Capítulo 1

Introducción. Grupos y homomorfismos

1.1. Introducción

[1] Las permutaciones, el arma que Rejewski enarbolaba cuando cargó contra la máquina Enigma en otoño de 1932, tenían una historia milenaria, pero a diferencia de otros objetos y problemas matemáticos, no concitaron la atención de verdaderos genios hasta bien avanzado el siglo XVIII. Desde la antigüedad la enorme cantidad de ordenaciones de un mismo conjunto había llamado la atención de sabios y filósofos. Unos pocos elementos dan lugar a cientos de ordenaciones, con solo siete ya se obtienen más de cinco mil. Los matemáticos indios, siempre a la busca de magnitudes gigantescas, habían admirado los números prodigiosos que se obtienen al ordenar dos o tres docenas de piedras. Pero a pesar de este curioso efecto, todos los que habían estudiado las permutaciones con un ánimo matemático o analítico habían concluido que eran más aparatosas que instructivas, y que clasificar las miles de quasi-repeticiones que generaba un conjunto mediano no requería de más virtud intelectual que la paciencia.

Todo cambió cuando en 1770 Joseph-Louis de Lagrange decidió utilizarlas para atacar un problema que empezaba a acumular siglos. Desde el origen mismo del álgebra se habían encontrado fácilmente métodos para resolver ecuaciones de segundo, tercer y cuarto grado, expresando las soluciones en función de los coeficientes de la ecuación. En cambio, todos los que habían buscado procedimientos para resolver ecuaciones de quinto grado habían salido con las manos vacías. El plan de Lagrange para romper esa barrera era examinar cuidadosamente los métodos conocidos y construir un caso general que se pudiera utilizar no solo con las de quinto grado sino con las de cualquier grado. Sus antecesores habían buscado las soluciones, llamadas en la jerga *raíces*, de miles de ecuaciones y después las habían analizado. No habían hallado nada realmente sólido pero sí aportaron pistas prometedoras.

Por ejemplo, las soluciones de una ecuación de segundo grado están relacionadas entre sí por un conjunto de fórmulas y eso mismo sucede con las tres soluciones de una ecuación de tercer grado y con las cuatro soluciones de una ecuación de cuarto grado. Las fórmulas varían en cada uno de estos tres casos pero tienen una curiosa propiedad en común, son las mismas con algunos cambios del orden de las soluciones. De todos

[1] La presente introduccion está copiada, prácticamente, de la página Kriptópolis de Román Ceanos, en el apartado de Enigma (ver `http://kriptopolis.com`).

los valores con que es posible sustituir las variables de esas fórmulas, solo son conjuntos de soluciones del polinomio aquellos cuyo orden se puede intercambiar. Es decir, las soluciones de una ecuación son los números que cumplen una serie de fórmulas pero solo aquellos que pueden ser intercambiados entre sí dentro de estas. Las ecuaciones de segundo grado solo tienen dos soluciones y por tanto estas solo pueden ordenarse de dos maneras, pero las de cuarto grado tienen cuatro soluciones que se pueden ordenar de 24 maneras, proporcionando un material mucho más jugoso para el análisis. No existía una doctrina clara pero se sabía que solo algunos reordenamientos eran aceptables como criterio. Lagrange estudió qué tenían en común los que eran aceptables y para ello trajo las permutaciones al centro del debate matemático de su época. Lagrange realizó muchos descubrimientos y su nombre es familiar a cualquier estudiante de matemáticas, pero en el caso concreto de las ecuaciones de quinto grado sus esfuerzos fueron vanos. No encontró ninguna forma general de resolverlas aunque tampoco quedó convencido de que fuera imposible. Muchos matemáticos soñaban con la fama que les daría ser los descubridores de un método que llevaría para siempre su nombre.

Paolo Ruffini pertenecía a la generación siguiente y era un experto en álgebra de polinomios. Estaba convencido que el fracaso de Lagrange y de todos sus antecesores debía tomarse como prueba empírica de que para las ecuaciones de quinto grado no podían construirse las fórmulas que permitían hallar soluciones a partir de los coeficientes, como se hacía en las ecuaciones de grado menor y que por tanto no tenían solución. Esta opinión no era compartida por nadie, pero Ruffini, convencido de tener razón, decidió demostrar algebraicamente la imposibilidad de la existencia de tales fórmulas. Para ello retomó el estudio de Lagrange sobre los *reordenamientos* de las soluciones pero subiendo un paso en la escala de abstracción. En lugar de trabajar con los ordenamientos en sí, definió las transformaciones de una ordenación en otra y las llamó *permutazioni*. Así caracterizó un conjunto en el que las propias *permutazioni* eran los elementos y estudió sus propiedades. Si se combinan dos *permutazioni* de cambio de orden entre sí se obtiene una tercera, pero el orden en que se haga la combinación afecta al resultado (al contrario de lo que pasa p.e. con la suma y la multiplicación). Sobre este armazón de una incipiente álgebra de permutaciones edificó Ruffini su demostración sobre la insolubilidad de las quínticas. Cada uno de los conjuntos de cinco soluciones tendría 120 ordenamientos posibles, pero solo algunos serían aceptables. La estructura de estos sería producto de las fórmulas que debían permitir hallar los conjuntos de cinco soluciones. Ruffini buscaba probar la inexistencia de las formulas demostrando la imposibilidad de esas estructuras. Una vez terminada la demostración se la envió al ya anciano Lagrange pero pasaron los meses y este no le contestó. Ruffini pensó que su demostración era demasiado complicada y que Lagrange no la había podido descifrar. La reconstruyó simplificando muchos pasos y justificando con más detalle las partes que utilizaban notación novedosa. Para ello se adentró más y más en el estudio de las permutaciones, describiendo una taxonomía completa que constaba de dos clases –semplize y composta– y tres subtipos dentro de la segunda clase. Nuevamente solo recibió silencio de parte de Lagrange. Esta vez además, recibió cartas de amigos que se hacían eco de los rumores que corrían sobre errores en su demostración. Ruffini la repasó una y otra vez, mejorándola y perfeccionándola sin encontrar esos supuestos errores pero sin lograr que fuera aceptada. El problema era que la combinación de dos permutaciones para formar una tercera resultaba demasiado abstracta incluso para Lagrange, que había estado muy cerca de formalizar el concepto. La falta de reconocimiento de su trabajo matemático hizo que Rufini se decantara hacia su segunda profesión, la de médico. Murió en 1821 tras unos últimos años de vida muy

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

condicionados por las secuelas de un tifus que cogió tratando a sus pacientes. La de Ruffini es una historia trágica de incomprensión que tiene sin embargo una coda amable que puede hacer las veces de irónico final feliz. Un año antes de morir, se enteró que Agustin-Louis Cauchy, el coloso llamado a refundar toda la matemática, había aceptado su demostración y le había dedicado uno de los pocos halagos que dirigió nunca a alguien que no fuera el mismo. El chiste final es que Cauchy estaba equivocado y aunque el resultado de Ruffini era cierto, la demostración contenía un error como muchos habían afirmado sin saber ni de qué hablaban. El motivo por el que Cauchy no se apercibió del error de Ruffini era que apenas utilizaba los resultados de los demás sin reformularlos de arriba a abajo. Cuando Cauchy trabajaba sobre un tema, lo hacía con el impulso de un urbanista moderno. Al igual que estos arrasaban las intrincadas callejas de los centros medievales para construir barrios de amplias avenidas y manzanas cuadradas, Cauchy hacia tabula rasa de siglos de notación confusa y definiciones ambiguas. Redactaba de nuevo todos los axiomas y colocaba cada uno en su lugar para construir sobre ellos un solido entramado de teoremas y corolarios. En el barrio de la majestuosa ciudad que construyó Cauchy, uno de los edificios estaba dedicado a las permutaciones. No era muy grande ni muy vistoso porque el tema no tenía la vastedad conceptual ni la belleza de otros objetos matemáticos, pero contenía todo lo que se podía decir sobre el tema, ordenado y sistematizado con elegancia y precisión. Como no les daba más importancia que la instrumental, el libro sobre permutaciones fue uno de los últimos que publicó. Allí se establecía la notación moderna de ciclos, se actualizaba la taxonomía de Ruffini, se enumeraban las propiedades de las combinaciones de permutaciones y se describía el teorema de las conjugadas que tan útil sería a Rejewski casi un siglo más tarde.

Cauchy puso en el mapa a las permutaciones y les dio el marchamo de alta matemática que les permitiría participar en el mayor acontecimiento matemático del siglo XIX. Lo protagonizaron dos románticos personajes que practicaban la matemática con una voluntad mucho más artística que científica, nada que ver con el institucionalismo feroz de Cauchy y sus compañeros de la Ŕcole Polytechnique. Ellos demostraron de una vez por todas la insolubilidad de las ecuaciones de quinto grado y de paso fundaron el álgebra moderna.

El primero era Niels Henrik Abel, el hijo del párroco luterano de un remoto pueblo noruego que llegó a Paris en 1826, con solo 24 años, trayendo un folio por las dos caras en que demostraba la imposibilidad de resolver ecuaciones de quinto grado. Entregó el folio a Joseph Fourier, a la sazón secretario de la Academia de las Ciencias quien encontró la letra muy apretada, la tinta demasiado clara y la notación muy deforme por lo que se lo entregó a Cauchy para que lo descifrara. Este último lo extravió por los cajones de su lugar de trabajo y se olvidó del tema. Abel esperó respuesta unos meses pero al final volvió a su país natal para morir de tuberculosis a los 27 años sin haber visto reconocido su trabajo. Años más tarde Cauchy fue obligado a buscar el documento hasta encontrarlo y eso hizo que se haya conservado hasta nuestros días.

El segundo fue Evariste Galois, otro romántico joven que murió a los veinte años en un duelo. Su muerte sucedió dos años después que la de Abel y la leyenda del primero se mezcló curiosamente con la del segundo. Galois también presentó a Fourier una prueba de la insolubilidad de las quínticas utilizando el álgebra de permutaciones. Este también se la dio a Cauchy que tampoco le dio curso. En este caso sin embargo parece que la negligencia no fue tan grande sino que hubo algunos accidentes –la muerte de Fourier y Galois– y malentendidos que el antecedente de Abel hizo ver a los historiadores bajo una luz exagerada.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Aunque no se conocieron, ambos utilizaron la misma metodología: el estudio de la estructura del conjunto de permutaciones que se pueden aplicar a las raíces de un polinomio sin que dejen de cumplirse las ecuaciones que relacionan dichas variables. Resultó que la estrategia de Lagrange era correcta y que el camino para demostrar la diferencia entre el quinto grado y los grados menores, era proyectar en los conjuntos de soluciones las restricciones que impone el álgebra de permutaciones. Para encontrar esas restricciones, Galois había creado un vocabulario matemático que describía de manera precisa lo que era posible y lo que era imposible cuando se combinan permutaciones. A esas alturas el problema de las soluciones a las ecuaciones de quinto grado ya no era perentorio porque existían nuevas técnicas de encontrarlas, hasta el punto que la forma tradicional ahora tenía nombre, *solución por radicales*, para diferenciarla del resto de métodos. Lo que dio a Galois (y a Abel hasta cierto punto) fama inmortal fue que el vocabulario matemático creado para describir el mundo de las permutaciones funciona con más o menos restricciones para la mayoría de objetos matemáticos. Las permutaciones fueron las operaciones sobre las que primero se describió la estructura matemática llamada *grupo* , considerado el hallazgo matemático más importante de todos los tiempos. Aunque la abstracción en sentido moderno significa alejarse de la realidad para poder construir estructuras comunes a muchas partes de esta, en la forma de ver las cosas anterior a Gödel, esa misma abstracción era percibida como vislumbrar los principios fundamentales que dan forma a los mecanismos matemáticos que crean las irregularidades que percibimos en la aritmética, la geometría, el análisis y el cálculo.

En el otoño de 1932 Rejewski se dió cuenta que Enigma era una máquina de generar permutaciones y que el álgebra descrita por Cauchy –que Galois había generalizado– era el lenguaje en que se debía escribir el conjuro que la rompería.

1.2. Definiciones, ejemplos y primeras propiedades

Definición 1.1. Un grupo G es un conjunto con una operación binaria interna asociativa, con elemento neutro e inverso para cada elemento. Con notación multiplicativa, la operación se denota $\cdot$, o simplemente por yuxtaposición, el neutro se denota 1 y el inverso de g se denota g^{-1}. Es decir, para elementos $g, h, z \in G$ cualesquiera se tiene:

i) $(gh)z = g(hz)$,

ii) $1 \cdot g = g \cdot 1 = g$,

iii) $gg^{-1} = g^{-1}g = 1$.

Ejemplo 1.2. Sea E el conjunto de los puntos de un espacio afín euclídeo (se conoce desde el bachillerato y se ha desarrollado en álgebra lineal). Recuerda que un movimiento es una aplicación biyectiva que conserva las distancias entre los puntos.

Se tiene que la composición de movimientos es movimiento y la inversa de un movimiento también lo es. Así que el conjunto de todos los movimientos es un grupo con la operación composición.

Dado un conjunto A de puntos del espacio (por ejemplo los vértices de un poliedro) pensemos en los movimientos f que dejan invariante ese conjunto de puntos, es decir $P^f \in A$ para todo $P \in A$. Este conjunto de movimientos que fijan A es claramente un grupo (de transformaciones de A). Al grupo de los movimientos que dejan fijo un poliedro se le llama grupo de simetrías del poliedro.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Estudiando geometría lineal se sabe que los movimientos que dejan fijo algún punto son giros (o rotaciones) alrededor de un eje, simetrías respecto de un plano (ó reflexiones) y composiciones de rotaciones y reflexiones respecto de un plano perpendicular al eje. De estos, son movimientos directos los giros. A los otros se les llama inversos (¿encuentras una explicación?)

Ejercicio 1.3. Describe el grupo de rotaciones y el de simetrías de los prismas y pirámides rectas de base polígono regular de 4 y 5 lados. En general, para $n > 3$ lados.

Ejercicio 1.4. Describe el grupo de simetrías de un tetraedro regular.

Ejercicio 1.5. Describe el grupo de rotaciones de un cubo.

Ejemplo 1.6. Son ejemplos de grupos:

- $\mathbb{Z}$. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma ordinaria.
- Las unidades de un anillo con la multiplicación, en particular los elementos no nulos de un cuerpo.
- Conjunto S_n de todas las aplicaciones biyectivas de un conjunto de n elementos en sí mismo (grupo de permutaciones de grado n).
- $GL(n, K)$ con la multiplicación de matrices, que se llama grupo general lineal, donde $GL(n, K)$es el conjunto de matrices cuadradas $n \times n$ de rango n sobre el cuerpo K.
- El subconjunto de $\mathbb{C}$, $C = \{a + bi | a^2 + b^2 = 1\} = \{e^{i\varphi} | 0 \leq \varphi \rangle 2\pi\}$ con la multiplicación de complejos, que se llama grupo circular.
- $C_n = \{e^{2\pi ki/n} | k = 1, 2, \cdots, n\}$ con la multiplicación de complejos (grupo cíclico de orden n).

Ejemplo 1.7. Sea $X = \{x_1, \ldots, x_n\}$ un conjunto finito de símbolos (también podría ser un conjunto arbitrario). Ponemos $X^- = \{x_1^{-1}, \ldots, x_n^{-1}\}$. Consideramos el conjunto de sucesiones finitas (palabras) de elementos en $X \cup X^-$ y llamamos 1 a la palabra vacía. Además, identificamos dos palabras w y w' si una se puede obtener a partir de la otra eliminando o añadiendo subpalabras de la forma $x_i x_i^{-1}$ ó $x_i^{-1} x_i$. El conjunto que se obtiene al hacer estas identificaciones es un grupo con la operación de yuxtaposición. Este grupo se llama *grupo libre* en X y se denota $F(X)$.

Proposición 1.8. *En todo grupo G se tiene:*

a) El neutro es único.

b) El inverso es único.

c) Si $uv = 1$, entonces $u^{-1} = v$ y $v^{-1} = u$.

d) Para todo $g \in G$, la aplicación $G \to G$ que asocia a cada $x \in G$ el elemento xg es una biyección en G.

e) Para todo $g \in G$, la aplicación $G \to G$ que asocia a cada $x \in G$ el elemento gx es una biyección en G.

Demostración. Ejercicio. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

1.3. Subgrupos, coclases y subgrupos normales

Definición 1.9. Un *subgrupo* H de un grupo G es un subconjunto de G que con la operación restringida es también grupo. Se escribe $H \leq G$.

Por ejemplo, los grupos de simetrías de un poliédro en $\mathbb{R}^3$ son subgrupos del grupo de todos los movimientos del espacio. El grupo de todos los movimientos del espacio es subgrupo del grupo de todas las permutaciones posibles de los puntos (aplicaciones biyectivas del espacio en sí mismo).

$SL(n, K)$ el conjunto de las matrices $n \times n$ con determinante 1 es un subgrupo de $GL(n, K)$. A $SL(n, K)$ se le llama grupo especial lineal.

Proposición 1.10. *Sea G un grupo.*

a) Si H es un subconjunto no vacío de G, H es subgrupo si y solo si $xy^{-1} \in H$ para todo $x, y \in H$.

b) La intersección de una familia cualquiera de subgrupos es subgrupo.

c) Si H es un subconjunto finito no vacío de G, H es subgrupo si y solo si $xy \in H$ para todo $x, y \in H$.

Demostración. Ejercicio.

□

Notación Si $K \subseteq G$ denotamos $\langle K \rangle$ al menor subgrupo de G que contiene a K (la intersección de todos los subgrupos que contienen a K). A $\langle K \rangle$ se le llama subgrupo generado por K. Si $\langle K \rangle = G$ se dice que K genera G o que es una familia generadora.

Sean $X, Y \subseteq G$. Se denota $XY = \{xy \,|\, x \in X, y \in Y\}$.

Proposición 1.11. *Sea G un grupo con dos subgrupos finitos H, K. Se tiene que*

$$|HK| = |H|\,|K| \,/\, |H \cap K|$$

Demostración. Ejercicio. □

Si G es un grupo finito llamaremos *orden* de G al número de sus elementos, se denota mediante $|G|$.

Proposición 1.12. *Si H, K son subgrupos finitos de un grupo G, se tiene que HK es subgrupo de G si y solo si $HK = KH$.*

Demostración. Ejercicio. □

Ejercicio 1.13. Prueba el resultado anterior pero sin la hipótesis de que G es finito.

Ejercicio 1.14. Encuentra en S_3 dos subgrupos H y K tales que HK no es subgrupo.

Definición 1.15. Si H es un subgrupo de G y $x \in G$ al conjunto $Hx = \{hx | h \in H\}$ se le llama *clase* a derecha de x módulo H (o coclase). Al conjunto $xH = \{xh | h \in H\}$ se le llama clase izquierda de x módulo H. En general $Hx \neq xH$ aunque ambos conjuntos contienen a x.

Proposición 1.16. *Sean H subgrupo de G ($H \leq G$), $x, y \in G$. Se tiene:*

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

(a) Hx *e* yH *son biyectivos con* H*.*

(b) $xH = yH$ *si y solo si* $y \in xH$*.*

(c) $xH \cap yH \neq \emptyset$ *si y solo si* $xH = yH$*. Así las clases a izquierda (también las clases a derecha) forman una partición de* G*.*

Demostración. Ejercicio. □

Definición 1.17. Si $H \leq G$, llamaremos *índice* de H en G al número de clases a derecha y lo denotamos $|G : H|$. El teorema de Lagrange 1.18 implica que $|G : H|$ es también el número de clases a izquierda de H en G.

Teorema 1.18 (Lagrange)**.** *Sea* G *finito y* H *subgrupo de* G*. Se tiene*

$$|G| = |G : H|\,|H|.$$

Demostración. Por (b) de la proposición 1.16 $|Hx| = |H| = |xH|$ para todo x, luego todas las clases tienen el mismo número de elementos y por (d) son disjuntas. □

Ejercicio 1.19. Sea G un grupo finito, $H \leq K \leq G$. Prueba que

$$|G : H| = |G : K||K : H|.$$

En general la operación producto de clases a derecha (o a izquierda) no está bien definida. Se puede ver que la condición necesaria y suficiente para multiplicar coclases (por herencia de la multiplicación en G) es la siguiente.

Definición 1.20. Un subgrupo N de G se dice *subgrupo normal* y se escribe $N \trianglelefteq G$ si se verifica

$$xN = Nx,$$

para todo $x \in G$. Esta condición es equivalente a $x^{-1}Nx = N$ para todo $x \in G$.

Observación 1.21. Para probar que un subgrupo N es normal basta probar que para todo $x \in G$, $x^{-1}Nx \subseteq N$. Esto es trivial en el caso finito, ya que ambos conjuntos tienen el mismo número de elementos, luego si se cumple un contenido se ha de tener también la igualdad. En el caso general, si se cumple esa condición, entonces considerando un $x \in G$ y su inverso, tenemos $x^{-1}Nx \subseteq N$ y $xNx^{-1} \subseteq N$ y de esto último se deduce $N \subseteq x^{-1}Nx$

Notemos que si G es abeliano todos sus subgrupos son normales.

Proposición 1.22. *Sea* $N \trianglelefteq G$ *y* $H \leq G$*. Se tiene que* $NH = HN \leq G$*.*
Además

$$N \cap H \trianglelefteq H$$

Demostración. Para todo $x \in H$ se tiene que $x^{-1}(H \cap N)x \subseteq x^{-1}Nx \subseteq N$ pues $N \trianglelefteq G$. Además $x^{-1}(H \cap N)x \subseteq H$ por ser $x \in H$, luego se tiene

$$x^{-1}(H \cap N)x \subseteq H \cap N$$

y $H \cap N \trianglelefteq H$

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

La siguiente proposición es de demostración fácil.

Proposición 1.23. *Sea $N \trianglelefteq G$. El conjunto $G/N = \{xN | x \in G\}$ es grupo con la operación*

$$(xN)(yN) = xyN$$

para todo $x, y \in G$, denominado grupo cociente. El neutro de G/N es N.

Ejercicio 1.24. Sea H un subgrupo de G que no es normal en G. Prueba que para todo par $x, y \in G$, existen $x' \in Hx$, $y' \in Hy$ tales que $x'y' \notin Hxy$.

1.4. Homomorfismos y conjugación

Definición 1.25. Un homomorfismo entre dos grupos $(G, .)$ y $(H, .)$ es una aplicación $f : G \to H$ tal que $f(ab) = f(a)f(b)$ para todo $a, b \in G$ (conserva la operación).

Un homomorfismo biyectivo se llama isomorfismo (se trata casi del mismo grupo con distintos nombres de los elementos).

