ÍNDICE

VI. Cuerpos finitos.

Lección 16: Cuerpos finitos.

VII. La Correspondencia de Galois.

Lección 17: El grupo de Galois.
Lección 18: Teorema de Artin.
Lección 19: Teorema Fundamental de la Teoría de Galois.

VIII. Consecuencias de la Teoría de Galois.

Lección 20: Reencuentro con la Teoría de Grupos.
Lección 21: Construcciones con regla y compás.
Lección 22: Teorema del Elemento Primitivo.

IX. Resolubilidad de ecuaciones por radicales.

Lección 23: Resolubilidad de ecuaciones por radicales.
Lección 24: El grupo de Galois visto como subgrupo del grupo simétrico.
Lección 25: Resolución de la ecuación general de grado n.

Bibliografía.

INTRODUCCIÓN

El presente programa ha sido pensado para ser impartido en una asignatura troncal de 6 créditos del primer ciclo (curso tercero) de la Licenciatura de Matemáticas de la Universidad de Málaga denominada Álgebra Clásica.

Nos encontramos en esta asignatura, por su carácter troncal, con todos los alumnos de la Licenciatura de Matemáticas, los cuales llevan normalmente un año sin haber cursado asignaturas propias del Álgebra, ya que en los nuevos planes de estudio no se contempla ninguna asignatura de esta materia en el segundo curso de la licenciatura. No obstante, gracias a que los problemas que trata son en sí interesantes, se consigue una buena respuesta por parte del alumno desde un primer momento, simplemente recordando las nociones y los resultados básicos que vayan siendo de utilidad.

El principal objetivo de esta asignatura es el estudio de la llamada teoría de Galois. Con esta teoría se consiguen contestar problemas propuestos desde la Grecia Clásica, aunque más interesantes que la solución de dichos problemas son las técnicas utilizadas para resolverlos. Estos problemas son: por un lado, el estudio de ciertas construcciones geométricas, las llamadas construcciones con regla y compás, y, por otro, la solubilidad de ecuaciones polinómicas por radicales. Veamos en qué consisten dichos problemas:

Si nos centramos en la ecuación de segundo grado $aX^2 + bX + c = 0$ tenemos que sus soluciones son:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Dicho resultado ya era conocido en esencia por los babilónicos. La solución general de la ecuación de tercer grado fue resuelta por Scipione de Ferro no después de 1541. Cuatro años más tarde, en 1545, Niccolo Tartaglia dará una solución independiente conocida como la fórmula de Cartan para la resolución de la ecuación de tercer grado. Expliquemos dicho proceso: dada una ecuación de tercer grado $aX^3+bX^2+cX+d = 0$, haciendo el cambio de variable $X \rightsquigarrow X-\frac{1}{3}a$ nos encontramos con una ecuación de tercer grado en forma reducida, $X^3 + pX + q = 0$. Denotemos por $\alpha_1, \alpha_2, \alpha_3$ a las raíces de esta ecuación reducida y sean $\delta = -4p^3 - 27p^2$, $\phi = -\frac{1}{2}(1+\sqrt{-3})$, $y_1 = \alpha_1+\phi^2\alpha_2+\phi\alpha_3$ y $y_2 = \alpha_1+\phi\alpha_2+\phi^2\alpha_3$. Entonces, las fórmulas de Cartan dicen que:

$$y_1 = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3\delta}}$$
$$y_2 = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3\delta)}}$$

Por tanto sólo hay que resolver un sistema lineal de tres ecuaciones con tres incógnitas para obtener las soluciones del sistema reducido (ya que $\alpha_1+\alpha_2+\alpha_3 = 0$). Un método general para la ecuación de grado cuarto fue publicado por Cardano en Ars Magna aunque es atribuido a un alumno suyo, Ludovico Ferrari. Lo interesante de este método es que en él también se pone de manifiesto que las soluciones de la ecuación de cuarto grado están dadas en términos de sumas, productos, cocientes y raíces de números racionales junto con los coeficientes de dicha ecuación. Cuando esto sucede se dice que la ecuación es soluble por radicales. En 1813 A. Ruffini e independientemente en 1827 N. H. Abel demuestran que la ecuación general de grado n, con $n > 4$, no es soluble por radicales. Más tarde, en 1830, E. Galois (a la edad de 19 años) da un criterio que permite saber si una ecuación concreta de grado n es o no es soluble por radicales.

El segundo problema que podremos contestar gracias a las técnicas usadas en la teoría de Galois tiene sus orígenes en la Grecia Clásica y consiste en saber si ciertas construcciones geométricas son posibles usando sólo una regla (sin marcas) y un compás. Las cuestiones más importantes son:

(1) ¿ Es posible trisecar un ángulo?
(2) ¿ Es posible construir un cubo con volumen el doble de uno dado?
(3) ¿ Es posible construir el polígono regular de n lados?
(4) ¿ Es posible cuadrar el circulo?

Como veremos, la respuesta a las tres primeras preguntas no siempre será afirmativa (dependerá del ángulo que queramos trisecar, del cubo al que queramos duplicar el volumen o del polígono que queramos construir). La cuarta pregunta la contestaremos gracias al resultado establecido por F. Lindemann que afirma que π es trascendente.

El proyecto que aquí presentamos es esencialmente Teoría de Extensiones de Cuerpos. Consideramos que esta asignatura es particularmente bonita: por un lado, tenemos la elegancia de los resultados intrínsecos de la teoría de Galois y, por otro, su fineza a la hora de resolver problemas en principio ajenos a dicha teoría. Es importante que el alumno se de cuenta de que a veces, y en esta asignatura hay muchos ejemplos de ello, la mejor forma para resolver un problema es verlo desde otro punto de vista. Así, calcular extensiones intermedias puede realizarse calculando subgrupos para un cierto grupo, o poder trisecar un ángulo con regla y compás depende de que cierta extensión de cuerpos tenga grado potencia de dos.

Comenzamos en el Tema 1 con las nociones básicas de la teoría de Galois: definimos extensión de cuerpos, grado de una extensión, extensión algebraica y trascendente y damos algunos resultados que relacionan dichos conceptos.

Sólo con estas nociones y sin hacer uso de ningún resultado teórico potente abordamos en el Tema 2 los problemas clásicos de construcciones con regla y compás: estudiamos los problemas de la trisección del ángulo y de la cuadratura del círculo contestándolos en su totalidad y damos una primera respuesta parcial a la pregunta de qué polígonos regulares son construibles con regla y compás.

