangle + \langle p\rangle = \{sa + tp \,/\, s,t \in R\} = R$$

Por lo tanto existen s, t en R tal que $sa + tp = 1$, luego,

$$\begin{array}{rcll} sa + tp + \langle p\rangle & = & 1 + \langle p\rangle & \\ (sa + \langle p\rangle) + (tp + \langle p\rangle) & = & 1 + \langle p\rangle, & (tp \in \langle p\rangle \Rightarrow tp + \langle p\rangle = \langle p\rangle) \\ (sa + \langle p\rangle) + \langle p\rangle & = & 1 + \langle p\rangle & \\ sa + \langle p\rangle & = & 1 + \langle p\rangle & \\ (s + \langle p\rangle)(a + \langle p\rangle) & = & 1 + \langle p\rangle & \end{array}$$

Así $R \,/\, \langle p\rangle$ es un campo.

$3) \Rightarrow 1)$.

Si p no es irreducible, entonces existen r, s diferentes de la unidad tal que $p = rs$. Entonces $r + \langle p\rangle$ y $s + \langle p\rangle$ ambos diferentes de cero están en $R \,/\, \langle p\rangle$, pero

$$\begin{array}{rcl} (r + \langle p\rangle)(s + \langle p\rangle) & = & p + \langle p\rangle \\ (r + \langle p\rangle)(s + \langle p\rangle) & = & \langle p\rangle \\ (r + \langle p\rangle)(s + \langle p\rangle) & = & 0 + \langle p\rangle \end{array}$$

De este modo $R \,/\, \langle p\rangle$ tiene divisores de cero, de aquí $R \,/\, \langle p\rangle$ no es un campo. Esto es de haber supuesto que p es no irreducible.

Luego, p es irreducible. ■

Definición 2.3.6. Un domino entero R es un *dominio de factorización única* (DFU) si todo elemento $a \in R$ distinto de cero y que no sea unidad se descompone como producto de elementos irreducibles $a = p_1 p_2 \cdots p_n$ y la descomposición es única salvo ordenación o cambio por asociados, es decir, si $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

son dos descomposiciones de a en elementos irreducibles, entonces $n = m$ y ordenando los factores adecuadamente, cada p_i es asociado a q_i.

2.3.2. Polinomios.

Definición 2.3.7. Sea R un anillo conmutativo con unitario, llamaremos conjunto de los polinomios en la indeterminada x con coeficientes en R al conjunto

$$R[x] = \{ f(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n \,/\, a_i \in R, \forall i = 0,1,\ldots,n;\ n \geq 0 \}$$

donde los a_i se denominan *coeficientes* de x^i en $f(x)$ y las expresiones a_ix^i, para $0 \leq i \leq n$ se llaman *términos* del polinomio $f(x)$. Dos polinomios en x se consideran iguales si para cada i los coeficientes de x^i son iguales.

Operaciones en $R[x]$.

Sean $f(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n$ y $g(x) = b_0x^0 + b_1x^1 + \cdots + b_mx^m$ polinomios de $R[x]$. Suponiendo que $n \geq m$, definimos en $R[x]$ dos operaciones (suma y multiplicación) de la forma siguiente:

- **Suma.**

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n$$

- **Multiplicación.**

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0)x + \cdots + a_n \cdot b_m x^{n+m} \\ &= c_0 + c_1x + \cdots + c_{n+m}x^{n+m} \end{aligned}$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

donde $c_k = \sum_{i=0}^{k} a_i b_{k-i},\ \forall k \in [0, n+m]$.

Las dos operaciones definidas satisfacen las siguientes propiedades:

1. El neutro de la suma es el polinomio cero $f(x) = 0$, y de la multiplicación es el polinomio 1, $f(x) = 1$.
2. El inverso de $f(x)$ para la suma es $-f(x)$.
3. La suma y multiplicación de polinomios es asociativo y conmutativo.
4. La suma es distributiva con respecto a la multiplicación.

Con estas propiedades y con las operaciones suma y multiplicación, la terna $R[x], +, \cdot$ es un *anillo conmutativo con unitario.*

Definición 2.3.8. Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ en $R[x]$. Si, $a_n \neq 0$, entonces diremos que $f(x)$ tiene **grado** n ($grad(f(x)) = n$), con *coeficiente principal* a_n y *término principal* $a_n x^n$. Se dice que $f(x)$ es *mónico* si $a_n = 1$.

Proposición 2.3.1. Sea R un dominio entero. Si $f(x)$ y $g(x)$ son dos polinomios no nulos en $R[x]$, de grados n y m respectivamente. Entonces

1. $R[x]$ es un dominio de entero.
2. $grad\ f(x) + g(x) \leq \max\{n, m\}$
3. $grad(f(x) \cdot g(x)) = n + m$.

Demostración.

1. Si R es conmutativo, $R[x]$ también es conmutativo. Si R tiene elemento unidad, $R[x]$ también lo tiene.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Sean a_n y b_m coeficiente principal de $f(x)$ y $g(x)$ respectivamente. El coeficiente principal del producto de $f(x)$ y $g(x)$ es $a_n b_m$ diferente de cero. Así $f(x)g(x) \neq 0$, esto es; $R[x]$ no tiene divisores de cero.

Por tanto, $R[x]$ es un dominio entero.

2. Supongamos que $n \geq m$.

   Si $n > m$, entonces el grado de $f(x) + g(x)$ es n. Así $grad[f(x) + g(x)] = \text{máx}\{n, m\}$.

   Si $n = m$, sea a_n coeficiente principal de $f(x)$ y b_m el coeficiente principal de $g(x)$, entonces $a_n + b_m = 0 \vee a_n + b_m \neq 0$. Así $grad[f(x) + g(x)] \leq \text{máx}\{n, m\}$.

3. Puesto que $f(x)$ y $g(x)$ son distintos de cero entonces tienen grado, además sus coeficientes principales son distintos de cero.

   Sean a_n el coeficiente principal de $f(x)$ y b_m el coeficiente principal de $g(x)$.

   Puesto que R es un dominio entero entonces, $a_n b_m \neq 0$, se sigue que $a_n b_m$ es el coeficiente principal del producto $f(x)g(x)$, donde el grado de $a_n b_m x^{n+m}$ es $n + m$. ■

Observación. Sabemos que todo dominio entero posee un campo de cocientes. Por tanto $R[x]$ tiene su campo de cocientes, cuyos elementos son de la forma

$$\frac{a_0 + a_1 x + \cdots + a_m x^m}{b_0 + b_1 x + \cdots + b_n x^n},$$

donde el denominador no es el polinomio cero y el campo es denotado por $R(x)$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2.3.3. El algoritmo de división.

En este tema consideramos el anillo de polinomios sobre un campo K, el cual será denotado por $K[x]$.

Teorema 2.3.4 (algoritmo de la división**).** *Sea K un campo. Si $f(x)$ y $g(x)$ son polinomios distintos de cero en $K[x]$, entonces existen polinomios únicos $q(x), r(x) \in K[x]$ tales que*

$$f(x) = q(x)g(x) + r(x),$$

donde, $grad(r(x)) < grad(g(x))$ o bien $r(x) = 0$.

Demostración.

Si $f(x) = 0$ o bien $grad(f(x)) < grad(g(x))$, entonces $f(x) = 0g(x) + f(x)$, lo cual satisface el resultado del teorema.

Supongamos que $grad(f(x)) \geq grad(g(x))$. Entonces sean

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \text{ donde } a_n \neq 0$$

$$g(x) = b_m x^m + \cdots + b_1 x + b_0, \text{ donde } b_m \neq 0$$

con $n \geq m$.

Por inducción sobre n se tiene.

- Si $n = 0$, entonces

  $$f(x) = a_0,\ g(x) = b_0 \quad \text{y} \quad f(x) = a_0 b_0^{-1} g(x) + 0,$$

  de donde, tomando $q(x) = a_0 b_0^{-1}$ y $r(x) = 0$ se obtiene el resultado.

- Supongamos que el teorema es cierto para todo polinomio de grado k, con $k < n$. Luego,

$$f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

es un polinomio de grado menor que n y por la hipótesis de inducción existen $q_1(x)$ y $r_1(x)$ tales que

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r_1(x)$$

lo cual por transposición nos da

$$f(x) = \left[q_1(x) + a_n b_m^{-1} x^{n-m}\right] g(x) + r_1(x).$$

Si $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ y $r(x) = r_1(x)$, se tiene $f(x) = q(x)g(x) + r(x)$, donde, $grad(r(x)) < grad(g(x))$ o bien $r(x) = 0$.

Para la unicidad, si $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, entonces

$$[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$$

Como $grad[r_2(x) - r_1(x)] < grad(g(x))$, esto puede valer sólo si $q_1(x) - q_2(x) = 0$ o $q_1(x) = q_2(x)$. Entonces, debemos tener $r_1(x) - r_2(x) = 0$ o $r_1(x) = r_2(x)$. ■

Observación. Los polinomios $q(x)$ y $r(x)$ se llaman respectivamente *cociente* y *residuo* de dividir $f(x)$ entre $g(x)$.

Si K es un campo, entonces $K[x]$ es un dominio euclidiano.

Teorema 2.4.5. *Si K es un campo, entonces $K[x]$ es un dominio euclidiano.*

Demostración. Como K es un campo, entonces K es un dominio entero, de donde por la proposición 2.3.1, $K[x]$ es un dominio entero.

