Álgebra I

Grado en Matemáticas

Colección manuales uex - 91

91

ÁLGEBRA I

GRADO EN MATEMÁTICAS

MANUALES UEX

91

PEDRO SANCHO DE SALAS

ÁLGEBRA I

GRADO EN MATEMÁTICAS

UNIVERSIDAD DE EXTREMADURA

2014

UNIVERSIDAD DE EXTREMADURA

UNIÓN EUROPEA
FONDO EUROPEO DE DESARROLLO REGIONAL: UNA MANERA DE HACER EUROPA

GOBIERNO DE EXTREMADURA
Consejería de Empleo, Empresa e Innovación

Edita

Universidad de Extremadura. Servicio de Publicaciones
C./ Caldereros, 2 - Planta 2ª - 10071 Cáceres (España)
Telf. 927 257 041 - Fax 927 257 046
publicac@unex.es
www.unex.es/ publicaciones

ISSN 1135-870-X
ISBN de méritos 978-84-695-9988-4

Índice general

Introducción

El presente texto está concebido por el autor como el manual de la asignatura cuatrimestral Álgebra I, del tercer curso del Grado de Matemáticas de la UEX. En este curso estudiamos la Teoría de Galois como elemento nucleador para introducir tópicos fundamentales en Matemáticas y Álgebra como la Teoría de Grupos, la Teoría de Cuerpos y herramientas como el producto tensorial de módulos y álgebras, y la toma de invariantes por la acción de un grupo. Los únicos requisitos exigidos en esta asignatura son la noción de grupo y cociente por subgrupos, la clasificación de los grupos abelianos finitos, las nociones de anillos, anillos íntegros y cuerpos, cociente por ideales y el teorema chino de los restos, y la noción de módulo y cociente por submódulos.

El manual está divido en cinco temas. En cada tema incluimos un cuestionario, una lista de problemas (con sus soluciones) y la biografía de un matemático relevante (en inglés). Al final incluimos una extensa práctica de ordenador que usa el programa Mathematica.

Hagamos una breve descripción del contenido de la asignatura.

Puede definirse el Álgebra, con ingenua concisión, como la rama de las Matemáticas que estudia las raíces de una ecuación algebraica $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$. Con mayor generalidad, podría decirse que es la disciplina que estudia las soluciones de los sistemas de ecuaciones algebraicas en n indeterminadas

$$\begin{aligned} &p_1(x_1,\ldots,x_n) = 0\\ &p_2(x_1,\ldots,x_n) = 0\\ &\cdots\\ &p_r(x_1,\ldots,x_n) = 0 \end{aligned}$$

Así pues, un primer curso en Álgebra debería estudiar las ecuaciones $p(x) = 0$. Luego, un primer curso en Álgebra debería explicar la Teoría de Galois.

Consideremos un polinomio con coeficientes racionales $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$. El teorema fundamental del Álgebra, que probaremos, afirma que existen $\alpha_1,\ldots,\alpha_n \in \mathbb{C}$ de modo que $p(x) = a_0 \cdot (x-\alpha_1)\cdots(x-\alpha_n)$.

Cada raíz, pareja de raíces, terna de raíces, etc., verifican ciertas relaciones algebraicas. El grupo G formado por las permutaciones de las raíces que respetan estas relaciones (es decir, si $\alpha_{i_1},\ldots,\alpha_{i_r}$ cumplen cierta relación algebraica y $\sigma \in G$, entonces $\sigma(\alpha_{i_1}),\ldots,\sigma(\alpha_{i_r})$ también la cumplen) se denomina el grupo de la ecuación $p(x) = 0$. Si $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ es el cuerpo de descomposición de $p(x)$, es decir, es el mínimo subcuerpo de $\mathbb{C}$ que contiene a las raíces $\alpha_1,\ldots,\alpha_n$ de $p(x)$, se demuestra que G coincide con el grupo de todos los automorfismos de cuerpos de $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$.

Se dice que un grupo G es resoluble si y sólo si existe una cadena de subgrupos

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s = G \qquad (*)$$

de modo que G_{i-1} es normal en G_i y el orden de G_i/G_{i-1} es primo, para todo i.

Se dice que las raíces de $p(x)$ se obtienen por radicales, si pueden expresarse mediante las cuatro operaciones fundamentales (suma, resta, producto y división) y la toma de radicales ($\sqrt[s]{\ }$), de números racionales.

La teoría de Galois prueba que las raíces de $p(x)$ pueden obtenerse por radicales si y sólo si el grupo, G, de la ecuación $p(x) = 0$ es resoluble; y si es conocida la cadena $(*)$, da el procedimiento para calcular las raíces de $p(x)$.

En general, los polinomios de grado n tiene como grupo el grupo de permutaciones S_n. Estos grupos, como probaremos, sólo son resolubles para $n = 2, 3, 4$. De esto se deduce que las raíces de las ecuaciones de grado $2, 3$ y 4 pueden obtenerse por radicales. Por ejemplo, probamos que las raíces $\alpha_1, \alpha_2, \alpha_3$ de $p(x) = x^3 + a_1x^2 + a_2x + a_3$ son

$$\alpha_i = \frac{1}{3}\Big(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\Big)$$

Por otra parte, se obtiene que en general las raíces de las ecuaciones de grado superior a 4 no se pueden expresar mediante radicales.

Históricamente al estudiar las raíces de un polinomio aparecieron los cuerpos $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, como objetos que aclaraban y simplificaban la teoría. Aparecieron los grupos: el grupo de las permutaciones "admisibles" de las raíces de $p(x)$. Recordemos que decíamos que el grupo de permutaciones "admisibles" de las raíces coincide con el grupo G de automorfismos del cuerpo $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Apareció la noción de invariantes por la acción de un grupo: Dado un subgrupo $H \subseteq G$, el subcuerpo de los invariantes de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ por H, que denotamos $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^H$, está definido por

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^H := \{a \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \colon h(a) = a,\ \forall h \in H\}$$

Por el teorema de Artin, $\mathbb{Q} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^G$. Si G es un grupo resoluble y tenemos la cadena de subgrupos

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s = G \qquad (*)$$

de modo que G_{i-1} es normal en G_i y el orden de G_i/G_{i-1} es un número primo p_i, para cada i, entonces tenemos la cadena de subcuerpos de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$,

$$\mathbb{Q} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_s} \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_{s-1}} \subset \cdots \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_0} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

El teorema 90 de Hilbert, prueba que existen $a_i \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i}$ (calculables) tales que

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_{i-1}} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} + \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} \cdot \sqrt[p_i]{a_i} + \cdots + \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{G_i} \cdot (\sqrt[p_i]{a_i})^{p_i - 1}$$

Recurrentemente, tendremos que $\alpha_1,\dots,\alpha_n \in \mathbb{Q}(\alpha_1,\dots,\alpha_n)$ se podrán expresar mediante radicales de elementos de $\mathbb{Q}(\alpha_1,\dots,\alpha_n)^{G_n} = \mathbb{Q}$, afirmación que hemos enunciado más arriba.

La Teoría de Galois resuelve clásicos problemas de construcción con regla y compás. Demos algunos ejemplos:

1. Dice qué polígonos regulares podemos construir (con regla y compás). Por ejemplo, los polígonos regulares de n lados que podemos construir, para $n < 50{,}000$ cumplen
$$n = 2^{m_1}\cdot 3^{m_2}\cdot 5^{m_3}\cdot 17^{m_4}\cdot 257^{m_5}, \qquad m_1 \geq 0, 0 \leq m_2,\dots,m_5 \leq 1$$
2. Demuestra que la cuadratura del círculo es imposible. No se puede construir con regla y compás un cuadrado de área la del círculo unidad.
3. Demuestra que no se puede construir un cubo de volumen 2.
4. Demuestra que en general, los ángulos no se pueden trisectar.

El estudio de las raíces de $p(x)$ es equivalente al estudio del álgebra $\mathbb{Q}[x]/(p(x))$. Con mayor generalidad: Consideremos un sistema de ecuaciones
$$\begin{aligned} &p_1(x_1,\dots,x_n) = 0\\ &p_2(x_1,\dots,x_n) = 0\\ &\cdots\\ &p_r(x_1,\dots,x_n) = 0 \end{aligned}$$
y denotemos por $X \subseteq \mathbb{A}^n$ el conjunto de todas las soluciones de este sistema de ecuaciones. Dos funciones sobre X, es decir, dos polinomios $f(x), g(x) \in \mathbb{Q}[x_1,\dots,x_n]$ coinciden sobre X, si y sólo $f(x)-g(x) \in (p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n)) \subseteq \mathbb{Q}[x_1,\dots,x_n]$. Por lo tanto, podemos considerar el anillo
$$A := \mathbb{Q}[x_1,\dots,x_n]/(p_1(x_1,\dots,x_n),\dots,p_r(x_1,\dots,x_n))$$
como el anillo de todas las funciones (polinómicas) de X. Un resultado general nos dice que el estudio de X coincide con el estudio del anillo A. Con mayor rigor y precisión, el estudio de las soluciones complejas del sistema de ecuaciones anterior (no sólo las soluciones racionales), con sus posibles multiplicidades, etc., es equivalente al estudio del correspondiente anillo de funciones, A.

Si $X' \subseteq \mathbb{A}^m$ es el conjunto de todas las soluciones de este sistema de ecuaciones $q_1(y_1,\dots,y_m) = \cdots = q_s(y_1,\dots,y_m) = 0$ entonces por razones evidentes se dice que
$$\mathbb{Q}[x]/(p_1(x),\dots,p_r(x)) \otimes_{\mathbb{Q}} \mathbb{Q}[y]/(q_1(y),\dots,q_s(y)) = \mathbb{Q}[x,y]/(p_1(x),\dots,p_r(x),q_1(y),\dots,q_s(y))$$
(a falta de definición de producto tensorial $\otimes$, entienda el lector esta igualdad como una definición[1]) es el anillo de funciones de $X \times X'$.

[1]En el curso introducimos el producto tensorial. En Álgebra Lineal, con las aplicaciones multilineales, tensores, determinantes, etc., y en Geometría Diferencial y Física, con el cálculo diferencial tensorial, el producto tensorial es una herramienta y concepto fundamental. En Geometría Algebraica es esencial para la definición de producto directo de variedades algebraicas. En nuestro curso será esencial para cambiar de cuerpo base los objetos considerados.

Dada $A = \mathbb{Q}[x]/(q(x))$ y un cuerpo $K \subseteq \mathbb{C}$, se cumple que

$$A \otimes_{\mathbb{Q}} K = K[x]/(q(x))$$

El teorema chino de los restos mostrará que $A \otimes_{\mathbb{Q}} K$ es isomorfa a un "álgebra trivial" $K \times \overset{n}{\cdots} \times K$ si y sólo si K contiene todas las raíces de $q(x)$ (estamos suponiendo que $q(x)$ no tiene raíces múltiples, por ejemplo cuando sea irreducible). Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $q(x)$, entonces $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es el mínimo cuerpo tal que $A \otimes_{\mathbb{Q}} K$ es trivial. En la Teoría de Galois hay dos procesos fundamentales. El proceso de "trivialización", que consiste en cambiar de cuerpo base, de $\mathbb{Q}$ a $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, es decir, tensar por $\otimes_{\mathbb{Q}}\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, y el proceso inverso de toma de invariantes por el grupo G. Múltiples cuestiones se resuelven primero por cambio de cuerpo base de $\mathbb{Q}$ a $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, y por toma de invariantes por G volvemos a $\mathbb{Q}$.

En diversas ramas de las Matemáticas hay las correspondientes teorías de Galois, con definiciones, teoremas y demostraciones equivalentes. En Topología (y Geometría Diferencial) hay la correspondiente teoría de Galois de revestimientos. El estudio de los revestimientos de los espacios topológicos, la Teoría de Galois de los revestimientos topológicos, es fundamental para la clasificación de los espacios topológicos. Aquí, consideraremos los espacios topológicos en vez de tratar con sus anillos de funciones. Un revestimiento es una aplicación continua $f: X \to Y$ (suele suponerse Y conexo), de modo que para cada punto $y \in Y$ existe un entorno U_y de y, de modo que $f^{-1}(U_y) = U_y \coprod \overset{n}{\cdots} \coprod U_y$. Si $f': Y' \to Y$ es una aplicación continua, se define $X \times_Y Y' := \{(x, y') \in X \times Y' : f(x) = f'(y')\}$. Pues bien, si $f: X \to Y$ es un revestimiento existe un revestimiento mínimo $f': Y' \to Y$ trivializante de X, es decir, tal que $X \times_Y Y' = Y' \coprod \overset{n}{\cdots} \coprod Y'$. En el estudio del revestimiento $X \to Y$ es fundamental el estudio del grupo $G = \mathrm{Aut}_Y(Y') := \{$ Homeomorfismos $\sigma: Y' \to Y'$, tales que $f' \circ \sigma = f'\}$. En el cuadro que sigue relacionamos los objetos de la Teoría de Galois del Álgebra con los de la Topología.

Álgebra	**Topología**
$\mathbb{Q}$	Espacio topológico Y
$\mathbb{Q} \hookrightarrow \mathbb{Q}[x]/(q(x)) =: A$	Revestimiento $X \to Y$
Mín. ext. triv. de A, $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$	Mín. revst. triv. de X, Y'
$A \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$	$X \times_Y Y'$
$G = \mathrm{Aut}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n))$	$G = \mathrm{Aut}_Y(Y')$

Capítulo 1

Teoría de grupos finitos

1.1. Introducción

La estructura más básica y fundamental en Álgebra es la estructura de grupo (y semigrupo). Los anillos, los espacios vectoriales, los módulos, etc. necesitan para su definición de la noción de grupo.