En el Tema 3 demostramos la existencia y la unicidad, salvo automorfismos, del cuerpo de descomposición de una familia finita de polinomios, obteniendo a la vez

información sobre el número de tales automorfismos. En la última sección de este tema introducimos la noción de clausura algebraica y demostramos que todo cuerpo posee, salvo isomorfismos, una única clausura algebraica.

En los temas 4 y 5 estudiamos de forma independiente las distintas nociones que aparecen en la definición de extensión de Galois. El Tema 4 está dedicado al estudio de las extensiones normales y el Tema 5 al estudio de las extensiones separables. Cabe destacar que, en este último tema, se introduce la noción de cuerpo perfecto y se demuestra que todo cuerpo de característica cero y todo cuerpo finito es perfecto.

En el Tema 6 se demuestra que toda extensión finita de un cuerpo finito es normal, separable, y simple. Por último se demuestra un resultado de Galois que afirma que para cada primo p y para cada natural n existe un único cuerpo, salvo isomorfismos, con p^n elementos.

El Tema 7 se dedica a establecer la correspondencia de Galois: se introduce la noción de grupo de Galois asociado a una extensión de cuerpos, se establecen distintas aplicaciones entre los subgrupos del grupo de Galois y los cuerpos intermedios de la extensión y se demuestra que, en caso de que la extensión sea de Galois, dichas aplicaciones son biyectivas. Cabe destacar de este tema el Teorema de Artin, así como que se establece un algoritmo para calcular el grupo de Galois de una extensión de Galois dada.

En los temas 8 y 9 comprobamos la gran fortaleza del resultado de Galois obtenido en el tema anterior. En el Tema 8, tras un breve repaso de teoría de grupos, resolvemos completamente los problemas de construcciones con regla y compás y obtenemos el Teorema del Elemento Primitivo. Por otra parte, en el Tema 9 se caracterizan los polinomios resolubles por radicales en cuerpos de característica cero como aquéllos que su grupo de Galois es soluble. Hasta este momento el proceso que habíamos explicado para calcular el grupo de Galois de un polinomio hacía uso explícito de sus raíces. Obviamente esto no nos permite en la práctica aplicar el criterio anterior para saber si un polinomio en concreto es resoluble. Por tanto, damos un nuevo método para calcular el grupo de Galois de cierta clase de polinomios sin necesidad de conocer sus raíces. Finalizamos el tema probando que la ecuación general de grado n para $n \geq 5$ no es resoluble por radicales.

Los 6 créditos de la asignatura se dividen en 4 teóricos y 2 prácticos. Consideramos que se debe ser flexible a la hora de fijar clases teóricas y prácticas, adaptando unas y otras al desarrollo de la asignatura. Hay temas más conceptuales y abstractos y otros en los que los ejemplos y ejercicios cobran mayor importancia.

Los ejercicios se suministrarán a los alumnos con anterioridad a su resolución en pizarra, de modo que puedan ser ellos mismos los que los expliquen a sus compañeros. En este sentido, ha de exigirse a los alumnos claridad, precisión y justificación de sus razonamientos, obligándolos a organizar conocimientos y a resumir ideas, consiguiendo, en última instancia, una mayor comprensión de la materia.

Consideramos que en las clases teóricas debe propiciarse la intervención del alumno, huyendo de la lección magistral tradicional, y planteando cuestiones y preguntas que fomenten el diálogo entre profesor y alumno. Además, el profesor servirá de guía para que los alumnos interesados puedan profundizar en el tema y,

en este sentido, se propondrán lecturas y ejercicios complementarios.

TEMA 1.

EXTENSIONES DE CUERPOS.

Lección 1.- Definiciones y ejemplos.

Lección 2.- Grado de una extensión.

Lección 3.- Extensiones algebraicas. Extensiones trascendentes.

Las primeras clases de esta asignatura estarán dedicadas a plantear los distintos problemas clásicos que son contestados gracias a la teoría de Galois.

Se introduce el concepto de construcción con regla y compás y se discuten algunos de los problemas procedentes de dicha teoría, tales como la bisección y trisección del ángulo, el cálculo de la perpendicular o paralela a una recta dada que pase por un punto determinado, la cuadratura del círculo, la duplicación del cubo, etc. Se discuten soluciones dadas por los alumnos, así como la posibilidad de que algunas de las cuestiones anteriores posean una respuesta negativa.

Por otro lado se discute la resolución de ecuaciones polinómicas. Se recuerda la fórmula de resolución de la ecuación de grado dos y se da un sistema general para resolver la de grado tres. Se plantea si pueden ser encontradas fórmulas similares para grados superiores.

Antes de empezar con la materia propia de la asignatura hacemos un breve repaso de los resultados que vamos a necesitar en los primeros temas: Recordamos el anillo de polinomios sobre un anillo conmutativo y unitario R y lo caracterizamos por su propiedad universal. Recordamos el algoritmo de la división en $F[X]$, con F un cuerpo y obtenemos que $F[X]$ es un D.I.P. Por último, se recuerdan las nociones de divisibilidad entre polinomios, la definición de polinomio irreducible y damos varios criterios que nos permiten concluir si ciertos polinomios son irreducibles.

Definiciones y ejemplos.

Sea F un cuerpo. Se dirá que (K, σ) es una extensión de F y se denotará por $F \preccurlyeq K$ si K es un cuerpo y $\sigma : F \to K$ es un monomorfismo de anillos unitarios.

Damos dos procesos interesantes para la construcción de extensiones de cuerpos:

1) Sean F un cuerpo y $F[X]$ el anillo de los polinomios con coeficientes en F. Dado un polinomio irreducible $f(X) \in F[X]$ se tiene que $K = F[X]/ < f(X) >$ es un cuerpo. Además, la aplicación $\sigma : F \to K$ definida por $\sigma(a) = \overline{a}$ es un monomorfismo de anillos unitarios. Así, (K, σ) es una extensión de F.

2) Sea (K, σ) una extensión de F y sea $S \subset K$. Se define $F[S]$ como el menor subanillo de K que contiene a $\sigma(F)$ y a S. Se denota por $F(S)$ al menor subcuerpo de K que contiene a $\sigma(F)$ y a S. Claramente se tiene que $F[S] \subset F(S)$. Se demuestra que $F(S)$ es el cuerpo de fracciones de $F[S]$ y que dados S, T dos subconjuntos de K, $F(S)(T) = F(S \cup T)$. Concluimos que para cada subconjunto $S \subset K$ se tiene que $(F(S), \sigma|_{F(S)})$ es una extensión de F.