Ejercicio 1.26. a) Prueba que los grupos $(\mathbb{Z}_n, +)$ y $(C_n, .)$ son isomorfos.

b) Establece distintos homomorfismos de C_n en C_n.

Proposición 1.27. *Sea f un homomorfismo entre $(G, .)$ y $(H, .)$. Se tiene*

a) $f(1) = 1$ y para todo $a \in G$, $f(a^{-1}) = (f(a))^{-1}$.

b) Se define $\ker f = \{a \in G | f(a) = 1\}$ (núcleo de f) y se tiene que $\ker f \trianglelefteq G$

c) Se define $\mathrm{im} f = f(G) = \{f(a) | a \in G\}$ (imagen de f) y se tiene que $\mathrm{im} f \leq H$ (es subgrupo de H).

d) $\ker f = 1$ si y solo si f es inyectiva.

e) La composición de homomorfismos de grupos es homomorfismo.

f) La inversa de un isomorfismo es isomorfismo.

Demostración. Ejercicio. □

Ejercicio 1.28. Sea $f : G \to H$ un homomorfismo suprayectivo. Prueba que si $N \trianglelefteq G$, $f(N) \trianglelefteq H$

Ejercicio 1.29. Sea $f : G \to H$ homomorfismo y $Y \leq H$. Se tiene que $f^{-1}(Y) = \{x \in G \,|\, f(x) \in Y\} \leq G$.

Proposición 1.30 (Teorema de isomorfía)**.** *Sea $f : G \to H$ homomorfismo. La aplicación*

$$\overline{f} : G/\ker f \to f(G),$$

dada por $\overline{f}(x \ker f) = f(x)$, es un isomorfismo de grupos.

Demostración. Ejercicio. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Nota Si tenemos un homomorfismo inyectivo $f : G \to H$, se tiene que G es isomorfo a un subgrupo de H. Y si renemos un homomorfismo suprayectivo $f : G \to H$, se deduce que $G/\ker f \cong H$.

Proposición 1.31. *Sea $N \trianglelefteq G$.*

a) La aplicación $\pi : G \to G/N$ dada por $\pi(g) = gN$ es un homomorfismo suprayectivo y si $H \leq G$, $\pi(H) = HN/N$.

b) Existe una biyección entre el conjunto $\{N \subseteq K \leq G\}$ y el conjunto de los subgrupos de G/N dada por $K \to K/N$. Además $K \trianglelefteq G$ si y solo si $K/N \trianglelefteq G/N$

c) Si $H \leq G$, entonces $H \cap N \trianglelefteq H$ y

$$H/H \cap N \simeq NH/N.$$

d) Si $M \trianglelefteq G$ con $N \subseteq M$, entonces

$$G/M \simeq G/N/M/N.$$

Demostración. a) Es claro que π es un homomorfismo. Si $h \in H$, $\pi(h) = hN \in HN/N$. Recíprocamete si $hn \in HN$, se tiene que $hnN = hN = \pi(h)$.

b) Dado un $N \subseteq K \leq G$ le asociamos el subgrupo imagen por la aplicación del apartado a) que es K/N. Si tenemos un subgrupo Y de G/N, por el ejercicio 1.29, $f^{-1}(Y) = K$ es un subgrupo de G y además $N \subseteq K$ pues $f(N) \subseteq Y$. Es claro que estas correspondencias son inversas una de la otra, luego son una biyección.

Por el ejercicio anterior se tiene la correspondencia entre subgrupos normales.

c) Consideramos la restricción de la aplicación π del apartado a) al subgrupo H, $H \to G/N$ que tiene de imagen HN/N y de núcleo $H \cap N$. Por el teorema del isomorfismo se tiene la tesis.

d) Consideramos la aplicación $G/N \to G/M$ dada por $gN \to gM$. Veamos que está bien definida.

Sea $xN = yN$ se tiene que $y^{-1}x \in N \subseteq M$ luego $xM = yM$.

Es claramente un homorfismo suprayectivo, el núcleo es $\{gN | g \in M\} = M/N$ y por el teorema del isomorfismo se tiene la tesis.

□

Ejercicio 1.32. (optativo) Considera el grupo $GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \,|\, A \text{ es regular}\}$ con el producto de matrices. Sea E es el conjunto de puntos del espacio $\mathbb{R}^3$, identificando cada punto con una terna $(x, y, z) \in \mathbb{R}^3$ de modo que la distancia entre dos puntos (x, y, z), (x', y', z'), es $\sqrt{(x - x')^2 + (y - y')^2 + (z - z')^2}$.

Establece (de modo natural) un homomorfismo entre $GL(3, \mathbb{R})$ y S_E. ¿Es inyectivo, suprayectivo o biyectivo?

Ahora considera $O_n = \{P \in GL(n, \mathbb{R}) | PP^t = I_n\}$. Ver que es subgrupo de $GL(n, \mathbb{R})$. Prueba que las imágenes de los elementos de O_3 por el homomorfismo que has definido antes son movimientos que fijan en origen de coordenadas (es decir, son aplicaciones que preservan distancias). En realidad los movimientos de este tipo son precisamente los que proceden de O_3 (grupo ortogonal).

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Nota Sea G un grupo. El conjunto de todos los automorfismos de G con la composición de aplicaciones, es un grupo que llamamos grupo de los automorfismos de G, $\mathrm{Aut}(G)$. Dado un elemento $\alpha \in \mathrm{Aut}(G)$ a veces será más conveniente denotar la acción de α en el grupo de la forma habitual, es decir, como $\alpha(x)$ para $x \in G$ y a veces de forma exponencial, es decir, como x^α. Para pasar de la una a la otra definimos la notación exponencial así:

$$x^\alpha := \alpha^{-1}(x).$$

Equivalentemente, $\alpha(x) = x^{\alpha^{-1}}$.

Proposición 1.33. *Sea G un grupo y $g \in G$. Denotamos $x^g = g^{-1}xg$ y lo llamamos conjugado de x por g. Se tiene*

a) La aplicación $G \to G$ definida exponencialmente por $x^{\alpha_g} := x^g$ (equivalentemente, $\alpha_g(x) = x^{\alpha_g{}^{-1}} = x^{g^{-1}}$), es un automorfismo de G.

b) $\alpha_g\alpha_h = \alpha_{gh}$ para $g, h \in G$.

Demostración. Ejercicio. □

Proposición 1.34. *Los automorfismos de G que son de la forma α_g se llaman internos. El conjunto de los automorfismos internos de G, $\mathrm{Int}(G)$ es un subgrupo normal de $\mathrm{Aut}(G)$.*

Demostración. Ejercicio. Si se usa notación exponencial, hay que ver que $(\alpha_g)^\beta = \beta^{-1}\alpha_g\beta = \alpha_{g^\beta}$. □

1.5. Grupos cíclicos. Orden de un elemento

Definición 1.35. Sea $x \in G$, al conjunto $\langle x\rangle = \{x^n \mid n \in Z\}$ (se conviene que $x^0 = 1$ y $x^n = x \cdots x$, n-veces y $x^{-n} = (x^{-1})^n$) se le llama *subgrupo generado* por el elemento x (ver que efectivamente es un subgrupo).

Un grupo G se dice *cíclico* si existe $x \in G$ tal que $G = \langle x\rangle$.

Ejemplos El grupo de las rotaciones de una pirámide de base n-ágono regular es cíclico y es isomorfo al grupo aditivo $\mathbb{Z}_n$.

$(\mathbb{Z}, +)$ es cíclico.

$(\mathbb{Q}, +)$ es un grupo abeliano que no es cíclico.

Proposición 1.36. *Los subgrupos de $(\mathbb{Z}, +)$ son $n\mathbb{Z} = \{nx \mid n \in \mathbb{Z}\}$.*

Demostración. Para cada subgrupo H de $\mathbb{Z}$ tomar el menor n positivo tal que $n \in H$ y ver que $H = n\mathbb{Z}$. □

Proposición 1.37. *Todo grupo cíclico es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.*

Demostración. Sea $G = \langle x\rangle$, la aplicación $\mathbb{Z} \to \langle x\rangle$ definida por $m \to x^m$ es un homomorfismo suprayectivo. Por el teorema del isomorfía se tiene el resultado. □

Proposición 1.38. *Todo subgrupo de un grupo cíclico es cíclico.*

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Demostración. Si el grupo es infinito es isomorfo a $\mathbb{Z}$ y ya hemos visto que los subgrupos de $\mathbb{Z}$ son $n\mathbb{Z} = \langle n \rangle$. Supondremos ahora que G es finito. Sea $G = \langle x \rangle$ y $H \leq G$. Si $H = \{1\}$ obviamente es cíclico. En otro caso sea d el menor entero positivo tal que $x^d \in H$. Veamos que $H = \langle x^d \rangle$. Sea n tal que $x^n \in H$. Por el algoritmo de la división en $\mathbb{Z}$ se tiene $n = cd + r$ con $r < d$ y $x^n = (x^d)^c x^r$ Como x^n y $(x^d)^c$ están en H se tiene que $x^r \in H$ y por la minimalidad de d tiene que ser $r = 0$ luego $x^n = (x^d)^c$. □

Definición 1.39. Sea $x \in G$. Si existe un natural n tal que $x^n = 1$, al menor tal n se le llama *orden* de x. Si no existe n se dice que x no tiene orden finito o que es de orden infinito.

Notemos que si x tiene orden n, se tiene que $x^{-1} = x^{n-1}$, así que todas las potencias de exponente negativo son potencias también de exponente positivo y

$$\langle x \rangle = \{1, x, \cdots, x^{n-1}\}.$$

Para el siguiente resultado, recordar que ϕ denota a la función de Euler, es decir, si $0 < n$ es un entero,

$$\phi(n) = |\{0 < s < n \mid s, n \text{ son relativamente primos}\}|.$$

Proposición 1.40. *Si G es un grupo cíclico de orden n se tiene:*

a) Todo elemento tiene orden divisor de n,

b) Para todo d divisor de n hay exactamente $\phi(d)$ elementos de G de orden d.

c) Para todo d divisor de n existe un único subgrupo de orden d.

Demostración. El apartado a) se deduce del Teorema de Lagrange.

Ahora, sea x tal que $G = \langle x \rangle$ y ponemos k tal que $n = kd$. Para el apartado b) vamos a probar que un elemento de G tiene orden d si y solo si es de la forma x^{ks} con d y s relativamente primos.

Suponemos primero que el elemento x^i tiene orden d. Entonces, $x^{id} = 1$ luego n divide a id, es decir, para cierto s se tiene $id = ns = dks$ luego $i = ks$. Veamos ahora que s y d son relativamente primos. Si no lo fueran, tendríamos que existe algún primo p que divide a ambos, es decir, $s = ps_1$ y $d = pd_1$ con $d_1 < d$. Por lo tanto

$$(x^i)^{d_1} = x^{ksd_1} = x^{kps_1d_1} = x^{ks_1d} = x^{ns_1} = 1$$

lo que contradice el que el orden de x^i sea d.

A la inversa, tenemos que ver que si d y s son relativamente primos, el elemento x^{ks} tiene orden d. Claramente $(x^{ks})^d = x^{ksd} = x^{ns} = 1$. Supongamos que el orden es menor que d, es decir, que existe un $0 < d_1 < d$ con $x^{ksd_1} = 1$. Por la identidad de Bezout existen t, r con $1 = td + rs$. Por tanto $x = x^{td}x^{rs}$ luego

$$x^{kd_1} = x^{tdkd_1}x^{rskd_1} = 1$$

pero como $0 < d_1 < d$, $0 < kd_1 < kd = n$ lo que contradice el que x tiene orden n.

Nos falta probar c), pero notemos que es consecuencia de a): por un lado, si k es como antes, el subgrupo $H = \langle x^k \rangle$ tiene orden d luego en H hay exactamente $\phi(d)$ elementos de orden d. Como en todo G también hay exactamente $\phi(d)$ elementos de orden d, todos están en H así que no puede haber ningún otro subgrupo de orden d (recordemos que todos los subgrupos de G son cíclicos). □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Corolario 1.41. *Si G es cíclico con n elementos, tiene exactamente $\phi(n)$ generadores distintos*

Ejercicio 1.42. Para todo $n \in \mathbb{N}$, se tiene que

$$\sum_{d|n} \phi(d) = n.$$

Ejercicio 1.43. Sea p primo y $x \in \mathbb{Z}$ que no es múltiplo de p. Prueba que $x^{p-1} \equiv 1$ (módulo p) (pequeño teorema de Fermat).

Ejercicio 1.44. Sea G cíclico de n elementos, describe los elementos de $\mathrm{Aut}(G)$ y comprueba que es un grupo abeliano.

1.6. Productos de grupos

Proposición 1.45. *Sean N y M dos subgrupos normales de G tales que $M \cap N = 1$. Para todo $n \in N$ y $m \in M$ se tiene que $mn = nm$.*

Demostración. Se tiene que $n^{-1}m^{-1}nm \in N \cap M = 1$ luego $nm = mn$. □

Proposición 1.46. *a) Sean G_1 y G_2 grupos. El producto cartesiano (conjunto de pares ordenados) $G_1 \times G_2$ con la operación $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$ para cada $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$ es un grupo que se llama producto directo de G_1 y G_2y se denota $G_1 \times G_2$. Este grupo tiene un subgrupo normal isomorfo a G_1 y otro isomorfo a G_2 con intersección trivial y producto todo el grupo.*

b) Si G es un grupo y $N_1, N_2 \trianglelefteq G$ tales que $N_1 \cap N_2 = 1$ y $N_1N_2 = G$. Se tiene que $G \simeq N_1 \times N_2$. Se dice que G es producto directo de N_1 y N_2.

Demostración. Ejercicio. □

Ejercicio 1.47. Repasa los grupos abelianos finitos.

Proposición 1.48. *a) Si $N \trianglelefteq G$ y $H \leq G$ tales que $NH = G$ y $H \cap N = 1$, se tiene que cada $g \in G$ se escribe de manera única como $g = nh$ con $n \in N$, $h \in H$. Además la operación de G se puede realizar a través de las N y H mediante*

$$g_1g_2 = n_1h_1\, n_2h_2 = n_1n_2^{h_1^{-1}}h_1h_2.$$

b) Sea $\varphi : H \to \mathrm{Aut}(N)$ un homorfismos de grupos. En el producto cartesiano $N \times H$ definimos la operación $(n_1, h_1)(n_2, h_2) = (n_1n_2^{\varphi(h^{-1})}, h_1h_2)$. Se tiene que es un grupo que se llama producto semidirecto de H por N vía φ y se denota $[N]H$ o $N \rtimes H$.

c) Si $N \trianglelefteq G$ y $H \leq G$ tales que $NH = G$ y $H \cap N = 1$, podemos definir $\varphi : H \to \mathrm{Aut}(N)$ dado por $n^{\varphi(h)} = n^h$. Se tiene que G es isomorfo al producto semidirecto de H por N vía φ.

Demostración. Ejercicio. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Ejemplo 1.49. Sea $H = \langle x \rangle$ un grupo cíclico de orden 2 y $N = \langle y \rangle$ un grupo cíclico de orden n. Sea

$$\varphi : H \to \mathrm{Aut}N$$

definida por $\varphi(1) = 1_N$ y $\varphi(x) : N \to N$ dada por $n^{\varphi(x)} = n^{-1}$ para todo $n \in N$. Se tiene que $\varphi(x)$ es automorfismo de N por ser N abeliano. Es claro que φ es un homorfismo.

El producto semidirecto de H por N vía φ tiene $2n$ elementos, que son

$$(1,1), (y,1), (y^2,1), \cdots, (y^{n-1},1), (1,x), (y,x), (y^2,x), \cdots, (y^{n-1},x)$$

y la operación es $(n,1)(n',1) = (nn',1)$, $(n,1)(n',x) = (nn',x)$, $(n,x)(n',1) = (n(n')^{-1},x)$, $(n,x)(n',x) = (n(n')^{-1},1)$,$(n,1)(n',x) = (nn',x)$.

Ejercicio 1.50. Prueba que un grupo G tal que para todo $x \in G$, $x^2 = 1$, es un grupo abeliano.

Ejercicio 1.51. Prueba que todo grupo de orden primo es cíclico.

Ejercicio 1.52. Prueba que dos grupos cíclicos de orden n, son isomorfos.

Ejercicio 1.53. Prueba que en cualquier grupo todo subgrupo de índice dos es normal.

Ejercicio 1.54. Consideremos los elementos de $GL(2,\mathbb{C})$ siguientes:

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \; b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Prueba que $Q_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b \rangle$ es un subgrupo de $GL(2,\mathbb{C})$ de orden 8. Prueba que este grupo se puede escribir como

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

con las relaciones $ij = k$, $ki = j$, $jk = i$, $ji = -k$, $ik = -j$, $kj = -i$, $i^2 = j^2 = k^2 = -1$.

Ejercicio 1.55. Sea n un entero positivo. Consideremos los elementos de $GL(2,\mathbb{C})$ siguientes:

$$a = \begin{pmatrix} \xi & 0 \\ 0 & \overline{\xi} \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

donde $\xi = e^{2\pi i/n} \in \mathbb{C}$.

a) Prueba que el orden de a es n, el orden de b es 2 y que $bab = a^{-1}$.

b) Prueba que $D_{2n} = \{1, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots a^{n-1}b\}$ es un subgrupo de $GL(2,\mathbb{C})$ de orden $2n$.

c) Prueba que este grupo es isomorfo al del último ejemplo.

Ejercicio 1.56. Prueba que el grupo de los movimientos del plano que dejan fijo un polígono regular de n lados es isomorfo al grupo que se ha descrito en el último ejemplo. Notar que es isomorfo al grupo de las rotaciones de un prisma de base un polígono regular de n lados.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 2

El grupo simétrico y el alternado

2.1. Definiciones, notaciones y primeras propiedades

Una *permutación* de un conjunto $\mathcal{C}$ no vacío es una aplicación biyectiva de $\mathcal{C}$ en sí mismo. Estamos interesados en conjuntos finitos del tipo

$$\mathcal{C} = \{1, 2, \ldots, n\} \quad \text{o bien} \quad \mathcal{C} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\},$$

en este segundo caso se supone que $\mathcal{C}$ contiene las 26 letras usuales del abecedario. A los elementos de $\mathcal{C}$ los llamaremos, indistintamente, *cifras* o *letras*. Las permutaciones se indican frecuentemente mediante letras griegas minúsculas.

Para indicar que la permutación α aplica la cifra i en la j utilizaremos la notación por la izquierda, es decir $i\,\alpha = j$. Si $i \neq j$ diremos que α *mueve* i, o que la cifra i está en α, en otro caso se dice que α *fija* i.

Si por ejemplo $\mathcal{C} = \{1, 2, \ldots, n\}$, una permutación α de $\mathcal{C}$ se representa mediante

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ 1\,\alpha & 2\,\alpha & 3\,\alpha & \ldots & n\,\alpha \end{bmatrix}.$$

No obstante la notación por ciclos, que se presenta a continuación es más usual e interesante.

Definición 2.1. Se dice que una permutación α es un *ciclo* de longitud r, o un r-ciclo si existen r cifras distintas y ordenadas, $c_1, c_2, \ldots, c_r$, de tal forma que α mueve cada cifra en la siguiente, la última en la primera y fija el resto de cifras, es decir, $c_i\,\alpha = c_{i+1}$ para $i = 1, \ldots, r-1$, $c_r\,\alpha = c_1$ y $c\,\alpha = c$ para $c \neq c_i$. Un tal ciclo se suele indicar de la forma

$$\alpha = (c_1\, c_2\, \ldots\, c_r).$$

Claramente un ciclo está determinado por esas cifras y por su ordenación, salvo por la ordenación cíclica, es decir $(c_1\, c_2\, \ldots\, c_r) = (c_r\, c_1\, c_2\, \ldots\, c_{r-1})$.

Por abuso de notación permitimos que $r = 1$. Así un 1–ciclo es la aplicación identidad ι, y admitimos que $\iota = (c)$ para cualquier cifra c.

La composición de permutaciones α y β es una nueva permutación que denotaremos simplemente por $\alpha\beta$. De acuerdo con la notación por la izquierda en el producto anterior actúa primero α y después β, es decir

$$i\,\alpha\beta = (i\,\alpha)\beta.$$

así, la composición define una operación interna que llamaremos *producto*. Por otra parte, como una permutación α es una aplicación biyectiva, entonces existe la permutación inversa, α^{-1}. Por ejemplo

$$(c_1\, c_2\, \ldots\, c_r)^{-1} = (c_r\, c_{r-1}\, \ldots\, c_2\, c_1).$$

Definición 2.2. El conjunto de todas las permutaciones de los elementos de un conjunto no vacío $\mathcal{C}$ tiene estructura de grupo respecto de la operación composición. Este grupo se denota $S_{\mathcal{C}}$ y se llama *grupo simétrico sobre* $\mathcal{C}$. Si $\mathcal{C}$ tiene n elementos pondremos S_n en lugar de $S_{\mathcal{C}}$ y diremos *grupo simétrico de grado* n.

Observemos que el orden del grupo S_n es $n!$. Y claramente el orden de un r-ciclo es r.

Dos permutaciones se dicen *disjuntas* si no existe ninguna cifra que la muevan ambas permutaciones. Claramente si las permutaciones α y β son disjuntas, entonces $\alpha\beta = \beta\alpha$. Por ejemplo

$$(\texttt{abc})(\texttt{de}) = (\texttt{de})(\texttt{abc}) = \begin{bmatrix} \texttt{a}\ \texttt{b}\ \texttt{c}\ \texttt{d}\ \texttt{e} \\ \texttt{b}\ \texttt{c}\ \texttt{a}\ \texttt{e}\ \texttt{d} \end{bmatrix}.$$

De hecho, se tiene:

Proposición 2.3. *Toda permutación α se puede expresar como producto de ciclos disjuntos dos a dos y esta expresión es única salvo por la ordenación de los factores, y los 1–ciclos. La expresión determina el orden de la permutación de la siguiente manera: si $l_1, \ldots, l_k$ son las longitudes de los ciclos que aparecen en la expresión de σ, entonces*

$$|\sigma| = \text{mcm}\{l_1, \ldots, l_k\}$$

Demostración. Para una cifra c_1 cualquiera, considerar la sucesión

$$c_1,\ c_1\,\alpha,\ c_1\,\alpha^2, \ldots$$

Sea r_1 el menor exponente con $r_1 > 0$ para el que existe $s < r_1$ con $c_1\,\alpha^{r_1} = c_1\,\alpha^s$. Se sigue $c_1\,\alpha^{r_1-s} = c_1$, por lo que $s = 0$, es decir, r_1 es el menor número natural tal que $c_1\,\alpha^{r_1} = c_1$. Consideremos el r_1-ciclo $\gamma_1 = (c_1\ c_1\,\alpha\ \ldots\ c_1\,\alpha^{r_1-1})$. Sea ahora una cifra c_2 que no esté en γ_1, y de manera análoga formamos el ciclo $\gamma_2 = (c_2\ c_2\,\alpha\ \ldots\ c_2\,\alpha^{r_2-1})$, siendo r_2 el menor número natural tal que $c_2\,\alpha^{r_2} = c_2$. Por ser α inyectiva, estos ciclos son disjuntos. Procedemos de manera análoga hasta agotar las cifras de $\mathcal{C}$. Finalmente se ve que α es producto de todos los ciclos así formados, que son disjuntos dos a dos.