Demos una justificación de carácter muy general para la introducción de la teoría de grupos, siguiendo a Felix Klein en su Erlanger Programm. Dar una teoría (geométrica) es dar una estructura, un espacio con cierta estructura. En esta teoría es fundamental el estudio del grupo de automorfismos de la estructura, es decir, de aquellas biyecciones del espacio que respetan la estructura del espacio. Las nociones y objetos de este espacio, o de la teoría, serán aquéllos que queden invariantes por el grupo de automorfismos recién mencionado. El estudio de las funciones, campos diferenciables, etc., que quedan invariantes por el grupo y el estudio de las relaciones que verifican éstos, son todos los teoremas de la teoría. Es pues el estudio de los grupos (y la teoría de invariantes) un tópico fundamental en Matemáticas.

En el cálculo de las raíces de un polinomio, es conveniente conocer el grupo de aquellas permutaciones de las raíces, que respetan las relaciones algebraicas que verifican éstas. Ya veremos que las raíces de un polinomio se pueden obtener mediante radicales si y sólo si el grupo de permutaciones mencionado es resoluble (noción que más adelante explicaremos).

1.2. Preliminares de teoría de grupos

1. Definición: Sea G un conjunto. Diremos que una aplicación $m : G \times G \to G$ (seguiremos las notaciones $m(g,g') = g \cdot g' = gg'$ y diremos que m ó $\cdot$ es una operación[1]) dota a G de estructura de grupo si cumple las siguientes condiciones:

1. Propiedad asociativa: $g \cdot (g' \cdot g'') = (g \cdot g') \cdot g''$, para todo $g, g', g'' \in G$.
2. Existencia de elemento neutro: Existe un elemento de G, que denotamos por 1 y denominamos elemento neutro, tal que $1 \cdot g = g \cdot 1 = g$, para todo $g \in G$.

[1] La operación $\cdot$, a veces, se denota con otros símbolos: $*$, $\circ$, etc.

3. Existencia de inversos: Para cada $g \in G$ existe un elemento de G, que denotamos por g^{-1} y denominamos inverso de g, tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Si además se cumple que $g \cdot g' = g' \cdot g$, para todo $g, g' \in G$, diremos que G es un grupo abeliano o conmutativo; en cuyo caso, e menudo denotaremos la operación del grupo por $+$, al elemento neutro por 0 y al inverso de cada g por $-g$ (y lo denominaremos opuesto de g).

2. Ejemplos: El conjunto de los números enteros, $\mathbb{Z}$, con la suma es un ejemplo básico de grupo conmutativo. El conjunto de todas las biyecciones de un conjunto X en sí mismo, $Biy X$, con la operación composición de aplicaciones, es un grupo no conmutativo (cuando X contenga más de dos elementos).

Si 1 y $1'$ son elementos neutros del grupo G entonces $1 = 1'$: $1 = 1 \cdot 1' = 1'$. Si h y h' son inversos de $g \in G$, entonces $h = h'$: $h = h \cdot 1 = hgh' = 1 \cdot h' = h'$.

3. Definición: Sea $(G, \cdot)$ un grupo. Diremos que un subconjunto $H \subseteq G$ es un subgrupo de G si cumple las siguientes condiciones:

1. Si $h, h' \in H$ entonces $h \cdot h' \in H$.
2. $1 \in H$.
3. Si $h \in H$ entonces $h^{-1} \in H$.

Si H es un subgrupo de G, entonces la operación de G define en H una estructura de grupo. Recíprocamente, si H es un subconjunto de un grupo G y la operación de G define en H una estructura de grupo entonces H es un subgrupo.

4. Proposición: *La intersección de cualquier familia de subgrupos de un grupo es un subgrupo.*

5. Definición: Dado un subconjunto X de un grupo G, llamaremos subgrupo generado por X y lo denotaremos $\langle X \rangle$, al mínimo subgrupo de G que contiene a X, es decir, a la intersección de todos los subgrupos de G que contienen a X.

6. Notación: Sea $(G, \cdot)$ un grupo y $g \in G$. Si $n > 0$, se define $g^n := g \overset{n}{\cdots} g$; si $n < 0$, se define $g^n := g^{-1} \overset{-n}{\cdots} g^{-1}$; y $g^0 := 1$. Dado $g \in G$, entonces $\langle g \rangle = \{g^n, \text{ con } n \in \mathbb{Z}\}$.

Si G es un grupo conmutativo y escribimos el grupo G con notaciones aditivas (en vez de $\cdot$ escribimos $+$), escribiremos $n \cdot g$, en vez de g^n (como es natural).

Por ejemplo, el subgrupo de $\mathbb{Z}$ generado por $n \in \mathbb{Z}$, es igual a $\langle n \rangle = \{m \cdot n, m \in \mathbb{Z}\} =: n\mathbb{Z}$. El subgrupo de $\mathbb{Z}$ generado por $n, n' \in \mathbb{Z}$, es $\langle n, n' \rangle = \{mn + m'n', m, m' \in \mathbb{Z}\}$.

Dado un número entero $z \in \mathbb{Z}$, llamaremos valor absoluto de z y denotaremos $|z|$, al máximo entre z y $-z$.

7. Teorema de división de números enteros: *Sean n y $d \neq 0$ dos números enteros. Existe una única pareja de números enteros c y r (denominados cociente y resto de dividir n por d), tales que $0 \leq r < |d|$ y*

$$n = c \cdot d + r$$

Demostración. Procedamos por inducción sobre $|n|$, para probar la existencia de c y r.

Si $|n| = 0$, entonces $c = 0$ y $r = 0$. Podemos suponer que $|n| > 0$. El teorema es cierto para d si y sólo si lo es para $-d$ (sólo hay que cambiar c por $-c$), luego podemos suponer que $d > 0$.

Supongamos $n > 0$. Si $n < d$, entonces $c = 0$ y $r = n$. Si $n \geq d$. Sea $n' = n - d$, luego $|n'| = n - d < n = |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' + 1)d + r'$ y hemos concluido.

Supongamos, ahora, $n < 0$. Sea $n' = n + d$, luego $|n'| < |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' - 1)d + r'$ y hemos concluido.

Veamos la unicidad de c y r. Sea $n = cd + r = c'd + r'$, cumpliendo c, c', r, r' lo exigido. Podemos suponer $r \geq r'$. Entonces, $(c - c')d + (r - r') = 0$ y $|c - c'| \cdot |d| = |(c - c')d| = r - r' \leq r < |d|$, luego $c - c' = 0$. Por tanto, $c = c'$ y $r = n - cd = r'$.

□

8. Teorema: *Si H es un subgrupo del grupo (aditivo) de los números enteros $\mathbb{Z}$, entonces existe un único número natural n tal que $H = n\mathbb{Z}$.*

Demostración. Si $H = \{0\}$ entonces $H = 0 \cdot \mathbb{Z}$.

Supongamos $H \neq \{0\}$. Existen naturales positivos en H, porque el opuesto de cada número entero de H pertenece a H. Sea $n \in H$ el mínimo número natural no nulo contenido en H. Veamos que $H = n\mathbb{Z}$: Obviamente, $n\mathbb{Z} \subseteq H$. Dado $m \in H \subset \mathbb{Z}$, existen números enteros c y r tales que

$$m = cn + r, \quad 0 \leq r < n$$

Luego, $r = m - cn \in H$, porque $m, -cn \in H$. Por la definición de n, se tiene que $r = 0$. Luego, $m \in n\mathbb{Z}$, $H \subseteq n\mathbb{Z}$ y $H = n\mathbb{Z}$.

Por último, demostremos la unicidad: observemos que si un número natural m pertenece a $n\mathbb{Z}$, entonces $m \geq n$. Por tanto, si $m\mathbb{Z} = n\mathbb{Z}$, $m \geq n$ y $n \geq m$, luego $m = n$.

□

Si $m \in n\mathbb{Z}$ diremos que m es un múltiplo de n y que n es un divisor de m.

Sea $(G, +)$ un grupo abeliano y $G_1, G_2 \subseteq G$ dos subgrupos. Denotamos $\langle G_1, G_2 \rangle = G_1 + G_2$ y el lector puede comprobar que $G_1 + G_2 = \{g_1 + g_2,\ g_1 \in G_1\ g_2 \in G_2\}$.

Por la proposición anterior, dados $n, n' \in \mathbb{Z}$, existe $m \in \mathbb{N}$ tal que $n\mathbb{Z} + n'\mathbb{Z} = m\mathbb{Z}$. Observemos que $n, n' \in m\mathbb{Z}$, luego m es divisor de n y n'. Si $m' \in \mathbb{N}$ es divisor de n y n' entonces $m \in n\mathbb{Z} + n'\mathbb{Z} \subseteq m'\mathbb{Z}$, y m' divide a m. Por tanto, m es el máximo común divisor de n y n'.

Por la proposición anterior, dados $n, n' \in \mathbb{Z}$, existe $m \in \mathbb{N}$ tal que $n\mathbb{Z} \cap n'\mathbb{Z} = m\mathbb{Z}$. El lector, puede comprobar que m es el mínimo común múltiplo de n y n'.

9. Definición: Diremos que una aplicación $f : G \to G'$ entre dos grupos es un morfismo de grupos si para todo $g, g' \in G$ se cumple que

$$f(g \cdot g') = f(g) \cdot f(g')$$

Diremos que f es un isomorfismo de grupos si f es biyectiva (en tal caso la aplicación inversa f^{-1} es un isomorfismo de grupos). Diremos que es un epimorfismo (resp. monomorfismo) de grupos si f es epiyectiva (resp. inyectiva).

Si $f: G \to G'$ es un morfismo de grupos entonces $f(1) = 1$: $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ y multiplicando por $f(1)^{-1}$ obtenemos $1 = f(1)$. Además, $f(g^{-1}) = f(g)^{-1}$: $1 = f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$ y multiplicando por $f(g)^{-1}$ obtenemos $f(g)^{-1} = f(g^{-1})$.

Denotaremos $\mathrm{Hom}_{grp}(G, G')$ al conjunto de todos los morfismos de grupos de G en G'.

10. Definición: Sea $f: G \to G'$ un morfismo de grupos. Llamaremos núcleo de f y lo denotaremos $\mathrm{Ker}\, f$, al subconjunto de G

$$\mathrm{Ker}\, f := f^{-1}(1) = \{g \in G : f(g) = 1\}$$

Llamaremos imagen de f, que denotaremos $\mathrm{Im}\, f$, a la imagen de la aplicación f, es decir,

$$\mathrm{Im}\, f := \{f(g) \in G', g \in G\}$$

11. Proposición: $\mathrm{Ker}\, f$ *es un subgrupo de* G *e* $\mathrm{Im}\, f$ *es un subgrupo de* G'. *En general, la antimagen por un morfismo de grupos de un subgrupo es subgrupo y la imagen de un subgrupo es subgrupo.*

Dado un morfismo de grupos $f: G \to G'$ y $g \in G$, calculemos el conjunto de elementos $g' \in G$ tales que $f(g') = f(g)$: $f(g') = f(g)$ si y sólo si $1 = f(g)^{-1} \cdot f(g') = f(g^{-1} \cdot g')$, es decir, si y sólo si $g^{-1} \cdot g' \in \mathrm{Ker}\, f$, que equivale a decir que $g' \in g \cdot \mathrm{Ker}\, f := \{g \cdot h, h \in \mathrm{Ker}\, f\}$.

12. Proposición: *Un morfismo de grupos* $f: G \to G'$ *es inyectivo si y sólo si* $\mathrm{Ker}\, f = \{1\}$.

Si identificamos los elementos de G cuando tengan la misma imagen, obtenemos un conjunto biyectivo con la imagen. Por tanto, el conjunto $\bar{G} := \{\bar{g}, g \in G : \bar{g}' = \bar{g}$ si y sólo si $g' \in g \cdot \mathrm{Ker}\, f\}$ es biyectivo con $\mathrm{Im}\, f$. De hecho esta biyección es un isomorfismo de grupos como veremos.

Sea $H \subseteq G$ un subgrupo y $g, g' \in G$.

Si $g' \in gH$ entonces $g'H = gH$: Sea $h \in H$, tal que $g' = gh$. Entonces, $g'H = ghH = gH$.

Si $g' \notin gH$, entonces $g'H \cap gH = \emptyset$, pues si $z \in g'H \cap gH$, entonces $g'H = zH = gH$.

En conclusión, dados $g, g' \in G$, o $gH = g'H$ o bien $g'H \cap gH = \emptyset$.

13. Definición: Sea $H \subseteq G$ un subgrupo. Llamaremos conjunto cociente de G por H, que denotaremos G/H, al conjunto

$$G/H := \{\bar{g},\ \text{con } g \in G : \bar{g}' = \bar{g} \text{ si y sólo si } g' \in g \cdot H \text{ (o equivalentemente } g'H = gH)\}$$

Es decir, si en G identificamos cada $g \in G$ con todos los elementos de $gH \subseteq G$, obtenemos el conjunto G/H.

14. Notación: Se dice que g es congruente con g' módulo H y se denota $g \equiv g' \, mod\, H$, cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g'H$ (o $g'^{-1}g \in H$). En notaciones aditivas, si $(G, +)$ es un grupo abeliano y $H \subset G$ es un subgrupo, entonces $g \equiv g' \, mod\, H$ cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g' + H$ (o $-g' + g \in H$).

La aplicación $G \to G/H$, $g \mapsto \bar{g}$, se denomina el morfismo de paso cociente (por H).

15. Definición: Llamaremos orden de un conjunto X, que denotaremos $|X|$, al número de elementos del conjunto. Si el conjunto tiene un número infinito de elementos diremos que es de cardinal infinito.

16. Ejemplo: Si $n > 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un conjunto de orden n, explícitamente $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \ldots, \overline{n-1}\}$: Dado $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$, por el teorema de división de números enteros, existen números enteros únicos c y r, con $0 \leq r < n$, de modo que $m = cn + r$. Por tanto, $\bar{m}$ es igual a un único $\bar{r} \in \{\bar{0}, \ldots, \overline{n-1}\}$.