Si $F \preccurlyeq K$, la imagen $\sigma(F)$ es un subcuerpo de K isomorfo a F, por lo que cuando convenga se podrá considerar $F \subset K$.

Grado de una extensión.

Dada una extensión de cuerpos $F \preccurlyeq K$, se puede dotar, de forma natural, a K de estructura de F–espacio vectorial. Se define el grado de K en F y se representa por $[K : F]$ como la dimensión de este espacio vectorial. Si $[K : F] < \infty$ se dice que K es una extensión finita de F. Se calcula entonces el grado de toda extensión del tipo 1): si F es un cuerpo y $f(X)$ es un polinomio irreducible de $F[X]$ de grado n se demuestra que $[K : F] = n$, en donde K denota a $F[X]/ < f(X) >$.

Se pone de manifiesto que la propiedad de ser una extensión finita es una propiedad transitiva dentro de las extensiones de cuerpos. Es más, se demuestra que $[K : F] = [K : L][L : F]$ para F, L y K tres cuerpos tales que $F \preccurlyeq L \preccurlyeq K$.

Para finalizar la sección se introduce el concepto de extensión simple de cuerpos (se dice que una extensión de cuerpos $F \preccurlyeq K$ es simple si existe $u \in K$ tal que $K = F(u)$; en este caso se dirá que u es un elemento primitivo de la extensión) y se demuestra que toda extensión del tipo 1), así como toda extensión de grado primo, es simple.

Extensiones algebraicas. Extensiones trascendentes.

Sea $F \preccurlyeq K$ una extensión de cuerpos y sea $u \in K$. Se considera el anillo de polinomios $F[X]$ con coeficientes en F. Por la propiedad universal de los anillos de polinomios existe un único homomorfismo de anillos $\phi : F[X] \to K$ tal que $\phi|_F = Id|_F$ y $\phi(X) = u$. En estas condiciones se tiene que $Im(\phi) = F[u]$ y que, al ser $F[X]$ un dominio de ideales principales, existe $f(X) \in F[X]$ tal que $Ker(\phi) =< f(X) >$. Tenemos dos posibilidades mutuamente excluyentes:

1) Si $Ker(\phi) = \{0\}$, entonces $F[X] \cong Im(\phi) = F[u]$ y por tanto $[F(u) : F] = \infty$. En este caso se dice que u es trascendente sobre F.

2) Si $\{0\} \neq Ker(\phi) =< f(X) >$, entonces es fácil ver que $f(X)$ es un polinomio irreducible de $F[X]$ y por tanto, aplicando el Primer Teorema de Isomorfía, $F[u] =$

$Im(\phi) \cong F[X]/ < f(X) >$ es un cuerpo. Así, $F[u] = F(u)$ y $[F(u) : F] = deg(f(X))$. En este caso se dice que u es algebraico sobre F.

Reuniendo la información obtenida tendremos, respectivamente, la caracterización de elemento trascendente y de elemento algebraico:

Sea $F \preccurlyeq K$ una extensión de cuerpos y sea $u \in K$. Las siguientes condiciones son equivalentes:

(1) u es trascendente sobre F.
(2) $F[u] \cong F[X]$.
(3) $F(u) \cong F(X)$.
(4) $[F(u) : F] = \infty$.

Sea $F \preccurlyeq K$ una extensión de cuerpos y sea $u \in K$. Las siguientes condiciones son equivalentes:

(1) u es algebraico sobre F.
(2) Existe un (único) polinomio (mónico) irreducible $f(X) \in F[X]$ tal que u es raíz de $f(X)$.
(3) $F[u] = F(u) \cong F[X]/ < f(X) >$.
(4) $[F(u) : F] < \infty$.

Además, en este caso $[F(u) : F] = deg(f(X))$. Este único polinomio mónico irreducible sobre F que anula a u será llamado el polinomio mínimo de u sobre F.

A continuación se define cuándo una extensión de cuerpos es algebraica, trascendente y finitamente generada, y se relacionan estos conceptos demostrando que si $F \preccurlyeq K$ es una extensión de cuerpos, es equivalente que sea finita a que sea finitamente generada y algebraica, o a que sea de la forma $K = F(u_1, u_2, \ldots, u_n)$, con u_i elemento de K algebraico sobre F para $i = 1, 2, \ldots, n$.

Se define la clausura algebraica de una extensión de cuerpos $F \preccurlyeq K$ como el conjunto $\mathcal{A}_K(F) = \{u \in K \mid u \text{ es algebraico sobre } F\}$, y se prueba que es un subcuerpo de K. Se demuestra también que la propiedad de ser una extensión algebraica es una propiedad transitiva dentro de las extensiones de cuerpos.

Para finalizar la sección se introduce la noción de cuerpo algebraicamente cerrado y se caracteriza dicho concepto de varias maneras interesantes.

TEMA 2.

CONSTRUCCIONES CON REGLA Y COMPÁS.

Lección 4.- Definiciones previas.

Lección 5.- Criterios de constructibilidad.

Lección 6.- Aplicaciones.

En estos momentos ya podemos abordar algunos de los problemas clásicos de construcciones con regla y compás. La idea clave para resolver estos problemas está simplemente en mirarlos desde otro punto de vista, y que esto, y no resultados complicados en sí, es lo que nos permite resolverlos.

Definiciones previas.

Sea $\mathbb{R}$ el cuerpo de los números reales y $\mathbb{R}^2$ el plano geométrico. Denotemos por S a un subconjunto de $\mathbb{R}^2$ que contenga a $\{(0,0),(1,0)\}$.

Se dirá que una recta r es construible a partir de S si contiene dos puntos distintos de S. Se dirá que una circunferencia c es construible a partir de S si el centro es un punto de S y el radio es la distancia entre dos puntos de S. Se define el conjunto de puntos construible a partir de S y se denota por $G(S)$ como $\cup_{n\in\mathbb{N}} S_n$ en donde S_n se define de forma inductiva como sigue: $S_1 = S$; S_n son puntos de intersecciones de dos rectas (distintas), una recta y una circunferencia o dos circunferencias (distintas) construibles a partir de S_{n-1}. Diremos que un punto p es construible si pertenece a $G(S)$. Diremos que una recta o una circunferencia es construible si es construible a partir de $G(S)$

Se demuestra que si p y r son respectivamente un punto y una recta construible, entonces tanto la recta perpendicular como la recta paralela a r que pasan por p es construible.