La aplicación

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

$$\delta : K^*[x] \to \mathbb{Z}^+, \left(K^*[x] = K[x] - \{0\}\right)$$

definida por $\delta(f(x)) = grad(f(x))$, $f(x) \in K^*[x]$, cumple con las condiciones requeridas en la definición 2.3.3. En efecto, si $f(x) \neq 0$ y $g(x) \neq 0$, se tiene que $grad(f(x)) \geq 0$ y $grad(g(x)) \geq 0$, en consecuencia

$$grad(f(x)g(x)) \geq grad(f(x)), f(x), g(x) \in K^*[x],$$

puesto que $grad(f(x)g(x)) = grad(f(x)) + grad(g(x))$.

Por otra parte, por el algoritmo de la división para polinomios, se tiene:

para todo $f(x),\ g(x) \in K[x]$, existen $d(x), r(x) \in K[x]$ tal que $f(x) = g(x)d(x) + r(x)$, en donde $\delta(r(x)) < \delta(d(x))$. ■

Teorema 2.4.6. *Sea K un campo. Entonces,*

1. *cada par de polinomios $f(x)$ y $g(x)$ en $K[x]$ tiene un máximo común divisor $d(x)$ que puede ser expresado como $d(x) = r(x)f(x) + s(x)g(x)$, con $r(x)$ y $s(x)$ en $K[x]$;*

2. *$K[x]$ es un dominio de ideales principales;*

3. *$K[x]$ es un dominio de factorización única;*

4. *si $f(x) \in K[x]$, entonces $K[x] \big/ \langle f(x) \rangle$ es un campo si y solo si $f(x)$ es irreducible.*

Demostración. Si K es un campo, entonces por el teorema anterior $K[x]$ es un dominio euclidiano.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

1. Sea $d(x)$ el polinomio mónico de grado mínimo en el conjunto

$$S = \left\{ p(x)f(x) + q(x)g(x) \,/\, p(x), q(x) \in K[x] \right\}$$

Como $d(x) \in S$, entonces $d(x) = r(x)f(x) + s(x)g(x)$, donde $r(x), s(x) \in K[x]$.

- Mostraremos primero que $d(x) \,\big|\, f(x)$ y $d(x) \,\big|\, g(x)$. En efecto, Por el algoritmo de la división existen polinomios $a(x)$ y $b(x)$ tal que $f(x) = d(x)a(x) + b(x)$, donde $b(x) = 0$ o bién $grad(b(x)) < grad(d(x))$.

  Por consiguiente,

$$\begin{aligned} b(x) &= f(x) - a(x)d(x) \\ &= f(x) - a(x)(r(x)f(x) + s(x)q(x)) \\ &= f(x)(1 - a(x)r(x)) + g(x)(-a(x)s(x)) \end{aligned}$$

  es decir $b(x)$ es combinación lineal de $f(x)$ y $g(x)$, de donde $b(x) \in S$ ($\longrightarrow\!\!\!\!\longleftarrow$).

  Luego, $b(x) = 0 \;\Rightarrow\; f(x) = d(x)a(x) \;\Rightarrow\; d(x) \,\big|\, f(x)$.

  En forma similar se muestra que $d(x) \,\big|\, g(x)$; se sigue que $d(x) \,\big|\, f(x)$ y $d(x) \,\big|\, g(x)$.

- Supongamos que $d'(x)$ es otro divisor común de $f(x)$ y $g(x)$. Debemos mostrar que $d'(x) \,\big|\, d(x)$. En efecto,

  puesto que $d'(x) \,\big|\, f(x)$, entonces existe $u(x)$ tal que

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

$$f(x) = d'(x)u(x),$$

puesto que $d'(x) \mid g(x)$, entonces existe $v(x)$ tal que

$$g(x) = d'(x)v(x).$$

Luego, en $d(x) = r(x)f(x) + s(x)g(x)$, tenemos:

$$\begin{aligned} d(x) &= r(x)(d'(x)u(x)) + s(x)(d'(x)v(x)) \\ d(x) &= d'(x)(r(x)u(x) + s(x)v(x)) \end{aligned}$$

Así, $d'(x) \mid d(x)$.

Por tanto, $d(x) = \text{MCD}\big(f(x), g(x)\big)$.

2. Como $K[x]$ es un dominio euclidiano, entonces por el teorema 2.3.2, $K[x]$ es un dominio de ideal principal (DIP).
3. Si $K[x]$ es un dominio euclidiano, entonces por el corolario 2.3.1, $K[x]$ es un dominio de factorización única (DFU).
4. Por el teorema 2.3.3, $f(x)$ es irreducible si y solo si $K[x] \big/ \langle f(x) \rangle$ es un campo.

■

Observación. Si $\text{MCD}\big(f(x), g(x)\big) = 1$, se dice que $f(x)$ y $g(x)$ son *coprimos* o *primos relativos.*

Teorema 2.4.7. *Sea K un campo y sea $c \in K$. Entonces se tiene un homomorfismo $\phi_c : K[x] \to K$ definida por*

$$\phi_c(f(x)) = f(c) = a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n,$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

donde $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.

Demostración. Sean

$$\begin{aligned} f(x) &= \sum_{i=0}^{n} a_i x^i = a_0x^0 + a_1x^1 + \cdots + a_nx^n \\ g(x) &= \sum_{i=0}^{m} b_i x^i = b_0x^0 + b_1x^1 + \cdots + b_mx^m \end{aligned}$$

tal que $f(x),\ g(x) \in K[x]$.

- Si $f(x),\ g(x) \in K[x]$, entonces $\phi_c[f(x) + g(x)] = \phi_c(f(x)) + \phi_c(g(x))$.

  En efecto,

$$\begin{aligned} \phi_c[f(x) + g(x)] &= \phi_c[(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots] \\ &= (a_0 + b_0) + (a_1 + b_1)c + (a_2 + b_2)x^2 + \cdots \\ &= (a_0 + a_1c + a_2c^2 + \cdots) + (b_0 + b_1c + b_2c^2 + \cdots) \\ &= f(c) + g(c) \\ &= \phi_c(f(x)) + \phi_c(g(x)) \end{aligned}$$

- Si $f(x),\ g(x) \in K[x]$, entonces $\phi_c[f(x)g(x)] = \phi_c(f(x))\phi_c(g(x))$.

  En efecto,

$$\begin{aligned} \phi_c[f(x)g(x)] &= \phi_c[a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + (a_nb_m)x^{n+m}] \\ &= a_0b_0 + (a_0b_1 + a_1b_0)\mathrm{c} + (a_0b_2 + a_1b_1 + a_2b_0)\mathrm{c}^2 + \cdots + (a_nb_m)\mathrm{c}^{n+m} \\ &= (a_0 + a_1c + a_2c^2 + \cdots + a_n\mathrm{c}^n)(b_0 + b_1c + b_2c^2 + \cdots + b_m\mathrm{c}^m) \\ &= f(c)g(c) \\ &= \phi_c(f(x))\phi_c(g(x)) \end{aligned}$$

  Por tanto, ϕ_c es un homomorfismo. ■

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Observación. La aplicación $\phi_c : K[x] \to K$ es llamado el *homomorfismo de evaluación* en c.

Definición 2.4.9. Sea K un campo y $f(x) \in K[x]$, diremos que $c \in K$ es un *cero* o *raíz* de $f(x)$, si $f(c) = 0$.

Teorema 2.4.8 (teorema del resto**).** *Sea K un campo y $c \in K$. Si $f(x) \neq 0$ es un polinomio en $K[x]$, entonces el resto al dividir $f(x)$ por un polinomio lineal $x - c$ es igual al valor $f(c)$. En particular, c es una raiz de $f(x)$ si y solo si $(x - c) \mid f(x)$.*

Demostración. Por el algoritmo de la división, existen únicos $q(x), r(x) \in K[x]$ tal que

$$f(x) = (x - c)q(x) + r(x), \text{ con } grad(r(x)) < grad(x - c) = 1 \text{ (si } r(x) \neq 0)$$

Así $grad(r(x)) = 0$, es decir $r(x) = r$ (es una constante).

Como la evaluación en c es un homomorfismo $K[x] \to K$, se tiene que

$$f(c) = (c - c)q(c) + r = r$$

En particular,

$$\begin{aligned} f(c) = 0 \quad &\Leftrightarrow \quad r = 0 \quad \Leftrightarrow \quad f(x) = (x - c)q(x) \\ &\Leftrightarrow \quad (x - c) \mid f(x) \ \blacksquare \end{aligned}$$

2.3.4. Polinomios irreducibles.

Definición 2.3.10. Sea K un campo. Un polinomio no constante $f(x) \in K[x]$ es *irreducible* sobre K, si no es posible factorizarlo en la forma

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

$$f(x) = p(x)q(x)$$

donde $p(x), q(x) \in K[x]$ son polinomios no constantes, tales que sus grados son menores que el grado $f(x)$.