17. Teorema de Lagrange: *Sea G un grupo de orden finito. Si H es un subgrupo de G entonces*

$$|G| = |G/H| \cdot |H|$$

Demostración. $G = \coprod_{\bar{g} \in G/H} g \cdot H$ y $|gH| = |H|$ (porque la aplicación $H \to gH$, $h \mapsto gh$ es biyectiva). Por tanto, $|G| = |G/H| \cdot |H|$.

□

18. Definición: Se dice que un subgrupo $H \subseteq G$ es normal (en G) cuando $gHg^{-1} \subseteq H$, para todo $g \in G$, es decir, si $ghg^{-1} \in H$, para todo $g \in G$ y $h \in H$.

Si G es un grupo conmutativo, todo subgrupo de G es normal en G.

Si H es normal y tomamos $g^{-1} \in G$, tendremos $g^{-1}Hg \subseteq H$, como $g^{-1}Hg \subseteq H$ entonces $gHg^{-1} = H$ (para todo $g \in G$). Por tanto, $gH = Hg$, para todo $g \in G$, y recíprocamente si un subgrupo cumple esta condición el subgrupo es normal.

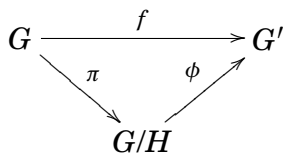
19. Teorema: *Sea $H \subseteq G$ un subgrupo y $\pi : G \to G/H$ la aplicación de paso al cociente. H es un subgrupo normal de G si y sólo si existe en G/H una (única) estructura de grupo, de modo que π sea un morfismo de grupos.*

Demostración. Supongamos que H es normal en G. Definamos en G/H la operación $\bar{g} \cdot \bar{g'} := \overline{gg'}$, que está bien definida porque $gHg'H = gg'HH = \underline{gg'H}$. La propiedad asociativa se cumple de modo obvio, $\bar{1}$ es el elemento neutro y $\overline{g^{-1}}$ es el inverso de $\bar{g} \in G/H$. Luego, G/H es grupo. Además, $\pi : G \to G/H$ es morfismo de grupos, pues $\pi(g \cdot g') = \overline{gg'} = \bar{g} \cdot \bar{g'} = \pi(g) \cdot \pi(g')$.

Recíprocamente, si π es un morfismo de grupos, entonces $\bar{g} \cdot \bar{g'} = \pi(g) \cdot \pi(g') = \pi(gg') = \overline{gg'}$. Por tanto, la operación en G/H está determinada. Además, dado $h \in H$ y $g \in G$, tenemos que $\bar{h} \cdot \bar{g} = \bar{1} \cdot \bar{g} = \bar{g}$, luego $hg \in gH$, para todo $h \in H$, es decir, $Hg \subseteq gH$. Por tanto, $g^{-1}Hg \subseteq H$, para todo $g \in G$ y tomando $g^{-1} \in G$, $gHg^{-1} \subseteq H$ y H es normal en G.

□

20. Propiedad universal del grupo cociente: *Sea $H \subseteq G$ un subgrupo normal y $\pi : G \to G/H$ el morfismo de paso al cociente. Un morfismo de grupos $f : G \to G'$ factoriza a través de π, es decir, existe un (único) morfismo de grupos $\phi : G/H \to G'$ de modo que el diagrama*



es conmutativo si y sólo si $H \subseteq \operatorname{Ker} f$.

Demostración. Si existe ϕ (cumpliendo lo exigido), entonces $\phi(\bar{g}) = \phi(\pi(g)) = f(g)$, luego está determinado. Además, $1 = \phi(\bar{1}) = \phi(\bar{h}) = f(h)$, para todo $h \in H$, luego $H \subseteq \operatorname{Ker} f$.

Recíprocamente, supongamos $H \subseteq \operatorname{Ker} f$. Definamos $\phi(\bar{g}) := f(g)$, que está bien definida porque $f(gH) = f(g)f(H) = f(g)$. Además, $\phi(\pi(g)) = \phi(\bar{g}) = f(g)$.

□

21. Teorema de isomorfía: *Sea $f: G \to G'$ un morfismo de grupos. La aplicación, $\phi: G/\operatorname{Ker} f \to \operatorname{Im} f$, $\phi(\bar{g}) := f(g)$, es un isomorfismo de grupos.*

Demostración. Por la propiedad universal del grupo cociente, sabemos que $\phi \circ \pi = f$ y $\operatorname{Im} f = \operatorname{Im}(\phi \circ \pi) = \operatorname{Im} \phi$, porque π es epiyectiva. Veamos que ϕ es inyectiva: si $1 = \phi(\bar{g}) = f(g)$, entonces $g \in \operatorname{Ker} f$ y $\bar{g} = \bar{1}$, luego $\operatorname{Ker} \phi = \{\bar{1}\}$. □

1.3. Grupos cíclicos

1. Definición: Diremos que un grupo G es cíclico si está generado por uno de sus elementos, es decir, existe $g \in G$ de modo que $G = \langle g \rangle$.

2. Proposición: *Un grupo G es cíclico si y sólo si es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, para algún un número natural n.*

Demostración. $\mathbb{Z}/n\mathbb{Z}$ es un grupo (aditivo) cíclico, generado por $\bar{1}$.

Supongamos que $G = \langle g \rangle$ es cíclico. Sea $f: \mathbb{Z} \to G$, el morfismo definido por $f(n) = g^n$. Es fácil comprobar que f es un morfismo de grupos. $\operatorname{Im} f$ es un subgrupo de G, que contiene a g, luego $\operatorname{Im} f = G$ y f es epiyectivo. $\operatorname{Ker} f$ es un subgrupo de $\mathbb{Z}$, luego existe $n \in \mathbb{N}$ tal que $\operatorname{Ker} f = n\mathbb{Z}$. Por el teorema de isomorfía $\mathbb{Z}/n\mathbb{Z} \simeq G$. □

$\mathbb{Z}/n\mathbb{Z}$ es un grupo conmutativo, pues es cociente de $\mathbb{Z}$ que es conmutativo. Por tanto, todo grupo cíclico es conmutativo.

3. Definición: Llamaremos orden de un elemento $g \in G$ de un grupo, al orden del subgrupo $\langle g \rangle$ de G que genera.

En la proposición anterior hemos dado el isomorfismo $\mathbb{Z}/n\mathbb{Z} \simeq \langle g \rangle$, $\bar{m} \mapsto g^m$. Por tanto, si $n > 0$, el orden de g es igual a $|\langle g \rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$, $\langle g \rangle = \{1, g^1, \ldots, g^{n-1}\}$ y n es el mínimo número natural positivo tal que $g^n = 1$, además, si $g^m = 1$, entonces m es un múltiplo del orden de g. Si $n = 0$, entonces el orden de g es $|\langle g \rangle| = |\mathbb{Z}| = \infty$ y $\langle g \rangle = \{\ldots, g^{-m}, \ldots, 1, g^1, \ldots, g^m, \ldots\}$ (cumpliendo $g^i \neq g^j$, para todo $i, j \in \mathbb{Z}$, $i \neq j$).

4. Si G es un grupo de orden $m < \infty$, entonces el orden de todo elemento $g \in G$ divide a m, ya que el orden de todo subgrupo $\langle g \rangle$ divide al orden del grupo G, por el teorema de Lagrange. Es decir, $g^{|G|} = 1$.

5. Proposición: *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sea $G = \langle g \rangle$ un grupo cíclico y $\pi: \mathbb{Z} \to G$, $\pi(n) := g^n$ un epimorfismo de grupos. Dado un subgrupo $H \subseteq G$, se cumple que $H = \pi(\pi^{-1}(H))$. Ahora bien, $\pi^{-1}(H)$ es un subgrupo de $\mathbb{Z}$, luego es cíclico (es decir, generado por un elemento z). Por tanto, $H = \pi(\pi^{-1}(H))$ está generado por $\pi(z)$ y es cíclico. □

6. Proposición: *El elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es un generador si y sólo si el máximo común divisor de m y n es 1 ("m y n son primos entre sí").*

Demostración. Consideremos el epimorfismo natural $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(z) = \bar{z}$. Es claro que $\pi^{-1}(\langle \bar{m} \rangle) = m\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$, donde r es el máximo común divisor de m y n. Por otra parte, $\bar{m}$ es un generador de $\mathbb{Z}/m\mathbb{Z}$, es decir, $\langle \bar{m} \rangle = \mathbb{Z}/m\mathbb{Z}$, si y sólo $\pi^{-1}(\langle \bar{m} \rangle) = \mathbb{Z}$. Por tanto, $\bar{m}$ es un generador de $\mathbb{Z}/m\mathbb{Z}$ si y sólo si $r = 1$. □

Así pues, si $G = \langle g \rangle$ es un grupo cíclico de orden $n > 0$, entonces g^m es un generador de G si y sólo si m y n son primos entre sí.

1.4. Grupo simétrico

El grupo simétrico S_n es el grupo de todas las biyecciones (o "permutaciones") de un conjunto de n-elementos en sí mismo, con la operación composición de aplicaciones.

Comentario: Una biyección entre dos conjuntos $\tau\colon X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f\colon X \to X$, que aplica x en $f(x)$, tenemos la correspondiente aplicación en Y: "la que aplica $\tau(x)$ en $\tau(f(x))$, es decir, la aplicación $\tau \circ f \circ \tau^{-1}\colon Y \to Y$". Así el grupo de las permutaciones de X se identifica con el grupo de las permutaciones de Y (vía la identificación de X con Y). Con mayor precisión, el morfismo

$$BiyX \to BiyY, \quad \sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$$

es un isomorfismo de grupos (como el lector puede comprobar).

Si Y es un conjunto de orden n, entonces Y es biyectivo con $\{1,\dots,n\} =: X$ y $BiyY = BiyX =: S_n$. El número de permutaciones de n elementos es $n!$, luego $|S_n| = n!$.

1. Definición: Dados r elementos distintos $x_1,\dots,x_r \in X$, con $r > 1$, denotaremos $(x_1,\dots,x_r) = \sigma \in BiyX$ a la permutación definida por $\sigma(x_i) = x_{i+1}$, para todo $i < r$; $\sigma(x_r) = x_1$; y $\sigma(x) = x$, para todo $x \notin \{x_1,\dots,x_r\}$. Diremos que $(x_1,\dots,x_r)$ es un ciclo y observemos que es de orden r. Si $r = 2$, diremos que el ciclo (x_1,x_2) es una transposición. Diremos que dos ciclos $(x_1,\dots,x_r),(x'_1,\dots,x'_{r'})$ de $BiyX$ son disjuntos si $x_i \neq x'_j$ para todo i,j.

2. Lema: *Si $\sigma = (x_1,\dots,x_r)$ y $\sigma' = (x'_1,\dots,x'_{r'})$ son disjuntos, entonces conmutan, es decir, $\sigma \circ \sigma' = \sigma' \circ \sigma$.*

Demostración. Para $x \in \{x_1,\dots,x_r\}$, $(\sigma \circ \sigma')(x) = \sigma(x) = (\sigma' \circ \sigma)(x)$. Para $x \in \{x'_1,\dots,x'_r\}$, $(\sigma \circ \sigma')(x) = \sigma'(x) = (\sigma' \circ \sigma)(x)$. Para $x \notin \{x_i,x'_j\}_{i,j}$, $(\sigma \circ \sigma')(x) = x = (\sigma' \circ \sigma)(x)$.

De otro modo (siguiendo el comentario anterior): $\sigma' \circ \sigma \circ \sigma'^{-1} = (\sigma'(x_1),\dots,\sigma'(x_r)) = (x_1,\dots,x_r) = \sigma$ y hemos concluido.

□

3. Teorema: *Toda permutación $\sigma \in S_n$, distinta de la identidad, es igual a un producto de ciclos disjuntos, de modo único salvo el orden de los factores.*

Demostración. Sea $x \in X$, tal que $\sigma(x) \neq x$. Sea r el mínimo número natural positivo tal que $\sigma^r(x) = x$ (tal número existe porque el orden de σ, que divide al orden de S_n, es finito). Para todo $0 \leq s < s' < r$, se cumple que $\sigma^{s'}(x) \neq \sigma^s(x)$: pues componiendo con σ^{-s} son distintos, pues $\sigma^{s'-s}(x) \neq x$, porque $0 < s' - s < r$. Sea $\sigma_1 = (x, \sigma(x), \ldots, \sigma^{r-1}(x))$. Entonces, como σ_1 y σ coinciden sobre $\{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$ y σ_1 es la identidad sobre $X \setminus \{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$, se cumple que $\sigma_1^{-1} \circ \sigma$ deja fijos $\{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$ y los que dejaba fijos σ. Reiterando el proceso obtenemos ciclos disjuntos $\sigma_1, \ldots, \sigma_s$ tales que $\sigma_s^{-1} \circ \cdots \circ \sigma_1^{-1} \circ \sigma = \mathrm{Id}$. Luego, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$.

Sea otra descomposición $\sigma = \tau_1 \circ \cdots \tau_t$ en producto de ciclos disjuntos. Reordenando, podemos suponer que $\tau_1(x) \neq x$. Es decir, x "aparece" en el ciclo τ_1 (y en el de σ_1). Luego, $\tau_1(x) = \sigma(x) = \sigma_1(x)$. Obviamente, $\tau_1(x) = \sigma(x) = \sigma_1(x)$ "aparece" en ciclo de τ_1 y en el de σ_1. Luego, $\tau_1^2(x) = \sigma^2(x) = \sigma_1^2(x)$. Así sucesivamente, $\tau_1^i(x) = \sigma^i(x) = \sigma_i^2(x)$, para todo i. Por tanto, $\tau_1 = \sigma_1$ y $\sigma_2 \circ \cdots \sigma_s = \tau_2 \circ \cdots \circ \tau_t$. Reiterando el argumento concluimos que, después de reordenar los factores, $\sigma_2, \ldots, \sigma_s$ coinciden con $\tau_2, \ldots, \tau_t$.