En este momento se identifican los puntos del plano geométrico $\mathbb{R}^2$ con el cuerpo de los complejos. El conjugado de un elemento $z = a + bi \in \mathbb{C}$ se denota por $\overline{z}$. Dado el subconjunto S, como subconjunto de $\mathbb{C}$, se denota por $\overline{S}$ a $\{z, \overline{z}, \mid z \in S\}$

Se demuestra que si S es un subconjunto de $\mathbb{C}$, la suma, el producto, el cociente, los conjugados y las raíces cuadradas de elementos construibles son construibles. Es más, se demuestra que $G(S)$ es el menor subcuerpo de $\mathbb{C}$ que contiene a S y es cerrado para conjugados y raíces cuadradas.

Criterios de constructividad.

Dado un cuerpo F, se define una extensión de torres de raíces cuadradas sobre F como una cadena

$$F = F(u_0) \subset F(u_1) \subset F(u_1, u_2) \subset \cdots \subset F(u_1, u_2, \ldots, u_n)$$

tal que $u_i^2 \in F(u_1, u_2, \ldots, u_{i-1})$ para $i \in \{1, 2, \ldots, n\}$.

Un resultado que será muy útil en la práctica es que si la característica de F es distinta de dos, una extensión K de F es de grado dos si y sólo si existe $x \in K$ tal que $K = F(x)$ con $x^2 \in F$.

Se demuestra entonces que dado un conjunto S en las condiciones del tema, un punto $z \in \mathbb{C}$ es construible si y sólo si existe una extensión de torres de raíces cuadradas sobre $F = \mathbb{Q}(\overline{S})$,

$$F = F(u_0) \subset F(u_1) \subset F(u_1, u_2) \subset \cdots \subset F(u_1, u_2, \ldots, u_n)$$

tal que $z \in F(u_1, u_2, \ldots, u_n)$.

Como corolario se obtiene que si z es un punto construible, $[F(z), F] = 2^n$.

Aplicaciones.

En esta lección estudiamos cada uno de los problemas clásicos ya mencionados. Así, se ve que no siempre es posible construir con regla y compás un cubo de volumen el doble a uno dado. Se demuestra que el cubo de arista 1 no se puede duplicar. En ejercicios se verá que hay cubos a los que se les puede duplicar el volumen, con o sin necesidad de usar su arista como dato.

Se estudia ahora el problema de la trisección del ángulo. Se define cuándo un ángulo es construible y se demuestra que un ángulo α es construible (con regla y compás) si y sólo si $z = e^{i\alpha} = cos(\alpha) + sen(\alpha)i$ es construible, y esto sucede si y sólo si se puede construir $sen(\alpha)$ o $\cos(\alpha)$. Se demuestra que existen ángulos que no se pueden trisecar. Como en el caso de la duplicación del cubo, se demuestra que existen ángulos, digamos α, que se pueden trisecar simplemente porque el ángulo $\alpha/3$ es construible a partir de $S = \{0, 1\}$, y otros que para poder trisecarlos hace falta partir del dato inicial.

Continuamos el tema dando una respuesta parcial a la pregunta de qué polígonos regulares se pueden construir con regla y compás. Más adelante, cuando tengamos el Teorema Fundamental de la Teoría de Galois, la contestaremos en su totalidad. Estudiamos la construcción de polígonos regulares con un número primo p de lados,

llegando a la conclusión que son construibles si y sólo si p es un primo de Fermat, es decir, p es un número primo de la forma $2^{(2^n)} + 1$. Por tanto, se establece que se pueden construir los polígonos regulares de $3, 5, 17, 257$ y 65537 lados

Por último, gracias al resultado de F. Lindemann que establece que π es trascendente, se demuestra que no es posible cuadrar el círculo.

TEMA 3.

CUERPOS DE DESCOMPOSICIÓN.

Lección 7.- Cuerpo de descomposición de un polinomio.

Lección 8.- Extensiones de isomorfismos a extensiones simples.

Lección 9.- Unicidad (salvo isomorfismo) del cuerpo de descomposición.

Lección 10.- Clausura algebraica.

Cuerpo de descomposición de un polinomio.

Sean F un cuerpo, $f(X) \in F[X]$ y K una extensión de F. Se dice que $f(X)$ se descompone totalmente en K si existen $c, u_1, u_2, \ldots, u_n \in K$ tales que $f(X) = c(X-u_1)(X-u_2)\cdots(X-u_n) \in K[X]$ (obsérvese que $c \in F$). Si además $K = F(u_1, u_2, \ldots, u_n)$ se dice que K es cuerpo de descomposición de $f(X)$ sobre F. En general, dada una familia de polinomios $\mathcal{F} = \{f_i |\ i \in I\}$ y una extensión K de F, se dice que K es cuerpo de descomposición de la familia $\mathcal{F}$ si para cualquier $i \in I$, $f_i(X)$ se descompone en K y $K = F(S)$, en donde S es el conjunto de todas las raíces de los polinomios de $\mathcal{F}$.

Usando el hecho conocido de que todo polinomio se factoriza como producto de polinomios irreducibles y de que dado un polinomio irreducible $f(X) \in F[X]$ existe una extensión K de F que contiene una raíz de $f(X)$, se demuestra, por un proceso inductivo, que todo polinomio posee, al menos, un cuerpo de descomposición. Además, si $f(X)$ tiene grado n y K es un cuerpo de descomposición de $f(X)$ sobre F, $[K : F] \leq n!$.

Extensiones de isomorfismos a extensiones simples.

Sean $F \preccurlyeq K$ y $F' \preccurlyeq K'$ dos extensiones de cuerpos y $\sigma : F \to F'$ un isomorfismo de cuerpos. Se dice que $\sigma' : K \to K'$ es un isomorfismo extensión de σ si σ' es un isomorfismo de cuerpos tal que $\sigma'|_F = \sigma$.

Dados dos cuerpos F y F' y $\sigma : F \to F'$ un isomorfismo de cuerpos, se denotará por $\phi_\sigma : F[X] \to F'[X]$ al único isomorfismo de anillos que verifica que $\phi_\sigma|_F = \sigma$ y $\phi_\sigma(X) = X$. En lo que sigue denotaremos por $p^\sigma(X) := \phi_\sigma(p(X))$. De este hecho se deduce un primer resultado de extensión de isomorfismos a extensiones simples, ya que dado un polinomio irreducible $f(X) \in F[X]$,

$$F[X]/ < f(X) > \cong F'[X]/ < f^\sigma(X) > .$$

Por tanto, dados dos cuerpos F y F', un isomorfismo $\sigma : F \to F'$ de cuerpos y dos extensiones algebraicas (y simples) de F y F' (respectivamente denotadas por $F(u)$ y $F'(v)$), es equivalente el que $p(X) \in F[X]$ polinomio mínimo de u sobre F, implique que $p^\sigma(X) \in F'[X]$ sea el polinomio mínimo de v sobre F' a que exista un (único) isomorfismo de anillos $\sigma' : F(u) \to F'(v)$ que extienda a σ con $\sigma'(u) = v$. Además, en tal caso, el número de isomorfismos $\sigma' : F(u) \to F'(v)$ que extienden a σ coincide con el número de raíces distintas que posea $p^\sigma(X)$ en $F'(v)$.