La unicidad se sigue puesto que si la cifra c está en el r–ciclo γ entonces

$$\gamma = (c\ c\,\alpha\ \ldots\ c\,\alpha^{r-1}).$$

□

Por ejemplo, la siguiente permutación de $\mathcal{C}$ ={a,b,...,z} se descompone en ciclos disjuntos de esta forma

$$\begin{bmatrix} \texttt{a}\ \texttt{b}\ \texttt{c}\ \texttt{d}\ \texttt{e}\ \texttt{f}\ \texttt{g}\ \texttt{h}\ \texttt{i}\ \texttt{j}\ \texttt{k}\ \texttt{l}\ \texttt{m}\ \texttt{n}\ \texttt{o}\ \texttt{p}\ \texttt{q}\ \texttt{r}\ \texttt{s}\ \texttt{t}\ \texttt{u}\ \texttt{v}\ \texttt{w}\ \texttt{x}\ \texttt{y}\ \texttt{z} \\ \texttt{e}\ \texttt{k}\ \texttt{m}\ \texttt{f}\ \texttt{l}\ \texttt{g}\ \texttt{d}\ \texttt{q}\ \texttt{v}\ \texttt{z}\ \texttt{n}\ \texttt{t}\ \texttt{o}\ \texttt{w}\ \texttt{y}\ \texttt{h}\ \texttt{x}\ \texttt{u}\ \texttt{s}\ \texttt{p}\ \texttt{a}\ \texttt{i}\ \texttt{b}\ \texttt{r}\ \texttt{c}\ \texttt{j} \end{bmatrix} =$$

$$= \texttt{(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)}.$$

Definición 2.4. Se llama *tipo* o estructura de ciclo de una permutación a la sucesión decreciente de las longitudes de los ciclos de su expresión como producto de ciclos disjuntos, incluyendo en esa sucesión tantos 1 como cifras fije dicha permutación.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

2.2. Conjugación de permutaciones

Recordemos que dos elementos α y β de un grupo G se dicen *conjugados* si existe otro $\gamma \in G$ tal que

$$\alpha = \gamma^{-1}\beta\,\gamma,$$

y se escribe $\alpha = \beta^\gamma$. También se dice que γ conjuga β a α.

Algunas propiedades de la conjugación que son consecuencia de resultados que hemos visto ya son las siguientes. Sea G un grupo y $\alpha, \beta, \gamma, \delta \in G$. Se tiene:

(a) $(\alpha\,\beta)^\gamma = \alpha^\gamma\beta^\gamma$.

(b) $(\beta^\gamma)^{-1} = (\beta^{-1})^\gamma$.

(c) $(\beta^\gamma)^\delta = \beta^{\gamma\delta}$.

(d) Si $\alpha = \beta^\gamma$, entonces $\alpha^{\gamma^{-1}} = \beta$.

En el caso de grupos simétricos, además, tenemos un método muy sencillo para calcular conjugados.

Proposición 2.5. *En un grupo simétrico se verifica:*

(a) $(c_1\ c_2\ \ldots\ c_r)^\gamma = (c_1\gamma\ \ c_2\gamma\ \ \ldots\ \ c_r\gamma)$.

(b) Dos permutaciones son del mismo tipo si y solo si son conjugadas.

(c) Si α y β son conjugadas, entonces el número de permutaciones que las conjugan es

$$\#\{\gamma \mid \alpha = \beta^\gamma\} = r_1 r_2 \ldots r_s t_1! \ldots t_m!,$$

donde $(r_1, r_2, \ldots, r_s)$ es el tipo común de ambas permutaciones y los valores $t_1, \ldots, t_m$ representan el numero de ciclos de cada una de las longitudes posibles en ese tipo común.

Demostración. Para el apartado (a), sea c una cifra cualquiera. Si $c = c_j\,\gamma$ par algún j, se tiene

$$\begin{aligned} c\,(c_1\ c_2\ \ldots\ c_r)^\gamma &= c\,\gamma^{-1}(c_1\ c_2\ \ldots\ c_r)\,\gamma = c_j\,(c_1\ c_2\ \ldots\ c_r)\,\gamma = \\ &= c_{j+1}\,\gamma = c_j\gamma\,(c_1\gamma\ \ c_2\gamma\ \ \ldots\ \ c_r\gamma) = c\,(c_1\gamma\ \ c_2\gamma\ \ \ldots\ \ c_r\gamma). \end{aligned}$$

Si fuese $c \neq c_j\gamma$ para $j = 1, \ldots, r$, como $c\gamma^{-1} \neq c_j$, podemos poner

$$c\,(c_1\ c_2\ \ldots\ c_r)^\gamma = c\,\gamma^{-1}(c_1\ c_2\ \ldots\ c_r)\,\gamma = c\,\gamma^{-1}\gamma = c = c\,(c_1\gamma\ \ c_2\gamma\ \ \ldots\ \ c_r\gamma).$$

Para (b), notemos primero que (a) implica que permutaciones conjugadas tienen el mismo tipo. Para ver el inverso basta expresar permutaciones que tienen el mismo tipo como producto de ciclos disjuntos y una debajo de la otra, alineando los ciclos de la misma longitud. Así, la permutación que aplica una cifra en la que se encuentre inmediatamente debajo en esa expresión, es una permutación que conjuga las permutaciones iniciales.

Finalmente, el número de permutaciones que conjugan las dos dadas se obtiene contando las formas esencialmente distintas de colocar una permutación debajo de la otra según se ha explicado en el párrafo anterior. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

El apartado (b) de esta proposición se conoce como el «teorema que permitió ganar la segunda guerra mundial».

Ejercicio 2.6. En el grupo simétrico de grado n, ¿cuántos ciclos hay de longitud k?, ¿cuál es el orden de un ciclo de longitud k?, ¿cuál es el orden de una permutación que es producto se ciclos disjuntos de longitudes $k_1, \cdots, k_l$?

Ejercicio 2.7. Construye las tablas del grupo multiplicativo de las rotaciones de una pirámide de base hexagonal y del grupo aditivo $\mathbb{Z}_6$. Compara estos dos grupos. Compáralos con el grupo S_3.

2.3. Trasposiciones y grupo alternado

Definición 2.8. Los 2–ciclos se denominan *trasposiciones*. Una *involución* es una permutación α de orden 2, es decir $\alpha \neq \iota$ y $\alpha^2 = \iota$. En este caso,

$$\alpha = \alpha^{-1}.$$

Proposición 2.9. *Una permutación α es una involución si y solo si es producto de trasposiciones disjuntas.*

Demostración. Basta tener en cuenta que el producto de ciclos disjuntos es conmutativo y que el orden de un ciclo coincide con su longitud. □

Las trasposiciones son elementos de gran importancia, de hecho vamos a ver que constituyen una familia generadora del grupo simétrico y que son clave para definir un importante subgrupo, el grupo alternado.

Proposición 2.10. *Toda permutación se puede expresar como un producto de trasposiciones.*

Demostración. Ya hemos visto que toda permutación es producto de ciclos, como

$$(a_1, a_2, \cdots, a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k)$$

(no es la única forma) vemos que todo ciclo es producto de trasposiciones.

□

Proposición 2.11. *Si α es producto de un número par de trasposiciones, no puede ser producto de un número impar de trasposiciones.*

Demostración. Supongamos que la permutación α se descompone de dos maneras distintas como producto de trasposiciones, $\alpha = \tau_1 \cdots \tau_r = \gamma_1 \cdots \gamma_s$, siendo τ_i y γ_j trasposiciones. Veamos que s es par si y solo si r también lo es.

Puesto que una trasposición es inversa de ella misma se tiene que $\tau_1 \cdots \tau_r \gamma_s \cdots \gamma_1 = 1$. Así probar que s es par si y solo si r también lo es, equivale a probar que 1 no se puede poner como producto de un número impar de trasposiciones.

Probaremos esta última afirmación. Para ello previamente vemos que si tenemos dos transposiciones λ_1, λ_2 distintas de modo que λ_1 mueve la letra k, entonces existen otras dos δ_1, μ_2 tal que $\lambda_1 \lambda_2 = \delta_1 \mu_2$ y δ_1 fija k y μ_2 mueve k.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Analicemos todas las posibilidades para λ_1 y λ_2,

$$(k,a)\,(k,b) = (a,b)\,(a,k)$$
$$(k,a)\,(a,b) = (a,b)\,(b,k)$$
$$(k,a)\,(b,c) = (b,c)\,(k,a).$$

Probaremos que 1 no se puede poner como producto de un número impar de trasposiciones. Razonamos por reducción al absurdo: suponemos que 1 se puede expresar como producto de un número impar de trasposiciones. Podemos elegir el menor l impar tal que hay una expresión de esa forma, es decir, tal que $\lambda_1 \cdots \lambda_l = 1$ con los λ_i, $i = 1, \ldots, l$ trasposiciones. Es claro que $l \neq 1$ ya que 1 no es una trasposición, por lo tanto $l \geq 3$. Vamos a probar que a partir de esta expresión se puede conseguir otra con como producto de $l-2$ trasposiciones con lo que tendremos una contradicción (por la forma en la que hemos elegido l). Si $\lambda_1 = \lambda_2$ se tiene $1 = \lambda_1\lambda_2 \cdots \lambda_l = \lambda_3 \cdots \lambda_l$. En otro caso, sea k una cifra que mueve λ_1. Como $\lambda_1 \neq \lambda_2$, utilizando la observación anterior deducimos que existen otras dos trasposiciones δ_1, μ_2 tal que $\lambda_1\lambda_2 = \delta_1\mu_2$ y δ_1 fija k y μ_2 mueve k. Así $1 = \lambda_1\lambda_2 \cdots \lambda_l = \delta_1\mu_2 \cdots \lambda_l$.

Si $\mu_2 = \lambda_3$ los eliminamos y tenemos un producto de dos factores menos, en otro caso los sustituimos por $\delta_2\mu_3$ tales que δ_2 fija k y μ_3 mueve k. Así $1 = \lambda_1\lambda_2 \cdots \lambda_l = \delta_1\delta_2\mu_3 \cdots \lambda_l$.

Reiterando el proceso en algún paso eliminamos dos factores o llegamos a un producto de deltas y una μ. Como las delta fijan k y μ la mueve, el producto no puede ser la identidad. Así que forzosamente en algún paso se eliminan dos factores. □

Definición 2.12. Un elemento α de S_n se dice que es par y que tiene signatura 1 si es producto de un número par de transposiciones. En otro caso se dice impar y que tiene signatura -1. La signatura de α se denota $\operatorname{sign}(\alpha)$.

El conjunto de las permutaciones pares es un subgrupo de S_n que se llama *grupo alternado de grado n* y se denota A_n

Proposición 2.13. *Sea $C_2 = \{1, -1\}$ (subgrupo multiplicativo de $\mathbb{C} - \{0\}$). La aplicación* $\operatorname{sign} : S_n \to C_2$ *que asocia a cada permutación su signatura, es un homomorfismo suprayectivo. Su núcleo es A_n luego se tiene que $A_n \trianglelefteq S_n$ y*

$$S_n/A_n \simeq C_2.$$

Demostración. La primera afirmación es clara y la segunda es consecuencia del teorema de isomorfía. □

Muchas de las aplicaciones de los grupos simétricos se basan en resultados sobre descomposiciones de elementos como producto de involuciones (o, equivalentemente, de trasposiciones). Un ejemplo es el teorema de Rejewski que incluimos aquí para leer a modo de ejercicio.

Proposición 2.14. *(Teorema de Rejewski) .*

(a) El producto de dos r–ciclos disjuntos es producto de dos involuciones, más concretamente

$$(c_1\ c_3\ c_5\ \ldots\ c_{2r-1})(c_{2r}\ c_{2r-2}\ \ldots\ c_4\ c_2) =$$
$$= [(c_1\ c_2)(c_3\ c_4)\ldots(c_{2r-1}\ c_{2r})]\ [(c_2\ c_3)(c_4\ c_5)\ldots(c_{2r}\ c_1)].$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

(b) Si las permutaciones α y β son involuciones sin puntos fijos, entonces cada número que forma parte del tipo de $\alpha\,\beta$ aparece un número par de veces.

(c) Si α y β son involuciones sin puntos fijos y la trasposición $(c_1\ c_2)$ forma parte de α entonces las cifras c_1 y c_2 pertenecen a distintos ciclos de la misma longitud de entre los que forman parte de $\alpha\,\beta$ (y de $\beta\,\alpha$).

(d) Si α y β son involuciones sin puntos fijos y la trasposición $(c\ c')$ forma parte de α y

$$(\ldots\ c_1\ c\ c_2\ \ldots)\ (\ldots\ c_1'\ c'\ c_2'\ \ldots) \subset \alpha\beta,$$

entonces la trasposición $(c_1\ c_2')$ también forma parte de α y la $(c\ c_2')$ de β.

(e) Si γ es una permutación tal que cada número de su tipo aparece un número par de veces, entonces $\gamma = \alpha\,\beta$, con α y β involuciones sin puntos fijos.

Demostración. (a) La igualdad es una simple comprobación. Ahora se sigue la afirmación teniendo en cuenta la proposición 2.9.

(b) Por la proposición 2.9, α y β son producto del mismo número de trasposiciones disjuntas, y por no tener puntos fijos todas las cifras están en esas trasposiciones, en particular el grado de las mismas debe ser par. Dada una cifra c, podemos formar una sucesión de $2r$ cifras distintas $c = c_1, c_2, \ldots, c_{2r}$ tales que

$$\begin{aligned}(c_1\ c_2)(c_3\ c_4)\ldots(c_{2r-1}\ c_{2r}) &\subset \alpha\\ (c_2\ c_3)(c_4\ c_5)\ldots(c_{2r}\ c_1) &\subset \beta.\end{aligned}$$

Nótese que r debe ser mayor o igual que 1. Teniendo en cuenta que ciclos disjuntos conmutan, al calcular el producto $\alpha\,\beta$, por el apartado (a) anterior, se sigue que

$$(c_1\ c_3\ c_5\ \ldots\ c_{2r-1})(c_{2r}\ c_{2r-2}\ \ldots\ c_4\ c_2) \subset \alpha\,\beta.$$

Si con las cifras anteriores se han agotado todas las cifras, la proposición ha quedado demostrada, en caso contrario tomamos otra cifra c_{2r+1} y procedemos de forma análoga hasta agotar todas las cifras de $\mathcal{C}$.

(c) Basta observar la igualdad del apartado (a) precedente.

(d) De nuevo se sigue observando el apartado (a), o bien directamente como se indica a continuación. Se tiene que $c'\,\alpha = c$, por lo que $c'\,\alpha\,\beta = c\,\beta$, es decir $c_2' = c\,\beta$. Por otra parte $c_1\,\alpha\,\beta = c$, luego $c_1\,\alpha = c\,\beta = c_2'$ como queríamos.

(e) Teniendo en cuenta la expresión de γ como producto de ciclos disjuntos, emparejando ciclos de la misma longitud y aplicando a cada pareja el apartado (a) anterior, se tiene lo que se quería. □

Ejercicio 2.15. Expresa la siguiente permutación como producto de dos involuciones sin letras fijas de dos maneras distintas,

$$\beta = (1,2,4,5,6)(23,24,26,7,9)(3)(17)(13,20,21,8,22,19,25)(18,11,12,14,15,16,10).$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 3

Acciones de grupos. Simplicidad de A_5 y teoremas de Sylow

3.1. Acciones de grupos

Definición 3.1. Decimos que el grupo G *actúa* sobre el conjunto Ω si tenemos un homomorfismo de grupos

$$\varphi : G \to S_\Omega.$$

Si no hay lugar a error para $i \in \Omega$ y $g \in G$, escribiremos i^g en vez de $i^{\varphi(g)}$. De forma equivalente, G actúa en Ω si y solo si cada $g \in G$ induce una permutación

$$\begin{aligned} \varphi_g : \Omega &\to \Omega \\ i &\mapsto i^g \end{aligned}$$

tal que si $g, h \in G$, se tiene$(i^g)^h = i^{gh}$. El *núcleo de la acción* es

$$\ker \varphi = \{g \in G \mid i^g = i \text{ para todo } i \in \Omega\}.$$

Si el núcleo es trivial, es decir, si φ es inyectiva, se dice que G *actúa fielmente* sobre Ω y en este caso G es isomorfo a un subgrupo del grupo simétrico S_Ω.

Ejercicio 3.2. Sea G el grupo de las rotaciones de un cubo. Considerando la acción de G en los vértices, las caras, y las diagonales internas, establece homomorfismos inyectivos de G a cada uno de los grupos simétricos S_8, S_6 y S_4.

Ejemplo. Sea H subgrupo de G y $\Omega = \{Hx \mid x \in G\}$ (las co-clases a derecha). La aplicación

$$\varphi : G \to S_\Omega$$

dada por $\varphi(g) : Hx \to Hxg$ para cada $x \in G$ es una acción de G sobre $\Omega = \{Hx \mid x \in G\}$.

Ejercicio 3.3. a) Prueba que el núcleo de la acción anterior es

$$\cap_{x \in G} H^x,$$

siendo $H^x = \{x^{-1}hx \mid h \in H\}$

b) Prueba que si H es subgrupo de G, $H^x = \{x^{-1}hx \mid h \in H\}$ también es subgrupo y se llama conjugado de H por x

c) Prueba que la acción anterior es fiel si y solo si G no tiene subgrupos normales no triviales contenidos en H.

Definición 3.4. Sea G actuando sobre el conjunto finito Ω, (así los elementos de G están asociados a elementos de S_Ω. La *órbita* de $i \in \Omega$ es

$$\mathrm{Orb}_G(i) = \{i^g \,|\, g \in G\} \subseteq \Omega$$

y el *estabilizador* de i es

$$\mathrm{Stab}_G(i) = \{g \in G \,|\, i^g = i\} \leq G.$$

El estabilizador de i es un subgrupo de G (ejercicio). Por otra parte, si un elemento j de Ω está en la órbita de otro elemento j, entonces de hecho $\mathrm{Orb}_G(i) = \mathrm{Orb}_G(j)$. Si existe algún elemento tal que $\mathrm{Orb}_G(i) = \Omega$ (y esto es equivalente a que solo haya una órbita), entonces diremos que la acción es *transitiva*.

Ejemplo. Considera el grupo G de las rotaciones de un pirámide exagonal que actúa sobre las 12 aristas. Se puede considera como subgrupo de S_Ω siendo Ω las aristas de la pirámide. Encuentra las órbitas y los estabilizadores.

Lo mismo con las rotaciones de un cubo actuando sobre sus 6 caras.

Proposición 3.5. *a) Sea G un grupo que actúa sobre Ω, $i \in \Omega$, O la órbita de i, H el estabilizador de i. Se tiene que $|O| = |G|/|H|$.*

b) El conjunto de todas las órbitas forman una partición de Ω.

c) El estabilizador de i^g es H^g, en particular tiene el mismo orden que H.

d) (Este apartado no entra para examen) el número de órbitas es $|G|^{-1} \sum_{g \in G} |Fi(g)|$ siendo $Fi(g) = \{i \in \Omega \,|\, i^g = i\}$.

Demostración. a) $i^{g_1} = i^g$ si y solo si $i^{g_1 g^{-1}} = i$ si y solo si $g_1 g^{-1} \in H$ si y solo si $g_1 = hg$ para algún $h \in H$ si y solo si $g_1 \in Hg$.

El cardinal de $Hg := \{hg \,|\, h \in H\}$, que es el mismo que el de H, luego hay $|H|$ elementos de G que me llevan i al mismo i^g, así $|O| = |G|/|H|$.

b) Sean $i, j \in \Omega$ tales que sus órbitas tienen un elemento en común. Veamos que son la misma órbita. Si existen $g_1, g_2 \in G$ tales que $i^{g_1} = j^{g_2}$, entonces $i^{g_1 g_2^{-1}} = i^x = j$ (siendo $x = g_1 g_2^{-1}$). Así para todo $y \in G$, $j^y = i^{xy} \in O(I)$ y se tiene $O(j) \subset O(i)$. Por reciprocidad el otro contenido.

c) Sean i, j de la misma órbita, existe $g \in G$ tal que $i^g = j$.

x pertenece al estabilizador de j si y solo si $j^x = j$ si y solo si $i^{gx} = i^g$ si y solo si $i^{gxg^{-1}} = i$ si y solo si $gxg^{-1} \in H$ si y solo si $x \in g^{-1}Hg = H^g$.

d) Consideramos el conjunto de pares $\{(i, g) \in A \times G \,|\, i^g = i\}$. Contamos sus elementos de dos modos y tenemos que el número de tales pares es

$$\sum_{i \in A} |St(i)| = \sum_{g \in G} |Fi(g)|,$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

con $St(i)$ el estabilizador de i y $Fi(g) = \{i \in A \,|\, i^g = i\}$. Como los estabilizadores de dos elementos de la misma órbita tienen el mismo orden, si las órbitas distintas son $O_1, \cdots, O_r$ y elegimos una cifra $x_i \in O_i$ se tiene

$$\sum_{i=1,\cdots,r} |St(x_i)|\,|O_i| = \sum_{g\in G} |Fi(g)|.$$

Por a) $|O_i| = |G|/|St(x_i)|$, luego sustituyendo queda $r|G| = \sum_{g\in G} |Fi(g)|$ y por tanto $r = |G|^{-1}\sum_{g\in G} |Fi(g)|$. □

Ejercicio 3.6. (Este ejercicio no entra para examen.) Supón que tienes bolas blancas, rojas y negras esféricas por las que se puede pasar un hilo por el centro. ¿Cuántos collares de 20 bolas puedes hacer?, ¿y de 21 bolas?

Ayuda. Si pones el collar sobre la mesa, puedes formar 3^{20} collares. Podemos hacer movimientos que me trasforman un collar en otro. Así que esos dos collares no son en realidad distintos cuando ya no están fijos encima de la mesa.