Teorema 2.3.9. *Sea K un campo y $g(x)$ un polinomio irreducible en $K[x]$. Entonces $K[x]\big/\langle g(x)\rangle$ es un campo isomorfo al campo K.*

Demostración. Por el teorema 2.3.7, sabemos que $K[x]\big/\langle g(x)\rangle$ es un campo. La aplicación $\varphi : K \to K[x]\big/\langle g(x)\rangle$, definida por

$$\varphi(a) = a + \langle g(x)\rangle, a \in K$$

es un homomorfismo. *En efecto,*

- Sean $a, b \in K$, entonces

$$\begin{aligned} \varphi(a+b) &= (a+b) + \langle g(x)\rangle \\ &= (a + \langle g(x)\rangle) + (b + \langle g(x)\rangle) \\ &= \varphi(a) + \varphi(b) \end{aligned}$$

- Sean $a, b \in K$, entonces

$$\begin{aligned} \varphi(ab) &= (ab) + \langle g(x)\rangle \\ &= (a + \langle g(x)\rangle)(b + \langle g(x)\rangle) \\ &= \varphi(a)\varphi(b) \end{aligned}$$

φ es un epimorfismo, puesto que para todo $a + \langle g(x)\rangle \in K[x]\big/\langle g(x)\rangle$ existe $a \in K$, tal que

$$f(a) = a + \langle g(x)\rangle$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

φ es un monomorfismo, *en efecto*

Sean $a,b \in K$, $a+\langle g(x)\rangle = b+\langle g(x)\rangle$ de aquí $(a-b)\in\langle g(x)\rangle$, luego $a=b$. ■

Teorema 2.3.10 (lema de Gauss**).** *Sea* $f(x)\in\mathbb{Z}[x]$ *un polinomio mónico. Si* $f(x)$ *admite una factorización* $f(x)=g(x)h(x)$ *con* $g(x),h(x)\in\mathbb{Q}[x]$ *entonces existen* $g_1(x),h_1(x)\in\mathbb{Z}[x]$ *con* $\partial(g_1(x))=\partial(g(x))$, $\partial(h_1(x))=\partial(h(x))$ *y tales que* $f(x)=g_1(x)h_1(x)$.

Demostración. Podemos asumir que:

$$\begin{aligned} g(x) &= \frac{c_1}{d_1}(a_0+a_1x+\cdots+a_mx^m) = \frac{c_1}{d_1}g'(x) \\ h(x) &= \frac{c_2}{d_2}(b_0+b_1x+\cdots+b_nx^n) = \frac{c_2}{d_2}h'(x) \end{aligned}$$

donde: los $\begin{cases} a_i \text{ son PESI} \\ b_i \text{ son PESI} \end{cases}$, al igual que $\begin{cases} c_1 \text{ y } d_1 \\ c_2 \text{ y } d_2 \end{cases}$.

Se sigue que:

$$\begin{aligned} f(x) &= g(x)h(x) \\ &= \frac{c_1c_2}{d_1d_2}g'(x)h'(x) \\ &= \frac{c}{d}g'(x)h'(x) \end{aligned}$$

donde $\frac{c}{d}$ es irreducible equivalente a $\frac{c_1c_2}{d_1d_2}$.

Luego,

$$df(x)=cg'(x)h'(x)$$

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Probaremos que $d = 1$ con lo que el teorema quedará demostrado. *En efecto,* supongamos que $d \neq 1$. Puesto que

$$\text{MCD}(c, d) = 1,$$

entonces existe $p \in \mathbb{Z}$ primo tal que $p \mid d$ y $p \nmid c$. También, puesto que los coeficientes a_i de $g'(x)$ son PESI, entonces existe algún coeficiente a_{i_0} tal que $p \nmid a_{i_0}$.

De la misma forma, existe un coeficiente b_{i_0} de $h'(x)$, tal que $p \nmid b_{i_0}$.

Sean $g''(x)$ y $h''(x)$ los polinomios de $\mathbb{Z}_p$ obtenidos a partir de $g'(x)$ y $h'(x)$ respectivamente reduciendo los coeficientes según la congruencia módulo p.

Puesto que, $p \mid d$, se tiene que $g''(x)h''(x) = 0$ en $\mathbb{Z}_p$. Pero $g''(x) \neq 0$, $h''(x) \neq 0$ y $\mathbb{Z}_p[x]$ es domino de integridad. Entonces obtenemos una contradicción. Así, $d = 1$.

Luego, $f(x) = g_1(x)h_1(x)$ y $\partial(g_1(x)) = \partial(g(x))$, $\partial(h_1(x)) = \partial(h(x))$. ■

Corolario 2.3.1. *Sea* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ *tal que sus coeficientes están en* $\mathbb{Z}$ *y* $a_0 \neq 0$. *Si* $f(x)$ *tiene un cero en* $\mathbb{Q}$, *entonces* $f(x)$ *tiene un cero* c *en* $\mathbb{Z}$, *más aún,* $c \mid a_0$.

Demostración. Si $a \in \mathbb{Q}$ es una raíz de $f(x)$, entonces $f(x)$ tiene un factor lineal $(x - a)$ en $\mathbb{Q}[x]$ por lema de Gauss,

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

$$f(x) = \underbrace{(x-c)}_{\in \mathbb{Z}[x]}\underbrace{\left(x^{n-1}+\cdots-\frac{a_0}{c}\right)}_{\in \mathbb{Z}[x]}$$

$$f(0) = (-c)\left(-\frac{a_0}{c}\right) = a_0$$

Notar que $c \in \mathbb{Z}$ y es una raiz de $f(x)$ del mismo modo, $\frac{a_0}{c} \in \mathbb{Z}$ esto es, $c \mid a_0$ ■

Teorema 2.3.11 (criterio de Eisenstein**).** *Sea* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *un polinomio en* $\mathbb{Z}[x]$ *y* p *un número primo. Si* $p \mid a_i$ *para* $i = 0,1,\ldots,n-1$, $p \nmid a_n$ *y* $p^2 \nmid a_0$, *entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$.

Demostración. Por el lema de Gauss, es suficiente probar que $f(x)$ no es factorizable en factores de grado menor que el grado de $f(x)$ en $\mathbb{Z}[x]$.

Supongamos por contradicción que

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s)$$

con $b_i, c_j \in \mathbb{Z}$, $r + s = n$, $r, s \geq 1$.

Puesto que $\begin{cases} p \mid a_0 = b_0c_0 \\ p^2 \nmid a_0 = b_0c_0 \end{cases}$, entonces podemos suponer que $p \mid b_0$ y $p \nmid c_0$.

Puesto que $p \nmid a_n = b_rc_s$, entonces $p \nmid b_r$ y $p \nmid c_s$.

Si k es el primer indice, tal que $p \nmid b_k$, $k \leq r < n$, entonces

$$p \mid a_k = \underbrace{b_0c_k + b_1c_{k-1} + \cdots + b_kc_0}_{p \text{ divide a cada uno de estos sumandos}} \Rightarrow \begin{cases} p \mid b_kc_0 \\ p \nmid b_k \end{cases}$$

de donde: $p \mid c_0$ esto es una contradicción, esto se debe por haber supuesto que $f(x)$ es reducible. Por lo tanto $f(x)$ es irreducible. ■

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2.4. Campos y sus extensiones

Definición 2.4.1 (campo**).** Un *campo* es un conjunto K, diferente del vacío, con dos operaciones $(+)$ y $(\cdot)$ (suma y multiplicación) tales que verifican:

a) $(K,+)$ es un grupo abeliano,

b) $(K-\{0\},\cdot)$ es un grupo abeliano,

c) La multiplicación es distributiva respecto de la suma

$a\cdot(b+c)=a\cdot b+a\cdot c,\ \forall a,b,c\in K$

2.4.1. Característica de un campo y subcampos.

Definición 2.4.2. Si en un campo K existe $n\in\mathbb{Z}^+$ tal que

$n\cdot a=\underbrace{a+a+\cdots+a}_{n\text{ veces}}=0$, para todo $a\in K$, entonces

$m=\min\{n\in\mathbb{Z}^+ \,/\, n\cdot a=0,\ \forall a\in K\}$ es *característica* de K.

Si tal n no existe se dice que el campo K es de característica 0.

Teorema 2.4.1. *La característica de un campo es cero o bien un número primo.*

Demostración. Los campos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son de característica cero.

Sea K un campo de característica $n\neq 0$ y supongamos que n no es primo,

$$n=r\cdot s;\ \text{con}\ 1<r,\ s<n,$$

por la propiedad minimal de n, se tiene que $r\cdot 1\neq 0$ y $s\cdot 1\neq 0$, además

$$(r\cdot 1)(s\cdot 1)=(r\cdot s)\cdot 1=n\cdot 1=0$$

y esto es imposible ya que K es un campo, y no tiene divisores de cero. Luego, n es un número primo, por tanto la característica de K es un número primo. ■

Corolario 2.4.1. *Si p es primo, entonces $\mathbb{Z}_p$ es un campo.*

Demostración. Como $\mathbb{Z}_p$ es un dominio entero de p elementos, por el teorema 2.2.1 se concluye que $\mathbb{Z}_p$ es un campo ■

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Definición 2.4.3 (Subcampo**).** Sea K un campo. Un *subcampo* de K es un subconjunto F de K que, con las operaciones de K, tiene estructura de campo no trivial.

Observación. La intersección de una familia no vacía de subcampos de un campo K, es un subcampo de K.

Definición 2.4.4. Sea K un campo. El subcampo primo (o campo primo) de K es la intersección de todos los subcampos de K. Es decir, el subcampo primo de K es el menor subcampo de K.