Unicidad (salvo isomorfismo) del cuerpo de descomposición.

En esta sección vamos a demostrar la unicidad, salvo isomorfismo, del cuerpo de descomposición de un polinomio. Además, vamos a obtener información sobre el número de automorfismos en ciertas extensiones de cuerpos.

Sean F y F' dos cuerpos y $\sigma : F \to F'$ un isomorfismo de cuerpos. Sea $f(X) \in F[X]$ un polinomio y consideremos $f^\sigma(X) \in F'[X]$. Sean K y K' cuerpos de descomposición respectivamente de $f(X)$ sobre F y $f^\sigma(X)$ sobre F'. En estas condiciones se demuestra que K es isomorfo a K' y que el número de isomorfismos $\sigma' : K \to K'$ que extienden a σ es menor o igual que $[K : F]$, coincidiendo con este último cuando todas las raíces de $f^\sigma(X)$ en K' son distintas.

Sea $F \preccurlyeq K$ una extensión de cuerpos. Se dice que un automorfismo $\sigma : K \to K$ es un F–automorfismo si σ extiende a la identidad en F.

Como corolario al teorema anterior se obtiene que el cuerpo de descomposición de un polinomio $f(X) \in F[X]$, digamos K, es único salvo F–automorfismos y que el número de tales F–automorfismos es menor o igual que el grado de la extensión $F \preccurlyeq K$, coincidiendo con este cuando todas las raíces de $f(X)$ en K son distintas.

Clausura algebraica.

Se define la clausura algebraica de un cuerpo F, y se denota por $\overline{F}$, como un cuerpo K extensión algebraica de F tal que todo polinomio de F se descompone en $\overline{F}$. Se prueba que la clausura algebraica de un cuerpo es algebraicamente cerrada. Se demuestra que todo cuerpo F está contenido en un cuerpo K algebraicamente cerrado y que la clausura algebraica de F en este cuerpo algebraicamente cerrado K es justamente la clausura algebraica de F. Por último se demuestra la unicidad, salvo isomorfismos, de la clausura algebraica. Hacemos notar que ambos resultados, tanto el de existencia como el de unicidad de la clausura algebraica, hacen uso del Lema de Zorn.

TEMA 4.
EXTENSIONES NORMALES.

Lección 11.- Definiciones y ejemplos.

Lección 12.- Distintas caracterizaciones de extensión normal.

Lección 13.- Algunas propiedades de las extensiones normales.

Definiciones y ejemplos.

Dada una extensión de cuerpos $F \preccurlyeq K$, se dice que dos elementos $u, v \in K$ son conjugados sobre F si poseen el mismo polinomio mínimo sobre F. Una extensión de cuerpos $F \preccurlyeq K$ se dice que es normal si es cerrada para conjugados, es decir, para cualquier extensión L de K, si $u \in K$ y $v \in L$ son conjugados sobre F, entonces $v \in K$.

Se dan algunos ejemplos de extensiones normales y se demuestra que si $F \preccurlyeq K$ es una extensión cuerpos de grado dos, o si K es un cuerpo algebraicamente cerrado, la extensión es normal.

Distintas caracterizaciones de extensión normal.

Se da una primera caracterización de extensión normal como aquella extensión de cuerpos $F \preccurlyeq K$ tal que los polinomios irreducibles de $F[X]$ que poseen una raíz en K se descomponen en K.

Caracterizamos entonces las extensiones de cuerpos, $F \preccurlyeq K$, que son normales y algebraicas como aquéllas en las que K es el cuerpo de descomposición de una familia de polinomios de $F[X]$. Como corolario se obtiene que una extensión de cuerpos, $F \preccurlyeq K$, es normal y finita si y sólo si K es el cuerpo de descomposición de un polinomio $f(X) \in F[X]$.

Se observa que si $F \preccurlyeq K$ es una extensión normal y L es un cuerpo intermedio, entonces $L \preccurlyeq K$ es también normal y que $F \preccurlyeq L$ no tiene por qué serlo.

Algunas propiedades de las extensiones normales.

En esta sección se caracterizará el conjunto de soluciones de un polinomio irreducible $f(X) \in F$ con una raíz, digamos u, en una extensión normal K de F como el conjunto de las imágenes de u por cada uno de los F–automorfismos de K. Para

concluir se demuestra que si $F \preccurlyeq K$ es una extensión algebraica de cuerpos y L es un cuerpo intermedio entre F y K, entonces, la extensión $F \preccurlyeq L$ es normal si y sólo si para todo F–automorfismo $\sigma : K \to K$, se verifica que $\sigma(L) \subset L$. Este resultado será de utilidad para el cálculo del grupo de Galois de una extensión de Galois.

TEMA 5.
EXTENSIONES SEPARABLES.

Lección 14.- Derivada formal.

Lección 15.- Extensiones separables. Cuerpos perfectos.

Derivada formal.

Se define la derivada formal de un polinomio y se comprueba que verifica propiedades análogas a las usuales. Se caracterizan los polinomios $f(X) \in F[X]$ que poseen una raíz doble (en el cuerpo de descomposición de $f(X)$ sobre F) como aquéllos que verifican que $f(x)$ y $D(f(X))$ no son primos relativos.

Extensiones separables. Cuerpos perfectos.

Sea F un cuerpo. Se dice que un polinomio irreducible $f(X) \in F[X]$ es separable si no posee raíces múltiples en un cuerpo de descomposición de $f(X)$ sobre F. Se observa que la definición anterior es independiente del cuerpo de descomposición que tomemos. Se dice que un polinomio $f(X) \in F[X]$ es separables si lo es cada uno de sus factores irreducibles.