¿Cuál es el grupo de los movimientos que puedo hacer? Si numero los lugares en los que pongo las bolas, los movimientos son elementos de S_{20}, deduce que son 40 movimientos. Este grupo de 40 elementos actúa sobre los 3^{20} collares y tengo que contar el número de órbitas para ver cuántos collares hay distintos de verdad. Para cada movimiento hay que contar los collares que deja invariantes.

Mira que la permutación $(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20)$ deja fijos los collares que tienen igual color la bola de 1 que la de 2, ... todas iguales, hay tres collares ...

Ejercicio 3.7. (Este ejercicio no entra para examen.) ¿Cuantos cubos distintos se pueden hacer si tenemos tres colores para pintar las caras?

Definición 3.8. Consideramos la acción del grupo G sobre G dada por la aplicación

$$\varphi : G \to Per_G$$

definida por $\varphi(g) : x \to x^g$ para cada $x \in G$. (Para ver que efectivamente es una acción ten en cuenta que conjugar era un automorfismo, en particular es una biyección y además se tiene $(x^g)^h = x^{gh}$ para todos los $g, h, x \in G$.)

El núcleo de esta acción se llama *centro* de G, $Z(G)$ (son los elementos que conmutan con todos, $g \in G$ tales que $x^g = x$ para todos $x \in G$, es decir $gx = xg$). A las órbitas de esta acción se les llama clase de conjugación de G.

Para cada $x \in G$ se llama *centralizador* en G de x al subgrupo

$$C_G(x) = \{g \in G \,|\, xg = gx\}.$$

Fíjate que es el estabilizador de la acción anterior y por tanto es subgrupo de G y además en la clase de conjugación de x hay $|G|/|C_G(x)|$, que es un divisor de $|G|$.

Observación 3.9. Considerando la acción de un grupo en sí mismo por conjugación se deduce que un subgrupo N de un grupo G es normal si y solo si es unión de clases de conjugación de G.

Ejercicio 3.10. Describe todos los subgrupos de A_4 y prueba que hay uno normal de orden 4 (se le llama 4-grupo de Klein).

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

3.2. Simplicidad de A_n

Probaremos que el grupo alternado A_n con $n > 4$ no tiene subgrupos normales propios.

Definición 3.11. Un grupo G se dice *simple* si no tiene subgrupos normales propios. Es decir si $N \trianglelefteq G$ implica $N = 1$ o $N = G$.

Ejercicio 3.12. Prueba que todo grupo abeliano simple, es cíclico de orden primo.

Proposición 3.13. *Si $n > 4$, A_n es simple.*

Demostración. Primero hacemos la siguiente observación: Si $H \leq S_n$ y $H \not\leq A_n$, se tiene que $|H \cap A_n| = \frac{|H|}{2}$. Efectivamente, por ser $H \not\leq A_n$, $HA_n = S_n$ y $S_n/A_n \simeq H/(H \cap A_n)$. Así

$$|H| = 2|H \cap A_n|.$$

Comenzamos con A_5, para ello vamos ver cuantas clases de conjugación hay.

Los elementos de A_5 son 3-ciclos, 5-ciclos o con estructura $(a, b)(c, d)$. Hay 20, 24 y 15 de cada tipo. Si dos elementos de A_5 son conjugados en A_5, son conjugados en S_5 luego son del mismo tipo. Veamos con detalle cada uno de ellos.

- Sea g un 3-ciclo. Su clase de conjugación en S_5 tiene 20 elementos, luego $|C_{S_5}(g)| = |S_5|/20 = 6$ (podemos deducir que $C_{S_5}(g) = \langle g\rangle\langle(4, 5)\rangle$). Se tiene que $(4, 5) \in S_5 - A_5$ y por tanto $C_{S_5}(g) \not\leq A_5$, luego $C_{A_5}(g) = C_{S_5}(g) \cap A_5$ tiene orden la mitad, es decir 3 elementos. Por tanto en la clase de conjugación de g en A_5, que denotaremos $cl_{A_5}(g)$, hay $60/3 = 20$ elementos (o sea todos los 3-ciclos son conjugados en A_5).

- Para $g = (1, 2)(3, 4)$ tenemos que $(1, 3, 2, 4) \in C_{S_5}(g) - C_{A_5}(g)$, luego $C_{A_5}(g) < C_{S_5}(g)$ y tiene la mitad de elementos. $|C_{S_5}(g)| = |S_5|/15 = 8$. Así $C_{A_5}(g) = C_{S_5}(g) \cap A_5$ tiene 4 elementos. Por tanto $|cl_{A_5}(g)| = 60/4 = 15$ (o sea todos los elementos del tipo $(a, b)(c, d)$ son conjugados en A_5).

- Si g es un 5-ciclo tenemos $|C_{S_5}(g)| = |S_5|/24 = 5$, luego $C_{S_5}(g) = \langle g\rangle = C_{A_5}(g)$ y por tanto $|cl_{A_5}(g)| = 60/5 = 12$, luego hay dos clases de conjugación en A_5 formadas por 5-ciclos.

Resumiendo, las clases de conjugación tienen los siguientes números de elementos $1, 20, 12, 12, 15$ y no hay ninguna suma con el 1 que de un divisor de 60, luego A_5 no tiene ningún subgrupo propio normal.

Sea ahora A_n con $n > 5$ y supongamos que A_m es simple para todo $m < n$. Veamos que A_n es simple. Notemos que A_n actúa transitivamente sobre $\{1, 2, \ldots, n\}$ (para cada $i, j \in \{1, 2, \ldots, n\}$, existe $g \in A_n$ tal que $i^g = j$).

Sea H el estabilizador de n, (permutaciones pares de $\{1, 2, \cdots n\}$ que dejan fija la letra n). Se tiene que $H = A_{n-1}$. Además, por ser la acción transitiva si $\sigma \in A_n$ fija una letra (está en el estabilizador de una letra), σ está en H^g para algún $g \in A_n$.

Sea $N \trianglelefteq A_n$. Se tiene que $H \cap N \trianglelefteq H = A_{n-1}$ y por la simplicidad de H se tiene que $H \leq N$ o $H \cap N = 1$.

Suponemos primero que $H \leq N \trianglelefteq A_n$. Entonces, tendríamos que $H^g \leq N$ para todo $g \in A_n$ y por lo dicho anteriormente N contiene a todos los $\sigma \in A_n$ que fijan alguna letra. En particular N contiene a todos los productos de elementos de la forma $(a, b)(c, d)$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Como todo elemento de A_n es un producto de un número par de trasposiciones, todo elemento de A_n estaría en N, $N = A_n$.

Podemos suponer pues que $H \cap N = 1$ y por tanto $H^g \cap N = (H \cap N)^g = 1$. Así que $1 \neq \sigma \in A_n$ que fija alguna letra, no está en N. Supongamos que $N > 1$ y sea $1 \neq \sigma \in N$. La descomposición de σ como producto de ciclos disjuntos puede tener sólo trasposiciones o tener un ciclo de longitud mayor o igual que tres.

En el primer caso, $\sigma = (a,b)(c,d)\cdots$ es producto de trasposiciones disjuntas (al menos dos por ser de A_n). Sea e una cifra distinta de a, b, c, d, entonces $(a,b)(d,e) \in A_n$ luego $\sigma^{(a,b)(d,e)} = (b,a)(c,e)\cdots = \tau \in N$. Se tiene $\sigma\tau \in N$ y $\sigma\tau$ fija a y lleva d a e, así que no es la identidad, lo que contradice lo dicho.

En el segundo, $\sigma = (a,b,c,\ldots)\ldots$ es producto de ciclos disjuntos. Sean d, e cifras distintas de a, b, c, así $(c,d,e) \in A_n$, luego $\sigma^{(c,d,e)} = (a,b,d,\ldots) = \tau \in N$. Como $\sigma \neq \tau$, se tiene que $1 \neq \sigma\tau^{-1} \in N$ y fija a, otra vez contradicción. Así que $N = 1$ □

Ejercicio 3.14. Prueba que en S_n, con $n > 2$, el único elemento del centro (el único elemento que conmuta con todos) es la identidad.

Proposición 3.15. *S_n se puede generar con una trasposición y un ciclo de longitud n, o sea $S_n = \langle (1,2), (1,2,\cdots,n)\rangle$.*

Demostración. Sabemos que toda permutación es producto de trasposiciones, luego S_n se puede generar con todas las trasposiciones. Veamos que también se puede generar con unas pocas trasposiciones, exactamente con estas

$$(1,2), (2,3), (3,4), \ldots, (n-1,n).$$

En efecto, si $H = \langle (1,2), (2,3), (3,4), \cdots, (n-1,n)\rangle$, para todo $i < j$, se tiene

$$(i,j) = (i,i+1)^{(i+1,i+2)(i+2,i+3)\ldots(j-1,j)} \in H,$$

luego H tienen todas las trasposiciones y por tanto $H = S_n$.

Ahora sea $H = \langle (1,2), (1,2,\ldots,n)\rangle$, podemos escribir $(1,2)^{(1,2,\ldots,n)} = (2,3) \in H$, $(2,3)^{(1,2,\ldots,n)} = (3,4) \in H$ y hasta $(n-1,n) \in H$. Por lo anterior $H = S_n$. □

3.3. Grupos resolubles

Definición 3.16. Un grupo G se dice *resoluble* si existen subgrupos G_i verificando

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G \tag{3.1}$$

y G_{i+1}/G_i es abeliano para todo i.

Proposición 3.17. *Sea G un grupo.*

a) Si $H \leq G$ y G es resoluble, entonces H es resoluble.

b) Si $N \trianglelefteq G$, entonces G es resoluble si y solo si N y G/N lo son.

Demostración. a) Como G es resoluble podemos considerar la serie (3.1) anterior. Recordemos que si $N \trianglelefteq G$ y $H \leq G$, $H \cap N \trianglelefteq H$ y $H/(H \cap N) \simeq HN/N$. Tenemos $H \cap G_{i+1} \leq G_{i+1}$ y $G_i \trianglelefteq G_{i+1}$, luego $H \cap G_{i+1} \cap G_i \trianglelefteq H \cap G_{i+1}$, es decir $H \cap G_i \trianglelefteq H \cap G_{i+1}$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Así tenemos la serie

$$1 = H_0 \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_{k-1} \cap H \trianglelefteq G_k \cap H = H,$$

y se tiene

$$(H \cap G_{i+1})/(H \cap G_i) = (H \cap G_{i+1})/(H \cap G_{i+1} \cap G_i) \simeq (H \cap G_{i+1})G_i/G_i.$$

El grupo $(H \cap G_{i+1})G_i/G_i$ es abeliano por ser subgrupo de G_{i+1}/G_i, luego H es resoluble.

b) Si G es resoluble y $N \trianglelefteq G$, por lo anterior N es resoluble. Veamos que G/N es resoluble. A partir de la serie (3.1) anterior construimos

$$1 = G_0 \leq G_1N/N \leq \cdots \leq G_{k-1}N/N \leq G_kN/N = G/N$$

Para ver que cada subgrupo es normal en el anterior, veamos que $G_iN \trianglelefteq G_{i+1}N$

Veamos que $(G_iN)^x = G_iN$ para todo $x = g_{i+1}m \in G_{i+1}N$ con $g_{i+1} \in G_{i+1}, m \in N$. Un elemento $z \in G_iN$ arbitrario es de la forma $z = g_in$ con $g_i \in G_i, n \in N$. Entonces

$$z^x = ((g_in))^{g_{i+1}m} = (g_i^{g_{i+1}}n^{g_{i+1}})^m$$

Como $G_i \trianglelefteq G_{i+1}$, $g_i^{g_{i+1}} = h_i \in G_i$ y como $N \trianglelefteq G$, $n^{g_{i+1}} = n_1 \in N$ así que la expresión anterior queda

$$z^x = (h_in_1)^m = h_i^m n_1^m = m^{-1}h_imn_1^m = h_ih_i^{-1}m^{-1}h_imn_1^m \in G_iN$$

donde hemos vuelto a utilizar que N es normal en G.

Así tenemos

$$1 = G_0 \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_{k-1}N/N \trianglelefteq G_kN/N = G/N$$

y se tiene

$$(NG_{i+1}/N)/(NG_i/N) \simeq NG_{i+1}/NG_i = NG_iG_{i+1}/NG_i \simeq G_{i+1}/(NG_i \cap G_{i+1}).$$

Como $L = NG_i \cap G_{i+1}$ es un subgrupo tal que $G_i \trianglelefteq L \trianglelefteq G_{i+1}$. Se tiene que $(G_{i+1}/G_i)/(L/G_i) \simeq G_{i+1}/L$, y por tanto $G_{i+1}/(NG_i \cap G_{i+1})$ es un cociente de un abeliano y por tanto es abeliano para todo i.

Recíprocamente, supongamos ahora que N y G/N son resolubles. Recordar que los subgrupos normales de G/N son de la forma L/N siendo $L \trianglelefteq G$. As por hipótesis tenemos

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = N$$

tales que N_{i+1}/N_i es abeliano y recordando cómo son los subgrupos normales de un cociente,

$$1 = G_0 \trianglelefteq G_1/N \trianglelefteq \cdots \trianglelefteq G_{n-1}/N \trianglelefteq G_n/N = G/N$$

tales que $(G_{i+1}/N)/G_i/N$ es abeliano. Luegoí

$$G_{i+1}/G_i \simeq (G_{i+1}/N)/G_i/N$$

es abeliano y por tanto la serie

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = N \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

prueba que G es resoluble. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Proposición 3.18. *Un grupo finito G es resoluble si y solo si existen subgrupos G_i verificando*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G,$$

con G_{i+1}/G_i cíclico de orden primo.

Demostración. La implicación hacia la izquierda es obvia. Demostraremos el recíproco por inducción sobre $|G|$.

Si existe $1 \neq N \trianglelefteq G$ y $N \neq G$, como G/N y N tienen orden menor que G y son resolubles, por inducción, cada uno de ellos tiene una serie con cocientes cíclicos de orden primo. Las dos series se pueden juntar como hemos hecho en la demostración del teorema anterior construyendo una serie de G con cocientes cíclicos de orden primo. Si G es simple y resoluble, por la definición tiene que ser abeliano y por tanto cíclico de orden primo y tenemos la serie con un único eslabón. □

Proposición 3.19. *Si $n > 4$, A_n es el único subgrupo normal propio de S_n.*

Demostración. Como $|S_n : A_n| = 2$, $A_n \trianglelefteq S_n$. Sea $1 \neq N \trianglelefteq S_n$. Se tiene que $N \cap A_n \trianglelefteq A_n$ y por la simplicidad de A_n, $N \cap A_n = A_n$ o $N \cap A_n = 1$.

Si $N \cap A_n = A_n$, $A_n \leq N \leq S_n$ y por ser el índice de A_n en S_n primo, se tiene que $N = A_n$ o $N = S_n$.

Si $N \cap A_n = 1$, $A_n < A_n N \leq S_n$ y por la misma razón que antes, $A_n N = S_n$. Se tendría que el grupo

$$N = N/N \cap A_n \simeq A_n N/A_n = S_n/A_n$$

es cíclico de dos elementos.

Si $n \in N$ para todo $g \in S_n$, por ser N normal, $n^g \in N$ y por tener sólo dos elementos $n^g = n$, luego n conmuta con todos los elementos de S_n. Por el ejercicio 33 es una contradicción. □

3.4. Teoremas de Sylow

Ejercicio 3.20. El orden del grupo G es potencia de p. Prueba que $Z(G) \neq 1$.

Pista: Considera la acción de G sobre G por conjugación y suma los elementos de cada órbita.

Ejercicio 3.21. Si $G/Z(G)$ es cíclico, prueba que G es abeliano.

Ejercicio 3.22. Prueba que los grupos de orden p^2 con p primo, son abelianos.

Pista: Utiliza los dos ejercicios anteriores.

Ejercicio 3.23. El orden del grupo G es potencia de p y $1 < N \trianglelefteq G$. Prueba que $Z(G) \cap N \neq 1$.

Pista: Considera la acción de G sobre N por conjugación y y suma los elementos de cada órbita.

Ejercicio 3.24. Sabiendo que el primo p divide al orden de G, prueba que existe un elemento de orden p y por tanto un subgrupo de orden p.

Nota: Este resultado se conoce como el Teorema de Cauchy. Los teoremas de Sylow afirman más: que para cada potencia de un primo p que divida al orden del grupo existen subgrupos de ese orden.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Pista: Por inducción sobre el orden de G. Si G tiene un subgrupo H propio de orden divisible por p, ya está. En otro caso considera la acción de G sobre G por conjugación y cuanta las órbitas. Mira que las órbitas tiene un elemento o un número divisible por p y mira que p divide al orden del $Z(G)$.

Ejercicio 3.25. Sea p el primo más pequeño que divide al orden de G. Prueba que si G tiene un subgrupo H de índice p, entonces H es normal en G.

Pista: Considera la acción de G sobre las coclases de H y mira el orden que tiene que tener el núcleo.

Probamos a continuación los teoremas de Sylow que afirman que para cada grupo finito G y cada primo p divisor del orden de G existen subgrupos de orden la máxima potencia de p que divide al orden de G. Estos subgrupos se llamarán p-subgrupos de Sylow y son todos ellos conjugados.

Comenzamos con una propiedad de números. Por comodidad, para un natural a denotamos a_p la mayor potencia de p que divide a a.

Lema 3.26. *Sean m y n enteros positivos y p un primo. Si p no divide a m, entonces p no divide al número combinatorio $\binom{p^n m}{p^n}$.*

Demostración. El tal número combinatorio es un cociente e/f con

$$e = p^n m(p^n m - 1)(p^n m - 2)\dots(p^n m - (p^n - 1))$$

y $f = p^n(p^n - 1)\dots 1$. Tenemos p^n factores en el numerador y en el denominador. Simplificamos por p^n y buscamos los factores donde puede aparecer p como divisor.

Los factores del denominador son a tales que $1 \leq a \leq p^n - 1$ y los del numerador $p^n m - a$ (en m no aparece el factor p porque p no divide a m).

Para un entero x vamos a llamar x_p a la mayor potencia de p que divide a x.

Veamos ahora que $(p^n m - a)_p = a_p$ con lo que no nos quedara ningún factor primo p y tendremos la tesis.

Ponemos $a = p^b a_1$ con a_1 primo con p. Sabemos que $a \leq p^n - 1$ luego $b < n$. Entonces

$$p^n m - a = p^b(p^{n-b}m - a_1)$$

y como p no divide a $p^{n-b}m - a_1$ se deduce que $a_p = p^b = (p^n m - a)_p$.

Así $c \leq n - 1$ y p^c dividen a p^n, de donde se sigue que p^c divide a a y ya tenemos que $a_p = (p^n m - a)_p$. □

Proposición 3.27 (Teorema de Sylow)**.** *Sea G un grupo y $|G| = p^n m$ con p primo y tal que p no divide a m. Existen subgrupos P de G tales que $|P| = p^n$. A tales subgrupos se les llama subgrupos de Sylow de G.*

Demostración. Sea Ω el conjunto de todos los subconjuntos X de G que tienen p^n elementos. Veamos que alguno de ellos es grupo. Se verifica que Ω tiene un número de elementos que coincide con el combinatorio de $p^n m$ sobre p^n y por tanto el número de elementos de Ω no es divisible por p.

Por otra parte, para cada $X \in \Omega$ y cada $g \in G$, el conjunto Xg también tiene p^n elementos, luego está en Ω. Es claro que la aplicación

$$G \to S_\Omega \quad (g \to (X \to Xg))$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

es una acción de G sobre Ω. Si todas las órbitas tuvieran un número de elementos divisible por p, Ω, que es unión disjunta de las órbitas, tendría un número de elementos divisible por p y hemos dicho que no es así. Así que existe un $X \in \Omega$ tal que en su órbita O_X hay un número de elementos que no es divisible por p.

Como $|O_X| = p^n m/|St(X)|$ se tiene que $P = St(X) = \{g \in G | Xg = X\}$ es un subgrupo de G que verifica $|P| \geq p^n$. Además si fijamos un $x \in X$ podemos considerar la aplicación de P en X dada por

$$P \to X \quad (g \to xg),$$

que es claramente inyectiva, luego $|P| \leq p^n$. Por ser X y P finitos y ser $|P| \geq p^n = |X|$ se sigue que $|P| = |X| = p^n$ y como P es subgrupo tenemos la tesis. □

Proposición 3.28. *Sea p un primo divisor del orden del grupo finito G. Si H es un subgrupo de G de orden potencia de p y P es un p-subgrupo de Sylow de G, entonces existe $g \in G$ tal que $H \leq P^g$.*

Demostración. Sea $\Omega = \{Pg \mid g \in G\}$ sabemos que $|\Omega|$ no es divisible por p. El grupo H actúa sobre Ω por multiplicación a derecha

$$H \to S_\Omega \quad (h \to (Pg \to Pgh)).$$

Tenemos Ω es la unión disjunta de las órbitas y como en las órbitas hay un número de elementos divisor del orden del grupo que actúa que es H, el número de elementos de una órbita es 1 o multiplo de p (potencia de p exactamente). Por ser la suma de múltiplos de p, múltiplo de p y como $|\Omega|$ no es divisible por p, hay al menos una órbita con un sólo elemento.

Así existe $g \in G$ tal que $Pgh = Pg$ para todo $h \in H$ y por tanto $ghg^{-1} \in P$ para todo $h \in H$, es decir $h \in P^g$ para todo $h \in H$ y por tanto $H \leq P^g$. □

Corolario 3.29. *Si P y Q son p-subgrupos de Sylow de G, existe $g \in G$ tal que $Q = P^g$.*

Demostración. Por el teorema anterior existe $g \in G$ tal que $Q \leq P^g$ y por tener el mismo orden se tiene la igualdad. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 4

Anillos, cuerpos y polinomios. Existencia de raíces

4.1. Anillo de polinomios sobre un cuerpo

Si R es anillo se de denota con $R[x]$ el anillo de polinomios sobre la indeterminada x y con coeficientes en R. El grado de un polinomio $p(x)$ se denota mediante $\delta(p)$.

Definición 4.1. Sean R y S anillos. Un homomorfismo de anillos, $f : R \to S$, es un homomorfismo entre los grupos aditivos de R y S tal que para todo $x, y \in R$ se tiene $f(xy) = f(x)f(y)$ y $f(1) = 1$.

El núcleo de un homorfismo de anillos, $\ker(f) = \{r \in R | f(r) = 0\}$, es un ideal de R (un ideal I es un subgrupo de R tal que para todo $r \in R$ y $x \in I$, se tiene que $xr,\ rx \in R$).

Ejercicio 4.2. Prueba que todo homomorfismo de cuerpos es inyectivo.

