UNIVERSIDAD DE GRANADA

CONCURSO PARA ACCESO A LOS CUERPOS DOCENTES UNIVERSITARIOS

PROFESOR TITULAR DE UNIVERSIDAD

ÁREA : **Álgebra**

DEPARTAMENTO : **De Álgebra**

PROYECTO DOCENTE

MÓDULO:

Estructuras Algebraicas y Matemática Discreta,

12 créditos, obligatorio.

(Titulación: Grado en Matemáticas)

Asignaturas

Álgebra II, ***6 créditos, segundo curso*** **y** ***Álgebra III,*** ***6 créditos, tercer curso.***

Laiachi El Kaoutit Zerri

Julio 2010

Proyecto Docente

Presentado por

Laiachi El Kaoutit Zerri

para participar en las pruebas de selección del concurso para acceso a los cuerpos docentes universitarios: Profesor Titular de Universidad del departamento de álgebra de la Universidad de Granada, con fecha de resolusión 19 de Marzo de 2010 (BOE de 12 de Abril de 2010).

Índice general

INTRODUCCIÓN

En la resolución de 14 de octubre de 2008 (BOJA 214, 28 de octubre de 2008), de la universidad de Granada, por la que se hace pública la normativa que regula el procedimiento de los concursos de acceso a los cuerpos universitarios; y en su noveno artículo, párrafo 5.b.2º, se le exige a cualquier concursante la entrega de un proyecto docente conforme con el perfil docente de la plaza convocada. Así la presente memoria es el proyecto docente que debe de presentar el presente candidato antes la comisión de selección.

La actividad docente asignada a la plaza a concurso tiene como perfil la palabra "Álgebra". Esto conlleva a cualquier opositor a la plaza, en el momento de abordar las materias del proyecto, a un vasto abanico de elecciones que en mi punto de vista no hace más que poner de manifiesto la sutileza de una apropiada elección. De ese modo, es importante explicar o al menos indicar los motivos que han empujado a un candidato a elegir las materias que ha presentado.

El principal motivo, bajo mi punto de vista, debe de ser la consideración de la entrada en vigor en el curso que viene en la Universidad de Granada de los nuevos grados. Esto supone, primero tener en cuenta la elección del titulo de grado en el cual el departamento de álgebra tenga adscrita docencia [1]. Segundo, que las materias que han de formar un Proyecto Docente tienen que ser coherentes con los contenidos de los módulos presentados en un grado [2].

En la elección del grado, esta bastante claro desde del punto de vista profesional, que la elección acertada es la titulación del grado de Matemáticas. En mi caso, como llevo años desarrollando tareas docente en lo que va ser el antiguo

[1] Esto se pueda averiguar en los documentos publico del vicerrectorado de grado y post-grado de la Universidad de Granada.

[2] Dichos contenidos podrán consultarse en el 'verifica': el documento oficial presentado por la UGR ante la ANECA, para cada titulación.

plan de la titulación del grado de informática, debo de confesar que hay más razones que me han empujado a elegir tal grado de Matemática. Además del sueño que persigue cualquier algebrista (resolver problemas de álgebra y enseñar álgebra), lo que me ha empujado a elegir tal grado, es el reto personal de demostrar capacidad de impartir con profesionalidad asignaturas en un grado más especializado y con contenidos de naturaleza puramente algebraicos.

Respecto a la elección de las materias, me he decidido por las materias del módulo **Estructuras Algebraicas y Matemática Discreta**, que se divide en dos asignaturas **Álgebra II** (segundo curso) y **Álgebra III** (tercer curso) ambas obligatorias y con seis créditos cada una. Mis razones para la elección de este módulo, la puedo resumir en varios puntos.

Por un lado, el módulo embarca una de las teoría más atractivas y importantes de lo que es el Álgebra, a saber la teoría de Galois de ecuaciones algebraicas. Además de ser importante por su valor histórico y los problemas que persigue y resuelve, pienso que es de importancia también que cualquier cuerpo de universidad del área de álgebra debe de tener conocimientos y un adiestrado manejo de esa teoría.

Por otro lado, los contenidos de ambas asignaturas (excepto quizás la parte de matemática discreta) se entrelazan de manera objetiva, en el sentido de que tienen la virtud de mostrar que las estructuras algebraicas (espacios vectoriales, grupos, anillo, cuerpos, anillos de polinomios, cuerpos de fracciones racionales) se complementan dando lugar a un trazado de ideas que combinadas entres ellas dibujan un procedimiento de estudiar y resolver ecuaciones algebraicas que ninguna otra materia de matemática es capaz ni si quiera de analizar (excepto quizás en algunos casos muy particulares). A un nivel más profundo, la estructura algebraica de las extensiones de Galois se refleja en los subgrupos de los grupos de Galois, lo que permite la aplicación de ideas teóricas de grupos al estudio de cuerpos. Esta correspondencia de Galois es una

idea poderosa que puede ser generalizada, de hecho lo ha sido, para aplicar la en campos tan diversos como la teoría de anillos, teoría de números algebraica, geometría algebraica, ecuaciones diferenciales y topología algebraica. Debido a esto, la teoría de Galois en sus diversas manifestaciones es un tema central para la matemática moderna.

Ante estas últimas argumentaciones, es necesario explicar como puede uno hacer germinar un interés ambicioso en el alumno hacia dicha teoría, o al menos convertirla atractiva para su prematuro gusto matemático. Una de la maneras podría ser de plantare al alumno ciertas preguntas quizás que el mismo se haya planteado alguna vez y que no obtuvo respuesta en los programas de las asignaturas cursadas anteriormente.

La primera de estas pregunta, podría venir del "álgebra elemental": ¿Existen "fórmulas" parecidas a las que permiten resolver una ecuación cuadrática para solucionar ecuaciones de grado mayor? Para ello es conveniente trazar al alumno una breve reseña histórica del problema desde el siglo XVI (fórmulas de Cadrano) hasta su solución completa en el siglo XIX (seguro que el número de siglos de diferencia impresiona a cualquiera).

La segunda cuestión hunde sus raíces en los primeros tiempos de la tradición matemática Griega. Se trata de los problemas de números (o medidas) constructibles mediante la regla y compás. La historia empieza cuando los Griegos descubrieron que su sistema de numeración (números racionales) es insuficiente, dado que la medida de la diagonal de un cuadrado de lado 1 no entraba en este sistema. Esto les llevo a ampliar su sistema de numeración añadiendo los números constructibles. También, le lleva a ciertas preguntas que jamas supieron responder: la cuadratura de un círculo, la duplicación del cubo, la trisección de un ángulo. Algo de lo antes, seguro que le sueña a cualquier alumno que ha cursado la asignatura de dibujo técnico en el instituto de segundaría.

Recordaremos, no obstante, que la teoría de Galois de ecuaciones algebrai-

cas, tiene un interés que rebasa ampliamente los problemas motivados expuestos. De un modo general, el alumno podrá percibir que la introducción y utilización de nociones abstractos, como la de espacio vectorial, grupo, cuerpo; así como el establecimiento de teoremas generales (como el teorema principal de Galois), permiten resolver problemas que, aunque planteados en términos elementales, se resisten a ser tratados por métodos elementales. Esta forma de visualizar la solución de problemas elementales, es de hecho un manifiesto de la matemática pura moderna. Así, creemos que para la formación de un matemático moderno es esencial que la anterior idea cale en su modo de entender la Matemática.

Finalizada la exposición de los motivos de la elección de la materia general que componen el presente proyecto, paso a comentar en groso modo los contenidos de cada asignatura y la escala de los requisitos previos para cada curso del proyecto, así como la manera del reparto de los créditos sobre los contenidos de cada materia. Una exposición detallada de los contenidos de cada tema, se encuentra justamente en el principio del mismo. Para más especificación sobre los objetivos y comentarios de cada curso, hemos dotado cada uno de ellos de un pequeño sumario y de una sección preliminar donde abordaremos con detalles estos objetivos y comentarios.

Los contenidos de la asignatura **Álgebra II** (excepto quizás la parte de Matemática Discreta) son meramente básicos para el desarrollo de la asignatura **Álgebra III**, el alumno no necesita requisito ninguno para cursarla. Esta asignatura contiene cuatro Temas, aparte de los Temas I y II que abordan la materia de Matemática Discreta y contemplan elementos de combinatoria y elementos de la teoría de grafos donde daremos varios algoritmos de busqueda que tienen cierto interés informático.

El primero de esos cuarto temas restantes, lo hemos consagrado a la introducción de estructuras algebraicas tal como anillos y cuerpos, donde además

abordaremos con detalles los dominios de integridad y sus cuerpos de fracciones. Los dos siguientes temas son para introducir el anillo de polinomios en varias indeterminadas con coeficientes en un cuerpo, así como sus cuerpo de fracciones racionales, además de los polinomios simétricos y las fracciones simétricas.

El último tema de ese curso esta consagrado para introducir el alumno al la teoría de grupos, y especialmente a la de grupos finitos. Hablaremos de las definiciones de grupos sus morfismos, subgrupos y grupos cocientes, teorema de isomorfía y daremos la demostración del teorema de Jordan-Hölder. Abordaremos también la acción de un grupo sobre un conjunto, estabilizadores, orbitas y insistimos sobre los los G-conjuntos homogéneos. Llegaremos así a la introducción de unas de la clases de grupos más importantes para la teoría de Galois, a saber los grupos resolubles y los grupos nilpotentes. Daremos por supuesto varias caracterizaciones de esta clases mediante ciertas nociones de series de subgrupos como la serie derivada o la serie central decreciente. Llegaremos así a los grupos finitos y especialmente los p-grupos de Sylow, donde daremos los celebres teoremas de Cayley y de Frobenius.

Antes de entrar en la descripción de los contenido del otro curso, creo que es importante explicarle a la comisión el reparto de los seis créditos que tiene la asignatura de **Álgebra II** sobre los contenidos anteriormente expuestos. Pensamos darle a la parte de Matemática Discreta, Temas I y II, un total de $1,5$ créditos. Los dominios de integridad, anillos de polinomios en varias indeterminadas y las fracciones simétricas, Temas III, IV y V, un total de $1,5$ créditos. Así, los 3 créditos restantes, se los reservamos a los elementos de la Teoría de grupos, Tema VI. En caso que es reparto sufra algún tipo de desequilibrado, tenemos pues pensado en nuestra metodología general de incluir en lo que llamamos *Trabajos Dirigidos y seminarios* toda aquella parte del temario que estimamos importante y que ha quedado fuera su impartición en las clases magistrales.

Laiachi El Kaoutit Zerri

Paso ahora a la descripción de los contenidos de la asignatura **Álgebra III**. Las materias de esta asignatura la engloban seis temas. El Tema I es introductorio, recordaremos pues algunas definiciones básica: anillos, cuerpos; luego hablamos de anillos de polinomios en una y varias indeterminadas, así como la factorización y la irreducibilidad de polinomios. Daremos varios test de irreducibilidad, y también algunos métodos clásicos de busqueda de raíces complejas en grados pequeños. Finalizaremos el tema con la definición de los grupos de automorfismo de un anillo y de un cuerpo.

En el Tema II abordaremos las extensiones de cuerpos, hablaremos de las extensiones simples, finitas y finitamente generadas; donde daremos la noción de torre de cuerpos. Introducimos los elementos algebraicos y transcendentales, y daremos varios ejemplos de números que han resistido a lo largo de mucho tiempo de ser demostrados números transcendentales. Incluimos en ese tema los números constructible mediante la regla y el compás; terminaremos con los teoremas de independencia lineal y algebraica de alguno homomorfismos dado paso al Teorema de Dedekind.

Las extensiones algebraicas de cuerpos le dedicaremos el Tema III, donde primero daremos el teorema de Kronecker sobre la existencia de un cuerpo de descomposición de un polinomio. Luego, daremos los Teorema de Steinitz sobre la existencia y la unicidad (salvo isomorfía) de la clausura algebraica de cuerpo dado y sobre la extensión a un automorfismo de cualquier monomorfismo con codominio dicha clausura. Hablaremos también sobre la multiplicidad de las raíces y los elementos separables en una extensión. Llegaremos así, a las extensiones separables y el teorema del elemento primitivo que relaciona la existencia de tal elemento con la finitud del retículo de las subextensiones. Finalizaremos el tema con la noción de elementos conjugados y subcuerpos conjugados, y también introducimos allí las extensiones normales que las caracterizamos como cuerpos de descomposición de una familia de polinomios.

De esa forma llegaremos a la introducción de las extensiones de Galois en el Tema IV. Serían pues las extensiones normales y separables finitas. Después de definir el grupo de Galois de un extensión de Galois y sus propiedades, daremos el teorema de la base normal y hablaremos del grupo de Galois relativo. Abordaremos luego la relación entre el conjunto sus subgrupos y el conjunto de los subcuerpos de elementos invariantes, dando así el Teorema principal de Galois o el de la correspondencia de Galois que establece un biyección compatible con el orden entre ambos conjuntos. Como aplicación trataremos las extensiones de Galois dentro de los complejos. Finalizaremos el tema con un Teorema de Kaplansky, que determina el grupo de Galois de ciertos polinomios con coeficientes racionales de grado 4. Las extensiones de Galois en característica positiva, la vamos a trata aparte en el Tema V. Hablaremos pues sobre los cuerpos finitos y sus grupos de Galois, y definimos lo que son las aplicaciones de Frobenius, la Norma y la Traza.

El Tema VI es vital para hacer le visualizar al alumno el objetivo principal de la asignatura. Trataremos primero la demostración del Teorema fundamental del álgebra, es decir comprobar que los números complejos forma un cuerpo algebraicamente cerrado. Trataremos luego con más detalles las extensiones ciclotómicas. Daremos aparte el teorema de Artin sobre la independencia lineal de los caracteres, y como aplicación deducimos el Teorema 90 de Hilbert. Llegaremos así a las extensiones radicales simples y las llamadas extensiones n-Kummer. Introducimos luego la noción de resolución por radical (de un polinomio) sobre un cuerpo base y pasaremos la introducción de las extensiones resolubles. Demostraremos la relación entre la resolubilidad de una extensión de Galois (finita) y la de su grupo de Galois. Una aplicación directa de ese teorema serían la extensiones de Galois que surjan de la fracciones racionales simétricas, y como corolario obtendremos el famoso Teorema de Abel-Ruffini.

Los prerrequisitos para cursar la asignatura **Álgebra III** son sin duda ninguna los contendidos de la asignatura **Álgebra II** y **Álgebra I** (asignatura obli-

gatoria de primer curso). Respecto al reparto de créditos sobre los contenidos, aquí la verdad es difícil hacer un equilibrio justo dado que en realidad la materia de la asignatura en cuestión es más intrincada y entrelazada, eso no hace más que incrementar los tiempos de la presentación y la exposición. Como ya venimos diciendo, vamos a insistir siempre sobre los contenidos primordiales para el desarrollo de la asignatura. Luego completaremos los otros contenido que posiblemente escapan al tiempo estipulado para las clases magistrales, en forma de trabajos dirigidos y seminarios de exposición. Pensamos consagrar le a los Temas I y II un total de un 1 créditos, los Temas III y IV un total de 3 créditos, y los 2 créditos restantes son para los Temas V y VI.

METODOLOGÍA GENERAL.

Dado que este poyecto embarca dos 'distintos' cursos, es conveniente especificar la metodología que hemos de seguir independientemente para cada curso. Para ello hemos dotado cada curso de una pequeña introducción donde abordaremos parte de esta metodología. Sin embargo, esto no exime de explicar nuestra metodología general para las enseñanza superior, basándose sobre la experiencia adquirida como docente. No puedo negar que exista una influencia, seguramente viene de mi experiencia personal como alumno de carrera de matemáticas en un sistema extranjero (sistema Francés), sobre cualquier metodología que he de adoptar. Ante esa situación, pienso que lo más razonable es quedarse con las mejores ventajas de dicho sistema.

A continuación paso a detallar algunas consideraciones metodológicas a tener en cuenta en el desarrollo del presente proyecto docente: En cuanto al desarrollo de las clases, seguiremos las pautas siguientes:

- Al principio de cada bloque temático se hará, en una lección magistral, una exposición general de los objetivos perseguidos y una descripción de los contenidos que se van a desarrollar y de los problemas que pretendemos resolver. Daremos en esta exposición la bibliografía que se va a utilizar.

- Las clases teorícas, de carácter también eminentemente magistral, aunque estaremos muy atentos a las preguntas y sugerencias de los alumnos, seguirán, usualmente, un esquema inductivo-deductivo. Se plantearán los problemas que se quieren resolver, comenzando, de ser posible, con problemas particulares sencillos cuya resolución pueda efectuarse o, al menos, intuirse sin necesidad de desarrollar la teoría general, para pasar posteriormente a la exposición propiamente dicha de los contenidos del tema. A veces puede ser conveniente, para no perder el hilo argumental,

dejar algunas partes no centrales de las demostraciones para desarrollar en las clases prácticas.

- Las clases prácticas serán de un carácter más colectivo. Para ello sería muy deseable poder hacerlas en grupos reducidos (veinte alumnos). Los problemas que se resolverán en estas clases deben haber sido trabajados previamente por los alumnos, y serán estos, preferentemente, los que deben exponer su resolución en la pizarra. También es de interés que los alumnos que no han logrado resolver un problema expongan qué ideas han ensayado y dónde han encontrado las dificultades. Las iniciativas para la resolución de un problema deberán partir, siempre que sea posible, de los propios alumnos.
- En estas prácticas se harán también, en forma de pequeños seminarios o exposiciones, las demostraciones no realizadas en las clases teorícas o de cualquier parte complementaria del temario que le ha sido asignada previamente al alumno para su estudio.

A lo que atañe el tema del sistema de evaluación y calificación, este consistirá, aparte de la realización de un examen final, en un seguimiento de la evolución del alumno en tutoría y su participación en clase. Se tendrá en cuenta también el grado de responsabilidad a la hora de cumplir con las fechas de entrega de trabajos dirigidos, las tares de casa o las prácticas. De todas formas, vamos a seguir de modo general el método que marque el documento 'verifica' para el grado en Matemática en su página 46.

Curso 1º

Álgebra II

SUMARIO

Objetivos y comentarios del curso

La asignatura de *Álgebra II*, como ya se ha podido ver en el sumario, tiene dos parte esenciales. La primera consiste en elementos de la Matemática Discreta cuyo objetivo es de familiarizar el alumno con ciertos métodos discretos, tal como la combinatoria, teoría de grafos, y ciertos algoritmos de busqueda con interés informático. La segunda parte representa la base fundamental para poder cursar la asignatura de **Álgebra III** y sobre la cual tenemos pesando insistir más. Esa parte consiste pues en estructuras algebraicas tal como anillos, cuerpos y dominios de integridad; anillo de polinomios en varias indeterminadas y sus cuerpos de fracciones racionales. Por el ínteres que representa la teroría elemental de groups, le hemos dedicado un tema aparte.

Los objetivos que se pretendan cubrir con esa última parte del presente curso son :

- Que el alumno reconozca sin dificultad y que se sienta familiarizado con la estructuras de anillos conmutativo, morfismos de anillos, ideales primos y maximales, anillos cocientes, y los todos teoremas de isomorfía.
- Que el alumno sepa detectar con facilidad los dominios de integridad, y saber con detalles la construcción de su cuerpos de fracciones, así como todas sus propiedades.
- Que el alumno tenga un adiestrado manejo de técnicas de cálculo en los polinomios en varias indeterminadas y sus fracciones racionales, también sus fracciones simétricas.
- Introducir el alumno en la teoría de grupos finitos. Que tenga amplio conocimientos sobre esta teoría y aparte de saber las definiciones básicas, pretendemos que al alumno aprenda a manejar las series de composición, las series de Jordan-Hölder, las series centrales y las series derivadas. Así,

tendrá un conocimiento profundo de algunas clases de grupos que son de interés para el curso que viene, tal como los grupos resolubles y los grupos nilpotentes.

- Que el alumno tenga amplio conocimiento sobre los grupos finitos, y especialmente los p-grupos de Sylow, y los teorema de Sylow. También pretendemos que al alumno aprenda a "clasificar" los grupos finitos de orden muy pequeño (menor que 8).

Tema I

Elementos de Combinatoria.

Lecciones

Este Tema contiene nociones básicas sobre combinatoria que ha de saber cualquier alumno del segundo curso del Grado en Matemáticas. El objetivo principal de la combinatoria es el estudio de las posibles agrupaciones de objetos. Contar el número de objetos que verifican ciertas propiedades es uno de los objetivos de la combinatoria. Problemas muy diversos, como determinar el número posible de apuestas diferentes en una quiniela, el número posible de posiciones en que unos corredores pueden terminar una carrera, el número posible de matrículas de los coches de un país o las diferentes formas de distribuir una serie de objetos en cajas son problemas que se abordan mediante las técnicas de conteo que veremos en este Tema. Lo que se pretende es por tanto, calcular el número de elementos de un conjunto finito (o el 'cardinal' del conjunto). Usaremos la notación $\#X$ (o a veces en otros Temas más adelante por $|X|$) para denotar el cardinal de un conjunto X.

LECCIÓN 1 PRINCIPIOS GENERALES EN COMBINATORIA.

Existen dos principios generales que debemos estudiar para adentrarnos en las técnicas de conteo. Aunque la interpretación más intuitiva de los mismos se refiere a posibilidades de elección dentro de una gama de alternativas, la presentación más algebraica hace referencia a cardinales de conjuntos. La cuenta más simple que podemos analizar es la siguiente.

TEOREMA (Principio de la suma). Sean A y B dos subconjuntos de un conjunto X que son disjuntos (i.e. $A \cap B = \varnothing$). Entonces $\#(A \cup B) = \#A + \#B$.

Le explicaremos al alumno que en términos de opciones y elecciones uno debe interpretar el principio de la suma de la siguiente forma. Para tomar una decisión tenemos dos alternativas. La primera nos lleva a seleccionar una opción entre n posibles, y la segunda una opción entre m posibles. Si no hay opciones comunes entre ambas alternativas entonces nuestra actuación consiste en decantarnos por una de las $n + m$ opciones totales.

El siguiente principio analiza aquellas situaciones en las que tenemos que realizar varias elecciones distintas entre alternativas no necesariamente iguales.

TEOREMA (Principio del producto). Si $X_1, \ldots, X_r$ son conjuntos de cardinal finito entonces $\#(X_1 \times \cdots \times X_r) = \#X_1 \cdots \#X_r$.

La interpretación de este principio es la siguiente: Si tenemos que realizar cadena de k selecciones independientes, la primera entre n_1 posibilidades, la segunda entre n_2 y así sucesivamente hasta la última selección que debemos realizar entre n_k alternativas, las alternativas totales entre las que debemos optar son $n_1 n_2 \cdots n_k$.

LECCIÓN 2 ORDEN IMPORTA. FACTORIAL

El principio del producto nos permite calcular el número de palabras de longitud dada r que podemos formar con un alfabeto de n caracteres. Este número es n^r. La clave está en que podemos repetir las letras en cada elección. Antes de analizar situaciones en las que no podemos realizar dicha repetición, recordaremos al alumno la definición del factorial

Sean $r \leq n$ dos naturales. Una r-*permutación* en n es una aplicación inyectiva $\sigma : \{1, \dots, r\} \to \{1, \dots, n\}$. Al conjunto de las r-permutaciones en n lo denotamos $P(n, r)$. El cardinal de dicho conjunto es:

$$\#P(n, r) = \frac{n!}{(n-r)!} = n(n-1)\cdots(n-r+1)$$

El Lema de conteo lo presentaremos después de definir los que es una *partición ordenada* en un conjunto X (i.e., una partición en la que los subconjuntos están ordenados. Cabe mencionar al alumno de que esto no significa que los elementos dentro de cada subconjunto están ordenados).

TEOREMA (Lema de conteo). Sea $\phi : A \to B$ una aplicación suprayectiva entre conjuntos finitos. Para cada $b \in B$ recordemos que $\phi^{-1}(b) = \phi^*(\{b\}) = \{a \in A \mid \phi(a) = b\}$. Si existe $k \in \mathbb{N}$ tal que $\#\phi^{-1}(b) = k$ para todo $b \in B$, entonces $\#A = k \cdot \#B$.

La demostración del siguiente teorema se basa sobre el lema de conteo

TEOREMA (Número de particiones ordenadas). Sea X un conjunto con $\#X = n$, y sean $n_1, \dots, n_k$ números naturales tales que $n = n_1 + \cdots + n_k$. El número de particiones ordenadas $\langle A_1, \dots, A_k \rangle$ con $\#A_j = n_j$ para cada $1 \leq j \leq k$ es

$$\frac{n!}{n_1! n_2! \cdots n_k!}$$

LECCIÓN 3 ORDEN NO IMPORTA. COEFICIENTES BINOMIALES

Se define el *coeficiente binomial* $\binom{n}{r}$ como el número de subconjuntos de r elementos que tiene un conjunto de n elementos. Luego se deduce que

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Después de presentar las propiedades básicas de los coeficientes binomial enunciaremos lo siguiente

TEOREMA. El número de cadenas compuestas por $n-r$ ceros y r unos es $\binom{n}{r}$
Existen $\binom{n+k-1}{k-1}$ formas de descomponer $n \in \mathbb{N}$ como suma de k números naturales.

La segunda parte describe el número de formas en las que n objetos indistinguibles pueden distribuirse en k cajas distinguibles. También nos dice de cuantas formas podemos seleccionar n objetos de entre k objetos distintos, permitiendo repeticiones.

LECCIÓN 4 OTROS PRINCIPIOS DE CONTEO

TEOREMA (Principio de inclusión-exclusión). Sean $A_1, \ldots, A_n \subseteq X$ subconjuntos finitos. Entonces

$$\#(A_1 \cup \cdots \cup A_n) = \\ = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\{i_1,\ldots,i_k\}\subseteq\{1,\ldots,n\}} \#(A_{i_1} \cap \cdots \cap A_{i_k}),$$

es decir, sumamos los cardinales de los conjuntos obtenidos al realizar la intersección de un número impar de subconjuntos y restamos los cardinales de los conjuntos obtenidos al intersecar un número par de subconjuntos.

Dada la complejidad de esta fórmula, es conveniente presentar ante el alumno el caso tres conjuntos.

Terminamos con otro principio aparentemente sencillo, pero de gran utilidad a la hora de resolver problemas. Se le conoce con el nombre de principio del palomar o de Dirichlet.

TEOREMA (Principio de Dirichlet). Sea $\{A_1, \ldots, A_k\}$ una partición de un conjunto X tal que $\#X = n$. Existe $i \in \{1, \ldots, k\}$ tal que $\#A_i \geq \frac{n}{k}$.

Como aplicación del principio de Dirichlet daremos el siguiente resultado

Sea $\varphi : X \to Y$ una aplicación entre conjuntos finitos tales que $\#X > k\#Y$ para cierto $k \in \mathbb{N}$. Existe $y \in Y$ tal que $\#\varphi^{-1}(y) > k$.

BIBLIOGRAFÍA

[1] J. A. Anderson. *Discrete Mathematics With Combinatorics*. Prentice-Hall, 2001.

[2] N. L. Biggs. *Matemática Discreta*. Ed. Vicens vives, 1994.

[3] R. P. Grimaldi. *Matemática Discreta y Combinatoría Una introducción con aplicaciones*. Addison Wesley Longman, 1998.

[4] J. Leach y M. Rodríguez M. T. Hortalá. *Matemática Discreta y Lógica Matematica*. Editorial Complutense, 1998.

[5] J. Matoušek and J. Nešetřil. *Invitation to Discrete Mathematics*. Clarendon Press. Oxford, 2004.

TEMA II

TEORÍA ELEMENTAL DE GRAFOS.

LECCIONES

En este Tema introducimos el alumno a la teoría de Grafos. Es evidente, y como ya uno ha podido realizar, el contenido es muy básico. El principal objetivo es de familiarizar el alumno con estructuras discreta: objetos y aristas entre si, así como el estudio de algunas de sus propiedades. También es de nuestro interés que un alumno de Matemáticas descubra algunos algoritmos (de búsqueda) en esta teoría que son de interés informático.

El tema contiene en total nueve lecciones cuyos contenidos abordan: Representación de grafos. Grafos completos. Grafos regulares. Homomorfismos de grafos. Subgrafos. Grafos isomorfos. Grafos conexos. Geodésicas. Número de caminos. Grafos de Euler. Caminos de Hamilton. Árboles. Grafos bipartidos. Grafos planos. Grafos planos coloreados. Grafos dirigidos. Algoritmos en grafos.

LECCIÓN 5 DEFINICIÓN DE GRAFO Y PROPIEDADES.

Presentaremos la siguiente definición: Un *grafo (no dirigido)* G está definido por dos conjuntos $V(G)$ y $E(G)$ junto con una aplicación $\gamma_G : E(G) \to \{\{u,v\} \mid u,v \in V(G)\}$. $V(G)$ son los *vértices* del grafo, y $E(G)$ son los *lados* o aristas del grafo. La aplicación γ_G dice cuales son los vértices unidos por el grafo G. Se dice que un lado e es un *lazo* si $\gamma_G(e) = \{v\}$. Dos lados e, e' se dicen *paralelos* si $\gamma_G(e) = \gamma_G(e')$. Conviene definir también los grafos dirigidos: Un *grafo dirigido u orientado* está definido por dos conjuntos $V(G)$ y $E(G)$ junto con dos aplicaciones $s, t : E(G) \to V(G)$. Al igual que en el caso no orientado $E(G)$ es el conjunto de los lados, y $V(G)$ el conjunto de los vértices. Si $e \in E(G)$, $s(e)$ y $t(e)$ son el origen y el destino de e. A cada grafo dirigido G podemos asociar un grafo no dirigido $\overline{G}$ cuyos vértices y lados son los mismos, y cuya aplicación γ viene dada por $\gamma(e) = \{s(e), t(e)\}$.

La figura II.1 representa tres grafos. En el grafo G de la misma los vértices son $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ y los lados $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, algunos valores de γ_G son $\gamma_G(e_1) = \{v_1, v_2\}$, $\gamma_G(e_4) = \{v_2, v_5\} = \gamma_G(e_6)$, $\gamma_G(e_8) = \{v_4\}$. Los lados e_4 y e_6 son paralelos, y el lado e_8 es un lazo. Los grafos G y H son no dirigidos, y el grafo I está orientado. Observemos además que $\overline{I} = G$.

Un *camino de longitud* n es una sucesión de lados $e_1 \dots e_n$ junto con una sucesión de vértices $v_1 \dots v_n v_{n+1}$ tales que $\gamma_G(e_i) = \{v_i, v_{i+1}\}$. Si $u = v_1$ y $v = v_{n+1}$ decimos que el camino une o conecta u y v. En este caso el camino $e_n \dots e_1$ conecta v con u, luego el que dos vértices estén conectados por un camino es una propiedad simétrica. Si $v_1 = v_{n+1}$ se dice que el camino es *cerrado*. Un camino en el que no hay lados repetidos se llama *simple*. Un camino cerrado en el que no hay vértices repetidos se llama *ciclo*. Es sencillo observar que un camino de longitud mayor o igual que tres en el que todos sus vértices son distintos (salvo posiblemente los extremos) es simple, ya que si se repite un lado se repiten sus vértices. Por tanto todo ciclo es simple. Volviendo a la figura

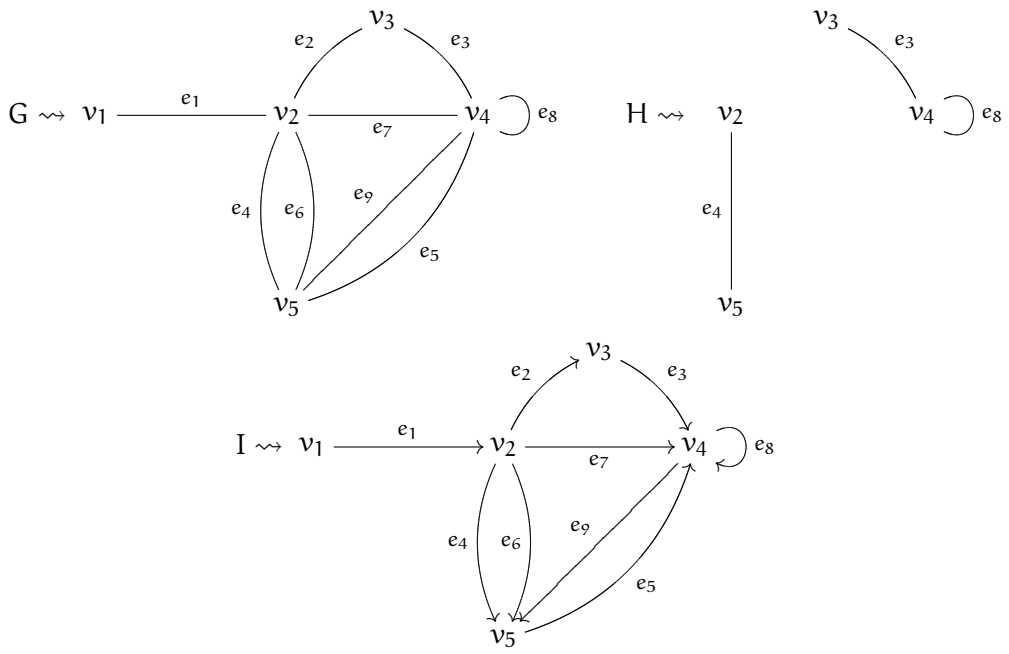


Figura II.1:

II.1 podemos dar ejemplos de lo que acabamos de mencionar: Por ejemplo en el grafo G de la figura la sucesión $e_1e_4e_6e_7$ es un camino simple, mientras que el camino $e_4e_7e_8e_7e_6$ es un camino no simple. El camino $e_4e_7e_3e_2e_6$ es un camino cerrado y simple, pero no es un ciclo ya que el vértice v_2 aparece repetido. Un ejemplo de ciclo en $e_4e_2e_3e_5$.

Pasaremos ahora a la definición de subgrafo y grafos conexos. Decimos que un grafo H es un subgrafo de un grafo G si $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$ y $\gamma_H = \gamma_{G|E(H)}$. El grafo H de la figura II.1 es un subgrafo del grafo G de la misma figura. Un grafo se dice *conexo* si dos vértices cualesquiera están conectados por un camino. G en la figura II.1 es conexo, mientras que H no lo es ya que no hay ningún camino en H que conecte v_2 y v_4 por ejemplo.

Un grafo que no contiene ciclos se llama *acíclico*. Un camino se dice acíclico si el subgrafo formado por sus vértices y sus lados es acíclico. Comprobare-

mos que un camino tiene todos sus vértices distintos si, y sólo si, es simple y acíclico. Podemos ahora enunciar:

Sean u, v vértices de G distintos. Si hay un camino de u a v entonces hay un camino simple y acíclico de u a v.
En particular si hay un camino simple cerrado en G con v como vértice entonces existe un ciclo en G con v como vértice.

TEOREMA. Si un grafo G tiene dos vértices distintos unidos por dos caminos simples distintos entonces G contiene un ciclo.

LECCIÓN 6 MATRICES ASOCIADAS A GRAFOS E ISOMORFISMO DE GRAFOS

Todo grafo finito lleva asociadas dos matrices que lo determinan completamente.

Sea G un grafo cuyos vértices son $V(G) = \{v_1, \ldots, v_n\}$. La *matriz de adyacencia* de G es una matriz cuadrada $A = (a_{ij})_{n\times n}$ en la que a_{ij} indica el número de lados que conectan los vértices v_i y v_j. Tenemos el siguiente resultado:

> Sea A la matriz de adyacencia de un grafo G cuyos vértices son $V(G) = \{v_1, \ldots, v_n\}$. El número de caminos de longitud n entre los vértices v_i y v_j es el valor de la entrada i, j de la matriz A^n.

Sea G un grafo cuyos vértices son $V(G) = \{v_1, \ldots, v_n\}$ y cuyos lados son $E(G) = \{e_1, \ldots, e_m\}$. La *matriz de incidencia* de G es una matriz $A = (a_{ij})_{n\times m}$ en la que a_{ij} vale 1 si $v_i \in \gamma(e_j)$, y 0 en caso contrario.

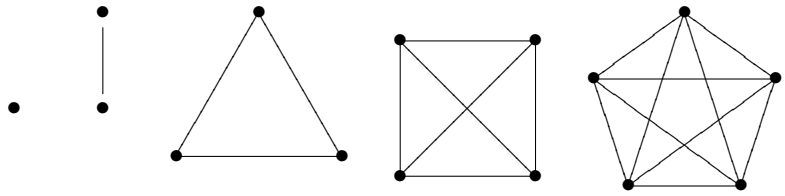
Un *isomorfismo* entre dos grafos G y H está formado por dos aplicaciones biyectivas $f : V(G) \to V(H)$ y $g : E(G) \to E(H)$ tales que $\gamma_H(g(e)) = f_*(\gamma_G(e))$. Dos grafos son *isomorfos* si existe un isomorfismo entre ellos. Una propiedad se dice *invariante por isomorfismo* si dados dos grafos isomorfos G y H, G satisface dicha propiedad si, y sólo si, H la satisface. Por ejemplo, ser conexo es un invariante por isomorfismo. Normalmente estamos interesados en propiedades definidas por valores numéricos, como el número de vértices o el número de lados, que son invariantes por isomorfismo.

Pasaremos ahora a definir la sucesión de grados de un grafo. Definimos el grado de un vértice v de un grafo G como el número de lados no lazos que tienen a v como uno de sus extremos más dos veces el número de lazos que tienen a v como extremo. El grado cuenta el número de lados que tocan a un vértice dado.

Se denota $\deg(v)$. Denotamos $D_k(G)$ el número de vértices de grado k en G. La sucesión $(D_0(G), D_1(G), D_2(G), \dots)$ se llama *sucesión de grados*. Demostraremos que esta sucesión invariante por isomorfismos, pero antes daremos el siguiente resultado

TEOREMA. La suma de los grados de todos los vértices de un grafo finito es igual a dos veces el número de sus lados.

Un grafo se dice que es *regular*, si el grado es el mismo para todos y cada uno de los vértices. Un grafo sin lazos ni lados paralelos de n vértices y en el que el grado de cada vértice es $n-1$ se llama *completo*. Presentaremos al alumno los cinco primeros grafos completos.



LECCIÓN 7 GRAFOS DE EULER

En esta lección todos los grafos bajo consideración son conexos.

Un *camino de Euler* de un grafo G es un camino simple que recorre todos los lados de G. Si el camino es cerrado lo llamamos *circuito de Euler*. Un grafo es de *Euler* si posee un circuito de Euler.

TEOREMA (Grafo de Euler). Sea G un grafo conexo. G tiene un circuito de Euler si, y sólo si, el grado de todos y cada uno de los vértices es par.

TEOREMA. Sea G un grafo conexo. Entonces G tiene un camino de Euler si, y sólo si, G tiene exactamente dos vértices de grado impar.

Terminaremos esta lección dando el algoritmo de Fleury que permite encontrar caminos de Euler en aquellos grafos que los tengan. Antes es conveniente dar el siguiente resultado

TEOREMA. Sea e un lado en un grafo conexo G. Las siguientes afirmaciones son equivalentes:

(I) El grafo obtenido al quitar e de G es conexo.

(II) e es un lado de algún ciclo en G.

(III) e es un lado de algún camino cerrado y simple en G.

ALGORITMO DE FLEURY

Entrada, un grafo G. Salida, SE y SV, que son las sucesiones de lados y vértices que dan el camino de Euler.

(1) Si todos los vértices de G tienen grado par llamamos v a un vértice cualquiera, si G tiene dos vértices de grado impar llamamos v a uno de los dos.

Asignamos $SE = []$ y $SV = [v]$.

(2) Si G sólo tiene a v entonces el algoritmo termina.

(3) Si existe un único lado e con inicio en v, llamamos w al final de e, quitamos e y v de G y vamos al paso (5).

(4) Si existen más de un lado con inicio en v, seleccionamos como e cualquier lado que toque a v tal que al ser quitado el grafo sigue siendo conexo. Llamamos w al otro extremo de e y quitamos e de G.

(5) Añadimos w al final de SV y e al final de SE. Cambiamos v por w y volvemos al paso (2).

LECCIÓN 8 GRAFOS DE HAMILTON

Un *camino de Hamilton* en un grafo G es un camino que recorre todos los vértices de G sin repetir ninguno (salvo posiblemente los extremos). Si el camino es cerrado recibe el nombre de *circuito de Hamilton*. Un grafo con un circuito de Hamilton recibe el nombre de *grafo de Hamilton* o *grafo hamiltoniano*. La primera propiedad que podemos enunciar sobre los grafos de Hamilton es: Si G es un grafo Hamiltoniano con n vértices entonces G tiene al menos n lados.

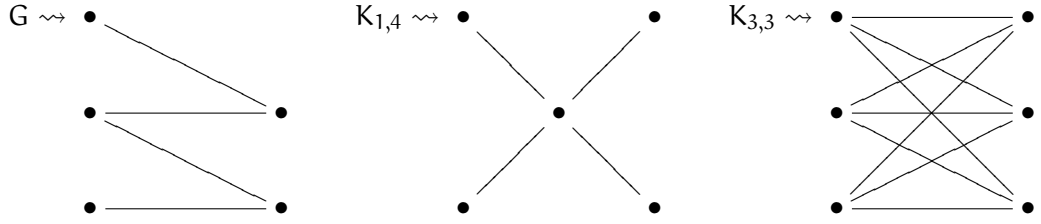
Presentaremos algunos resultados que garantizan que un grafo es de Hamilton. Estos resultados no son sin embargo suficientes, y los grafos de la figura II.2 son ejemplos de grafos hamiltonianos que no satisfacen las hipótesis de los teoremas siguientes.

TEOREMA (Grafos de Hamilton). Sea G un grafo con n vértices sin lazos ni lados paralelos.

(1) Si G tiene al menos $\frac{1}{2}(n-1)(n-2)+2$ lados es hamiltoniano.

(2) Si $n \geq 3$ y para cada par de vértices v y w no adyacentes se verifica que $\deg(v) + \deg(w) \geq n$, entonces G es hamiltoniano.

Hay un tipo de grafos en los que el estudio de los caminos de Hamilton es especialmente sencillo. Un grafo G se llama *bipartido* si $V(G) = V_1 \cup V_2$ con $V_1 \cap V_2 = \varnothing$ y para cada $e \in E(G)$ si $\gamma(e) = \{v, w\}$ entonces $v \in V_1$ y $w \in V_2$. Un grafo bipartido se llama *bipartido completo* si para cada pareja $(v, w) \in V_1 \times V_2$ existe un único $e \in E(G)$ tal que $\gamma(e) = \{v, w\}$. Los grafos representados a continuación son todos bipartidos.