□

4. Definición: Sea $\sigma \in S_n$ una permutación distinta de la identidad. Sea $\sigma = \sigma_1 \circ \cdots \sigma_s$ una descomposición en producto de ciclos disjuntos y d_i el orden de σ_i. Reordenando podemos suponer que $d_1 \geq d_2 \geq \cdots \geq d_s$. Diremos que $d_1, \ldots, d_s$ es la forma de σ.

5. Definición: Dado un elemento $g \in G$, diremos que el morfismo $\tau_g : G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h, h' \in G$ son conjugados si y sólo si existe $g \in G$, de modo que $\tau_g(h) = h'$.

6. Teorema: *La condición necesaria y suficiente para que $\sigma, \sigma' \in S_n$ sean conjugadas es que tengan la misma forma.*

Demostración. Sea $\sigma = (x_{11}, \ldots, x_{1d_1}) \circ \cdots \circ (x_{s1}, \cdots, x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_{11}), \ldots, \tau(x_{1d_1})) \circ \cdots \circ (\tau(x_{s1}), \cdots, \tau(x_{sd_s}))$$

que tiene la misma forma. Sea $\sigma' = (x'_{11}, \ldots, x'_{1d_1}) \circ \cdots \circ (x'_{s1}, \cdots, x'_{sd_s})$. Si τ es cualquier permutación que cumpla $\tau(x_{ij}) = x'_{ij}$, para todo i, j, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

7. Proposición: *Si $d_1, \ldots, d_s$ es la forma de $\sigma \in S_n$, entonces el orden de σ es el mínimo común múltiplo de $d_1, \ldots, d_s$.*

Demostración. Escribamos $\sigma = \sigma_1 \cdots \sigma_s$ como producto de ciclos disjuntos. Entonces, $\sigma^n = \sigma_1^n \cdots \sigma_s^n$ y σ_i^n es "disjunta" con σ_j^n, para $i \neq j$. Luego, $\sigma^n = \mathrm{Id}$ si y sólo si $\sigma_1^n = \cdots = \sigma_s^n = \mathrm{Id}$. Luego el orden de σ es el mínimo común múltiplo de los órdenes de los σ_i. □

8. Proposición: *Todo permutación $\sigma \in S_n$ es producto de transposiciones.*

Demostración. Como toda permutación es producto de ciclos, basta probar que todo ciclo es producto de transposiciones. Sea, pues, un ciclo $(x_1, \ldots, x_r) \in S_n$. Obviamente,

$$(x_1, \ldots, x_r) = (x_1, x_2)(x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3)(x_3, \ldots, x_r) = \cdots = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r)$$

□

Signo de una permutación.

Cada permutación $\sigma \in S_n = Biy(\{1,2,\dots,n\})$ define una biyección del anillo de polinomios en n variables con coeficientes números racionales, $\mathbb{Q}[x_1,\dots,x_n]$: $\mathbb{Q}[x_1,\dots,x_n] \to \mathbb{Q}[x_1,\dots,x_n]$, $p(x_1,\dots,x_n) \mapsto p(x_1,\dots,x_n)^\sigma := p(x_{\sigma(1)},\dots,x_{\sigma(n)})$.

Sea $\delta(x_1,\dots,x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1,\dots,x_n]$. Dada una permutación $\sigma \in S_n = Biy(\{1,2,\dots,n\})$, es fácil comprobar que $\delta(x_1,\dots,x_n)^\sigma = \delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \pm\delta(x_1,\dots,x_n)$.

9. Definición: Dada $\sigma \in S_n$, llamaremos signo de σ, que denotaremos $\operatorname{sign}(\sigma)$, al número entero 1 ó -1 tal que $\delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \operatorname{sign}(\sigma)\cdot\delta(x_1,\dots,x_n)$.

10. Proposición: *Consideremos el grupo (multiplicativo)* $\{1,-1\}$. *El morfismo natural*

$$\operatorname{sign}\colon S_n \to \{1,-1\},\ \sigma \mapsto \operatorname{sign}(\sigma)$$

es un morfismo de grupos.

Demostración. $\operatorname{sign}(\sigma'\sigma)\cdot\delta = \delta^{\sigma'\sigma} = (\delta^\sigma)^{\sigma'} = (\operatorname{sign}(\sigma)\delta)^{\sigma'} = \operatorname{sign}(\sigma')\cdot\operatorname{sign}(\sigma)\cdot\delta$. Luego, $\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\sigma') = \operatorname{sign}(\sigma\cdot\sigma')$. □

Es fácil ver que $\operatorname{sign}(\mathrm{Id}) = 1$ y que $\operatorname{sign}((1,2)) = -1$.

Evidentemente, sign es un epimorfismo (para $n > 1$). Evidentemente, sign es un epimorfismo (para $n > 1$).

11. Definición: Llamaremos subgrupo alternado de S_n, que denotaremos A_n, al núcleo del morfismo sign, es decir, al subgrupo (normal) de S_n formado por las permutaciones de signo positivo.

Por el teorema de isomorfía $S_n/A_n \simeq \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Por el teorema de Lagrange, $|A_n| = |S_n|/2 = n!/2$ $(n > 1)$.

Observemos que el signo es invariante por conjugaciones, es decir,

$$\operatorname{sign}(\tau\sigma\tau^{-1}) = \operatorname{sign}(\tau)\cdot\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\tau)^{-1} = \operatorname{sign}(\sigma)$$

En particular, el signo de toda transposición es -1, porque todas son conjugadas de la transposición $(1,2)$.

12. Proposición: *Si la forma de una permutación* $\sigma \in S_n$ *es* $d_1,\dots,d_r$, *entonces*

$$\operatorname{sign}(\sigma) = (-1)^{d_1-1}\cdots(-1)^{d_r-1} = (-1)^{d_1+\cdots+d_r-r}.$$

Demostración. Si $\sigma = (x_1,\dots,x_r)$ es un ciclo, entonces

$$(x_1,\dots,x_r) = (x_1,x_2)(x_2,x_r)\cdots(x_{r-1},x_r)$$

es producto de $r-1$ transposiciones. Como el morfismo sign es un morfismo de grupos, $\operatorname{sign}(\sigma) = (-1)^{r-1}$.

En general, $\sigma = \sigma_1\cdots\sigma_r$, donde σ_i es un ciclo de orden d_i. Por tanto, $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma_1)\cdots\operatorname{sign}(\sigma_r) = (-1)^{d_1-1}\cdots(-1)^{d_r-1}$. □

1.5. Producto directo y semidirecto de grupos

1. Definición: Dados dos grupos G_1, G_2 se define el producto directo de ellos al conjunto producto cartesiano de ambos, $G_1 \times G_2$, con la operación de grupo definida por la fórmula:

$$(g_1, g_2) \cdot (g_1', g_2') := (g_1 g_1', g_2 g_2')$$

2. Ejemplo: Los grupos abelianos generados por un número finito de elementos son isomorfos a un producto directo de grupos cíclicos.

3. Notación: Dados dos subgrupos $H, H' \subseteq G$, denotamos $H \cdot H' := \{hh' \in G$, con $h \in H$ y $h' \in H'\}$.

4. Proposición: *Sean $H, H' \subseteq G$ dos subgrupos normales. Supongamos $H \cap H' = \{1\}$. Entonces, los elementos de H conmutan con los de H' y HH' es un subgrupo de G isomorfo a $H \times H'$.*

Demostración. Dados $h \in H$ y $h' \in H'$, se tiene que $(hh'h^{-1})h'^{-1} = h(h'h^{-1}h'^{-1}) \in H \cap H' = \{1\}$, luego $hh' = h'h$. Ahora ya, la aplicación

$$m : H \times H' \to G,\ m((h, h')) := hh'$$

es un morfismo de grupos inyectivo. Luego, $H \times H' \simeq \operatorname{Im} m = HH'$. □

5. Definición: Sea $H \subseteq G$ un subgrupo. Llamaremos normalizador de H en G, que denotaremos $N(H)$ (o $N_G(H)$), al subgrupo de G definido por

$$N(H) := \{g \in G : gHg^{-1} = H\}$$

El normalizador de H en G es el máximo subgrupo de G en el que H es normal.

6. Proposición: *Sean $H, H' \subseteq G$ dos subgrupos. Supongamos $H \cap H' = \{1\}$ y que $H' \subseteq N(H)$. Entonces, HH' es un subgrupo de G y la aplicación*

$$m : H \times H' \to H \cdot H', \quad m(h, h') := hh'$$

es biyectiva.

Demostración. Dados $h_1 h_1' \in HH'$ y $h_2 h_2' \in HH'$, entonces

$$(h_1 h_1') \cdot (h_2 h_2') = (h_1 (h_1' h_2 {h_1'}^{-1})) \cdot (h_1' h_2') \in HH'.$$

Dado $hh' \in HH'$, $(hh')^{-1} = h'^{-1}h^{-1} = h'^{-1}h^{-1}h') \cdot h'^{-1} \in HH'$. Además, $1 \in HH'$. Por tanto, HH' es un subgrupo de G.

Veamos que m es inyectiva: Si $m((h_1, h_1')) = m((h_2, h_2'))$, entonces $h_1 h_1' = h_2 h_2'$. Por lo tanto, $h_2^{-1} h_1 = h_2' {h_1'}^{-1} \in H \cap H' = \{1\}$, y $h_1 = h_2$ y $h_1' = h_2'$. Obviamente, m es epiyectiva.

□

Observemos, en la proposición anterior, que aunque $H \times H' \to HH'$, $(h,h') \mapsto hh'$ es una biyección no es morfismo de grupos, pues $(h_1h'_1)\cdot(h_2h'_2) = (h_1(h'_1h_2{h'_1}^{-1}))\cdot(h'_1h'_2)$. Si $H \rtimes H'$ es el grupo que como conjunto es $H \times H'$ y cuya operación $*$ está definida por

$$(h_1,h'_1)*(h_2,h'_2) := (h_1(h'_1h_2{h'_1}^{-1}),h'_1h'_2)$$

entonces $m: H \rtimes H' \to HH'$, $m((h,h')) := hh'$ es un isomorfismo de grupos. Se dice que $H \rtimes H'$ es el producto semidirecto de H y H'.

7. Ejercicio: Sean G y G' dos grupos y $\phi: G' \to \mathrm{Aut}_{grp}(G)$ un morfismo de grupos. Consideremos las aplicaciones $i_1: G \to \mathrm{Biy}(G \times G')$, $i_1(g)$ definida por $i_1(g)(g_1,g') := (gg_1,g')$ y $i_2: G' \to \mathrm{Biy}(G \times G')$, $i_2(g')$ definida por $i_2(g')(g,g'_1) := (\phi(g')(g),g'g'_1)$. Probar que i_1 e i_2 son morfismos inyectivos de grupos. Si identificamos G y G' con sus imágenes por i_1 e i_2 respectivamente, probar que $G \cap G' = \{1\}$. Probar que $g'gg'^{-1} = \phi(g')(g)$ y que $G' \subseteq N(G)$. Se dice que $G \rtimes G'$ es el producto semidirecto de los grupos G y G'. Probar que $(g_1,g'_1)*(g_2,g'_2) = (g_1\phi(g'_1)(g_2),g'_1g'_2)$.

8. Ejercicio: Sea $G' \to \mathrm{Aut}_{gr}(G)$, $g' \mapsto \mathrm{Id}$, para todo $g' \in G'$, el morfismo trivial. Probar que $G \rtimes G' = G \times G'$.

9. Grupo de afinidades de $\mathbb{R}^n$: *Sea $G = \mathbb{R}^n$ (con la operación +) y $G' = Gl_n(\mathbb{R})$ el grupo de las matrices de orden n invertibles (con la operación componer matrices). Consideremos G como subgrupo de* $\mathrm{Biy}(\mathbb{R}^n)$ *vía el morfismo inyectivo $G \to \mathrm{Biy}(\mathbb{R}^n)$, $e \mapsto T_e$, donde $T_e(e') := e + e'$. Consideremos G' como subgrupo de* $\mathrm{Biy}(\mathbb{R}^n)$ *vía la inclusión obvia. Entonces, $G \cap G' = \{\mathrm{Id}\}$ y $G' \subset N(G)$. Al producto semidirecto $\mathbb{R}^n \rtimes Gl_n(\mathbb{R})$, se le denomina grupo de afinidades de $\mathbb{R}^n$.*

10. El grupo diédrico D_n: *Se denomina grupo diédrico D_n ($n > 2$) al grupo formado por todas las isometrías del plano que dejan estable el polígono regular de n-lados (la operación de D_n es la composición de isometrías).*

Puede demostrarse que D_n está generado por el giro g de $2\pi/n$ radianes y una simetría τ (del polígono). Además, se tiene que $\langle g\rangle \cap \langle\tau\rangle = \{\mathrm{Id}\}$ y $\tau g\tau^{-1} = g^{-1}$. Por tanto, $\langle g\rangle$ es normal en D_n, y por la proposición 1.5.6, $D_n = \langle g\rangle \rtimes \langle\tau\rangle = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, explícitamente

$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_n,\ (\bar{r},\bar{s}) \mapsto g^r \cdot \tau^s$$

Las isometrías del plano que dejan estable un polígono regular de n-lados están determinadas por cómo permutan los vértices. Por tanto, si numeramos consecutivamente los vértices del polígono regular con los números $1,\ldots,n$, tenemos un morfismo inyectivo $D_n \hookrightarrow S_n$, de modo que g se corresponde con la permutación $(1,2,\ldots,n)$ y τ con la permutación que asigna $i \mapsto n-i$, para todo $1 \le i < n$.