Proposición 4.3. Homomorfismo evaluación. *Sea R un anillo conmutativo y $a \in R$. La aplicación $e_a : R[x] \to R$ definida por $e_a(p) = p(a)$ es un homomorfismo de anillos.*

Demostración. Ejercicio. □

Recordemos que $K[x]$ es dominio euclídeo con la función grado que denotamos gr, es decir, que dados $0 \neq f, g \in K[x]$ existen $q, r, q \in K[x]$ únicamente determinados (salvo unidades) tales que $f = gq + r$ y $\text{gr}(r) < \text{gr}(g)$.

Proposición 4.4. $K[x]$ es dominio de ideales principales. *Si K es un cuerpo y I es un ideal no nulo de $K[x]$, existe un único $p \in K[x]$ mónico tal que $I = (p)$ (se denota $I = (p) = \{pq \,|\, q \in K[x]\}$ al ideal generado por p, es decir. el menor ideal que contiene a p).*

Demostración. Elegimos en I un polinomio mónico f de grado de mínimo, utilizando el algoritmo de la división se prueba que f genera I y que es el único mónico que lo genera. □

Proposición 4.5. Máximo común divisor. *Sean $f, g \in K[x]$, no nulos, entonces existe un único $d \in K[x]$, mónico tal que $(f) + (g) = (d)$ y se tiene d divide a f y a g, y si e divide a f y a g, d divide a e.*

Demostración. Por ser $K[x]$ dominio de ideales principales y ser $(f)+(g)$ un ideal de $K[x]$ se tiene que existe un único $d \in K[x]$ mónico tal que $(f)+(g)=(d)$ y d divide a f y a g. Si e divide a f y a g, se tiene $(f),(g) \subseteq (e)$ luego $(f)+(g)=(d) \subseteq (e)$ y e divide a d. □

4.2. Polinomios irreducibles y cuerpos

Proposición 4.6. *Sean $p \in K[x]$ y $a \in K$, entonces $p(a)=0$ si y solo si $x-a$ divide a p.*

Demostración. Utilizando que $K[x]$ es dominio Euclídeo se deduce que existen unos únicos $q, r \in K[x]$ tales que $p=q(x-a)+r$ y o bien $r=0$ o bien $\mathrm{gr}(r) < \mathrm{gr}(g)=1$, es decir en ambos casos $r \in K$ y se tiene $r=p(a)$. □

Proposición 4.7. *El polinomio p es irreducible si y solo si $K[x]/(p)$ es un cuerpo.*

Demostración. Supongamos que $K[x]/(p)$ es un cuerpo. Si $p=fg$ con $f,g \in K[x]$ y $\mathrm{gr}(f), \mathrm{gr}(g) < \mathrm{gr}(p)$, tendríamos $(f+(p))(g+(p)=(p)$, es decir que $(f+(p)), (g+(p)$ son divisores de cero en $K[x]/(p)$ luego no tienen inverso y por tanto $K[x]/(p)$ no es cuerpo. Luego si $p=fg$ con $f,g \in K[x]$, uno de los dos polinomios es constante y por tanto p es irreducible.

Supongamos que p es irreducible y sea $f+(p) \neq (p)$. Se tiene que el máximo común divisor de f y p es 1 y por lo anterior existen $a, b \in K[x]$ tales que $af+bp=1$. Así se tiene $(a+(p))(f+(p)=1+(p)$ y por tanto todo $f+(p)$ no nulo es unidad y $K[x]/(p)$ es cuerpo. □

Proposición 4.8. *Supongamos que $p \in K[x]$ es irreducible, entonces existe un cuerpo E que contiene a K como subcuerpo tal que p tiene una raíz en E.*

Demostración. Supongamos que $p(x)=a_0+a_1x+\cdots+a_nx^n$. Por la proposición 4.7, sabemos que $E=K[x]/(p(x))$ es un cuerpo. Consideramos el homomorfismos de anillos $K[x] \to E$ dado por $f \longmapsto \overline{f}=f+(p)$.

Notemos que si $0 \neq a \in K$, entonces $\overline{a} \neq \overline{0}$, por lo que K es isomorfo a $\overline{K}=\{\overline{a} \,|\, a \in K\} \subseteq E$. Identificamos K con $\overline{K}$. Con esta identificación tenemos que el el polinomio p se transforma en

$$p_0(X)=\overline{a}_0+\overline{a}_1X+\cdots+\overline{a}_nX^n \in \overline{K}[X].$$

Consideramos el elemento $e=\overline{x} \in E$. Se tiene

$$p_0(e)=\overline{p}=\overline{0}$$

y la proposición queda demostrada. □

Definición 4.9. El cuerpo primo del cuerpo K es la intersección de todos los subcuerpos de K.

Proposición 4.10. *Sea F el cuerpo primo de K. Si la característica de K es cero, entonces F es isomorfo a $\mathbb{Q}$ y si la característica es p, entonces F es isomorfo a $\mathbb{Z}_p$.*

Demostración. Ejercicio. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Ejercicio 4.11. (Binomio de Newton). Sean a, b elementos del anillo R tales que $ab = ba$. Si n es un entero positivo, probar que

$$(a+b)^n = \sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j}.$$

(Dar la definición de $\left(\begin{array}{c} n \\ j \end{array} \right)$.)

Ejercicio 4.12. En un cuerpo de característica p probar que

$$(a+b)^p = a^p + b^p.$$

(Demostrar previamente que si $1 \leq j \leq p-1$, entonces p divide a $\left(\begin{array}{c} n \\ j \end{array} \right)$.)

4.3. Raíces y polinomios irreducibles

En el resultado siguiente denotaremos por f' la derivada del polinomio f

Proposición 4.13. *Sea K un subcuerpo de E y $f \in K[x]$. Se tiene:*

a) Si $a \in E$, a es raíz multiple de f si y solo si $f(a) = f'(a) = 0$

b) Si $f' \neq 0$ y $(f, f') = 1$, entonces f no tiene raíces múltiples en E.

c) Si f es irreducible en $K[x]$ y $f' \neq 0$ y, entonces todas las raíces de f son distintas.

d) Si la característica de K es cero, los irreducibles de $K[x]$ no tienen raíces múltiples en ningún cuerpo extensión de K.

e) Si la característica de K es p, los irreducibles de $K[x]$ de grado no múltiplo de p, no tienen raíces múltiples en ningún cuerpo extensión de K.

Demostración. a) Se dice que $a \in E$ es raíz múltiple de f si en $E[x]$ tenemos $f = (x-a)^n q$ para algún $n > 1$ y $q \in E[x]$. En este caso $f' = n(x-a)^{n-1}q + (x-a)^n q'$ y $f'(a) = 0$ (recuerda que $f' \in K[x]$).

Recíprocamente, si a no es raíz múltiple, $f = (x-a)q$ de modo que $q(a) \neq 0$. En este caso $f' = q + (x-a)q'$ y $f'(a) = q(a) \neq 0$.

b) Si $(f, f') = 1$, existen $A, B \in K[x]$ tales que $Af + Bf' = 1$ y si existiera una raíz múltiple a, sería por a) $f(a) = f'(a) = 0$, y así $1 = 1(a) = 0$, que es contradicción.

c) Por ser $f' \neq 0$, se deduce la tesis de b).

d) La derivada de un polinomio no constante no es nula y se puede aplicar lo anterior.

e) La derivada de un polinomio de grado no múltiplo de p no es nula y se puede aplicar lo anterior. □

Proposición 4.14. Criterio de Eisenstein. *Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_1 \in \mathbb{Z}$. Supongamos que existe un primo p de $\mathbb{Z}$ tal que $p | a_i$ para $0 \leq i \leq n-1$, p no divide a a_n y p^2 no divide a a_0. Entonces f es irreducible en $\mathbb{Q}[x]$.*

Demostración. Se conoce de segundo curso. □

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Proposición 4.15. *Sea E un cuerpo de característica cero ó p tal que p no divide a n, en el que $f = x^n - 1$ factoriza como producto de polinomios de grado 1, sus raíces se llaman raíces n–ésimas de la unidad.*

El polinomio f tiene exactamente n raíces distintas y forman un grupo cíclico con la multiplicación de E.

Demostración. Como la característica de K es cero, $f' = nx^{n-1} \neq 0$, además f y f' son primos entre sí, luego por lo anterior se tiene que las raíces de f en E son todas distintas.

Sea H el conjunto de las n raíces de f. Es claro que H es un grupo abeliano con la multiplicación de E. Los elementos de H que están en un subrupo de orden p, con p divisor de n, son raíces de $x^p - 1$, luego solo pueden existir p elementos de este tipo, es decir, solo existe un subgrupo de H de orden p, que solo lo cumplen los grupos cíclicos (repasar lo visto en segundo curso sobre grupos abelianos). □

Así para $H = \{\text{raíces de } x^n - 1\}$ existe $\xi \in H$ tal que $H = \langle \xi \rangle = \{1, \xi, \xi^2, \cdots, \xi^{n-1}\}$. A una tal ξ se le llama *raíz n-ésima primitiva de la unidad*.

Ejercicio 4.16. Recuerda que las raíces en $\mathbb{C}$ de $x^n - 1$ forman un grupo cíclico para el producto, generado por $\epsilon = e^{2\pi i/n} = cos2\pi/n + isen2\pi/n$. Encuentra las raíces de $x^n - a$ siendo $a \in \mathbb{R}$ positivo (conociendo $\mathbb{C}$).

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 5

Extensiones de cuerpos

5.1. Extensiones de cuerpos y grado de la extensión

Definición 5.1. Decimos que E/K es una *extensión de cuerpos* si K es un subcuerpo de E.

Es claro que E es un K–espacio vectorial. La extensión se dice finita si la dimensión de E como K–espacio vectorial es finita. Escribiremos $|E : K| = dim_K(E)$ y a este número lo llamaremos grado de la extensión.

Observamos que si E/K es una extensión finita, existen $a_1, \cdots, a_n \in E$ tales que todo elemento de E es una K–combinación lineal de $a_1, \cdots, a_n$.

Definición 5.2. Si E/K es una extensión y $X \subseteq E$ escribiremos $K(X)$ para denotar la intersección de todos los subcuerpos de E que contienen a K y a X. Es obvio que $K(X)$ es el menor subcuerpo de E que contiene a K y a X. Notemos también que $K(X)$ no depende realmente de E siempre que $K, X \subseteq E$.

Notaemos que si E/K es una extensión y $a \in E$, entonces el cuerpo $K(a)$ debe contener a todos los elementos $f(a)$ con $f \in K[x]$ y sus inversos. Se tiene lo siguiente

Ejercicio 5.3. Prueba que si E/K es una extensión y $a \in E$, entonces

$$K(a) = \{f(a)/g(a) \mid f, g \in K[x], g(a) \neq 0\}.$$

Ejercicio 5.4. Sea E/K una extensión de cuerpos y L un cuerpo intermedio, $K \subseteq L \subseteq E$. Entonces E/K es finita si y solo si E/L y L/K lo son. En este caso probar que se tiene que $|E : K| = |E : L||L : K|$.

Ejercicio 5.5. Sean E_1/K_1 una extensión finita y $\sigma : E_1 \to E_2$ un isomorfismo de cuerpos. Si $K_2 = \sigma(K_1)$, probar que $|E_1 : K_1| = |E_2 : K_2|$.

Ejercicio 5.6. Sea E/K una extensión y $a_1, \cdots, a_n \in E$. Prueba que $K(a_1, \cdots, a_n) = (K(a_1, \cdots, a_k))(a_{k+1}, \cdots, a_n)$.

5.2. Extensiones algebraicas

Definición 5.7. Si E/K es una extensión y $a \in E$, diremos que a es *algebraico* sobre K si existe $0 \neq p(x) \in K[x]$ tal que $p(a) = 0$. La extensión se dice algebraica si todos los elementos de E son algebraicos sobre K. Diremos que a es *transcendente* sobre K si no es algebraico.

Es claro que todos los elementos de K son algebraicos sobre K porque $x-k$ se anula en k. Los números reales π y e son transcendentes sobre $\mathbb{Q}$, aunque estos teoremas son complicados de probar.

Proposición 5.8. *Si E/K es finita, entonces E/K es algebraica.*

Demostración. Sea $a \in E$ y supongamos que $|E:K| = n$. Queremos probar que a es raíz de algún polinomio no cero de $K[x]$. Podemos suponer que $a \neq 0$. Si existen $i > j \geq 0$ tales que $a^i = a^j$, entonces a es raíz del polinomio $x^{i-j} - 1 \in K[x]$. En caso contrario el conjunto $1, a, a^2, \cdots, a^n$ tiene $n+1$ elementos y por tanto es K-ligado. Por tanto existen $k_0, k_1, \cdots, k_n \in K$ no todos nulos tales que

$$k_0 + k_1 a + \cdots + k_n a^n = 0.$$

Entonces el polinomio no nulo

$$k_0 + k_1 x + \cdots + k_n x^n \in K[x]$$

se anula en a, luego a es algebraico sobre K.

□

Proposición 5.9. Teorema del elemento algebraico. *Sean E/K una extensión y $a \in E$ algebraico sobre K. Se tiene:*

a) Existe un único polinomio mónico $p \in K[x]$ irreducible en $K[x]$ tal que $p(a) = 0$. Además, para todo $q \in K[x]$, entonces $q(a) = 0$ si y solo si p divide a q.

b) $K(a) = \{f(a) \mid f \in K[x]\}$.

c) Si $\mathrm{gr}(p) = n$, entonces $\{1, a, \cdots, a^{n-1}\}$ es una K-base del espacio vectorial $K(a)$. Por tanto $|K(a):K| = \mathrm{gr}(p)$.

Demostración. a) Definimos $\varphi : K[x] \to E$ por $\varphi(f) = f(a)$, que es la restricción a $K[x]$ del homomorfismo evaluación, luego es homomorfismo de anillos. Como a es algebraico, el ideal $I = \ker(\varphi)$ no es cero. Por ser $K[x]$ un dominio de ideales principales (ver 4.4) existe un único $p \in K[x]$ mónico tal que $I = (p)$ (de grado mínimo en I). Tenemos que si $q \in K[x]$ entonces $q(a) = 0$ si y solo si p divide a q. Para ver que p es irreducible, supongamos que $p = gh$. Entonces se tiene que $0 = g(a)h(a)$ luego g ó h están en I en contra de la minimalidad del grado de p, luego p es irreducible. Cualquier otro polinomio de I es divisible por p, luego p es el único polinomio de I irreducible y mónico.

b) $\varphi(K[x]) = \{f(a) \mid f \in K[x]\} \subseteq K(a)$. Como p es irreducible $K[x]/(p) = K[x]/\ker\varphi$ es cuerpo, luego $\varphi(K[x]) \simeq K[x]/\ker\varphi$ es cuerpo, claramente contiene a K y al elemento $a \in E$, luego $\varphi(K[x]) = K(a)$ y $\{f(a) | f \in K[x]\} = K(a)$.

c) Sea $\mathrm{gr}(p) = n$, si $\{1, a, \cdots, a^{n-1}\}$ fuese K–ligada existiría un polinomio no nulo $g \in K[x]$ de grado $n-1$ tal que $g(a) = 0$ en contra de a). Todo elemento de $K(a)$ es de la forma $f(a)$ para algún $f \in K[x]$ por c). Por ser $K[x]$ dominio euclídeo, existen $q, r \in K[x]$ tales que $f = qp + r$ y $\mathrm{gr}(r) < \mathrm{gr}(p) = n$. Se tiene que

$$f(a) = q(a)p(a) + r(a) = r(a)$$

y como $\mathrm{gr}(r) < n$, $r(a)$ es una K-combinación lineal de $\{1, a, \cdots, a^{n-1}\}$. Así $\{1, a, \cdots, a^{n-1}\}$ genera $K(a)$ y se tiene d).

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Notación. Al polinomio p anterior se le llama *polinomio mínimo* o irreducible de a sobre K.

Ejercicio 5.10. Consideremos $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Este polinomio es irreducible por el criterio de Eisenstein. Consideramos la única raíz real que tiene, $\sqrt[3]{2} \in \mathbb{R}$. Por la proposición anterior tenemos

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}.$$

Si $u = 1 + \sqrt[3]{2}$, vamos a ver de dos formas distintas cómo expresar $1/u$ como $\mathbb{Q}$-combinación lineal de la base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Forma 1: La aplicación $f : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ dada por $f(x) = ux$ es una aplicación $\mathbb{Q}$-lineal y es biyectiva.

La matriz de f en la base anterior (por columnas) es

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Resolviendo el sistema

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

obtenemos $1/u = 1/3(1 - \sqrt[3]{2} + \sqrt[3]{4})$.

Forma 2: sabemos que $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$ y el isomorfismo lleva $\sqrt[3]{2}$ a la clase de X. El elemento u corresponde por tanto a la clase del polinomio $1 + x$ en el cociente de la derecha. Para calcular inversos en un cociente de esta forma podemos usar la identidad de Bezout, es decir, buscamos polinomios s y t en $\mathbb{Q}[x]$ tales que

$$1 = (1 + x)s + (x^3 - 2)t$$

y al tomar clases en el cociente, vemos que la clase de s será inversa de la de $1 + x$. Para buscar s y t dividimos y obtenemos

$$x^3 - 2 = (1 + x)(x^2 - x + 1) - 3$$

luego

$$1 = (1 + x)(x^2 - x + 1)/3 - (x^3 - 1)/3$$

así que $s = (x^2 - x + 1)/3$. Bajo el isomorfismo anterior este elemento corresponde a $(\sqrt[3]{2}^2 - \sqrt[3]{2} + 1)/3$ que es por tanto el inverso de u.

Proposición 5.11. *Sean E/K una extensión y $a_1, \cdots, a_n \in E$ algebraicos sobre K. Entonces $K(a_1, \cdots, a_n)/K$ es finita.*

Demostración. Lo demostramos por inducción sobre n. Para $n = 1$ se tiene por el teorema del elemento algebraico. En otro caso, sea $L = K(a_1, \cdots, a_{n-1})$, por inducción L/K es finita y también lo es $L(a_n)/L$. Por el ejercicio 5.4, $L(a_n)/K$ es finita y como, por el ejercicio 5.6, $L(a_n) = K(a_1, \cdots, a_n)$ se tiene lo que queríamos.

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Consecuencia. De las dos proposiciones anteriores se sigue que la suma y producto de elementos algebraicos es algebraico.

Lema 5.12. *Un isomorfismo de cuerpos se extiende (de forma natural) a un isomorfismo en los correspondientes anillos de polinomios.*

Demostración. Sea $\sigma : K_1 \to K_2$ homomorfismo de cuerpos, entonces es la aplicación

$$\sigma(a_0 + a_1x + \cdots + a_nx^n) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$$

define un isomorfismo de anillos $\sigma : K_1[x] \to K_2[x]$.

□

En particular se tiene que $p \in K_1[x]$ es irreducible si y solo si lo es $\sigma(p) \in K_2[x]$. Observar que también hemos llamado σ al isomorfismo en los anillos de polinomios.

Proposición 5.13. *Sean E_1/K_1 y E_2/K_2 extensiones, $\sigma : K_1 \to K_2$ un isomorfismo, $p_1 \in K_1[x]$ irreducible y $p_2 = \sigma(p_1) \in K_2[x]$. Supongamos que $a_i \in E_i$ es raíz de p_i para $i = 1, 2$. Entonces σ se extiende a un isomorfismo $\theta : K_1(a_1) \to K_2(a_2)$ tal que $\theta(a_1) = a_2$.*

Demostración. Podemos suponer que p_1 es mónico (y por tanto también p_2). Entonces tenemos que p_1 es el polinomio irreducible de a_1 y p_2 es el polinomio irreducible de a_2. Sabemos por la proposición 5.9 (apartado c) que $K_1(a_1) = \{f(a_1) \,|\, f \in K_1[x]\}$ y $K_2(a_2) = \{g(a_2) \,|\, g \in K_2[x]\}$.

Definimos $\theta : K_1(a_1) \to K_2(a_2)$ del siguiente modo. Si $f \in K_1[x]$, entonces

$$\theta(f(a_1)) = \sigma(f)(a_2)$$

Para ver que esta aplicación está bien definida notemos que si $f, g \in K_1[x]$, $f(a_1) = g(a_1)$ si y solo si $(f-g)(a_1) = 0$ si y solo si p_1 divide a $f-g$ si y solo si $\sigma(p_1)$ divide a $\sigma(f)-\sigma(g)$ si y solo si p_2 divide a $\sigma(f) - \sigma(g)$ si y solo si $\sigma(f)(a_2) = \sigma(g)(a_2)$.

Esto prueba que la aplicación está bien definida y que es inyectiva. Es inmediato comprobar que es suprayectiva y que respeta la multiplicación y la suma. Además θ extiende a σ y $\theta(a_1) = a_2$.

□

Corolario 5.14. *Supongamos que E/K es una extensión y $p \in K[x]$ irreducible. Si $a, b \in E$ son raíces de p, entonces existe un isomorfismo de cuerpos $\theta : K(a) \to K(b)$ tal que $\theta(a) = b$ y $\theta(k) = k$ para todo $k \in K$.*

Demostración. En la proposición anterior considerar $\sigma = 1_K$. □

Ejercicio 5.15. También se cumple a la inversa, es decir: si E/K es una extensión y $a, b \in E$ son algebraicos sobre K tales que existe un isomorfismo de cuerpos $\theta : K(a) \to K(b)$ tal que $\theta(a) = b$ y $\theta(k) = k$ para todo $k \in K$, entonces b es raíz del polinomio mínimo de a, es decir, existe $p \in K[x]$ irreducible tal que a, b son raíces de p.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

5.3. Cuerpos de escisión

Definición 5.16. Sea $f \in K[x]$ un polinomio no constante, decimos que f se *escinde* en E si existen $a, a_1, \cdots, a_n \in E$ tales que $f = a(x - a_1) \cdots (x - a_n)$. Si además $E = K(a_1, \cdots, a_n)$, se dice que E es *cuerpo de escisión* de f sobre K.

Si todo polinomio no constante en $K[x]$ se escinde en K, se dice que K es *algebraicamente cerrado*.

Nota. Teniendo en cuenta la factorización única en el anillo $K[x]$, podemos escribir lo siguiente.

- Todo polinomio de grado 1 en $K[x]$ se escinde en K.
- Un polinomio f en $K[x]$ se escinde en K si todos los polinomios no constantes en la descomposición de f como producto de irreducibles son de grado 1.
- Si $f = a(x - a_1) \cdots (x - a_n)$ se escinde en K con $a, a_1, \cdots, a_n \in K$, las raíces de f en cualquier extensión E de K son exactamente $a_1, \cdots, a_n$.
- Si f en $K[x]$ se escinde en K y $p \in K[x]$ es no constante con $p \mid f$, entonces p se escinde en K .