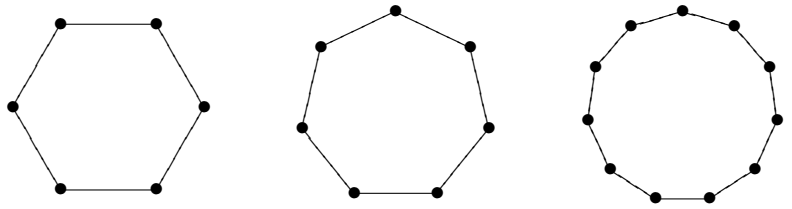


Figura II.2:

Los dos últimos son bipartidos completos. Es sencillo observar que un grafo bipartido completo depende exclusivamente de los cardinales de V_1 y V_2 . Por eso se representan mediante la letra K seguida de dichos cardinales como subíndice.

En un grafo bipartido con la partición del conjunto de vértices $V = V_1 \cup V_2$. Supongamos que $v_1v_2\cdots v_m$ es un camino en G y que $v_1 \in V_1$. Entonces $\{v_1, v_3, v_5, \cdots\} \subseteq V_1$ y $v_2, v_4, \cdots\} \subseteq V_2$. Gracias a esta observación podemos caracterizar los grafos bipartidos:

TEOREMA. Sea G un grafo. Entonces G es bipartido si, y sólo si, G no contiene ciclos de longitud impar.

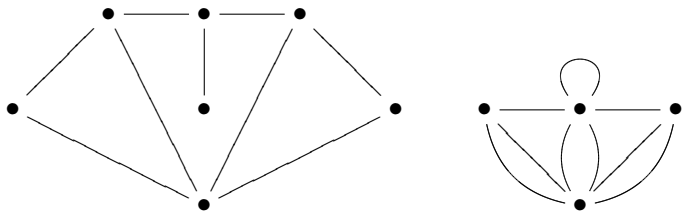
TEOREMA. Sea G un grafo bipartido en el que n y m son los cardinales de V_1 y V_2. Si G tiene un camino de Hamilton entonces $|n - m| \leq 1$, y si G es hamiltoniano entonces $n = m$. Si G es bipartido completo entonces el recíproco es cierto.

LECCIÓN 9 GRAFOS PLANOS

Una representación de un grafo G se llama plana si los vértices y los lados se encuentran en un plano y líneas que representan lados distintos no se cruzan entre sí. Dada una representación plana de un grafo llamamos *cara* a cualquier región del grafo que no corta a la representación del grafo y máximal con respecto a esta propiedad. Un grafo se dice *plano* si admite una representación plana.

TEOREMA (Característica de Euler). En un grafo plano G, si llamamos v, l y c al número de vértices, lados y caras de G respectivamente, entonces $v + c - l = 2$. En general, si G es un grafo plano, y χ es el número de sus componentes conexas entonces $v + c - l = 1 + \chi$.

Dada una representación plana de un grafo G, definimos el grafo dual G_D asociado a la representación anterior de la siguiente forma: cada cara de G nos da un vértice de G_D; cada lado e de G nos da un lado de G_D uniendo los vértices asociados a las caras que separa e. El siguiente es un ejemplo de un grafo y su dual.



TEOREMA. Sea G un grafo plano con v vértices, l lados y c caras. Si cada cara en la representación plana de G tiene al menos r lados fronterizos, entonces

$$rc \leq 2l, \qquad (r-2)l \leq r(v-2).$$

En particular si G no tiene ni lazos ni lados paralelos, entonces $3c \leq 2l$ y $l \leq 3v - 6$.

El grafo dual depende de la representación plana elegida. Sin embargo, el dual de un grafo plano es también un grafo plano. Terminaremos esta lección presentando el teorema de Kuratowski que caracteriza los grafos planos.

Una *contracción simple* de un grafo G es el grafo obtenido al identificar dos vértices unidos por un lado. Una *contracción* de un grafo G es una cadena de contracciones simples que parte de G. Observemos que si G es un grafo plano entonces cualquier contracción suya también lo es.

TEOREMA (Kuratowski). Un grafo no es plano si, y sólo si, contiene un subgrafo que se puede contraer a K_5 o a $K_{3,3}$.

LECCIÓN 10 COLORACIÓN DE GRAFOS Y POLINOMIOS CROMÁTICOS.

Una *coloración* en un grafo G es una aplicación $c : V(G) \to C$ tal que para cada $e \in E(G)$, si $\gamma(e) = \{v, w\}$ con $v \neq w$ entonces $c(v) \neq c(w)$. Es decir, una coloración es una asignación de colores a los vértices de G de tal manera que dos vértices unidos por un lado tienen distinto color. Dado un grafo G, llamamos *índice cromático* al menor número de colores necesario para colorear G. Este número lo representamos por $\chi(G)$.

Para un grafo plano es posible demostrar que su índice cromático es menor o igual que 4. Para un grafo G dado el siguiente concepto puede ayudar a calcular el índice. Sea G un grafo y $n \in \mathbb{N}$. Llamamos $p(n)$ al número de coloraciones que tiene G utilizando n colores. Esta aplicación es de hecho una función polinómica en n. Dicho polinomio recibe el nombre de *polinomio cromático* de G. Algunas propiedades de este polinomio son:

(I) El polinomio cromático de K_n es $x(x-1)\dots(x-n+1) = \prod_{k=0}^{n-1}(x-k)$.

(II) Dados dos vértices v, w no adyacentes, podemos descomponer las coloraciones de G como la unión disjunta de las coloraciones que asignan el mismo color a v y w junto con las coloraciones que asignan distinto color a v y w.

(III) Las coloraciones que asignan a dos vértices no adyacentes v y w colores distintos son exactamente las coloraciones totales del grafo obtenido al añadir un nuevo lado entre v y w.

(IV) Las coloraciones que asignan a dos vértices no adyacentes v y w el mismo color son exactamente las coloraciones totales del grafo obtenido al identificar como uno sólo los vértices v y w.

LECCIÓN 11 GEODÉSICAS

Una *ponderación* en un grafo G es una aplicación $\omega : E(G) \to \mathbb{R}$. Para cada $e \in E(G)$, el valor $\omega(e)$ recibe el nombre de *peso* de e. Podemos extender el concepto de peso de un lado a caminos y árboles generadores. Así, si $e_1 \dots e_n$ es un camino en G, su peso se define como $\omega(e_1) + \cdots + \omega(e_n)$. Dados dos vértices v y w, una *geodésica* de v a w es un camino entre ambos vértices cuyo peso es mínimo entre los caminos que los conectan.

El cálculo de geodésicas es un problema importante dentro de la teoría de grafos. Vamos a presentar el algoritmo de Dijkstra que calcula todas las geodésicas que conectan un vértice dado con todos los demás. Es evidente que los lazos no deben aparecer en las geodésicas, y en aquellos vértices en los que hay lados paralelos podemos limitarnos a seleccionar el lado de menor peso. Por tanto podemos suponer que nuestro grafo carece de lazos y lados paralelos, por lo que los lados vienen determinados por los vértices que unes. Pasamos a describir el algoritmo. En primer lugar nombramos los vértices $V(G) = \{1, \dots, n\}$ de forma que pretendemos encontrar las geodésicas que parten del vértice 1. Para cada vértice j, $D(j)$ va a ser el peso de la geodésica que termina en j, y $P(j)$ es un vértice tal que $\{j, P(j)\}$ es el último lado de una geodésica que conecta 1 y j. Al terminar el algoritmo $D(j) = \infty$ si no existe un camino de 1 a j, mientras que $P(j) = 0$ si no existe un camino de 1 a j, y en caso de que sí exista $j, P(j), P(P(j)), P(P(P(j))), \dots$ proporciona una sucesión de vértices tal que los lados correspondientes forman la geodésica de j a 1. La idea consiste en crear un conjunto L de vértices ya examinados. En cada etapa tanto D como P nos dan salida dentro del conjunto de los vértices ya examinados. Dado que los lados vienen determinados por los vértices que unen la función de pesos ω actúa sobre parejas de vértices. Escribimos $\omega(i, j) = \infty$ si no existe lado que conecte i y j.

ALGORITMO DE DIJKSTRA

`entrada`: Un grafo ponderado G sin lazos ni lados paralelos

`salida`: Las funciones D y P descritas anteriormente.

`inicio`

$L = \{1\}$

`Desde` $i = 2$ `a` n

    $D(i) = \omega(1, i)$

    `si` $\omega(1, i) = \infty$

        $P(i) = 0$

    `si no`

        $P(i) = 1$

    `fin si`

`fin desde`

`mientras` $V(G) \setminus L \neq \varnothing$

    Elige $k \in V(G) \setminus L$ tal que $D(k)$ sea el menor posible

    $L = L \cup \{k\}$

    `Para cada` $j \in V(G) \setminus L$

        `si` $D(j) > D(k) + \omega(k, j)$

            Reemplaza $D(j)$ por $D(k) + \omega(k, j)$

            Reemplaza $P(j)$ por k

        `fin si`

    `fin para cada`

`fin mientras`

`devuelve` D y P.

`fin`

LECCIÓN 12 ÁRBOLES

Un *árbol* es un grafo acíclico y conexo. Un grafo acíclico no conexo suele llamarse también *bosque*. Sea G un grafo conexo. Un subgrafo T de G se dice *árbol generador* si T es un árbol y $V(T) = V(G)$. En consecuencia: Todo grafo conexo tiene un árbol generador.

Para caracterizar los árboles podemos suponer que nuestro grafo carece de lazos o lados paralelos.

TEOREMA. Sea G un grafo con más de un vértice pero sin lazos ni lados paralelos. Las siguientes afirmaciones son equivalentes.

(I) G es un árbol.

(II) Dos vértices distintos cualesquiera están conectados por exactamente un camino simple.

(III) G es conexo, pero deja de ser-lo si quitamos algún lado.

(IV) G es acíclico, pero deja de ser-lo si añadimos algún lado.

Este teorema nos dice que los árboles son los grafos conexos más pequeños posibles y los acíclicos más grandes. Esta caracterización puede ser mejorada en cierto sentido.

Una *hoja* en un árbol T es un vértice de grado uno. Una inducción bastante sencilla permite demostrar que un árbol con n vértices tiene exactamente $n-1$ lados. El número de lados también sirve para caracterizar los árboles, como muestra el siguiente teorema.

TEOREMA. Sea G un grafo con n vértices, pero sin lazos ni lados paralelos. Las siguientes afirmaciones son equivalentes.

(I) G es un árbol.

(II) G es acíclico y tiene exactamente $n-1$ lados.

(III) G es conexo y tiene exactamente $n-1$ lados.

Sea G un grafo ponderado. Si T es un árbol generador de lados $\{e_1,\dots,e_m\}$, definimos el peso de T como $\omega(e_1)+\cdots+\omega(e_m)$. Un *árbol generador minimal* es un árbol generador de peso mínimo. El siguiente algoritmo da como salida los lados de un árbol generador minimal. En dicho algoritmo, un conjunto de lados representa el subgrafo con todos los vértices y con dichos lados.

ALGORITMO DE KRUSKAL

`entrada`: Un grafo ponderado G cuyos lados están ordenados de tal forma que
$$\omega(e_1)\le\cdots\le\omega(e_m)$$
`salida`: Un conjunto E formado por los lados de un árbol generador minimal.
`inicio`
$E=\varnothing$
`para` $j=1\dots m$ `hacer`
    `si` $E\cup\{e_j\}$ es acíclico `entonces` reemplaza E por $E\cup\{e_j\}$
`devuelve` E
`fin`

LECCIÓN 13 ÁRBOLES CON RAÍZ Y ALGORITMOS DE BÚSQUEDA

En esta última Lección trataremos los grafos dirigidos.

Sea G un grafo dirigido y sea $v \in V(G)$. Llamamos *grado de entrada* o *ingrado* de v al número de lados que llegan a v; llamamos *grado de salida* u *outgrado* de v al número de lados que salen de v.

Sea T un árbol y sea $r \in V(T)$. Vamos a construir un grafo dirigido a partir de los datos anteriores. Sea $v \in V(T) \setminus \{r\}$. Existe un único camino de r a v. Un lado definido por los vértices $\{w, v\}$ va de w a v si dicho lado es el último lado del único camino que conecta r con v. Denotamos dicho grafo por T_r, y lo llamamos árbol con raíz r. Demostraremos por inducción sobre el número de vértices que en un árbol con raíz T_r, el ingrado de r es cero, y el ingrado de todos los demás vértices es 1.

Si $\langle w, v\rangle$ es un lado que va de w a v decimos que w es el *padre* de v y v es el *hijo* de w. En general, si existe un camino dirigido de w a v decimos que v es un *descendiente* de w. Si v es un vértice cualquiera de T definimos el *subárbol con raíz* v como el subárbol formado por v y todos sus descendientes. Los vértices de grado 1 se llaman *hojas*.

Un árbol con raíz recibe el nombre de *árbol* m*-ario* si el grado de salida de todos los vértices es menor o igual que m, es decir, si cada vértice tiene a lo sumo m hijos. Un árbol 2-ario se llama *árbol binario*. Un árbol m-ario se dice *regular* si el grado de salida de todos los vértices que no son hojas es exactamente m. El *nivel* de un vértice es la longitud del único camino que lo conecta con r. La *altura* de un árbol con raíz es el máximo de los niveles de sus vértices. Un árbol m-ario regular se dice *completo* si todas sus hojas tienen el mismo nivel.

TEOREMA. Sea T_r un árbol m-ario regular completo de altura h. El número de vértices de T es

$$1 + m + m^2 + \cdots + m^h = \frac{m^{h+1} - 1}{m - 1}$$

El número anterior es una cota superior es una cota superior para todos los árboles m-arios de altura h.

Terminamos con algunos algoritmos que tratan de recorrer todos los vértices de un árbol con raíz. Los algoritmos presentados son recursivos, y para ello debemos construir los árboles de forma recursiva.

(A) Un vértice sólo r es un árbol con raíz r.

(B) Si $T_{r_1}, \ldots, T_{r_k}$ son árboles con raíz tales que $V(T_{r_1}), \ldots, V(T_{r_k})$ son conjuntos disjuntos y r es un elemento que no está en $V(T_{r_1}) \cup \cdots \cup V(T_{r_k})$, entonces T_r es un árbol con raíz donde $V(T_r) = \{r\} \cup V(T_{r_1}) \cup \cdots \cup V(T_{r_k})$, r es la raíz y tiene por hijos $r_1, \ldots, r_k$ y todos los demás vértices tienen los mismos hijos que antes.

A partir de esta definición podemos dar fácilmente tres algoritmos de búsqueda, los tres basados en el recorrido recursivo del árbol. La diferencia está en el orden en el que escribimos los vértices. Podemos escribir la raíz antes que sus hijos, después de sus hijos o entre sus hijos si el árbol es binario. Escribimos uno de ellos, ya que los otros dos son fáciles de adaptar.

ALGORITMO DE PREORDEN

`entrada`: Un árbol con raíz T_r
`salida`: Una lista de sus vértices
`inicio`
$L = [r]$

`para cada` w hijo de r

    $L = L \cdot \text{Preorden}(w)$

`fin para cada`

`Devuelve` L

`fin`

BIBLIOGRAFÍA

[1] R. Balakrishnan and K. Ranganathan. *A Textbook of Graph Theory*. Springer, 2000.

[2] R. Garnier and J. Taylor. *Discret Matematics for New Techonology*. IOP, second edition, 2002.

[3] R. P. Grimaldi. *Matemática Discreta y Combinatoría*
Una introducción con aplicaciones. Addison Wesley Longman, 1998.

[4] J. Matoušek and J. Nešetřil. *Invitation to Discrete Mathematics*. Clarendon Press. Oxford, 2004.

[5] K. H. Rosen. *Matemática discreta y sus aplicaciones*. McGraw-Hill, 2004.

[6] K. A. Roos y C. R. Wright. *Discrete Mathematics*. Prentice-Hall, 1988.

Tema III

Dominios de integridad y cuerpos.

Lecciones

Este Tema contiene las nociones básica que han de utilizarse (o que el al alumno debe de aprender) para el desarrollo de más temas de este curso. Contiene en total tres lecciones cuyos contenidos principalmente abordan: La definición de un anillo, la definición de un morfismo de anillos, ideales y anillos cocientes; dominios de integridad y sus cuerpos de fracciones.

LECCIÓN 14 ANILLOS, IDEALES Y MORFISMOS DE ANILLOS

En esta lección le recordaremos al alumno las definiciones básicas de un anillo (insistimos sobre los anillos conmutativos), ideales y morfismos de anillos. Así como el anillo cociente y los isomorfismos modulares en el retículo de todos los ideales. Destacaremos también algunos ideales notable: los ideales finitamente generados (en particular los principales), los ideales máximales y los ideales primos.

Conviene dar la definición de un morfismo de anillos. *Un homomorfismo (o morfismo) de anillos* es una aplicación $\varphi : A \to A'$ que satisface las siguientes condiciones:

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(a+b) = \varphi(a)+\varphi(b), \quad \varphi(1_A) = 1_{A'},$$

para cualquier par de elementos $a, b \in A$. Un morfismo de anillos $\varphi : A \to A'$, se dice que es un *monomorfismo*, si φ es inyectiva, es decir si tenemos $\varphi(a) = \varphi(b)$, para cierto par de elementos $a, b \in A$, entonces $a = b$. Esto es equivalente a que $\mathrm{Ker}(\varphi) = 0$. Se dice que φ es un *epimorfismo* si es suprayectiva, es decir para cualquier elemento $a' \in A'$, existe un $a \in A$ tal que $\varphi(a) = a'$. Un *isomorfismo de anillos* es un morfismo inyectivo y suprayectivo, i.e. la aplicación subyacente es biyectiva. Un *automorfismo* es entonces un endomorfismo biyectivo.

A base de indicación y después de dar las definiciones básicas, procederemos como sigue: Sea X un subconjunto de un anillo A. Dado, que el retículo de ideales de A, es estable bajo cualquier intercesión, podemos considerar el ideal que es la intersección de todos los ideales $I \lhd A$ tal que $X \subseteq I$. Este ideal, es por definición el *ideal generado* por el conjunto X. Esta claro, que es el más pequeño (por el orden de inclusión) entre todos los ideales que contienen a X. En el caso que X sea finito, i.e. $X = \{a_1, \cdots, a_n\}$, el ideal generado por X, se denota por $\langle a_1, \cdots, a_n \rangle$. De este modo, se dice que un ideal $I \lhd A$ es *finitamente generado*, si

$I = \langle a_1, \cdots, a_n \rangle$ para algún subconjunto $\{a_1, \cdots, a_n\} \subseteq I$. Se puede ver fácilmente que

$$\langle a_1, \cdots, a_n \rangle \;=\; \left\{ \sum_{1 \leq i \leq n} x_i a_i \,|\, x_i \in A \right\}.$$

Dado un ideal $I \lhd A$, se define el *anillo cociente* como el grupo abeliano cociente A/I dotado de la única multiplicación que convierte a la aplicación canónica $\pi : A \to A/I$ un epimorfismo de anillos.

Sea A un anillo y $I \lhd A$ un ideal propio.

- I es un *ideal primo*, si para cualquier par de elementos $a, b \in A$, se tiene

$$ab \in I \Longrightarrow a \in I \text{ o } b \in I.$$

- I es un *ideal máximal*, si no hay ningún $J \lhd A$ tal que $I \subsetneq J$. Es decir que I es un elemento máximal en el retículo de todos los ideales de A.

- I se dice que *principal*, si esta generado por un solo elemento:

$$I = \langle a \rangle = \{xa \,|\, x \in A\}$$

  para algún elemento $a \in A$. Observar, que si $a, b \in A$, entonces $\langle a \rangle = \langle b \rangle$ si, y sólo si $a = ub$ para algún elemento invertible u. Emplearemos la notación, $a|x$ para decir que $x \in \langle a \rangle$, decimos también que a *divide a* x.

Explicaremos como las propiedades de un ideal reflejan otras propiedades en el anillo cociente. Los ejemplos básicos que se presentan son los números enteros, racional, real y complejos, así como los residuos módulos un número natural $\mathbb{Z}_m$. El ejemplo de anillo de polinomios le dedicaremos una lección aparte.

LECCIÓN 15 CUERPOS Y DOMINIOS DE INTEGRIDAD

Antes de definir lo que es *un cuerpo* es conveniente dar la definición de un *dominio de integridad*. Un anillo A, se dice que es un *dominio de integridad*, si para $a, b \in A$

$$ab = 0 \Longrightarrow a = 0 \text{ o } b = 0.$$

Es decir que es un anillo sin *divisores de cero*, o la multiplicación es cancelativa respecto a los elementos no nulos. Se dice que A es un *dominio de integridad principal*, si es un dominio de integridad donde cualquier ideal es principal.

Pasaremos luego a definir lo que es un *elemento primo* (que genera un ideal primo) y *elemento irreducible* (sus único divisores son lo asociados). Luego llamaremos la atención del alumno sobre el hecho de que en un Dominio de integridad, cualquier primo es irreducible.

Daremos la definición de cuerpo, como aquel anillo conmutativo ($1 \neq 0$) donde cualquier elemento no nulo es invertible. Así le haremos observar al alumno que cualquier cuerpo es de hecho un dominio de integridad principal, y que el recíproco no es cierto , tomando como contra-ejemplo los números enteros. Comprobaremos el siguiente resultado, para hacer ver al alumno de que manera se puedan construir cuerpos

TEOREMA (Anillos cocientes). Sea A un anillo y $I \lhd A$ un ideal.

(i) El anillo cociente A/I es un dominio de integridad si, y sólo si I es un ideal primo.

(ii) El anillo cociente A/I es un cuerpo si, y sólo si I es un ideal máximal.

Son cuerpos, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ y los cocientes primos de $\mathbb{Z}$: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, donde p es un número primo.

Dado que la noción de característica en la teoría de Galois es importante (más general en teoría de cuerpos). Daremos la definición de la *característica de un anillo* y luego definimos lo que son los *cuerpos primos*: $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \cdots, \mathbb{F}_p, \cdots, \mathbb{Q}$.

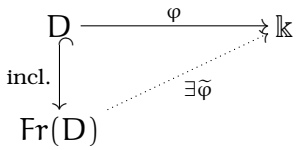
LECCIÓN 16 CUERPOS DE FRACCIONES.

En esta lección nos proponemos a explicar la construcción del *cuerpo de fracción de un dominio de integridad*. Empezaremos planteando la siguiente pregunta ¿es un dominio de integridad isomorfo a un subanillo de un cuerpo?. El porque de esta pregunta lo justificaremos con el ejemplo de los enteros y los racionales. Por supuesto le explicaremos al alumno de que el interese de la respuesta reside en elegir cuerpo con un cierta propiedad universal. Daremos pues la demostración del siguiente resultado que resume la propiedades esenciales de dicha construcción

TEOREMA (Cuerpos de fracciones). Sea D un dominio de integridad.

(i) Existe un cuerpo $\mathrm{Fr}(D)$, llamado el cuerpo de fracciones de D, que contiene a D como subanillo.

(ii) Si $\varphi : D \to \Bbbk$ es un monomorfismo de anillos, cuyo codominio $\Bbbk$ es un cuerpo, entonces existe un único morfismo de cuerpos $\widetilde{\varphi} : \mathrm{Fr}(D) \to \Bbbk$ tal que



es un diagrama conmutativo. Es decir que $\widetilde{\varphi}(t) = \varphi(t)$, para cualquier $t \in D \hookrightarrow \mathrm{Fr}(D)$.

(iii) Sean D y D' dos dominios de integridad y $\varphi : D \to D'$ es un monomorfismo de anillos. Entonces, existe un único morfismo de anillo $\varphi_* : \mathrm{Fr}(D) \to \mathrm{Fr}(D')$ que satisface $\varphi_*(d) = \iota'(\varphi(d))$, siempre y cuando $d \in D$ (aquí $\iota' : D' \to \mathrm{Fr}(D')$ es la inyección canónica)

En particular, si $\Bbbk$ es un cuerpo, entonces $\mathrm{Fr}(\Bbbk) = \Bbbk$, y si D es un subanillo de un cuerpo $\Bbbk$, entonces $\mathrm{Fr}(D) \subseteq \Bbbk$.

BIBLIOGRAFÍA

[1] N. Bourbaki. *Elements of Mathematics. Commutative Algebra. Chapitres 5 á 7.* Hermann, 1972.

[2] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 1 á 4.* Springer-Verlag, Berlin Heidelberg, 2006.

[3] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 5 á 7.* Springer-Verlag, Berlin Heidelberg, 2007.

[4] J. B. Fraleigh. *A First Course in Abstract Algebra.* Addison Wesley, 1999.

[5] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, 1985.

[6] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

Tema IV

Polinomios y fracciones en varias indeterminadas.

Lecciones

Los anillos de polinomios a varias indeterminadas y sus cuerpos de fracciones son imprescindibles en cualquier curso de álgebra. A parte de eso y con visión a los contenidos de los temas de la asignatura del tercer curso **Álgebra III**, este tema es primordial para el buen desarrollo de dicha materia.

Bajo esta perspectiva, el objetivo principal de este tema es introducir el alumno de manera constructiva al mundo de los polinomios y las fracciones racionales en varias indeterminadas. De este modo, hemos intentado dar un definición lo más completa posible del anillo de polinomios en varias indeterminadas evitando las definiciones formales. Por eso hemos incluido el contenido de la primera lección donde introducimos la noción de un álgebra conmutativa libre de un conjunto. En la segunda lección entramos directamente a definir el anillo de polinomios en varias indeterminadas. En la tercera lección daremos la definición de las derivadas parciales, así como algunas de sus propiedades entre otra la fórmula de Taylor y la identidad de Euler. Finalizaremos el tema introduciendo el cuerpo de las fracciones racionales.

Centraremos nuestro interés en que el alumno aprenda a manejar con eficiencia y rapidez las técnicas de cálculo con polinomios y fracciones racionales en varias indeterminadas.

Lección 17 Álgebras tensoriales y álgebras simétricas.

Esta lección es una introducción primordial para poder dar a un alumno del Grado de Matemáticas una definición coherente y completa de lo que es un anillo de polinomios a varias indeterminadas.

Empezaremos, la lección con un recordatorio sobre los espacio vectoriales sobre un cuerpo cualquiera, el producto tensorial, así como la suma directa de un conjunto de espacios vectoriales. Al final del recordatorio, definimos lo que es un álgebra sobre un cuerpo y hablamos del producto tensorial de dos álgebras. Hablaremos también sobre los espacios vectorial $\mathbb{N}$-*graduados* y las álgebras $\mathbb{N}$-*graduadas*.

Pasaremos luego a la definición del álgebra tensorial. Fijamos $\Bbbk$ un cuerpo. Todos los espacios vectoriales son $\Bbbk$-espacio vectoriales. Dado V un espacio vectorial, para cualquier natural $n \geq 1$, consideramos el siguiente producto tensorial

$$V^{\otimes n} := \underbrace{V \otimes_{\Bbbk} \cdots \otimes_{\Bbbk} V}_{n-\text{veces}}$$

con la convención de que $V^{\otimes 0} = \Bbbk$. Denotaremos pues

$$\mathcal{T}_{\Bbbk}(V) = \bigoplus_{n \in \mathbb{N}} V^{\otimes n},$$

esto es un espacio vectorial cuyos elementos se expresan de la siguiente forma

$$p = \sum_{\text{finita}} \alpha_i, \qquad \text{donde cada } \alpha_i \in V^{\otimes i}.$$

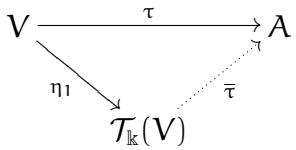
Esta claro que existen aplicaciones canónicas inyectivas: $\eta_0 : \Bbbk \to \mathcal{T}_{\Bbbk}(V)$, $\eta_n : V^{\otimes n} \to \mathcal{T}_{\Bbbk}(V)$. Además $\mathcal{T}_{\Bbbk}(V)$ tiene estructura de anillo[1] cuya regla de multipli-

[1] De hecho un $\Bbbk$-álgebra con el morfismo de anillos η_0

cación viene dada por

$$p \,.\, q \;=\; \left(\sum_i \alpha_i\right) . \left(\sum_j \beta_j\right) \;=\; \sum_{i,j} \alpha_i \otimes_{\Bbbk} \beta_j .$$

$\mathcal{T}_{\Bbbk}(V)$ se le llama la *álgebra tensorial de* V *sobre* $\Bbbk$. Esta satisface la propiedad universal: dada un aplicación $\tau : V \to A$ de V a cualquier $\Bbbk$-álgebra A (no necesariamente conmutativa), existe un único morfismo de $\Bbbk$-álgebra $\overline{\tau} : \mathcal{T}_{\Bbbk}(V) \to A$ que completa la conmutatividad del diagrama



La $\Bbbk$-álgebra $\mathcal{S}_{\Bbbk}(V)$ se define como el cociente de $\mathcal{T}_{\Bbbk}(V)$ por el ideal bilátero generado por el conjunto $\langle v \otimes_{\Bbbk} u - u \otimes_{\Bbbk} v \rangle_{u,v \in V}$, es decir

$$\mathcal{S}_{\Bbbk}(V) \;=\; \mathcal{T}_{\Bbbk}(V) / \langle v \otimes_{\Bbbk} u - u \otimes_{\Bbbk} v \rangle_{u,v \in V} .$$

Esta $\Bbbk$-álgebra conmutativa satisface la misma propiedad universal para las $\Bbbk$-álgebras conmutativas.

Sea ahora I un conjunto cualquiera y consideramos $V = \Bbbk^{(I)}$ el espacio vectorial cuya base viene indexada por I. Salvo isomorfismos canónicos, llamaremos a $\mathcal{S}_{\Bbbk}(V)$ la *álgebra libre conmutativa generada por el conjunto* I. Dada un I-upla $\alpha \in \mathbb{N}^I$ de suporte finito[2], definimos los elementos

$$e^{\alpha} \;=\; \prod_{i \in I} e_i^{\alpha_i}.$$

Entonces el conjunto $\{e^{\alpha}\}_{\alpha \in \mathbb{N}^I \text{ con suporte finito}}$, forma una base del $\Bbbk$-espacio vectorial $\mathcal{S}_{\Bbbk}(V)$. De esta manera la multiplicación de dicha álgebra viene dada por la regla

$$e^{\alpha} \,.\, e^{\beta} \;=\; e^{\alpha+\beta},$$

donde $\alpha + \beta \in \mathbb{N}^I$ es de suporte finito definida por $(\alpha+\beta)_i = \alpha_i + \beta_i$, para todo $i \in I$.

[2]Es decir con un número finito de componentes no nulas

LECCIÓN 18 ANILLOS DE POLINOMIOS EN VARIAS INDETERMINADAS.

En esta lección aplicaremos las nociones generales ya explicadas en la Lección 17, para poder introducir el anillo de polinomios en varias indeterminadas.

Fijamos $\Bbbk$ un cuerpo. Sea I un conjunto, y denotaremos por $\Bbbk[(X_i)_{i\in I}]$ la $\Bbbk$-álgebra conmutativa libre generada por I como ya hemos visto en la Lección 17. Los elementos de esta álgebra se llaman *polinomios con indeterminadas* X_i *a coeficientes en* $\Bbbk$. Cuando $I = \{1, 2, \cdots, \ell\}$, para algún número natural n, denotaremos simplemente $\Bbbk[X_1, X_2, \cdots, X_\ell]$ en vez de $\Bbbk[(X_i)_{i\in I}]$. Para cualquier I-upla $\nu \in \mathbb{N}^I$ de suporte finito[3], ponemos

$$X^\nu = \prod_{i\in I} X_i^{\nu_i}, \quad \text{donde } \nu = (\nu_i)_{i\in I}.$$

como ya se sabe este conjunto es una base del $\Bbbk$-espacio vectorial $\Bbbk[X_1, X_2, \cdots, X_\ell]$. Los elementos X^ν, se llaman *monomios* en las indeterminadas X_i. Para $\nu = 0$, la I-upla nula, se tiene el 1 del anillo. Cada elemento de $f \in \Bbbk[X_1, \cdots, X_\ell]$ se expresa de una forma única como suma finita

$$f = \sum_{\text{finita}} a_\nu X^\nu,$$

con los $a_\nu \in \Bbbk$ no nulos, son en cantidad finita; los a_ν se le llaman *los coeficientes de* f; y los $a_\nu X^\nu$ son los *términos de* f. El *término constante* es pues $a_0 X^0$ que se identifica con a_0. *Un polinomio constante* es cualquier múltiplo por un escalar de 1.

Para cualquier número natural n, consideramos en $\Bbbk[X_1, \cdots, X_\ell]$ el subespacio vectorial $\mathcal{P}_n$ generado por los monomios X^ν tal que $|\nu| = \sum_{1\le i\le \ell} \nu_i \le n$. Un polinomio $f \in \Bbbk[X_1, \cdots, X_\ell]$, se dice que es *homogéneo de grado* n si $f \in \mathcal{P}_n$. La *componente homogénea de grado* n de un polinomio $f = \sum_\nu a_\nu X^\nu \in \Bbbk[X_1, \cdots, X_\ell]$,

[3]véase la Lección 17 de este curso.

es entonces $f_n = \sum_{|\nu|=n} a_\nu X^\nu$, y evidentemente tenemos $f = \sum_n f_n$[4]. Cuando $f \neq 0$, no todos los f_n son nulos, así llamaremos al *grado* (o *grado total*) de f, que denotamos por $\mathrm{grado}(f)$, al número natural más grande n tal que $f_n \neq 0$. Dicho de otra forma al grado de f, es el número natural más grande $|\nu|$ para los milti-índices ν, tal que $\alpha_\nu \neq 0$. Por convención el grado del polinomio nulo es $-\infty$.

El número de monomios en $\Bbbk[X_1, \cdots, X_\ell]$ de grado total q coincide con el número de ℓ-uplas $(n_k)_{1\leq k\leq \ell} \in \mathbb{N}^\ell$ tales que $\sum_{1\leq k\leq \ell} n_k = q$, es decir $\binom{q+\ell-1}{q}$.

Terminaremos esta lección dando las propiedades del grado total respecto a la suma y la multiplicación de dos polinomios. Como conclusión, enunciaremos el hecho de que $\Bbbk[X_1, \cdots, X_\ell]$ es un dominio de integridad.

[4]Esto de hecho induce sobre el anillo de polinomios a ℓ-indeterminadas una $\mathbb{N}$-graduación.

LECCIÓN 19 SUSTITUCIÓN, DIFERENCIAL Y DERIVACIÓN

Esta lección la dedicaremos a la introducción de las sustituciones y las derivaciones en el anillo polinomios a varias indeterminadas. Esto será crucial para el estudio de fracciones racionales, y desde luego más tarde en el estudio es las ecuación algebraicas.

Sea A un $\Bbbk$-álgebra conmutativa. Consideramos una ℓ-upla $\mathbf{a} = (a_1, \cdots, a_\ell)$ de elementos de A. Usando la propiedad universal de la Lección 17, existe pues un morfismo de anillos conmutativos (de hecho de $\Bbbk$-álgebras) definido por

$$\mathcal{S}_{\mathbf{a}} : \Bbbk[X_1, \cdots, X_\ell] \longrightarrow A, \quad \Big(f \longmapsto f(a_1, \cdots, a_\ell)\Big)$$

que se llama la *aplicación de sustitución* (sustituimos cada X_i por el elemento a_i en A).

Si la aplicación de sustitución $\mathcal{S}_{\mathbf{a}}$ es inyectiva, se dice que la familia de elementos $\{a_1, \cdots, a_\ell\}$ son *álgebraicamente independientes (o libres) sobre* $\Bbbk$.

Fijamos ahora un polinomio cualquiera $u \in \Bbbk[X_1, \cdots, X_\ell]$, podemos definir lo que se llama la *función polinómica*:

$$\mathcal{F}_u : A^\ell \longrightarrow A, \quad \Big(\mathbf{b} = (b_1, \cdots, b_\ell) \longmapsto u(b_1, \cdots, b_\ell)\Big)$$

Finalizaremos la primera parte de esta lección con el siguiente resultado.

TEOREMA. Sea $\Bbbk$ un cuerpo, y $\mathbf{a} \in \Bbbk^\ell$, $\ell \geq 1$ un número natural.

(i) Sea $u \in \Bbbk[X_1, \cdots, X_\ell]$, y consideramos el polinomio v obtenido después de sustituir X_i por $X_i - a_i$, para cada $i = 1, \cdots, \ell$. Entonces el término constante de v es justamente $u(\mathbf{a})$.

(ii) Sea $\mathfrak{M}$ el ideal de $\Bbbk[X_1, \cdots, X_\ell]$ generado por los polinomios u tal que satisfacen $u(\mathbf{a}) = 0$. Entonces $\mathfrak{M}$ está generado por los polinomios $X_i - a_i$, para $i = 1, \cdots, \ell$.

Pasaremos ahora a definir lo que son las derivaciones parciales. Se sabe que las aplicaciones $\Bbbk$-lineales:

$$\mathcal{D}_i : \Bbbk[X_1, \cdots, X_\ell] \longrightarrow \Bbbk[X_1, \cdots, X_\ell], \quad \left(X_j \longmapsto \begin{cases} 1, & \text{si } i = j \\ 0, & \text{si no} \end{cases} \right)$$

define una *derivación* del anillo (de hecho de $\Bbbk$-álgebra) de polinomios $\Bbbk[X_1, \cdots, X_\ell]$[5]. La imagen $\mathcal{D}_i(P)$ de un polinomio $P \in \Bbbk[X_1, \cdots, X_\ell]$, se le llamada la *derivada parcial de* P *respecto a* X_i (o simplemente la i-*iésima derivada parcial de* P). A veces se usa la notación $\frac{\partial P}{\partial X_i}$ en vez de $\mathcal{D}_i(P)$.

Dado $\nu = (\nu_i) \in \mathbb{N}^\ell$, se tiene que

$$\mathcal{D}_i(X^\nu) = \begin{cases} \nu_i X_i^{\nu_i - 1} \prod_{j \neq i} X_j^{\nu_j}, & \text{si } \nu_i > 0 \\ 0, & \text{si } \nu_i = 0. \end{cases}$$

De allí se deduce que las aplicaciones $\mathcal{D}_i$ conmutan entre si, es decir $\mathcal{D}_i \circ \mathcal{D}_j = \mathcal{D}_j \circ \mathcal{D}_i$, para cualquier par de índices i, j.

Para $\nu \in \mathbb{N}^\ell$ consideramos

$$\mathcal{D}^\nu = \prod_{1 \leq i \leq \ell} \mathcal{D}_i^{\nu_i}, \quad \text{y } \nu! = \prod_{1 \leq i \leq \ell} (\nu_i!).$$

Dotamos el monoide $\mathbb{N}^\ell$ con el orden producto, se tiene que

$$\mathcal{D}_\nu(X^\mu) = \begin{cases} \frac{\mu!}{(\mu - \nu)!} X^{\mu - \nu}, & \text{si } \nu \leq \mu \\ 0, & \text{si no.} \end{cases}$$

TEOREMA. Sea A un $\Bbbk$-álgebra conmutativa y $\mathbf{a} = (a_1, \cdots, a_\ell)$ una familia de elementos de A junto con un polinomio $u \in \Bbbk[X_1, \cdots, X_\ell]$, y ponemos $\mathbf{b} = u(\mathbf{a})$. Entonces, para cualquier derivación δ de A en A, se tiene que

$$\delta(\mathbf{b}) = \sum_{1 \leq i \leq \ell} \Big(\mathcal{D}_i(u) \Big) (\mathbf{a}) \, . \, \delta(a_i).$$

[5]Esto es cualquier aplicación $\Bbbk$-lineal δ que satisface $\delta(uv) = \delta(u)\, v + u\, \delta(v)$.

Como consecuencia de este resultado se tiene.

TEOREMA (Fórmula de Taylor). Consideramos el anillo de polinomios $\Bbbk[X_1, \cdots, X_\ell, Y_1, \cdots, Y_j]$ donde $\Bbbk$ tiene característica cero. Entonces,

$$u(X+Y) = \sum_\nu \frac{1}{\nu!} \left(\mathcal{D}^\nu u\right)(X)\, Y^\nu.$$

$$u(X) = \sum_\nu \frac{1}{\nu!} \left(\mathcal{D}^\nu u\right)(\mathbf{a})\, (X-\mathbf{a})^\nu.$$

$$u(X) = \sum_\nu \frac{1}{\nu!} \left(\mathcal{D}^\nu u\right)(0)\, X^\nu.$$

para cualquier polinomio $u \in \Bbbk[X_1, \cdots, X_\ell, Y_1, \cdots, Y_j]$ y $\mathbf{a} \in \Bbbk^\ell$.

TEOREMA (Identidad de Euler). Consideramos un polinomio $u \in \Bbbk[X_1, \cdots, X_\ell]$ homogéneo de grado r. Entonces,

$$\sum_{1 \le i \le \ell} X_i\, \mathcal{D}_i(u) = ru.$$

LECCIÓN 20 FRACCIONES RACIONALES.

Finalizaremos, este Tema con esta lección donde introducimos las fracciones racionales y daremos algunas de sus propiedades básicas.

Sea $\Bbbk$ un cuerpo, y consideramos el conjunto totalmente ordenado $I = \{1, \cdots, \ell\}$. Consideramos pues el anillo de polinomios $\Bbbk[X_1, \cdots, X_\ell]$. Como ya se sabe da la Lección 19, este anillo es un dominio de integridad, luego podemos construir su cuerpo de fracciones $\mathrm{Fr}(\Bbbk[X_1, \cdots, X_\ell])$ que denotaremos por $\Bbbk(X_1, \cdots, X_\ell)$. Los elementos de este cuerpo se llaman las *fracciones racionales con coeficientes en* $\Bbbk$ *respecto a las indeterminadas* X_i.

Definimos el *grado (o grado total) de una fracción racional* $f = uv^{-1} \in \Bbbk(X_1, \cdots, X_\ell)$, como $\mathrm{grado}(f) = \mathrm{grado}(u) - \mathrm{grado}(v)$. Daremos luego las propiedades del grado de la suma y la multiplicación de fracciones.

Utilizaremos la propiedad universal de cuerpo de fracciones para poder extender las nociones de sustitución y diferenciales, explicados en la Lección 19, al cuerpo de fracciones racionales.

Sea K un cuerpo que contiene al cuerpo base $\Bbbk$. Escogemos una fracción racional $f = uv^{-1} \in \Bbbk(X_1, \cdots, X_\ell)$ y un elemento $\mathbf{a} = (a_1, \cdots, a_\ell) \in K^\ell$. Se dice que $\mathbf{a}$ es *sustituible en* K *por* f, si $v(\mathbf{a}) \neq 0$; el sustituto es el elemento $f(\mathbf{a}) := u(\mathbf{a})v(\mathbf{a})^{-1}$.