11. Ejercicio: Sea $n \ge 2$, $A_n \subseteq S_n$ y $\mathbb{Z}/2\mathbb{Z} = \langle(1,2)\rangle \subseteq S_n$. Probar que $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

1.6. G-conjuntos

1. Definición: Sea G un grupo y X un conjunto. Dotar a un conjunto X de estructura de G-conjunto, es dar una aplicación $\phi: G \times X \to X$, tal que si denotamos $\phi((g,x)) = g\cdot x$, entonces se verifican las dos condiciones

1. $1 \cdot x = x$, para todo $x \in X$.
2. $g \cdot (g' \cdot x) = (g \cdot g') \cdot x$, para todo $x \in X$ y $g, g' \in G$.

2. Notación: Si X es un G conjunto se suele decir que G "opera" en X.

Sean X e Y dos G-conjuntos. Entonces,

1. $X \times Y$ es G-conjunto: $g \cdot (x, y) := (gx, gy)$.
2. Obviamente, $X \coprod Y$ es G-conjunto.
3. $\mathrm{Aplic}(X, Y)$ es G-conjunto: $(g \cdot f)(x) := g \cdot f(g^{-1} \cdot x)$, para todo $f \in \mathrm{Aplic}(X, Y)$.

3. Ejemplo: Sea $T : \mathbb{R}^2 \to \mathbb{R}^2$ el giro del plano de 120 grados, es decir, el endomorfismo lineal de matriz en las bases usuales $\begin{pmatrix} cos(2\pi/3) & -sen(2\pi/3) \\ sen(2\pi/3) & cos(2\pi/3) \end{pmatrix}$. Dotemos a $\mathbb{R}^2$ de estructura de $\mathbb{Z}/3\mathbb{Z}$-conjunto: Dada $\bar{n} \in \mathbb{Z}/3\mathbb{Z}$ y $(x_1, x_2) \in \mathbb{R}^2$ definimos

$$\bar{n} * (x_1, x_2) := T^n((x_1, x_2))$$

4. Ejemplos: Sea $(G, \cdot)$ un grupo. G es naturalmente G-conjunto de los siguientes modos:

1. Operando por la izquierda: Se define $g * x := g \cdot x$, para cada $g, x \in G$, donde $*$ indica la operación de G en G como G-conjunto.
2. Operando por la derecha: Se define $g * x = x \cdot g^{-1}$, para cada $g, x \in G$.
3. Operando por conjugación: Se define $g * x = g \cdot x \cdot g^{-1}$, para cada $g, x \in G$.

5. Ejemplo: Sea $H \subset G$ un subgrupo. El cociente G/H es un G-conjunto con la acción $g \cdot \bar{g'} := \overline{gg'}$, para cada $g \in G$ y $\bar{g'} \in G/H$.

6. Definición: Dados dos G-conjuntos X, Y diremos que una aplicación $f : X \to Y$ es un *morfismo de G-conjuntos*, cuando conmute con la acción de G, es decir,

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

para todo $g \in G$ y $x \in X$. Al conjunto de los morfismos de G-conjuntos de X en Y lo denotaremos:

$$\mathrm{Hom}_G(X, Y)$$

Diremos que f es *isomorfismo* de G-conjuntos, cuando sea un morfismo biyectivo. Si $f : X \to X$ es un isomorfismo de G-conjuntos, entonces diremos que es un *automorfismo* de X como G-conjunto.

7. Observación: Se comprueba fácilmente las siguientes propiedades:

1. La *composición de morfismos* de G-conjuntos *es morfismo* de G-conjuntos, es decir: si X, Y, Z son G-conjuntos y $f : X \to Y$ y $h : Y \to Z$ son morfismos de G-conjuntos, entonces la composición $h \circ f : X \to Z$ es morfismo de G-conjuntos.

2. *La identidad es morfismo* de G-conjuntos: si X es un G-conjunto, entonces la aplicación $Id_X : X \to X$ definida por la fórmula $Id_X(x) = x$, es morfismo de G-conjuntos.

3. *La aplicación inversa de un isomorfismo* de G-conjuntos *es morfismo* de G-conjuntos: si $f : X \to Y$ es un isomorfismo de G-conjuntos, entonces $f^{-1} : Y \to X$ es morfismo de G-conjuntos.

De aquí se obtiene inmediatamente el siguiente teorema.

8. Teorema: *Si X es un G-conjunto y denotamos* $\mathrm{Aut}_G(X)$ *al conjunto de los isomorfismos de G-conjuntos $\tau : X \to X$, entonces* $\mathrm{Aut}_G(X)$ *es grupo con la composición de aplicaciones.*

1.7. Fórmula de clases

1. Definición: Sea X un G-conjunto y $x \in X$. Llamaremos órbita de x, que denotaremos $G \cdot x$, al subconjunto de X definido por

$$G \cdot x := \{g \cdot x \in X, \text{ con } g \in G\}$$

Si $x' \in G \cdot x$ entonces $G \cdot x' = G \cdot x$: Obviamente, $G \cdot x' \subseteq G \cdot G \cdot x = G \cdot x$. Por otra parte, $x' = g \cdot x$, para cierto $g \in G$, luego, $x = g^{-1} \cdot x' \in G \cdot x'$. Por tanto, $G \cdot x \subseteq G \cdot x'$ y $G \cdot x' = G \cdot x$.

Si $x' \notin G \cdot x$, entonces $(G \cdot x') \cap (G \cdot x) = \emptyset$: Si $z \in (G \cdot x') \cap (G \cdot x)$, entonces $G \cdot x' = G \cdot z = G \cdot x$. Luego, $x' \in G \cdot x$ y llegamos a contradicción.

Por tanto, las órbitas de dos puntos o son iguales o disjuntas.

2. Definición: Llamaremos subgrupo de isotropía de x, que denotaremos I_x, al subgrupo de G definido por

$$I_x := \{g \in G : g \cdot x = x\}$$

3. Proposición: *La órbita de x es un G-conjunto isomorfo a G/I_x. Explícitamente, la aplicación*

$$G/I_x \to G \cdot x, \quad \bar{g} \mapsto g \cdot x$$

es un isomorfismo de G-conjuntos.

Demostración. La aplicación $f : G/I_x \to G \cdot x$, $f(\bar{g}) := g \cdot x$ es un morfismo de G-conjuntos: $f(g' \cdot \bar{g}) = f(\overline{g' \cdot g}) = (g' \cdot g) \cdot x = g' \cdot (g \cdot x) = g' \cdot f(\bar{g})$.

La aplicación f es inyectiva: si $f(\bar{g}) = f(\overline{g'})$, entonces $g \cdot x = g' \cdot x$, luego $x = (g^{-1} \cdot g) \cdot x$ y $g^{-1} \cdot g' \in I_x$, luego $\bar{g} = \overline{g'}$.

La aplicación f es epiyectiva: dado $g \cdot x \in G \cdot x$, $f(\bar{g}) = g \cdot x$.

□

4. Ejercicio: Sea $G_m = \mathbb{R} \setminus \{0\}$, con la operación producto de $\mathbb{R}$. Consideremos la operación de G_m en $\mathbb{R}^2$ definida por:

$$\lambda * x := \lambda \cdot x, \quad \text{para todo } \lambda \in G_m \text{ y } x \in \mathbb{R}^2$$

Calcular las órbitas y subgrupos de isotropía de todos los puntos de $\mathbb{R}^2$.

5. Definición: Sea X un G-conjunto. Llamaremos conjunto cociente de X por la acción de G en X, que denotaremos X/G, al conjunto

$$X/G := \{\bar{x},\ \text{con } x \in X : \bar{x'} = \bar{x} \text{ si y sólo si } x' \in G \cdot x (\text{o equivalentemente } G \cdot x' = G \cdot x)\}$$

X/G es igual al conjunto de las órbitas de X. Es decir, si en X identificamos todos los puntos de cada órbita obtenemos el conjunto cociente.

6. Ejercicio: Calcular el conjunto cociente del G-conjunto considerados en el ejercicio 1.7.4.

7. Definición: Sea X un G-conjunto. Diremos que $x \in X$ es invariante por G si $g \cdot x = x$, para todo $g \in G$. Denotaremos X^G al subconjunto de X formado por todos los invariantes por G, es decir,

$$X^G = \{x \in X : g \cdot x = x \text{ para todo } g \in G\}$$

8. Ejercicio: Dado un grupo G, llamaremos *centro* $Z(G)$ *de* G a aquellos elementos $z \in G$ que conmutan con todos los de G, es decir, $zg = gz$ (para todo $g \in G$). Probar:

1. $Z(G)$ es un grupo conmutativo y es un subgrupo normal de G.
2. Si consideramos la operación de G en sí mismo por conjugación, entonces $Z(G) = G^G$.

9. Definición: Sea $p \in \mathbb{N}$ un número primo y G un grupo finito. Diremos que G es un p-grupo cuando $|G| = p^n$, con $n > 0$.

10. Fórmula de clases: *Sea G un grupo finito y X un G-conjunto finito. Entonces,*

$$|X| = |X^G| + \sum_{\bar{x} \in X/G, x \notin X^G} |G|/|I_x|$$

Además, si G es un p-grupo, entonces

$$\boxed{|X| \equiv |X^G| \, mod\, p}$$

Demostración. X es la unión disjunta de sus órbitas,

$$X = \coprod_{\bar{x} \in X/G} G \cdot x = X^G \coprod_{\bar{x} \in X/G, x \notin X^G} G \cdot x.$$

Como $G \cdot x \simeq G/I_x$, entonces, por el teorema de Lagrange

$$|X| = |X^G| + \sum_{\bar{x} \in X/G, x \notin X^G} |G|/|I_x|$$

Si G es un p-grupo, por el teorema de Lagrange $|G/I_x| = p^i$ (e $i = 0$ si y sólo si $x \in X^G$). Luego,

$$|X| \equiv |X^G| \, mod\, p$$

□

11. Proposición: *Si G es un p-grupo, entonces su centro es no trivial (i.e. $|Z(G)| > 1$).*

Demostración. Por la fórmula de clases $|Z(G)| = |G^G| = |G| \, mod\, p = 0 \, mod\, p$, como $1 \in Z(G)$ se concluye que $|Z(G)| \geq p > 1$. □

1.8. Teorema de Cauchy. Teoremas de Sylow

1. Teorema de Cauchy: *Si G es un grupo de orden múltiplo de un número primo p, entonces contiene un subgrupo de orden p.*

Demostración. Tenemos que probar que existe un morfismo de grupos no trivial de $\mathbb{Z}/p\mathbb{Z}$ en G.

Sean G y G' dos grupos y $X = \mathrm{Hom}_1(G',G)$ el conjunto de las aplicaciones f de G' en G, tales que $f(1) = 1$. Definamos la operación de G' en X,

$$(g_1 * f)(g_2) := f(g_2 g_1) \cdot f(g_1)^{-1}, \text{ para } f \in X \text{ y } g_1, g_2 \in G',$$

que dota a X de estructura de G'-conjunto. Se tiene que

$$\mathrm{Hom}_1(G',G)^{G'} = \mathrm{Hom}_{grp}(G',G)$$

Observemos que $|X| = |G|^{|G'|-1}$. Si p es un número primo, G es un grupo de orden múltiplo de p y $G' = \mathbb{Z}/p\mathbb{Z}$, entonces por la fórmula de clases

$$|\mathrm{Hom}_{grp}(\mathbb{Z}/p\mathbb{Z},G)| = |X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| \mod p \equiv 0 \mod p$$

Luego, $|\mathrm{Hom}_{grp}(\mathbb{Z}/p\mathbb{Z},G)| > 1$.

□

2. Proposición: *Sea $H \subseteq G$ un subgrupo finito. Consideremos G/H como H-conjunto con la operación $h \cdot \bar{g'} := \overline{hg'}$. Entonces se cumple que*

$$\begin{aligned}(G/H)^H &= \{\bar{g} \in G/H : H \cdot \bar{g} = \bar{g}\} = \{\bar{g} \in G/H : Hg \subseteq gH\} = \{\bar{g} \in G/H : H \subseteq gHg^{-1}\} \\ &= \{\bar{g} \in G/H : H = gHg^{-1}\} = \{\bar{g} \in G/H : g \in N(H)\} \\ &= N(H)/H\end{aligned}$$

3. Definición: Sea G un grupo de orden $p^n \cdot m$, p primo, $n > 0$ y $m.c.d.(p,m) = 1$. A los subgrupos de G de orden p^n se les denomina p-subgrupos de Sylow.

4. Primer teorema de Sylow: *Si G es un grupo de orden múltiplo de un número primo p, entonces contiene p-subgrupos de Sylow.*

Demostración. Escribamos $|G| = p^n \cdot m$, $n > 0$ y $m.c.d.(p,m) = 1$. Sabemos por el teorema de Cauchy que G contiene subgrupos de orden p. Basta probar que si G contiene un subgrupo H de orden p^i, con $i < n$, entonces H está incluido un subgrupo H' de G (y es normal en H') de orden p^{i+1}. Consideremos la acción de H en G/H: $h \cdot \bar{g'} = \overline{hg'}$. Entonces, $(G/H)^H = N(H)/H$ y por la fórmula de clases $|N(H)/H| = |(G/H)^H| \equiv |G/H| \, mod \, p = 0 \, mod \, p$. Luego, $|N(H)/H| = \dot{p}$ y por el teorema de Cauchy existe un subgrupo $Z \subseteq N(H)/H$ de orden p. Sea $\pi : N(H) \to N(H)/H$ el morfismo de paso al cociente. Entonces, $H' := \pi^{-1}(Z) \subseteq N(H)$ es un subgrupo que contiene a $\pi^{-1}(1) = H$ (y H es normal en él) y tal que $H'/H = Z$. Luego, H' es el subgrupo de orden p^{i+1} buscado. □

5. Segundo teorema de Sylow: *Sea G un grupo de orden múltiplo de un número primo p. Entonces, todos los p-subgrupos de Sylow de G son conjugados entre sí.*

Demostración. Sean H, H' dos subgrupos de un grupo G. Observemos que $H' \subseteq gHg^{-1}$ $\iff H'g \subseteq gH \iff H'gH \subseteq gH \iff \bar{g} \in (G/H)^{H'}$.