Nuestro próximo objetivo es probar que todo polinomio $p \in K[x]$ tiene cuerpo de escisión y que este es único salvo un isomorfismo que fija los elementos de K. Para ello será fundamental la proposición 4.8.

Teorema 5.17. Existencia cuerpos de escisión. *Sea $f \in K[x]$ no constante, entonces existe un cuerpo de escisión de f sobre K.*

Demostración. Lo probamos por inducción sobre el grado de f. Si f se escinde en K, entonces K es cuerpo de escisión de f. Así podemos suponer que hay un factor irreducible f_1 de f que no se escinde en K.

Por la proposición 4.8 sabemos que existe una extensión F/K tal que F contiene una raíz a de f_1. Por tanto $f(a) = 0$. En este caso $f \in K(a)[x]$ y sabemos que existe $g \in K(a)[x]$ tal que

$$f = (x - a)g.$$

Ahora por inducción existe un cuerpo de escisión para g sobre $K(a)$, es decir existe una extensión $E/K(a)$ donde

$$g = b(x - b_1)(x - b_2) \cdots (x - b_k)$$

con

$$E = K(a)(b_1, \cdots b_k).$$

Por el ejercicio 5.6 tenemos que $E = K(a, b_1, \cdots b_k)$ y como $f = b(x-a)(x-b_1)(x-b_2) \cdots (x-b_k)$, el teorema queda probado.

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Ejemplo 5.18. El polinomio $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ es irreducible por el criterio de Eisenstein. Las raíces de f en $\mathbb{R}$ son $\alpha = \sqrt{2+\sqrt{2}}$, $\beta = \sqrt{2-\sqrt{2}}$, $-\alpha$ y $-\beta$. Por tanto el cuerpo (deberíamos decir "un", pero probaremos la unicidad) de escisión de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha, \beta)$.

Ahora $\alpha\beta = \sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$ con lo que $\beta \in \mathbb{Q}(\alpha)$ y $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. Además $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$.

Definición 5.19. Una extensión E/K se dice que es *normal* si existe un polinomio f en $K[x]$ no constante tal que E es cuerpo de escisión de f sobre K.

Nota. Por la proposición 5.11 las extensiones normales son finitas. Si E/K es normal y L es un cuerpo intermedio $K \subseteq L \subseteq E$, se tiene que E/L es normal.

Ahora nos proponemos probar la unicidad de los cuerpos de escisión.

Teorema 5.20. *Sean $\sigma : K_1 \to K_2$ isomorfismo, $f_1 \in K_1[x]$ no constante, $f_2 = \sigma(f_1) \in K_2[x]$ y E_i cuerpo de escisión de f_i sobre K_i para $i = 1, 2$, entonces existe un isomorfismo $\tau : E_1 \to E_2$ que extiende σ.*

Demostración. Probaremos el teorema por inducción sobre $|E_1 : K_1|$. Tenemos que $|E_1 : K_1| = 1$ si y solo si f_1 se escinde sobre K_1. En este caso las raíces de f_1 sobre cualquier extensión de K_1 están en K_1 (ver la nota tras 5.16). Así $E_1 = K_1$. Como σ es un homomorfismo de anillos $f_2 = \sigma f_1$ se escinde en $K_2 = \sigma(K_1)$ y también $E_2 = K_2$ y se tiene el teorema.

Supongamos $|E_1 : K_1| > 1$. En este caso existe un factor irreducible p de f_1 de grado mayor o igual que 2. Como f_1 se escinde en E_1, p se escinde en E_1 y $\sigma(p)$ se escinde en E_2.

Sea a una raíz de p en E_1 y b una raíz de $\sigma(p) \in K_2[x]$ en E_2. Por la proposición 5.13 existe un isomorfismo de cuerpos $\rho : K_1(a) \to K_2(b)$ que extiende σ. Notemos que E_1 es un cuerpo de escisión de f_1 sobre $K_1(a)$ y que E_2 es un cuerpo de escisión de $\sigma(f_1)$ sobre $K_2(b)$. Además

$$|E_1 : K_1| = |E_1 : K_1(a)||K_1(a) : K_1| = |E_1 : K_1(a)|\mathrm{gr}(p) > |E_1 : K_1(a)|.$$

Por inducción existe un isomorfismo $\tau : E_1 \to E_2$ que extiende ρ, luego extiende σ.

□

Corolario 5.21. Unicidad de los cuerpos de escisión. *Sean E_1 y E_2 cuerpos de escisión de un polinomio no constante sobre K, entonces existe un isomorfismo $\tau : E_1 \to E_2$ tal que $\tau(k) = k$ para todo $k \in K$.*

Demostración. Hacer $\sigma = 1_K$ y se tiene lo que queremos.

□

Corolario 5.22. *Sean E/K una extensión normal y $K \subseteq M_1, M_2 \subseteq E$ subcuerpos. Si $\sigma : M_1 \to M_2$ es un isomorfismo que fija K, entonces existe un isomorfismo $\theta : E \to E$ que extiende σ.*

Demostración. Por hipótesis E es cuerpo de escisión de algún polinomio $f \in K[x]$ no constante. Tenemos que E es cuerpo de escisión de f sobre M_i para $i = 1, 2$ y además $\sigma(f) = f$. El resultado se sigue por el teorema.

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Corolario 5.23. *Sea E/K una extensión normal y $p \in K[x]$ irreducible. Si a, b son raíces de p en E, entonces existe un isomorfismo $\tau : E \to E$ tal que $\tau(a) = b$ y $\tau(k) = k$ para todo $k \in K$*

Demostración. Aplicar sucesivamente los corolarios 5.14 y el anterior.

□

Ejercicio 5.24. Hallar los polinomios mínimos en $\mathbb{Q}[x]$ de i, $\frac{\sqrt{5}+1}{2}$, $\frac{i\sqrt{3}-1}{2}$ y $\sqrt{2}-\sqrt{3}$.

Ejercicio 5.25. Hallar los grados de las siguientes extensiones de cuerpos: $\mathbb{Q}(\sqrt[6]{3})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2},\sqrt{3},i)/\mathbb{Q}$, $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$.

Ejercicio 5.26. Sea $f(x) = (x^2-3)(x^3+1) \in \mathbb{Q}[x]$ y $g(x) = (x^2-2x-2)(x^2+1) \in \mathbb{Q}[x]$. Prueba que $\mathbb{Q}(\sqrt{3}, i)$ es cuerpo de escisión de f y g sobre $\mathbb{Q}$.

Ejercicio 5.27. Prueba que toda extensión de grado 2 es normal.

Ejercicio 5.28. Prueba que las extensiones $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(i)$ son isomorfas como $\mathbb{Q}$–espacios vectoriales pero no como cuerpos.

Teorema 5.29. *Sea E/K una extensión finita. Entonces E/K es normal si y solo si todo $p \in K[x]$ irreducible que tiene una raíz en E se escinde en E.*

Demostración. Supongamos primero que todo polinomio irreducible que tenga una raíz en E se escinde en E. Como E/K es finita, podemos encontrar $\{a_1, \cdots, a_n\}$ una K-base de E. En particular, $E = K(a_1, \cdots, a_n)$. Por 5.8 los elementos a_i son algebraicos sobre K. Sea p_i el polinomio irreducible de a_i sobre K. Por hipótesis tenemos que todo p_i se escinde en $E[x]$. Ahora está claro que E es el cuerpo de escisión de $p_1 \cdots p_n \in K[x]$. Concluimos que E/K es normal.

Supongamos que E/K es normal. Existe un polinomio $f \in K[x]$ no constante tal que $f = c(x - c_1) \cdots (x - c_n)$ con $E = K(c_1, \cdots, c_n)$. Sea $p \in K[x]$ irreducible con una raíz a en E.

Queremos probar que p se escinde en E. Como $p \in E[x]$, por 5.17 podemos encontrar una extensión M/E tal que p se escinde en M. Por tanto $p = d(x - d_1) \cdots (x - d_m)$ con $d_i \in M$. Basta probar que $d_i \in E$ para todo i. Sea $b = d_i$, por 5.13 existe un isomorfismo $\sigma : K(a) \to K(b)$ que fija los elementos de K.

Se tiene que E es cuerpo de escisión de f sobre $K(a)$. Además $f \in K(b)[x]$ y como $E(b) = K(b)(c_1, \cdots, c_n)$ se tiene que $E(b)$ es cuerpo de escisión de f sobre $K(b)$.

Como $\sigma(f) = f$ por 5.20 existe un isomorfismo $\tau : E \to E(b)$ que extiende σ luego extiende a la identidad. Así por el ejercicio 5.5,

$$|E : K| = |E(b) : K|.$$

Y también

$$|K(a) : K| = |K(b) : K|.$$

Ahora,

$$|E : K| = |E(b) : K| = |E(b) : E||E : K|,$$

luego se deduce que $E(b) = E$ y $b \in E$.

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

5.4. Cuerpos finitos

Teorema 5.30. *Sea K un cuerpo finito, entonces existe algún primo p y algún entero n tal que $|K| = p^n$. Además, $\mathbb{Z}_p$ es el cuerpo primo de K y K es el cuerpo de escisión sobre $\mathbb{Z}_p$ del polinomio $f = x^{p^n} - x$.*

Demostración. Sabemos que por ser finito la característica debe ser un primo p y por 4.10, el cuerpo primo de K es $\mathbb{Z}_p$. Por ser K finito K es $\mathbb{Z}_p$-espacio vectorial de dimensión finita luego existen $a_1, \cdots, a_n \in K$ que son una $\mathbb{Z}_p$-base. Como cada elemento de K se escribe de manera única como $\mathbb{Z}_p$-combinación lineal de los elementos a_i concluimos que $|K| = p^n$.

Veamos ahora que todo elemento $a \in K$ es raíz de f. Esto es evidente si $a = 0$, así que podemos suponer $a \neq 0$. Entonces a pertenece al grupo multiplicativo K_0 que tiene $p^n - 1$ elementos, luego a tiene orden finito que divide a $p^n - 1$ y por tanto

$$1 = a^{p^n - 1}$$

luego multiplicando por a

$$a = a^{p^n}.$$

Así, los p^n elementos de K son todos raíces de f. Como f tiene grado p^n no puede tener más raíces en ninguna extensión, luego escinde completamente en K y evidentemente K está generado sobre $\mathbb{Z}_p$ por estas raíces. □

Así, vemos que todo cuerpo finito tiene p^n elementos para algún primo p. De hecho, vamos a ver ahora que para cada posible cardinal hay un único cuerpo finito.

Teorema 5.31. *Para todo primo p y entero positivo n, existe, salvo isomorfismo, un único cuerpo de p^n elementos.*

Demostración. Sea E el cuerpo de escisión de $f = x^{p^n} - x$ sobre $\mathbb{Z}_p$. Notemos que $f' = -1$, luego no tiene factores comunes con f y en tal caso por 4.13 las raíces son distintas y $|U| = p^n$, siendo U el conjunto de las raíces de f en E. Si $a, b \in U$ se tiene por el ejercicio 4.12 que $a - b \in U$, y si $b \neq 0$, $a/b \in U$. Tenemos pues que U es un subcuerpo de E y como $E = \mathbb{Z}_p(U)$ se tiene que $U = E$ y $|E| = p^n$.

Sea K otro cuerpo de p^n elementos. Por el Teorema 5.30 K es el cuerpo de escisión de $x^{p^n} - x$ sobre $\mathbb{Z}_p$ y por la unicidad de los cuerpos de escisión de un mismo polinomio (ver 5.21) se tiene que K es isomorfo a E.

□

Al cuerpo de p^n elementos se le denota $\mathrm{GF}(p^n)$ (GF por "Galois Field").

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 6

El grupo de Galois

6.1. Grupo de Galois de una extensión

Definición 6.1. El grupo de Galois de la extensión E/K es el grupo

$$\mathrm{Gal}(E/K) = \{\sigma : E \to E \text{ isomorfismo tal que } \sigma(k) = k \text{ para todo } k \in K\}.$$

Es inmediato comprobar que $\mathrm{Gal}(E/K)$ es un subgrupo del grupo $\mathrm{Aut}(E) = \{\sigma : E \to E \text{ isomorfismo}\}$, respecto de la operación composición de aplicaciones. Si f es un polinomio en $K[X]$, definimos su grupo de Galois como

$$\mathrm{Gal}_K(f) = \mathrm{Gal}(E/K)$$

con E el cuerpo de escisión de f sobre K. Si el cuerpo K está claro por el contexto, pondremos simplemente $\mathrm{Gal}(f)$.

Definición 6.2. Sea E un cuerpo y $\sigma \in \mathrm{Aut}(E)$. El *cuerpo fijo* de σ es

$$\mathrm{Fix}_E(\sigma) = \{e \in E \mid \sigma(e) = e\}$$

(es fácil comprobar que $\mathrm{Fix}_E(\sigma)$ es efectivamente subcuerpo de E). Análogamente, si G es un subgrupo de $\mathrm{Aut}(E)$, definimos

$$\mathrm{Fix}_E(G) = \bigcap_{\sigma \in G} \mathrm{Fix}_E(\sigma) = \{e \in E \mid \sigma(e) = e \text{ para todo } \sigma \in G\}.$$

Notemos que si $H \leq G \leq \mathrm{Aut}(E)$, entonces $\mathrm{Fix}_E(G) \leq \mathrm{Fix}_E(H)$.

Ejercicio 6.3. Si $E = K(a_1, \cdots, a_n)$ y $\sigma \in \mathrm{Gal}(E/K)$ son tales que $\sigma(a_i) = a_i$ para todo i, entonces $\sigma = 1_E$. (*Ayuda:* ver que el subcuerpo $\mathrm{Fix}_E(\sigma)$ contiene a K y a los elementos a_i.)

Proposición 6.4. *Sean E/K una extensión y $f \in K[x]$. Si $a \in E$ es una raíz de f y $\sigma \in \mathrm{Gal}(E/K)$, entonces $\sigma(a)$ es raíz de f. Además $\mathrm{Gal}(E/K)$ actúa sobre el conjunto de las raíces de f en E.*

Demostración. Sea $f = a_0+a_1x+\cdots+a_nx^n$, $f(a) = 0$, entonces $f(\sigma(a)) = a_0+a_1\sigma(a)+\cdots+a_n\sigma(a)^n = \sigma(a_0 + a_1a + \cdots + a_na^n) = 0$. Luego $\sigma(a)$ es raíz de f.

Con lo anterior es claro que la restricción de σ en el conjunto Ω de las raíces de f en E es una permutación. Así tenemos un homomorfismo de grupos $\mathrm{Gal}(E/K) \to S_\Omega$ donde S_Ω es el grupo simétrico sobre el conjunto Ω, es decir que a cada elemento de $\mathrm{Gal}(E/K)$ le corresponde una permutación de Ω.

□

Proposición 6.5. *Sea E/K una extensión de cuerpos, $f \in K[X]$ y Ω el conjunto de las raíces de f en E. Entonces $\mathrm{Gal}(E/K)$ actúa en Ω y se tiene:*

a) Si E es el cuerpo de escisión de f sobre K, la acción es fiel. En particular G es isomorfo a un subgrupo de S_Ω.

b) Si E/K es normal y f es irreducible en $K[x]$, la acción es transitiva, es decir, dados $a, b \in \Omega$ existe algún $\sigma \in \mathrm{Gal}(E/K)$ con $\sigma(a) = b$.

Demostración. Por la proposición 6.4 tenemos que G actúa sobre Ω. Para a), suponemos que $\Omega = \{a_1, \ldots, a_n\}$ y $E = K(a_1, \cdots, a_n)$ y entonces el ejercicio 6.3 implica que la acción es fiel.

Para b), si f es irreducible, entonces la acción es transitiva por el corolario 5.23.

□

6.2. Extensiones normales y grupo de Galois

Ejercicio 6.6. Sea E/K una extensión y $a_1, \cdots, a_n$ elementos de E. Sea $\sigma : E \to L$ isomorfismo de cuerpos. Prueba que

$$\sigma(K(a_1, \cdots, a_n)) = \sigma(K)(\sigma(a_1), \cdots, \sigma(a_n)).$$

Si tenemos una extensión E/K y un cuerpo intermedio $K \subseteq L \subseteq E$, sabemos que si E/K es normal también lo es la extensión E/L pero L/K no tiene porqué serlo. De hecho se puede caracterizar cuando lo es utilizando el grupo de Galois.

Proposición 6.7. *Sea $K \subseteq L \subseteq E$. Se tiene:*

a) $\mathrm{Gal}(E/L) \leq \mathrm{Gal}(E/K)$.

b) Si L/K es normal, entonces $\sigma(L) = L$ para todo $\sigma \in \mathrm{Gal}(E/K)$.

c) Si E/K es normal, entonces L/K es normal si y solo si $\sigma(L) = L$ para todo $\sigma \in \mathrm{Gal}(E/K)$. En este caso $\mathrm{Gal}(E/L) \trianglelefteq \mathrm{Gal}(E/K)$ y

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/K).$$

Demostración. a) Es claro que los automorfismos que fijan L en particular fijan K.

b) Como L/K es normal se tiene que $L = K(a_1, \cdots, a_n)$, donde $\Omega = \{a_1, \cdots, a_n\}$ son las raíces de un cierto polinomio $f \in K[x]$ no constante. Si $\sigma \in \mathrm{Gal}(E/K)$ sabemos por 6.4 que $\sigma(\Omega) \subseteq \Omega$ y por ser finito, $\sigma(\Omega) = \Omega$ y por el ejercicio anterior $\sigma(L) = L$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

c) Supongamos que $\sigma(L) = L$ para todo $\sigma \in \mathrm{Gal}(E/K)$, veamos que L/K es normal. Sea $p \in K[x]$ irreducible con una raíz $a \in L$. Por 5.29 basta probar que p se escinde en L. Sabemos, por ser E/K normal que p se escinde en E. Sea $b \in E$ otra raíz de p. Por ser la acción transitiva existe $\sigma \in \mathrm{Gal}(E/K)$ con $\sigma(a) = b$. Como $\sigma(L) = L$ se tiene que $\sigma(a) = b \in L$.

Consideramos la aplicación de $\mathrm{Gal}(E/K) \to \mathrm{Gal}(L/K)$ que a cada automorfismo σ le asocia su restricción a L que está definida por ser $\sigma(L) = L$. Es suprayectiva por 5.22 y su núcleo es $\mathrm{Gal}(E/L)$. Por los teoremas de isomorfía de grupos se tiene lo que queremos.

□

Ejercicio 6.8. Sean E_1/L_1 un extensión y $\tau : E_1 \to E_2$ un isomorfismo. Si $L_2 = \tau(L_1)$, prueba que $\mathrm{Gal}(E_1/L_1) \simeq \mathrm{Gal}(E_2/L_2)$ via $\sigma \mapsto \tau\sigma\tau^{-1}$.

Ejercicio 6.9. Sean $K \subseteq L \subseteq E$, $H = \mathrm{Gal}(E/L) \leq \mathrm{Gal}(E/K)$ y $\tau \in \mathrm{Gal}(E/K)$. Prueba que

$$H^{\tau^{-1}} = \mathrm{Gal}(E/\tau(L)).$$

Ejercicio 6.10. Decidir si las siguientes extensiones son normales.

a) $\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}$.

b) $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$.

Ejercicio 6.11. Si E/L y L/K son normales probar que E/K no tiene por qué ser normal.

Ejercicio 6.12. Construir cuerpos de escisión sobre $\mathbb{Q}$ de los polinomios $x^3 - 1$, $x^4 + 5x^2 + 5$ y $x^6 - 8$.

Ejercicio 6.13. Prueba que $\mathrm{Aut}(\mathbb{Q}) = 1$ y $\mathrm{Aut}(\mathbb{R}) = 1$. *Ayuda:* Prueba que para todo $\sigma \in \mathrm{Aut}(\mathbb{R})$ si $x < y$ se tiene que $\sigma(x) < \sigma(y)$ y tener en cuenta que para todo par de números reales distintos existe un racional entre ellos.

Ejercicio 6.14. Sea $f \in K[x]$ irreducible y $a \in E$ raíz de f. Supongamos que f se escinde en $K(a)$. Prueba que entonces $|\mathrm{Gal}(K(a)/K)| = |K(a) : K|$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

6.3. Extensiones de Galois

Definición 6.15. Una *extensión de Galois* es una extensión normal E/K tal que los polinomios irreducibles en K que tienen alguna raíz en E, las tienen todas distintas (no tienen raíces múltiples en E). En particular, en característica cero, toda extensión normal es de Galois.

Proposición 6.16. *Si E/K es de Galois, entonces se tiene*

$$|E:K| = |\mathrm{Gal}(E/K)| \quad y \quad \mathrm{Fix}_E(\mathrm{Gal}(E/K)) = K.$$

Demostración. Sea $G = \mathrm{Gal}(E/K)$. Tenemos

$$K \subseteq \mathrm{Fix}_E(G) \subseteq E.$$

Si $a \in \mathrm{Fix}_E(G) - K$, como E/K es finita, a es algebraico sobre K. Sea $p \in K[x]$ el polinomio irreducible de a. Tenemos que grado de p es al menos 2 luego existe al menos otra raíz b, además, por la definición de extensión de Galois esta otra raíz ha de ser distinta de a, es decir $b \neq a$. Por ser E/K normal, $b \in E$ y por la transitividad de la acción de G existe $\sigma \in G$ tal que $\sigma(a) = b$, así que $a \notin \mathrm{Fix}_E(G)$, es decir, tenemos una contradicción. Por lo tanto deducimos $\mathrm{Fix}_E(G) = K$.

Probaremos $|E:K| = |\mathrm{Gal}(E/K)|$ por inducción sobre $|E:K|$. Si $|E:K| = 1$, $E = K$ y $\mathrm{Gal}(E/K) = 1_E$.

Si $E \neq K$ tomamos $a \in E - K$ y p su polinomio mínimo sobre K. Sea Ω el conjunto de las raíces de p, sabemos que $|\Omega|$ es el grado de p.

Por 5.23 $G = \mathrm{Gal}(E/K)$ actúa transitivamente sobre Ω. Además, el estabilizador del elemento a es precisamente $\mathrm{Gal}(E/K(a))$ luego por la fórmula del orden de una órbita

$$|\Omega| = |G|/|\mathrm{Gal}(E/K(a))|.$$

Además

$$|K(a):K| = \text{grado del polinomio } p = |\Omega|.$$

Así se tiene

$$|G| = |\Omega|\ |\mathrm{Gal}(E/K(a))| = |K(a):K|\ |\mathrm{Gal}(E/K(a))|.$$

Como $E/K(a)$ también es de Galois, podemos aplicar la hipótesis de inducción y poner

$$|E:K(a)| = |\mathrm{Gal}(E/K(a))|,$$

por lo que nos queda

$$|G| = |K(a):K||E:K(a)| = |E:K|.$$

□

Proposición 6.17 (Teorema del elemento primitivo)**.** *Sea E/K una extensión finita de característica cero, entonces existe $a \in E$ tal que $E = K(a)$.*

Demostración. Sabemos que existen $a_1, \cdots a_n \in E$ tales que $E = K(a_1, \cdots a_n)$ con lo que es suficiente probar que si $E = K(b,c)$ existe $a \in E$ tal que $E = K(a)$.