Respecto al las derivación, se sabe que cualquier derivación de $\Bbbk[X_1, \cdots, X_\ell]$ se extiende de manera única a una derivación del cuerpo de fracciones racionales $\Bbbk(X_1, \cdots, X_\ell)$. Enunciaremos las posibles propiedades análogas de la Lección 19 para el cuerpo de fracciones $\Bbbk(X_1, \cdots, X_\ell)$.

BIBLIOGRAFÍA

[1] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[2] J. B. Fraleigh. *A First Course in Abstract Algebra.* Addison Wesley, 1999.

[3] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, 1985.

[4] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

Tema V

Funciones simétricas.

Lecciones

Los cuerpos de las fracciones simétricas juegan un papel primordial en la Teoría de Galois de la ecuaciones algebraicas que el alumno afrentará en el tercer curso del grado en la asignatura de **Álgebra III**.

De es modo, el objetivo principal de este tema es introducir las fracciones racionales simétrica. Luego comprobar, usando las herramientas y las definiciones del Tema III de este curso, que las fracciones simétricas sobre un cuerpo base, forman un cuerpo que es el cuerpo de fracciones de los polinomios simétricos.

Centraremos nuestro interés en que el alumno aprenda a manejar con eficiencia y rapidez las técnicas de cálculo con polinomios simétricos y fracciones racionales simétricas en varias indeterminadas.

LECCIÓN 21 POLINOMIOS SIMÉTRICOS.

En esta lección introduciremos lo que son los polinomios simétricos en varias indeterminadas. Daremos la definición de los polinomios simétrico elementales; así como la propiedad de que son álgebraicamente independientes entre otra propiedades básicas. Esto es de hecho un preliminar para las fracciones racionales de la siguiente lección.

Fijamos $\Bbbk$ un cuerpo de base. Sea ℓ un número natural. Para cualquier permutación $\sigma \in \mathcal{S}_\ell$, consideramos el automorfismo

$$\varphi_\sigma : \Bbbk[X_1, \cdots, X_\ell] \longrightarrow \Bbbk[X_1, \cdots, X_\ell], \quad \left(X_i \longmapsto X_{\sigma(i)}\right).$$

La operación $\sigma \mapsto \varphi_\sigma$ define un morfismo de grupos de $\mathcal{S}_\ell$ en $\mathrm{Aut}_\Bbbk(\Bbbk[X_1, \cdots, X_\ell])$. Denotaremos $\sigma f = \varphi_\sigma(f)$ para $\sigma \in \mathcal{S}_\ell$ y $f \in \Bbbk[X_1, \cdots, X_\ell]$. Se dice que el *polinomio* f *es simétrico* si $\sigma f = f$, para toda permutación $\sigma \in \mathcal{S}_\ell$. Los polinomios simétricos forman una $\Bbbk$-subalgebra (graduada) de $\Bbbk[X_1, \cdots, X_\ell]$ que a continuación denotaremos por $\Bbbk[X_1, \cdots, X_\ell]^{\mathrm{sim}}$.

Para cualquier número natural $k \leq \ell$, consideramos el conjunto $\mathcal{P}_k$ de partes de $I = \{1, 2, \cdots, \ell\}$ con k elementos, y ponemos

$$\mathfrak{s}_k = \sum_{J \in \mathcal{P}_k} \prod_{i \in J} X_i.$$

En particular se tiene que

$$\begin{aligned}
\mathfrak{s}_0 &= 1 \\
\mathfrak{s}_1 &= \sum_{1 \leq i \leq \ell} X_i \\
\mathfrak{s}_2 &= \sum_{1 \leq i < j \leq \ell} X_i X_j \\
&\vdots \quad\quad \vdots \\
\mathfrak{s}_\ell &= X_1 X_2 \cdots X_\ell.
\end{aligned}$$

Convenimos también que $\mathfrak{s}_k = 0$, para $k > \ell$. A veces utilizaremos la notación $\mathfrak{s}_{k,\ell}$, para poder distinguir entre el número de indeterminadas que hemos escogido. Esta claro que los $\mathfrak{s}_k$ son polinomios simétricos homogéneos de grado k; se le llaman *polinomios simétricos elementales de grado* k.

En el anillo de polinomios $\Bbbk[X_1, \cdots, X_\ell, U, V]$, se tiene la relación

$$\prod_{i=1}^{\ell}(U + VX_i) = \sum_{k=0}^{\ell} U^{\ell-k}V^k\mathfrak{s}_k;$$

haciendo sustituciones convenientes se llega a las relaciones:

$$\prod_{i=1}^{\ell}(1 + TX_i) = \sum_{k=0}^{\ell} \mathfrak{s}_k T^k,$$

$$\prod_{i=1}^{\ell}(X - X_i) = \sum_{k=0}^{\ell} (-1)^{n-k}\mathfrak{s}_{n-k}X^k.$$

esta relaciones y otras se usan para comprobar el siguiente resultado

TEOREMA (Polinomios simétricos). Sea $A := \Bbbk[X_1, \cdots, X_\ell]$ un anillo de polinomios en ℓ-indeterminadas y $S := \Bbbk[X_1, \cdots, X_\ell]^{sim}$ el subanillo de polinomios simétricos.

(a) S es, como $\Bbbk$-álgebra, generado por los polinomios elementales $\mathfrak{s}_1, \cdots, \mathfrak{s}_\ell$. Es decir que el conjunto $\{\mathfrak{s}_1^{n_1} \cdots \mathfrak{s}_\ell^{n_\ell}\}_{(n_1,\cdots,n_\ell)\in\mathbb{N}^\ell}$ es una $\Bbbk$-base de S.

(b) Los elementos $\mathfrak{s}_1, \cdots, \mathfrak{s}_\ell$ de A, son álgebraicamente independientes sobre $\Bbbk$.

(c) La familia de monomios $X^\nu = X_1^{\nu_1} \cdots X_\ell^{\nu_\ell}$ tal que $0 \leq \nu_i < i$ para $1 \leq i \leq \ell$, es una base de A como S-módulo. En particular, A es S-libre de base $\ell!$.

Este resultado, permite afirmar que dado un polinomio simétrico f en ℓ-indeterminadas $X_1, \cdots, X_\ell$ homogéneo de grado m, existe un polinomio $Q \in$

$\Bbbk[Y_1, \cdots, Y_m]$ tal que $f = Q(\mathfrak{s}_{1,\ell}, \cdots, \mathfrak{s}_{\ell,\ell})$. Presentaremos pues al alumno, el siguiente procedimiento del cálculo del polinomio Q. La idea es encontrar un polinomio $P \in \Bbbk[Y_1, \cdots, Y_{\ell-1}]$ y un polinomio h simétrico en $X_1, \cdots, X_\ell$ homogéneo de grado $m - \ell$ tal que

$$f = P(\mathfrak{s}_{1,\ell}, \cdots, \mathfrak{s}_{\ell-1,\ell}) + \mathfrak{s}_{\ell,\ell} h. \tag{V.1}$$

Para cualquier polinomio $u \in \Bbbk[X_1, \cdots, X_\ell]$, denotaremos por $\overline{u}$ el polinomio en $X_1, \cdots, X_{\ell-1}$

$$\overline{u}(X_1, \cdots, X_{\ell-1}) = u(X_1, \cdots, X_{\ell-1}, 0).$$

Con esta notación los polinomios $\overline{\mathfrak{s}_{1,\ell}}, \cdots, \overline{\mathfrak{s}_{\ell-1,\ell}}$ son los polinomios simétricos elementales en las indeterminadas $X_1, \cdots, X_{\ell-1}$ y la fórmula de la ecuación (V.1), se convierte en

$$\overline{f} = P\left(\overline{\mathfrak{s}_{1,\ell}}, \cdots, \overline{\mathfrak{s}_{\ell-1,\ell}}\right).$$

A modo de ejemplo para $\ell = 3$ y

$$f = X_1^2(X_2 + X_3) + X_2^2(X_1 + X_3) + X_3^2(X_2 + X_1), \text{ tenemos}$$
$$\overline{f} = X_1^2 X_2 + X_1 X_2^2 = X_1 X_2 (X_1 + X_2) = \overline{\mathfrak{s}_1}\,\overline{\mathfrak{s}_2}.$$

Formulamos ahora $g = f - \mathfrak{s}_1\mathfrak{s}_2$, se tiene que $g = -3X_1X_2X_3$, luego

$$f = \mathfrak{s}_1\mathfrak{s}_2 - 3\mathfrak{s}_3.$$

Otra de las aplicación del resultado anterior, es el siguiente isomorfismo de $\Bbbk$-álgebras $\mathbb{N}$-graduadas. Consideramos ℓ indeterminadas $S_1, \cdots, S_\ell$ y consideramos la $\Bbbk$-álgebra de polinomios $\Bbbk[S_1, \cdots, S_\ell]$ con la $\mathbb{N}$-graduación donde cada S_i es homogéneo de grado (o *peso*) i. Los elementos homogéneos de peso k, son los polinomios $\sum_\nu a_\nu S^\nu$ con $a_\nu = 0$ cuando $\sum_{1 \le i \le \ell} i.\nu_i \neq k$. Por otro lado, consideramos $\Bbbk[X_1, \cdots, X_\ell]$ con la $\mathbb{N}$-graduación ordinaria, donde cada uno de los polinomios simétricos $\mathfrak{s}_{k,\ell}$ es homogéneo de grado k. Según el Teorema anterior se tiene que la aplicación

$$\varphi_\ell : \Bbbk[S_1, \cdots, S_\ell] \longrightarrow \Bbbk[X_1, \cdots, X_\ell]^{\mathrm{sim}}, \quad \left(g \longmapsto g(\mathfrak{s}_{1,\ell}, \cdots, \mathfrak{s}_{k,\ell})\right),$$

es un isomorfismo de $\Bbbk$-álgebras $\mathbb{N}$-graduadas, tal que para cualquier $0 \leq j \leq \ell$, el siguiente diagrama es conmutativo

$$\begin{array}{ccc} \Bbbk[S_1, \cdots, S_j] & \xrightarrow{\quad \iota \quad} & \Bbbk[S_1, \cdots, S_\ell] \\ \downarrow{\scriptstyle \varphi_j} & & \downarrow{\scriptstyle \varphi_\ell} \\ \Bbbk[X_1, \cdots, X_j]^{\mathrm{sim}} & \xleftarrow{\quad \tau \quad} & \Bbbk[X_1, \cdots, X_\ell]^{\mathrm{sim}}, \end{array}$$

donde ι es la inclusión canónica y τ es el morfismo

$$g \longmapsto g(X_1, \cdots, X_j, 0, \cdots, 0).$$

De allí sacaremos el siguiente resultado

> TEOREMA. Para cualquier par de número naturales ℓ, k, sea $S_k^{(\ell)}$ el $\Bbbk$-espacio vectorial generado por los polinomios simétricos en $X_1, \cdots, X_\ell$, homogéneos de grado k. Entonces, para cualquier otro número natural j que satisface $0 \leq k \leq j \leq \ell$, la aplicación $f \longmapsto f(X_1, \cdots, X_j, 0, \cdots, 0)$ es un isomorfismo entre $S_k^{(\ell)}$ y $S_k^{(j)}$.

a modo de ejemplo, tenemos

$$\sum_{i=1}^{\ell} X_i^3 \;=\; \mathfrak{s}_{1,\ell}^3 - 3\mathfrak{s}_{1,\ell}\,\mathfrak{s}_{2,\ell} + 3\mathfrak{s}_{3,\ell}\,,$$

para cualquier $\ell \geq 3$. La conmutatividad del diagrama anterior, nos da

$$\begin{aligned} X_1^3 + X_2^3 \;&=\; \mathfrak{s}_{1,2}^3 - 3\mathfrak{s}_{1,2}\,\mathfrak{s}_{2,2} \\ X_1^3 \;&=\; \mathfrak{s}_{1,1}^3. \end{aligned}$$

LECCIÓN 22 FRACCIONES RACIONALES SIMÉTRICAS.

Finalizaremos pues este Tema con esta lección sobre las fracciones racionales. Daremos la demostración del hecho que el cuerpo de fracciones de los polinomios simétricos coincide con el cuerpo de fracciones racionales simétricas.

Como ya hemos explicado en la Lección 21, para cualquier permutación $\sigma \in \mathcal{S}_\ell$, consideramos el automorfismo

$$\varphi_\sigma : \Bbbk[X_1, \cdots, X_\ell] \longrightarrow \Bbbk[X_1, \cdots, X_\ell], \quad \left(X_i \longmapsto X_{\sigma(i)}\right).$$

Este automorfismo se extiende de forma canónica, según la Lección 16, a un automorfismo del cuerpo de fracciones racionales $\Bbbk(X_1, \cdots, X_\ell)$, que denotaremos por ψ_σ. La operación $\sigma \mapsto \psi_\sigma$ define un morfismo de grupos de $\mathcal{S}_\ell$ en $\mathrm{Aut}_\Bbbk(\Bbbk(X_1, \cdots, X_\ell))$. Denotaremos $\sigma f = \psi_\sigma(f)$ para $\sigma \in \mathcal{S}_\ell$ y $f \in \Bbbk(X_1, \cdots, X_\ell)$. Se dice que el *la fracción racional* f *es simétrica* si $\sigma f = f$, para toda permutación $\sigma \in \mathcal{S}_\ell$. El conjunto de todas las fracciones simétricas forma un subcuerpo de $\Bbbk(X_1, \cdots, X_\ell)$ que a continuación denotaremos por $\Bbbk(X_1, \cdots, X_\ell)^{\mathrm{sim}}$.

De otro lado, es fácil comprobar que el anillo de polinomio simétricos es un dominio de integridad. El cuerpo de fracciones de este último coincide pues con las fracciones racionales simétricas.

TEOREMA (De fracciones simétricas). El cuerpo de fracciones racionales simétricas en $X_1, \cdots, X_\ell$ es el cuerpo de fracciones del anillo de polinomios simétricos en $X_1, \cdots, X_\ell$. Es decir

$$\Bbbk(X_1, \cdots, X_\ell)^{\mathrm{sim}} = \mathrm{Fr}(\Bbbk[X_1, \cdots, X_\ell]^{\mathrm{sim}}).$$

como consecuencia se tiene

TEOREMA. Sean $\mathfrak{s}_1, \cdots \mathfrak{s}_\ell$ los polinomios simétricos elementales en $X_1, \cdots, X_\ell$. Para cualquier fracción racional $g \in \Bbbk(S_1, \cdots, S_\ell)$, la sucesión $(\mathfrak{s}_1, \cdots \mathfrak{s}_\ell)$ es sustituible en g, y la aplicación $g \longmapsto g(\mathfrak{s}_1, \cdots \mathfrak{s}_\ell)$ es un isomorfismo de $\Bbbk(S_1, \cdots, S_\ell)$ en el cuerpo de fracciones racionales simétricas $\Bbbk(X_1, \cdots, X_\ell)^{\mathrm{sim}}$.

BIBLIOGRAFÍA

[1] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[2] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, 1985.

Tema VI

Elementos de Teoría de Grupos finitos.

Lecciones

En este tema trataremos las nociones básica de la teoría de grupos finitos. El listado de las lecciones viene expuesto en el anterior sumario, mientras que en el preámbulo de cada una de ellas viene resumido su contenido.

El objetivo principal del tema es de dotar al alumno con las herramientas necesarias de la teoría de grupos finitos, para poder afrentar el imprescindible uso de las mismas en el desarrollo del aprendizaje de la teoría de Galois de ecuaciones algebraicas en el tercer curso de la asignatura **Álgebra III**. Especialmente, que el alumno sea capaz de determinar completamente ciertos grupos de Galois de extensiones de Galois finitas; ó al menos que detecte algunas de las propiedades de estos grupos, por ejemplo ser resoluble ó ser nilpotente, etc.

Centraremos pues nuestro objetivo en que el alumno coordinará bien todas las definiciones así como las propiedades básicas de algunos grupos con especial interés. Para ello expondremos varios ejemplos concretos.

LECCIÓN 23 GRUPOS Y HOMOMORFISMOS DE GRUPOS.

En esta lección introducimos la noción de grupo, así como morfismos entre grupos. Completaremos la lección con varios ejemplos de grupos: el grupo simétrico, el grupo lineal y el grupo diedro.

Un *grupo* es un conjunto G dotado de una *ley de composición (o operación interna)*, que es una aplicación $-.-: G \times G \to G$ que satisface [1]

- *La asociatividad*:

$$x.(y.z) = (x.y).z, \quad \text{para todos } x, y, z \in G.$$

- *Elemento neutro*: existe un elemento (*neutro*) $e \in G$ tales que

$$x.e = e.x = x, \quad \text{para todo } x \in G.$$

- *Inverso*: Para cada elemento $x \in G$ existe un elemento $y \in G$ tal que

$$x.y = y.x = e, \quad \text{donde } e \text{ es el elemento neutro de } G.$$

G se dice que es *abeliano* cuando la ley de composición satisface

- *La conmutatividad*:

$$x.y = y.x, \quad \text{para todo } x, y \in G.$$

Enunciaremos las propiedades básica que se deducen directamente de esta definición: El neutro es único, el inverso de cada elemento lo es también, etc.

[1] Un conjunto con una ley de composición que satisface nada más que la asociatividad y la existencia del elemento neutro, se le llama un *monoide*.

Un morfismo de grupos es una aplicación $f : G \to G'$ que satisface

$$f(xy) = f(x)f(y), \text{ para todo } x, y \in G, \quad f(e) = e',$$

donde e (respectivamente e') es el elemento neutro de G (respectivamente de G'). *Un isomorfismo de grupo* es un morfismo de grupos cuya aplicación subyacente es biyectiva. A modo de ejemplo, dado un grupo cualquiera G y fijamos un elemento $g \in G$, existe pues un morfismo de grupos $\varphi_g : (\mathbb{Z}, +) \to G$ definido por $n \mapsto g^n$ del grupo abeliano de los números entero hacia G.

Dado un grupo G con elemento neutro e y x un elemento de G. Se dice que x *tiene orden* k, si k *es el más pequeño número natural* que satisface $x^k = e$. Si tal número no existe, se dice que x *es de orden infinito. El orden de un grupo finito*, es el número de sus elementos.

Se dice que un subconjunto $\chi \subseteq G$, es *un conjunto generador de* G, si cualquier elemento $x \in G$ se escribe de forma

$$x = \mathfrak{x}_1^{n_1} \cdots \mathfrak{x}_l^{n_l}, \quad \text{donde cada } \mathfrak{x}_i \in \chi \text{ y } n_i \in \mathbb{N}.$$

Presentaremos los siguientes ejemplos no triviales de grupos que van hace de mucho interese durante este curso:

EL GRUPO SIMÉTRICO (O DE PERMUTACIONES) $\mathcal{S}_n$. Se trata del grupo de permutaciones de n elementos. Es decir el grupo de las aplicación biyectivas de un conjunto de n elementos cuya ley de composición viene dada por la composición usual de aplicaciones y cuyo elemento neutro es la aplicación identidad. Dada la importancia de estos grupos, conviene dar al alumno más detalles sobre estos.
Para denotar los elementos de $\mathcal{S}_n$, vamos a emplear la siguiente notación: un conjunto de n-elementos pueda numerase como $\{1, 2, \cdots, n\}$; así una permuta-

ción σ la podemos representar como

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix},$$

donde los k_i son en total n elementos con $1 \leq k_i \leq n$. Esto significa que $\sigma(i) = k_i$, para todo $i \in \{1, 2, \cdots, n\}$. Para $n = 4$, tenemos por ejemplo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix},$$

y sus composiciones son

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \qquad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Como ya se puede apreciar $\mathcal{S}_n$ no es abeliano. De otro lado, es un grupo *finito*, es decir con un número finito de elementos que son en total $n!$. Es decir que $\mathcal{S}_n$ es de Orden $n!$, (recuerde *el orden de un grupo finito* es el número de su elementos).

Un cíclo es cualquier permutación de $\mathcal{S}_n$ de forma

$$\sigma = \begin{pmatrix} k_1 & k_2 & k_3 & \cdots & k_n \\ k_2 & k_3 & k_4 & \cdots & k_1 \end{pmatrix}, \quad \text{o simplemente } \sigma = \left(k_1, k_2, \cdots, k_n\right).$$

Una transposición es un cíclo de forma (k_i, k_j) para $k_i \neq k_j$, es decir aquella permutación γ tal que $\gamma(k_i) = k_j$, $\gamma(k_j) = k_i$ y $\gamma(l) = l$ para $l \neq k_i, k_j$. Dicho de otra forma, γ permuta k_i con k_j y deja inalterables los de más elemento de $\{1, 2, \cdots, n\} \backslash \{k_i, k_j\}$. Comprobaremos que cualquier permutación es producto de cíclos, de allí producto de transposiciones. La descomposición en producto de transposiciones no es única, sin embargo el *número* de transposiciones que la forma *es* bien definido módulo 2 (es decir *par o impar*). *Una permutación es par (o impar)* cuando lo sea ese número de transposiciones. A modo de ejemplo, la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 7 & 1 & 3 & 4 \end{pmatrix}, \quad \text{es la composición } \sigma = (1, 2, 5)(3, 6)(4, 7).$$

Usando cíclos uno puede calcular los elementos de $\mathcal{S}_n$ (usando ordenador). Por ejemplo para $n = 3$, se tiene las seis permutaciones,

$$\mathcal{S}_3 = \Big\{1; (1,2); (1,3); (2,3); (1,2,3) = (1,2)(2,3); (1,3,2) = (1,3)(2,3)\Big\}.$$

EL GRUPO LINEAL $GL_n(\Bbbk)$. Sea $\Bbbk$ un cuerpo y consideramos $GL_n(\Bbbk)$ el conjunto de todas las $n \times n$-matrices invertibles. Este es un grupo con ley de composición la multiplicación usual de matrices y cuyo elemento neutro es la matriz identidad. Otra forma de definir tal grupo, salvo isomorfismo, es mediante el grupo de automorfismos $\Bbbk$-lineales del $\Bbbk$-espacio vectorial de dimensión n, $\Bbbk^n$.

EL GRUPO DIEDRO D_n. Abstracta-mente D_n es un grupo generado por dos elementos $\{a, b\}$ con a que es de orden $n \geq 3$, y b de orden 2, sujetos a la relación $ba = a^{-1}b$. Los elementos de D_n se ponen pues en forma estándar $a^i b^j$, con $0 \leq i < n$, $0 \leq j < 2$.

Lección 24 Subgrupos, grupos cocientes y teoremas de isomorfía.

En esta lección introduciremos la noción de un subgrupos, subgrupos normales y grupos cocientes. Abordaremos también las relaciones de equivalencia módulo subgrupos y en particular la de conjugación, así como el índice de un subgrupo junto con el Teorema de Lagrange. Concluimos la lección enunciando el teorema la descomposición de un morfismo de grupos, así como varios teoremas de isomorfía.

Sea G un grupo y H un subconjuto de G. Se dice que H es *un subgrupo de* G si H satisface lo siguiente:

(i) $e \in H$;

(ii) $x \in H$ e $y \in H$, implica que $xy \in H$;

(iii) $x \in H$ implica $x^{-1} \in H$.

Esta definición implica las siguientes equivalentes aserciones:

(i) H es un subgrupo de G;

(ii) H es un subconjunto no vacío, y si $x, y \in H$, entonces $xy^{-1} \in H$;

(iii) H es un subconjunto no vacío, y si $x, y \in H$, entonces $x \in H$ y $y^{-1} \in H$;

(iv) H es estable por la ley de composición de G, y esta ley induce una estructura de grupo sobre H.

El conjunto $\{e\}$ es el subgrupo más pequeño de G. Así, la intersección de cualquier familia de subgrupos de G es también un subgrupo de G. Dado pues

un conjunto I de G, podemos considerar le familia de todos los subgrupos de G que contiene a I. Esto nos da un subgrupo de G, que llamaremos *el subgrupo generado por* I *(o que* I *es un sistema de generadores de ese subgrupo).*

Dado un morfismo de grupos $f : G \to G'$, el *núcleo* de f,

$$\mathrm{Ker}(f) = \{x \in G | \, f(x) = e'\}$$

es un subgrupo de G, así lo es también la *imagen* de f,

$$\mathrm{Im}(f) = \{f(x) \in G' | \, x \in G\}.$$

Si $x \in \mathrm{Ker}(f)$, entonces $yxy^{-1} \in \mathrm{Ker}(f)$, para cualquier $y \in G$. De allí la siguiente definición, un subgrupo H de G, se dice que es *un subgrupo normal* si

$$yHy^{-1} = H, \quad \text{para todo } y \in G.$$

Emplearemos la siguiente notación: $H \leq G$ para decir que H es un subgrupo de G y $H \lhd G$, para decir que H es un soubgrupo normal de G.

Sea $\mathcal{R}$ una relación de equivalencia en un grupo G. Se dice que $\mathcal{R}$ es *compatible por la derecha* con la ley de composición de G, si toda relación $x \mathcal{R} y$ implica $xz \mathcal{R} yz$, para todo $z \in G$.

TEOREMA (Relación de equivalencia compatible). Sea $\mathcal{R}$ una relación de equivalencia compatible por la derecha con la ley de composición de un grupo G. Entonces, los elementos de la clase de equivalencia del elemento neutro e de G, forma un subgrupo H de G y la relación $x\mathcal{R}y$ es equivalente a la relación $xy^{-1} \in H$, para todo $x, y \in G$. Recíprocamente, dado un subgrupo H de G, la relación $xy^{-1} \in H$ es una relación de equivalencia compatible por la derecha con la ley de composición de G, por la cual H es la clase de e.

El cardinal del conjunto de clases de equivalencia [módulo H] por la derecha (i.e. con la relación $xy^{-1} \in H$), se le llama *el índice de* H *respecto a* G, que

denotaremos por $(G : H)$. Este cardinal coincide con el cardinal del conjunto de clases de equivalencia por la izquierda.

TEOREMA (Lagrange). Sea G un grupo y $H \subset K$ dos subgrupos de G.

(i)
$$(G : K)(K : H) = (G : H) :$$

(ii) Si G es un grupo finito de orden n y H un subgrupo de orden m, entonces
$$n = (G : H)\, m.$$

Sea G un grupo y H un subgrupo normal de G. Consideramos la relación de equivalencia $xy^{-1} \in H$, dado que H es normal esto es equivalente a que $x^{-1}y \in H$. Es decir, que ambas relaciones (izquierda derecha) coinciden. Esto permite dotar el conjunto cociente G/H con un estructura de grupo, tal que $G \to G/H$ es un morfismo de grupos suprayectivo.

Un grupo G, se dice que es *simple*, si $G \neq \{e\}$ y no tiene subgrupos normales propios, es decir distintos de G y $\{e\}$.

TEOREMA (Descomposición de homomorfismos.). Sea $f : G \to G'$ un morfismo de grupos.

(a) El núcleo de $\mathrm{Ker}(f)$ es un subgrupo normal de G.

(b) La imagen de f, $\mathrm{Im}(f)$ es un subgrupo de G'.

(c) La aplicación $\widetilde{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ inducida por f pasando al cociente, es un isomorfismo de grupos.

(d) f se descompone de forma $f = \tau \widetilde{f} \pi$, donde $\tau : \mathrm{Im}(f) \to G'$ es la inyección canónica y $\pi : G \to G/\mathrm{Ker}(f)$ es la proyección canónica.

TEOREMA (Lema de Zassenhaus). Sea G un grupo y $H, K \leq G$ dos subgrupos de G juntos con dos subgrupos normales $N \lhd H$, $M \lhd K$. Entonces

(a) $M.(K \cap N)$ es un subgrupo normal de $M.(H \cap K)$.

(b) $N.(H \cap M)$ es un subgrupo normal de $N.(H \cap K)$.

(c) Hay un isomorfismo de grupos

$$\Big(M.(H \cap K)\Big) / \Big(M.(K \cap N)\Big) \;\cong\; \Big(N.(H \cap K)\Big) / \Big(N.(H \cap M)\Big).$$

Finalizaremos esta lección con el siguiente teorema de isomorfía.

TEOREMA (De isomorfía.). Sea G un grupos, A, B dos subgrupos de G y N un subgrupo normal de G.

(i) Si para cualquier $a \in A$ y $b \in B$, se tiene que $aba^{-1} \in B$ (se dice que A *normaliza* a B), entonces $AB = BA$ es un subgrupo de G, $A \cap B$ es un subgrupo normal de A, y B es un subgrupo normal de AB. Además, la inyección canónica $A \to AB$, define pasando al cociente un isomorfismo $A/A \cap B \;\cong\; AB/B$.

(ii) Sea H un subgrupo de G que contiene a N. El cociente H/N es un subgrupo normal de G/N si, y sólo si H es normal en G, y los grupos G/N, $(G/H)/(H/N)$ son isomorfos.

(iii) Sea H un subgrupo de G. Entonces HN es un subgrupo de G, y N es normal también en HN. Además $H \cap N$ es normal es G y los grupos cocientes $G/(H \cap N)$ y HN/N son isomorfos.

LECCIÓN 25 TEOREMA DE JORDAN-HÖLDER.

En la primera parte de esta lección introducimos las series de composición en grupos, luego definimos lo que es la serie de Jordan-Hölder. La segunda parte la dedicaremos a la demostración del teorema de Jordan-Hölder. Este resultado será crucial en abordar los grupos resolubles y nilpotentes en la Lección 27.

Dado G un grupo con elemento neutro e, *una serie de composición de* G, es una sucesión $\{G_i\}_{0\leq i\leq n}$ finita de subgrupos de G tales que

$$G_n = \{e\} \lhd G_{n-1} \lhd \cdots\cdots \lhd G_1 \lhd G_0 = G,$$

es decir que cada G_{i+1} es normal en G_i, $i = 0, 1\cdots, n-1$. Los grupos cocientes G_i/G_{i+1}, se llaman *lo cocientes (o factores) de la serie*. Una serie Σ' se dice que *es más fina* que otra serie Σ, si Σ es extraída de Σ', es decir que cada término de la sucesión Σ pertenece a Σ' y hay más términos en Σ' que Σ.

Sean $\{G_i\}_{0\leq i\leq n}$ y $\{H_j\}_{0\leq j\leq m}$ dos sucesiones de composición, respectivamente, de dos grupos G y H. Se dice que las dos sucesiones *son equivalentes*, si $n = m$ y existe una permutación σ del conjunto $\{0, 1, \cdots, n-1\}$ tales que los grupos cocientes de serie son mutuamente isomorfos:

$$H_{\sigma(i)}/H_{\sigma(i)+1} \cong G_i/G_{i+1}, \quad \text{para todo } i = 0, 1\cdots, n-1.$$

TEOREMA (Schreier). Sean Σ_1, Σ_2 dos series de composición de un grupo G. Entonces existen dos series de composición Σ_1', Σ_2' de G equivalentes y más finas que Σ_1, Σ_2, respectivamente.

Una serie de Jordan-Hölder de un grupo G, es una serie de composición estrictamente decreciente Σ de G, tal que no exista otra serie de composición estrictamente decreciente, diferente de Σ y más fina que Σ.

TEOREMA (Jordan-Hölder). Sea G un grupo.

(a) Para que una serie de composición de G sea una serie de Jordan-Hölder, es necesario y suficiente que todos sus cocientes sen grupos simple.

(b) Dos sucesiones de Jordan-Hölder de G, son siempre equivalentes.

(c) Supongamos que G tiene una serie de Jordan-Hölder. Si Σ es cualquier serie de composición estrictamente decreciente de G, entonces existe una serie de Jordan-Hölder más fina que Σ.

La longitud de un grupo, es la cota superior de todos los números n tales que exista una serie de composición estrictamente decreciente $\{G_i\}_{0\leq i\leq n}$ de G.

Como primera consecuencias, se tiene: Si G tiene una serie de Jordan-Hölder, entonces la longitud de G es finita y coincide con la longitud de esta misma serie. Si G no admite una serie de Jordan-Hölder, entonces su longitud es infinita. El grupo reducido a su elemento neutro, es de longitud 0, mientras que un grupo es simple si y sólo si su longitud es 1. De allí, se tiene también que

- Para cualquier subgrupo normal $N \lhd G$, se tiene que la longitud de G es la suma de las longitudes de los grupos N y G/N.
- Si $\{G_i\}_{0\leq i\leq n}$ es una serie de composición de G, entonces la longitud de G es la suma de las longitudes de los grupos cocientes de la serie G_i/G_{i+1}, $0 \leq i \leq n-1$.

LECCIÓN 26 GRUPOS ACTUANDO SOBRE CONJUNTOS.

Esta lección la dedicaremos al estudio de la acción de grupos sobre conjuntos. Después de dar las definiciones básicas de lo que es una acción, los estabilizadores, las orbitas, etc. Pasaremos a analizar la acción canónica del caso del grupo de automorfismos de un grupo sobre el mismo grupo, en particular la acción de conjugación mediante automorfismos interiores. Finalizaremos la lección con un resultado sobre los G-conjuntos homogéneos.

Sea E un conjunto y G un grupo con elemento neutro e. Se dice que G *actúa por la derecha sobre* E, si existe una aplicación $E \times G \to E$, $(u, x) \mapsto u^x$, que satisface

$$(u)^{xy} = \Big((u)^x\Big)^y, \quad u^e = u, \quad \text{para todo } x, y \in G, \text{ y } u \in E.$$

Dar una acción por la derecha de G sobre E, es equivalente, a dar un morfismo de grupos de G hacia al grupo opuesto de todas las auto-biyecciones de E. Emplearemos a veces, la frase E *es un* G*-conjunto por la derecha*, para decir que G actúa por la derecha sobre E. De este modo podemos definir lo que es un *morfismo de* G*-conjuntos* $f : E \to E'$, como aquellas aplicaciones que son compatibles con la acción de G, es decir que satisfacen:

$$f(u^x) = \Big(f(u)\Big)^x, \quad \text{para todo }, u \in E, \ x \in G.$$

A modo de ejemplo, consideramos $\mathcal{S}_G$ el conjunto de todos los subgrupos de G. Se puede fácilmente ver que, si $H \in \mathcal{S}_G$, entonces el conjunto $x^{-1}Hx$ es también un subgrupo de G. Esto quiere decir que G actúa por la derecha, mediante *conjugación*, sobre $\mathcal{S}_G$. Esta claro que esta acción es un caso particular de la acción de todo el grupo de automorfismo de G sobre $\mathcal{S}_G$. De allí, la siguiente definición: Si H_1, H_2 son dos grupos de G, entonces se dice que H_1 es *conjugado con* H_2, si existe un elemento $y \in G$, tal que

$$H_1 = y^{-1}H_2y.$$

Consideramos un grupo G actuando sobre un conjunto E. Para cualquier subconjunto U de E, se consideran los siguientes subconjuntos de G:

$$\mathcal{E}_U = \left\{x \in G | U^x = U\right\} \quad \text{y } \mathcal{F}_U = \left\{x \in G | u^x = u,\ \forall u \in U\right\}.$$

llamado, respectivamente, *estabilizador* y *fijador de* U. Allí, la notación U^x significa todos los elemento de de forma v^x, para algún $v \in U$. Por definición, se tiene pues que $\mathcal{E}_U$ y $\mathcal{F}_U$ son dos subgrupos de G, con $\mathcal{F}_U$ es normal.

A continuación resumimos algunas de las propiedades de los *automorfismos interiores*. Sea G un grupo.

(a) Dado un elemento $g \in G$, la aplicación $\mathrm{Int}_g : G \to G$, definida por $x \mapsto xgx^{-1}$ es un automorfismo de grupos de G, llamado *automorfismo interior de* G *definido por* g.

(b) La aplicación $g \in G \mapsto \mathrm{Int}_g \in \mathrm{Aut}(G)$ es un morfismo de grupos cuyo núcleo es el centro de G y su imagen es subgrupo normal de $\mathrm{Aut}(G)$.

(c) Un subgrupo de G es normal si, y sólo si es estable bajo automorfismos interiores de G.

Sea H un subgrupo de G, se dice que H es *característico* si es estable bajo cualquier automorfismo de G. Es decir que $\mathcal{E}_H = H$, respecto de la acción por la izquierda de $\mathrm{Aut}(G)$ sobre G. El centro de G es un ejemplo de de tipo de subgrupos.

Sea G un grupo y E un G-conjunto por la derecha. Dado un elemento $u \in E$, se dice que $v \in E$ es *conjugado* de u en la operación de G sobre E, si existe $g \in G$ tal que $v = u^g$. El conjunto de todos los elementos *conjugados a* u, se le denota por $\mathcal{O}\mathrm{rb}_u$ y se le llama *la orbita* de u. De allí las siguientes observaciones:

(d) La relación definida por $\ll u$ es conjugado de $v \gg$ define una relación de

equivalencia en E. Por ejemplo, en $\mathcal{S}_3$ hay tres clases de equivalencia módulos conjugación:

$$\Big[1\Big]\,,\ \Big[(1,2),(1,3),(2,3)\Big]\,,\ \Big[(1,2,3),(1,3,2)\Big]\,.$$

(e) La aplicación $x \mapsto u^x$ de G en E, se le llama *la aplicación orbital definida por* $u \in E$.

(f) La acción de G sobre E se dice que es *fiel (o* G *actúa fielmente sobre* E*)*, si para cualquier $u \in E$, la aplicación orbital de u es inyectiva.

(g) Los estabilizadores de dos elementos conjugados en E, son subgrupos conjugados.

Sea E un G-conjunto, se dice que G actúa *transitivamente* sobre E, o la acción de G sobre E es *transitiva*, si existe elemento de $u \in E$ tal que $\mathcal{O}rb_u = E$. Es decir que hay una sola orbita. Un G-conjunto E, se dice que es *homogéneo* si G actúa transitivamente sobre E. Un ejemplo es el siguiente
Dado un subgrupo H de G, es fácil ver que G actúa por la derecha sobre el conjunto cociente G/H módulos la relación de equivalencia translación por la derecha $xy^{-1} \in H$, i.e. $(Hx)^g = Hxg$. Sea $N = \{x \in G|, xH = Hx\}$ el *normalizador* de H. N opera por la izquierda sobre G/H, mediante $(n, Hx) \mapsto nHx = Hnx$. Esta acción induce una acción trivial sobre H, luego se pueda pasar a una acción del grupo cociente N/H sobre G/H. Sea $\varphi : (N/H)^o \to \mathcal{S}_{G/H}$ [2] el morfismo de grupo asociado, se tiene pues:

(•) G/H es un G-conjunto homogéneo.

(•) La aplicación φ induce un isomorfismo de $(N/H)^o$ sobre el grupo de automorfismos del G-conjunto G/H.

[2]La notación G^o, para un grupo G, significa el grupo opuesto de G.

Finalizaremos esta lección con el siguiente resumen:

TEOREMA (G-conjuntos homogéneos). Sea G un grupo.

(i) Sea E un G-conjunto homogéneo y $u \in E$, $\mathcal{E}_{\{u\}} = H$ y $K \leq G$ tal que $H \subseteq K$. Existe un único morfismo de G-conjuntos suprayectivo, $f : G/K \to E$ tal que $f(K) = u$. Si $H = K$, entonces f es un isomorfismo.

(ii) Cualquier G-conjunto homogéneo es isomorfo a un G-conjunto homogéneo de forma G/H, donde H es un subgrupo de G.

(iii) Si H_1, H_2 son dos subgrupos de G, entonces G/H_1, G/H_2 son dos G-conjuntos isomorfos, si y sólo si H_1 y H_2 son conjugados.

LECCIÓN 27 EXTENSIONES, GRUPOS RESOLUBLES Y GRUPOS NILPOTENTES.

En esta lección introducimos unas importantes clases de grupos, resolubles y nilpotentes. Después de dar las definiciones, le presentaremos al alumno varias caracterizaciones de ambas clases. La lección contiene, también una pequeña introducción sobre las extensiones de grupos, que nos servirá para abordar los producto semi-directos.

Sean G, G' dos grupos, *una extensión de* G *por* G' es un terna $\mathcal{E} = (E, i, p)$ formada por un grupo E y una inyección $i : G' \to E$, y una proyección $p : E \to G$ tales que $\mathrm{Im}(i) = \mathrm{Ker}(p)$. *Una sección* (resp. *retracción*) de $\mathcal{E}$ es un morfismo de grupos $s : G \to E$ (resp. $r : E \to G'$) tal que $p \circ s = id_G$ (resp. $r \circ i = id_G$). *Una extensión central*, es un extensión de G por un grupo abeliano G'. De manera natural, se definen los morfismos y isomorfismos entre extensiones.

Dados dos grupos G, E y un morfismo $\tau : G \to \mathrm{Aut}(E)$, denotaremos por $\tau(g)(f) = f^g$. Se define el producto *semi-directo de* G *por* E *relativamente a* τ $E \times_\tau G$, al conjunto $E \times G$, con la ley de composición (i.e. la multiplicación):

$$(u, g) ._\tau (v, h) = (uv^g, gh).$$

El producto semi-directo $E \times_\tau G$ es un grupo con $i : E \to E \times_\tau G$ es la inyección canónica, es un morfismos de grupos, así lo es también la proyección canónica $p : E \times_\tau G \to G$. Además (E, i, p) es una extensión de G por E con la sección $s : G \to E \times_\tau G$, $g \mapsto (e, g)$ (e es el elemento neutro de E).

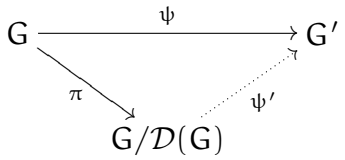
TEOREMA. Sea G un grupo con elemento neutro e, H, K dos subgrupos de G, con H normal, $H \cap K = \{e\}$ y $H.K = G$. Sea τ la acción de K sobre H por automorfismos interiores. La aplicación $(h, k) \longmapsto hk$ del producto semi-directo $H \times_\tau K$ hacia a G, es un isomorfismo de grupos (*se dice pues que* G *es el producto semi-directo de* K *por* H).

Dado G un grupo, x, y dos elementos de G, se le llama el *conmutador* de x e y, al elemento $(x, y) = x^{-1}y^{-1}xy \in G$. Se le llama al *subgrupo derivado de* G, al subgrupo de G generado por todos los conmutadores. Presentaremos las siguientes propiedades básicas de este grupo:
Para cualquier grupo G, se denota por $\mathcal{D}(G)$ su subgrupo derivado.

(1) Si $f : G \to G'$ es un morfismo de grupos, entonces $f(\mathcal{D}(G)) \subseteq \mathcal{D}(G')$.

(2) $\mathcal{D}(G)$ es un subgrupo característico. En particular, es un subgrupo normal.