Sean $H, H' \subseteq G$ dos p-subgrupos de Sylow. Basta probar que $(G/H)^{H'} \neq \emptyset$. Por la fórmula de clases $|(G/H)^{H'}| \equiv |G/H| \, mod \, p \neq 0 \, mod \, p$ y hemos terminado.

□

6. Tercer teorema de Sylow: *Sea G un grupo de orden $p^n \cdot m$, con p primo, $n > 0$ y $m.c.d.(p,m) = 1$. Entonces, el número de p-subgrupos de Sylow de G es divisor de m y congruente con 1 módulo p.*

Demostración. Sea H un p-subgrupo de Sylow y X el conjunto de los conjugados de H. Por el segundo teorema de Sylow, el número de p-subgrupos de Sylow de G es igual a $|X|$. Consideremos la acción de G en X, $g * H' = gH'g^{-1}$, para $g \in G$ y $H' \in X$. El subgrupo de isotropía de $H \in X$, es igual $N(H)$ y X es igual a la órbita de H, luego $X = G/N(H)$. Por lo tanto,

$$m = |G/H| = |G|/|H| = (|G|/|N(H)|) \cdot (|N(H)|/|H|) = |X| \cdot |N(H)/H|$$

y $|X|$ divide a m.

H opera en X pues es un subgrupo de G. Por la fórmula de clases $|X| \equiv |X^H| \, mod \, p$. Ya sólo nos falta probar que $|X^H| = 1$. Si $H' \in X^H$ entonces $h \cdot H' \cdot h^{-1} = H'$, para todo $h \in H$, luego $hH' = H'h$, para todo $h \in H$ y $H \cdot H' = H' \cdot H$. Por tanto, $H \cdot H'$ es un subgrupo de G, H' es normal en $H \cdot H'$ y $(H \cdot H')/H' \simeq H/(H \cap H')$. Entonces, $|H \cdot H'| = |H'| \cdot |H/(H \cap H')|$ y $H \cdot H'$ es un p-grupo, que ha de coincidir con H. En conclusión, $H' = H$ y $|X^H| = 1$.

□

1.9. Grupos resolubles

1. Definición: Se llama *serie normal* en G a cada cadena de subgrupos $1 \subset G_1 \subset \cdots \subset G_r = G$ tal que cada G_i es normal en el siguiente, G_{i+1}. Se llaman *factores* de la serie normal a los grupos G_{i+1}/G_i.

2. Definición: Se dice que un grupo G de orden finito es resoluble si contiene una serie normal de factores grupos de orden primo.

3. Teorema: *S_2 es resoluble.*

Demostración. Inmediato, por ser $|S_2| = 2! = 2$. □

4. Teorema: *S_3 es resoluble. Explícitamente, tenemos la serie normal*

$$\{Id\} \subset A_3 \subset S_3$$

Demostración. En efecto, $|A_3| = 3$ y $|S_3/A_3| = 2$. □

Sea $K_4 = \{Id, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\} \subset S_4$ que es un subgrupo normal de S_4, que denominaremos *grupo de Klein*. Todos los elementos de $K_4 \setminus \{\text{Id}\}$ tiene orden 2 y $K_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5. Teorema: *S_4 es un grupo resoluble. Explícitamente, tenemos la serie normal*

$$\{Id\} \subset \mathbb{Z}/2\mathbb{Z} \subset K_4 \subset A_4 \subset S_4$$

6. Proposición: *Sea $f : G \to G'$ un morfismo de grupos.*

a. Si $H' \subseteq G'$ un subgrupo normal, entonces, $H := f^{-1}(H')$ es un subgrupo normal de G y el morfismo natural

$$\bar{f} : G/H \to G'/H', \bar{f}(\bar{g}) := \overline{f(g)}$$

es inyectivo. Además, si f es un epimorfismo, entonces $\bar{f}$ es un isomorfismo.

b. Si f es un epimorfismo y $H \subseteq G$ es un subgrupo normal, entonces $f(H)$ es un subgrupo normal de G' y el morfismo natural

$$\bar{f} : G/H \to G'/f(H)$$

es un epimorfismo de grupos.

Demostración. a. Dado $g \in G$ y $h \in f^{-1}(H')$, entonces $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$, luego $ghg^{-1} \in H'$ y H es un subgrupo normal de G.

Si $\bar{f}(\bar{g}) = \bar{1}$, entonces $\overline{f(g)} = \bar{1}$ y $f(g) \in H'$, es decir, $g \in f^{-1}(H') = H$, que equivale a decir que $\bar{g} = \bar{1} \in G/H$. En conclusión, $\bar{f}$ es inyectivo.

Por último, supongamos que f es epiyectivo. Dado $\overline{g'} \in G'/H'$, sea $g \in G$ tal que $f(g) = g'$, entonces $\bar{f}(\bar{g}) = \overline{g'}$, $\bar{f}$ es epiyectivo, luego isomorfismo.

b. Dado $g' = f(g) \in G'$ y $h' = f(h) \in f(H)$, entonces $g' \cdot h' \cdot g'^{-1} = f(ghg^{-1}) \in f(H)$. Luego $f(H)$ es un subgrupo normal de G'. Dado $\overline{g'} \in G'/f(H')$, se tiene que $g' = f(g)$ para cierto $g \in G$, luego $\bar{f}(\bar{g}) = \overline{f(g)} = \overline{g'}$. Luego, $\bar{f}$ es un epimorfismo de grupos.

□

7. Proposición: *Sea G un grupo y $H \subseteq G$ un subgrupo normal. Entonces, G es resoluble si y sólo si H y G/H son resolubles.*

Demostración. Sea G resoluble y $1 \subset G_1 \subset \cdots \subset G_r = G$ una serie normal de factores grupos de orden primo.

La cadena $1 \subseteq G_1 \cap H \subseteq \cdots \subseteq G_r \cap H = H$ es una serie normal (considérese en 1.9.6 a. el morfismo $G_i \cap H \hookrightarrow G_i$ y el subgrupo normal $G_{i-1} \subset G_i$). Además, $(G_i \cap H)/(G_{i-1} \cap H)$ es de orden primo porque es subgrupo de G_i/G_{i-1}. Luego H es resoluble.

Sea $\pi : G \to G/H$ el morfismo de paso al cociente. La cadena $\bar{1} \subseteq \pi(G_1) \subseteq \cdots \subseteq \pi(G_r) = G/H$ es una serie normal (considérese en 1.9.6 b. el epimorfismo $\pi : G_i \to \pi(G_i)$ y el subgrupo normal $G_{i-1} \subset G_i$). Además, $\pi(G_i)/\pi(G_{i-1}$ es de orden primo porque es un cociente de G_i/G_{i-1}. Luego G/H es resoluble.

Supongamos ahora que H y G/H son resolubles. Sean $1 \subseteq H_1 \subseteq H_s = H$ y $\bar{1} \subset G'_1 \subset \cdots \subset G'_t = G/H$ series normales de factores grupos de orden primo. Sean $G_i := \pi^{-1}(G'_i)$. Entonces, G_{i-1} es normal en G_i y $G_i/G_{i-1} = G'_i/G'_{i-1}$ (considérese en 1.9.6 a. el epimorfismo $\pi : G_i \to G'_i$ y el subgrupo $G'_{i-1} \hookrightarrow G'_i$.

Por tanto, la cadena $1 \subseteq H_1 \subseteq H_s = H = \pi^{-1}(\bar{1}) \subset G_1 \subset \cdots \subset G_t = G$ es una serie normal de factores grupos de orden primo. En conclusión, G es resoluble.

□

8. Proposición : *Si $G_1,\dots,G_n$ son grupos resolubles, entonces $G = G_1 \times \cdots \times G_n$ es resoluble.*

Demostración. Procedamos por inducción sobre n. Si $n = 1$ la proposición es obvia. Supongamos $n > 1$. $H = G_1 \times \cdots \times G_{n-1}$ es resoluble por hipótesis de inducción. Tenemos que probar que $H \times G_n = G_1 \times \cdots \times G_n$ es resoluble. Vía la inclusión $H \hookrightarrow H \times G_n$, $h \mapsto (h,1)$, tenemos que H es un subrupo normal de $H \times G_n$. Además, $(H \times G_n)/H \simeq G_n$, $\overline{(h,g)} \mapsto g$. Por la proposición anterior, como H y G_n son resolubles, entonces $H \times G_n$ es resoluble. □

9. Proposición: *Los grupos finitos abelianos son resolubles.*

Demostración. Si G es un grupo finito abeliano entonces $G \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$. Basta que probar que los grupos cíclicos $\mathbb{Z}/p^n\mathbb{Z}$, con p primo, son resolubles.

Tenemos la cadena

$$\bar{0} \subset \langle \overline{p^{n-1}} \rangle \subset \langle \overline{p^{n-2}} \rangle \subset \cdots \langle \overline{p} \rangle \subseteq \mathbb{Z}/p^n\mathbb{Z}$$

es una serie normal de factores grupos de orden p. Luego $\mathbb{Z}/p^n\mathbb{Z}$ es resoluble.

□

10. Teorema: *Sea $p > 0$ un número primo y G un p-grupo. Entonces, G es un grupo resoluble.*

Demostración. Procedamos por inducción sobre el orden del grupo. Por 1.7.11, $Z(G)$ no es trivial y es resoluble, porque es conmutativo. $G/Z(G)$ es resoluble por hipótesis de inducción. Por tanto, G es resoluble. □

1.10. Irresolubilidad de S_n, para $n > 4$.

1. Lema: *El grupo alternado, A_n, está generado por los tres ciclos ($n > 2$).*

Demostración. Si $\sigma = (i,j,k) \in S_n$ es un tres ciclo, entonces $\operatorname{sign}(\sigma) = (-1)^2 = 1$ y $\sigma \in A_n$. Por la proposición 1.4.8, toda permutación par es producto de un número par de transposiciones. Tenemos que probar que todo producto de dos transposiciones es producto de tres ciclos. Basta observar que $(1,2)(2,3) = (1,2,3)$ (cuando las transposiciones no sean disjuntas) y $(1,2)(3,4) = (1,2,3)(2,3,4)$ (cuando las transposiciones sean disjuntas). □

Consideremos la inclusión obvia $S_3 \hookrightarrow S_4$. Es claro que $S_3 \cap K_4 = \{\mathrm{Id}\}$, luego el morfismo $S_3 \to S_4/K_4$, $\sigma \mapsto \bar{\sigma}$ es inyectivo y por órdenes ha de ser un isomorfismo.

2. Teorema: *Si $n \neq 4$, el único subgrupo normal propio de S_n es A_n. Los únicos subgrupos normales propios de S_4 son el alternado A_4 y el grupo de Klein K_4.*

Demostración. Por lo visto anteriormente, el teorema es claro para $n = 2,3$, luego podemos suponer $n \geq 4$.

Por ser $H \subset S_n$ normal y el teorema 1.4.6, si $\sigma \in H$, entonces todas las permutaciones con la misma forma que σ pertenecen también a H.

Sea $Id \neq \sigma \in H$ y sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_h$ su descomposición en ciclos disjuntos de órdenes respectivos $n_1 \geq \cdots \geq n_h$.

• Si $n_1 \geq 3$, digamos $\sigma_1 = (a_1, a_2, a_3, \ldots, a_{n_1})$, sea $\overline{\sigma}_1 = (a_{n_1}, \ldots, a_3, a_1, a_2)$. Se verifica que $\overline{\sigma} = \overline{\sigma}_1 \circ \sigma_2^{-1} \circ \cdots \circ \sigma_h^{-1} \in H$, pues tiene la misma forma que σ. Luego, $\overline{\sigma} \circ \sigma = (a_1, a_{n_1}, a_2) \in H$ y por el lema 1.10.1, se concluye que H contiene a A_n. Por tanto, $H = A_n$ ó S_n.

• Si $n_1 = 2$ y $h = 1$, entonces σ es una transposición y H las contiene a todas, luego $H = S_n$ (proposición 1.4.8).

• Por último, si $n_1 = 2$ y $h \geq 2$, entonces $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ \sigma_3 \circ \cdots \circ \sigma_h$. Eligiendo la permutación con la misma forma $\overline{\sigma} = (a_1, a_3) \circ (a_2, a_4) \circ \sigma_3^{-1} \circ \cdots \circ \sigma_h^{-1}$, se obtiene que

$$\tau := (a_1, a_4) \circ (a_2, a_3) = \overline{\sigma} \circ \sigma \in H$$

y, por tanto H contiene a todos los pares de trasposiciones disjuntas. Si $n > 4$, sea $\tau' = (a_2, a_3) \circ (a_1, a_5)$, entonces $(a_1, a_5, a_4) = \tau \circ \tau' \in H$. Luego, H contiene a todos los tres ciclos y $A_n \subseteq H$. Entonces, $H = S_n$ ó $H = A_n$. Si $n = 4$, entonces H contiene al grupo de Klein y $H/K_4 \subset S_4/K_4 \approx S_3$ es un subgrupo normal, es decir, es trivial o A_3 y, por tanto, $H = K_4$ o A_4. □

3. Definición: Se dice que un grupo es simple si no contiene subgrupos normales propios.

4. Teorema: *A_n es simple para $n \neq 4$.*

Demostración. Sea $H \subset A_n$ normal no trivial. Se verifica que $N_{S_n}(H) = A_n$ (por el teorema anterior). Es decir, que H tiene exactamente dos conjugados (por S_n) uno es H y el otro es $H' = \sigma \circ H \circ \sigma^{-1}$ para cualquier permutación impar σ. $H \cap H' = \{id\}$ y $H \cdot H' = A_n$, pues ambos son subgrupos normales en S_n. Por tanto, $A_n \approx H \times H'$. Como $|A_n| = |H| \cdot |H'| = |H|^2$, $n \neq 3$. De aquí que H tiene orden par (por tenerlo A_n) y, por tanto, contiene un elemento μ de orden 2 (por el teorema de Cauchy). De aquí que μ descompone en producto de trasposiciones disjuntas $\mu = \sigma_1 \circ \cdots \circ \sigma_h$. Por tanto, $\mu = \sigma_1 \circ \mu \circ \sigma_1^{-1} \in H'$, es decir, $\mu \in H \cap H' = \{Id\}$ y se obtiene una contradicción.