Teorema 2.4.2. *Si F es un subcampo primo de un campo K, entonces $F \cong \mathbb{Q}$ o $F \cong \mathbb{Z}_p$ para algún primo p.*

Demostración. Sean 0_K y 1_K, respectivamente, identidades de las operaciones suma y producto en el campo K.

Claramente, $0_K \in F$ y $1_K \in F \Rightarrow n \cdot 1_K \in F,\ \forall n \in \mathbb{Z} \Rightarrow \{n \cdot 1_K \,/\, n \in \mathbb{Z}\} \subset F$.

Definamos $\varphi : \mathbb{Z} \to K$ por $\varphi(n) = n \cdot 1_K$. Se demuestra que φ es un homomorfismo de anillos.

El $\ker\varphi$ es un ideal de $\mathbb{Z}$ y $\operatorname{Im}\varphi = \{n \cdot 1_K \,/\, n \in \mathbb{Z}\} \subset F$. Entonces se pueden presentar los siguientes casos:

a) $\ker\varphi = \{0\} \Rightarrow \varphi$ es inyectivo: si $0 \neq n \in \mathbb{Z} \Rightarrow \varphi(n) \neq 0$ en K, de donde $\varphi(n)$ es invertible, entonces existe el homomorfismo de campos $\hat{\varphi} : \mathbb{Q} \to K$, tal que el diagrama conmuta.

Si $\hat{\varphi}$ es inyectivo, entonces $\varphi \cong \operatorname{Im}\varphi = \left\{ \dfrac{\varphi(n)}{\varphi(m)} \Big/ n, m \in \mathbb{Z}, m \neq 0 \right\}$

Como $\operatorname{Im}\varphi \subset F$ y F es un subcampo, entonces

$$\begin{cases} \operatorname{Im}\hat{\varphi} \subset F \\ \mathbb{Q} \cong \operatorname{Im}\hat{\varphi}, \text{de donde } \mathbb{Q} \text{ es un subcampo de } K \end{cases} \Rightarrow \operatorname{Im}\varphi = F$$

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

Por tanto, $F \cong \mathbb{Q}$.

b) $\ker\varphi \neq \{0\}$, entonces existe $p \in \mathbb{Z}^+$ tal que $\ker\varphi = \langle p \rangle$ y existe el homomorfismo inyectivo de anillos $\bar{\varphi} : \mathbb{Z}_p \to K$, tal que el diagrama conmuta:

con $\mathrm{Im}\bar{\varphi} = \mathrm{Im}\varphi$.

Como $\mathrm{Im}\bar{\varphi} \subset K$ es un subanillo y K es campo, entonces $\mathrm{Im}\bar{\varphi}$ es un dominio entero.

Luego, $\mathbb{Z}_p$ es un dominio entero, entonces $\mathbb{Z}_p$ es un campo y p es primo.

De donde: $\mathrm{Im}\varphi \cong \mathbb{Z}_p$ es un subcampo de K y $\mathrm{Im}\varphi \subset F$ lo que implica $F = \mathrm{Im}\varphi$

Por tanto, $F \cong \mathbb{Z}_p$, ■

2.4.2. Espacios vectoriales

Definición 2.4.5. Un conjunto V se dice ser un espacio vectorial sobre un campo F si V es un grupo abeliano bajo la adción (denotado por +), tal que para cada $a \in F$ y $v \in V$ existe $av \in V$, de tal modo que para cada $a, b \in F$ y $u, v \in V$ se cumplen las siguientes condiciones:

1. $a(v+u) = av + au$
2. $(a+b)v = av + bv$
3. $a(bv) = (ab)v$
4. $1v = v$.

Definición 2.4.6 (subespacio**).** Sea V un espacio vectorial sobre un campo F y sea U un subconjunto de V. Se dice que U es un subespacio de V si U es también un espacio vectorial sobre F bajo las operaciones de V.

Dependencia e independencia lineal.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Definición 2.4.7. Un conjunto S de vectores se dice que son linealmente dependiente sobre un campo F si hay vectores $v_1, v_2, \ldots, v_n$ de S y elementos $a_1, a_2, \ldots, a_n$ de F no todos igual a cero, tal que $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0$. Un conjunto de vectores que no es linealmente dependiente sobre F se llama linealmente independiente sobre F.

Definición 2.4.8 (Base**).** Sea V un espacio vectorial sobre un campo F. Un subconjunto B de V es llamado una base para V si B es linealmente independiente sobre F y cada elemento de V es una combinación lineal de elementos de B.

2.4.3. Extensión de campos.

Definición 2.4.9. Sean K y L dos campos. Se dice que L es una *extensión* de K, si existe un homomorfismo de campos $\varphi : K \to L$, donde K es denominado el campo de base. En general usaremos la *notación* $L : K$ para indicar que L es una extensión de K.

Observación. Como un homomorfismo de campos es siempre inyectivo, podemos identificar los elementos de K con sus imágenes en L. Esto nos permite ver a K como un subcampo de L y por eso también se puede escribir $K \subseteq L$. Entonces L puede ser considerado como un *espacio vectorial* sobre K.

Grado de una extensión.

Definición 2.4.10. Sea $L : K$ una extensión de campos. Si L, considerado como un espacio vectorial sobre K es de dimensión finita, entonces L se llama una extensión finita de K. A la dimensión de este espacio vectorial se le llama *grado de la extensión* y se representa como $[L : K]$.

Proposición 2.4.1. *Si $L : K$ es una extensión de campos, entonces $[L : K] = 1$ si y solo si $L = K$.*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Demostración.

$\Rightarrow]$ Si $[L:K]=1$, entonces $L=K$.

En efecto, sea $\{x\}$ una base de L sobre K, donde $x\neq 0$. Así en particular debe existir $a\in K$, tal que $1=ax$, de donde $x=\dfrac{1}{a}\in K$.

Para cada $y\in L$ existe $b\in K$ tal que

$$\begin{aligned} y &= bx \\ y &= b\left(\frac{1}{a}\right) = \frac{b}{a}\in K \end{aligned}$$

luego $y\in K$. Por lo tanto $L=K$.

$\Leftarrow]$ Si $L=K$, entonces $[L:K]=1$.

En efecto, si $L=K$, entonces $\{1\}$ es una base de L sobre K ya que cualquier $x\in L$ se escribe como $x=x1$, donde $x\in K$. Así $[L:K]=1$ ■

Teorema 2.4.3 (Teorema de transitividad de grados**).** *Sean E, L y K campos. Si E es una extensión finita de L y L una extensión finita de K, entonces E es una extensión finita de K y $[E:K]=[E:L][L:K]$.*

Demostración. Sea $X=\{x_1,x_2,\ldots,x_n\}$ una base de E sobre L y $Y=\{y_1,y_2,\ldots,y_m\}$ una base de L sobre K. Es suficiente probar que

$$YX=\{y_jx_i \,/\, 1\leq j\leq m, 1\leq i\leq n\}$$

es una base de E sobre K. En efecto, sea $a\in E$. Entonces hay elementos $\beta_1,\beta_2,\ldots,\beta_n\in L$ tal que

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

$$a = \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n = \sum_{i=1}^{n} \beta_i x_i$$

y para cada $i = 1,2,\ldots,n$, hay elementos $\alpha_{i1},\alpha_{i2},\ldots,\alpha_{im} \in K$, tal que

$$\beta_i = \alpha_{i1} y_1 + \alpha_{i2} y_2 + \cdots \alpha_{im} y_m = \sum_{j=1}^{m} \alpha_{ij} y_j$$

Así,

$$\begin{aligned} a &= \sum_{i=1}^{n} \beta_i x_i \\ a &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij} y_j \right) x_i = \sum_{ij} \alpha_{ij} (y_j x_i) \end{aligned}$$

lo cual prueba que XY es un sistema de generadores de E sobre K.

Ahora supongamos que hay elementos α_{ij} en K tal que

$$0 = \sum_{i,j} \alpha_{ij} (y_j x_i) = \sum_{i} \left(\sum_{j} \alpha_{ij} y_j \right) x_i .$$

Puesto que $\sum_j \alpha_{ij} y_j \in L$ y X es una base de E sobre L, entonces

$$\sum_j \alpha_{ij} y_j = 0$$

Como $\alpha_{ij} \in K$ y Y es una base de L sobre K, entonces

$$\alpha_{ij} = 0, \text{ para cada } i = 1,\ldots,n \text{ y para cada } j = 1,\ldots,m$$

lo cual prueba que el conjunto XY es linealmente independiente. ■

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2.4.4. Extensiones y polinomios.

Definición 2.4.11. Sea K un subcampo del campo L y sea S cualquier subconjunto de L. Entonces, el campo $K(S)$ se define como la intersección de todos los subcampos de L conteniendo $K \cup S$. Es claro que $K(S)$ es el subcampo más pequeño conteniendo $K \cup S$, y es una extensión de K generado por S. Para S finito, $S = \{u_1,\ldots,u_n\}$, se escribe $K(S) = K(u_1,\ldots,u_n)$. Si S consta de un solo elemento $u \in L$, entonces $K(u)$ se llama *extensión simple* de K y u se llama un elemento primitivo de L.