(3) El grupo cociente $G/\mathcal{D}(G)$ es abeliano, sea $\pi : G \to G/\mathcal{D}(G)$ la proyección canónica. Entonces, cualquier morfismo $\psi : G \to G'$ en un grupo abeliano G' se factoriza por π. Es decir existe un morfismo de grupos abelianos $\psi' : G/\mathcal{D}(G) \to G'$ tal que el diagrama



(4) Sea H un subgrupo de G. Son equivalente:

(4i) $\mathcal{D}(G) \subseteq H$;

(4ii) H es un subgrupo normal y G/H es abeliano.

(5) Si X es un subconjunto generador de G, entonces $\mathcal{D}(G)$ es el subgrupo normal generado por los conmutadores de los elementos de X.

Dadas A, B, dos parte de un grupo G, se define el conmutador de A y B como el conjunto

$$(A, B) := \{a^{-1}b^{-1}ab |\ a \in A,\ b \in B\}$$

De allí la siguiente definición. *La serie central decreciente de un grupo* G, es la sucesión de $\{\mathcal{C}^n(G)\}_{1 \leq n \in \mathbb{N}}$ definida por

$$\mathcal{C}^1(G) = G, \quad \mathcal{C}^{n+1} = (G, \mathcal{C}^n(G)), \text{ para } n \geq 2.$$

Se dice que un grupo G con elemento neutro e, es *nilpotente*, si existe un entero natural n tal que $\mathcal{C}^{n+1}(G) = \{e\}$. La *clase de nilpotencia* es el entero natural más pequeño n, tal que $\mathcal{C}^{n+1}(G) = \{e\}$.

TEOREMA. Sea G un grupo y n un número natural. Son equivalentes.

(i) G es nilpotente de clase $\leq n$;

(ii) Existe una sucesión de subgrupos

$$G = G^1 \supset \cdots\cdots \supset G^{n+1} = \{e\},$$

tal que $(G, G^k) \subseteq G^{k+1}$, para cualquier $k \in \{1, \cdots, n\}$.

(iii) Existe un subgrupo H de G contenido en el centro de G, tal que A es nilpotente de clase $\leq n-1$.

Como corolario, se tiene que: Una extensión central de un grupo nilpotente (por un grupo necesariamente abeliano), es nilpotente. Resumimos más propiedades de grupos nilpotentes:
Sea G un grupo nilpotente de clase $\leq n$ y H un subgrupo de G.

(a) Existe un sucesión de subgrupos

$$G = H^1 \supset H^2 \supset \cdots\cdots \supset H^{n+1} = H,$$

tal que H^{k+1} es normal en H^k y el cociente H^k/H^{k+1} es abeliano, para todo $k \leq n$.

(b) Si $H \subsetneq G$, entonces el normalizador $N_G(H)$ de H en G es estrictamente contenido en G.

(c) Si $H \subsetneq G$, entonces existe un subgrupo normal N de G, tales que $H \subseteq N \subsetneq G$ y G/N abeliano.

(d) Si $G = H(G, G)$, entonces $G = H$.

(e) Si $f : G' \to G$ es un morfismo de grupos y $f' : G'/(G', G') \to G/(G, G)$ deducido de f pasando al cociente es suprayectivo, entonces f es mismo suprayectivo.

Continuamos con las propiedades de un grupo nilpotente. Sea G un grupo nilpotente de clase $\leq n$ cuyo centro es Z y sea N un subgrupo normal de G. Entonces

(f) Existe una sucesión de subgrupos

$$N = N^1 \supset N^2 \supset \cdots\cdots \supset N^{n+1} = N,$$

tal que $(G, N^k) \subset N^{k+1}$, para todo $k \leq n$.

(g) Si $N \neq \{e\}$, entonces $N \cap Z \neq \{e\}$.

(h) Si $f : G \to G'$ es un morfismo de grupos cuya restricción a Z es inyectiva, también lo es f.

Sea G un grupo, *la serie derivada* de G es la sucesión de subgrupos de G, $\{\mathcal{D}^n(G)\}_{n\in\mathbb{N}}$ definida de forma recurrente:

$$\mathcal{D}(G) = G; \qquad \mathcal{D}^{n+1}(G) = \mathcal{D}(\mathcal{D}^n(G)), \text{ para todo } n \geq 1.$$

G se dice que es *un grupo resoluble* si existe algún n, tal que $\mathcal{D}^n(G) = \{e\}$. Si G es un grupo resoluble, llamaremos *la clase de* G, al más pequeño natural n tal que $\mathcal{D}^n(G) = \{e\}$.

TEOREMA. Sea G un grupo y n un número natural. Son equivalentes.

(i) G es resoluble de clase $\leq n$;

(ii) Existe una sucesión de subgrupos normales

$$G = G^0 \supset G^1 \supset \cdots\cdots \supset G^n = \{e\},$$

tal que los cocientes G^k/G^{k+1} son abelianos.

(iii) Existe una sucesión de subgrupos

$$G = G^0 \supset G^1 \supset \cdots\cdots \supset G^n = \{e\},$$

tal que, para todo $k \leq n$, G^{k+1} es un subgrupo normal de G^k, y el cociente G^k/G^{k+1} es abeliano.

(iii) Existe un subgrupo conmutativo H de G contenido en el centro de G, tal que A es nilpotente de clase $\leq n-1$.

TEOREMA. Sea G un grupo finito y

$$G = G^0 \supset G^1 \supset \cdots\cdots \supset G^n = \{e\},$$

es una serie de Jordan-Hölder de G. Para que G sea resoluble es necesario y suficiente que cada cociente G^k/G^{k+1} sea cíclico de orden un número primo.

LECCIÓN 28 p-GRUPOS Y SUBGRUPOS DE SYLOW.

En esta lección estudiaremos los subgrupos de un grupo con orden potencia de un número primo positivo. Después de dar las propiedades básica de estos así como algunos ejemplos, pasaremos a introducir los subgrupos de Sylow, luego enunciar el teorema de Sylow. Finalizamos la lección con un resultado que caracteriza los grupos nilpotentes mediante los subgrupos de Sylow.

Denotaremos por p un número primo natural. Sea G un grupo, se dice que G es *un* p*-grupo* si G es finito de orden una potencia de p, es decir de forma p^k. A modo de ejemplo cualquier p-grupo conmutativo es isomorfo a un producto de los grupos cíclico $\mathbb{Z}/p^n\mathbb{Z}$. El grupo de los cuaternion $\{\pm 1, \pm i, \pm j, \pm k\}$ es un 2-grupo. Los siguientes son las primeras propiedades sobre los p-grupos:

Consideramos G un p-grupo con elemento neutro e.

(i) Sea E un G-conjunto finito (por la derecha) con $E^G = \{u \in E | u^x = u, \forall x \in G\}$ el conjunto de los elementos fijos. Entonces

$$|E^G| \equiv |E| \, [p],$$

el cardinal de E^G es congruente al cardinal de E módulo p.

(ii) Sea p^r el orden de G. Entonces existe una sucesión de subgrupos de G,

$$G = G^1 \supset G^2 \supset \cdots\cdots \supset G^{r+1} = \{e\},$$

tales que $(G, G^k) \supset G^{k+1}$ y G^k/G^{k+1} es cíclico de orden p, para todo $1 \leq k \leq r$. En particular, cualquier p-grupo es nilpotente.

(iii) Si $G \neq \{e\}$, entonces su centro $Z(G) \neq \{e\}$.

(iv) Sea H un subgrupo de G distinto de G. Entonces

(1-iv) El normalizador $N_G(H)$ de H en G, es distinto de G.

(2-iv) Existe un subgrupo normal N de G, de índice p en G y que contiene a H.

En particular, cualquier subgrupo de índice p es un subgrupo normal.

Sea G un grupo finito. Se le llama *un* p*-subgrupo de Sylow* a todo subgrupo P de G que satisface:
(a) P es un p-grupo;
(b) $(G : P)$ no es un múltiple de p.

Cualquier cíclo τ de orden p, engendra un subgrupo de Sylow de $\mathcal{S}_p$. Sea $\mathbb{F}$ un cuerpo finito de característica p, y n un entero positivo. Entonces el subgrupo de $(n \times n)$-matrices triangulares superiores con 1 en la diagonal es un p-subgrupo de Sylow del grupo lineal $GL_n(\mathbb{F})$. Resumimos las propiedades de los p-grupos de Sylow.

TEOREMA. Sea G, G' dos grupos finitos.

(a) G contiene un p-subgrupo de Sylow.

(b) Si el orden de G es divisible por p, entonces G tiene un elemento de orden p.

(c) Los p-subgrupos de Sylow son conjugados dos por dos. Su número es congruente a 1 módulo p.

(d) Cualquier subgrupo de G que es un p-grupo, esta contenido en un p-subgrupo de Sylow.

(e) Sea P un psubgrupo de Sylow de G y $M \leq G$ un subgrupo que contiene $N_G(P)$ el normalizador de P en G. Entonces $N_G(M) = M$.

(f) Sea $f : G \to G'$ un morfismo de grupos. Para cualquier p-subgrupo de Sylow P de G, existe un p-subgrupo P' de G' tal que $f(P) \supset P'$.

TEOREMA. Sean G un grupo, H un subgrupo y N un subgrupo normal ambos de G.

(a) Para cualquier p-subgrupo de Sylow P de H, existe un p-subgrupo de Sylow Q de G tal que $P = Q \cap H$.

(b) Si Q es un p-subgrupo de Sylow de G, entonces $Q \cap N$ es p-subgrupo de Sylow de N.

(c) La imagen de un p-subgrupo de Sylow en G/N es un p-subgrupos de Sylow. Además cualquier p-subgrupo de Sylow de G/N se obtiene de esta forma

El siguiente es una caracterización de grupos nilpotente finitos:

TEOREMA. Sea G un grupo finito. Las siguientes condiciones son equivalentes.

(i) G es nilpotente;

(ii) G es producto de p-grupos;

(iii) Para cualquier número primo positivo, existe un p-subgrupo de Sylow de G normal.

El grupo simétrico $\mathcal{S}_3$ es de orden 6 y tiene un 3-subgrupo de Sylow normal de orden 3, de hecho es $\mathcal{A}_3$. También, tiene tres 2-subgrupos de Sylow de orden 2, los subgrupos $\{e, \tau\}$, donde τ es una transposición. De allí, $\mathcal{S}_3$ no es nilpotente.

LECCIÓN 29 GRUPOS FINITOS.

Esta lección aborda los resultado básicos sobre los grupos finito. Entre otros, presentaremos al alumno los Teoremas de Frobenius sobre estos grupos.

Empezaremos la lección pues llamando la atención del alumno sobre el número finito de grupos (salvo isomorfía) de un orden pre-asignado n. Así dado un grupo G de orden n cuyos elementos son $\{g_1, g_2, \cdots, g_n\}$. Elegimos un elemento cualquiera g_i, se tiene n-distintos elementos de G,

$$g_1g_i,\ g_2g_i,\ \cdots\ g_ng_i.$$

De allí la permutación

$$\sigma_i = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1g_i & g_2g_i & \cdots & g_ng_i \end{pmatrix}$$

Es decir a cada elemento de G le corresponde un tipo de permutación de n símbolos.

> TEOREMA (Cayley). Cualquier grupo de orden n es isomorfo a un subgrupo de permutaciones de n símbolos.

Por lo tanto el número de grupo (salvo isomorfía) de orden n, no excede a $\binom{n!}{n}$. Otro resultado en este sentido es

> TEOREMA (Landau). Sea k un entero natural. Hay un número finito (salvo isomorfía) de grupos finito que posean exactamente k clases de equivalencia módulo conjugación.

Hay otra relación de equivalencia en un G que es tan importante en grupos finitos como la conjugación. Sean U, V dos subgrupos de un grupo G. Consideramos la siguiente relación

$$\ll x \text{ esta relacionado con } y \gg \iff x = uyv, \text{ para algunos } u \in U,\ v \in V.$$

Por definición esta es una relación de equivalencia y las clases de equivalencias son de forma UxV, para un cierto $x \in G$.

TEOREMA (Frobenius). Sea G un grupo finito de orden n y U, V dos subgrupos de G de orden a, b, respectivamente. Entonces, existen elementos $g_1, \cdots, g_r$ de G tal que G es unión disjunta de clases de equivalencia:

$$G = \bigcup_{i=1}^{r} Ug_iV.$$

El número de elemento en Ug_iV es ab/d_i, donde

$$d_i = |(g_i^{-1}Ug_i) \cap V|, \quad i = 1, \cdots, r.$$

En consecuente,

$$n = ab\left(\sum_{i=1}^{r} d_i\right).$$

Finalizaremos esta lección con otro resultado de Frobenius

TEOREMA (Frobenius). Sea G un grupo finito de orden n.

(i) Si el orden de G es de forma $n = ab$ con $mcd(a, b) = 1$ y H es un subgrupo invariante (por la conjugación) de G de orden a. Entonces cualquier elemento de G con orden un divisor de a, es un elemento de H.

(ii) Si H es un subgrupo de G de orden a con $n = ab$, si $b \leq p$ donde p es el número primo más pequeño de a. Entonces H es invariante.

LECCIÓN 30 LOS GRUPOS DE ORDEN 8.

En esta lección le vamos a mostrarle al alumno como encontrar todos los grupos (salvo isomorfía) de orden 8.

Empezaremos pues con la siguiente observación. Hasta el momento, ningún método de éxito se ha descubierto para la construcción de todos los posibles grupos abstractos (salvo isomorfía) de un orden preasignado, ni sabemos de antemano cuantos exactamente puedan haber de estos grupos, salvo en casos sencillos. Sin embargo, los medios elementales que hemos desarrollado hasta ahora, son suficientes para dar una lista completa de grupos de hasta orden por ejemplo 8. El método sirve para discutir con más detalle los casos en que el orden, n es igual a 4 o 6 o 8.

HAY DOS GRUPOS DE ORDEN 4, AMBOS SON ABELIANOS. Para ello si G es un grupo con $|G| = 4$, un elemento que no sea e (el elemento neutro), puede tener como orden 4 o 2

(4-I) Si G contiene un elemento g de orden 4, este elemento genera a G, así

$$G = \mathcal{C}_4 = \langle g \rangle$$

el grupo cíclico de orden 4.

(4-II) Supongamos que G no tiene elementos de orden 4. Entonces cualquier elemento que no sea e, es de orden 2. De allí

$$G = \mathcal{C}_2 \times \mathcal{C}_2,$$

el producto de copias de $\mathcal{C}_2$ el grupo cíclico de orden 2. Por lo tanto G esta generado por dos elementos g, h sujetos a las relaciones

$$g^2 = h^2 = e, \quad gh = hg.$$

Este es el *grupo de Klein 'Vierergruppe'*.

HAY DOS GRUPOS DE ORDEN 6, UNO ES CÍCLICO Y EL OTRO NO ES ABELIANO. Para ello si G es un grupo con $|G| = 6$, un elemento que no sea e (el neutro), puede tener como orden 6 o no

(6-I) Si G contiene un elemento g de orden 6, este elemento genera a G, así

$$G = \mathcal{C}_6 = \langle g \rangle$$

el grupo cíclico de orden 6.

(6-II) Supongamos que G no tiene elementos de orden 6. Entonces cualquier elemento que no sea e, es de orden 2 o 3. Ahora no todos los elemento de G son de orden 2, porque si fuese así $|G|$ sería potencia de 2. Sin embargo no es el caso. De allí, existe un elemento de orden 3, llamaremos lo g. Se tiene pues tres elemento $\{e, g, g^2\}$, faltan pues otros tres. Luego, si h es otro elemento distinto de esos, tendríamos seis elementos

$$\left\{e, g, g^2, h, hg, hg^2\right\}.$$

Esto conlleva a tres casos:

$$(1)\ h^2 = e, \quad (2)\ h^2, = g, \quad (3)\ h^2 = g^2.$$

Los casos $(2), (3)$, llevan a las ecuaciones $e = hg$ y $e = hg^2$ lo que no puede ser. Por lo tanto, quedaría el caso (1), es decir que $h^2 = e$. Al final no encontraremos con que G es el grupo generado por $\{g, h\}$ sujetos a la relación

$$g^3 = h^2 = (gh)^2 = e.$$

Esto no quiere decir que tal grupo existe. Sin embargo, la tabla VI.1 detalla su tabla de multiplicación

HAY CINCO GRUPOS DE ORDEN 8, TRES DE ELLOS SON ABELIANOS Y DOS NO LO SON. Los tres grupos abelianos de orden 8, son

	e	g	g^2	h	hg	hg^2
e	e	g	g^2	h	hg	hg^2
g	g	g^2	e	hg^2	h	hg
g^2	g^2	e	g	hg	hg^2	h
h	h	hg	hg^2	e	g	g^2
hg	hg	hg^2	h	g^2	e	g
hg^2	hg^2	h	hg	g	g^2	e

Cuadro VI.1: G de orden 6 generado por a, b con $g^3 = h^2 = (gh)^2 = e$.

	e	g	g^2	g^3	h	hg	hg^2	hg^3
e	e	g	g^2	g^3	h	hg	hg^2	hg^3
g	g	g^2	g^3	e	hg	hg^2	hg^3	h
g^2	g^2	g^3	e	g	hg^2	hg^3	h	hg
g^3	g^3	e	g	g^2	hg^3	h	hg	hg^2
h	h	hg	hg^2	hg^3	e	g	g^2	g^3
hg	hg	hg^2	hg^3	h	g	g^2	g^3	e
hg^2	hg^2	hg^3	h	hg	g^2	g^3	e	g
hg^3	hg^3	h	hg	hg^2	g^3	e	g	g^2

Cuadro VI.2: $\mathcal{C}_4 \times \mathcal{C}_2 = \langle g \rangle \times \langle h \rangle$, donde $g^4 = h^2 = e$.

(8-I) $\mathcal{C}_8 = \langle g \rangle$, donde $g^8 = e$.

(8-II) $\mathcal{C}_4 \times \mathcal{C}_2 = \langle g \rangle \times \langle h \rangle$, donde $g^4 = h^2 = e$, $hg = gh$. Véase la tabla VI.2.

(8-III) $\mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2 = \langle g \rangle \times \langle h \rangle \times \langle f \rangle$, donde $g^2 = h^2 = f^2 = e$, g, h, f conmutan dos por dos. Véase la tabla VI.3.

El primer y el tercer casos corresponden a la situación de que G tiene un elemento g distinto de e de orden 8, ó que todos los elementos distintos de e son de orden 2. Quedarían pues los caso donde G tiene un elemento distinto de e que es o bien de orden 2 o bien de orden 4, y que hay al menos uno de orden

	e	g	h	f	hg	fg	fh	fhg
e	e	g	h	f	hg	fg	fh	fhg
g	g	e	hg	fg	h	f	fhg	fh
h	h	hg	e	fh	g	fhg	f	fg
f	f	fg	fh	e	fhg	g	h	hg
hg	hg	h	g	fhg	e	fh	fg	f
fg	fg	f	fhg	g	fh	e	hg	h
fh	fh	fhg	f	h	fg	hg	e	g
fhg	fhg	fh	fg	hg	f	h	g	e

Cuadro VI.3: $\mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2 = \langle g \rangle \times \langle h \rangle \times \langle f \rangle$, donde $g^2 = h^2 = f^2 = e$.

4, sea pues es elemento g, donde $g^4 = e$, $g^2 \neq e$. Si h es un elemento que no pertenece a $\langle g \rangle$, entonces los ocho elementos

$$\left\{e, g, g^2, g^3, h, hg, hg^2, hg^3\right\}.$$

son distintos y forman en total un grupo (si ese existe). Ahora h^2 debe de ser uno de ellos, de hecho uno de los cuatro primeros, dado que h no es potencia de g. Las ecuaciones $h^2 = g$ o $h^2 = g^3$, implicarían que h es de orden 8 y eso no es el caso que estamos tratando. Quedan pues dos posibilidades:

$$(1)\ h^2 = e, \quad (2)\ h^2, = g^2.$$

(8-11) Si $h^2 = e$, entonces $gh \in \{hg, hg^2, hg^3\}$. Así si $hg = gh$, esto conlleva el grupo descrito en el caso $(8 - II)$.

(8-12) Si $h^2 = e$ y $gh = hg^2$, esto implica que $g^2 = e$ lo que descarta este caso.

(8-13) Si $h^2 = e$ y $gh = hg^3$, o equivalentemente $(hg)^2 = e$. Sería pues el grupo generado por $\{g, h\}$ sujeto a la relación:

$$g^4 = h^2 = (hg)^2 = e.$$

Tal grupo existe, es el grupo diedro $\mathcal{D}_8$ (o en algunos texto $\mathcal{D}_4$) de orden 8, véase la tabla VI.4

	e	g	g^2	g^3	h	hg	hg^2	hg^3
e	e	g	g^2	g^3	h	hg	hg^2	hg^3
g	g	g^2	g^3	e	hg	hg^2	hg^3	h
g^2	g^2	g^3	e	g	hg^2	hg^3	h	hg
g^3	g^3	e	g	g^2	hg^3	h	hg	hg^2
h	h	hg^3	hg^2	hg	e	g^3	g^2	g
hg	hg	h	hg^3	hg^2	g	e	g^3	g^2
hg^2	hg^2	hg	h	hg^3	g^2	g	e	g^3
hg^3	hg^3	hg^2	hg	h	g^3	g^2	g	e

Cuadro VI.4: $\mathcal{D}_8$ el grupo diedro de orden 8, donde $g^4 = h^2 = = (hg)^2 = e$.

Nos falta pues el caso (2), es decir $h^2 = g^2$. En este caso ambos h, g tiene orden 4. Aquí, también gh tiene que ser uno de los elementos $\{hg, hg^2, hg^3\}$.

(8-21) Si $h^2 = g^2$ y $hg = gh$, esto conlleva también al grupo descrito en el caso $(8 - II)$.

(8-22) Si $h^2 = g^2$ y $gh = hg^2$, esto implica que $h^2 = g$ inadmisible.

(8-23) Si $h^2 = g^2$ y $gh = hg^3$. Sería pues el grupo generado por $\{g, h\}$ sujeto a la relación:

$$g^4 = e, \quad h^2 = g^2, \quad gh = hg^3. \tag{VI.1}$$

Tal grupo existe. En efecto, sea

$$a = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Estos elemento satisfacen, de manera adecuada, las relaciones de la ecuación (VI.1). Constituyen pues un grupo multiplicativo, de matrices que es isomorfo al grupo bajo consideración. Este grupo es conocido por el nombre de *el grupo de los cuaternion* $\mathcal{Q}_2$, véase la tabla VI.5 por su tabla de

	e	g	g^2	g^3	h	hg	hg^2	hg^3
e	e	g	g^2	g^3	h	hg	hg^2	hg^3
g	g	g^2	g^3	e	hg	hg^2	hg^3	h
g^2	g^2	g^3	e	g	hg^2	hg^3	h	hg
g^3	g^3	e	g	g^2	hg^3	h	hg	hg^2
h	h	hg^3	hg^2	hg	g^2	g	e	g^3
hg	hg	h	hg^3	hg^2	g^3	g^2	g	e
hg^2	hg^2	hg	h	hg^3	e	g^3	g^2	g
hg^3	hg^3	hg^2	hg	h	g	e	g^3	g^2

Cuadro VI.5: El grupo de cuaternion $\mathcal{Q}_2$, donde $g^4 = e$, $h^2 = g^2$, $gh = hg^3$..

multiplicación. El nombre viene del hecho de que el los cuaternion de Hamilton, es decir el $\mathbb{R}$-espacio vectorial generado por $\{1, i, j, k\}$ (dotado de una ley de composición) tales que

$$i^2 = j^2 = -1, \quad ij = -ji = k,$$

o equivalentemente

$$i^4 = 1, \quad i^2 = j^2, \quad ij = ji^3,$$

satisfacen pues las mismas relaciones que en la ecuación (VI.1)

BIBLIOGRAFÍA

[1] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[2] W. Burnside. *The Theory of Groups of finite order*. Cambridge University Press. Cambridge, 1897.

[3] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, 1985.

[4] W. Ledermann. *Introduction to Group Theory*. Longman Group. London, 1973.

[5] Harold Hilton M.A. *Introduction of Theory of Groups of Finite Order*. Oxford At The Clarendon Press, 1908.

[6] O. U. Schmidt. *Abstract Theory of Groups*. A Serie of Books in Mathematics. W. H. Freeman and Company. San Francisco London, 1966.

BIBLIOGRAFÍA

[1] J. A. Anderson. *Discrete Mathematics With Combinatorics*. Prentice-Hall, 2001.

[2] M. Anzola and J. Garuncho. *Problemas de álgebra (Tomo 2)*. Ed. Bumar. Madrid, 1976.

[3] M. Artin. *Algebra*. Prentice Hall inc. 1991.

[4] R. Balakrishnan and K. Ranganathan. *A Textbook of Graph Theory*. Springer, 2000.

[5] N. L. Biggs. *Matemática Discreta*. Ed. Vicens vives, 1994.

[6] N. Bourbaki. *Elements of Mathematics. Commutative Algebra. Chapitres 5 á 7.* Hermann, 1972.

[7] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[8] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 4-7.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[9] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 1 á 4.* Springer-Verlag, Berlin Heidelberg, 2006.

[10] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 5 á 7.* Springer-Verlag, Berlin Heidelberg, 2007.

[11] W. Burnside. *The Theory of Groups of finite order*. Cambridge University Press. Cambridge, 1897.

[12] A. Clark. *Elementos de Álgebra abstracta*. Alhambra, 1970.

[13] D. S. Dummit, R. M. Foote. *Abstract Algebra*. John Wiley, 1999.

[14] N. Deo. *Graph theory with applications to Engeneering and Computer Science*. Prentice–Hall, 1974.

[15] D. E. Ensley and J. W. Crawley. *Discret Matematics. Mathematical Reasoning and Proof with Puzzles, Patterns, and Games*. Willy, 2006.

[16] G. Hernández Peñalver y A. Nevot Luna F. García Merayo. *Problemas Resueltos de Matemática Discreta*. Thomson, 2003.

[17] J. B. Fraleigh. *Álgebra Abstracta*. Addison Wesley, Iberoamericana, 1987.

[18] J. B. Fraleigh. *A First Course in Abstract Algebra*. Addison Wesley, 1999.

[19] R. Garnier and J. Taylor. *Discret Matematics for New Techonology*. IOP, second edition, 2002.

[20] R. P. Grimaldi. *Matemática Discreta y Combinatoría*
Una introducción con aplicaciones. Addison Wesley Longman, 1998.

[21] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, 1985.

[22] R. Johnsonbaugh. *Matemáticas Discretas*. Prentice-Hall, 1997.

[23] K. D. Joshi. *Foundation of Discrete Mathematics*. John Wiley and sons, 1989.

[24] M. Hall Jr. *The Theory of Groups*. The Macmillan Co., New York, 1959.

[25] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[26] W. Ledermann. *Introduction to Group Theory*. Longman Group. London, 1973.

[27] S. Lipschutz. *Matemática Discreta, Tería y 600 Problemas Resueltos*. Serie Schaum. McGraw-Hill, 1990.

[28] J. Leach y M. Rodríguez M. T. Hortalá. *Matemática Discreta y Lógica Matematica*. Editorial Complutense, 1998.

[29] Harold Hilton M.A. *Introduction of Theory of Groups of Finite Order*. Oxford At The Clarendon Press, 1908.

[30] J. Matoušek and J. Nešetřil. *Invitation to Discrete Mathematics*. Clarendon Press. Oxford, 2004.

[31] F. García Merayo. *Matemática Discreta*. Thomson, 2005.

[32] K. H. Rosen. *Matemática discreta y sus aplicaciones*. McGraw-Hill, 2004.

[33] J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Text in Mathematics*. Springer-Verlag, New York, 1995.

[34] O. U. Schmidt. *Abstract Theory of Groups*. A Serie of Books in Mathematics. W. H. Freeman and Company. San Francisco London, 1966.

[35] L. E. Sigler. *Álgebra*. Ed. Reveté, 1981.

[36] K. A. Roos y C. R. Wright. *Discrete Mathematics*. Prentice-Hall, 1988.

Curso 2º

Álgebra III

SUMARIO

Objetivos y comentarios del curso

La asignatura de *Álgebra III* contiene, como ya hemos dicho anteriormente en la introducción, una de las importantes teorías de la matemática fundamental: la teoría de Galois de ecuaciones algebraicas. Uno de los objetivos de esta teoría es el problema de resolución de una ecuación polinómica general 'por radical". Podemos decir entonces que el objetivo final de este curso es llegar al teorema de Abel-Ruffini que da un marco satisfactorio para la plena comprensión de este problema y la realización de que la ecuación general polinomio de grado mayor que 5 no siempre podrán ser resueltas por radical. En este curso nos centraremos en marcar los siguientes objetivos:

- La solución de ecuaciones polinómicas sobre un cuerpo, incluyendo las relaciones entre las raíces, métodos de soluciones y la ubicación de las raíces.
- La estructura de las extensiones finitas y algebraica de cuerpos y sus automorfismos.
- Estudiaremos en detalle, la construcción de una teoría de las extensiones algebraicas de cuerpos y sus grupos de automorfismos y su aplicación para resolver cuestiones acerca de las raíces de ecuaciones polinómicas.
- Enseñare al alumno técnicas clásicas como la cuadratura del círculo, la duplicación del cubo, los números construibles y polígonos construibles.
- Esperemos que las técnicas aprendidas en este curso sirvan de utilidad en otros cursos avanzados: Aplicaciones de las ideas de la teoría de Galois en Teoría de Números, el estudio de ecuaciones diferenciales y geometría algebraica.

Tema I

Anillos, cuerpos y anillos de polinomios.

Lecciones

El principal objetivo de este tema, es de familiarizar el alumno con los anillos de polinomios con una sola (o varias) indeterminada sobre cuerpos: el algoritmo de división, teorema de Bezout, anillos de polinomios cocientes, etc. Abordaremos con especial interés, las nociones de factorización y la irreducibilidad, presentando para ello el lema de Gauss y los criterios de Eisenstein. A modo de ejemplo le presentaremos al alumno los polinomios ciclotómicos. Hablaremos también sobre la busqueda de la raíces de polinomios de grados inferior a 4, enunciando los métodos de Cardan y Ferrari. Finalizaremos la lección con una introducción sobre los grupos de automorfismos de cuerpos; al mismo tiempos daremos ejemplos conocidos de esos grupos.

Cabe mencionar que este tema representa las técnicas y las nociones básicas que han de ser manejadas con destreza por parte del alumno, para poder acceder con comodidad al resto de los temas de este curso. Centraremos pues nuestro esfuerzo sobre el aprendizaje por parte del alumno, de las técnicas de busqueda de raíces, irreducibilidad y cálculo con polinomios y fracciones racionales.

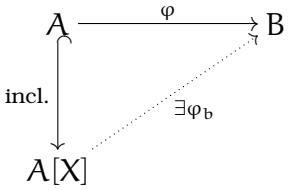
LECCIÓN 1 ANILLOS DE POLINOMIOS: FACTORIZACIÓN Y IRREDUCIBILIDAD

Empezaremos esta lección explicando lo que es un anillo de polinomios con una *sola indeterminada* sobre un anillo conmutativo cualquiera, dando las reglas de la suma y la multiplicación en este nuevo anillos en relación con las operaciones del anillo base. Definimos lo que es un *coeficiente líder* así como el *grado de un polinomio*. Pasaremos luego al caso de varias indeterminadas, usando para ello un breve recordatorio del Tema IV del curso **Álgebra II**.

Después de las definiciones básicas, conviene dar las siguientes propiedades de anillos de polinomios. Sea $\varphi : A \to B$ un morfismo de anillo (conmutativos).

(1) Para cualquier $b \in B$, existe un único morfismo de anillos $\varphi_b : A[X] \to B$ para el cual

- $\varphi_b(a) = \varphi(a)$, para todo $a \in A$,
- $\varphi_b(X) = b$.

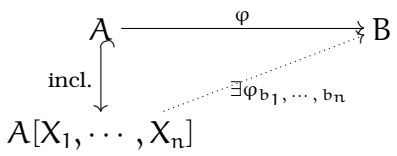


(2) Para cualquier $n \geq 1$, y $b_1, \cdots, b_n$, existe un único morfismo

$$\varphi_{b_1,\cdots,b_n} : A[X_1, \cdots, X_n] \longrightarrow b$$

para el cual

- $\varphi_{b_1,\cdots,b_n}(a) = \varphi(a)$, para todo $a \in A$,
- $\varphi_{b_i}(X_i) = b_i$, para todo $i = 1, \cdots, n$.



Presentaremos el siguiente ejemplo que vamos a usar repetidamente en es curso. Sea $\mathrm{incl}.\mathbb{Q} \to \mathbb{C}$ la inclusión de los números racional en los complejos. Se tiene pues la evaluación ε_i de i en $\mathbb{C}$ ($i^2 = -1$) dada por $\varepsilon_i(X) = i$. Luego $\varepsilon_i(\mathbb{Q}[X]) \subseteq \mathbb{C}$ es el subanillo $\mathbb{Q}[i]$ de $\mathbb{C}$ que consiste en los números complejos $a + ib$ con $a, b \in \mathbb{Q}$. Si usaremos $-i$ en vez de i, tenemos la siguiente relación entre ε_i y ε_{-i}

$$\varepsilon_i = \overline{(-)} \circ \varepsilon_i,$$

donde $\overline{(-)} : \mathbb{C} \to \mathbb{C}$ es la aplicación dada por la conjugación. De esta forma, se tiene que

$$\mathrm{Ker}(\varepsilon_i) = \mathrm{Ker}(\varepsilon_{-i}) = X^2 + 1 \lhd \mathbb{Q}[X]$$

Lo que implica que

$$\mathbb{Q}[i] \cong \mathbb{Q}[X]/\left\langle X^2 + 1 \right\rangle.$$

$\left\langle X^2 + 1 \right\rangle$ es de hecho un ideal máximal de $\mathbb{Q}[X]$, lo que nos dice que $\mathbb{Q}[i]$ es un subcuerpo de $\mathbb{C}$.

Terminaremos esta parte de la lección indicando al alumno que el anillo de polinomios a varias indeterminadas sobre un dominio de integridad vuelve a ser un dominio de integridad.

Pasaremos ahora a especializar las nociones anteriores al caso de polinomios sobre un cuerpo. Primero comprobaremos los siguientes resultados importantes

TEOREMA (Algoritmo de división). Sea $\Bbbk$ un cuerpo, y $p(X), q(X) \in \Bbbk[X]$ con $q(X) \neq 0$. Entonces existen únicos polinomios $r(X)$ y $c(X)$ en $\Bbbk[X]$ tales que

$$p(X) = c(X)q(X) + r(X), \quad r(X) = 0 \text{ o } grad(r(X)) < grad(q(X)).$$

$r(X)$ se le llama el *resto*, $c(X)$ el *cociente* y $q(X)$ el *dividiendo*.

TEOREMA (Algoritmo de Euclid). Sea $\Bbbk$ un cuerpo y X una indeterminada. Sean $f(X), g(X) \text{in} \Bbbk[X]$ dos polinomios no nulos. Entonces existen únicos polinomios $a(X)$ y $b(X)$ en $\Bbbk[X]$ tale que

$$f(X)a(X) + g(X)b(X) = mcd(f(X), g(X)),$$

donde $mcd(f(X), g(X))$ es el máximo común divisor de $f(X)$ y $g(X)$, es decir el polinomio monoico de grado superior entre los grados de todos los divisores de $f(X)$ y $g(X)$.

Como ya hemos explicado al alumno antes, dado que $\Bbbk[X]$ es un dominio de integridad, entonces podemos hablar de elementos primos y elementos irreducibles. Resumimos todas estas propiedades entre otras , en el siguiente resultado: Sea $\Bbbk$ un cuerpo y X una indeterminada.

(i) Un polinomio no constante $p(X) \in \Bbbk[X]$ es irreducible si, y sólo si es primo.

(ii) Cualquier ideal $I \lhd \Bbbk[X]$ es principal. Es decir que $\Bbbk[X]$ es un dominio principal. Además cualquier ideal tiene como generador un único polinomio monoico.

(iii) El ideal $\langle p(X) \rangle \lhd \Bbbk[X]$ es primo si, y sólo si $p(X) = 0$ ó $p(X)$ es irreducible en $\Bbbk[X]$.

(iv) El anillo cociente $\Bbbk[X]/\langle p(X) \rangle$ es un dominio de integridad si y sólo si $p(X) = 0$ ó $p(X)$ es irreducible en $\Bbbk[X]$.

(v) El anillo cociente $\Bbbk[X]/\langle p(X)\rangle$ es un cuerpo si y sólo si $p(X)$ es irreducible en $\Bbbk[X]$.

Pasaremos luego a hablar sobre la factorización de polinomios. Pero antes le daremos al alumno la definición de lo que es *una raíz de un polinomio*, señalando el hecho de que a es raíz de $p(X)$ si y sólo si $(X-a)|p(X)$ (divide).

TEOREMA. Sea $\Bbbk$ un cuerpo y X una indeterminada.

(i) Cualquier polinomio no constante, $f(X) \in \Bbbk[X]$ tiene una factorización

$$f(X) = c\,p_1(X)\cdots p_k(X),$$

donde $c \in \Bbbk$, y $p_1(X),\cdots,p_k(X) \in \Bbbk[X]$ son polinomios monoicos irreducibles. Además, c es único, y la sucesión $p_1(X),\cdots,p_k(X)$ es única salvo el orden de sus términos.

(ii) Supongamos que $f(X) \in \Bbbk[X]$ admite una factorización en factor lineales:

$$f(X) = c\,(X-\mu_1)\cdots(X-\mu_l),$$

donde $\mu_1,\cdots,\mu_l \in \Bbbk$. Entonces, la sucesión de raíces $\mu_1,\cdots,\mu_l$ es única salvo el orden de sus términos. In particular, si $\nu_1,\cdots,\nu_k \in \Bbbk$ son distintas raíces de $f(X)$, entonces

$$f(X) = c\,(X-\nu_1)^{m_1}\cdots(X-\nu_k)^{m_k},$$

donde $m_i > 0$ y esta factorización es única salvo el orden de las parejas (ν_i, m_i).

En particular, señalaremos que el número de las raíces distintas de un polinomio no constante $f(X) \in \Bbbk[X]$ no excede al grado de $f(X)$, $\mathrm{grad}(f(X))$.

LECCIÓN 2 IDENTIFICANDO POLINOMIOS IRREDUCIBLES

En esta lección mostraremos al alumno métodos efectivos para poder decidir si un polinomio es irreducible o no. Primero presentaremos criterios para polinomios con coeficientes en $\mathbb{Z}$, luego con coeficientes en un dominio de integridad de forma $D = \Bbbk[t]$ donde $\Bbbk$ es un cuerpo cualquiera. De paso abordaremos los polinomios ciclotómicos.

Empezaremos primero por el caso de $\mathbb{Z}$ y $\mathbb{Q}$. Si $f(X)$ es un polinomio en $\mathbb{Z}[X]$, se puede ver como elemento de $\mathbb{Q}[X]$. Sea A uno de los anillos $A = \mathbb{Z}$ o $A = \mathbb{Q}$, se dice que $f(X)$ tiene una *factorización propia sobre* A, si $f(X) = g(X)h(X)$ para algún $g(X), h(X)$ en $A[X]$ con $grad(g(X)) > 0$, $grad(h(X)) > 0$. Enunciaremos con demostración el Lema de Gauss: Sea $f(X) \in \mathbb{Z}$. Entonces $f(X)$ tiene una factorización propia sobre $\mathbb{Z}$ si y sólo si la tiene sobre $\mathbb{Q}$. Luego el siguiente criterio

TEOREMA (El Test de Eisenstein en $\mathbb{Z}[X]$). Sea $f(X) \in \mathbb{Z}[X]$ y $s \in \mathbb{Z}$. Sean $a_i \in \mathbb{Z}$, tal que

$$f(X) = a_0 + a_1(X-s) + \cdots + a_{d-1}(X-s)^{d-1} + a_d(X-s)^d,$$

donde $d = grad(f(X))$. Supongamos dado $p > 0$ primo para el cual se tiene las siguientes condiciones:

- p divide a a_k, para todo $k = 0, 1, \cdots, , d-1$.
- p^2 no divide a a_0.
- p no divide a a_d.

Entonces $f(X)$ es irreducible en $\mathbb{Q}[X]$, y luego irreducible en $\mathbb{Z}[X]$.

Como aplicación del criterio anterior, presentaremos al alumno el siguiente ejemplo.

POLINOMIOS CICLOTÓMICOS. Sea $p \geq 2$ un primo. Entonces el polinomio

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1} \in \mathbb{Z}[X]$$

es irreducible en $\mathbb{Q}[X]$ y luego lo es en $\mathbb{Z}[X]$ (usar el Criterio de Eisenstein para $s = 1$). Estos son ejemplos de *polinomios ciclotómicos* $\Phi_n(X) \in \mathbb{Z}[X]$ que se definen, para $n \geq 1$, por

$$\prod_{d \in D(n)} \Phi_d(X) = X^n - 1,$$

donde $D(n)$ es el conjunto de los divisores positivos de n. Por ejemplo,

$$\begin{aligned}
X^2 - 1 &= (X-1)(X+1) = \Phi_1(X)\Phi_2(X),\\
X^3 - 1 &= (X-1)(X^2+X+1) = \Phi_1(X)\Phi_3(X),\\
X^4 - 1 &= (X-1)(X+1)(X^2+1) = \Phi_1(X)\Phi_2(X)\Phi_4(X),\\
X^5 - 1 &= (X-1)(X^4+X^3+X+1) = \Phi_1(X)\Phi_5(X),\\
X^{12} - 1 &= (X-1)(X+1)(X^2+X+1)(X^2+1)(X^2-X+1(X^4-X^2+1)\\
&= \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X).
\end{aligned}$$

Los polinomios ciclotómicos, se pueden calcularse de una manera recursiva: Dados, $\Phi_k(X)$, a para $k < n$, se tiene

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d < n \\ d \in D(n)}} \Phi_d(X)}$$

El grado de un polinomio ciclotómico $\phi_n(X)$ es la función de Euler en n: $\varphi(n)$. Recuerde que, $\varphi : \mathbb{N} \to \mathbb{N}$ es definida por

$$\begin{aligned}
\varphi(n) &= \text{el número de los } k = 1, \cdots, n, \text{ tal que } mcd(k,n) = 1\\
&= |(\mathbb{Z}/n\mathbb{Z})^\times| = \text{el número de elementos del grupo de unidades de } \mathbb{Z}_n\\
&= \text{el número de generadores del grupo cíclico } \mathbb{Z}_n.
\end{aligned}$$

Resumimos algunas propiedades de la función de Euler: $\varphi(1) = 1$, $\varphi(p) = p - 1$ para cualquier primo $p \geq 2$. Para cualquier natural $n \in \mathbb{N}$,

$$n = \sum_{d \in D(n)} \varphi(d).$$

Si $m, n \in \mathbb{N}$ son *primos relativos, ó coprimos*, es decir que $mcd(n, m) = 1$, entonces, $\varphi(mn) = \varphi(n)\varphi(m)$.