Sea p_1 el polinomio mínimo de b sobre K y p_2 el polinomio mínimo de c sobre K. En algún cuerpo de excisión E_1 de p_1p_2 que contenga a E, están todas las raíces. Sean

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

$b = b_1, \cdots, b_n$ las distintas raíces de p_1 y $c = c_1, \cdots, c_m$ las de p_2 (en ambos casos, en E_1).

En E_1 tenemos $n \times (m-1)$ elementos de la forma $(b_i - b)/(c - c_j)$. Por ser K infinito existe $t \in K$ tal que, para $i = 1, \ldots, n$, $j = 2, \ldots, m$,

$$t \neq (b_i - b)/(c - c_j)$$

y se tiene

$$t(c - c_j) \neq (b_i - b),$$

luego

$$a = tc + b \neq tc_j + b_i.$$

Vamos a ver que $c, b \in K(a)$ (notemos que $a \in K(c, b)$, ya que $t \in K$). Consideramos el polinomio que resulta al sustituir x en p_1 por $a - tx$, es decir, $h(x) = p_1(a - tx) \in K(a)[x]$, que es un polinomio de grado n. Además se tiene que

$$h(c) = p_1(b) = 0$$

pero para $j = 2, \ldots, n$,

$$h(c_j) = p_1(a - tc_j) \neq 0$$

porque $a - tc_j \neq b_i$.

Así el polinomio mínimo de c sobre $K(a)$ es divisor de $h(x)$ y de p_2. Si fuese un polinomio de grado mayor que 1, en el cuerpo E_1 tendríamos dos raíces comunes a p_2 y a h que no existen, ya que hemos visto que el resto de las raíces de p_2 no son raíces de h. Así el polinomio mínimo de c sobre $K(a)$ es de grado 1 y $c \in K(a)$. Como $b = a - tc \in K(a)$ y $K(a) \subseteq K(b, c)$ se deduce $K(a) = K(b, c)$.

□

Proposición 6.18. *Sean K un cuerpo de característica cero, E/K una extensión de Galois y H un subgrupo de $G = \mathrm{Gal}(E/K)$, entonces se tiene que*

$$H = \mathrm{Gal}(E/\mathrm{Fix}_E(H)).$$

Demostración. Sea $L = \mathrm{Fix}_E(H)$, tenemos

$$K \subseteq L = \mathrm{Fix}_E(H) \subseteq E.$$

Es claro que $H \leq \mathrm{Gal}(E/L)$, luego

$$|E : L| = |\mathrm{Gal}(E/L)| \geq |H|.$$

Por el teorema del elemento primitivo, existe $a \in E$ tal que $E = L(a)$. Consideramos el polinomio

$$h(x) = \prod_{\alpha \in H} (x - \alpha(a)).$$

Recuerda que si β es un automorfismo de E, también induce un automorfismo del anillo de polinomios $E[x]$, en particular esto sucede para los elementos de H. Para todo $\beta \in H$ se tiene que $\beta(h(x)) = h(x)$ porque $\beta H = H$. Así que los coeficientes de $h(x)$ quedan fijos por todos los $\beta \in H$ luego están en $L = \mathrm{Fix}_E(H)$ y $h(x) \in L[x]$. Como $h(a) = 0$,

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

el polinomio mínimo de a sobre L es un divisor de $h(x)$ luego su grado es menor o igual que el grado de $h(x)$ que es $|H|$. Así

$$|E : L| = |L(a) : L| \leq |H|$$

y se tiene la igualdad

$$|E : L| = |H|$$

y como sabemos que $H \leq \mathrm{Gal}(E/L)$, tenemos de hecho

$$\mathrm{Gal}(E/L) = H.$$

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Capítulo 7

Teoría de Galois

7.1. La correspondencia de Galois

Relacionaremos los cuerpos intermedios de una extensión con los subgrupos del grupo de Galois.

Proposición 7.1. (Teorema fundamental de la teoría de Galois). *Supongamos que E/K es Galois, $G = \mathrm{Gal}(E/K)$, $\mathcal{S}$ el conjunto de los subgrupos de G y $\mathcal{K}$ el conjunto de los subcuerpos intermedios de la extensión E/K, entonces se tiene:*

(a) Las aplicaciones $f : \mathcal{S} \to \mathcal{K}$ y $g : \mathcal{K} \to \mathcal{S}$, dadas por $f(H) = \mathrm{Fix}_E(H)$ y $g(L) = \mathrm{Gal}(E/L)$ son biyecciones, una inversa de la otra.

(b) Si $K \subseteq L \subseteq E$, entonces L/K es normal si y solo si $\mathrm{Gal}(E/L) \trianglelefteq \mathrm{Gal}(E/K)$. En este caso

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/K).$$

Demostración. (a) Sea $K \subseteq L \subseteq E$ un cuerpo intermedio. Entonces $g(L) = \mathrm{Gal}(E/L)$ y $f \circ g(L) = \mathrm{Fix}_E(\mathrm{Gal}(E/L))$. Sabemos que E/L es de Galois y por la proposición 6.16, tenemos que

$$\mathrm{Fix}_E(\mathrm{Gal}(E/L)) = L$$

luego $f \circ g(L)$, es decir, $f \circ g$ es la identidad (y en particular f es suprayectiva y g inyectiva).

Al contrario, sea ahora $H \leq G$ un subgrupo. Entonces $f(H) = \mathrm{Fix}_E(H)$ y $g \circ f(H) = \mathrm{Gal}(E/\mathrm{Fix}_E(H))$. Por 6.18,

$$H = \mathrm{Gal}(E/\mathrm{Fix}_E(H)).$$

Así $g \circ f(H) = H$, $f \circ g$ es la identidad (y en particular g es suprayectiva y f inyectiva). (b) Sea $K \subseteq L \subseteq E$ y $H = \mathrm{Gal}(E/L)$. Se tiene que $H \trianglelefteq G$ si y solo si $H^\tau = H$ para todo $\tau \in G$. Por el ejercicio 6.9 $H \trianglelefteq G$ si y solo si $\mathrm{Gal}(E/\tau(L) = H = \mathrm{Gal}(E/L)$ para todo $\tau \in G$. Y por (a) esto ocurre si y solo si $\tau(L) = L$ para todo $\tau \in G$ y por el apartado c) de la proposición 6.7 esto ocurre si y solo si L/K es normal. En este caso también por 6.7 c) se tiene el isomorfismo.

□

Observación 7.2. Las aplicaciones f y g de la correspondencia de Galois invierten contenidos, es decir, si tenemos (con la notación anterior) subgrupos $H_1 \leq H_2 \leq G$, entonces

$$\mathrm{Fix}_E(H_1) = f(H_1) \supseteq f(H_2) = \mathrm{Fix}_E(H_2)$$

y si tenemos cuerpos intermedios $K \subseteq L_1 \subseteq L_2 \subseteq E$, entonces

$$\mathrm{Gal}(E/L_1) = g(L_1) \geq g(L_2) = \mathrm{Gal}(E/L_2).$$

Ejemplo 7.3. En un ejemplo en una lección anterior (ver 5.18) consideramos el polinomio $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. Observamos que f es irreducible por el criterio de Eisenstein. Las raíces de f en $\mathbb{R}$ son h

$$\alpha = \sqrt{2+\sqrt{2}}, \quad \beta = \sqrt{2-\sqrt{2}}, \quad -\alpha, \quad -\beta. \tag{7.1}$$

Vimos que el cuerpo de escisión de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha)$. Además $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$ y $E/\mathbb{Q}$ es Galois con $E = \mathbb{Q}(\alpha)$. Vamos a calcular el grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$.

Sabemos que $|G| = 4$ y $1, \alpha, \alpha^2, \alpha^3$ es $\mathbb{Q}$ base de E, luego cada elemento $\sigma \in G$ queda determinado por $\sigma(\alpha)$. Como las raíces de f son (7.1), hay un $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Sabemos que $\alpha\beta = \alpha^2 - 2$ y por tanto $\beta = \alpha^{-1}(\alpha^2 - 2)$. Calculamos ahora

$$\alpha^{-1} = a + b\alpha + c\alpha^2 + d\alpha^3; \quad (a + b\alpha + c\alpha^2 + d\alpha^3)\alpha = 1.$$

Como se tiene que $\alpha^4 - 4\alpha^2 + 2 = 0$, es $a\alpha + b\alpha^2 + c\alpha^3 + d(4\alpha^2 - 2) = 1$, por tanto $1 = -2d, a = 0, b + 4d = 0, c = 0$ y $\alpha^{-1} = 2\alpha - \frac{1}{2}\alpha^3$. Así

$$\beta = (2\alpha - \frac{1}{2}\alpha^3)(\alpha^2 - 2) = 2\alpha^3 - 4\alpha - \frac{1}{2}\alpha^5 + \alpha^3 = 2\alpha^3 - 4\alpha - \frac{1}{2}(4\alpha^3 - 2\alpha) + \alpha^3,$$
$$\beta = -3\alpha + \alpha^3.$$

Se tiene que

$$\begin{aligned}\sigma^2(\alpha) = \sigma(\beta) = \sigma(-3\alpha + \alpha^3) = -3\beta + \beta^3 = -3\beta + (2-\sqrt{2})\beta = \\ = (-3 + 2 - \sqrt{2})\beta = (-1 - \sqrt{2})\beta = (-1 - (\alpha^2 - 2))\beta = (1 - \alpha^2)(-3\alpha + \alpha^3) = \\ = -3\alpha + \alpha^3 + 3\alpha^3 - \alpha^5 = -3\alpha + 4\alpha^3 - (4\alpha^3 - 2\alpha) = -\alpha.\end{aligned}$$

Así que $\sigma \in G$ tiene orden 4 y por tanto G es cíclico. Por el teorema de los subcuerpos intermedios solo existe una extensión intermedia $\mathbb{Q} \subset L \subset E$ tal que $|L : \mathbb{Q}| = 2$ y $L = \mathrm{Fix}_E(\sigma^2)$, es decir,

$$\begin{aligned}L &= \{a + b\alpha + c\alpha^2 + d\alpha^3 | \sigma^2(a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha + c\alpha^2 + d\alpha^3\}, \\ L &= \{a + b\alpha + c\alpha^2 + d\alpha^3 | a - b\alpha + c\alpha^2 - d\alpha^3 = a + b\alpha + c\alpha^2 + d\alpha^3\}, \\ L &= \{a + c\alpha^2 | a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}).\end{aligned}$$

Ejemplo 7.4. Consideramos el polinomio irreducible $f = x^3 - 2 \in \mathbb{Q}[x]$. Sea $\omega = \frac{-1+\sqrt{3}i}{2}$ raíz tercera primitiva de la unidad (las otras son 1 y ω^2). Las raíces de f en $\mathbb{C}$ son

$$\{\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2}\}$$

y el cuerpo de escisión de f sobre $\mathbb{Q}$ es $E = \mathbb{Q}(\omega, \sqrt[3]{2})$, que no está contenido en $\mathbb{R}$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Como $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ y $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ se tiene que $|E : \mathbb{Q}| > 3$ y si G es su grupo de Galois sobre $\mathbb{Q}$ sabemos que $|E : \mathbb{Q}| = |G|$ y G es un subgrupo de S_3 y como no hay subgrupos propios de más de 3 elementos, $G \simeq S_3$. Vamos a describir los elementos de G y los cuerpos intermedios.

El polinomio mínimo de ω es de segundo grado, x^2+x+1. La otra raíz es ω^2, además $\sigma \in G$ queda determinado por $\sigma(\omega)$ y $\sigma(\sqrt[3]{2})$. Una $\mathbb{Q}$ base de E es

$$\{1, \omega, \sqrt[3]{2}, \omega\sqrt[3]{2}, \sqrt[3]{4}, \omega\sqrt[3]{4}\}.$$

Proposición 7.5. *Sea K un cuerpo de característica cero, E/K una extensión y sean $K \subseteq F, L \subseteq E$ cuerpos intermedios. Supongamos que F/K es de Galois, E está generado por los subcuerpos L y F y $M = L \cap F$. Entonces E/L es de Galois y la restricción*

$$\mathrm{Gal}(E/L) \to \mathrm{Gal}(F/M)$$

está bien definida y es un isomorfismo de grupos.

Demostración. Por ser F/K normal, existe $f \in K[x]$ tal que $f = (x-a_1)\cdots(x-a_n)$ y $F = K(a_1, \cdots, a_n)$. Además, como E está generado por L y F se tiene $E = L(F)$ luego $E = L(a_1, \cdots, a_n)$ y como $f \in L[x]$, se deduce que la extensión E/L es normal luego es de Galois ya que estamos en característica cero. Claramente F/M es de Galois.

Por ser F/M normal, la restricción $\mathrm{Gal}(E/M) \to \mathrm{Gal}(F/M)$ está bien definida y por tanto tenemos

$$\psi : \mathrm{Gal}(E/L) \hookrightarrow \mathrm{Gal}(E/M) \to \mathrm{Gal}(F/M).$$

Veamos primero que ψ es inyectiva. Sea $\sigma \in \mathrm{Gal}(E/L)$, si sigma está en $\ker\psi$, se deduce que el cuerpo $\mathrm{Fix}_E(\sigma)$ contiene tanto a F como a L. Como E es el cuerpo generado por L y F, esto implica $\mathrm{Fix}_E(\sigma) = E$ luego $\sigma = 1$.

Veamos para terminar que ψ es también suprayectiva. Sea $H = \mathrm{im}\psi \leq G = \mathrm{Gal}(F/M)$. Por ser F/M de Galois, utilizando la correspondencia de Galois, para ver que $G = H$ basta ver que tienen el mismo cuerpo fijo, es decir, que $\mathrm{Fix}_F(H) = M$. Es obvio que $M \subseteq \mathrm{Fix}_F(H)$. Si $x \in \mathrm{Fix}_F(H)$, se tiene que $\tau(x) = x$ para todo $\tau \in \mathrm{Gal}(E/L)$, luego $x \in \mathrm{Fix}_E(\mathrm{Gal}(E/L)) = L$ por el teorema 7.1 y así $x \in L \cap F = M$.

□

7.2. Polinomio resoluble por radicales

Definición 7.6. Una extensión E/K se dice *radical* si existe subcuerpos $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = E$ tales que $K_i = K_{i-1}(a_i)$ donde $a_i^{n_i} \in K_{i-1}$ para ciertos enteros positivos n_i, para $i = 1, \cdots, m$.

Decimos que un polinomio no constante en $K[x]$ es resoluble por radicales si existe una extensión radical E/K que contenga un cuerpo de escisión de f.

Ejemplo 7.7. Todo polinomio de grado 2 es resoluble por radicales. También lo son los polinomios de la forma $x^n - a$ con $a \in K$.

En esta sección veremos que el grupo de Galois de un polinomio resoluble por radicales, es resoluble. En la siguiente, demostraremos el recíproco.

Proposición 7.8. *Sea E/K una extensión y $\xi \in E$ una raíz n-ésima primitiva de la unidad. La extensión $K(\xi)/K$ es normal con grupo de Galois abeliano.*

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Demostración. Sabemos que las raíces de $f = x^n - 1 \in K[x]$ son $H = \{1, \xi, \xi^2, \cdots, \xi^{n-1}\}$, luego $K(\xi)$ es cuerpo de escisión de f sobre K y $K(\xi)/K$ es normal.

Sea $\sigma \in G = \mathrm{Gal}(K(\xi)/K)$, se tiene por 6.3 que $\sigma(H) \subseteq H$ y como σ es biyectivo y H finito $\sigma(H) = H$ y σ es un automorfismo de H (conserva el producto de H, $\cdot$). Además, como $K(\xi)$ es el cuerpo de escisión de f sobre K, la acción es fiel, es decir, $\sigma|_H = 1_H$ se tiene que $\sigma(\xi) = \xi$ y $\sigma = 1_{K(\xi)}$. Así que G es un subgrupo del grupo de los automorfismos de un grupo cíclico, que por el ejercicio 1.38 sabemos que es abeliano.

□

Proposición 7.9. *Sea K de característica cero y E/K una extensión. Supongamos que K contiene una raíz n-ésima primitiva de la unidad y que $E = K(a)$ para un cierto $a \in E$ tal que $b = a^n \in K$. Se tiene que E/K es de Galois y $\mathrm{Gal}(E/K)$ es cíclico de orden un divisor de n.*

Demostración. Sea $\xi \in K$ una raíz n-ésima primitiva de la unidad. Si $a = 0$ $E = K$ y la tesis es obvia.

Si $a \neq 0$ consideramos el polinomio $f = x^n - b \in K[x]$. Los elementos

$$\{a, \xi a, \xi^2 a, \cdots, \xi^{n-1} a\}$$

son todos distintos y son raíces del polinomio f y como todas están en E, E es cuerpo de escisión de f sobre K y E/K es de Galois.

Para cada $\sigma \in G = \mathrm{Gal}(E/K)$ sabemos que σ queda determinado por $\sigma(a)$ ya que $1, a, a^2, \cdots$ es K-base de E. Ademas $\sigma(a)$ tiene que ser por 6.3 raíz del mismo polinomio mínimo de a divisor de f luego $\sigma(a) = \xi^i a$ para algún i.

Definimos la aplicación $\psi : \mathrm{Gal}(E/K) \to \langle \xi \rangle$ que asocia a cada $\sigma \in \mathrm{Gal}(E/K)$, el elemento $\xi^i \in \langle \xi \rangle$ tal que $\sigma(a) = \xi^i a$. Se tiene que si $\sigma_1, \sigma_2 \in \mathrm{Gal}(E/K)$ y $\sigma_1(a) = \xi^i a$ y $\sigma_2(a) = \xi^j a$, entonces

$$\sigma_1\sigma_2(a) = \sigma_1(\xi^j a) = \xi^j \sigma_1(a) = \xi^j \xi^i a.$$

Lo anterior prueba que la aplicación ψ es un homomorfismo de grupos. Es claro que si a un $\sigma \in \mathrm{Gal}(E/K)$ le asociamos el elemento $1 \in \langle$ es que $\sigma(a) = a$ y entonces $\sigma = 1_E$. Así que tenemos un homomorfismo inyectivo de grupos y $\mathrm{Gal}(E/K)$ es isomorfo a un subgrupo de un cíclico de orden n y por 1.40 es cíclico de orden divisor de n.

□

Lema 7.10. *Sea K un cuerpo de característica cero y L/K una extensión. Sea la cadena de subcuerpos*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L,$$

tales que K_{i+1}/K_i es de Galois con grupo de Galois abeliano para $i = 0, \cdots, m-1$. Supongamos $K \subset E \subset L$ tal que E/K es de Galois. Entonces $\mathrm{Gal}(E/K)$ es resoluble.

Demostración. Lo probamos por inducción sobre m. Si $m = 0$ y $E = K$ el resultados es obvio. Sea E_1 el subcuerpo de L generado por K_1 y E y $M = K_1 \cap E$, como E/K es de Galois, también lo es E/M y por 7.1 se tiene que E_1/K_1 es de Galois con grupo de Galois isomorfo a $\mathrm{Gal}(E/M)$. Aplicando inducción a la cadena $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L$ y al subcuerpo intermedio E_1 tenemos que $\mathrm{Gal}(E_1/K_1)$ es resoluble y por tanto lo es $\mathrm{Gal}(E/M)$.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Como $\mathrm{Gal}(K_1/K)$ es abeliano, todos sus subgrupos son normales y por el teorema 7.1 (b) todas las extensiones intermedias son normales, así que M/K es normal. Además, su grupo de Galois cumple

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(K_1/K)/\mathrm{Gal}(K_1/M)$$

luego es abeliano. De nuevo por el teorema 7.1 pero ahora aplicado a la extensión E/K tenemos

$$\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/M)$$

y por 3.17 (b) deducimos que $\mathrm{Gal}(E/K)$ es resoluble.

□

Proposición 7.11. *Sea K de característica cero, si $f \in K[x]$ es resoluble por radicales, su grupo de Galois es resoluble.*

Demostración. Sea E cuerpo de escisión de f y R/K una extensión radical tal que $E \subseteq R$. Sabemos que existe una cadena de subcuerpos $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = R$ tales que $K_i = K_{i-1}(a_i)$ con $a_i^{n_i} \in K_{i-1}$ para ciertos enteros positivos n_i y para cada $1 \leq i \leq m$.

Sea $n = n_1 \cdots n_m$ y ω una n-ésima raíz primitiva de la unidad. Consideramos las extensiones

$$K \subseteq K(\omega) = K_0(\omega) \subseteq K_1(\omega) \subseteq \cdots \subseteq K_m(\omega) = R(\omega).$$

Tenemos $K_i(\omega) = K_{i-1}(\omega)(a_i)$ y como $K(\omega)/K$ es radical, $R(\omega)/K$ es radical. Cada extensión $K_{i-1}(\omega)(a_i)/K_{i-1}(\omega)$ tiene grupo de Galois cíclico por 7.9 y además el de $K(\omega)/K$ es abeliano por 7.8, luego por el lema 7.10 $\mathrm{Gal}(E/K)$ es resoluble.

□

Nuestro siguiente objetivo será ver un ejemplo concreto de un polinomio con coeficientes racionales no resoluble por radicales. Necesitaremos algunos resultados y consideraciones previas. El cuerpo de escisión del polinomio $x^1 + 1$ sobre $\mathbb{R}$ es el cuerpo complejo $\mathbb{C} = \mathbb{R}(i)$. El grupo de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ es el grupo cíclico de dos elementos generado por τ, la conjugación compleja, dada por $\tau(a + bi) = a - bi$ con $a, b \in \mathbb{R}$.

Lema 7.12. *Sea E/K una extensión normal con $E \subset \mathbb{C}$ y $K \subseteq \mathbb{R}$. Sea τ la conjugación compleja. Entonces $\tau(E) = E$ luego $\tau|_E \in \mathrm{Gal}(E/K)$.*

Demostración. Basta usar 6.4 b). □

En el siguiente lema vamos a utilizar el teorema fundamental del álgebra, que afirma que todo polinomio con coeficientes complejos escinde completamente en $\mathbb{C}$. Esto implica que el cuerpo de escisión de todo polinomio $f \in \mathbb{Q}[x]$ está contenido en $\mathbb{C}$.