Teorema 2.4.4. *Sea $L : K$ una extensión de campos y $u \in L$. Entonces o bien,*

1. *$K(u)$ es isomorfo a $K(x)$, donde $K(x)$ es el campo de todas las formas racionales con coeficientes en K; o bien,*
2. *existe un único polinomio mónico irreducible $p(x)$ en $K[x]$ con la propiedad de que, para todo $f(x)$ en $K[x]$ se verifica:*

- *$f(u) = 0$ si y solo si $p(x) \mid f(x)$;*
- *el campo $K(u)$ coincide con $K[u]$, el anillo de todo los polinomios en u con coeficientes en K; y*
- *$[K[u] : K] = grad(p(x))$.*

Demostración.

1. Supongamos que no existe un polinomio $f(x) \neq 0$ tal que $f(u) = 0$, esto en particular indica que $u \notin K$ ya que de otro modo se podría tomar que $f(x) = x - u$. Entonces hay una aplicación $\varphi : K(x) \to K(u)$ definida por $\varphi\left(\dfrac{f(x)}{g(x)}\right) = \dfrac{f(u)}{g(u)}$, donde $g(u) = 0$ si $g(x) = 0$. Claramente φ es un homomorfismo sobreyectivo.

   Mostremos que φ esta bien definido y es inyectiva para ello sean

   $\dfrac{f(x)}{g(x)}, \dfrac{p(x)}{q(x)} \in K(x)$, con $g(x) \neq 0$, $q(x) \neq 0$, entonces

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

$$\begin{array}{rcl} \varphi\left(\dfrac{f(x)}{g(x)}\right) = \varphi\left(\dfrac{p(x)}{q(x)}\right) & \Leftrightarrow & \dfrac{f(u)}{g(u)} = \dfrac{p(u)}{q(u)} \\ & \Leftrightarrow & \dfrac{f(u)}{g(u)} - \dfrac{p(u)}{q(u)} = 0 \\ & \Leftrightarrow & f(u)q(u) - p(u)g(u) = 0 \quad \text{en } L \\ & \Leftrightarrow & f(x)q(x) - p(x)g(x) = 0 \quad \text{en } K[x] \\ & \Leftrightarrow & \dfrac{f(u)}{g(u)} = \dfrac{p(u)}{q(u)} \quad \text{en } K[x] \end{array}$$

Por consiguiente $\varphi : K(x) \to K(u)$ es un isomorfismo.

2. Ahora supongamos que existe un polinomio $g(x) \neq 0$ en $K[x]$ tal que $g(u) = 0$. Mas aún admitamos que $g(x)$ es un polinomio de grado mínimo tal que $g(u) = 0$.

   Si a es el coeficiente principal de $g(x)$ entonces $p(x) = \dfrac{g(x)}{a}$ es un polinomio mónico de grado mínimo tal que $p(u) = 0$.

   - $\Leftarrow]$ Si $p(x) \mid f(x)$ entonces $f(x) = p(x)h(x)$, $h(x) \in K[x]$; de donde $f(u) = 0$.

     $\Rightarrow]$ Supongamos que $f(u) = 0$ por el algoritmo de la división para polinomios existen $q(x), r(x) \in K[x]$ tal que

     $$f(x) = q(x)p(x) + r(x), grad(r(x)) < grad(p(x))$$

     luego, $0 = f(u) = q(u)p(u) + r(u) = 0 + r(u) = r(u)$, de donde $r(u) = 0$, esto es una contradicción a menos que $r(x) = 0$. Por lo tanto $f(x) = q(x)p(x)$ esto es $p(x) \mid f(x)$.

     Para mostrar que el polinomio $p(x)$ es único, supongamos que existe otro polinomio $p'(x) \in K[x]$ que tiene las mismas características. Entonces $0 = p(u) = p'(u)$ esto es $p(x) \mid p'(x)$ y $p'(x) \mid p(x)$, puesto que ambos polinomios son mónicos, se concluye que $p'(x) = p(x)$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Para mostrar que $p(x)$ es irreducible, supongamos por contradicción que $p(x)$ es no irreducible esto es existen $a(x), b(x) \in K[x]$ tal que $p(x) = a(x)b(x)$, con $grad(a(x)) < grad(p(x))$, $grad(b(x)) < grad(p(x))$. Entonces $0 = p(u) = a(u)b(u)$ de donde $a(u) = 0 \ \vee \ b(u) = 0$. Esto es una contradicción ya que el grado de $a(x)$ y $b(x)$ es menor al grado de $p(x)$, de aquí $p(x)$ es irreducible.

- Sea $\frac{f(u)}{g(u)}$ un elemento arbitrario en $K(u)$, donde $g(u) \neq 0$. Entonces $p(x) \nmid g(x)$ y puesto que $p(x)$ solo acepta como divisores a 1 y $p(x)$, entonces existen polinomios $s(x)$ y $t(x)$ en $K[x]$ tal que

$$s(x)q(x) + t(x)p(x) = 1$$

evaluando en u se tiene:

$$g(u)s(u) = 1$$

luego,

$$\frac{f(u)}{g(u)} = f(u)s(u) \in K[u]$$

de donde $K(u) = K[u]$.

- Finalmente supongamos $grad(p(x)) = n$ y sea $h(u) \in K[u] = K(u)$, por el algoritmo de la división para polinomios, existen $q(x)$, $r(x) \in K[x]$ tal que

$$h(x) = q(x)p(x) + r(x), \ grad(r(x)) < grad(p(x)) = n$$

evaluando en u se tiene: $h(u) = r(u)$, así existen $a_0, a_1, a_2, \ldots, a_n \in K$ tal que

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$$

puede ser que algunos de los coeficientes a_i sea nulo, luego se sigue que

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

$$h(u) = r(u) = a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$$

esto es $\{1, u, u^2, \ldots, u^{n-1}\}$ genera a $K[u]$.

Luego, mostraremos que $\{1, u, u^2, \ldots, u^{n-1}\}$ es linealmente independiente sobre K para ello, supongamos que

$$b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1} = 0$$

donde $b_i \in K$, para $i = 0,1,\ldots,n-1$, entonces $b_i = 0$, por que de otra forma existiria el polinomio

$$h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}, \text{ tal que } h(u) = 0$$

y que su grado es menor que n, lo cual es una contradicción.

Por consiguiente $\{1, u, u^2, \ldots, u^{n-1}\}$ es una base para $K[u]$ sobre K. Por lo tanto $[K[u] : K] = grad(p(x)) = n$. ■

Definición 2.4.12. Sea K un campo. Si u tiene un polinomio mínimo sobre K, se dice que u es *algebraico* sobre K y que $K(u) : K$ es un *extensión algebraica simple*. Si $K(u)$ es isomorfo al campo $K(x)$, se dice que u es *trascendente* sobre K y que $K(u) : K$ es una *extensión trascendente simple*.

Teorema 2.4.5. *Si $K(u) : K$ es una extensión trascendente simple de campos, entonces $[K(u) : K] = \infty$.*

Demostración. Veamos que $\{1, u, u^2, \ldots, u^n, \ldots\}$ es un conjunto linealmente independiente de $K(u)$ sobre K. Sea $t \in \mathbb{N}$ y sean $a_0, a_1, \ldots, a_t \in K$ tales que

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

$$a_0 + a_1u + a_2u^2 + \cdots + a_tu^t = 0.$$

Como u es trascendente sobre K, $f(u) \neq 0$, $\forall f(x) \neq 0$ en $K[u]$; en particular, si $a_0 + a_1x + a_2x^2 + \cdots + a_tx^t = p(x)$ y $p(u) = 0$, necesariamente $p(x) = 0$, luego $a_i = 0, \forall i$ ■

Definición 2.4.13. Una extensión de campos $L : K$ se dice ser una *extensión algebraica* si cada elemento de L .es algebraico sobre K. En caso contrario se dice que $L : K$ es una *extensión trascendente*.

Teorema 2.4.6. *Toda extensión finita es algebraica.*

Demostración. Sea $F : K$ una extensión finita. Probaremos que para cada $u \in F$ es algebraico sobre K. Se tiene $K \subset K(u) \subset F$. En virtud del teorema del grado $[K(u) : K]$ es también finito ya que divide a $[F : K]$. Si $[K(u) : K] = n$ y si los $n+1$ elementos $1, u, \ldots, u^n \in K(u)$ son diferentes, entonces son necesariamente linealmente dependientes sobre K y por lo tanto existen $a_0, a_1, \ldots, a_n \in K$, no todos nulos, tales $a_0 + a_1u + \cdots + a_nu^n = 0$. El polinomio no nulo $f(x) = a_nx^n + \cdots + a_1x + a_0 \in K[x]$ es tal que $f(u) = 0$. Si por el contrario, existen $i \neq j$, con $0 \leq i < j \leq n$, tales que $u^i = u^j$, entonces $u^{j-i} = 1$, lo que indica que u es una raiz del polinomio $x^{j-i} - 1 \in K[x]$. En cualquier caso resulta que u es algebraico sobre K. ■

Teorema 2.4.7. *Sean $L : K$ y $E : L$ extensiones de campos, y $u \in E$. Si u es algebraico sobre K, entonces es también algebraico sobre L.*

Demostración. Puesto que si u es algebraico sobre K, entonces existe un polinomio distinto de cero $f(x)$ en $K[x]$ tal que $f(u) = 0$. Como $f(x)$ pertenece a $L[x]$, se deduce que u es algebraico sobre L. ■

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

2.4.5. Polinomios y extensiones.

Si un polinomio irreducible $f(x) \in K[x]$, donde K es un campo, tiene una raíz u tal que $u \notin K$, es posible construir, a partir de K y $f(x)$, un campo L tal que $K \subset L$ y $u \in L$.