Pasaremos luego a la noción de la raíces primitivas de la unidad. Un elemento ζ de un cuerpo $\Bbbk$, se dice que es la *n-esima raíz primitiva* de la unidad, si

$$\text{mín}\left\{k |\ 1 \leq k,\ \zeta^k = 1\right\} \ = \ n.$$

Pensaremos en los elementos $\zeta_n = e^{2\pi i/n}$ como la *estándar n-esima raíz primitiva compleja de la unidad*. Entonces la n-esima raíz de la unidad, es de la forma $\zeta_n^k = e^{2\pi ik/n}$, para $k = 0, 1, \cdots, (n-1)$.

TEOREMA (Raíz primitiva de la unidad). Para cualquier $n \geq 1$, el polinomio ciclotómico $\Phi_n(X)$ es irreducible en $\mathbb{Q}[X]$ y también en $\mathbb{Z}[X]$. Las raíces complejas de $\Phi_n(X)$ son las n-esima raíces primitivas de la unidad,

$$\zeta_n^k = e^{2\pi ik/n}, \ \text{ para } \ k = 0, 1, \cdots, (n-1), \ \text{ con } \ mcd(n, k) = 1,$$

y son de número $grad(\Phi_n(X)) = \varphi(n)$ (el número de Euler de n). Luego

$$\Phi_n(X) \ = \prod_{\substack{t=1,\cdots,(n-1) \\ mcd(t,\,n)\,=\,1}} (X - \zeta_n^t).$$

Al final de esta lección, pasaremos al coso de dominios de integridad de forma $\mathbb{D} := \Bbbk[t]$, para una indeterminada t y donde $\Bbbk$ es un cuerpo, juntos con sus cuerpos de fracciones $\mathbb{K} := \Bbbk(t)$. Cualquier polinomio $f(X)$ en $\mathbb{D}[X]$ es claramente un elemento de $\mathbb{K}[X]$. Escogiendo por $A = \mathbb{D}[X]$ o $\mathbb{K}[X]$, decimos que $f(X)$ tiene *factorización propia sobre* A, si $f(X) = g(X)h(X)$ para algún $g(X), h(X)$ en $A[X]$ con $grad(g(X)) > 0$, $grad(h(X)) > 0$. Con esta definición dada y bajo las

consideraciones de antes, procederemos a mostrar el Lema de Gauss, que dice que si $f(X) \in \mathbb{D}$, entonces $f(X)$ tiene una factorización propia sobre $\mathbb{D}$ si y sólo si la tiene sobre $\mathbb{K}$. Luego daremos el siguiente importante criterio

TEOREMA (El Test de Eisenstein). Sea $\Bbbk$ un cuerpo y t una indeterminada. Denotaremos por $\mathbb{D} = \Bbbk[t]$ el anillo de polinomios sobre $\Bbbk$ y por $\mathbb{K} = \Bbbk(t)$ su anillo de fracciones. Sea $f(X) \in \mathbb{D}[X]$ y $s(t) \in \mathbb{D}$. Sean $a_i(t) \in \mathbb{D}$, tal que

$$f(X) = a_0(t) + a_1(t)(X - s(t)) + \cdots + a_{d-1}(t)(X - s(t))^{d-1} + a_d(t)(X - s(t))^d,$$

donde $d = grad(f(X))$. Supongamos dado $p(t) \in \mathbb{D}$ un elemento irreducible que satisface las siguientes condiciones:

- $p(t)$ divide a $a_k(t)$, para todo $k = 0, 1, \cdots, , d-1$.
- $p(t)^2$ no divide a $a_0(t)$.
- $p(t)$ no divide a $a_d(t)$.

Entonces $f(X)$ es irreducible en $\mathbb{K}[X]$, y luego irreducible en $\mathbb{D}[X]$.

Lección 3 Búsqueda de raíces complejas en grados pequeños.

Esta lección es en el fondo meramente de prácticas, cuyo objetivo es mostrarle al alumno algunas técnicas de busqueda de raíces de polinomios en grados pequeños, precisamente 3 y 4.

Se consideran cuerpos de base $\Bbbk = \mathbb{R}$ números reales ó complejos $\mathbb{C}$. La busqueda de raíces de un polinomio sobre $\Bbbk$ y que sea de grado 1 o 2, es un método muy familiar. Aquí vamos a considerar polinomios de grado 3 y 4.

Polinomios Cúbicos: El método de Cardan Un polinomio cúbico y monoico

$$f(X) \;=\; X^3 + aX^2 + bX + c, \quad \in \mathbb{C}[X]$$

puede transformarse en un polinomio sin monomio de grado 2 haciendo el cambio de variable $X \mapsto (X - a/3)$ dando lugar a

$$g(X) \;=\; f(X - a/3) \;=\; X^3 + \left(b - \frac{1}{3}a^2\right)X + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right) \quad \in \mathbb{C}[X].$$

Buscar las raíces de $f(X)$ es equivalente a buscar las de $g(X)$. De esta manera podemos suponer que queremos buscar las raíces del polinomio

$$f(X) \;=\; X^3 + pX + q \quad \in \mathbb{C}[X].$$

Supongamos que $x \in \mathbb{C}$ es una raíz de $f(X)$, es decir x satisface $x^3 + px + q = 0$. Introducimos un número $u \in \mathbb{C}$ tal que $x = u - \frac{p}{3u}$, entonces

$$\left(u - \frac{p}{3u}\right)^3 + p\left(u - \frac{p}{3u}\right) + q \;=\; 0$$

luego

$$u^3 - \frac{p^3}{27u^3} + q \;=\; 0, \quad \Rightarrow \quad u^6 + qu^3 - \frac{p^3}{27} \;=\; 0.$$

Resolviendo para, $y = u^3$, se tiene

$$u^3 \;=\; -\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}.$$

Así, cualquier raiz cúbica de estos números complejos nos da una raiz $x = u - \frac{p}{3u}$ de $f(X)$. Se pueda ver que hay solamente tres elecciones de x, que viene parametrizada por la raiz cúbica ω^r, $r = 0, 1, 2$, donde $\omega = e^{2i\pi/3}$.

POLINOMIOS CUÁRTICOS: EL MÉTODO DE FERRARI Un polinomio cuártico monoico

$$f(X) \;=\; X^4 + aX^3 + bX^2 + cX + d \;\in \mathbb{C},$$

pude transformarse en un polinomio sin monomio cúbico, haciendo el cambio de variable $X \mapsto X - a/4$, dando lugar a

$$\begin{aligned} g(X) \;&=\; f(X - a/4) \\ &=\; X^4 + \left(b - \frac{3}{8}a^2\right)X^2 + \left(\frac{1}{8}a^3 - \frac{1}{2}ab + c\right)X - \left(\frac{1}{16}ba^3 - \frac{3}{256}a^4 + \frac{1}{4}ac + d\right) \end{aligned}$$

Buscar las raíces de $f(X)$ es equivalente a buscar las de $g(X)$. Por lo tanto, sin perder generalidad, podemos suponer que $f(X)$ es de la siguiente forma:

$$f(X) \;=\; X^4 + pX^2 + qX + r \in \mathbb{C}[X].$$

Si x una raiz de $f(X)$, introducimos dos números y, z tal que $z = x^2 + y$ (sus valor serán fijado después). Entonces

$$\begin{aligned} z^2 \;&=\; x^4 + 2x^2y + y^2 \\ &=\; -px^2 - qx - r + 2x^2y + y^2 \\ &=\; (2y - p)x^2 - qx + y^2 - r. \end{aligned}$$

Escogemos ahora y de tal manera que esta última igualdad sea un cuadrado de un número lineal a x,

$$(2y - p)x^2 - qx + y^2 - r \;=\; (Ax + B)^2 \tag{I.1}$$

Esto se puede hacerse si pedimos que el discriminante de la ecuación de la izquierda sea nulo, i.e.

$$q^2 - 4(2y - p)(y^2 - r) \;=\; 0. \tag{I.2}$$

Observamos que si $y = p/2$, entonces estaremos pidiendo que $q = 0$ y luego

$$f(X) \;=\; X^4 + pX^2 + r \;=\; (X^2)^2 + pX^2 + r \;=\; 0$$

que se puede resolver, resolviendo

$$Z^2 + pZ + r \;=\; 0.$$

Dado que la ecuación (I.2) es cúbica en y, podemos usar el método de Cardan para resolverla. Así, sea $y = t$ una raiz de la misma. Entonces para la ecuación (I.1), tenemos

$$(x^2 + t) \;=\; (Ax + B)^2,$$

de allí

$$x^2 \;=\; -t \pm (Ax + B).$$

Llegaremos pues a cuatro valores de x que expresaremos simbólicamente como

$$x \;=\; \pm\sqrt{-t \pm (Ax + B)}.$$

Al final de la lección le representaremos al alumno algunos ejemplos estimulantes para los métodos de Cardan y Ferrari.

LECCIÓN 4 AUTOMORFISMOS DE ANILLOS Y CUERPOS.

En esta lección pretendemos introducir le al alumno los grupos de automorfismos de un anillo así como el anillo de elementos invariantes bajo la acción natural de este grupo sobre el propio anillo. Desde luego, abordaremos el caso que nos interesa para este curso, a saber los automorfismos de ciertos cuerpos. Emplearemos la siguiente notación: Sea A un anillo y $A_0 \subseteq A$ un subanillo.

($\diamond$) Un *automorfismo* de A es un isomorfismo de anillos $\alpha : A \to A$. El conjunto de todos los automorfismos de A, se denota por $\mathrm{Aut}(A)$.

($\diamond$) Un *automorfismo de* A *sobre* A_0 es un isomorfismo de anillos $\alpha : A \to A$ que satisface $\alpha(a_0) = a_0$, para cualquier elemento $a_0 \in A_0$ (i.e. deja estables los elementos de A_0). El conjunto de todos los automorfismos de A sobre A_0 se denota por $\mathrm{Aut}_{A_0}(A)$

Le haremos al alumno observar que estos conjuntos tienen estructura de grupos. Luego emplearemos el ejemplo de $A = \mathbb{Z}_n$, indicando que $\mathrm{Aut}(A) = \{\mathrm{id}\}$, y por lo tanto $\mathrm{Aut}_A(B) = \mathrm{Aut}(B)$, para cualquier anillo B que contiene a A como subanillo.

De allí, presentaremos el ejemplo del anillo de fracciones de $\mathbb{Z}$ que es $\mathbb{Q}$, para poder deducir que $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$. De esta manera podemos enunciar que si $\Bbbk$ es uno de los cuerpos primos $\mathbb{Q}$ o $\mathbb{F}_p$ ($p > 0$ primo) y si B es un anillo que contiene a $\Bbbk$ como subanillo, entonces $\mathrm{Aut}_\Bbbk(B) = \mathrm{Aut}(B)$.

Cabe mostrarle al alumno el siguiente resultado general.

TEOREMA (Automorfismos de anillos de fracciones). Sea D un dominio de integridad y $\alpha : D \to D$ un automorfismo de D. Entonces, la extensión canónica de α a $Fr(D)$, induce un automorfismo $\alpha_* : FrD \to Fr(D)$. Esto define un monomorfismo de grupos

$$\begin{array}{rcl}(-)_* : \mathrm{Aut}(D) & \longrightarrow & \mathrm{Aut}(Fr(D)) \\ \alpha & \longmapsto & \alpha_*.\end{array}$$

Por supuesto hay que explicar que esta aplicación no es en general un epimorfismo, como contra ejemplo indicaremos el siguiente: Consideramos el dominio de integridad $D = \mathbb{Q}[X]$. Entonces, el automorfismo $\beta : \mathbb{Q}(X) \to \mathbb{Q}(X)$ definido por $\beta(X) = X^{-1}$, claramente no se restringe a un automorfismo de $\mathbb{Q}[X]$.

Presentaremos al alumno algunos ejemplos geométricos. Sea $\Bbbk$ un cuerpo. El grupo de las 2×2-matrices invertibles con entradas en $\Bbbk$, es el 2×2 *grupo lineal general sobre* $\Bbbk$,

$$\mathrm{GL}_2(\Bbbk) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mid a_{ij} \in \Bbbk,\ a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}.$$

Las matrices escalares forman un subgrupo normal

$$\mathrm{Scal}_2(\Bbbk) = \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \mid t \in \Bbbk,\ t \neq 0 \right\} \lhd \mathrm{GL}_2(\Bbbk).$$

El grupo cociente, se llama el 2×2 *grupo lineal proyectivo sobre* $\Bbbk$,

$$\mathrm{PGL}_2(\Bbbk) = \mathrm{GL}_2(\Bbbk)/\mathrm{Scal}_2(\Bbbk).$$

El grupo lineal $\mathrm{GL}_2(\Bbbk)$, tiene también otro subgrupo interesante, el *grupo afín*

$$\mathrm{Aff}_1(\Bbbk) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \Bbbk,\ a \neq 0 \right\} \leq \mathrm{GL}_2(\Bbbk).$$

Bajo estas consideraciones, se presentan los isomorfismos de grupos:

$$\mathrm{Aut}_{\Bbbk}(\Bbbk[X]) \cong \mathrm{Aff}_1(\Bbbk), \qquad \mathrm{Aut}_{\Bbbk}(\Bbbk(X)) \cong \mathrm{PGL}_2(\Bbbk).$$

Finalizaremos esta lección, con la demostración del hecho que el grupo de automorfismos del cuerpo de los números reales es reducido a la identidad, $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$. Así como una discusión formal sobre la dificultad de encontrar los automorfismos del cuerpo de los números complejos, y mostraremos el hecho que $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \overline{(-)}\}$ es un grupo cíclico de orden 2 donde $\overline{(-)} : \mathbb{C} \to \mathbb{C}$, $z = x + iy \mapsto \overline{z} = x - iy$ es la aplicación conjugación.

BIBLIOGRAFÍA

[1] M. Artin. *Algebra*. Prentice Hall inc. 1991.

[2] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[3] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[4] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, 1985.

Tema II

Extensiones de cuerpos.

Lecciones

Las extensiones de cuerpos son claves para el desarrollo de la teoría de Galois de ecuaciones algebraicas. De hecho son las extensiones algebraicas las más destacadas. Así hemos visto conveniente empezar con un tema sobre extensiones de cuerpos generales, luego dedicarle a las extensión algebraicas un tema aparte. El presente tema contiene pues las definiciones generales de las extensiones de cuerpos, en particular abordaremos las extensiones finitas, simples y extensiones producto. Enunciaremos el teorema de multiplicidad para una inclusión de extensiones finita. Luego, daremos el criterio de los elementos algebraicos de una extensión, así varios ejemplos de números transcendentales.

Hubiera sido interesante para el alumno almenos una pequeña lección sobre las extensiones transcendentales de cuerpos; sin embargo por cuestiones de tiempo y espacio nos hemos visto forzado de no hablar en este curso sobre este tipo de extensiones. De todas maneras, hemos visto mejor incluir otras lecciones: de una parte los números constructibles, es decir la construcción con compás y regla, y de otra los teoremas de independencia lineal y independencia algebraica de ciertos homomorfismo, y en particular el teorema de Dedekind.

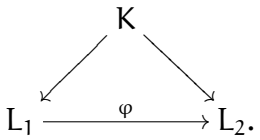
Nos hemos centrado también sobre la variedad de ejemplos a presentare al alumno, así hemos incluido detalladamente varios ejemplos.

LECCIÓN 5 CUERPOS Y SUBCUERPOS.

En esta lección trataremos las extensiones de cuerpos. Daremos pues las definiciones básicas, luego enunciaremos con demostración el teorema de la multiplicidad (conocido también por el nombre del Teorema de la Torre) para a las extensiones finitas.

Empezaremos esta lección por recordar le al alumno lo que es un subcuerpo de un cuerpo, donde emplearemos la notación $K \leq L$, para expresar que K en un subcuerpo de L, y la notación L/K para expresar *una extensión de cuerpos*. Llamaremos el *grado de un extensión de cuerpos* L/K a la dimensión del K-espacio vectorial L, $\dim_K(L)$. Denotaremos, pues $\left[L : K\right] = \dim_K(L)$. Diríamos pues que una extensión de cuerpos es *finita* (*dimensional*) si $\left[L : K\right] < \infty$, y si no se dice que es *infinita* (*dimensional*). El primer ejemplo es: la extensión $\mathbb{C}/\mathbb{R}$ es finita de grado 2, mientras las extensiones $\mathbb{C}/\mathbb{Q}$ y $\mathbb{R}/\mathbb{Q}$ son ambas infinitas. Se dice que L/K es una *subextensión* de T/K, notación $L/K \leq T/K$, cuando se tiene la cadena $K \leq L \leq T$ de cuerpos.

Sean L_1/K y L_2/K dos extensiones del cuerpo base K. *Un morfismo de extensiones* es mrofismos de cuerpos $\varphi : L_1 \to L_2$ que fija lo elementos de K, es decir que haga el siguiente diagrama conmutativo



La relación entre los diferentes grados para una subextensión la expresaremos mediante el siguiente resultado

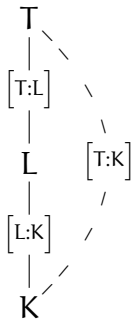
TEOREMA (La ley de Torre ó la multiplicidad de grados). Sea L/K una subextensión de T/K.

(i) Si uno ó los dos grados $\left[L : K\right]$ y $\left[T : L\right]$ es infinito, así es $\left[T : K\right]$.

(ii) Si ambos grados $\left[L : K\right]$ y $\left[T : L\right]$ son finitos, así es $\left[T : K\right]$. Además, se tiene en es caso la fórmula

$$\left[T : L\right]\,\left[L : K\right] \;=\; \left[T : K\right].$$

Una manera de esquematizar las extensiones de cuerpos finitas, es mediante diagrama de forma



donde el orden de inclusión es hacia arriba, y a veces se ignoran las composiciones, i.e. la linea de rayas.

LECCIÓN 6 EXTENSIONES SIMPLES Y FINITAMENTE GENERADAS.

Como ya viene indicando el titulo de esta lección, se trata de introducir las extensiones de cuerpos llamadas simples y las finitamente generadas. Así daremos pues el criterio sobre los elementos algebraicos, y abordaremos las extensiones producto, acompañando todas estas nociones con varios ejemplos.

Empezaremos explicando las siguientes observaciones. La intersección de cualquier familia de subanillos (no vacía) de un anillo es también un subanillo. Si $B \subseteq A$ es un subanillo de A junto con un subconjunto S de A, podemos preguntar por la intersección de todos los subanillos de A que contienen a B como subanillo y a su vez a S como subconjunto. Llamaremos este subanillo el *subanillo de* A *generado sobre* B *por* S, y le denotaremos por $B[S]$. Si $S = \{s_1, \cdots, s_r\}$, denotaremos $B[s_1, \cdots, s_r]$ por $B[S]$. Por el momento, se sabe que $\mathbb{R}[i] = \mathbb{R}[\sqrt{-1}] = \mathbb{C}$. Concluimos pues con las consecuencias:

- El anillo $B[S]$ consiste en elementos de A que se pueden expresarse como sumas finita de la siguiente forma

$$\sum_{\text{finita}} a_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \quad a_{i_1,\cdots,i_n} \in B, \;\; x_i \in S.$$

- Sea D un dominio de integridad que contiene un cuerpo F (como subanillo). Si D visto como F-espacio vectorial es de dimensión finita. Entonces D es un cuerpo.

Pasaremos luego al caso de cuerpos.
Sea F un cuerpo y $K \leq F$. Dado un conjunto de elementos $u_1, \cdots, u_r \in F$, consideramos

$$K(u_1, \cdots, u_r) \;=\; \bigcap_{\substack{K \leq L \leq F \\ u_1,\cdots,u_r \in L}} L$$

que es el subcuerpo más pequeño de F que contiene K y los elementos $u_1, \cdots, u_r$.

La extensión $K(u_1, \cdots, u_r)/K$ se dice que es *generada* por los elementos $u_1, \cdots, u_r$; también se dice que $K(u_1, \cdots, u_r)/K$ es *finitamente generada*. Una extensión de forma $K(u)/K$ se dice que es *una extensión simple de* K *con generador* u.

$$K(u_1, \cdots, u_r) = \left\{ \frac{p(u_1, \cdots, u_r)}{q(u_1, \cdots, u_r)} \in F \mid p(X_1, \cdots, X_r),\ q(X_1, \cdots, X_r) \in K[X_1, \cdots, X_r],\ q(u_1, \cdots, u_r) \neq 0 \right\}.$$

Esta claro que hay que indicar que cualquier reordenación de los u_i no afecta al cuerpo $K(u_1, \cdots, u_r)$. De esta forma se llega al enunciado: Sean $K(u)/K$ y $K(u, v)/K(u)$ dos extensiones simples. Entonces

$$K(u, v) = K(u)(v) = K(v)(u).$$

En general tenemos que

$$K(u_1, \cdots, u_n) = K(u_1, \cdots, u_{n-1})(u_n),$$

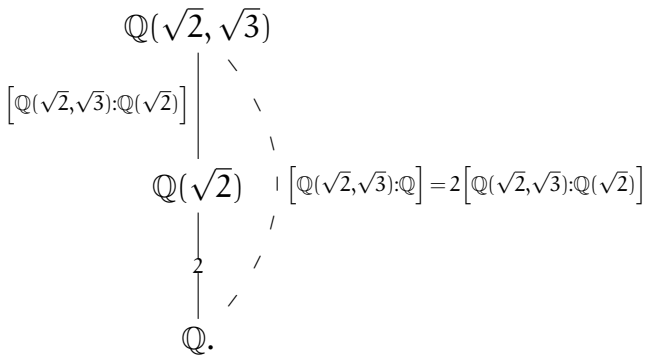
además esto es independientemente del orden de la sucesión de elementos $u_1, \cdots, u_n$. Después daremos el siguiente resultado importante sobre las extensiones simples.

TEOREMA (Extensiones simples). Consideramos $K(u)/K$ una extensión simple de cuerpos. Entonces, exactamente una de las siguientes condiciones es válida

(1) El morfismo de evaluación en u, $\varepsilon_u : K[X] \to K(u)$ es un monomorfismo (su núcleo es cero), y su prolongación al cuerpo de fracciones $(\varepsilon_u)_* : K(X) \to K(u)$ es un isomorfismo. En tal caso, $K(u)/K$ es infinita, y se dice que u **es transcendental sobre** K.

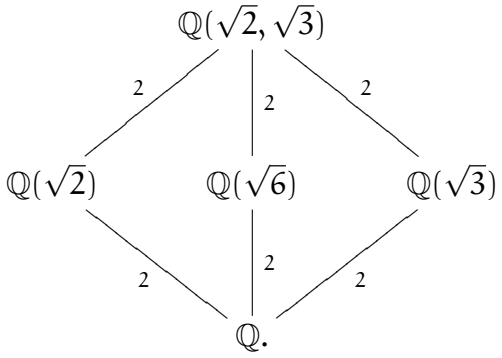
(2) El morfismo de evaluación en u, $\varepsilon_u : K[X] \to K(u)$ tiene un núcleo no nulo, es decir $\mathrm{Ker}(\varepsilon_u) = \langle p(X)\rangle$ donde $p(X) \in K[X]$ es un polinomio monoico irreducible de grado positivo y el morfismo cociente $\widetilde{\varepsilon_u} : K[X]/\langle p(X)\rangle \to K(u)$ es un isomorfismo. En tal caso, $K(u)/K$ es una extensión simple finita de grado $\left[K(u) : K\right] = \mathrm{grad}(p(X))$ y se dice que u **es algebraico sobre** K.

Como ejemplo de aplicación daremos el siguiente: El grado de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ es $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\right] = 4$. Como $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$, tenemos pues la siguiente torre de extensiones



Por supuesto que existen otras subextensiones de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,

como demuestra el diagrama



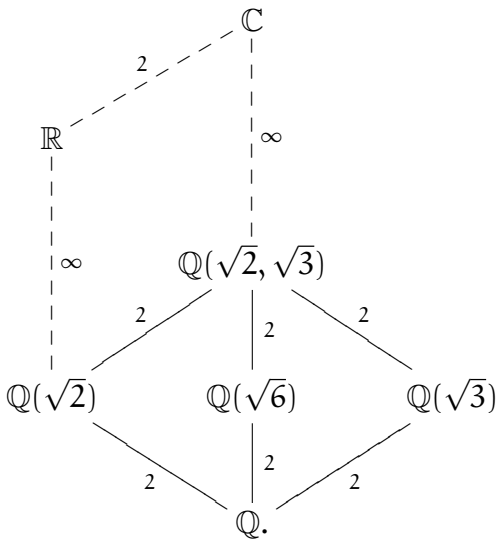
Una de las ideas empleadas en el Ejemplo anterior, sirve para demostrar un resultado más general: Consideramos $p_1, \cdots, p_n$ una sucesión de primos distintos $p_i > 0$. Entonces,

$$\sqrt{p_n} \notin \mathbb{Q}\left(\sqrt{p_1}, \cdots, \sqrt{p_{n-1}}\right).$$

Luego

$$\left[\mathbb{Q}\left(\sqrt{p_1}, \cdots, \sqrt{p_n}\right) : \mathbb{Q}\left(\sqrt{p_1}, \cdots, \sqrt{p_{n-1}}\right)\right] = 2, \text{ y } \left[\mathbb{Q}\left(\sqrt{p_1}, \cdots, \sqrt{p_n}\right) : \mathbb{Q}\right] = 2^n.$$

Para la extensión $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, tenemos $\left[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}\right] = 4$. Este ejemplo también contiene varias subextensiones:



Uno de los ejemplos más exóticos de extensiones simples son algunas extensiones especiales dentro de la extensión $\mathbb{R}/\mathbb{Q}$, los cuales preferimos incluir en las prácticas:
Sea $n \geq 1$ un número natural. Se define $E_n := \mathbb{Q}(2^{\frac{1}{n}})$ como subcuerpo de $\mathbb{R}$, donde $2^{\frac{1}{n}}$ denota la n-esima raiz positiva de 2. Con esta definición, se tiene que

(1) Como extensión $E_n/\mathbb{Q}$ tiene grado n, i.e. $\left[E_n : \mathbb{Q}\right] = n$.

(2) Si $m \geq 1$, con $m|n$ (m divide a n), entonces $E_m \leq E_n$ y se tiene que

$$n \;=\; m\left[E_m : E_n\right].$$

(3) Si $\mathrm{mcd}(m,n) = 1$ (primos relativo), entonces

$$E_{nm} \;=\; \mathbb{Q}\left(2^{\frac{1}{n}}, 2^{\frac{1}{m}}\right).$$

(4) * El grupo de automorfismos de la extensión $E_n/\mathbb{Q}$, viene determinado por

$$\mathrm{Aut}_{\mathbb{Q}}(E_n) \;=\; \begin{cases} \{id\} & \text{Si } n \text{ es impar} \\ \{id, \tau_n\} \cong \mathbb{Z}/2\mathbb{Z} & \text{Si } n \text{ es par} \end{cases}$$

para algún automorfismo τ_n de orden 2.

(5) * Sea $E = \bigcup_{n\geq 1} E_n \subseteq \mathbb{R}$, entonces $\mathrm{Aut}_{\mathbb{Q}}(E) = \{id\}$.

Pasaremos ahora a otro tipo de extensiones. Sea L una extensión de K junto con S, T, dos subcuerpos de L ambos contiene a K. Entonces ST, la *composición* de S y T, es el subcuerpo más pequeño de L que contiene simultáneamente a S y a T, y a su vez es una extensión de K. En otras palabras ST/K es la extensión más pequeña entre todas las subextensiones de L/K que contienen a la vez T/K y S/K. El subcuerpo ST consiste precisamente en elementos de forma

$$\left(\sum_i s_i t_i\right)\left(\sum_j s'_j t'_j\right)^{-1},$$

donde $s_i, s'_j \in S$ mientras que $t_i, t'_j \in T$.

Sea L una extensión de K junto con S, T, dos subcuerpos de L ambos contiene a K. Supongamos que $\left[T : K\right]$ es finito. Entonces $\left[ST : S\right] \leq \left[T : K\right]$ y

$$ST = \left\{ \sum_{i=1}^{n} s_i t_i \mid s_i \in S,\, t_i \in T \right\}.$$

Además,

$$\left[ST : K\right] \leq \left[S : K\right] \left[T : K\right].$$

Para $K = \mathbb{Q}$ y $L = E_{12}$ se puede ver que tenemos las siguientes igualdades de cuerpos

$$E_2 E_3 = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = E_6 = \mathbb{Q}(\sqrt[6]{2}).$$

Para $K = \mathbb{Q}$ y $L = \mathbb{R}$, $S = \mathbb{Q}(\sqrt[3]{2})$, $T = \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$, donde como antes ζ_3^2 es la raiz primitiva cubica de 1, observe que es también raiz del polinomio cuadrático $X^2 + X + 1$. Entonces, $ST = \mathbb{Q}(\zeta_3^2, \sqrt[3]{2})$, y además

$$ST = S(\zeta_3^2).$$

Tenemos, $\left[ST : S\right] = 2 < \left[T : K\right] = 3$ y $\left[ST : K\right] = 6 < \left[T : K\right]\left[S : K\right] = 9$. Tenemos que indicar que en ambos caso, se tiene que $S \cap T = K$.

LECCIÓN 7 ALGUNOS NÚMERO TRANSCENDENTALES.

Un número complejo se dice que es *algebraico* o *transcendental* según lo es sobre $\mathbb{Q}$.

- 1844: Liouville demuestra que algunos números, ahora llamados *números de Liouville*, son transcendentales (en su expansión decimal son de forma $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$)
- 1873: Hermite demuestra que e es transcendental.
- 1874: Cantor comprueba que el conjunto de los número transcendentales es numerable, pero $\mathbb{R}$ no lo es. Así hay muchos número transcendentales, pero es siempre difícil comprobar si algún número es transcendental.
- 1882: Lindemann demuestra que π es transcendental.
- 1934: Gel'fond y Schneider independientemente comprobaron que α^{β} es transcendental si α y β son algebraicos, con $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q}$ (esto era uno de los famosos problemas de Hilbert, el séptimo).
- 2004: La constante de Euler
$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log(n) \right)$$
no ha sido comprobada, hasta la fecha, si es un número transcendental ni si quiera irracional¡
- 2004: Los números $e+\pi$ y $e-\pi$ seguro que son transcendentales, pero ni si quiera, hasta la fecha, han sido comprobados de ser irracionles¡

TEOREMA (Liouville). El número de Liouville $\alpha = \sum_{n=0}^{\infty} \frac{1}{2^{n!}}$ es transcendental.

TEOREMA. El conjunto de números algebraicos es numerable.

LECCIÓN 8 CONSTRUCCIONES CON REGLA Y COMPÁS.

El principal problema es la construcción de un polígono regular en el plano, usando únicamente la regla y el compás. Este problema surgeo en la época Griega. Los Griegos sabían los números enteros y números racionales. Les ha sorprendido encontrar la medida de la diagonal de un cuadrado con longitud de lado 1, no es un número racional, de hecho $\sqrt{2}$. Llegaron pues a la conclusión de que deben implicar su sistema de numeración; deseando con eso que los números "constructibles" sean suficientes. Supongamos dada un medida 1 (o longitud, que consta pues de dos puntos que serían el centro del polígono y un vértice aleatorio), y que disponemos de una regla y un compás. Un número real (o mejor una longitud) es *constructible*, si se puede ser construido formando una intercesión sucesiva de

(◇) segmentos dibujados con puntos antes construidos, y

(◇) círculos con centro un punto antes construido y radio una longitud antes construida.

Esto llevo al los Griegos a formalizar las siguientes preguntas que no fueron capaces de responder: ¿Es posible la duplicación de un cubo, la trisección de un ángulo, o la cuadratura de un círculo? Como vamos ha explicar en está lección la respuesta es negativa.

Sea $\mathbb{F}$ un subcuerpo de $\mathbb{R}$. Para cualquier número positivo $a \in \mathbb{F}$, $\sqrt{a}$ denota la raíz positiva de $a \in \mathbb{R}$. El $\mathbb{F}$-*plano* es $\mathbb{F} \times \mathbb{F} \subseteq \mathbb{R} \times \mathbb{R}$. Se define pues

Una $\mathbb{F}$-*recta* es un recta en $\mathbb{R} \times \mathbb{R}$ con dos puntos en el $\mathbb{F}$-plano. Estas son rectas que vienen dadas por las ecuaciones:

$$ax + by = c, \quad \text{con } a, b, c \in \mathbb{F}.$$

Un $\mathbb{F}$-*círculo* es un círculo en $\mathbb{R}\times\mathbb{R}$ con centro un $\mathbb{F}$-punto y radio un elemento de $\mathbb{F}$. Estos son círculos dados por las ecuaciones

$$(x-a)^2+(y-b)^2 \;=\; c^2, \quad \text{con } a,b,c\in\mathbb{F}.$$

De esta definiciones pasaremos a enunciar los siguientes resultados.

TEOREMA. Sean $\mathbb{F}$ un subcuerpo de $\mathbb{R}$, $L\neq L$ dos $\mathbb{F}$-rectas distintas y $C\neq C'$ dos $\mathbb{F}$-círculos distintos.

(a) $L\cap L=\emptyset$ o consiste en solo $\mathbb{F}$-punto.

(b) $L\cap C=\emptyset$ o consiste en uno o dos puntos del $\mathbb{F}(\sqrt{e})$-punto, para un cierto $e\in\mathbb{F}$, $e>0$.

(c) $C\cap C'=\emptyset$ o consiste en uno o dos puntos del $\mathbb{F}(\sqrt{e})$-punto, para un cierto $e\in\mathbb{F}$, $e>0$.

(d) Si c y d con constructibles, así pues son $c+d,-c,cd$ y $\frac{c}{d}$ $(d\neq 0)$.

(e) Si $c>0$ es constructible, así pues es $\sqrt{c}$

TEOREMA.

(i) Los número constructibles forman un cuerpo.

(ii) Un número α es constructible si, y sólo si pertenece en un subcuerpo de $\mathbb{R}$ de la forma

$$\mathbb{Q}(\sqrt{a_1},\cdots,\sqrt{a_r}), \quad \text{con } a_i\in\mathbb{Q}(\sqrt{a_1},\cdots,\sqrt{a_{i-1}}), \quad a_i>0.$$

En particular, si α es un número constructible, entonces α es algebraico sobre $\mathbb{Q}$ y el grado $\left[\mathbb{Q}(\alpha):\mathbb{Q}\right]$ es una potencia de 2.

Como consecuencias se tiene:

(1) Es imposible duplicar el cubo usando la regla y el compás.

El problema es pues de construir un cubo con volumen 2. Esto requiere la construcción de una raíz real del polinomio $X^3 - 2$. Pero este polinomio es irreducible según el criterio de Eisenstein, y luego $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$.

(2) En general, es imposible la trisección de un ángulo con la regla y el compás.

Dar un ángulo es dar el cosenos del ángulo. Por lo tanto, para triseccionar 3α, se tiene que construir la solución de la ecuación:

$$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha).$$

Por ejemplo si $3\alpha = 60^o$, como $\cos(60^o) = \frac{1}{2}$, para construir α, se tiene que resolver la ecuación $8X^3 - 6X - 1 = 0$, que es irreducible.

(3) Es imposible cuadrar un círculo usando la regla y el compás.

Un cuadrado con la misma área que un círculo de radio r, tiene por lado $\sqrt{\pi r}$. Dado que π es un número transcendental, así pues es $\sqrt{\pi}$.

Ahora volvemos al antiguo y famoso problema de la construcción de un polígono regular. Notemos que $X^m - 1$ no es irreducible, dado que

$$X^m - 1 = (X - 1)(X^{m-1} + X^{m-2} + \cdots + 1).$$

Pero si tenemos

Si p es primo, entonces $X^{p-1} + X^{p-2} + \cdots + 1$ es irreducible; luego $\mathbb{Q}(e^{2\pi i/p})$ tiene grado $p - 1$ sobre $\mathbb{Q}$.

Para poder construir un p-polígono regular, con p primo $p \neq 2$, hace falta construir

$$\cos(\frac{2\pi}{p}) = \frac{e^{\frac{2\pi i}{p}} + e^{-\frac{2\pi i}{p}}}{2}.$$

Pero sabemos que existe la torre de cuerpos

$$\begin{array}{c} \mathbb{Q}(e^{\frac{2\pi i}{p}}) \\ \Big| \\ 2 \\ \Big| \\ \mathbb{Q}\left(\cos(\frac{2\pi}{p})\right) \\ \Big| \\ \frac{p-1}{2} \\ \Big| \\ \mathbb{Q} \end{array}$$

Así si el p-polígono es constructible, entonces $(p-1)/2 = 2^k$, para algún k, lo que implica que $p = 2^{k+1}+1$. Pero 2^r+1 es primo solo si r es potencia de 2, de otra manera r tendría un factor impar de t y para t impar

$$Y^t + 1 = (Y+1)(Y^{t-1} - Y^{t-2} + \cdots + 1);$$

de allí

$$2^{st} + 1 = (2^s - 1)((2^s)^{t-1} - (2^s)^{t-2} + \cdots + 1).$$

Es decir si el p-polígono regular es constructible, entonces $p = 2^{2^k} + 1$, para algún k.

La conjetura de Fermat aseguraba que todos los número de forma $2^{2^k}+1$ son primos (conocidos también por el nombre de primos de Fermat para $0 \leq k \leq 4$). Euler demostró que para $k = 5$ se tiene que $2^{32}+1 = (641)(6700417)$, y no se sabe hasta el día de hoy de otro número primo de Fermat. Gauss ha comprobado en sus 18 años que

$$\cos(\frac{2\pi}{17}) = -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

LECCIÓN 9 INDEPENDENCIAS LINEAL Y ALGEBRAICA DE HOMOMORFISMOS.

El principal objetivo de esta Lección es de demostrar el Teorema de Dedekind sobre la independencia de morfismos lineales. Así como la independencia algebraica de morfismos.

Sea L/K una extensión de cuerpos y V un K-espacio vectorial. Se denota por $\mathrm{Hom}_K(L, V)$ el conjunto de todas las aplicaciones K-lineales de L en V. Esto es un L-espacio vectorial cuya estructura viene dada por

$$x \,.\, f : V \longrightarrow L, \quad \Big(y \longmapsto xf(y)\Big), \forall\, x \in L,\ f \in \mathrm{Hom}_K(V, L).$$
$$f + g : V \longrightarrow L, \quad \Big(y \longmapsto f(y) + g(y)\Big), \forall\, f, g \in \mathrm{Hom}_K(V, L).$$

Es un ejercicio fácil de ver que, si V es de dimensión finita sobre K, entonces

$$\mathrm{Hom}_K(V, L) \cong L \otimes_K V, \qquad \text{isomorfismo de } L\text{-espacios vectoriales.}$$

De allí la fórmula de igualdad de dimensiones:

$$\Big[\mathrm{Hom}_K(V, L) : L\Big] \;=\; \Big[V : K\Big].$$

Estos argumentos son la clave para comprobar el siguiente resultado

TEOREMA. Sea L/K una extensión de cuerpos, y A un K-álgebra. Sea $\mathcal{H}$ el conjunto de todos los homomorfismos de K-álgebras de A en L. Entonces $\mathcal{H}$ es una parte libre del L-espacio vectorial $\mathrm{Hom}_K(A, L)$.

Recordaremos que *un monoide* es un conjunto dotado de una ley de composición y un elemento neutro donde no necesariamente todo elemento es invertible por esa ley. Por ejemplo $\mathbb{N}$. Así *un homomorfismo de monoides* es una aplicación compatible con las leyes de composición y respecta al elemento neutro.

Como consecuencia del resuelto anterior se tiene:

TEOREMA. Sean Γ cualquier monoide, L un cuerpo y $\mathcal{X}$ el conjunto de todos los homomorfismos de monoides de Γ en $L^\times$ el monoide multiplicativo de L. Entonces $\mathcal{X}$ es una parte libre del L-espacio vectorial L^Γ de todas las aplicaciones de Γ en L.

TEOREMA (Dedekind). Sean E/K y L/K dos extensiones de cuerpos de K. Entonces el conjunto de todas las aplicaciones K-lineales de E en L es libre sobre L. Además, si E es de grado finito sobre K, entonces el número de aplicaciones K-lineales de E en L es a lo sumo $\left[E : K\right]$.

Finalizaremos la lección con el siguiente resultado sobre la independencia algebraica.

TEOREMA. Sean K un cuerpo infinito, L/K una extensión de K y A un K-álgebra. Consideramos $u_1, \cdots, u_n$ homomorfismos distintos de K-álgebras de A en L y f un polinomio de $L[X_1, \cdots .X_n]$. Si tenemos $f(u_1(x), \cdots, u_n(x)) = 0$, para todo elemento $x \in A$, entonces $f = 0$.

BIBLIOGRAFÍA

[1] E. Artin. *Galois Theory*. Number 2 in Note Dame Mathematical Lectures. 1944.

[2] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[3] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 5 á 7.* Springer-Verlag, Berlin Heidelberg, 2007.

[4] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[5] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, 1985.

Tema III

Extensiones algebraicas de cuerpos.

Lecciones

Como ya hemos señalado antes las extensiones algebraicas juegan un papel crucial en la teoría de Galois de ecuaciones algebraicas. Este tema lo dedicaremos pues íntegramente al estudio de este tipo de extensiones.

Después de dar las definiciones y las propiedades básicas de una extensión algebraica; pasaremos a comprobar el teorema de Kronecker sobre la existencia del cuerpo de descomposición de un polinomio prefijado. Señalaremos también la posibilidad de construir el cuerpo de descomposición para un conjunto posiblemente infinito de polinomios no constantes. Acompañamos el teorema de Kronecker con varios ejemplos de aplicación. Luego abordaremos la relación entre los monomorfismos de una extensión simple en cualquier otra extensión y las raíces de un polinomio prefijado, usando para ello la noción de raíces conjugadas.

Pasaremos luego a definir lo que es la clausura algebraica de un cuerpo y intentar demostrar su existencia. Antes de enunciar y demostrar el teorema del elemento primitivo, hablaremos de la multiplicidad de una raíz así como la separabilidad de un polinomio. Completaremos esa parte del tema con el teorema de polinomios separable. Daremos pues la definición de una extensión separable y finalizaremos el tema con la definición de las extensiones normales, discutiendo su relación con los cuerpos de descomposición (o cuerpos de escisión).

LECCIÓN 10 EXTENSIONES ALGEBRAICAS.