Lema 7.13. *Sea $f \in \mathbb{Q}[x]$ irreducible de grado el primo p. Supongamos que f tiene exactamente dos raíces no reales, entonces* $\mathrm{Gal}(f) = S_p$.

Demostración. Sea E el cuerpo de escisión de f (que por el teorema fundamental del álgebra suponemos contenido en $\mathbb{C}$). Denotamos por α y β las dos raíces no reales de f. Como f tiene p raíces distintas sabemos que hay un homomorfismo inyectivo

$$\phi : \mathrm{Gal}(E/\mathbb{Q}) \to S_p$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

con S_p el grupo simétrico de grado p. Sea $H = \text{im}\phi$, entonces $H \cong \text{Gal}(E/\mathbb{Q})$, es decir, $\text{Gal}(E/\mathbb{Q})$ es isomorfo a un subgrupo de S_p. Además, $\mathbb{Q}(\alpha) \subseteq E$ y $|\mathbb{Q}(\alpha) : \mathbb{Q}| = p$ luego $p||E : \mathbb{Q}| = |\text{Gal}(E/\mathbb{Q})|$ y por el teorema de Cauchy, existe en $\text{Gal}(E/\mathbb{Q})$ un elemento σ de orden p. Por tanto $\phi(\sigma) \in H$ también tiene orden$p$. Notemos que en S_p los únicos elementos de orden p son los p-ciclos luego $\phi(\sigma)$ es un p-ciclo.

Por el lema 7.12, la restricción de la conjugación compleja es un elemento $\tau \in \text{Gal}(E/\mathbb{Q})$ que tiene orden 2, fija las raíces reales y tal que $\tau(\alpha) = \beta$, $\tau(\beta) = \alpha$. Por tanto $\phi(\tau) \in H$ es una trasposición.

Al establecer el isomorfismo ϕ, podemos numerar las raíces de forma que α corresponda con la cifra 1, $\sigma(\alpha)$ corresponda con la cifra 2, etcétera, de forma que $\phi(\sigma) = (1, 2, \cdots, p) \in H$. La otra raíz no real β corresponderá con alguna cifra k y por tanto $\phi(\tau) = (1, k) \in H$. Además, si consideramos la potencia $k-1$ de σ, tenemos un elemento de H de la forma

$$\phi(\sigma^{k-1})) = (1, k, \cdots) \in H$$

En 3.15 hemos probado que S_p está generado por $(1, 2, \cdots, p)$ y la transposición $(1, 2)$. Esto implica que si conjugamos por cualquier otro elemento g de S_p también tenemos una familia generadora. Observemos que podemos elegir un elemento $g \in S_p$ tal que $2^g = k$, $1^g = 1$ y $(1, 2, \ldots, p)^g = \phi(\sigma^{k-1})) \in H$. Las dos primeras condiciones implican $(1, 2)^g = (1, k) = \phi(\tau) \in H$. Es decir, los dos elementos $(1, 2, \ldots, p)^g$ y $(1, 2)^g$ generan todo S_p y están en H y por tanto $H = S_p$. □

Proposición 7.14. *El polinomio $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ no es resoluble por radicales.*

Demostración. El polinomio f es una función continua que toma valor negativo en -2 y positivo en -1, así que tiene una raíz real en $(-2, -1)$. En 1 vuelve a ser negativo luego tiene un raíz real en el intervalo $(-1, 1)$. En 2 es positiva, luego tiene otra raíz real en $(1, 2)$. Con cáculo elemental, estudiando el crecimiento y decrecimiento se tiene que sólo tiene tres cortes con el eje horizontal, tres raíces reales. Por el lema anterior $\text{Gal}(f)$ es isomorfo a S_5 que sabemos no es resoluble, luego por el teorema 7.13, f no es resoluble por radicales.

□

7.3. Grupo resoluble y polinomio resoluble por radicales

En esta sección probaremos el recíproco de la proposición 7.11, es decir, si un polinomio tiene su grupo de Galois resoluble, entonces es resoluble por radicales. Primero observemos que un automorfismo de un cuerpo K es una aplicación de K en K y recordemos que $K^K = \{\text{aplicaciones } K \to K\}$ es un K-espacio vectorial. Las combinaciones lineales de automorfismos son vectores de K^K pero no son automorfismos de K. En este contexto se tiene el siguiente importante teorema de Dedekind.

Proposición 7.15 (Teorema de Dedekind)**.** *Sea K un cuerpo y sean $\tau_1, \cdots, \tau_n$ automorfismos distintos de K. Entonces $\tau_1, \cdots, \tau_n$ son K-linealmente independientes.*

Demostración. Por inducción sobre n. Empezamos con el caso $n = 1$ y suponemos que para cierto $a \in K$ se tiene $a\tau = 0$. Entonces $0 = a\tau(1) = a$.

Supongamos ahora que es cierto hasta $n > 1$ y que tenemos sea $a_1\tau_1 + \cdots + a_n\tau_n = 0$. Entonces

$$a_1\tau_1(x) + \cdots + a_n\tau_n(x) = 0,$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

para todo $x \in K$. Si algún a_i es cero, por inducción todos son cero. Supongamos pues que $a_i \neq 0$ para todo i. Para $x, y \in K$ cualesquiera se tiene

$$0 = a_1\tau_1(xy) + \cdots + a_n\tau_n(xy) = a_1\tau_1(x)\tau_1(y) + \cdots + a_n\tau_n(x)\tau_n(y).$$

Como $a_1\tau_1(x) + \cdots + a_n\tau_n(x) = 0$, multiplicando por $\tau_1(y)$ se tiene

$$0 = a_1\tau_1(x)\tau_1(y) + \cdots + a_n\tau_n(x)\tau_1(y).$$

Restando esta última igualdad con la anterior, se tiene para todo $x \in K$

$$0 = a_2\tau_2(x)(\tau_2(y) - \tau_1(y)) + \cdots + a_n\tau_n(x)(\tau_n(y) - \tau_1(y)).$$

Así

$$0 = a_2(\tau_2(y) - \tau_1(y))\tau_2 + \cdots + a_n(\tau_n(y) - \tau_1(y))\tau_n = 0.$$

Por hipótesis de inducción $a_i(\tau_i(y) - \tau_1(y)) = 0$ para $2 \leq i \leq n$ y para todo $y \in K$. Como $a_i \neq 0$, se tiene $\tau_1 = \tau_i$ para $2 \leq i \leq n$, por ejemplo $\tau_1 = \tau_2$, que contradice la hipótesis.

□

Necesitamos el recíproco de la proposición 7.9, que probamos a continuación.

Proposición 7.16. *Sea K un cuerpo de característica cero y sea E/K una extensión de Galois de grado n. Supongamos que K contiene una raíz m-ésima primitiva de la unidad con $n|m$. Supongamos que* $\mathrm{Gal}(E/K)$ *es cíclico. Entonces existe $a \in E$ tal que $E = K(a)$ y $a^n \in K$.*

Demostración. Como K contiene una raíz m-ésima primitiva de la unidad y $n|m$, K contiene también una raíz n-ésima primitiva de la unidad que denotamos ξ.

Sea $\mathrm{Gal}(E/K) = \langle\tau\rangle$, como E/K es de Galois tenemos $|\langle\tau\rangle| = |E : K| = n$. Buscaremos un elemento $0 \neq a \in E$ tal que $\tau(a) = \xi a$. Veamos que este elemento cumple lo que queremos: por un lado, tendremos que $\tau(a^n) = \tau(a)^n = \xi^n a^n = a^n$ y por tanto $\tau^i(a^n) = a^n$ para todo $0 \leq in$ y $c := a^n \in \mathrm{Fix}_E(\mathrm{Gal}(E/K)) = K$. Además, a es raíz del polinomio $f = x^n - c \in K[x]$ luego si q es el polinomio mínimo de a sobre K, q es divisor de f así que el grado de q es menor o igual que n. Como $\tau(a) = \xi a$, $\tau^i(a) = \xi^i a$ y $\tau(a), \tau^2(a), \cdots \tau^{n-1}(a)$ son raíces distintas de q (son distintas ya que $a \neq 0$) y se concluye que q debe ser de grado al menos n. Por tanto $f = q$ tiene grado n. Así $|K(a) : K| = n$ luego $E = K(a)$.

Vamos pues a buscar un elemento $a \in E$ tal que $\tau(a) = wa$. Por el teorema de Dedekind, como $1_E, \tau, \tau^2, \cdots \tau^{n-1}$, son automorfismos distintos, se tiene que

$$1_E + \frac{1}{\xi}\tau + \frac{1}{\xi^2}\tau^2 + \cdots + \frac{1}{\xi^{n-1}}\tau^{n-1}$$

es una aplicación no nula y existe $b \in E$ tal que

$$a = b + \frac{1}{\xi}\tau(b) + \frac{1}{\xi^2}\tau^2(b) + \cdots + \frac{1}{\xi^{n-1}}\tau^{n-1}(b) \neq 0.$$

Este $a \in E$ verifica que $\tau(a) = \xi a$.

□

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Ahora probamos el teorema final de la teoría de Galois.

Proposición 7.17. *Sea K un cuerpo de característica cero y E el cuerpo de escisión de un polinomio $f \in K[x]$. Si $\mathrm{Gal}_K(f) = \mathrm{Gal}(E/K)$ es resoluble, entonces f es resoluble por radicales.*

Demostración. Sea $m = |E : K| = |\mathrm{Gal}(E/K)|$. Sea ξ una raíz m-ésima primitiva de la unidad en algún cuerpo $\overline{E}$ tal que $E \subseteq \overline{E}$ y $\overline{E} = E(\xi)$. Si llamamos $\overline{K} = K(\xi)$, se tiene que $\overline{E}$ está generado por E y $\overline{K}$. Sea $M = E \cap \overline{E}$. Por 7.5, $\overline{E}/\overline{K}$ es Galois y $G = \mathrm{Gal}(\overline{E}/\overline{K})$ es isomorfo a $\mathrm{Gal}(E/M)$ que es un subgrupo de $\mathrm{Gal}(E/K)$ y por tanto es resoluble y de orden divisor de m. Vamos a probar que la extensión $K \subseteq \overline{E}$ es radical, con esto ya estará probado el resultado ya que $\overline{E}$ contiene al cuerpo de escisión de f sobre K, que es E.

Como G es resoluble, tenemos una serie normal con cocientes cíclicos

$$1 = G_m \trianglelefteq G_{m-1} \trianglelefteq \ldots \trianglelefteq G_0 = G$$

y por la correspondencia de Galois, si denotamos

$$K_i = \mathrm{Fix}_{\overline{E}}(G_i),$$

se tiene

$$\overline{K} = K_0 \subseteq \cdots \subseteq K_m = \overline{E}$$

En cada paso tenemos $\mathrm{Gal}(\overline{E}/K_{i+1}) = G_{i+1} \trianglelefteq G_i = \mathrm{Gal}(\overline{E}/K_i)$ y como $\overline{E}/K_i$ es de Galois, se deduce que K_{i+1}/K_i es normal con grupo de Galois isomorfo al cociente

$$\mathrm{Gal}(\overline{E}/K_i)/\mathrm{Gal}(\overline{E}/K_{i+1}) = G_1/G_{i+1}$$

que es cíclico cuyo orden denotamos n_i y es un divisor de m. Además, K_i contiene una raíz m-ésima primitiva de la unidad luego también contiene una raíz primitiva de la unidad de orden n_i así que por la proposición 7.16 anterior, K_{i+1}/K_i es una extensión radical simple, es decir, existe algún $a_i \in K_{i+1}$ con $a_i^{n_i} \in K_i$ y $K_{i+1} = K_i(a_i)$. Como también $\overline{K} = K(\xi)$ con $\xi^m \in K$, se tiene que $\overline{E}/K$ es radical y por lo tanto f es resoluble por radicales.

□

7.4. Ejemplo de grupo de Galois de un polinomio

Ejemplo 7.18. Encuentra el grupo de Galois del polinomio $f = x^4 - 2$ sobre $\mathbb{Q}$.

Solución. Este polinomio es irreducible por el criterio de Eisenstein y tiene una raíz real $\sqrt[4]{2}$. Las raíces son $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$.

El cuerpo de escisión E sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[4]{2}, i)$. La extensión intermedia $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal, porque está en $\mathbb{R}$ y por tanto no contiene a las raíces que no son reales, así que el grupo de Galois no puede ser abeliano. Como $i \notin \mathbb{Q}(\sqrt[4]{2})$ el polinomio mínimo de i sobre $\mathbb{Q}(\sqrt[4]{2})$ es $x^2 + 1$ y $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})| = 2$, como $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 4$ se tiene que $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}| = 8$ y $|\mathrm{Gal}(f)| = 8$. Denotamos $a = \sqrt[4]{2}$.

Sea $N = \mathrm{Gal}(E/\mathbb{Q}(i))$, como $E/\mathbb{Q}(i)$ tiene grado 4 y $\mathbb{Q}(i)/\mathbb{Q}$ es normal, N es un subgrupo de orden 4 que es normal en G. Además E tiene como $\mathbb{Q}(i)$-base al conjunto

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

$\{1, a, a^2, a^3\}$ con lo que los elementos de $\sigma \in N$ quedan determinados por $\sigma(a)$. Además $\sigma(a)$ puede ser $a, ai, -a, -ai$.

Si elegimos $\sigma \in N$ tal que $\sigma(a) = ai$, tenemos $\sigma^2(a) = \sigma(ai) = i\sigma(a) = iai = -a$, y vemos que no es la identidad, luego σ no tiene orden 2 así que debe tener orden 4 y N es cíclico.

Sea $H = \mathrm{Gal}(E/\mathbb{Q}(a))$, como $E/\mathbb{Q}(a)$ tiene grado 2 y $\mathbb{Q}(a)/\mathbb{Q}$ no es normal, H es un subgrupo de orden 2 que no es normal. Es claro que los elementos de $\mathrm{Gal}(E/\mathbb{Q}(i)) \cap \mathrm{Gal}(E/\mathbb{Q}(a))$, fijan a y finan i luego son la identidad. Así $G = HN$.

Vamos a escribir los elementos de G como elementos de S_4 por su acción sobre las cuatro raices del polinomio que numeramos $1, 2, 3, 4$ en este orden $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$. Así el sigma anterior es el ciclo $(1, 3, 2, 4)$.

El elemento $1 \neq \beta \in H$ es tal que $\beta(i) = -i$ así que $\beta(a) = a$, $\beta(-a) = -a$, $\beta(ai) = -ai$ y $\beta(-ai) = ai$, luego es la transposición $(3, 4)$.(Notar que G no es todo S_4)

Ahora $(1, 3, 2, 4)^{(3,4)} = (1, 4, 2, 3) = (1, 3, 2, 4)^{-1}$ y G es isomorfo al diédrico de 8 elementos. Ademas de los subgrupos H y N que se corresponden con los cuerpos $\mathbb{Q}(a)$ y $\mathbb{Q}(i)$, tenemos los subgrupos siguientes:

1) $\langle\sigma^2\rangle = Z(G) \leq N$ y tiene 2 elementos. Le corresponde un cuerpo $K_1 = \{e \in E | \sigma^2(e) = e\}$ que contiene a $\mathbb{Q}(i)$. Notar que σ^2 no fija ninguna de las 4 raíces de p, es $(1, 2)(3, 4)$ y como $|E : K_1| = 2$, $|K_1 : \mathbb{Q}| = 4$. Buscamos $b = t_0 + t_1 a + t_2 a^2 + t_3 a^3 \in E$ ($t_i \in \mathbb{Q}(i)$), tal que $\sigma^2(b) = b$. Podemos escribir

$$\begin{aligned}\sigma^2(t_0 + t_1 a + t_2 a^2 + t_3 a^3) &= t_0 + t_1\sigma^2(a) + t_2\sigma^2(a^2) + t_3\sigma^2(a^3) = \\ &= t_0 - t_1 a + t_2 a^2 - t_3 a^3 = \\ &= t_0 + t_1 a + t_2 a^2 + t_3 a^3,\end{aligned}$$

y por tanto $t_1 = t_3 = 0$.

Es claro que $a^2 \in K_1$. Como $a^2 = \sqrt[2]{2}$ tiene polinomio mínimo sobre $\mathbb{Q}$ de grado 2, $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$. Y como $i \notin \mathbb{Q}(\sqrt{2})$, se tiene que $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$ y $K_1 = \mathbb{Q}(\sqrt{2}, i)$.

2) $\langle\sigma^2, \beta\rangle \simeq C_2 \times C_2$ tiene 4 elementos. Le corresponde un cuerpo $K_2 = \{e \in E | \sigma^2(e) = e, \beta(e) = e\}$. Notar que σ^2 no fija ninguna de las 4 raíces de p, es $(1, 2)(3, 4)$ y como $|E : K_2| = 4$, $|K_1 : \mathbb{Q}| = 2$. $\beta(a) = a$ luego $\beta(a^2) = a^2$ y como $\sigma^2(a^2) = a^2$, $\sqrt{2} = a^2 \in K_2$ y por dimensiones, $K_2 = \mathbb{Q}(\sqrt{2})$.

3)$\langle\sigma^2\beta\rangle \simeq C_2$. Le corresponde un cuerpo $K_3 = \{e \in E | (\beta \circ \sigma^2)(e) = e\}$ y como $|E : K_3| = 2$, $|K_3 : \mathbb{Q}| = 4$. $\sigma^2\beta = (1, 2)(3, 4)(3, 4) = (1, 2)$, luego fija la raíz ai y por dimensiones $K_3 = \mathbb{Q}(ai)$.

4) $\langle\sigma\beta\rangle \simeq C_2$. Le corresponde un cuerpo $K_4 = \{e \in E | (\beta \circ \sigma)(e) = e\}$ y como $|E : K_4| = 2$, $|K_1 : \mathbb{Q}| = 4$. $\sigma\beta = (1, 3, 2, 4)(3, 4) = (1, 4)(2, 3)$ así que no fija ninguna raíz.

Sea $b = t_0 + t_1 a + t_2 a^2 + t_3 a^3 + t_4 i + t_5 ai + t_6 a^2 i + t_7 a^3 i \in E$, ($t_i \in \mathbb{Q}$) tal que $(\beta \circ \sigma)(b) = b$ Se tiene

$$\begin{aligned}&(\beta \circ \sigma)(t_0 + t_1 a + t_2 a^2 + t_3 a^3 + t_4 i + t_5 ai + t_6 a^2 i + t_7 a^3 i) = \\ =&t_0 + t_1(\beta \circ \sigma)(a) + t_2(\beta \circ \sigma)(a^2) + + \ldots + t_6(\beta \circ \sigma)(a^2 i) + t_7(\beta \circ \sigma)(a^3 i) = \\ =&t_0 + t_1\beta(ai) + t_2\beta(-a^2) + t_3\beta(-a^3 i) + t_4\beta(i) + t_5\beta(aii) + t_6\beta(-a^2 i) + t_7\beta(-a^3 ii) \quad = \\ =&t_0 + t_1(-ai) + t_2(-a^2) + t_3(a^3 i) + t_4(-i) + t_5(-a) + t_6(a^2 i) + t_7(a^3).\end{aligned}$$

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza

Así tenemos $t_5 = -t_1, t_2 = 0, t_7 = t_3, t_4 = 0$, y $b = t_0+t_1(a-ai)+t_3(a^3+a^3i)+t_6(a^2i)$ y por tanto $K_4 = \mathbb{Q}((a-ai),(a^3+a^3i),(a^2i))$. Para expresarlo d eforma más sencilla tener en cuenta que $(a(1-i))^2 = -2a^2i$ y que $a^2i(a-ai) = a^3i+a^3$ esto prueba que $K_4 = \mathbb{Q}(a(1-i))$.

5) $\langle\sigma^3\beta\rangle \simeq C_2$. Le corresponde un cuerpo $K_5 = \{e \in E|(\beta\circ\sigma^3)(e) = e\}$ y como $|E : K_5| = 2$, $|K_5 : \mathbb{Q}| = 4$. $\sigma^3\beta = (1,4,2,3)(3,4) = (1,3)(4,2)$, así que no fija ninguna raíz. Notar que $\sigma^3(a) = \sigma^2(ai) = \sigma(aii) = aiii = -ai$.

Sea $b = t_0 + t_1a + t_2a^2 + t_3a^3 + t_4i + t_5ai + t_6a^2i + t_7a^3i \in E$, $(t_i \in \mathbb{Q})$ tal que $(\beta\circ\sigma^3)(b) = b$. Se tiene

$$\begin{aligned}&(\beta\circ\sigma^3)(t_0 + t_1a + t_2a^2 + t_3a^3 + t_4i + t_5ai + t_6a^2i + t_7a^3i) =\\ =&t_0 + t_1\beta(-ai) + t_2\beta(-a^2) + t_3\beta(a^3i) + t_4\beta(i) + t_5\beta(-aii) + t_6\beta(-a^2i) + t_7\beta(a^3ii) =\\ =&t_0 + t_1(ai) + t_2(-a^2) + t_3(-a^3i) + t_4(-i) + t_5(a) + t_6(a^2i) + t_7(-a^3).\end{aligned}$$

Así tenemos $t_5 = t_1, t_2 = 0, -t_7 = t_3, t_4 = 0$, y $b = t_0+t_1(a+ai)+t_3(a^3-a^3i)+t_6(a^2i)$ y por tanto

$$K_5 = \mathbb{Q}((a+ai),(a^3-a^3i),(a^2i)).$$

Para expresarlo de forma más sencilla tener en cuenta que $(a(1+i))^2 = 2a^2i$ y que $a^2i(a+ai) = a^3i-a^3$, esto prueba que $K_5 = \mathbb{Q}(a(1+i))$.

6) 2) $\langle\sigma^2,\sigma\beta\rangle \simeq C_2\times C_2$ tiene 4 elementos. Le corresponde un cuerpo $K_2 = \{e \in E|\sigma^2(e) = e, \sigma\beta(e) = e\}$. Notar que σ^2 no fija ninguna de las 4 raíces de p, es $(1,2)(3,4)$ y como $|E : K_2| = 4$, $|K_1 : \mathbb{Q}| = 2$. $\beta(a) = a$ luego $\beta(a^2) = a^2$ y como $\sigma^2(a^2) = a^2$, $\sqrt{2} = a^2 \in K_2$ y por dimensiones, $K_2 = \mathbb{Q}(\sqrt{2})$.

Hemos descritos todos los cuerpos intermedios porque no hay más subgrupos en el grupo diédrico.

Paz Jiménez Seral y Conchita Martínez Pérez
Departamento de Matemáticas
Universidad de Zaragoza