Teorema 2.4.8. *Sea K un campo y $f(x)$ un polinomio irreducible en $K[x]$, entonces existe una extensión L de K que contiene por lo menos una raíz de $f(x)$.*

Demostración. Como $K[x]$ es un dominio de factorización única, entonces $f(x)$ tiene un factor irreducible. Sea $p(x)$ dicho factor irreducible, luego el ideal de $K[x]$ es maximal, de donde por el teorema 2.3.3 el anillo cociente $L = K[x] \big/ \langle p(x) \rangle$ es un campo.

- K es un subcampo de L. Para ello es suficiente mostrar que existe una inyección de K en L.

  En efecto, podemos definir $\psi : K \to L$ por $\psi(a) = a + \langle p(x) \rangle$ para $a \in K$.

  Se demuestra que ψ es un homomorfismo de anillos. Además, ψ es inyectivo. Es decir, si $a, b \in K$ tales que $\psi(a) = \psi(b)$, entonces $a = b$. *En efecto,* de $\psi(a) = \psi(b)$ tenemos que $a + \langle p(x) \rangle = b + \langle p(x) \rangle$, de donde $a - b \in \langle p(x) \rangle$. Esto significa que $a - b = p(x)q(x)$ para algún $q(x) \in K[x]$, como $p(x)$ es de grado mínimo que está en $\langle p(x) \rangle$, se debe tener $q(x) = 0$, de donde $a = b$.

  Luego, L es una extensión de K.

- Existe $u = x + \langle p(x) \rangle \in L$ tal que $f(u) = 0$.

  En efecto, considerando el homomorfismo de evaluación

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

$\varphi_u : K[x] \to L$, para $p(x) = a_0 + a_1x + \cdots + a_nx^n$ donde los $a_i \in K$ y $u = x + \langle p(x) \rangle$ tenemos que

$$\begin{aligned} p(u) = \varphi_u(p(x)) &= a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n \\ &= (a_0 + a_1x + \cdots + a_nx^n) + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle \\ &= \langle p(x) \rangle \\ &= 0 \, en \, L \end{aligned}$$

Por otro lado, recordando que $p(x) | f(x)$, existe $q(x) \in K[x]$ tal que $f(x) = p(x)q(x)$, de donde, se deduce que $f(u) = p(u)q(u) = 0$, por que $p(u) = 0$.

Por lo tanto $u \in L$ es una raíz de $f(x)$. ■

Teorema 2.4.9. *Sean $L : K$ y $L' : K'$ dos extensiones de campos y $\varphi : K \to K'$ un isomorfismo con extensión canónica $\hat{\varphi} : K[x] \to K'[x]$. Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomio irreducible en $K[x]$ y sea $f'(x) = \hat{\varphi}(f(x)) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$. Sea $u \in L$ una raíz de $f(x)$ y $u' \in L'$ una raíz del polinomio $f'(x)$. Entonces φ se extiende a un isomorfismo $\overline{\varphi} : K[u] \to K'[u']$ tal que $\overline{\varphi}(u) = u'$.*

Demostración. Los elementos de $K[u]$ son de la forma

$$b_0 + b_1u + \cdots + b_{n-1}u^{n-1}$$

donde $b_i \in K$, $i = 0,1,2,\ldots,n-1$.

La suma en $K[u]$ es la habitual de polinomios, para la multiplicación se debe tener en cuenta la ecuación

$$u^n = -\frac{1}{a_n}(a_{n-1}u^{n-1} + \cdots + a_0)$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Definamos la aplicación $\overline{\varphi}$ por

$$\overline{\varphi}(b_0 + b_1u + \cdots + b_{n-1}u^{n-1}) = \overline{\varphi}(b_0) + \overline{\varphi}(b_1)u' + \cdots + \overline{\varphi}(b_{n-1})(u')^{n-1}$$

es decir, si $p(x) \in K[x]$ con $grad(p(x)) < n$,

$$\overline{\varphi}(p(u)) = \Big(\hat{\varphi}\big(p(x)\big)\Big)(u')$$

Se verifica que $\overline{\varphi}$ es inyectiva y sobreyectiva, además $\overline{\varphi}$ es una extensión de φ.

Sean $p(x), q(x) \in K[x]$ con $grad(p(x)) < n$, $grad(q(x)) < n$ tal que $\overline{\varphi}(p(u)) = \overline{\varphi}(q(u))$ entonces $\Big(\hat{\varphi}\big(p(x)\big)\Big)(u') = \Big(\hat{\varphi}\big(q(x)\big)\Big)(u')$ se sigue que $\overline{\varphi}$ es isomorfismo, luego $\overline{\varphi}$ es inyectiva.

Sean $p(x), q(x) \in K[x]$ con $grad(p(x)) < n-1$, se verifica que

$$\overline{\varphi}(p(u) + q(u)) = \overline{\varphi}(p(u)) + \overline{\varphi}(q(u))$$

Mostraremos que $\overline{\varphi}$ preserva la multiplicación. En efecto, supongamos que la multiplicación de $p(u)$ y $q(u)$ se reduce a $h(u)$, donde $grad(h(x)) \leq n-1$, mas precisamente hacemos uso del algoritmo de la división en $K[x]$ para obtener

$$\begin{array}{rcl} p(x)q(x) & = & a(x)b(x) + h(x), grad(h(x)) < n \\ \overline{\varphi}(p(u)q(u)) & = & \overline{\varphi}(h(u)) = \hat{\varphi}\ h(x)\ \ (u') \end{array}$$

por otro lado el isomorfismo $\hat{\varphi}$ asegura que el algoritmo de la división en $K[x]$ se vea como

$$\hat{\varphi}(p(x))\hat{\varphi}(q(x)) = \hat{\varphi}(a(x))\hat{\varphi}(b(x)) + \hat{\varphi}(h(x))$$

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Así

$$\begin{aligned}
\overline{\varphi}(p(u))\overline{\varphi}(q(u)) &= \hat{\varphi}(p(x))\ (u')\ \hat{\varphi}(q(x))\ (u') \\
&= \hat{\varphi}(p(x))\hat{\varphi}(q(x))\ (u') \\
&= \hat{\varphi}(p(x))\hat{\varphi}(q(x))\ (u') \\
&= \hat{\varphi}(a(x))\hat{\varphi}(b(x)) + \hat{\varphi}(h(x))\ (u') \\
&= \hat{\varphi}(a(x))\ (u')\ \hat{\varphi}(b(x))\ (u') + \ \hat{\varphi}(h(x))\ (u') \\
&= \hat{\varphi}(h(x))\ (u'), \text{ ya que } \ \hat{\varphi}(b(x))\ (u') = 0 \\
\overline{\varphi}(p(u))\overline{\varphi}(q(u)) &= \overline{\varphi}(p(u)q(u))
\end{aligned}$$

puesto que $\hat{\varphi}$ es un isomorfismo y $b(x)$ es el polinomio mínimo de u, entonces $\hat{\varphi}(a(x))$ es el polinomio mínimo de u'.

Luego, $\overline{\varphi} : K[x] \to K'[x]$ es un isomorfismo. ■

2.5. Campos factorizantes

Definición 2.5.1. Sea $L : K$ una extensión de campos y $f(x)$ un polinomio no constante en $K[x]$. Se dice que L es un *campo factorizante* para $f(x)$ sobre K, si

a) $f(x)$ se factoriza completamente sobre L;

b) $f(x)$ no se factoriza completamente sobre cualquier subcampo propio F de L.

Teorema 2.5.1. *Si K es un campo y $f(x) \in K[x]$ un polinomio de grado n, entonces existe un campo factorizante L para $f(x)$ sobre K, y $[L : K] \leq n!$.*

Demostración. El polinomio $f(x)$ tiene un factor irreducible por lo menos $g(x)$ (puede ser el propio $f(x)$). Así, se forma el campo $E_1 = K[x] \big/ \langle g(x) \rangle$ y sus elementos se denota como $u = x + \langle g(x) \rangle$. Entonces u tiene un polinomio mínimo

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

$g(x)$, y $g(u)=0$. Por lo tanto $g(x)$ tiene un factor lineal $y-u$ en el anillo de polinomios $E_1[y]$, es más $[E_1:K]=grad(g(x))\leq n$.

Luego, por inducción. Supongamos que para cada r en $\{1,2,\ldots,n-1\}$, se tiene una extensión E_r de K tal que $f(x)$ tiene un factor lineal r en $E_r[x]$, y

$$[E_r:K]\leq n(n-1)\cdots(n-r+1)$$

Así, en $E_r[x]$

$$f(x)=(x-u_1)(x-u_2)\cdots(x-u_r)f_r(x)$$

y $grad(f_r(x))=n-r$ y se repite el argumento del párrafo anterior, construyendo una extensión E_{r+1} de E_r donde $f_r(x)$ tenga un factor lineal $x-u_{r+1}$ y $[E_{r+1}:E_r]\leq n-r$. Luego,

$$[E_{r+1}:K]=[E_{r+1}:E_r][E_r:K]=n(n-1)\cdots(n-r)$$

Por inducción existe un campo E_n tal que $f(x)$ se divide completamente sobre E_n y $[E_n:K]\leq n!$.