□

5. Teorema: *S_n no es resoluble, para $n > 4$.*

Demostración. La única serie normal (no trivial) de S_n, para $n > 4$, es

$$\{Id\} \subset A_n \subset S_n$$

por los dos teoremas anteriores. Luego, S_n no es resoluble. □

1.11. Biografía de Cauchy

CAUCHY BIOGRAPHY

Paris was a difficult place to live in when Augustin-Louis Cauchy was a young child due to the political events surrounding the French Revolution. When he was four years old his father, fearing for his life in Paris, moved his family to Arcueil. There things were hard and he wrote in a letter:

We never have more than a half pound of bread - and sometimes not even that. This we supplement with the little supply of hard crackers and rice that we are allotted.

They soon returned to Paris and Cauchy's father was active in the education of young Augustin-Louis. Laplace and Lagrange were visitors at the Cauchy family home and Lagrange in particular seems to have taken an interest in young Cauchy's mathematical education. Lagrange advised Cauchy's father that his son should obtain a good grounding in languages before starting a serious study of mathematics. In 1802 Augustin-Louis entered the École Centrale du Panthéon where he spent two years studying classical languages.

From 1804 Cauchy attended classes in mathematics and he took the entrance examination for the École Polytechnique in 1805. He was examined by Biot and placed second. At the École Polytechnique he attended courses by Lacroix, de Prony and Hachette while his analysis tutor was Ampère. In 1807 he graduated from the École Polytechnique and entered the engineering school École des Ponts et Chaussées. He was an outstanding student and for his practical work he was assigned to the Ourcq Canal project where he worked under Pierre Girard.

In 1810 Cauchy took up his first job in Cherbourg to work on port facilities for Napoleon's English invasion fleet. He took a copy of Laplace's Mécanique Céleste and one of Lagrange's Théorie des Fonctions with him. It was a busy time for Cauchy, writing home about his daily duties he said:

I get up at four o'clock each morning and I am busy from then on. ... I do not get tired of working, on the contrary, it invigorates me and I am in perfect health...

Cauchy was a devout Catholic and his attitude to his religion was already causing problems for him. In a letter written to his mother in 1810 he says:

So they are claiming that my devotion is causing me to become proud, arrogant and self-infatuated. ... I am now left alone about religion and nobody mentions it to me anymore...

In addition to his heavy workload Cauchy undertook mathematical researches and he proved in 1811 that the angles of a convex polyhedron are determined by its faces. He submitted his first paper on this topic then, encouraged by Legendre and Malus, he submitted a further paper on polygons and polyhedra in 1812. Cauchy felt that he had to return to Paris if he was to make an impression with mathematical research. In September of 1812 he returned to Paris after becoming ill. It appears that the illness

was not a physical one and was probably of a psychological nature resulting in severe depression.

Back in Paris Cauchy investigated symmetric functions and submitted a memoir on this topic in November 1812. This was published in the Journal of the École Polytechnique in 1815. However he was supposed to return to Cherbourg in February 1813 when he had recovered his health and this did not fit with his mathematical ambitions. His request to de Prony for an associate professorship at the École des Ponts et Chaussées was turned down but he was allowed to continue as an engineer on the Ourcq Canal project rather than return to Cherbourg. Pierre Girard was clearly pleased with his previous work on this project and supported the move.

An academic career was what Cauchy wanted and he applied for a post in the Bureau des Longitudes. He failed to obtain this post, Legendre being appointed. He also failed to be appointed to the geometry section of the Institute, the position going to Poinsot. Cauchy obtained further sick leave, having unpaid leave for nine months, then political events prevented work on the Ourcq Canal so Cauchy was able to devote himself entirely to research for a couple of years.

Other posts became vacant but one in 1814 went to Ampère and a mechanics vacancy at the Institute, which had occurred when Napoleon Bonaparte resigned, went to Molard. In this last election Cauchy did not receive a single one of the 53 votes cast. His mathematical output remained strong and in 1814 he published the memoir on definite integrals that later became the basis of his theory of complex functions.

In 1815 Cauchy lost out to Binet for a mechanics chair at the École Polytechnique, but then was appointed assistant professor of analysis there. He was responsible for the second year course. In 1816 he won the Grand Prix of the French Academy of Sciences for a work on waves. He achieved real fame however when he submitted a paper to the Institute solving one of Fermat's claims on polygonal numbers made to Mersenne. Politics now helped Cauchy into the Academy of Sciences when Carnot and Monge fell from political favour and were dismissed and Cauchy filled one of the two places.

In 1817 when Biot left Paris for an expedition to the Shetland Islands in Scotland Cauchy filled his post at the Collège de France. There he lectured on methods of integration which he had discovered, but not published, earlier. Cauchy was the first to make a rigorous study of the conditions for convergence of infinite series in addition to his rigorous definition of an integral. His text Cours d'analyse in 1821 was designed for students at École Polytechnique and was concerned with developing the basic theorems of the calculus as rigorously as possible. He began a study of the calculus of residues in 1826 in Sur un nouveau genre de calcul analogue au calcul infinitésimal while in 1829 in Leçons sur le Calcul Différentiel he defined for the first time a complex function of a complex variable.

Cauchy did not have particularly good relations with other scientists. His staunchly Catholic views had him involved on the side of the Jesuits against the Académie des Sciences. He would bring religion into his scientific work as for example he did on giving a report on the theory of light in 1824 when he attacked the author for his view that Newton had not believed that people had souls. He was described by a journalist who said:

... it is certain a curious thing to see an academician who seemed to fulfil the respectable functions of a missionary preaching to the heathens.

An example of how Cauchy treated colleagues is given by Poncelet whose work on projective geometry had, in 1820, been criticised by Cauchy:

... I managed to approach my too rigid judge at his residence ... just as he was leaving ... During this very short and very rapid walk, I quickly perceived that I had in no way earned his regards or his respect as a scientist ... without allowing me to say anything else, he abruptly walked off, referring me to the forthcoming publication of his Leçons à 'École Polytechnique where, according to him, 'the question would be very properly explored'.

Again his treatment of Galois and Abel during this period was unfortunate. Abel, who visited the Institute in 1826, wrote of him:

Cauchy is mad and there is nothing that can be done about him, although, right now, he is the only one who knows how mathematics should be done.

Belhoste says:

When Abel's untimely death occurred on April 6, 1829, Cauchy still had not given a report on the 1826 paper, in spite of several protests from Legendre. The report he finally did give, on June 29, 1829, was hasty, nasty, and superficial, unworthy of both his own brilliance and the real importance of the study he had judged.

By 1830 the political events in Paris and the years of hard work had taken their toll and Cauchy decided to take a break. He left Paris in September 1830, after the revolution of July, and spent a short time in Switzerland. There he was an enthusiastic helper in setting up the Académie Helvétique but this project collapsed as it became caught up in political events.

Political events in France meant that Cauchy was now required to swear an oath of allegiance to the new regime and when he failed to return to Paris to do so he lost all his positions there. In 1831 Cauchy went to Turin and after some time there he accepted an offer from the King of Piedmont of a chair of theoretical physics. He taught in Turin from 1832. Menabrea attended these courses in Turin and wrote that the courses:

were very confused, skipping suddenly from one idea to another, from one formula to the next, with no attempt to give a connection between them. His presentations were obscure clouds, illuminated from time to time by flashes of pure genius. ... of the thirty who enrolled with me, I was the only one to see it through.

In 1833 Cauchy went from Turin to Prague in order to follow Charles X and to tutor his grandson. However he was not very successful in teaching the prince as this description shows:

... exams .. were given each Saturday. ... When questioned by Cauchy on a problem in descriptive geometry, the prince was confused and hesitant. ... There was also material on physics and chemistry. As with mathematics, the prince showed very little

interest in these subjects. Cauchy became annoyed and screamed and yelled. The queen sometimes said to him, soothingly, smilingly, 'too loud, not so loud'.

While in Prague Cauchy had one meeting with Bolzano, at Bolzano's request, in 1834. There are discussions on how much Cauchy's definition of continuity is due to Bolzano, Freudenthal's view that Cauchy's definition was formed before Bolzano's seems the more convincing.

Cauchy returned to Paris in 1838 and regained his position at the Academy but not his teaching positions because he had refused to take an oath of allegiance. De Prony died in 1839 and his position at the Bureau des Longitudes became vacant. Cauchy was strongly supported by Biot and Arago but Poisson strongly opposed him. Cauchy was elected but, after refusing to swear the oath, was not appointed and could not attend meetings or receive a salary.

In 1843 Lacroix died and Cauchy became a candidate for his mathematics chair at the Collège de France. Liouville and Libri were also candidates. Cauchy should have easily been appointed on his mathematical abilities but his political and religious activities, such as support for the Jesuits, became crucial factors. Libri was chosen, clearly by far the weakest of the three mathematically, and Liouville wrote the following day that he was:

deeply humiliated as a man and as a mathematician by what took place yesterday at the Collège de France.

During this period Cauchy's mathematical output was less than in the period before his self-imposed exile. He did important work on differential equations and applications to mathematical physics. He also wrote on mathematical astronomy, mainly because of his candidacy for positions at the Bureau des Longitudes. The 4-volume text Exercices d'analyse et de physique mathématique published between 1840 and 1847 proved extremely important.

When Louis Philippe was overthrown in 1848 Cauchy regained his university positions. However he did not change his views and continued to give his colleagues problems. Libri, who had been appointed in the political way described above, resigned his chair and fled from France. Partly this must have been because he was about to be prosecuted for stealing valuable books. Liouville and Cauchy were candidates for the chair again in 1850 as they had been in 1843. After a close run election Liouville was appointed. Subsequent attempts to reverse this decision led to very bad relations between Liouville and Cauchy.

Another, rather silly, dispute this time with Duhamel clouded the last few years of Cauchy's life. This dispute was over a priority claim regarding a result on inelastic shocks. Duhamel argued with Cauchy's claim to have been the first to give the results in 1832. Poncelet referred to his own work of 1826 on the subject and Cauchy was shown to be wrong. However Cauchy was never one to admit he was wrong. Valson writes:

...the dispute gave the final days of his life a basic sadness and bitterness that only his friends were aware of...

In a letter by Cauchy's daughter describing his death is given:

Having remained fully alert, in complete control of his mental powers, until 3.30 a.m.. my father suddenly uttered the blessed names of Jesus, Mary and Joseph. For the first time, he seemed to be aware of the gravity of his condition. At about four o'clock, his soul went to God. He met his death with such calm that made us ashamed of our unhappiness.

Numerous terms in mathematics bear Cauchy's name: the Cauchy integral theorem, in the theory of complex functions, the Cauchy-Kovalevskaya existence theorem for the solution of partial differential equations, the Cauchy-Riemann equations and Cauchy sequences. He produced 789 mathematics papers, an incredible achievement. This achievement is summed up (in "Augustin-Louis Cauchy. A Biography", by B. Belhoste) as follows:

... such an enormous scientific creativity is nothing less than staggering, for it presents research on all the then-known areas of mathematics ... in spite of its vastness and rich multifaceted character, Cauchy's scientific works possess a definite unifying theme, a secret wholeness. ... Cauchy's creative genius found broad expression not only in his work on the foundations of real and complex analysis, areas to which his name is inextricably linked, but also in many other fields. Specifically, in this connection, we should mention his major contributions to the development of mathematical physics and to theoretical mechanics... we mention ... his two theories of elasticity and his investigations on the theory of light, research which required that he develop whole new mathematical techniques such as Fourier transforms, diagonalization of matrices, and the calculus of residues.

His collected works, Oeuvres complètes d'Augustin Cauchy (1882-1970), were published in 27 volumes.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

1.12. Cuestionario

1. Sea X un conjunto de orden mayor que 1 ¿Es el conjunto de todas las aplicaciones de X en X con la composición de aplicaciones un grupo?
2. Sea G un grupo. Si $gg'g^{-1} = g'$, para todo $g, g' \in G$, ¿es G un grupo abeliano?¿Es cierto el recíproco?
3. Sea G un grupo y sea $g \in G$. La aplicación $\tau_g \colon G \to G$, $\tau_g(g') := gg'g^{-1}$, es un morfismo de grupos. Explicitar la aplicación inversa.
4. ¿Todo subgrupo de un grupo abeliano es abeliano?
5. ¿Todos los subgrupos de un grupo conmutativo son normales?
6. Sea $f : G \to G'$ un morfismo de grupos. ¿Es $\ker f$ un subgrupo normal de G?
7. Sea $f : G \to G'$ un morfismo de grupos y $H' \subseteq G'$ un subgrupo normal. ¿Es $f^{-1}(H')$, con seguridad, un subgrupo normal de G?