En esta lección, como ya indica su titulo, vamos abordar las extensiones algebraicas y sus principales propiedades. Insistimos en completar la teoría con varios ejemplos.

Antes de definir lo que es una extensión algebraica, daremos la siguiente caracterización de los elementos algebraicos:

TEOREMA (Elementos algebraicos). Sea $t \in L$. Entonces las siguientes condiciones son equivalentes.

(i) t es algebraico sobre K.

(ii) El homomorfismo de evaluación $\varepsilon_t : K[X] \to L$ tiene un núcleo no nulo.

(iii) La extensión $K(t)/K$ es finito dimensional.

Si $t \in L$ es algebraico sobre K, según ese resultado, se tiene que

$$\mathbf{Ker}(\varepsilon_t) \;=\; \langle \mathtt{Polmin}_{K,t}(X) \rangle \;\neq\; \langle 0 \rangle\,,$$

donde $\mathtt{Polmin}_{K,t}(X) \in K[X]$ es un polinomio monoico irreducible, llamado el *polinomio minimal de* t *sobre* K. El grado de $\mathtt{Polmin}_{K,t}(X)$ se llama *el grado de* t *sobre* K y lo denotaremos por $\mathtt{grado}_{K,t}$.

Otra manera diferente, aunque equivalente, de definir el polinomio minimal es la siguiente: Sea $t \in L$ un elemento algebraico sobre K. Entonces

$$\mathcal{J}(t) \;=\; \Big\{ f(X) \in K[X] \,|\, f(t) \;=\; 0 \Big\} \subseteq K[X]$$

es un ideal principal que tiene un generador monoico y irreducible $q(X) \in K[X]$. De hecho, $q(X) = \mathtt{Polmin}_{K,t}(X)$.

Como consecuencia de la Lección 6 del presente curso, se tiene lo siguiente:

Si $t \in L$ es un elemento algebraico sobre K, entonces

$$\Big[K(t) : K\Big] \;=\; \mathtt{grad}(\mathtt{Polmin}_{K,t}(X)) \;=\; \mathtt{grado}_{K,t}.$$

A modo de ejemplo presentaremos los siguientes ejemplos:

(1) para $t = \sqrt{2}$,

$$\mathtt{Polmin}_{\mathbb{Q},\sqrt{2}}(X) \;=\; X^2 - 2, \quad \mathtt{grado}_{\mathbb{Q},\sqrt{2}} \;=\; \Big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\Big] \;=\; 2.$$

(2) para $t = i$,

$$\mathtt{Polmin}_{\mathbb{Q},i}(X) \;=\; X^2 + 1, \quad \mathtt{grado}_{\mathbb{Q},i} \;=\; \Big[\mathbb{Q}(i) : \mathbb{Q}\Big] \;=\; 2.$$

(3) para $t = \zeta_6$ la sexta raiz primitiva de la unidad,

$$\mathtt{Polmin}_{\mathbb{Q},\zeta_6}(X) \;=\; X^2 - X + 1 = \Phi_6(X), \quad \mathtt{grado}_{\mathbb{Q},\zeta_2} \;=\; 2.$$

(4) Para $t = \sqrt{2} + \sqrt{3}$

$$\mathtt{Polmin}_{\mathbb{Q},\sqrt{2}+\sqrt{3}} \;=\; X^4 - 10X + 1, \quad \mathtt{grado}_{\mathbb{Q},\sqrt{2}+\sqrt{3}} \;=\; 4.$$

Pasaremos luego a la noción de elementos primitivos.
Sea L/K una extensión de cuerpos finita. Un elemento $u \in L$, se dice que es un *elemento primitivo para la extensión* L/K, si se verifica que $L = K(u)$. Cabe mencionar que más adelante explicaremos que en el caso $\mathtt{Cara}(K) = 0$, cualquier extensión finita L/K tiene un elemento primitivo. Los elementos primitivos en el caso finito, se caracterizan como sigue. Sea L/K un extensión de cuerpos finita y $u \in L$. Entonces, u es primitivo para L/K si y sólo si

$$\mathtt{grado}_{K,u} \;=\; \Big[L : K\Big].$$

La siguiente observación es de uso frecuente en lo largo de este curso. Sea L/K un extensión de cuerpos y supongamos dados $u_1, \cdots, u_n \in L$, n-elementos algebraicos sobre K. Entonces, $K(u_1, \cdots, u_n)/K$ es un extensión finita.

Llegaremos pues a una noción importante de extensiones.
Una extensión de cuerpos L/K, se dice que es *algebraica* si cualquier elemento $t \in L$ es algebraico sobre K. Presentaremos al alumno las primeras consecuencias de esta definición:

- Sea L/K una extensión finita de cuerpos. Entonces, L/K es una extensión algebraica.
- Sean S/L y L/K dos extensiones algebraicas de cuerpos. Entonces la extensión S/K es algebraica.

Es natural de definir para una extensión de cuerpos L/K cualquiera, el siguiente conjunto

$$L^{alg} = \left\{ t \in L \mid t \text{ es algebraico sobre } K \right\} \subseteq L.$$

Se tiene así que L^{alg} es un subcuerpo de L que contiene a K. Además L^{alg}/K es una extensión algebraica.

Finalizaremos esta lección enunciando el siguiente resultado

TEOREMA. Sea $K(u)/K$ una extensión simple finita de cuerpos. Entonces, hay solamente unas pocas subextensiones $F/K \leq K(u)/K$. Cualquiera de ellas es de forma $K(a_0, a_1, \cdots, a_{l-1})$, donde

$$a_0 + a_1 X + \cdots + a_{l-1} X^{l-1} + X^l \in K(u)[X]$$

es un factor de $\texttt{Polmin}_{K,u}(X) \in K(u)[X]$.

LECCIÓN 11 TEOREMAS DE KRONECKER Y CUERPOS DE DESCOMPOSICIÓN.

En esta lección queremos demostrar ante el alumno el teorema de Kronecker, que garantiza la existencia de una extensión de escisión para un polinomio con coeficientes en el cuerpo base, o lo que es lo mismo que el cuerpo de descomposición[1] de un polinomio. Como aplicación de dicho teorema, daremos un ejemplo concreto.

Antes de introducir lo que es un cuerpo de descomposición, conviene hacer la siguiente reflexión. Sea $p(X) \in K[X]$ un polinomio de grado positivo sobre un cuerpo K. Haremos las siguientes preguntas:

Pregunta (1).¿ Existe alguna extensión de cuerpos L/K por la cual $p(X)$ tendrá raíz en L?

Un versión más fuerte sería:

Pregunta (2).¿ Existe alguna extensión de cuerpos E/K por la cual $p(X)$ factoriza en factores lineales (i.e. de grado uno) en $E[X]$?

Luego daremos la definición:
Se dice que un polinomio $p(X) \in K[X]$ sobre un cuerpo K, *escinde en* E/K o *sobre* E, si se factoriza en factores lineales en $E[X]$ (i.e. de grado 1).

Por supuesto, si tal cuerpo E existe, entonces las raíces $u_1, \cdots, u_r$ de $p(X)$ en E generan el subcuerpo $K(u_1, \cdots, u_r) \leq E$ que será el subcuerpo más pequeño que responda a la pregunta **(1)**.

Tal extensión minimal de K, se le llama *el cuerpo de descomposición (o la extensión escindida) de* $p(X)$ *sobre* K, que se denota a veces por $K_{p(X)}$ o simple-

[1] A veces usaremos también el término: *cuerpo de escisión*

mente por K_p. Sabemos de antes como responder a la pregunta **(2)**.

> TEOREMA (De Kronecker). Sea K un cuerpo y $p(X) \in K[X]$ un polinomio de grado positivo.
>
> (i) Existe una extensión finita L/K por la cual $p(X)$ tiene una raíz en L.
>
> (ii) Existe una extensión finita E/K tal que E es el cuerpo de descomposición de $p(X)$ sobre K.

Pasaremos luego a una definición más general.
Sea K un cuerpo y $\{f_i\}_{i\in I}$ una familia de polinomios no constantes de $K[X]$. Se le llama al *cuerpo de descomposición* de $\{f_i\}_{i\in I}$, a cualquier extensión E de K que posee las siguientes propiedades:

(a) E es el cuerpo de descomposición de cada uno de los polinomios f_i, $i \in I$ sobre K.

(b) E es el cuerpo de fracciones sobre K con indeterminadas el conjunto de todas las raíces de todos los f_i, es decir

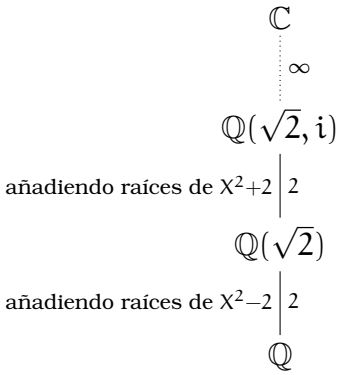
$$E = K\left(\bigcup_{i\in I} \mathtt{Raíz}(E, f_i)\right),$$

donde $\mathtt{Raíz}(E, f_i)$ es el conjunto de las raíces de f_i en E.

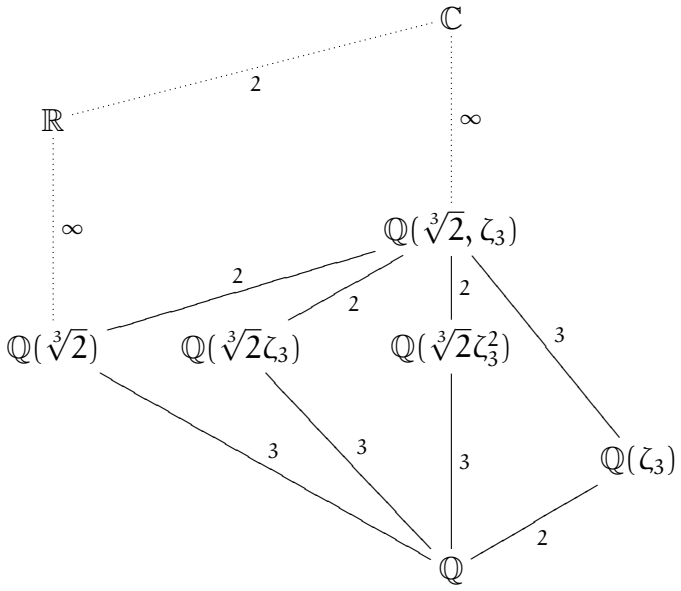
Se puede comprobar la existencia y la unicidad (salvo K-isomorfismo) de tal cuerpo de descomposición.

Los siguientes serán nuestro ejemplos para la aplicación del Teorema de Kronecker.
La extensión escindida de $p(X) = X^4 - 4$ sobre $\mathbb{Q}$ en $\mathbb{C}$ es $\mathbb{Q}(\sqrt{2}, i)$ y $\left[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}\right] =$

4, una torre de extensiones es



La extensión escindida de X^3-2 en $\mathbb{C}$ sobre $\mathbb{Q}$, es $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ con $\left[\mathbb{Q}(\sqrt[3]{2},\zeta_3):\mathbb{Q}\right] = 6$, y una torre de extensiones es



LECCIÓN 12 MONOMORFISMOS DE EXTENSIONES.

Empezaremos esta lección dando la definición de monomorfismos de extensiones de cuerpos y su relación con el conjunto de raíces de un polinomio. Adoptaremos la siguiente notación: Sean L/K, F/K dos extensiones de cuerpos, denotaremos por $\mathtt{Mono}_K(L, F)$ el conjunto de todos los monomorfismos $L \to F$ que dejan fijados los elementos de K (i.e. *monomorfismo de extensiones de cuerpos*). Esta claro que en general siempre se tiene que $\mathrm{Aut}_F(K) \subseteq \mathtt{Mono}_K(F, F)$. Si F/K es finita, entonces cualquier monofisismo K-lineal de F en F, es de hecho una biyección. Por lo tanto, si F/K es una extensión finita, entonces se tiene la igualdad, i.e. $\mathrm{Aut}_K(F) = \mathtt{Mono}_K(F, F)$. Usaremos ciertas notaciones. Sea F/K una extensión de cuerpos y $p(X) \in K[X]$. Consideramos

$$\mathtt{Raíz}(p, F) = \left\{u \in F \mid p(u) = 0\right\},$$

el conjunto de todas las raíces de $p(X)$ en F. Este es un conjunto finito, que pueda ser vacío (esto ocurre exactamente cuando $p(X)$ no tiene raíces en K).
De esta manera llegaremos a la siguiente biyección:

TEOREMA. Sea F/K una extensión de cuerpos. Sea $p(X) \in K[X]$ un polinomio irreducible de $K[X]$ junto con $t_0 \in F$ una raíz de $p(X)$. Existe una biyección de conjuntos

$$\mathtt{Raíz}(p, F) \simeq \mathtt{Mono}_K(K(t_0), F)$$

que viene dada por $t \mapsto \varphi_t$, donde $\varphi_t : K(t_0) \to F$ hace $\varphi_t(t_0) = t$.

Como ejemplo práctico, calculemos el número de elementos que tiene el conjunto $\mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})$. Se sabe ya que $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/\langle X^2 - 2\rangle$ donde $X^2 - 2$ es irreducible sobre $\mathbb{Q}$. Por lo tanto, queremos que los monomorfismo $\mathbb{Q}$-lineales envíen a $\sqrt{2}$ en $\pm\sqrt{2}$. De allí, se tiene los dos monomorfismos: $\mathrm{id}, \alpha : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, donde

$$\alpha(a + b\sqrt{2}) = a - b\sqrt{2}, \quad \forall a, b \in \mathbb{Q}.$$

Dado que la imagen de $\mathbb{Q}(\sqrt{2})$ mediante cualquier elemento de $\mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})$ queda dentro de $\mathbb{Q}(\sqrt{2})$ (no es siempre el caso), entonces

$$\mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) \;=\; \mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})) \;=\; \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})),$$

que contiene únicamente dos elementos como ya hemos enunciado en ejemplos anteriores.

TEOREMA (Monomorfismos y raíces). Sean L/K y F/K dos extensiones de cuerpos.

(i) Para algún $p(X) \in K[X]$, cada monomorfismo $\alpha \in \mathtt{Mono}_K(L, F)$, se restringe a una aplicación inyectiva $\alpha_p : \mathtt{Raíz}(p, L) \to \mathtt{Raíz}(p, F)$.

(ii) Si $\alpha \in \mathtt{Mono}_K(L, L)$, entonces $\alpha_p : \mathtt{Raíz}(p, L) \to \mathtt{Raíz}(p, F)$ es una biyección, para cualquier polinomio $p(X) \in K[X]$.

(iii) Sea $\alpha \in \mathtt{Mono}_K(L, L)$. Entonces α restringe a un automorfismo $\alpha^{\mathrm{alg}} : L^{\mathrm{alg}} \to L^{\mathrm{alg}}$.

Acompañamos este Teorema con un ejemplo, el de determinar el conjunto $\mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C})$. Construimos la lista de monomorfismos mediante varios pasos. Primero consideramos los monomorfismos que fijan $\sqrt[3]{2}$, luego deben de fijar $\mathbb{Q}(\sqrt[3]{2})$. Esto conlleva al subconjunto

$$\mathtt{Mono}_{\mathbb{Q}(\sqrt[3]{2})}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) \;\subseteq\; \mathtt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}).$$

Sabemos que $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \;=\; \mathbb{Q}(\sqrt[3]{2})(\zeta_3)$, y que ζ_3 es una raíz del polinomio ciclotómico $\Phi_3(X) \;=\; X^2 + X + 1 \in \mathbb{Q}(\sqrt[3]{2})$. Por lo tanto, hay dos monomorfismos, id, α_0, fijando $\mathbb{Q}(\sqrt[3]{2})$, donde

$$\alpha_0 : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{pmatrix}$$

Ahora centramos en los monomorfismos que envían $\sqrt[3]{2}$ sobre $\sqrt[3]{2}\zeta_3$. Hay dos de ellos

$$\alpha_1 : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3 \\ \zeta_3 \mapsto \zeta_3 \end{pmatrix} \qquad \alpha_{1'} : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3 \\ \zeta_3 \mapsto \zeta_3^2 \end{pmatrix}$$

Finalmente los que envíen $\sqrt[3]{2}$ sobre $\sqrt[3]{2}\zeta_3^2$. Hay también dos

$$\alpha_2 : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2 \\ \zeta_3 \mapsto \zeta_3 \end{pmatrix} \qquad \alpha_{2'} : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2 \\ \zeta_3 \mapsto \zeta_3^2 \end{pmatrix}$$

En total hay 6 monomorfismos. Aquí también se tiene las igualdades

$$\texttt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) = \texttt{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = \mathbf{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)),$$

esto es un grupo. Uno puede comprobar que

$$|\mathbf{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))| = \left[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}\right] = 6$$

En efecto $\mathbf{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathcal{S}_3$ al grupo simétrico de 3 objetos.

LECCIÓN 13 LA CLAUSURA ALGEBRAICA.

En esta lección abordaremos la clausura algebraica de un cuerpo. Nuestro objetivo es llegar a demostrar el teorema de extensión de monomorfismos con codominio la clausura algebraica del cuerpo base. Pero antes tenemos que comprobar la existencia de la clausura algebraica de un cuerpo, así como sus propiedades universales. Finalizaremos la lección dado un relación de equivalencia entre las raíces de un polinomio con coeficientes en un cuerpo base, a saber la relación de conjugación usando por supuesto los monomorfismo de extensión.

Empezaremos esta lección recordando lo que es una extensión *álgebraicamente cerrada*: Se dice que un subcuerpo K de un cuerpo L es *álgebraicamente cerrado en* L (o que L/K es *álgebraicamente cerrada*), si cualquier elemento algebraico de L sobre K, pertenece a K, es decir $L^{alg} = K$.

Para que el alumno pueda distinguir entre esta nueva definición y las anteriores de la Lección 10, conviene presentar la siguiente torre de cuerpo: Dada cualquier extensión de cuerpos L/K se tiene una torre

$$K \subseteq L^{alg} \subseteq L. \tag{III.1}$$

De allí:

L/K es una extensión *algebraicamente cerrada*, si $K = L^{alg}$ (es decir tenemos la igualdad en el término de la izquierda de la ecuación (III.1)).

L/K es una extensión *algebraica*, si $L^{alg} = L$ (es decir tenemos la igualdad en el término de la derecha de la ecuación (III.1)).

Bajo este punto de vista, tenemos pues dos consecuencias directas:
Sea E/K una extensión de cuerpos. Entonces E^{alg}/K es una extensión algebraica, mientras que E/E^{alg} es una extensión algebraicamente cerrada.

TEOREMA. Sea K un cuerpo. Las siguientes afirmaciones son equivalentes:

(i) Todo polinomio no constante de $K[X]$ se descompone en $K[X]$ como producto de polinomios de grado 1.

(ii) Todo polinomio no constante de $K[X]$ tiene almenos una raíz en K.

(iii) Todo polinomio irreducible de $K[X]$ es de grado 1.

(iv) Toda extensión algebraica de K es de grado 1 (dicho de otra forma, K es algebraicamente cerrado en cualquiera de sus extensiones).

Se dice que un cuerpo K es *algebraicamente cerrado*, si satisface una de las cuatro condiciones del Teorema anterior. Por ejemplo, sabemos que el cuerpo de los números complejos tiene la propiedad de ser *álgebraicamente cerrado*:

TEOREMA (Teorema fundamental del álgebra para $\mathbb{C}$). Cualquier polinomio no constante $p(X) \in \mathbb{C}$ tiene raíces in $\mathbb{C}$. En particular, $p(X)$ admite una factorización de forma:

$$p(X) = c\,(X-u_1)\cdots(X-u_d),$$

donde $c, u_1, \cdots, u_d \in \mathbb{C}$, que es única salvo el orden de las raíces u_i.

Un cuerpo K algebraicamente cerrado *en* E *una extensión de* K, no es necesariamente algebraicamente cerrado. De hecho cualquier cuerpo es algebraicamente cerrado en si mismo (i.e. en la extensión trivial K/K) y existen cuerpos que no son algebraicamente cerrados, por ejemplo $\mathbb{Q}$, $\mathbb{F}_p$, o $\mathbb{R}$.

Sea E/K una extensión de cuerpos y $L/K \leq E/K$ una subextensión, se dice que L *es la clausura algebraica de* K *en* E si L es la extensión algebraica más grande sobre K contenida en E. En general se tiene que

TEOREMA. Sean M un cuerpo algebraicamente cerrado y K un subcuerpo de M. La clausura algebraica de K en M es un cuerpo algebraicamente cerrado.

Le llamaremos la atención del alumno sobre el hecho:

Cualquier cuerpo algebraicamente cerrado es infinito.

TEOREMA (Steinitz). Sean K un cuerpo, E/K una extensión algebraica y M una extensión algebraicamente cerrada de K. Existe un K-homomorfismo de E en M.

Formularemos pues la siguiente pregunta: Dado un cuerpo K,

¿existe algún otro cuerpo álgebraicamente cerrado F, tal que $K \leq F$?

Escogiendo F^{alg} podemos delimitar la pregunta sobre la existencia de aquellos cuerpos que son algebraicos sobre K.

De allí, presentaremos la definición:

Sea K un cuerpo. Se dice que una extensión F/K es *la clausura algebraica de* K si F es, simultáneamente, algebraico sobre K y álgebraicamente cerrado.

Presentaremos al alumno las siguientes propiedades de la clausura algebraica de un cuerpo.

TEOREMA (Steinitz). Sea K un cuerpo.

(i) Existe la clausura algebraica de K.

(ii) Si F_1, F_2 son dos clausuras algebraicas de K. Entonces existe un isomorfismo entre las extensiones F_1/K y F_2/K (notación $F_1 \cong_K F_2$).

Es decir que la clausura algebraica existe y es única salvo isomorfismo.

Denotaremos por $\overline{K}$ o a veces por $K^{\text{alg cl}}$, `la` clausura algebraica de K. En particular tenemos,

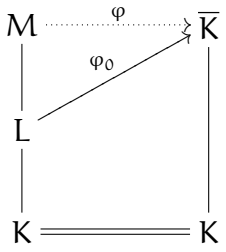
(iii) Si L/K es una extensión algebraica, entonces $\overline{L} \cong_K \overline{K}$ (isomorfismo de extensiones de K).

(iv) Si L/K es una extensión, entonces $\overline{L}/K$ lo es también y $(\overline{L})^{\text{alg}} \cong_K \overline{K}$.

Finalizaremos esta lección relacionando monomorfismos de cuerpos y las extensiones algebraica, dando también la noción de raíces conjugadas.

TEOREMA (De Extensión de Monomorfismo (Steinitz)). Sea M/K una extensión algebraica y $L/K \leq M/K$. Supongamos que $\varphi_0 : L \to \overline{K}$ es un monomorfismo que fija los elementos de K. Entonces existe una extensión de φ_0 a un monomorfismo $\varphi : M \to \overline{K}$.

Es decir se puede completar el siguiente diagrama conmutativo



(las dos columnas son torres de cuerpos).

De momento si $u \in \overline{K}$ y supongamos que $p(X) = \texttt{Polmin}_{K,u}(X) \in K[X]$. Entonces para cualquier otra raíz de $p(X)$, por ejemplo $v \in \overline{K}$, se tiene que existe un monomorfismo $\varphi_v : K(u) \to \overline{K}$ con $\varphi_v(u) = v$. Este se extiende, según el Teorema anterior, a un monomorfismo $\varphi : \overline{K} \to \overline{K}$.

De allí la siguiente definition:
Sea K un cuerpo y $\overline{K}$ su clausura algebraica y consideramos $u, v \in \overline{K}$. Entonces, se dice que v es *conjugado de* u *sobre* K, si existe un monomorfismo $\varphi : \overline{K} \to \overline{K} \in \texttt{Mono}_K(\overline{K}, \overline{K})$ con la propiedad $\varphi(u) = v$. Como consecuencias de la definición se tiene

TEOREMA. Consideramos dos elementos $u, v \in \overline{K}$. Las siguientes afirmaciones son equivalentes:

(i) u y v son conjugados sobre K.

(ii) Existe un K-isomorfismo $\varphi : K(u) \to K(v)$ tal que $\varphi(u) = v$.

(iii) u y v tienen el mismo polinomio minimal sobre K.

En particular, si $u \in \overline{K}$, entonces se tiene la igualdad de conjuntos

$$\texttt{Raíz}(\texttt{Polmin}_{K,u}, \overline{K}) = \texttt{Conj}_{\overline{K}}(u),$$

donde el último es el conjunto de todos los elementos de $\overline{K}$ conjugados de u sobre K.

LECCIÓN 14 LA MULTIPLICIDAD DE RAÍCES Y SEPARABILIDAD.

En esta lección introducimos las extensiones separables de cuerpos. Primero abordaremos las raíces múltiples y sus propiedades, luego definimos lo que es la separabilidad de un polinomio y daremos las consecuencias de esta definición. Introducimos el grado de separabilidad, luego daremos un resultado sobre las extensiones finita separables.

Empezaremos esta lección con la definición de lo que es una *raíz múltiple*, y el *operador derivación*. Luego, le indicaremos al alumno el lema que caracteriza las raíces múltiples: Sea $f(X) \in K[X]$ que tiene una raíz $u \in L$ en alguna extensión L/K. Entonces, u es una raíz múltiple de $f(X)$ si y sólo si $f(X)$ y $f'(X)$ tienen un factor común de grado positivo en $K[X]$ que se anula en u.

Cabe mencionar el siguiente resultado

TEOREMA. Sea K un cuerpo.

(i) Si $f(X) \in K[X]$ es irreducible, entonces un raíz u (en $\overline{K}$) es múltiple si y sólo si $f'(X) = 0$. En particular, esto ocurre solamente cuando $Car(K) > 0$.

(ii) Si $Car(K) = 0$ y $f(X)$ es irreducible en $K[X]$, entonces cualquier raíz de $f(X)$ es simple.

A modo de ejemplo: Para cualquier $n \geq 1$, las raíces de $f(X) = X^n - 1$ en $\mathbb{C}$ son simples. En efecto, tenemos que $f'(X) = nX^{n-1}$, entonces para cualquier raíz ζ de $f(X)$,

$$f'(\zeta) = n\zeta^{n-1} \neq 0.$$

De otra parte, si $L/\mathbb{F}_p$ ($p > 0$ es un primo) es una extensión de cuerpos. Entonces cada raíz de $f(X) = X^p - 1$ en L es múltiple. De hecho 1 es la única raíz!

Pasaremos ahora a la definición importante de esta lección.
Un polinomio irreducible $p(X) \in K[X]$ se dice que es *separable sobre* K si cualquier raíz de $p(X)$ en la extensión L/K es simple. Esto es equivalente, según el resultado anterior, a que $p'(X) = 0$. Si $u \in L$ es raíz múltiple de $p(X)$, entonces *la multiplicidad de* u *en* $p(X)$ es el número máximo m tal que $p(X) = (X-u)^m q(X)$, para algún $q(X) \in L[X]$.

TEOREMA (De Polinomios Separables). Sea K un cuerpo y $\overline{K}$ su clausura algebraica.

(i) Si un polinomio irreducible $p(X) \in K[X]$ tiene distintas raíces $u_1, \cdots, u_k \in \overline{K}$, entonces las multiplicidades de los u_j son iguales. Luego,

$$p(X) = c(X-u_1)^m \cdots (X-u_k)^m \in \overline{K}[X],$$

donde $c \in K$ y $m \geq 1$.
En particular, si son todas simples, entonces

$$p(X) = c(X-u_1) \cdots (X-u_k) \in \overline{K}[X],$$

donde $c \in K$ y $k = \mathrm{grado}(p(X))$.

(ii) Si $u \in \overline{K}$, entonces el número de conjugados de u es

$$\frac{\mathrm{grado}\left(\mathtt{Polmin}_{K,u}(X)\right)}{m}$$

donde m es la multiplicidad de u en $\mathtt{Polmin}_{K,u}(X)$.

Un elemento algebraico $u \in L$ en una extensión L/K se dice que es *separable sobre* K, si su polinomio minimal $\mathtt{Polmin}_{K,u}(X) \in K[X]$ es separable.
Una extensión algebraica L/K se dice que es *una extensión separable* si cualquier elemento de L es separable sobre K.
Una extensión algebraica L/K de cuerpos de característica 0 es siempre una

extensión separable.

Sea L/K una extensión finita. El *grado de separabilidad de* L *sobre* K es por definición

$$(L : K) := |\mathtt{Mono}_K(L, \overline{K})|.$$

Es decir el número de monomorfismos de la extensión $\overline{K}/L$ sobre K.
Para una extensión finita simple $K(u)/K$, se tiene que

$$(K(u) : K) = |\mathtt{Raíz}(\mathtt{Polmin}_{K,u}, \overline{K})|.$$

Si $K(u)/K$ es separable, entonces $\left[K(u) : K\right] = (K(u) : K)$.

Como ya se ha venido observando, una extensión finita L/K viene construida a partir de sucesiones de extensiones simples

$$K(u_1)/K,\ K(u_1, u_2)/K(u_1), \cdots, K(u_1, \cdots, u_k)/K(u_1, \cdots, u_{k-1}) = L. \qquad \text{(III.2)}$$

El siguiente resultado sirve entre otras cosa para calcular el grado $(K(u_1, \cdots, u_k) : K)$.

TEOREMA (De extensiones separables finitas). Sean L/K y M/L dos extensiones finitas. Entonces

(i) $(M : K) = (M : L)\,(L : K)$.

(ii) $(L : K) \mid \left[L : K\right]$.

(iii) L/K es separable si y sólo si $(L : K) = \left[L : K\right]$.

(iv) M/K es separable si y sólo si L/K y M/L son separables.

LECCIÓN 15 EL TEOREMA DEL ELEMENTO PRIMITIVO.

Esta lección la dedicaremos a comprobar el teorema del elemento primitivo. Como aplicación daremos ejemplos concretos. Antes de enunciar dicho Teorema, empezaremos la lección recordando lo al alumno la definición de lo que ese elemento.

Sea L/K una extensión simple. Recuede que un elemento $u \in L$ se llama *un elemento primitivo para la extensión* L/K, si se tiene que $L = K(u)$.

TEOREMA (Teorema del Elemento Primitivo). Sea L/K una extensión de cuerpos. Las siguientes afirmaciones son equivalentes:

1. L posee un elemento primitivo;
2. el retículo de los cuerpos intermediarios de L/K es finito.

Esta condiciones se satisfacen cuando L/K es una extensión separable finita. En particular, si L/K es una extensión finita de cuerpos con característica 0, entonces L tiene un elemento primitivo.

Conviene dar ejemplos de busqueda de elementos primitivos. Cabe explicarle al alumno que para encontrar un elemento primitivo uno puede guiarse con la demostración del Teorema anterior, sin embargo, el método "Observa luego comprueba" es a veces suficiente. A modo de ejemplo en ese sentido presentaremos la busqueda de un elemento primitivo en la extensión $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$: Consideramos $\sqrt{3} + i$. Entonces tarabajando con la extensión $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3}, i)$, encontraremos que $i \notin \mathbb{Q}(\sqrt{3}) \leq \mathbb{R}$ y

$$\left(X - (\sqrt{3} + i)\right)\left(X - (\sqrt{3} - i)\right) \;=\; X^2 - 2\sqrt{3}X + 4 \in \mathbb{Q}(\sqrt{3})[X].$$

Luego

$$X^2 - 2\sqrt{3}X + 4 \;=\; \texttt{Polmin}_{\mathbb{Q}(\sqrt{3}),\, \sqrt{3}+i}(X).$$

De otra parte

$$\left(X^2 - 2\sqrt{3}X + 4\right)\left(X^2 + 2\sqrt{3}X + 4\right) \;=\; X^4 - 4X^2 + 16 \in \mathbb{Q}[X],$$

es decir que $\texttt{Polmin}_{\mathbb{Q}(\sqrt{3}),\,\sqrt{3}+i}(X) \,|\, (X^4 - 4X^2 + 16) \in \mathbb{Q}[X]$. Dado que

$$(\sqrt{3} - i) \;=\; 4(\sqrt{3} + i)^{-1} \in \mathbb{Q}(\sqrt{3} + i),$$

se tiene que

$$\sqrt{3} \;=\; \frac{1}{2}\left((\sqrt{3} + i) + (\sqrt{3} - i)\right), \quad i \;=\; \frac{1}{2}\left((\sqrt{3} + i) - (\sqrt{3} - i)\right) \in \mathbb{Q}(\sqrt{3} + i).$$

Luego $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3} + i)$ y $\mathbb{Q}(i) \leq \mathbb{Q}(\sqrt{3} + i)$, así $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3} + i)$. Es decir debemos de tener que $\texttt{grado}(\texttt{Polmin}_{\mathbb{Q},\,\sqrt{3}+i}) = 4$, de allí $\texttt{Polmin}_{\mathbb{Q},\,\sqrt{3}+i}(X) = X^4 - 4X^2 + 16$. Por lo tanto $\sqrt{3} + i$ es un elemento primitivo en $\mathbb{Q}(\sqrt{3}, i)$.
Cabe mencionar que hay un fenómeno general ilustrado por el Ejemplo anterior: Antes hay que recordare de la Lección 14 lo que es un elemento separable.

TEOREMA. Sea $u \in \overline{K}$ un elemento separable sobre K. Entonces,

$$\texttt{Polmin}_{K,u}(X) \;=\; (X - \alpha_1(u)) \cdots (X - \alpha_d(u)),$$

donde $\alpha_1, \cdots, \alpha_d$ son los elementos de $\texttt{Mono}_K(K(u), \overline{K})$. En particular, el polinomio

$$(X - \alpha_1(u)) \cdots (X - \alpha_d(u)) \;\in \overline{K}[X]$$

tiene coeficientes en K, y es irreducible en $K[X]$.

Volviendo al ejemplo de la extensión $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$, se tiene que

$$\left[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}\right] \;=\; \left[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})\right]\left[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\right] \;=\; 2{,}2 \;=\; 4.$$

Luego, hay cuatro monomorfismos $\alpha_k : \mathbb{Q}(\sqrt{3}, i) \to \mathbb{Q}(\sqrt{3}, i)$ dados por

$$\alpha_1 = \mathrm{id}, \quad \alpha_2 = \begin{pmatrix} \sqrt{3} \mapsto \sqrt{3} \\ i \mapsto -i \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{3} \mapsto -\sqrt{3} \\ i \mapsto i \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{3} \mapsto -\sqrt{3} \\ i \mapsto -i \end{pmatrix}.$$

Entonces

$$\alpha_2(\sqrt{3} + i) = (\sqrt{3} - i), \quad \alpha_3(\sqrt{3} + i) = (-\sqrt{3} + i), \quad \alpha_4(\sqrt{3} + i) = (-\sqrt{3} - i),$$

y luego

$$\left(X-\sqrt{3}-i\right)\left(X-\sqrt{3}+i\right)\left(X+\sqrt{3}-i\right)\left(X+\sqrt{3}+i\right) = X^4-4X^2+16 \in \mathbb{Q}[X].$$

Por lo tanto este polinomio es irreducible en $\mathbb{Q}[X]$, y tenemos que $\left[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}\right] = 4$ y $\mathbb{Q}(\sqrt{3},i) = \mathbb{Q}(\sqrt{3}+i)$.

Lección 16 Extensión Normal y cuerpos de descomposición.

Introducimos en esta lección las extensiones normales de cuerpos, así como el cuerpo de descomposición de un polinomio prefijado. Finalizaremos la lección dando, en el caso finito, una relación entre ambas nociones.

Empezaremos la lección con el siguiente resultado, que es un acompañante del Teorema de Extensión de monomorfismo (el Teorema de Steinitz) de la Lección 13.

Teorema. Sea $\overline{K}$ la clausura algebraica de un cuerpo K y sea $E/K \leq \overline{K}/K$ una subextensión finita. Consideramos $\varphi : E \to \overline{K}$ un K-homomorfismo de extensiones.

(i) Si $\varphi \in \mathrm{Mono}_K(E, \overline{K})$, entonces $\varphi(E) = E$ si y sólo si $\varphi(E) \leq E$.

(ii) Existe un K-automorfismo de $\overline{K}$, cuya restricción a E es φ.

Podemos pues hablar de la relación de conjugación entre extensiones de K dentro de su clausura algebraica $\overline{K}$. Es decir, sean E, E' dos extensiones de K con $E/K, E'/K \leq \overline{K}/K$, se dice E *en conjugado de* E' *sobre* K, si existe un K-automorfismo $\psi \in \mathrm{Aut}_K(\overline{K})$ tal que $\psi(E) = E'$.

De allí presentaremos la siguiente definición:

Una extensión E/K, se dice que es una *extensión normal* si $\varphi(E) = E$ para cualquier elemento $\varphi \in \mathrm{Mono}_K(E, \overline{K})$.

Observaremos que si dada una extensión normal E/K, entonces cada polinomio irreducible $p(X) \in K[X]$ que tiene raíz en E, escinde en E, como ya se sabe de la lección 12 que dos raíces son conjugadas sobre K y una de elles es la

imagen de la otra mediante un monomorfismo $\overline{K} \to \overline{K}$ cuya restricción sobre E tiene imagen en E.

Agruparemos estas observaciones y otras más en el siguiente enunciado.

TEOREMA (De extensiones "quasi"-Galois). Sea K un cuerpo y $E/K \leq \overline{K}/K$ una subextensión. Las siguientes afirmaciones son equivalente.

(i) E/K es una extensión normal.

(ii) Para cualquier elemento $u \in E$, $\mathtt{Conj}_{\overline{K}}(u) \subseteq E$ (los conjugados de u sobre K en $\overline{K}$, pertenecen a E).

(iii) Cualquier polinomio irreducible de $K[X]$ que tenga una raiz en E, se descompone en producto de polinomio de grado 1 (distintos o no) en $E[X]$.

(iv) E se identifica con cualquiera de sus conjugados.

(v) E es el cuerpo de descomposición en $\overline{K}$ de una familia de polinomios $\{f_i\}_{i\in I}$ no constantes en $K[X]$.

En particular, se tiene

TEOREMA. Sea K un cuerpo. Una extensión finita de cuerpos E/K es normal si y sólo si es un cuerpo de descomposición sobre K para algún polinomios $f(X) \in K[X]$.

Esto nos permite detectar las extensiones normales finita usando los cuerpos de descomposición sobre K de algunos polinomio. En el próximo Tema vamos a ver las extensiones normal separables, que van a jugar un papel central en la Teoría de Galois, de hecho estas son las conocidas como *extensiones de Galois*.

BIBLIOGRAFÍA

[1] E. Artin. *Galois Theory*. Number 2 in Note Dame Mathematical Lectures. 1944.

[2] M. Artin. *Algebra*. Prentice Hall inc. 1991.

[3] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7*. Springer-Verlag, New York Berlin Heidelberg, 1990.

[4] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 5 á 7*. Springer-Verlag, Berlin Heidelberg, 2007.

[5] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[6] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, 1985.

Tema IV

Extensiones de Galois y la correspondencia de Galois.

Lecciones

El presente tema contiene la parte principal de este curso: Las extensiones de Galois y el teorema de correspondencia de Galois. Los temas anteriores III y II han de servir de base para introducir las extensiones de Galois finitas. Esto lo haremos en la primera lección junto con la definición del grupo de Galois, así como la relación entre los automorfismos de la extensión de la clausura algebraica (o cualquier extensión normal finita) y los elementos del grupo de Galois. Las propiedades de ese grupo las estudiaremos en la siguiente lección, donde demostraremos entre otra cosas, que la acción del grupo de Galois sobre el conjunto de las raíces de un polinomio adecuado, es fielmente transitiva. Daremos varios ejemplos donde se aplica esta situación calculando de manera efectiva dicho grupo.

Antes de presentarle al alumno el teorema de la correspondencia de Galois, hablaremos sobre los subgrupos del grupo de Galois y los subcuerpos de elementos invariantes. Así daremos la relación entre el orden de un subgrupo de Galois y el grado de la extensión del cuerpo invariante asociado. De paso dedicaremos una lección propia para a la demostración del teorema de la base normal para las extensiones de Galois finitas. Estudiaremos en una lección aparte los grupos de Galois relativos. De esta manera llegaremos a la correspondencia de Galois que establece una biyección entre el conjunto de subgrupos del grupo de Galois y el conjunto de las subextensiones de la extensión de Galois asociada. Así pues los subgrupos normales corresponden a las subextensiones normales. Daremos detalladamente un ejemplo de aplicación, como el caso de las extensión de Galois dentro de los números complejos que le dedicaremos una lección aparte.

Finalizaremos el tema con otras dos aplicaciones, que en nuestro punto de vista, son importante. A saber la primera trata la cuestión de cuando un grupo de Galois se identifica con el grupo alternado, es decir con las permutaciones pares y la segunda trata el teorema de Kaplansky sobre el grupos de Galois asociados a polinomios racionales monoico de grado cuatro.

LECCIÓN 17 EXTENSIONES DE GALOIS.

Antes de dar la definición de una extensión de Galois, le recordaremos al alumno las definiciones de extensiones normales y separables introducidas, respectivamente, en las lecciones 16 y 14. Luego pasaremos a la demostración del siguiente resultado

TEOREMA. Sea E/K una extensión algebraica de cuerpos y $\Gamma = \mathrm{Aut}_K(E)$ el grupo de K-automorfismos asociado. Entonces las siguientes afirmaciones son equivalentes:

(i) Cualquier elemento Γ-invariante de E, pertenece a K, i.e. $E^\Gamma = K$.

(ii) E/K es una extensión separable y normal.

(iii) El polinomio minimal de cualquier elemento $u \in E$ sobre K, se descompone en $E[X]$ como producto de polinomios distintos cada uno de grado 1.

Un extensión de cuerpos E/K finita, se dice que es una *extensión de Galois (finita)* si es una extensión separable y normal, es decir satisface una de las equivalentes condiciones del teorema anterior.

Se sabe del tema anterior, que en una extensión de Galois E/K, se tiene que $\left[E : K\right] = (E : K)$, y que cualquier monomorfismo $\varphi \in \mathtt{Mono}_K(E, \overline{K})$ envía E en E, luego su restricción $\varphi_{|E}$ define un elemento del grupo de automorfismos $\mathrm{Aut}_K(E)$.

De otra parte, según el Teorema (De Extensión de Monomorfismos) Lección 13, se tiene que cualquier automorfismo $\alpha \in \mathrm{Aut}_K(E)$ extiende a un monomorfismo $E \to \overline{K}$ fijando los elementos de K. De esa manera, existe una biyección

$$\mathtt{Mono}_K(E, \overline{K}) \simeq \mathrm{Aut}_K(E), \quad \text{con } |\mathrm{Aut}_K(E)| = \left[E : K\right] = (E : K). \tag{IV.1}$$

Luego pasaremos a definir el grupo de Galois y explicar sus relaciones con otros grupos de automorfismos.
Para una extensión de Galois E/K, el grupo

$$\mathtt{Gal}(E/K) := \mathrm{Aut}_K(E),$$

se llama *el grupo de Galois de* E *sobre* K. Los elementos de $\mathtt{Gal}(E/K)$ se le llama los *automorfismos de Galois* de E/K.