Se caracterizan los polinomios irreducibles $f(X) \in F[X]$ que son separables como aquéllos tales que $Df(X) \neq 0$. Como consecuencia se obtiene que todo polinomio en un cuerpo de característica cero es separable y que los polinomios irreducibles y no separables en cuerpos de característica p se caracterizan por ser de la forma $f(X) = g(X^p)$ con $g(X) \in F[X]$

Una extensión de cuerpos, $F \preccurlyeq K$, se dice que es separable si es algebraica y todo polinomio irreducible de F con una raíz en K es separable. Un cuerpo se dice que es perfecto si toda extensión algebraica suya es separable. Se obtiene por tanto que los cuerpos de característica cero son perfectos y que los cuerpos perfectos de característica p son aquéllos tales que todo elemento admite una raíz p-ésima (es decir, dado $u \in F$, existe $v \in F$ tal que $v^p = u$).

Para concluir se demuestra que todo cuerpo finito es perfecto y se da un ejemplo de cuerpo no perfecto.

TEMA 6.
CUERPOS FINITOS.

Lección 16.- Cuerpos finitos.

En este tema vamos a clasificar todos los cuerpos finitos. Así, como los anillos de división y los dominio de integridad finitos son cuerpos tendremos también clasificadas estas estructuras.

Como primer resultado se recuerda que si F es un cuerpo finito existe $p \in \mathbb{Z}$ (p es la característica de F) tal que F es extensión de $\mathbb{Z}_p$. Como consecuencia se obtiene que $\#F = p^n$ en donde $n = [F : \mathbb{Z}_p]$.

Haciendo uso de la clasificación de los grupos abelianos finitos y del hecho de que un polinomio de grado n tiene a lo sumo n raíces se demostrará que cualquier subgrupo finito del grupo multiplicativo de un cuerpo es cíclico. Esto probará que todo cuerpo finito es extensión primitiva de su cuerpo primo.

Asimismo se verá que si F es un cuerpo finito con p^n elementos, F es isomorfo al cuerpo de descomposición sobre $\mathbb{Z}_p$ del polinomio $X^{n-1} - 1 \in \mathbb{Z}_p[X]$. Esto implica que todo cuerpo finito es extensión normal y separable de su cuerpo primo, así como da la clave para demostrar el Teorema de Galois que afirma que para cada primo p y cada natural n existe un único cuerpo con p^n elementos.

TEMA 7.

LA CORRESPONDENCIA DE GALOIS.

Lección 17.- El grupo de Galois.

Lección 18.- Teorema de Artin.

Lección 19.- Teorema Fundamental de la Teoría de Galois.

En este capítulo vamos a desarrollar el resultado central de la Teoría de Galois, en donde se establece una correspondencia biyectiva entre los cuerpos intermedios de una extensión normal, separable y finita y los subgrupos de cierto grupo finito (el grupo de Galois de la extensión). Este resultado permitirá demostrar la existencia de ecuaciones polinómicas no resolubles por radicales así como abordar de forma definitiva ciertos problemas de construcciones con regla y compás. Más adelante, en ejercicios, se usará este resultado para calcular las raíces de ciertos polinomios separables.

El grupo de Galois.

Se comienza la sección definiendo el grupo de Galois, $Gal_F(K)$, de una extensión de cuerpos $F \preccurlyeq K$. Se prueba que si K es una extensión finitamente generada de un cuerpo F, $K = F(u_1, u_2, \ldots, u_n)$, y consideramos $\sigma \in Gal_F(K)$, entonces: 1) σ queda determinada una vez que se conoce la imagen de u_i, para $i = 1, 2, \ldots, n$. 2) u_i y $\sigma(u_i)$ son conjugados sobre F, para $i = 1, 2, \ldots, n$. A continuación se calcula el grupo de Galois de distintas extensiones.

Dado una extensión de cuerpos $F \preccurlyeq K$ se definen los siguientes conjuntos:

$$\mathcal{S} = \{L \mid \ L \text{ es un cuerpo intermedio entre } F \text{ y } K\},$$
$$\mathcal{T} = \{H| \ H \text{ es un subgrupo del grupo de Galois de } F \preccurlyeq K\},$$

y las siguientes aplicaciones:

(1) $\phi : \mathcal{S} \to \mathcal{T}$, en donde para cada cuerpo $L \in \mathcal{S}$ definimos $\phi(L) = Gal_L(K)$, y
(2) $\Phi : \mathcal{T} \to \mathcal{S}$, en donde para cada subgrupo $H \in \mathcal{T}$ definimos $\Phi(H) = Inv(H) := \{a \in K \mid f(a) = a \quad \forall \ f \in H\}$.

Se demuestran entonces las siguiente propiedades:

(i) Si $H_1 \subset H_2$, $Inv(H_2) \subset Inv(H_1)$.

(ii) Si $L_1 \subset L_2$, $Gal_{L_2}(K) \subset Gal_{L_1}(K)$.

(iii) $F \subset Inv(Gal_F(K))$.

(iv) $Gal_F(K) = Gal_{Inv(G)}(K)$, en donde G denota $Gal_F(K)$.

El Teorema de Artin.

Se comienza la sección haciendo notar que el cuerpo de descomposición de un polinomio separable coincide con el cuerpo de descomposición de un polinomio sin raíces dobles. De aquí se deduce, gracias al Teorema de Unicidad del Cuerpo de Descomposición de un polinomio, que si F es un cuerpo, $f(X) \in F[X]$ un polinomio separable y K el cuerpo de descomposición de $f(X)$ sobre F, $\#Gal_F(K) = [K : F]$.

Se enuncia y demuestra el Teorema de Artin que establece que si K es un cuerpo y H un subgrupo finito de $Aut(K)$, entonces $[K : Inv(H)] \leq \#H$.

Teorema Fundamental de la Teoría de Galois.

Se define una extensión de Galois como una extensión de cuerpos normal finita y separable.

Se caracteriza una extensión de Galois como una extensión de cuerpos, dígase $F \preccurlyeq K$, tal que verifica alguna de las siguientes condiciones equivalentes: 1) Existe un polinomio separable $f(X) \in F[X]$ tal que K es el cuerpo de descomposición de $f(X)$ sobre F. 2) $F = Inv(G)$ para G un subgrupo finito de $Aut(K)$. Además en las condiciones de 1), si tomamos como $G = Gal_F(K)$, $Inv(G) = F$; y en las condiciones de 2), $Gal_F(K) = G$.