Ahora sea $L=\mathbb{Q}(u_1,u_2,\ldots,u_n)\subseteq E_n$, donde $u_1,u_2\ldots u_n$ (no necesariamente distintos) son las raíces de $f(x)$ en E_n. Entonces $f(x)$ se divide completamente sobre L, y no se puede dividir sobre cualquier subcampo de L. ■

Teorema 2.5.2. *Sea $\varphi:K\to K'$ un isomorfismo de campos, extendiéndose a un isomorfismo $\hat{\varphi}:K[x]\to K'[x]$. Si L es un campo factorizante de $f(x)$ sobre K y*

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

L' es un campo factorizante de $f'(x) = \hat{\varphi}(f(x))$ sobre K', entonces existe un isomorfismo $\varphi^* : L \to L'$ que extiende φ.

Demostración. Supongamos que $grad(f(x)) = n$ y que en $L[x]$ se tiene la factorización

$$f(x) = a(x - u_1)(x - u_2)\cdots(x - u_n)$$

Donde $a \in K$ es el coeficiente principal de $f(x)$ y $u_1, u_2, \ldots, u_m$ no están en K y que $u_{m+1}, u_{m+2}, \ldots, u_n \in K$.

Demostraremos el teorema por inducción en m.
Si $m = 0$, entonces todas las raíces están en K, por lo que K es un campo factorizante de $f(x)$.

Por lo tanto, en $K[x]$, tenemos:

$$\hat{\varphi}(f(x)) = \varphi(u)(x - \varphi(u_1))(x - \varphi(u_2))\cdots(x - \varphi(u_n))$$

luego, K' es un campo factorizante de $\hat{\varphi}(f(x))$ y $\varphi^* = \varphi$.

Supongamos ahora que $m > 0$. Para cada campo E y cada polinomio $g(x)$ en $E[x]$ que tiene menos de m raíces fuera de E en un campo factorizante L de $g(x)$, todos los isomorfismos de E se puede extender a isomorfismos de L.

Nuestra hipótesis de que $m > 0$ implica que los factores irreducibles de $f(x)$ en $K[x]$ no son todos lineales. Sea $f_1(x)$ un factor no lineal irreducible de $f(x)$.
Entonces $\hat{\varphi}(f_1(x))$ es un factor irreducible de $\varphi(f(x))$ en K'. Las raíces de $f_1(x)$ en

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

el campo factorizante L están incluidos entre las raíces $u_1, u_2, \ldots, u_n$ y podemos suponer, sin pérdida de generalidad, que u_1 es una raíz de $f_1(x)$.

Del mismo modo, la lista $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ de las raíces de $\hat{\varphi}(f(x))$ incluye una raíz $v_1 = \varphi(u_i)$ de $\hat{\varphi}(f_1(x))$. (no se puede asumir $i = 1$).

Por el teorema 2.4.9. existe un isomorfismo $\varphi' : K(u_1) \to K'(v_1)$ que extiende φ. Dado que $f(x)$ tiene ahora menos de m raíces fuera de $K(u_1)$, podemos usar la hipótesis inductiva para afirmar la existencia de un isomorfismo $\varphi^* : L \to L'$ que se extiende $\varphi' : K(u_1) \to K'(v_1)$, y por loa tanto se extiende $\varphi : K \to K'$.

2.6. Glosario de términos básicos

Grupo, Grupo abeliano, Subgrupo, Grupo finito, Grupo cíclico, Subgrupo normal, Grupo cociente, Homomorfismo, Anillo, Dominio de integridad, Anillo de división, Subanillo, Ideal, Ideal maximal, Polinomio, Polinomios irreducibles, Campo, Subcampo, Extensión del campo, Campos factorizantes, Campos finitos.

2.7. Hipótesis de la investigación

Con el análisis de la teoría de campos, si se puede determinar una clasificación completa de los campos finitos.

2.7.1. Hipótesis específicos

- Con el análisis de las raíces de un polinomio $f(x) \in K[x]$, si se puede determinar que son distintos sobre un campo factorizante L.
- Con el análisis de una condición suficiente para que un grupo abeliano finito, si se puede determinar un grupo abeliano cíclico

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2.8. Operalización de variables

- **Variable independiente:** Teoría de campos.

- **Variable dependiente:** Clasificación completa de los campos finitos.

Variables	Dimensiones	Indicadores
VARIABLES INDEPENDIENTES	**Dimensión**	**Indicador**
Teoría de campos	✓ Campos y sus Extensiones ✓ Campos factorizantes	• Teorema 3.1.4 • Teorema 3.1.8 • Teorema 3.2.1
VARIABLES DEPENDIENTES	**Dimensión**	**Indicador**
Clasificación completa de los campos finitos	✓ Campos finitos	• Teorema 4.2.1

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Tipo de investigación

De acuerdo al propósito de la investigación, naturaleza del problema y los objetivos formulados, la investigación reúne las condiciones para ser calificada como una investigación científico básico (pura-fundamental), debido a que su desarrollo y los resultados sirven para profundizar y incrementar los conocimientos del tema de investigación.

3.2. Diseño de investigación

El diseño de investigación que adoptaremos, es de tipo descriptivo, de comprensión e interpretación, de carácter analítico y demostrativo.

3.3. Técnicas

En esta investigación se utilizará **técnica de lectura analítica**, con esta técnica se realiza lecturas y análisis de materiales de consulta para la asimilación (libros, artículos, paper, etc.).

3.4. Estrategias

- Búsqueda de información de la materia objeto de investigación.
- Revisión de saberes previos necesarios bibliográficos o de Internet que facilite desmenuzar o interpretar la lectura científica que se va a encarar.
- Lecturas detenidas para familiarización con la teoría y la simbología de los materiales de consulta para que una vez entendida sea redactada en un borrador, de cada parte que compondrá el trabajo de investigación.
- Consultas al asesor y otros entendidos e interesados en la materia objeto de investigación para consolidar las ideas desarrolladas o absolver dudas que se presenten.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

TESIS UNA - PUNO

Universidad Nacional del Altiplano

CAPÍTULO IV

4. ANALISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN.

4.1. Campos finitos.

Recordemos que un anillo en el que todo elemento no nulo es invertible se denomina *campo*. Se dice que un *campo es finito* si tiene un número finito de elementos.

El campo de enteros módulo un número primo es el ejemplo mas familiar de campo finito, pero muchas de sus propiedades se extienden a campos finitos arbitrarios.

Se sabe que un campo finito K tiene característica un número primo p y que su subcampo minimal, conocido como su subcampo primo, es

$$\{0_K, 1_K, 2(1_K), \ldots, (p-1)(1_K)\}$$

Este subcampo primo es isomorfo a $\mathbb{Z}_p$, el campo de los enteros modulo p.

Se sabe, también, que para todo x, y en un campo K de característica p y para todo $n \geq 1$,

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}.$$

Haciendo uso del marco teórico, pasamos a dar una clasificación completa de los campos finitos. Antes de todo necesitamos de una idea preliminar que se aplica a todos los campos.

Definición 4.1.1. Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio con coeficientes en un campo K. La derivada formal $Df(x)$ de $f(x)$ se define por

$$Df(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

Propiedades. Sea K un campo y $f(x), g(x) \in K[x]$. Entonces,

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

1. $D[kf(x)] = kDf(x),\ k \in K$

2. $D[f(x) \pm g(x)] = Df(x) \pm Dg(x)$

3. $D[f(x)g(x)] = [Df(x)]g(x) + f(x)[Dg(x)]$

Teorema 4.1.1. Sea $f(x)$ un polinomio con coeficientes en un campo K, y sea L un campo factorizante de $f(x)$ sobre K. Entonces las raíces de $f(x)$ sobre L son todas distintas si y solo si $f(x)$ y $Df(x)$ son coprimos, esto es, $f(x)$ y $Df(x)$ no tienen factores comunes no constantes.

Demostración. Supongamos primero que $f(x)$ tiene una raíz repetida α en L, así que $f(x) = (x-\alpha)^r g(x)$, donde $r \geq 2$. Entonces

$$Df(x) = (x-\alpha)^r [Dg(x)] + r(x-\alpha)^{r-1} g(x)$$

y así $f(x)$ y $Df(x)$ tienen el factor común $x-\alpha$.

Recíprocamente, supongamos que $f(x)$ no tiene raíces repetidas. Entonces, para cada raíz α de $f(x)$ en L, se tiene que $f(x) = (x-\alpha)g(x)$, donde $g(\alpha) \neq 0$. Luego,

$$Df(x) = g(x) + (x-\alpha)[Dg(x)],$$

de donde $Df(\alpha) = g(\alpha) \neq 0$. Luego, por el teorema del resto $(x-\alpha) \nmid Df(x)$. Esto se cumple para cada factor de $f(x)$ en $L[x]$, y así $f(x)$ y $Df(x)$ deben ser coprimos (primos entre si). ■

Finalmente establecemos el resultado central de este trabajo de investigación, esto es, el resutado que clasifica a todos los campos finitos.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Teorema A.