La ecuación (IV.1), implica que $|\mathtt{Gal}(E/K)| = \left[E : K\right] = (E : K)$. La noción de conjugación definida en la lecciones 13 y 14 , tiene una forma especial en el caso de extensiones de Galois.

Sea E/K una extensión de Galois finita y $v, u \in E$. Entonces v *es conjugado a* u, si existe un elemento $\varphi \in \mathtt{Gal}(E/K)$ tal que $v = \varphi(u)$; decimos también que v es *un conjugado de* u.

TEOREMA (Extensión de Galois). Si E/K es una extensión de Galois finita, entonces la aplicación

$$\mathrm{Aut}_K(\overline{K}) \longrightarrow \mathrm{Aut}_K(E) = \mathtt{Gal}(E/K), \qquad \left(\varphi \longmapsto \varphi_{|E}\right)$$

es morfismo de grupos suprayectivo.
Si $F/K \leq \overline{K}/K$ es cualquier subextensión finita normal con $E \leq F$, entonces existe un morfismo de grupos suprayectivo

$$\mathrm{Aut}_K(F) \longrightarrow \mathrm{Aut}_K(E) = \mathtt{Gal}(E/K), \qquad \left(\theta \longmapsto \theta_E^F\right).$$

Además, para $\varphi \in \mathrm{Aut}_K(\overline{K})$, tenemos que

$$(\varphi_{|E})_E^F = \varphi_{|E}.$$

LECCIÓN 18 GRUPOS DE GALOIS.

Antes de abordar con detalles las propiedades del grupo de Galois, explicaremos los siguientes hechos con algunos ejemplos.
Sea E/K una extensión de Galois finita. Sabemos pues que E es un cuerpo escisión para algún polinomio sobre K, dado que E/K es normal. Además, como E/K es separable, el Teorema del elemento primitivo, no dice que E es un extensión simple de K. Luego, E es un cuerpo escisión de cualquiera de los polinomios minimales de los elementos primitivos de E/K, estos tienen todos el mismo grado $\left[E : K\right]$. Es conveniente pues usar esto para interpretar los elementos de $\mathtt{Gal}(E/K)$ como permutaciones de las raíces de un polinomio que escinde sobre E.

A modo de ejemplo, describimos los elementos de $\mathtt{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ como subgrupo de permutaciones de las raíces del polinomio $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$. Sabemos que

$$\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right]\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 4.$$

y que los elementos de $\mathtt{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ son $\alpha_1 = \mathrm{id}$,

$$\alpha_2 = \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ -\sqrt{3} \mapsto -\sqrt{3} \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ -\sqrt{3} \mapsto \sqrt{3} \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ -\sqrt{3} \mapsto \sqrt{3} \end{pmatrix}.$$

Escribiendo las raíces en lista de forma $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$, y nombrarlos $1, 2, 3, 4,$. Esos automorfismos, se corresponden a las siguientes permutaciones:

$$\alpha_2 \mapsto (1\,2), \quad \alpha_4 \mapsto (3\,4), \quad \alpha_4 \mapsto (1\,2)(3\,4).$$

Utilizaremos un elemento primitivo u de la extensión bajo consideración para describir el grupo $\mathtt{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ como un subgrupo del grupo de las permutaciones de las raíces del polinomio $\mathtt{Polmin}_{\mathbb{Q},u}(X)$. Se sabe que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) =$

$\mathbb{Q}(\sqrt{2},\sqrt{3})$, y los conjugados de $u = \sqrt{2}+\sqrt{3}$ son $\pm\sqrt{2}\pm\sqrt{3}$, que viene dados en forma de la siguiente lista

$$\sqrt{2}+\sqrt{3}, \quad \sqrt{2}-\sqrt{3}, \quad -\sqrt{2}+\sqrt{3}, \quad -\sqrt{2}-\sqrt{3}.$$

Después de nombrarlos tal como vienen, tenemos la correspondencia

$$\alpha_2 \leftrightarrow (1\,3)(2\,4), \quad \alpha_3 \leftrightarrow (1\,2)(3\,4), \quad \alpha_2 \leftrightarrow (1\,4)(2\,3).$$

El resto de esta lección lo dedicamos a recordar todas la propiedades del grupo de Galois que ya se han visto hasta el momento, así como algunos ejemplos de grupos de Galois. Recordaremos que para una extensión cualquiera F/K, y un polinomio $f(X) \in K[X]$, $\mathtt{Raíz}(f, F)$ denota el conjunto de todas las raíces de $f(X)$ en F.

TEOREMA. Sea E/K una extensión de Galois finita. Supongamos que E es un cuerpo escisión de un polinomio separable irreducible $f(X) \in K[X]$ de grado n. Entonces ocurre lo siguiente.

(i) $\mathtt{Gal}(E/K)$ actúa transitiva y fielmente sobre $\mathtt{Raíz}(f, E)$.

(ii) $\mathtt{Gal}(E/K)$ se identifica con un subgrupo del grupo de las permutaciones de $\mathtt{Raíz}(f, E)$.
De hecho si ordenamos las raíces de $f(X)$ como, $u_1, \cdots, u_n$, entonces $\mathtt{Gal}(E/K)$ se identifica con un subgrupo de $\mathcal{S}_n$.

(iii) El orden de $\mathtt{Gal}(E/K)$, $|\mathtt{Gal}(E/K)|$ divide $n!$ y es divisible por n.

La extensión de Galois $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ tiene grado $\left[\mathbb{Q}(\zeta_8):\mathbb{Q}\right] = 4$ y tiene, aparte de la identidad, los siguientes automorfismos:

$$\alpha : \zeta_8 \mapsto \zeta_8^3, \quad \beta : \zeta_8 \mapsto \zeta_8^5, \quad \gamma : \zeta_8 \mapsto \zeta_8^7.$$

Si ponemos en lista las raíces del polinomio minimal

$$\mathtt{Polmin}_{\mathbb{Q},\zeta_8,} \;=\; \Phi_8(X) \;=\; X^4+1,$$

en el orden $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$, encontramos que estos automorfismos corresponden a las siguiente permutaciones en $\mathcal{S}_4$

$$\alpha \leftrightarrow (1\,2)(3\,4), \quad \beta \leftrightarrow (1\,3)(2\,4), \quad \gamma \leftrightarrow (1\,4)(2\,3).$$

De es manera $\mathtt{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ corresponde a

$$\Big\{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\Big\} \leq \mathcal{S}_4.$$

Ahora veamos que

$$\zeta_8 \;=\; \sqrt{2}^{-1}(1+\mathrm{i}),$$

podemos encontrar que $\sqrt{2}, \mathrm{i} \in \mathbb{Q}(\zeta_8)$, luego $\mathbb{Q}(\sqrt{2}, \mathrm{i}) \leq \mathbb{Q}(\zeta_8)$, como $\Big[\mathbb{Q}(\sqrt{2}, \mathrm{i}) : \mathbb{Q}\Big] = 4$, se tiene la igualdad entre $\mathbb{Q}(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\zeta_8)$. Notemos que $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ es la escisión del polinomio $f(X) = (X^2-2)(X^2+1)$ sobre $\mathbb{Q}$. Ahora ponemos la lista de raíces, $\sqrt{2}, -\sqrt{2}, \mathrm{i}, -\mathrm{i}$, podemos observar que

$$\alpha : \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ \mathrm{i} \mapsto -\mathrm{i} \\ -\mathrm{i} \mapsto \mathrm{i} \end{pmatrix} \leftrightarrow (1\,2)(3\,4), \;\; \beta : \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ \mathrm{i} \mapsto \mathrm{i} \\ -\mathrm{i} \mapsto \mathrm{i} \end{pmatrix} \leftrightarrow (1\,2), \;\; \gamma : \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ \mathrm{i} \mapsto -\mathrm{i} \\ -\mathrm{i} \mapsto \mathrm{i} \end{pmatrix} \leftrightarrow (3\,4).$$

Así $\mathtt{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ corresponde al subgrupo

$$\Big\{\mathrm{id}, (1\,2), (3\,4), (1\,2)(3\,4)\Big\} \leq \mathcal{S}_4.$$

La determinación del grupo de Galois de una extensión resulta una tarea difícil. Sin embargo, algunos argumentos especiales puedan a veces explorarlos.

Supongamos que $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ es un polinomio irreducible cúbico y que $f(X)$ tiene solamente un raíz real. Entonces $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathcal{S}_3$.

Sea $u_1 \in \mathbb{R}$ la raíz real de $f(X)$ y u_2, u_3 las otras complejas. Entonces $\mathbb{Q}(f(X)) = \mathbb{Q}(u_1, u_2, u_3)$ y de hecho $\Big[\mathbb{Q}(f(X)) : \mathbb{Q}\Big] = 6$, dado que $\Big[\mathbb{Q}(f(X)) : \mathbb{Q}\Big] \,|\, 6 = 3!$ y que

$u_2 \notin \mathbb{Q}(u_1) \leq \mathbb{R}$. Luego $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q})$ es isomorfo a un subgrupo de $\mathcal{S}_3$, y luego $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathcal{S}_3$, por tener el mismo orden.

Tal situación se aplica a cualquier polinomio cúbico $f(X)$ que tiene máximales y minimales locales en valores reales c_-, c_+ con $f(c_+), f(c_-) > 0$ o $f(c_+), f(c_-) < 0$. Por ejemplo la cúbica $f(X) = X^3 - 3X + 3$ que tiene extremos locales en ± 1, y $f(-1) = 1$, $f(-1) = 5$.

LECCIÓN 19 SUBGRUPOS DEL GRUPO DE GALOIS Y SUS CUERPOS DE INVARIANTES.

En esta lección nos interesamos a estudiar las subextensiones de una extensión de Galois en relación con los subgrupos del grupo de Galois.

Sea E/K una extensión de Galois y supongamos que $\Gamma \leq \mathtt{Gal}(E/K)$. Consideramos el subconjunto de E de elementos fijados por Γ,

$$E^{\Gamma} = \left\{ u \in E \mid \forall \gamma \in \Gamma, \gamma(u) = u \right\}.$$

Es fácil comprobar que $E^{\Gamma} \leq E$ es un subcuerpo de E que contiene a K.

El subcuerpo E^{Γ} se le llama *el subcuerpo de invariantes de* Γ (o *el subcuerpo fijado por* Γ). Según la lección 14 precisamente el Teorema de las extensión separables finitas, sabemos que E^{Γ}/K y E/E^{Γ} son extensiones separables. E/E^{Γ} es también normal, entonces es una extensión de Galois; veamos cuales su grupo de Galois. Observe que

$$\left[E : E^{\Gamma}\right] = (E : E^{\Gamma}) = |\mathtt{Gal}(E/E^{\Gamma})|.$$

Ahora cualquier elemento de $\mathtt{Gal}(E/E^{\Gamma})$ es también un elemento de $\mathtt{Gal}(E/K)$. Luego $\mathtt{Gal}(E/E^{\Gamma}) \leq \mathtt{Gal}(E/K)$. Notemos que por definición $\Gamma \leq \mathtt{Gal}(E/K)$, así por el Teorema de Lagrange se tiene que $\Gamma|$ divide a $|\mathtt{Gal}(E/E^{\Gamma})|$. De hecho tenemos

TEOREMA. Sea E/K una extensión de Galois finita. Para un subgrupo $\Gamma \leq \mathtt{Gal}(E/K)$, se tiene que $\Gamma = \mathtt{Gal}(E/E^{\Gamma})$ junto con la ecuaciones

$$\left[E : E^{\Gamma}\right] = |\mathtt{Gal}(E/E^{\Gamma})| = |\Gamma|, \quad \left[E^{\Gamma} : K\right] = \frac{|\mathtt{Gal}(E/E^{\Gamma})|}{|\Gamma|}.$$

LECCIÓN 20 EL TEOREMA DE LA BASE NORMAL.

En esta lección enunciaremos con demostración el teorema de la base normal de una extensión de Galois finita. Se trata de una base formada por un elemento primitivo de la extensión y todos sus conjugados con respecto del grupo de Galois asociado. El enunciado, así como la demostración, lo haremos en dos parte, primero para el caso en que el cuerpo base es finito, luego para el caso infinito.

Empezaremos la lección con la siguiente observación. Dada una extensión de Galois finita E/K de grado n, sabemos de la Lección 19, que $\mathtt{Gal}(E/K)$ es finito de orden n. Así es natural de preguntar si existe un elemento $u \in E$, tal que el conjunto $\{\alpha(u) | \ \alpha \in \mathtt{Gal}(E/K)\}$ de los conjugados de u, es una base de E como K-espacio vectorial. De hecho, vamos demostrar que esto es siempre cierto.

Un conjunto de elementos $\{u_1, \cdots .u_n\}$ de E se dice *que es una base normal de la extensión de Galois finita* E/K si

$$u_i \ = \ \alpha_i(u), \quad \text{para cierto elemento } u \in E,$$

donde $\mathtt{Gal}(E/K) = \{\alpha_1, \cdots, \alpha_n\}$.

Enunciaremos pues el primer caso, cuya demostración se basa sobre el lema de independencia lineal de caracteres de la Lección 9 (ó la Lección 31 más adelante)

> TEOREMA. Sea E/K una extensión de Galois finita. Supongamos que $\mathtt{Gal}(E/K)$ es cíclico. Entonces E tiene una base normal.
> En particular si K es un cuerpo finito, E tiene una base normal.

Ahora podemos enunciar y comprobar, usando para el caso K infinito el último Teorema de Lección 9 sobre la independencia algebraica, el siguiente resultado

TEOREMA (De la base Normal). Sea E/K una extensión de Galois finita. Entonces E tiene una base normal.

LECCIÓN 21 EL GRUPO DE GALOIS RELATIVO.

Esta lección la dedicaremos exclusivamente a la introducción y las propiedades básica del grupo de Galois relativo.
Sea E/K una extensión de Galois y supongamos que $L/K \leq E/K$ (i.e. $K \leq L \leq E$). Entonces, E/L es una extensión de Galois también, cuyo grupo de Galois $\mathtt{Gal}(E/L)$ es a veces llamado *el grupo de Galois relativo de la subextensión* $L/K \leq E/K$. El siguiente lema es inmediato

El grupo de Galois relativo de la subextensión $L/K \leq E/K$ es un subgrupo de $\mathtt{Gal}(E/K)$. E decir que

$$\mathtt{Gal}(E/L) \leq \mathtt{Gal}(E/K), \quad \text{y } |\mathtt{Gal}(E/L)| = \Big[E : L\Big].$$

Sea E/K una extensión de Galois y $L/K \leq E/K$ una subextensión. Entonces, $L = E^{\mathtt{Gal}(E/L)}$.

Una pregunta natural es cuando $\mathtt{Gal}(E/L)$ es un subgrupo normal de $\mathtt{Gal}(E/K)$. El siguiente resultado explica la conexión entre dos manera del uso de la palabra *normal*, que ambas viene derivadas de hecho de la Teoría de Galois.

TEOREMA (Grupo de Galois Relativo). Sea E/K una extensión de Galois finita y $L/K \leq E/K$.

(i) El grupo de Galois relativo $\mathtt{Gal}(E/L)$ de la subextensión $L/K \leq E/K$, es un subgrupo normal de $\mathtt{Gal}(E/K)$ si y sólo si L/K es un extensión normal.

(ii) Si L/K es una extensión normal y luego de Galois, entonces existe un isomorfismo de grupos

$$\mathtt{Gal}(E/K)/\mathtt{Gal}(E/L) \xrightarrow{\cong} \mathtt{Gal}(L/K) \qquad \Big(\alpha\mathtt{Gal}(E/L) \longmapsto \alpha_{|_L}\Big).$$

LECCIÓN 22 LA CORRESPONDENCIA DE GALOIS.

Estamos ahora preparados para enunciar el Teorema de correspondencia de Galois para extensiones de Galois finitas. Vamos a emplear la siguiente notación: Sea E/K una extensión de Galois finita, consideramos

$$\begin{aligned} \mathcal{S}(E/K) &= \text{el conjunto de todos los subgrupos de } \mathtt{Gal}(E/K); \\ \mathcal{F}(E/K) &= \text{el conjunto de todas la subextensiones de } E/K. \end{aligned}$$

Son dos conjunto parcialmente ordenados, por la inclusión. Dado que cada subgrupo de un grupo finito es finito, así como cada subconjunto de un conjunto finito es finito, podemos definir las siguientes aplicaciones:

$$\begin{aligned} &\Phi_{E/K} : \mathcal{F}(E/K) \longrightarrow \mathcal{S}(E/K), \qquad \Phi_{E/K}(L) = \mathtt{Gal}(E/L); \\ &\Theta_{E/K} : \mathcal{S}(E/K) \longrightarrow \mathcal{F}(E/K), \qquad \Theta_{E/K}(\Gamma) = E^{\Gamma}. \end{aligned}$$

TEOREMA (Teorema Principal de Galois). Sea E/K una extensión de Galois finita. Entonces, las aplicaciones $\Phi_{E/K}$ y $\Theta_{E/K}$ establecen una biyección mutuamente inversas y ambas preservan el orden

$$\mathcal{F}(E/K) \underset{\Theta_{E/K}}{\overset{\Phi_{E/K}}{\rightleftarrows}} \mathcal{S}(E/K).$$

Bajo esta biyección las subextensiones normal corresponden a los subgrupos normales.

Una consecuencia inmediata del Teorema Principal de Galois es el siguiente: Sea E/K una extensión de Galois finita, Entonces, existe un número finito de subextensiones $L/K \leq E/K$.

Una vez determinadas las subextensiones de una extensión de Galois finita, la representaremos en forma de diagrama indicando el orden de menor a mayor (de abajo a arriba) en forma de lineas (i.e. un diagrama de Hasse) con peso que indica el grado de la subextensión. Lo mismo hacemos con los subgrupos del

grupo de Galois de la misma extensión, con el peso de cada linea sería el índice del subgrupo. Usando la correspondencia de Galois, veamos que un diagrama es el inverso (o "dual") del otro.

Ya hemos explicado al alumno, que la extensión $\mathtt{E} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ es una extensión de Galois, cuyo grupo de Galois es isomorfo a $\mathcal{S}_3$. Vamos a detallar esto isomorfismo. Las tres raíces del polinomio X^3-2 que tienen a $\mathtt{E}$ como cuerpo de escisión sobre $\mathbb{Q}$, son $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$, que podemos nombrar en el orden que vienen. Entonces, los monomorfismos, $\mathrm{id}, \alpha_0, \alpha_1, \alpha_1', \alpha_2, \alpha_2'$ se extienden a automorfismos de $\mathtt{E}$, cada uno de ellos permuta las tres raíces de la siguiente manera:

$$\alpha_0 = (2\,3), \quad \alpha_1 = (1\,2\,3), \quad \alpha_1' = (1\,2), \quad \alpha_2 = (1\,3\,2), \quad \alpha_2' = (1\,3).$$

La correspondencia de Galois nos conduce al diagrama de la Figura IV.1. Se encuentra pues que

$$\mathtt{Gal}(\mathtt{E}/\mathbb{Q}(\zeta_3)) = \{\mathrm{id}, \alpha_1, \alpha_2\} \cong \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}, \ \mathtt{Gal}(\mathtt{E}/\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}, \alpha_0\} \cong \{\mathrm{id}, (2\,3)\},$$
$$\mathtt{Gal}(\mathtt{E}/\mathbb{Q}(\sqrt[3]{2}\zeta_3)) = \{\mathrm{id}, \alpha_2'\} \cong \{\mathrm{id}, (1\,3)\}, \ \mathtt{Gal}(\mathtt{E}/\mathbb{Q}(\sqrt[3]{2}\zeta_3^2)) = \{\mathrm{id}, \alpha_1'\} \cong \{\mathrm{id}, (1\,2)\}.$$

Observamos que $\{\mathrm{id}, (1\,2\,3), (1\,3\,2)\} \lhd \mathcal{S}_3$, luego $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ es una extensión normal. Por supuesto $\mathbb{Q}(\zeta_3)$ es una escisión de $X^3 - 1$ sobre $\mathbb{Q}$.

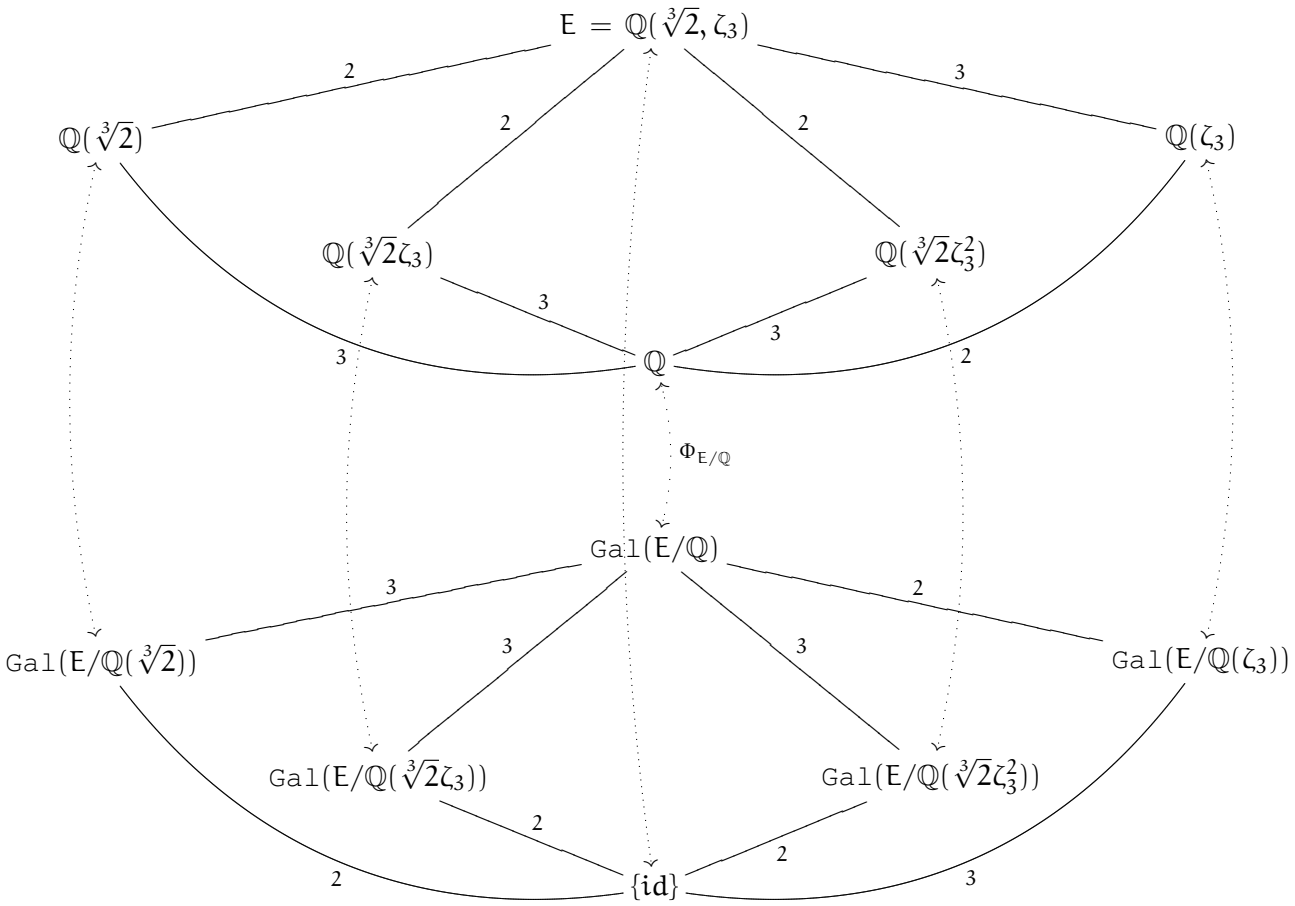


Figura IV.1: La correspondencia de Galois de la extensión $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

LECCIÓN 23 EXTENSIONES DE GALOIS DENTRO DE LOS COMPLEJOS.

Esta lección es un aplicación directa de las nociones adquiridas por al alumno en las lección anteriores. Se trata de hacer le visible las extensiones de Galois dentro de los números complejos.
Sea $E/\mathbb{Q}$ un extensión de Galois finita con $E/\mathbb{Q} \leq \mathbb{C}/\mathbb{Q}$. Denotaremos por $E_{\mathbb{R}} = \mathbb{R} \cap E$, se tiene pues que $\mathbb{Q} \leq E_{\mathbb{R}} \leq E$.

TEOREMA (La conjugación en $\mathbb{C}$). La conjugación de números complejos $\overline{(-)} : \mathbb{C} \to \mathbb{C}$ se restringe a un automorfismo de E sobre $\mathbb{Q}$, $\overline{(-)}_{E/\mathbb{Q}} : E \to E$. Además,

(i) $\overline{(-)}_{E/\mathbb{Q}}$ es la identidad si y sólo si $E_{\mathbb{R}} = E$.

(ii) Si $E_{\mathbb{R}} \neq E$, entonces

$$\left\langle \overline{(-)}_{E/\mathbb{Q}} \right\rangle = \{\mathrm{id}, \overline{(-)}_{E/\mathbb{Q}}\} \cong \mathbb{Z}_2,$$

luego, $E_{\mathbb{R}} = E^{\langle \overline{(-)}_{E/\mathbb{Q}} \rangle}$ y $\left[E : E_{\mathbb{R}}\right] = 2$.

A modo de ejemplo, consideramos la extensión ciclotómica $\mathbb{Q}(\zeta_8)/\mathbb{Q}$, donde

$$\zeta_8 = e^{\pi i/4} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i.$$

Sabemos de ejemplos anteriores que

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i), \quad \text{y} \quad \left[\mathbb{Q}(\zeta_8) : \mathbb{Q}\right] = 4,$$

y podemos fácilmente ver que

$$\mathbb{Q}(\zeta_8)_{\mathbb{R}} = \mathbb{Q}(\sqrt{2}).$$

Lección 24 Grupos de Galois de permutaciones pares y impares.

Dedicaremos esta lección para responder a la pregunta que a continuación formulemos.
Hemos visto que dado un polinomio monoico separable $f(X) \in K[X]$ de grado n, el grupo de Galois de su cuerpo de escisión E sobre K, pueda verse de manera natural como subgrupo del grupo simétrico $\mathcal{S}_n$, que vemos como grupo de permutaciones de las n-raíces de $f(X)$. Es razonable preguntar cuando $\mathtt{Gal}(E/K) \leq \mathcal{A}_n$ el subgrupo alternado de $\mathcal{S}_n$ (i.e. formado por las permutaciones pares).

Para cualquier permutación $\sigma \in \mathcal{S}_n$, denotaremos por $sgn(\sigma)$ al siguiente valor

$$sgn(\sigma) \;=\; \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i},$$

que es ± 1.

Supongamos que $f(X)$ se factoriza sobre E como

$$f(X) \;=\; (X-u_1)\cdots(X-u_n) \;=\; \prod_{i=1}^{n}(X-u_i).$$

Aquí los $u_1,\cdots,u_n \in E$ son las raíces de $f(X)$; dado que $f(X)$ es por hipótesis separable, los u_i son distintos.

El discriminante de $f(X)$ es

$$\mathrm{Disc}(f(X)) \;=\; \prod_{1\leq i<j\leq n} (u_j-u_i)^2 \in E.$$

Observe que $\mathrm{Disc}(f(X))) \neq 0$ dado que $u_i \neq u_j$ para $i \neq j$.

Hay una fórmula que describe $\mathrm{Disc}(f(X))$ explícitamente en términos de los

coeficientes de $f(X)$. Dado dos polinomios

$$p(X) = a_0 + a_1X + \cdots + a_nX^n, \quad q(X) = b_0 + b_1X + \cdots + b_mX^m,$$

su *resultante* es la $(m+n)\times(m+n)$-determinante (con m filas de los a_i y n filas de los b_j)

$$\mathrm{Resl}(p(X),q(X)) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & \cdots & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix}$$

Si $f(X)$ es un polinomio monoico con grado $\mathrm{grad}(fX) = d$, entonces

$$\mathrm{Disc}(f(X)) = (-1)^{d(d-1)/2}\ \mathrm{Res}(f(X), f'(x)).$$

Por ejemplo para $f(X) = X^3 + a_2X^2 + a_1X + a_0$ se tiene que

$$\mathrm{Disc}(f(X)) = -27a_0^2 + 18a_0a_1a_2 + a_1^2a_2^2 - 4a_2^3a_0 - 4a_1^3.$$

Ahora consideramos

$$\delta(f(X)) = \prod_{1\le i<j\le n} (u_j - u_i) \in E.$$

Entonces $\delta(f(X))^2 = \mathrm{Disc}(f(X))$, luego las raíces cuadradas de $\mathrm{Disc}(f(X))$ son $\pm\delta(f(X))$. Para un automorfismo $\sigma \in \mathtt{Gal}(E/K)$ tenemos como antes que

$$\sigma\left(\delta(f(X))\right) = \mathrm{sgn}(\sigma)\delta(f(X)) = \pm\delta(f(X)).$$

Si $\sigma\left(\delta(f(X))\right) = \delta(f(X))$, esto quiere decir que $\mathrm{sgn}(\sigma) = 1$. De otra parte, si $\delta(f(X)) \notin K$ entonces

$$K(\delta(f(X))) = E^{\mathtt{Gal}(E/K)\cap\mathcal{A}_n}$$

y por supuesto $|\mathtt{Gal}(E/K)/\mathtt{Gal}(E/K) \cap \mathcal{A}_n| = 2$. Hemos comprobado pues lo siguiente

TEOREMA (El Grupo de Galois de permutaciones pares). Sea E/K una extensión de Galois finita.

(i) Para cualquier $\sigma \in \mathtt{Gal}(E/K)$,

$$\sigma(\mathrm{Disc}(f(X))) = \mathrm{Disc}(f(X)).$$

Es decir que $\mathrm{Disc}(f(X)) \in E^{\mathtt{Gal}(E/K)} = K$.

(ii) El grupo de Galois $\mathtt{Gal}(E/K) \leq \mathcal{S}_n$ esta contenido en $\mathcal{A}_n$ si y sólo si $\mathrm{Disc}(f(X))$ es un cuadrado en K.

LECCIÓN 25 TEOREMA DE KAPLANSKY.

Esta lección es otro ejemplo de prácticas a presentar le al alumno para que pueda visualizar bien la teoría desatollada anteriormente. Se trata de detallar la Teoría de Galois de los polinomios racionales irreducibles de forma

$$f(X) = X^4 + aX^2 + b \in \mathbb{Q}.$$

TEOREMA (De Kaplansky). Sea $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polinomio irreducible.

(i) Si b es un cuadrado en $\mathbb{Q}$, entonces $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(ii) Si $b(a^2-4b)$ es un cuadrado en $\mathbb{Q}$, entonces $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}_4$.

(iii) Si ni b ni $b(a^2 - 4b)$ son cuadrados en $\mathbb{Q}$, entonces $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong D_8$ (el grupo diedro de orden 8).

Tenemos pues los siguiente grupos de Galois,

$$\mathtt{Gal}(\mathbb{Q}(X^4 + 1)/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2,$$
$$\mathtt{Gal}(\mathbb{Q}(X^4 + 4X^2 + 2)/\mathbb{Q}) \cong \mathbb{Z}_4,$$
$$\mathtt{Gal}(\mathbb{Q}(X^4 + 2X^2 + 2)/\mathbb{Q}) \cong D_8.$$

BIBLIOGRAFÍA

[1] M. Artin. *Algebra*. Prentice Hall inc. 1991.

[2] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7*. Springer-Verlag, New York Berlin Heidelberg, 1990.

[3] J. P. Escofier. *Galois Theory*. Springer-Verlag, New York, 2001.

[4] John M. Howie. *Fields an Galois Theory*. Springer Undergraduate Mathematics Serie. Springer-Verlag, London, 2006.

[5] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[6] J. Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, 1990.

[7] I. Steward. *Galois Theory*. Chapman and Hall, 2004.

[8] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 2006.

Tema V

Extensiones de Galois de cuerpos en característica positiva.

Lecciones

Este tema es meramente una continuación del tema anterior, su contenido pueda considerase como formación complementaria del alumno sobre la teoría de Galois (finita). Se trata pues de un caso particular de las extensiones de Galois: las extensiones de Galois en característica positiva.

En la primera lección abordaremos los cuerpos finitos, y luego introducimos los llamados cuerpos de Galois, terminaremos dando la clausura algebraica de los cuerpos primos finitos, así como las raíces primitivas sobre estos cuerpos. Antes de enunciar los teoremas sobre las aplicaciones Traza y Norma, en la última lección, abordaremos antes en la segunda lección las propiedades de la aplicación de Frobenius.

LECCIÓN 26 CUERPOS FINITOS.

En esta lección presentaremos al alumno algunas propiedades esenciales de los cuerpos finitos.
Durante lo largo de este Tema, vamos a suponer que K es un cuerpo con característica $\mathrm{char}(K) = p$ ($p > 0$ es un primo) que contiene el cuerpo primo finito $\mathbb{F}_p$. Así K será siempre considerado como un $\mathbb{F}_p$-espacio vectorial. Nuestro primer objetivo es contar los elementos de K.

TEOREMA (Extensión de cuerpo finitos). Sea F un cuerpo finito con q elementos y V es un F-espacio vectorial. Entonces, $\dim_F(V) < \infty$ si, y solo si V es finito y en tal caso se tiene que $|V| = q^{\dim_F(V)}$.
En particular

(i) Si F un cuerpo finito y E/F una extensión. Entonces, E es finito si, y sólo si E/F es finito y entonces $|E| = |F|^{[E:F]}$.

(ii) Si K un cuerpo finito. Entonces $K/\mathbb{F}_p$ es una extensión finita y $|K| = p^{[K:\mathbb{F}_p]}$.

En ahora adelante nos proponemos de comprobar que para cada potencia p^d existe un cuerpo finito de p^d elementos. Empezaremos con la clausura algebraica $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$ y consideramos el polinomio

$$\Theta_{p^d}(X) \;=\; X^{p^d} - X \;\in \mathbb{F}_p[X].$$

Observamos que $\Theta'_{p^d}(X) = -1$, luego según la lección 14, cada raíz de $\Theta_{p^d}(X)$ en $\overline{\mathbb{F}_p}$ es simple. Luego, por la misma lección, $\Theta_{p^d}(X)$ tiene exactamente p^d diferentes raíces en $\overline{\mathbb{F}_p}$, digamos que son $0, u_1, \cdots, u_{p^d-1}$. Entonces en $\overline{\mathbb{F}_p}[X]$ se tiene que

$$X^{p^d} - X \;=\; X(X-u_1)(X-u_2)\cdots(X-u_{p^d-1}),$$

y cada una de las raíces es separable sobre $\mathbb{F}_p$. Sea

$$\mathbb{F}_{p^d} \;=\; \left\{u \in \overline{\mathbb{F}_p} \mid \Theta_{p^d}(X) \;=\; 0\right\} \subseteq \overline{\mathbb{F}_p}, \quad \mathbb{F}^0_{p^d} \;=\; \left\{u \in \mathbb{F}_{p^d} \mid u \neq 0\right\}.$$

Observe que $u \in \mathbb{F}_{p^d}^0$ si y solo si $u^{p^d-1} = 1$.

Para cualquier $d \geq 1$, $\mathbb{F}_{p^d}$ es un subcuerpo finito de $\overline{\mathbb{F}_p}$ con p^d elementos y $\mathbb{F}_{p^d}^0 = \mathbb{F}_{p^d}^\times$. Además, la extensión $\mathbb{F}_{p^d}/\mathbb{F}_p$ es una escisión separable.

El subcuerpo finito $\mathbb{F}_{p^d} \leq \overline{\mathbb{F}_p}$ se le llama *el cuerpo de Galois de orden* p^d.

Usaremos a veces, la notación $GF(p^d)$ en vez de $\mathbb{F}_{p^d}$. Por supuesto, $\mathbb{F}_{p^1} = GF(p^1) = GF(p) = \mathbb{F}_p$ y $\left[\mathbb{F}_{p^d} : \mathbb{F}_p\right] = d$. Resumimos esto en el siguiente resultado

TEOREMA (Cuerpos de Galois). Sea $d \geq 1$ un número natural.

(i) $\mathbb{F}_{p^d} \leq \overline{\mathbb{F}_p}$ es el subcuerpo escisión para cada uno de los polinomios

$$X^{p^d} - X, \quad X^{p^d-1} - 1 \in \mathbb{F}_p[X].$$

(ii) $\mathbb{F}_{p^d} \leq \overline{\mathbb{F}_p}$ es el único subcuerpo de p^d elementos.

(iii) Si F es cualquier cuerpo con p^d elementos, entonces existe un monomorfismo $F \to \overline{\mathbb{F}_p}$ con imagen $\mathbb{F}_{p^d}$, luego $F \cong \mathbb{F}_{p^d}$.

Como consecuencia de los apartados anteriores, se tiene
Si K un cuerpo finito de característica p, entonces $K/\mathbb{F}_p$ es una extensión de Galois.

Presentaremos algunos ejemeplos:

(1) Consideramos el polinomio $X^4 - X \in \mathbb{F}_2[X]$, se puede ver que en $\mathbb{F}_2[X]$ se tiene que

$$X^4 - X = X(X+1)(X^2+X+1).$$

Ahora esta claro que X^2+X+1 es irreducible sobre $\mathbb{F}_2$. Su escisión es entonces la extensión cuadrática $\mathbb{F}_2(w)/\mathbb{F}_2$ donde w es una de las raíces de X^2+X+1, la otra es $w+1$. Esto nos dice que cada elemento de $\mathbb{F}_4 = \mathbb{F}_2(w)$ pueda expresarse únicamente de forma $a+bw$ con $a, b \in \mathbb{F}_2$ y las reglas de multiplicación usan la

fórmula $w^2 = w + 1$.

(2) Considere el polinomio $X^9 - X \in \mathbb{F}_3[X]$. Esta claro que $X^2 + 1$ es irreducible en $\mathbb{F}_3[X]$. Luego si $u \in \overline{\mathbb{F}_3}$ es raíz de $X^2 + 1$, entonces $\mathbb{F}_3(w)/\mathbb{F}_3$ tiene grado 2 y $\mathbb{F}_3(u) = \mathbb{F}_9$. Cualquier elemento de $\mathbb{F}_9$ pueda expresarse de forma única como $a + bu$ con $a, b \in \mathbb{F}_3$. Las reglas de multiplicación aquí usan la fórmula $u^2 = 2$. En $\mathbb{F}_3[X]$, tenemos

$$X^9 - X = (X^3 - X)(X^2 + 1)(X^2 + X - 1)(X^2 - X - 1).$$

Luego $X^2 + X - 1$ y $X^2 - X - 1$ son también polinomio cuadráticos irreducibles en $\mathbb{F}_3[X]$. Podemos encontrar sus raíces en $\mathbb{F}_9$ usando la fórmula cuadrática en $\mathbb{F}_3$, $2^{-1} = -1$. El determinante de $X^2 + X - 1$ es $1 - 4(-1) = 2 = u^2$, de allí sus raíces son $(-1)(-1 \pm u) = 1 \pm u$. De manera similar, el determinante de $X^2 - X - 1$ es $1 - 4(-1) = 2 = u^2$, y sus raíces son $(-1)(-1 \pm u) = -1 \pm u$. Entonces se tiene que

$$\mathbb{F}_9 = \mathbb{F}_3(u) = \mathbb{F}_3(1 \pm u) = \mathbb{F}_3(-1 \pm u).$$

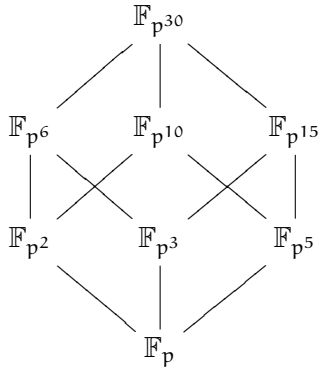


Figura V.1: El diagrama de Hasse de los subcuerpos de Galois del cuerpo $\mathbb{F}_{p^{30}}$

TEOREMA (Subcuerpos de Galois). Sea $\mathbb{F}_{p^m}$ y $\mathbb{F}_{p^n}$ dos extensiones de Galois en característica p. Entonces $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ si, y solo si $m|n$.

Esto quiere decir que el diagrama de subcuerpos del cuerpo de Galois $\mathbb{F}_{p^n}$ esta ordenado por la división de n. Dicho de otra forma ese diagrama coincide con el diagrama de Hasse de los números naturales divisores de n. Por ejemplo los subcuerpos de $\mathbb{F}_{p^{30}}$ vienen dados por la Figura V.1.

TEOREMA (La clausura de $\mathbb{F}_p$). La clausura algebraica de $\mathbb{F}_p$ es la unión de todos los cuerpos de Galois de característica p,

$$\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}.$$

Además, cada elemento $u \in \overline{\mathbb{F}_p}$ es separable sobre $\mathbb{F}_p$.

Sea K un cuerpo cualquiera. Entonces cada subgrupo finito $U \leq K^\times$ es cíclico. En particular, el grupo de unidades $\mathbb{F}_{p^d}^\times$ de $\mathbb{F}_{p^d}$ es cíclico.

Sea $w \in \mathbb{F}_{p^d}^\times$ se le llama *raíz primitiva* si es la (p^d-1)-raíz primitiva de la unidad, es decir su orden en el grupo $\mathbb{F}_{p^d}^\times$ es (p^d-1), luego $\langle w\rangle = \mathbb{F}_{p^d}^\times$.

Cabe hacer la siguiente observación sobre la terminología usada. Notemos aquí que la palabra primitivo ha sido usada anteriormente en la lección 15 para definir los elementos primitivos en un extensión de cuerpos. En efecto hay una relación entre los dos significados de *un elemento primitivo* y *raíz primitiva*. De hecho cualquier elemento primitivo es una raíz primitiva.

Terminamos esta lección enunciando el siguiente importante resultado

TEOREMA (Raíz primitiva en cuerpos finitos). Sean n, d dos números naturales.

(i) La extensión de cuerpos de Galois $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ es simple, es decir que $\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(u)$ para algún $u \in \mathbb{F}_{p^{nd}}$.

(ii) $\mathbb{F}_{p^d}$ contiene una n-iésima raíz primitiva de la unidad si, y sólo si $p^d \equiv 1 \left[n\right]$ y $p \nmid n$.