Estamos entonces ya en condiciones de dar el resultado central de la Teoría de Galois: sea $F \preccurlyeq K$ una extensión de Galois y

$$\mathcal{S} = \{L |\ L \text{ es un cuerpo intermedio entre } F \text{ y } K\},$$
$$\mathcal{T} = \{H |\ H \text{ es un subgrupo del grupo de Galois de } F \preccurlyeq K\}.$$

Entonces las aplicaciones:

$$\begin{array}{rccc} \phi: & \mathcal{S} & \to & \mathcal{T} \\ & L & \mapsto & Gal_L(K) \end{array} \qquad \begin{array}{rccc} \Phi: & \mathcal{T} & \to & \mathcal{S} \\ & H & \mapsto & Inv(H) \end{array}$$

son inversa la una de la otra. Además:

(i) $H_1 \subset H_2$ si y sólo si $\Phi(H_2) \subset \Phi(H_1)$.

(ii) $\#H = [K : Inv(H)]$.

(iii) $[Gal_F(K) : H] = [Inv(H) : F]$.

(iv) H es un subgrupo normal de $Gal_F(K)$ si y sólo si la extensión $F \preccurlyeq Inv(H)$ es normal. Además, en este caso, $Gal_F Inv(H) \cong G/H$.

Para concluir esta lección damos un resultado que será de utilidad a la hora de estudiar el grupo de Galois de ciertas extensiones y que establece que si $F \preccurlyeq K$ es una extensión de Galois y L_1 y L_2 son dos cuerpos intermedios entre F y K tales que:

1) $F \preccurlyeq L_i$ sea una extensión de Galois para $i = 1, 2$,

2) $L_1 \cap L_2 = F$,

3) $F(L_1 \cup L_2) = K$,

entonces $Gal_F(K) = Gal_F(L_1) \times Gal_F(L_2)$.

TEMA 8.

CONSECUENCIAS DE LA TEORÍA DE GALOIS.

Lección 20.- Reencuentro con la Teoría de Grupos.

Lección 21.- Construcciones con regla y compás.

Lección 22.- Teorema del Elemento Primitivo.

Reencuentro con la Teoría de Grupos.

En esta lección vamos a dar los resultados de Teoría de Grupos que serán necesarios en temas los siguientes temas. Por tratarse de resultados que se encuentran en los últimos temas de la asignatura de Introducción al Álgebra, algunos años hay simplemente que recordar los conceptos mientras que otros éstos tienen que ser explicados con detalle. No obstante, los resultados en Teoría de Grupos que vamos a necesitar son los siguientes:

Comenzamos introduciendo la noción de acción de un grupo sobre un conjunto y las nociones que involucra encaminados para dar la fórmula de ecuación de clase. Con este resultado demostramos el Teorema de Cauchy que asegura que para todo número primo p que divide al orden de un grupo G existe un elemento $g \in G$ de orden p. Se introduce la noción de p-subgrupo de Sylow y se demuestra el primer Teorema de Sylow. Se define el subgrupo conmutador de un grupo G y se ven algunas propiedades asociadas a él.

Se define la serie derivada de un grupo G y la noción de grupo soluble. Se caracteriza un grupo soluble como aquél en el que existe una sucesión de subgrupos $H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G$ tales que H_i/H_{i-1} es abeliano y se demuestra que si G es finito incluso se puede conseguir que los cocientes H_i/H_{i-1} sean isomorfos a $\mathbb{Z}_{p_i}$ para ciertos p_i números primos. Por último se demuestra que S_n es soluble si y sólo si $n \leq 4$.

Finalmente, y dependiendo del tiempo del que dispongamos, se demuestran el Segundo y el Tercer Teorema de Sylow.

Construcciones con regla y compás.

Usando el Teorema Fundamental de la Teoría de Galois, se demuestra un segundo criterio de constructividad que caracteriza a los elementos construibles con regla y compás a partir de un conjunto de datos S como los elementos algebraico $\alpha \in \mathbb{C}$

tales que $[K : \mathbb{Q}(\overline{S})]$ es potencia de dos, en donde K es el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}(\overline{S})$, o lo que es equivalente, si el grupo de Galois de la extensión $\mathbb{Q}(\overline{S}) \subset K$ es un 2–grupo.

En estos momentos ya podemos demostrar que un polígono regular de n lados es construible con regla y compás si y sólo si $\phi(n) = 2^n$, en donde ϕ denota la función de Euler. Por último se demuestra que esto sucede si y sólo si $n = 2^k p_1 \cdots p_n$, con $k \in \mathbb{N}$ y los p_i primos distintos de Fermat.

Teorema del Elemento Primitivo.

Comenzamos la sección con una caracterización, dada por Steinitz, de las extensiones de cuerpos que poseen un elemento primitivo. A saber: Una extensión de cuerpos $F \preccurlyeq K$ de grado finito es simple si y sólo si existen un número finito de cuerpos intermedios entre F y K.

Como consecuencia de esta caracterización, y de un resultado visto en ejercicios que asegura que dada $F \preccurlyeq K$ una extensión finita y separable, existe un cuerpo L extensión de K tal que $F \preccurlyeq L$ es de Galois, se demuestra el Teorema del Elemento Primitivo: toda extensión finita y separable es primitiva.

TEMA 9.

RESOLUBILIDAD DE ECUACIONES POR RADICALES.

Lección 23.- Resolubilidad de ecuaciones por radicales.

Lección 24.- El grupo de Galois visto como subgrupo del grupo simétrico.

Lección 25.- Resolución de la ecuación general de grado n.

Resolubilidad de ecuaciones por radicales.

Se comienza la lección dando la noción intuitiva de polinomio resoluble por radicales. A continuación se da una definición formal de dicho concepto: una extensión de torre radical sobre un cuerpo F es una cadena de cuerpos,

$$F = F_1 \subset F_2 \subset \cdots \subset F_n$$

tal que para cada $i \in \{1, 2, \ldots, n-1\}$, $F_{i+1} = F_i(d_i)$ con $d_i^{n_i} \in F_i$ para cierto $n_i \in \mathbb{N}$. Un polinomio $f(X) \in F[X]$ se dice que es resoluble por radicales sobre F si existe una torre radical $F = F_1 \subset F_2 \subset \cdots \subset F_n$ tal que $f(X)$ se descompone en F_n.

Se define el grupo de Galois de un polinomio $f(X) \in F[X]$ como el grupo de Galois de la extensión $F \subset K$ en donde K es el cuerpo de descomposición de $f(X)$ sobre F. Se hace notar que al ser el cuerpo de descomposición único salvo isomorfismos, el grupo de Galois de un polinomio es independiente del cuerpo de descomposición que tomemos.