1. *Sea* K *un campo finito. Entonces* $|K| = p^n$ *para algún número primo* p *y algún entero* $n \geq 1$. *Cada elemento de* K *es una raíz del polinomio* $f(x) = x^{n^p} - x$ *y* K *es un campo factorizante de este polinomio sobre* $\mathbb{Z}_p$.
2. *Sea* p *un número primo y sea* $n \geq 1$ *un entero. Existe salvo isomorfismo, exactamente un campo de orden* p^n.

Demostarción.

1. Sea p la característica del campo K, donde p es un número primo. Entonces K es una extensión finita de $\mathbb{Z}_p$. Supongamos que el grado de esta extensión es n. Si $\{\beta_1, \beta_2, \ldots, \beta_n\}$ es una base de K sobre $\mathbb{Z}_p$, entonces cada elemento de K se expresa únicamente como una combinación lineal de la forma

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

donde los $a_i \in \mathbb{Z}_p$, para $i = 1, \ldots, n$. Para cada cada $a_i \in \mathbb{Z}_p$, $i = 1, 2, \ldots, n$ existen p elecciones posibles, a saber $0, 1, \ldots, p-1$, y así existen p^n combinaciones lineales. De este modo, $|K| = p^n$.

El grupo $K^* = K - \{0\}$ es de orden $p^n - 1$. Sea $\alpha \in K^*$. Entonces por el teorema de Lagrange, el orden de α, que es el orden del subgrupo $\langle \alpha \rangle$ generado por α, debe dividir a $p^n - 1$. Ciertamente $\alpha^{p^n - 1} = 1$. Así $\alpha^{p^n} - \alpha = 0$. Puesto que también, $0^{p^n} - 0 = 0$. Así todo elemento de K es una raíz del polinomio $f(x) = x^{p^n} - x$.

Se sigue que el polinomio $f(x) = x^{p^n} - x$ se factoriza completamente sobre K, puesto que $x - \alpha$ es un factor lineal de $f(x)$, para cada uno de los p^n elementos α de K. Es claro que este polinomio no puede factorizarse completamente sobre cualquier subcampo propio de K, y así K debe ser el campo factorizante de $f(x) = x^{p^n} - x$ sobre $\mathbb{Z}_p$.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

2. Veamos en primer lugar la parte de existencia. Sean p y n dados, y sea L el campo factorizante de $f(x)=x^{p^n}-x$ sobre $\mathbb{Z}_p$. Puesto que L es un campo de característica p, entonces

$$Df(x)=p^n x^{p^n-1}-1=-1,$$

Así, $f(x)$ y $Df(x)$ son ciertamente coprimos. Luego $f(x)=x^{p^n}-x$ tiene p^n raíces distintas sobre L.

Sea K el conjunto que consiste de aquellos raíces. Mostremos que K es un subcampo de L. En efecto, es claro que los elementos 0 y 1 se encuentran en K.

Supongamos $a,b\in K$. Entonces

$$(a-b)^{p^n}=a^{p^n}-b^{p^n}=a-b$$

y así, $a-b\in K$ .También, si $b\in K-\{0\}$,

$$\left(ab^{-1}\right)^{p^n}=a^{p^n}\left(b^{p^n}\right)^{-1}=ab^{-1}$$

y así, $ab^{-1}\in K$. El campo K es en realidad el campo factorizante L, puesto que contiene (en realidad consiste) de todas las raíces de $f(x)=x^{p^n}-x$ y es claro que ningún subcampo propio de K tiene esta propiedad.

Se ha mostrado que, para todo número primo p y para todo entero $n\geq 1$, existe un campo de orden p^n. Se mostró también, que cualquier de orden p^n es el campo factorizante de $f(x)=x^{p^n}-x$, sobre $\mathbb{Z}_p$ y así usando resultados de unicidad de campos factorizantes, tales campos son isomorfos. ■

Hemos conseguido una extraordinaria clasificación completa de los campos finitos: solo existen campos de orden una potencia de un número primo, mas aún para p y n dados existe exactamente un campo de orden p^n. Llamaremos a este campo el campo de Galois de orden p^n y lo denotamos por $GF(p^n)$. Para completar esta descripción necesitamos probar un resultado final.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

Teorema B.
El grupo de los elementos distintos de cero del campo de Galois $GF(p^n)$ es cíclico.

Demostración. Denotemos por K el campo de Galois $GF(p^n)$. Sea K^* el grupo abeliano de los elementos distintos de cero de K. Sea e el exponente de K^*. Entonces $a^e = 1$ para todo a en K^* y así cada elemento de K^* es una raíz del polinomio $f(x) = x^e - 1$. Este polinomio tiene a lo más e raíces y así $|K^*| \leq e$. Por otro lado, e sabemos que $e \leq |K^*|$. De todo ello, $e = |K^*|$ y así por el corolario 2.1.3, K^* es cíclico. ■.

Ejemplo. Puesto que todos los campos de orden p^n son isomorfos, podemos construir $GF(p^n)$ simplemente encontrando un polinomio irreducible $f(x)$ de grado n en $\mathbb{Z}_p[x]$. Entonces $GF(p^n) = \mathbb{Z}_p[x] / \langle f(x) \rangle$. Existen, si embargo, muchas formas de eligir $f(x)$. Por ejemplo, en el anillo de polinomios $\mathbb{Z}_3[x]$ existen 9 polinomios mónicos cuadráticos, de los cuales los polinomios

$$x^2 + 1, x^2 + x - 1, x^2 - x - 1$$

son irreducibles sobre $\mathbb{Z}_3$. El campo $L = \mathbb{Z}_3[x] / \langle x^2 + 1 \rangle$ es precisamente el campo de Galois $GF(3^2)$, esto es, $GF(3^2) = \mathbb{Z}_3[x] / \langle x^2 + 1 \rangle$. Notar que

$$GF(9) = \{0, 1, -1, \alpha, 1+\alpha, -1+\alpha, -\alpha, 1-\alpha, -1-\alpha\}$$

donde $\alpha = x + \langle x^2 + x - 1 \rangle$ y $\alpha^2 = -1$. Similarmente, $L_1 = \mathbb{Z}_3[x] / \langle x^2 + x - 1 \rangle$ y $L_2 = \mathbb{Z}_3[x] / \langle x^2 - x - 1 \rangle$ son campos de orden 9. Se sigue, de acuerdo al teorema A que clasifica completamente un campo finito, que

$$GF(3^2) = L \cong L_1 \cong L_2.$$

Repositorio Institucional UNA-PUNO
No olvide citar esta tesis

CONCLUSIONES

1. Al estudiar un polinomio con coeficientes en un campo K, en donde no todas sus raíces estén dentro del campo K, siempre podemos construir una extensión de ese campo que contiene por lo menos una raíz del polinomio y, así formar un nuevo campo, "*un campo de extensión de* K" *Teorema 2.4.8.*

2. Dado un polinomio $f(x) \in K[x]$, donde K es un campo, existe y es único salvo isomorfismo un campo factorizante L para $f(x)$ sobre K, *Teorema 2.5.1* y *Teorema 2.5.2.*

3. Para todo primo p y todo entero $n \geq 1$ existe un campo finito con p^n elementos. Cualquier campo finito con p^n elementos es isomorfo al campo factorizante del polinomio $x^{p^n} - x$ sobre $\mathbb{Z}_p$, *Teorema A.*

4. El orden de un campo finito siempre es un número primo o potencia de un número primo. Por cada potencia de un número primo, existe exactamente un campo finito $GF(p^n)$, comúnmente escrito por F_{p^n}.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

SUGERENCIAS

1. Antes de iniciar el estudio del teorema que clasifica completamente a los campos finitos, se sugiere tener conocimientos básicos de la teoría de grupos, anillos, campos y extensión de campos.
2. Una de las aplicaciones de gran interés de los campos finitos es en criptografía, gracias a que existe un inverso aditivo y multiplicativo que permite cifrar y descifrar en el mismo campo eliminando así los problemas de redondeo o truncamiento de valores si tales operaciones de cifrado y descifrado se hubiesen realizado en aritmética real.
3. El **teorema A** se puede llamar también "*el teorema de existencia y unicidad de campos finitos*". Ya que este teorema establece no solo que el número de elementos de todo cuerpo finito es igual a una potencia de un número primo, si no que para cada número primo p y cada entero positivo n existe un cuerpo finito de p^n elementos y, además dicho campo es único salvo isomorfismos.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis

BIBLIOGRAFIA

B., F. J. (1987). *Algebra abstracta.* Wilmengton Delaware: Adison Wesley.

Gallian, J. A. (2008). *Contemporary Abstract Algebra .* Minesota: University of Minnesota Duluth.

Herstein, I. N. (1964). *Topics in Algebra.* Blaisdell: Publishing Company.

Herstein, I. N. (1996). *Abstract Algebra - Third Edition.* Inc.: Prentice - Hall.

Howie, J. M. (2006). *Fields and Galois Theory.* London: Springer - Verlag.

Hungerford, T. W. (1974). *Algebra.* Verlag New York: Springer.

Josep, R. (1979). *Galois Theory.* Nostrand: andrews.

Judson, T. W. (2009). *Abstract Algebra Theory and Applications.* New York: Springer - Verlag.

Nieves Rodríguez Gonzáles, E. V. (2013). *Curso de teoría de Galois.* Santiago de Compostela.

Repositorio Institucional UNA-PUNO

No olvide citar esta tesis