Como consecuencias de los apartados anteriores, se tiene que para cualquier $p > 0$ primo impar,

(a) Si $p \equiv 1 \left[4\right]$, el polinomio $X^2 + 1 \in \mathbb{F}_p[X]$ tiene dos raíces en $\mathbb{F}_p$.

(b) Si $p \equiv 3 \left[4\right]$, el polinomio $X^2 + 1 \in \mathbb{F}_p[X]$ es irreducible, luego

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p[X]/\left\langle X^2 + 1\right\rangle.$$

LECCIÓN 27 EL GRUPO DE GALOIS DE CUERPOS FINITOS Y LA APLICACIÓN DE FROBENIUS.

En esta lección analizaremos el grupo de Galois de extensiones de cuerpos de Galois.

Como ya se ha visto en la lección anterior 26, para cualquier par de número naturales n, d,tenemos en la extensión de Galois $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ que

$$|\mathtt{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})| \;=\; \left[\mathbb{F}_{p^{nd}} : \mathbb{F}_{p^d}\right] \;=\; n.$$

Introducimos ahora un elemento especial en el grupo $\mathtt{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$

La *aplicación de Frobenius (relativa) para la extensión* $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$, es la aplicación

$$f_d : \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}, \quad \left(t \longmapsto t^{p^d}\right).$$

Resumimos las propiedades de la aplicación de Frobenius.

LA APLICACIÓN DE FROBENIUS. Sean n, d dos números naturales.

(A) La aplicación de Frobenius relativa f_d es un elemento del grupo de Galois $\mathtt{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$ de orden n. Así $\mathtt{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle f_d \rangle$, el grupo cíclico generado por f_d.

(B) La aplicación de Frobenius existe en la clausura algebraica $\overline{\mathbb{F}_p}$,

$$f_d : \overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p}, \quad \left(t \longmapsto t^{p^d}\right).$$

Además, para $d \geq 1$

(Bi) $f_d \in \mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}_p})$. De hecho, para $u \in \overline{\mathbb{F}_p}$, $f_d(u) = u$ si, y sólo si $u \in \mathbb{F}_{p^d}$

(Bii) La restricción de f_d al subcuerpo de Galois $\mathbb{F}_{p^{nd}}$ coincide con la aplicación de Frobenius relativa de la extensión $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$.

(Biii) Si $k \geq 1$, entonces $f_d^k = f_{kd}$. Luego en el grupo de automorfismos $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}_p})$, f_d tiene un orden infinito. De allí $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}_p})$ es un grupo infinito.

La *aplicación de Frobenius (absoluta)* es f_1 que existe como elemento común de ambos grupos $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathcal{O}_p})$ y $\mathtt{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ para todo $n \geq 1$. En el grupo $\mathtt{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle f_d \rangle$, para cada k, con $k|n$, existe un subgrupo cíclico $\langle f_d^k \rangle$ de orden $|\langle f_d^k \rangle| = n/k$. El subcuerpo de elementos $\langle f_d^k \rangle$-invariantes en $\mathbb{F}_{p^{nd}}$ es

$$\mathbb{F}_{p^{nd}}^{\langle f_d^k \rangle} = \mathbb{F}_{p^{kd}}.$$

Así tenemos la siguiente torre

$$\begin{array}{c} \mathbb{F}_{p^{nd}} \\ \Big| \, n/k \\ \mathbb{F}_{p^{nd}}^{\langle f_d^k \rangle} = \mathbb{F}_{p^{kd}} \\ \Big| \, k \\ \mathbb{F}_{p^d} \end{array}$$

LECCIÓN 28 LAS APLICACIONES TRAZA Y NORMA.

En esta lección introducimos dos aplicaciones conocidas como *traza y norma* en el contexto de las extensión de Galois de cuerpos finitos que son de forma $E_{p;n,d} := (\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$. Dada un extensión de esta forma, se define la siguiente aplicación

$$\begin{aligned} \mathcal{T}_{E_{p;n,d}} : \mathbb{F}_{p^{nd}} &\longrightarrow \mathbb{F}_{p^{nd}} \\ u &\longmapsto \sum_{k=0}^{n-1} f_{kd}(u) \;=\; u + u^{p^d} + \cdots + u^{p^{(n-1)d}} \end{aligned}$$

Con esta definición, se tiene pues

$$f_d\left(\mathcal{T}_{E_{p;n,d}}\right) \;=\; \mathcal{T}_{E_{p;n,d}}.$$

Esto quiere decir según la lección 27 que $\mathcal{T}_{E_{p;n,d}} \in \mathbb{F}_{p^d}$. Esto sugiere definir la aplicación $\mathcal{T}_{E_{p;n,d}}$ con codominio el cuerpo $\mathbb{F}_{p^d}$

$$\mathcal{T}_{E_{p;n,d}} : \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^d}, \quad \left(u \longmapsto u + u^{p^d} + \cdots + u^{p^{(n-1)d}}\right).$$

Esta es *la aplicación traza relativa*.

TEOREMA (De la Traza). La aplicación traza relativa

$$\mathcal{T}_{E_{p;n,d}} : \mathbb{F}_{p^{nd}} \to \mathbb{F}_{p^d}$$

es una aplicación $\mathbb{F}_{p^d}$-lineal suprayectiva, cuyo núcleo es el $\mathbb{F}_{p^d}$-subespacio vectorial de dimensión $n-1$.

La versión multiplicativa de la traza, conlleva a la *aplicación norma*.

$$\begin{aligned} \mathcal{N}_{E_{p;n,d}} : \mathbb{F}^{\times}_{p^{nd}} &\longrightarrow \mathbb{F}^{\times}_{p^{nd}} \\ u &\longmapsto \prod_{k=0}^{n-1} f_{kd}(u) \;=\; u u^{p^d} \cdots u^{p^{(n-1)d}} \end{aligned}$$

Con esta definición, se tiene pues

$$f_d\left(\mathcal{N}_{E_{p;n,d}}\right) \;=\; \mathcal{N}_{E_{p;n,d}}.$$

Esto quiere decir según la lección 27 que $\mathcal{N}_{E_{p;n,d}} \in \mathbb{F}_{p^d}^{\times}$. Esto sugiere definir la aplicación $\mathcal{N}_{E_{p;n,d}}$ con codominio el cuerpo $\mathbb{F}_{p^d}^{\times}$

$$\mathcal{N}_{E_{p;n,d}} : \mathbb{F}_{p^{nd}}^{\times} \longrightarrow \mathbb{F}_{p^d}^{\times}, \quad \left(u \longmapsto u^1 u^{p^d} \cdots u^{p^{(n-1)d}}\right).$$

Esta es *la aplicación norma relativa*.

TEOREMA (De la Norma). La aplicación norma relativa

$$\mathcal{N}_{E_{p;n,d}} : \mathbb{F}_{p^{nd}}^{\times} \to \mathbb{F}_{p^d}^{\times}$$

es un morfismo de grupos suprayectivo.

BIBLIOGRAFÍA

[1] E. Artin. *Galois Theory*. Number 2 in Note Dame Mathematical Lectures. 1944.

[2] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7*. Springer-Verlag, New York Berlin Heidelberg, 1990.

[3] J. P. Escofier. *Galois Theory*. Springer-Verlag, New York, 2001.

[4] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[5] R. Lidl and H. Niederreiter. *An introduction to finite fields and thier applications.* Cambridge University Press, 1986.

[6] J. Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, 1990.

[7] I. Steward. *Galois Theory*. Chapman and Hall, 2004.

[8] Jean-Pierre Tignol. *Galois'Theory of Algebraic Equations*. World Scientific, Singapor, 2001.

[9] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 2006.

Tema VI

Antología de la Teoría de Galois.

Lecciones

Este tema agrupa varias lecciones la mayoría no se intercalan entre si. Se trata pues de una especie de recopilación de problemas o situaciones donde la teoría de Galois de ecuaciones algebraicas hace patente su presencia o más bien su utilidad.

La primera lección la dedicaremos integra a dar una demostración del teorema fundamental del álgebra; esta se basa sobre el cálculo de los subgrupos de Sylow del grupo de Galois de una extensión de Galois dentro de los números complejos. En la segunda lección abordaremos las extensiones ciclotómicas sobre un cuerpo base de característica no divisible por un número natural prefijado. Estimamos así el orden del grupo de Galois de tal extensión, de paso reciclaremos el caso clásico de los números racionales. Daremos el teorema de Artin sobre la dependencia de los carácteres debido, así como el Teorema 90 de Hilbert que asocia a cualquier extensión de Galois cuyo grupo es cíclico una sucesión exacta corta de grupos. Pasaremos luego a estudiar en la siguiente lección, las extensiones de Kummer (iteradas) sobre los cuerpos de característica cero y su relación con las extensiones radical simple. Las extensiones resolubles y radicales le dedicaremos una lección aparte, donde demostraremos el hecho de que una extensión de Galois es resoluble si y sólo si su correspondiente grupo Galois es resoluble. Daremos en este sentido, varios ejemplos de aplicación. Finalizaremos el tema con un resultado sobre las extensión de Galois con cuerpo de base las fracciones racionales simétricas, demostrando que este tipo de extensiones no es resoluble si el número de las indeterminada empleada es mayor o igual a 5. Como consecuencia directa se tiene el conocido teorema de Ruffini-Abel.

LECCIÓN 29 DEMOSTRACIÓN DEL TEOREMA FUNDAMENTAL.

En esta lección vamos a explicarle al alumno los pasos necesarios para demostrar el Teorema fundamental del álgebra para los números complejos:

TEOREMA (Fundamental del álgebra). El cuerpo de los números complejos $\mathbb{C}$ es álgebraicamente cerrado y $\overline{\mathbb{R}} = \mathbb{C}$.

Paso 1. Se sabe que $\left[\mathbb{C} : \mathbb{R}\right] = 2$, luego $\mathbb{C}/\mathbb{R}$ es una extensión algebraica, por la lección 10. Sea $p(X) \in \mathbb{C}[X]$ un polinomio irreducible. Entonces cualquier raíz u de $p(X)$ en la clausura algebraica $\overline{\mathbb{C}}$ es algebraica sobre $\mathbb{R}$. Por lo tanto, usando el Teorema de Polinomios separables lección 14, se tiene que $p(X)|\mathtt{Polmin}_{\mathbb{R},u}(X)$ en $\mathbb{C}[X]$. De allí, se pueda observar que el cuerpo de escisión de $p(X)$ sobre $\mathbb{C}$ esta contenido en el cuerpo E de escisión de $\mathtt{Polmin}_{\mathbb{R},u}(X)(X^2+1)$ sobre $\mathbb{R}$ (habrá que añadir la raíz de la unidad para cubrir a $\mathbb{C}$). Dado que $\mathbb{C} \leq E$, se tiene que $2| \left[E : \mathbb{R}\right]$, y luego $2||\mathtt{Gal}(E/R)|$.

Paso 2. Consideramos un subgrupo 2-Sylow $P \leq \mathtt{Gal}(E/\mathbb{R})$, recodaremos que $|\mathtt{Gal}(E/\mathbb{R})|/|P|$ es impar. El grado del subcuerpo de los elementos P-invariante, es

$$\left[E^P : \mathbb{R}\right] = \frac{|\mathtt{Gal}(E/\mathbb{R})|}{|P|},$$

lo que implica que $E^P/\mathbb{R}$ es una extensión de grado impar. Ahora el Teorema del elemento primitivo lección 15, nos dice que $E^P = \mathbb{R}(\nu)$ para algún elemento ν cuyo polinomio minimal sobre $\mathbb{R}$ debe de ser de grado impar. El Teorema del valor medio en análisis nos dice también que cualquier polinomio de grado impar tiene una raíz real, luego la irreducibilidad implica que ν tiene grado 1 sobre $\mathbb{R}$. Por lo tanto, $E^P = \mathbb{R}$, luego $\mathtt{Gal}(E/\mathbb{R}) = P$, de allí $\mathtt{Gal}(E/\mathbb{R})$ es un 2-grupo de Sylow.

Paso 3. Como $\mathbb{C}/\mathbb{R}$ es una extensión de Galois, consideramos el subgrupo normal $\mathtt{Gal}(E/\mathbb{C}) \lhd \mathtt{Gal}(E/\mathbb{R})$ para el cual se tiene $|\mathtt{Gal}(E/\mathbb{R})| = 2|\mathtt{Gal}(E/\mathbb{C})|$. Debe-

mos de comprobar que $|\mathtt{Gal}(E/\mathbb{C})| = 1$, así supongamos el contrario. DE la Teoría de grupos de Sylow, se sabe que existe un subgrupo normal $N \lhd \mathtt{Gal}(E/\mathbb{C})$ de índice 2. De allí, podamos considerar la extensión de Galois $E^N/\mathbb{C}$ de grado 2. Pero según las propiedades de $\mathbb{C}$, cualquier polinomio cuadrático $aX^2+bX+c \in \mathbb{C}[X]$ tiene raíces complejas (podemos encontrar la raíz cuadrada de cualquier número complejo). Por lo tanto no podemos encontrar polinomio cuadráticos irreducibles en $\mathbb{C}[X]$. Entonces $|\mathtt{Gal}(E/\mathbb{C})| = 1$, y $E = \mathbb{C}$.

LECCIÓN 30 EXTENSIONES CICLOTÓMICAS.

Esta lección la dedicaremos al estudio de las extensiones ciclotómicas, usando para ello las definiciones de la Lección 2. Sea $\zeta_n = e^{2\pi i/n}$ la n-iésima raíz primitiva de la unidad en $\mathbb{C}$. En la Lección 2, hemos visto que el polinomio irreducible sobre $\mathbb{Q}$ que tiene por ζ_n como raíz, es el n-iésimo polinomio ciclotómico

$$\Phi_n(X) = \prod_{\substack{t=1,\cdots,n-1 \\ mcd(t,n)=1}} (X - \zeta_n^t).$$

Comprobaremos el siguiente hecho sobre estos polinomios

TEOREMA (Polinomios ciclotómicos). Sea $n \geq 2$ un número natural y $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.

- $\mathbb{Q}(\zeta_n) = \mathbb{Q}[X]/\langle \Phi_n(X) \rangle$.
- $\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\right] = \varphi(n)$ (la aplicación de Euler).
- $\mathtt{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}_n)^\times$, donde un elemento $\left[t\right] \in (\mathbb{Z}_n)^\times$ actúa sobre $\mathbb{Q}(\zeta_n)$ con $\left[t\right].\zeta_n = \zeta_n^t$.

Para $n > 2$, en la extensión ciclotómica $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, se tiene que $\mathbb{Q}(\zeta_n)_{\mathbb{R}} \neq \mathbb{Q}(\zeta_n)$. Además,

$$\mathbb{Q}(\zeta_n)_{\mathbb{R}} = \mathbb{Q}(\zeta_n)_{\mathbb{R}}^{\langle \overline{()} \rangle} = \mathbb{Q}(\zeta_n + \overline{\zeta_n}) = \mathbb{Q}(\cos(2\pi/n)), \text{ y}$$

$$\left[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}.$$

A modo de ejemplo tenemos que

$$\left[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}\right] = \varphi(24) = 8, \quad \mathtt{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

El isomorfismo de grupos viene del hecho que $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(\zeta_{24})$.

Discutiremos pues el caso general. Sea ahora K un cuerpo con $\mathtt{Car}(K) \nmid n$. Los polinomios $\Phi_n(X)$ tiene coeficientes enteros, así puedan verse como elemen-

tos en $K[X]$ dado que $\mathbb{Q} \leq K$ o $\mathbb{F}_p \leq K$ y podemos reducir módulo p. En ambos caso pueda que $\Phi_n(X)$ se factoriza sobre K. Sin embargo, podamos describir el cuerpo de escisión de $X^n - 1$ sobre K y su grupo de Galois. En resumen se tiene

> TEOREMA. Sea K un cuerpo con $\mathrm{Car}(K) \nmid n$. Entonces el cuerpo de escisión de $X^n - 1$ sobre K es $K(\zeta)$, donde $\zeta \in \overline{K}$ es la n-iésima raíz primitiva de la unidad. El grupo de Galois $\mathtt{Gal}(K(\zeta)/K)$ es isomorfo a un subgrupo de $(\mathbb{Z}_n)^\times$, de allí es de orden divisible por $\varphi(n)$.

Cuando $\mathrm{Car}(K) = p > 0$, el grupo de Galois $\mathtt{Gal}(K(\zeta)/K)$ depende del subcuerpo más grande de K que es algebraico sobre $\mathbb{F}_p$. Por ejemplo, si $K = \mathbb{F}_{p^d}(t)$, entonces el valor de d es un factor crucial. Se puede determinar el resultado exacto con la ayuda del último Teorema de la Lección 26. A modo de ejemplo presentaremos la siguiente situación:

(1) El cuerpo de escisión del polinomio $X^4 - 1$ sobre $\mathbb{F}_3(t)$ es $\mathbb{F}_9(t)$ y

$$\mathtt{Gal}(\mathbb{F}_9(t)/\mathbb{F}_3(t)) = (\mathbb{Z}_4)^\times \cong \mathbb{Z}_2.$$

(2) Según el último Teorema de la Lección 26, $X^4 - 1$ escinde sobre $\mathbb{F}_5(t)$ y $\mathtt{Gal}(\mathbb{F}_5(t)/\mathbb{F}_5(t)$ es trivial.

Lección 31 El Teorema de Artin sobre la independencia lineal de carácteres.

Antes de empezar esta lección haremos un repaso sobre los resultados del la Lección 9, donde hemos explicado de manera general la independencia lineal o algebraica de ciertos morfismos. El resultado que presentaremos en esta lección es sobre la dependencia de los carácteres debido a E. Artin, a demás del Teorema 90 de Hilbert. El primero es de hecho un caso particular del Teorema de Dedekind enunciado en la Lección 9.

Sea G un grupo y K un cuerpo. Se le llama a un *carácter de* G *con valores en* K, todo morfismo de grupos $\chi : G \to K^\times$. Insistiremos sobre el siguiente ejemplo. Dad E/K una extensión de Galois junto con un elemento $\alpha \in \mathtt{Gal}(E/K)$. Entonces $\chi_\alpha : E^\times \to E^\times$ es un carácter.
Dada un familia finita de carácteres $\chi_1, \cdots, \chi_n$ de un grupo G con valores en K. Se dice que $\chi_1, \cdots, \chi_n$ son *linealmente independientes*, si para $t_1, \cdots, t_n$,

$$t_1\chi_1 + \cdots + t_n\chi_n = 0 \quad \Longrightarrow \quad t_1 = \cdots = t_n = 0.$$

Si no son linealmente independiente se dice que son *linealmente dependientes*. Por supuesto, la función en la ecuación de arriba es definida por

$$t_1\chi_1(x) + \cdots + t_n\chi_n(x) = 0, \quad \text{para todo } x \in G.$$

Teorema (De Artin). Sean $\chi_1, \cdots, \chi_n$, n carácteres distintos de un grupo G con valores en un cuerpo K. Entonces $\chi_1, \cdots, \chi_n$ son linealmente independientes.

Como consecuencias de este teorema presentaremos

TEOREMA. Sea K un cuerpo cualquiera.

(i) Supongamos que $\alpha_1, \cdots, \alpha_n$ son automorfismos distintos de K. Sea $t_1, \cdots, t_n \in K$ una sucesión de elementos, no todos nulos. Entonces existe un elemento $z \in K$ para el cual tenemos

$$t_1\alpha_1(z) + \cdots + t_n\alpha_n(z) \neq 0.$$

Por lo tanto, la transformación K-lineal $t_1\alpha_1 + \cdots + t_n\alpha_n : K \to K$ no es trivial.

(ii) Sea E/K una extensión de Galois finita de grado n y $\alpha_1, \cdots, \alpha_n$ distintos elementos del grupo de Galois $\mathtt{Gal}(E/K)$. Entonces, la aplicación $\alpha_1 + \cdots + \alpha_n : E \to E$ es una transformación K-lineal que no es trivial cuya imagen esta contenida en K. Luego, la transformación K-lineal asociada:

$$\mathrm{Tr}_{E/K} : E \longrightarrow E, \quad \Big(x \longmapsto \alpha_1(x) + \cdots + \alpha_n(x)\Big),$$

es suprayectiva.

Pasaremos ahora a definir *la aplicación norma* que va generalizar la aplicación que ya hemos definido en la Lección 28. Supongamos una extensión de Galois dada con el grupo de Galois cíclico, $\mathtt{Gal}(E/K) = \langle\sigma\rangle$ de orden n. Para cualquier $u \in E^\times$, el elemento $u\sigma(u)\cdots\sigma^{n-1}(u) \in E$ satisface

$$\sigma\Big(u\sigma(u)\cdots\sigma^{n-1}(u)\Big) = \sigma(u)\sigma^2(u)\cdots\sigma^n(u) = u\sigma(u)\cdots\sigma^{n-1}(u),$$

Es decir que $u\sigma(u)\cdots\sigma^{n-1}(u) \in E^{\langle\sigma\rangle} = K$. De allí, se puede definir la aplicación

$$N_{E/K} : E^\times \longrightarrow K^\times, \quad \Big(u \longmapsto u\sigma(u)\cdots\sigma^{n-1}(u)\Big).$$

Esta aplicación se le llama *la aplicación norma para* E/K. Existe otra aplicación

$$\delta_{E/K} : E^\times \longrightarrow E^\times, \quad \Big(u \longmapsto u\sigma^{-1}(u)\Big).$$

Para cualquier $u \in E^\times$, se tiene que $N_{E/K}\left(\delta_{E/K}\right) = 1$, dado que $\sigma^n(u) = u$. Por

lo tanto $\mathrm{Im}(\delta_{E/K}) \leq \mathrm{Ker}(N_{E/K})$. El siguiente importante resultado generaliza el último Teorema de la Lección 28.

TEOREMA (90 de Hilbert). Sea E/K una extensión de Galois finita con el grupo de Galois cíclico, $\mathtt{Gal}(E/K) = \langle\sigma\rangle$ de orden n. Entonces $\mathrm{Im}(\delta_{E/K}) = \mathrm{Ker}(N_{E/K})$. Explícitamente, si $u \in E^\times$ con $u\sigma(u)\cdots\sigma^{n-1}(u) = 1$, entonces existe $v \in E^\times$ tal que $u = v\sigma(v)^{-1}$.
Dicho de otra forma, tenemos una sucesión exacta de grupos

$$1 \longrightarrow E^\times \xrightarrow{\delta_{E/K}} E^\times \xrightarrow{N_{E/K}} K^\times \longrightarrow 1.$$

LECCIÓN 32 EXTENSIÓN RADICAL SIMPLE.

Nos centraremos en esta Lección en la busqueda de el cuerpo de escisión del polinomio $X^n - a$ donde $\mathrm{Car}a(K) \nmid n$. Llamaremos tal extensión *una extensión radical simple*. Más tarde en la Lección 33, introduciremos una noción más general, la de *extensión radical*.

Empezaremos demostrando el siguiente resultado

TEOREMA. Sea K un cuerpo con $\mathrm{Car}a(K) \nmid n$.

(i) Sea $f(X) = X^n - a \in K[X]$ un polinomio irreducible y separable sobre K. Entonces el cuerpo de escisión de $f(X)$ sobre K, tiene la siguiente forma

$$K_{f(X)} = K(u, \zeta),$$

donde u es una raíz de $f(X)$ y ζ la n-iésima raíz primitiva de la unidad. Además

$$\{\mathrm{id}\} \lhd \mathtt{Gal}(K(u,\zeta)/K(\zeta)) \lhd \mathtt{Gal}(K(u,\zeta)/K),$$

donde $\mathtt{Gal}(K(u,\zeta)/K(\zeta))$ es cíclico y

$$\mathtt{Gal}(K(\zeta)/K) \cong \mathtt{Gal}(K(u,\zeta)/K(\zeta))/\mathtt{Gal}(K(u,\zeta)/K(\zeta))$$

es abeliano. La correspondencia de Galois viene dad por la Figura VI.1

(ii) En particular, si K contiene a la n-iésima raíz primitiva de la unidad, ζ, entonces el cuerpo de escisión de $f(X) = X^n - a$ sobre K es $K_{f(X)} = K(u)$, donde u es una raíz de $f(X)$. El grupo de Galois $\mathtt{Gal}(K(u)/K)$ es cíclico de orden n con generador σ que actúa de forma $\sigma(u) = \zeta u$.

daremos la siguiente definición. Sea K un cuerpo con $\mathrm{Car}(K) \nmid n$ que contie-

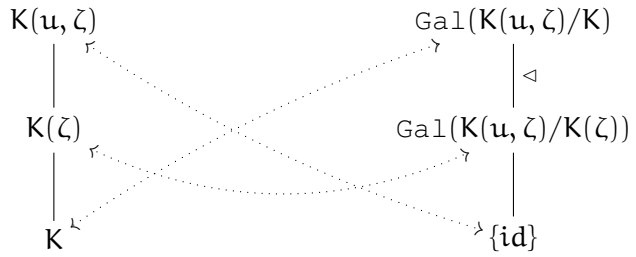


Figura VI.1: La correspondencia de Galois para K_{X^n-a} con $\mathrm{Car}a(K) \nmid n$.

ne la n-iésima raíz primitiva de la unidad, ζ. Entonces se dice que L/K es *una extensión n-Kummer simple* si $L = K(u)$ donde $u^n = a$, para algún $a \in K$. Se dice que es *una extensión n-Kummer simple iterada* si $L = K(u_1, \cdots, u_k)$ donde $u_1^n = a_1, \cdots, u_k^n = a_k$, para algunos elementos $a_1, \cdots, a_k \in K$. Aquí de hecho no se le pide que $X^n - a_j$ es irreducible.

TEOREMA (Extensiones n-Kummer simples). Sea K un cuerpo con $\mathrm{Car}a(K) \nmid n$.

(i) Sea $K(u)/K$ una extensión n-Kummer simple. Entonces $K(u)/K$ es una extensión de Galois y $\mathtt{Gal}(K(u)/K)$ es cíclico de orden divisible por n.

(ii) Supongamos que K contiene a la n-iésima raíz primitiva de la unidad, ζ. Si E/K es una extensión de Galois finita cuyo grupo de Galois es cíclico de orden n, entonces existe un elemento $v \in E$ tal que $E = K(v)$ y v es la raíz de un polinomio de forma $X^n - b$ con $b \in K$. Por lo tanto, E/K es una extensión n-Kummer simple.

A modo de ejemplo $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i)$ es una extensión 4-Kummer simple con $\mathtt{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i))$ es cíclico de orden 2.

LECCIÓN 33 EXTENSIONES RADICALES Y GRUPOS RESOLUBLES.

En esta lección introduciremos las extensiones radical y las extensiones resolubles. Trabajaremos con un cuerpo base de característica cero. Daremos pues la demostración del hecho que una extensión de Galois es resoluble si y sólo si el grupos de Galois asociado es resoluble. Presentaremos también varios ejemplos ilustrativos.

Empezaremos esta Lección con un recordatorio breve sobre algunas nociones en Teoría de grupos, nuestra referencia aquí el Tema VI del curso **Álgebra II**.

Un grupo G se dice que *resoluble*, si existe una cadena de subgrupos (llamada *serie subnormal*)

$$\{1\} = G_\ell \leq G_{\ell-1} \leq \cdots\cdots \leq G_1 \leq G_0 = G,$$

tales que $G_{k+1} \lhd G_k$ y cualquier *factor de composición* G_k/G_{k+1} es un grupo abeliano. La notación empleada es

$$\{1\} = G_\ell \lhd G_{\ell-1} \lhd \cdots\cdots \lhd G_1 \lhd G_0 = G.$$

Si cada factor de composición es un grupo cíclico de orden primo, la serie subnormal se le llama *serie de composición*. Un grupo que no es resoluble se dice que es *insoluble*. Vamos a agrupar algunas de las propiedades de los grupo resolubles necesarias para su uso en la Teoría de Galois. Las primeras son: Cualquier grupo abeliano finito es resoluble, y cualquier grupo finito que es un p-grupo con p primo, es resoluble.

TEOREMA (Grupos Resolubles.). Sea G un grupo.

(i) Si G es resoluble, entonces cualquier subgrupo $H \leq G$ y cualquier cociente G/N es resoluble.

(ii) Si $N \lhd G$ y G/N son resoluble, entonces G lo es también.

TEOREMA (Grupos Resolubles.). Sea G un grupo finito. Entonces G es insoluble si, y sólo si se satisfacen las siguientes condiciones:

(i) G contiene un subgrupo que es un grupo simple no abeliano (o tiene un cociente simple no abeliano)

(ii) G tiene un grupo cociente que es simple no abeliano.

(iii) G tiene una serie de composición que tiene un término que es simple no abeliano.

A modo de ejemplo $\{1\} \lhd \mathcal{A}_n \lhd \mathcal{S}_n$, para $n \geq 5$. Dado que $\mathcal{A}_n$ es simple no abeliano, $\mathcal{S}_n$ es insoluble. Así es también el grupo alternado $\mathcal{A}_n$, para $n \geq 5$.

Ahora explicaremos al alumno como se relacionan esta nociones con las extensiones de cuerpos. A continuación consideramos cuerpos con característica cero, i.e. sea K un cuerpo con $Car(K) = 0$.

- Sea L/K una extensión finita de cuerpos, se dice que L/K es *una extensión radical*, si es de forma $L = K(a_1, \cdots, a_n)$ con

$$a_k^{d_k} \in K(a_1, \cdots, a_{k-1}),$$

para algún $d_k \geq 1$. Es decir cualquier elemento de L se puede expresarse como raíz iterada de elementos de K.

- Si L es el cuerpo escisión de un polinomio $f(X) \in K[X]$, entonces $f(X)$ es resoluble por radical sobre K, si L está contenido en una extensión radical de K.

- La extensión L/K es *una extensión resoluble*, si $L \leq L'$ donde L'/K es un extensión de Galois finita y radical sobre K.

El siguiente es el resultado principal de esta Lección

TEOREMA (Grupos de Galois resolubles.). Sea E/K una extensión de Galois finita. Entonces, son equivalentes:

(i) E/K es un extensión resoluble;

(ii) $\mathtt{Gal}(E/K)$ es un grupo resoluble.

Como ejemplo citaremos la extensión $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$. Esta extensión es resoluble. Ya hemos explicado al alumno en el Tema IV, Lección 22 del presente curso, las propiedades de esta extensión. Es claramente radical y tenemos

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) \;=\; \mathrm{Qset}(\zeta_3)(\sqrt[3]{2}).$$

Sabemos también que hay un isomorfismo de grupos $\mathtt{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) \cong \mathcal{S}_3$, donde se identifica cualquier elemento del grupo de Galois con una permutación de las tres raíces de $X^3 - 2$ en $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$, que daremos en lista:

$$\sqrt[3]{2},\ \sqrt[3]{2}\zeta_3,\ \sqrt[3]{2}\zeta_3^2.$$

Se tiene pues la torre de subcuerpo y subgrupos relacionados mediante la correspondencia de Galois, véase la Figura VI.2. Aquí $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ es también una extensión de Galois y $\mathcal{A}_3 \lhd \mathcal{S}_3$. Se sabe que $\mathcal{A}_3 \cong \mathbb{Z}_3$ y que $\mathcal{S}_3/\mathcal{A}_3 \cong \mathbb{Z}_2$, tenemos pues la siguiente serie de composición

$$\{\mathrm{id}\} \lhd \mathcal{A}_3 \lhd \mathcal{S}_3.$$

Cabe explicarle al alumno el interés que tiene la cuestión del recíproco. Es decir si hay extensiones de cuerpos que no son resolubles. Esto es un famoso problema que ha sido persuadido por varios centenares de años. Para dar ejemplo, ponemos de manifiesto primero que el grupo simple no abeliano más

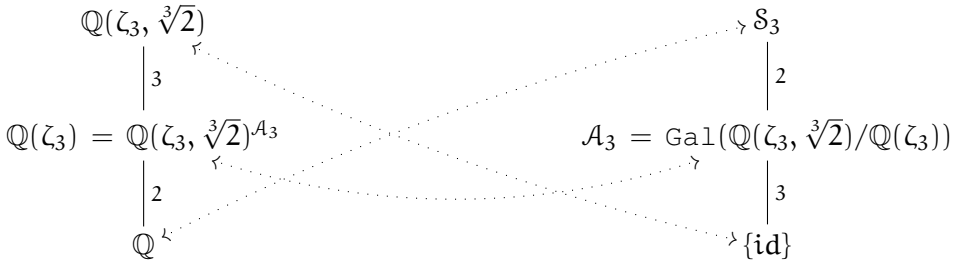


Figura VI.2: La correspondencia de Galois para $\mathbb{Q}_{X^3-2}$.

pequeño es $\mathcal{A}_5$ cuyo orden es 60. Habrá pues que ver polinomios de grado al menos 5 para encontrar un grupo de Galois para una escisión de cuerpos o bien que ocurre como un factor composición de tal grupo de Galois. A continuación presentaremos un ejemplo detallado:

El cuerpo de escisión del polinomio $f(X) = X^5 - 35X^4 + 7 \in \mathbb{Q}[X]$ no es resoluble.

Sea $E \leq \mathbb{C}$ el cuerpo de escisión de $f(X)$ sobre $\mathbb{Q}$. Usando el criterio de Eisenstein en la Lección 2 con $p = 7$, se tiene que $f(X)$ es irreducible en $\mathbb{Q}[X]$. Ahora según el primer Teorema de la Lección 18, se tiene que 5 divide al orden del grupo $\mathtt{Gal}(E/\mathbb{Q})$, y según el Lema de Cauchy, existe un elemento de ese grupo cuyo orden en 5. Dado que

$$f'(X) = 5X^3(X-28), \quad f''(X) = 20X^2(X-21),$$

hay puntos créticos, $x = 0$ y $x = 28$, además $f(0) > 0 > f(28)$. Esto quiere decir que existen tres raíces reales de $f(X)$ y dos no reales. La conjugación de números complejos se restringe a un elemento de orden 2 de $\mathtt{Gal}(E/\mathbb{Q})$ que intercambia las dos raíces no reales, y deja fijas las de más. Si nombramos todas esas raíces u_1, u_2, u_3, u_4, u_5, con u_1, u_2 siendo las raíces no reales, entonces la transposición $(1\,2)$ corresponde a ese mismo elemento. Además, el único elemento de $\mathcal{S}_5$ de orden 5 es un 5-cíclo. Escogiendo potencias apropiadas, podemos suponer que existe u 5-cíclo de forma $(1\,2\,3\,4\,5)$ correspondiente a un

elemento de $\mathtt{Gal}(E/\mathbb{Q})$ que estamos viendo como un subgrupo de $\mathcal{S}_5$. De hecho $\mathtt{Gal}(E/\mathbb{Q}) \cong \mathcal{S}_5$, según el siguiente resultado general en grupos: Sea $n \geq 1$, supongamos que $H \leq \mathcal{S}_n$ y que H contiene los elementos $(1\,2)$ y $(1\,2\cdots n)$, entonces $H = \mathcal{S}_n$.

Podemos usar el Teorema de la Lección 24, para comprobar que el grupo de Galois de $f(X) = X^5 + 20X + 16$ sobre $\mathbb{Q}$ es $\mathtt{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathcal{A}_5$, luego no es resoluble.

Lección 34 Funciones simétricas y extensiones no resolubles.

En esta lección daremos un ejemplo de una extensión de cuerpos que no resoluble. Se trata del subcuerpo de la funciones simétricas dentro del cuerpo de fracciones a varias indeterminadas. Cabe explicar el interés por este tipo de extensión: esto viene del siguiente famoso problema cuya respuesta es conocida como el Teorema de Ruffini y Abel. Recordaremos de la Lección 33, que un *polinomio* $f(Y) \in K[Y]$ *es resoluble por radical sobre* K, si existe un extensión radical de K que contiene todas las raíces de $f(Y)$. En general el tipo de ecuaciones que se presentan son de la forma

$$f(Y) \;=\; (Y - X_1)\cdots(Y - X_n) \;=\; Y^n - \mathfrak{s}_1 Y^{n-1} + \cdots + (-1)^n \mathfrak{s}_n \;=\; 0,$$

Así la pregunta era si para $n \geq 5$, este tipo de polinomios son resolubles por radical o no sobre el cuerpo de fracciones en $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$. De allí, se escoge como cuerpo de base el cuerpo de fracciones racionales en $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ que son los polinomios simétricos elementales en $X_1, \cdots, X_n$.

Sea $\Bbbk$ un cuerpo, y consideramos el cuerpo de fracciones $K = \Bbbk(X_1, \cdots, X_n)$. Cada elemento $\sigma \in \mathcal{S}_n$ actúa sobre $\Bbbk[X_1, \cdots, X_n]$ de la siguiente forma

$$\sigma \,.\, f(X_1, \cdots, X_n) \;=\; f^{\sigma}(X_1, \cdots, X_n) \;=\; f(X_{\sigma(1)}, \cdots, X_{\sigma(n)}).$$

Visto que aplicación $\sigma\,.(-) : \Bbbk[X_1, \cdots, X_n] \to \Bbbk[X_1, \cdots, X_n]$ es isomorfismo de anillos, que se extiende al un automorfismo de cuerpos $\sigma\,.(-) : \Bbbk(X_1, \cdots, X_n) \to \Bbbk(X_1, \cdots, X_n)$. Variando los elementos de $\mathcal{S}_n$, se tiene una acción del grupo $\mathcal{S}_n$ sobre el anillo $\Bbbk[X_1, \cdots, X_n]$ y el cuerpo $\Bbbk(X_1, \cdots, X_n)$ actuando vía automorfismos que dejan fijos los elementos del cuerpo base $\Bbbk$.
Se define el cuerpo *de funciones simétricas a* n *indeterminadas* como

$$\mathrm{Sim}_n(\Bbbk) \;=\; \Bbbk(X_1, \cdots, X_n)^{\mathcal{S}_n} \leq \Bbbk(X_1, \cdots, X_n).$$

Acorde con la notación de la Lección 22, tenemos que $\mathrm{Sim}_n(\Bbbk) = \Bbbk(X_1,\cdots,X_n)^{\mathrm{sim}}$. Es decir un elemento $P(X_1,\cdots,X_n) \in \Bbbk(X_1,\cdots,X_n)$ pertenece a $\mathrm{Sim}_n(\Bbbk)$ si , y sólo si

$$P(X_1,\cdots,X_n) = P(X_{\sigma(1)},\cdots,X_{\sigma(n)}), \quad \text{para todo } \sigma \in \mathcal{S}_n.$$

Hay funciones simétricas llamadas *funciones simétricas elementales*:

$$\mathfrak{s}_k = \sum_{i_1<i_2<\cdots<i_k} X_{i_1}X_{i_2}\cdots X_{i_k}, \quad 1 \leq k \leq n.$$

TEOREMA (De funciones simétricas). Sea $\Bbbk$ un cuerpo.

(i) La extensión $\Bbbk(X_1,\cdots,X_n)/\mathrm{Sim}_n(\Bbbk)$ es una extensión de Galois finita con $\mathtt{Gal}(\Bbbk(X_1,\cdots,X_n)/\mathrm{Sim}_n(\Bbbk)) \cong \mathcal{S}_n$.

(ii) Si $n \geq 5$, entonces la extensión $\Bbbk(X_1,\cdots,X_n)/\mathrm{Sim}_n(\Bbbk)$ no es resoluble.

Recordaremos de la Lección 22, que tenemos un isomorfismo de cuerpos

$$\mathrm{Sim}_n(\Bbbk) \cong \Bbbk(\mathfrak{s}_1,\cdots,\mathfrak{s}_n)$$

Así como aplicación directa del resultado anterior, se tiene

TEOREMA (Ruffini y Abel). Si $n \geq 5$ la ecuación general de grado n

$$f(X) = (X-x_1)\cdots(X-x_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n = 0$$

no es resoluble por radical ni sobre $\mathbb{Q}(s_1,\cdots,s_n)$ ni sobre $\mathbb{C}(s_1,\cdots,s_n)$.

BIBLIOGRAFÍA

[1] E. Artin. *Galois Theory*. Number 2 in Note Dame Mathematical Lectures. 1944.

[2] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7*. Springer-Verlag, New York Berlin Heidelberg, 1990.

[3] John M. Howie. *Fields an Galois Theory*. Springer Undergraduate Mathematics Serie. Springer-Verlag, London, 2006.

[4] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[5] J. Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, 1990.

[6] I. Steward. *Galois Theory*. Chapman and Hall, 2004.

[7] Jean-Pierre Tignol. *Galois'Theory of Algebraic Equations*. World Scientific, Singapor, 2001.

[8] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 2006.

BIBLIOGRAFÍA

[1] K. Pearson A. Jones, S. Morris. *Abstract Algebra and Famous Impossibilities*. Springer-Verlag, New York, 1994.

[2] E. Artin. *Galois Theory*. Number 2 in Note Dame Mathematical Lectures. 1944.

[3] M. Artin. *Algebra*. Prentice Hall inc. 1991.

[4] N. Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[5] N. Bourbaki. *Elements of Mathematics. Algebra II. Chapters 4-7.* Springer-Verlag, New York Berlin Heidelberg, 1990.

[6] N. Bourbaki. *Éléments de Mathématique. Algèbre Commutative. Chapitres 5 á 7.* Springer-Verlag, Berlin Heidelberg, 2007.

[7] Harold M. Edwards. *Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1984.

[8] J. P. Escofier. *Galois Theory*. Springer-Verlag, New York, 2001.

[9] J. B. Fraleigh. *A First Course in Abstract Algebra*. Addison Wesley, 1999.

[10] John M. Howie. *Fields an Galois Theory*. Springer Undergraduate Mathematics Serie. Springer-Verlag, London, 2006.

[11] N. Jacobson. *Lecture in Abstract Algebra. III-Theory of Fields and Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 1964.

[12] N. Jacobson. *Basic Algebra II*. W. H. Freeman and Company, 1985.

[13] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, 1985.

[14] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[15] R. Lidl and H. Niederreiter. *An introduction to finite fields and their applications*. Cambridge University Press, 1986.

[16] F. Lorenz. *Algebra vol. I: Fields and Galois Theory*. Springer-Verlag, New York. 2006.

[17] I. Kaplansky. *Fields and Rings*. Chicago University Press, 1972.

[18] M. P. Malliavin. *Algèbre Commutative, applications en géométrie et théories des nombres*. Masson, Paris, 1984.

[19] M. Nagata. *Field Theory*. Marcel Dekker, 1977.

[20] J. Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, 1990.

[21] I. Steward. *Galois Theory*. Chapman and Hall, 2004.

[22] John Swallow. *Exploratory Galois Theory*. Cambridge University Press. Cambridge, 2004.

[23] Jean-Pierre Tignol. *Galois'Theory of Algebraic Equations*. World Scientific, Singapor, 2001.

[24] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, New York Heidelberg Berlin, 2006.