Lo que sigue de lección se dedica a probar el criterio de resolubilidad por radicales de Galois. A saber, si F es un cuerpo de característica cero y $f(X) \in F[X]$, entonces $f(X)$ es resoluble por radicales sobre F si y sólo si el grupo de Galois de $f(X)$ sobre F es soluble.

Para demostrar que el grupo de Galois de un polinomio resoluble $f(X) \in F[X]$, con F un cuerpo de característica cero, es soluble nos basaremos en tres hechos:

1) El grupo de Galois del polinomio $X^n - 1 \in F[X]$ es abeliano.

2) Si F contiene una raíz primitiva n-ésima de la unidad, el grupo de Galois del polinomio $f(X) = X^n - a \in F[X]$ es cíclico.

3) Si $f(X) \in F[X]$ es un polinomio resoluble por radicales, entonces existe una torre radical $F = F_1 \subset F_2 \subset \cdots \subset F_n$ tal que $f(X)$ se descompone en F_n y para cada $i \in \{1, 2, \ldots, n\}$ se tiene que $F \subset F_i$ es una extensión normal.

Para demostrar el recíproco usaremos:

1) Si $F \preccurlyeq L$ es una extensión de cuerpos, $f(X) \in F[X]$, K es el cuerpo de descomposición de $f(X)$ sobre F y E el cuerpo de descomposición de $f(X)$ sobre L, entonces $Gal_L(E)$ es isomorfo a un subgrupo de $Gal_F(K)$.

2) Si F es un cuerpo que contiene a las raíces p-ésimas de la unidad y K es una extensión de Galois de F de grado primo p, entonces existe $a \in K$ tal que $a^p \in F$ y $K = F(a)$.

El grupo de Galois visto como subgrupo del grupo simétrico.

Sea $f(X) \in F[X]$ un polinomio separable. Denotemos por K al cuerpo de descomposición de $f(X)$ sobre F, por G al grupo de Galois de $f(X)$ y por $R = \{r_1, r_2., \ldots, r_k\}$ a las raíces de $f(X)$ en K. Se pondrá de manifiesto que G puede verse, de forma natural, como un cierto subgrupo del grupo de las permutaciones de R. Es más, cada una de las órbitas de la acción de G en R se corresponde con cada uno de los conjuntos de raíces de cada uno de los factores irreducibles de $f(X)$ sobre F, por lo que si $f(X) = \prod f_i(X)_i^s$ y R_i son las raíces de $f_i(X)$ en K, G queda como subgrupo de $\oplus S_{R_i}$. De lo anterior se deduce que $f(X)$ es irreducible sobre F si y sólo si la acción de G sobre R es transitiva.

Se plantea entonces calcular el cuerpo intermedio entre F y K correspondiente, según la correspondencia de Galois, al subgrupo $A_k \cap G$ (donde A_k denota al subgrupo alternante de S_k) del grupo de Galois, concluyendo que coincide con $F(D)$ en donde $D = \prod_{1 \leq i < j \leq n}(r_i - r_j)$. Se demuestra que D^2 pertenece a F, y se le denomina discriminante de $f(X)$. Como corolario se obtiene que el grupo de Galois G es subgrupo del grupo alternante si y sólo si el discriminante de $f(X)$ es el cuadrado de algún elemento de F.

Estos dos resultados anteriores nos serán útiles para calcular, en ejercicios, el grupo de Galois de los polinomios de grado ≤ 4.

Resolución de la ecuación general de grado n.

Sea F un cuerpo. Consideremos $\{y_1, y_2, \ldots, y_n\}$, n variables y el polinomio $f(X) = (X - y_1)(X - y_2) \cdots (X - y_n)$. Se observa, en un primer lugar, que $f(X)$ habita en $F(s_1, s_2, \ldots, s_n)$, en donde cada s_k se construye a partir de las funciones simétricas racionales, es decir, $s_k = \sum_{i_1 < i_2 < \cdots < i_k} y_{i_1} y_{i_2} \cdots y_{i_k}$. Por tanto, la extensión $F(s_1, s_2, \ldots, s_n) \subset F(y_1, y_2, \ldots, y_n)$ es de Galois.

Se demuestra que el grupo de Galois de esta extensión es isomorfo a S_n, de donde se deduce, ya que la acción de G sobre las raíces es transitiva, que $f(X)$ es irreducible sobre $F(s_1, s_2, \ldots, s_n)$ y que, gracias a la Teoría de Galois, $F(s_1, s_2, \ldots, s_n)$ es el

subcuerpo de $F(y_1, y_2, \ldots, y_n)$ formado por las expresiones racionales que quedan invariantes por toda permutación de las variables $\{y_1, y_2, \ldots, y_n\}$. Por último se obtiene que la ecuación general de grado n, $n \geq 5$, no es resoluble.

Bibliografía

E. Artin, *Teoría de Galois*, Editorial Vicens-Vives, U.S.A., 1970.

J. R. Bastida, *Field Extensions and Galois Theory*, Addison-Wesley Publishing Company, California, 1984.

P. M. Cohn, *Algebra (Second Edition)*, john Wiley and Sons, 1991.

Paul Dupuy, *La vie d'Evariste Galois*, vol. 13, Annales de l'Ecole Normale serie 3, pp. 197-266.

H. M. Edwards, *Galois Theory*, Springer-Verlag, Berlin, 1984.

G. Ellis, *Rings and Fields*, Oxford Science Publications, New York, 1992.

M.H. Fenrick, *Introduction to the Galois Correspondence (Second Edition)*, Birkhäuser Boston, Basel, Berlin, 1992.

J.B. Fraleigh, *Álgebra abstracta*, Addison-Wesley Iberoamericana, 1997.

L. Gaal, *Classical Galois Theory (Third Edition)*, Chelsea Publishing Company, New York, 1979.

D.J.H. Garling, *A course in Galois theory*, Cambridge University Press, London, 1986.

C.R. Hadlock, *Field Theory and Its Classical Problems*, The Carus Mathematical Monographs (number nineteen), 1978.

I.N. Herstein, *Topics in Algebra (Second Edition)*, John Wiley and Sons. New York, 1975.

T.W.Hungerford, *Algebra*, Springer-Verlag. New York, 1974.

N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, New York, 1985.

N. Jacobson, *Basic Algebra II*, W.H. Freeman and Company, New York, 1989.

I. Kaplansky, *Fields and Rings (Second Edition)*, Chicago Lectures in Mathematics, Chicago and London, 1972.

L. Kollros, *Evariste Galois*, Kurze Mathematiker-Biographien, Birkhäuser-Verlag, Basel, 1978.