8. ¿Todo cociente de un grupo abeliano por un subgrupo es un grupo abeliano?
9. Sea G un grupo y $g_1,\dots,g_n \in G$ ¿Es $\langle g_1,\dots,g_n\rangle$ el conjunto de elementos de G que son producto (con repeticiones) de elementos de $\{g_1,\dots,g_n,g_1^{-1},\dots,g_n^{-1}\}$?
10. ¿Todo cociente de un grupo cíclico por un subgrupo es un grupo cíclico?
11. ¿Todo subgrupo de un grupo cíclico es cíclico?
12. Si $g \in G$ es un elemento de orden 27, calcular un $n > 0$, tal que $g^n = g^{-1}$.
13. Sea G un grupo y $g \in G$ ¿Tiene g el mismo orden que g^{-1}?
14. Sea G un grupo y $g \in G$ un elemento tal que $g^{12} = 1$ ¿Puede ser el orden de g 8?
15. Sea $f : G \to G'$ un morfismo de grupos y $g \in G$ un elemento de orden 6 ¿Puede ser el orden de $f(g)$, 5?
16. Sea G un grupo de orden mayor que 1. ¿Es seguro que G contiene algún subgrupo conmutativo de orden mayor que 1?
17. Sea G un grupo de orden un número primo. ¿Es, entonces, G un grupo cíclico?
18. ¿Es S_2 un grupo conmutativo? y ¿S_3?
19. ¿Es S_n, para $n > 2$, conmutativo?
20. Escribir la permutación $\binom{12345}{53421}$ como producto de ciclos disjuntos.
21. ¿Cuál es el orden de la permutación $\binom{123456789}{293487651}$?
22. Sea $\sigma = \binom{123456789}{293487651}$. Calcular σ^{33}.
23. Escribir la permutación $\binom{12345}{53421}$ como producto de transposiciones.
24. ¿Es todo subgrupo de S_3 normal?
25. ¿Es A_3 isomorfo a $\mathbb{Z}/3\mathbb{Z}$?
26. ¿Cuántos epimorfismos de grupos $S_n \to \mathbb{Z}/2\mathbb{Z}$ existen?
27. ¿Qué orden tiene S_n? y ¿A_n? y ¿D_n?
28. ¿Es S_3 isomorfo a D_3?
29. ¿Cuántos grupos abelianos desisomorfos de orden 18 existen?
30. ¿Existen sistemas generadores del grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ con dos elementos?
31. ¿Existe algún sistema generador de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ con un único elemento?

32. Consideremos el morfismo natural de grupos $Gl(\mathbb{R}^2) \hookrightarrow \mathrm{Aut}_{gr}(\mathbb{R}^2)$, $T \mapsto T$. Consideremos el producto semidirecto $\mathbb{R}^2 \rtimes Gl(\mathbb{R}^2)$. Calcular

$$((1,2),\begin{pmatrix}1 & 1\\ 2 & -2\end{pmatrix})^2$$

33. Consideremos el morfismo de grupos $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{Aut}_{gr}(\mathbb{Z}/4\mathbb{Z})$, $\bar{0} \mapsto \mathrm{Id}$, $\bar{1} \mapsto -\mathrm{Id}$. Consideremos el producto semidirecto $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Calcular

$$(\bar{1},\bar{1})^2$$

34. Sea X un G-conjunto ¿Existe algún elemento de G que transforme $g \cdot x$ en x?

35. Sea el grupo $G_m = \mathbb{R}\backslash\{0\}$, con la operación el producto de $\mathbb{R}$. Consideremos la operación de G_m en $\mathbb{R}$ siguiente: $\lambda * e := \lambda \cdot e$, para todo $\lambda \in G_m$ y $e \in \mathbb{R}$ ¿Cuántas órbitas hay en $\mathbb{R}$?

36. Sea G un grupo y consideremos G como G-conjunto operando G en G por la izquierda ¿Cuántas órbitas hay en G?

37. Consideremos S_3 como S_3-conjunto operando S_3 en S_3 por conjugación. ¿Cuántas órbitas hay en S_3?

38. Consideremos S_4 como S_4-conjunto operando S_4 en S_4 por conjugación. ¿Cuántas órbitas hay en S_4?

39. Consideremos S_3 como S_3-conjunto operando S_3 en S_3 por conjugación. Calcular el grupo de isotropía de la transposición $(1,2)$.

40. ¿Todas las órbitas de un G-conjunto tienen el mismo orden?

41. Sea $H \subseteq G$ un subgrupo de orden finito. Consideremos G como H-conjunto como sigue: $h * g = h \cdot g$ ¿Tienen todas las órbitas de H-conjunto G el mismo orden?

42. Sea I_x el grupo de isotropía de $x \in X$ ¿Es gI_xg^{-1} el grupo de isotropía de gx?

43. Sea el grupo $G_m = \mathbb{R}\backslash\{0\}$, con la operación el producto ordinario de números reales. Consideremos la operación de G_m en $\mathbb{R}^2$ siguiente: $\lambda * e := \lambda \cdot e$, para todo $\lambda \in G_m$ y todo $e \in \mathbb{R}^2$. Calcular $(\mathbb{R}^2)^{G_m}$.

44. Sea X un conjunto, con la estructura de G-conjunto trivial, es decir, $g \cdot x = x$, para todo $g \in G$ y $x \in X$. Calcular X^G.

45. Sea X un G-conjunto. ¿Hay tantas órbitas en X de orden 1 como elementos de X invariantes por G?

46. Sea $G \neq \{1\}$ un grupo. Consideremos la operación de G en G por multiplicaciones por la izquierda. Calcular G^G.

47. Consideremos la acción de G en si mismo por conjugación ¿Se cumple que $G^G = Z(G)$?

48. Sea $\mathbb{Z}/3\mathbb{Z}$ un $\mathbb{Z}/2\mathbb{Z}$-conjunto. ¿Podemos afirmar que $(\mathbb{Z}/3\mathbb{Z})^{\mathbb{Z}/2\mathbb{Z}} \neq \emptyset$?

49. Sea p un número primo y X un conjunto de orden $q < p$ ¿Cuántas estructuras de $\mathbb{Z}/p\mathbb{Z}$-conjuntos no isomorfas distintas pueden definirse en X?

50. Sea G un grupo de orden p^n, $p > 0$ primo. Considerar la acción de G en si mismo por conjugación ¿Se puede deducir por la fórmula de clases que $Z(G) \neq \{1\}$?

51. ¿Cuántos 5-subgrupos de Sylow contiene $\mathbb{Z}/25\mathbb{Z}$?

52. Sea G un grupo de orden múltiplo de un número primo p ¿Son todos los p-subgrupos de Sylow de G isomorfos?

53. Sean $p \neq q$ dos números primos. Sea H_p un p-subgrupo de Sylow de G y H_q un q-subgrupo de Sylow de G. Determinar $H_p \cap H_q$.

54. Sea G un grupo de orden múltiplo de un número primo p y H_p un p-subgrupo de Sylow ¿G contiene un único p-subgrupo de Sylow si y sólo si H_p es normal en G?

55. Sea G un grupo de orden 35. ¿Cuántos 5-subgrupos de Sylow existen? ¿Cuántos 7-subgrupos de Sylow existen? ¿Es $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$? ¿Es G cíclico?

56. Sea G un grupo de orden 6 ¿Cuántos 3-subgrupos de Sylow contiene G?

57. ¿Cuántos 2-subgrupos de Sylow contiene S_3? y ¿$\mathbb{Z}/6\mathbb{Z}$?

58. ¿Es $D_4 \subset S_4$ un 2-subgrupo de Sylow? ¿Cuántos 2-subgrupos de Sylow contiene S_4?

59. ¿Es el grupo $S_3 \times \mathbb{Z}/5\mathbb{Z}$ resoluble?

60. ¿Es D_n resoluble para todo $n > 2$?

61. Sea G un grupo no resoluble ¿Contiene G algún subgrupo propio resoluble?

62. Sea G un grupo finito. Sea $\{1\} \subset G_1 \subset \cdots \subset G_n = G$ una serie normal de subgrupos de G de factores grupos abelianos ¿Es G_2 resoluble? ¿Es G resoluble?

63. Sea $f : S_5 \to \mathbb{Z}/3\mathbb{Z}$ un morfismo de grupos ¿Se cumple que $f(\sigma) = \bar{0}$, para todo $\sigma \in S_5$?

64. Sea H el subconjunto de S_n, (con $n \geq 4$) de las permutaciones que son iguales a un producto de 4-ciclos. ¿Es H un subgrupo normal de S_n? ¿Es $H = S_n$?

65. Sea H el subconjunto de S_n, (con $n > 4$) de las permutaciones que son iguales a un producto de 5-ciclos. ¿Es H un subgrupo normal de S_n? ¿Es $H = A_n$?

1.13. Problemas

1. Las siguientes condiciones sobre un grupo G son equivalentes:

   a) G es un grupo abeliano.

   b) La aplicación $\phi\colon G \to G$, $\phi(g) = g^{-1}$, es morfismo de grupos.

   c) La aplicación $\phi\colon G \to G$, $\phi(g) = g^2$, es morfismo de grupos.

   d) La aplicación $\phi\colon G \times G \to G$, $\phi(a,b) = ab$, es morfismo de grupos.

2. Sea G un grupo. Si $a, g \in G$, se dice que aga^{-1} es el *conjugado* de g por a. La conjugación $\tau_a\colon G \to G$, $\tau_a(g) = aga^{-1}$ es un automorfismo de grupos (tales automorfismos de G reciben el nombre de *automorfismos internos*), y la aplicación $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, es un morfismo de grupos.

3. Si H es un subgrupo de un grupo G, entonces

   $$N(H) := \{g \in G\colon gHg^{-1} = H\}$$

   es un subgrupo de G, llamado *normalizador* de H, y es el mayor subgrupo de G que contiene a H como subgrupo normal. Además, si $a \in G$, entonces $N(aHa^{-1}) = aN(H)a^{-1}$.

4. Si G es un grupo, entonces su *centro*

   $$Z(G) := \{a \in G\colon ag = ga,\ \forall g \in G\}$$

   es un subgrupo normal de G.

5. El centro del grupo simétrico S_n es trivial cuando $n \geq 3$.

6. Sean H y K dos subgrupos de un grupo G. Si $K \subseteq N(H)$, entonces $HK = KH$ es un subgrupo de G. Si además G es finito, entonces $|HK| = |H| \cdot |K| / |H \cap K|$.

7. Si H y K son dos subgrupos normales y $H \cap K = 1$, entonces los elementos de H conmutan con los de K.

8. Si G es un grupo de orden un número primo, entonces G es cíclico.

9. Si los únicos subgrupos de un grupo G son los triviales 1 y G, entonces $G \simeq \mathbb{Z}/p\mathbb{Z}$ para algún número primo p.

10. Todo grupo finito de orden par contiene algún elemento $g \neq 1$ tal que $g^2 = 1$.

11. Si un grupo G sólo tiene un número finito de subgrupos, entonces G es finito.

12. Si H es un subgrupo propio de un grupo finito G, entonces existe algún elemento de G que no está contenido en ninguno de los subgrupos conjugados de H.

13. Sea X un G-conjunto, $x \in X$ y $x' = g \cdot x$. Probar que $I_{x'} = g \cdot I_x \cdot g^{-1}$.

14. Los morfismos de G-conjuntos transforman órbitas en órbitas, y todo endomorfismo de G-conjuntos de una órbita finita es un automorfismo.

15. Sean H y K dos subgrupos de un grupo G. Los G-conjuntos G/H y G/K son isomorfos precisamente cuando H y K son subgrupos conjugados.

16. Sea X un G-conjunto, $H \subseteq G$ un subgrupo y consideremos G/H como G-conjunto de modo natural: $g \cdot \bar{g'} := \overline{gg'}$. Probar que la aplicación,

$$\mathrm{Hom}_G(G/H, X) \to X^H, f \mapsto f(\bar{1})$$

es biyectiva.

17. Si H es un subgrupo de un grupo G, el grupo de automorfismos del G-conjunto G/H es isomorfo al grupo $N(H)/H$.

18. Si H es un subgrupo de un grupo finito G, el número de subgrupos conjugados de H divide al índice, $|G/H|$, de H en G.

19. Todo subgrupo de índice 2 es normal. (*Indicación:* Si $g \notin H$, entonces gH es el complementario de H.)

20. Si el índice de un subgrupo H de un grupo finito G es el menor número primo que divide al orden de G, entonces H es un subgrupo normal de G. (*Indicación:* Considérese la acción de H, o la de G, en G/H.)

21. El grupo A_4 no tiene ningún subgrupo de orden 6 (aunque su orden es múltiplo de 6).

22. El núcleo del morfismo de grupos $G \to \mathrm{Aut}(G)$ que define la conjugación es el centro $Z(G)$ del grupo G. Si $G/Z(G)$ es un grupo cíclico, entonces G es abeliano.

23. Si p es un número primo, todo grupo de orden p^2 es abeliano. Clasificar los grupos de orden p^2.

24. Sea G un grupo finito. Si el conjunto de subgrupos de G está totalmente ordenado (i.e., no tiene pares incomparables), entonces G es un grupo cíclico de orden potencia de un primo.

25. Sea p un número primo. Un grupo finito G es un p-grupo precisamente cuando para todo G conjunto finito X se cumple que $|X| \equiv |X^G|$ (módulo p).

26. Todo subgrupo normal de orden p de un p-grupo G está contenido en el centro de G.

27. Todo subgrupo normal H de un p-grupo G tiene intersección no trivial con el centro de G; es decir, $Z(G) \cap H \neq 1$.

28. Si G es un p-grupo no abeliano de orden p^3, entonces todo subgrupo normal de G contiene al centro.

29. Si H es un subgrupo propio de un p-grupo, entonces $H \neq N(H)$.

30. Determinar los subgrupos de Sylow de los grupos simétricos S_3, S_4 y S_5.

31. Determinar todos los subgrupos normales de S_3, S_4 y A_4.

32. Si una potencia p^r de un número primo divide al orden de un grupo finito G, entonces G tiene algún subgrupo de orden p^r.

33. Todo grupo de orden 100 tiene algún subgrupo normal de orden 25.

34. Sea H un subgrupo de orden p^k de un grupo G de orden $p^n m$. Si $k < n$, entonces G tiene un subgrupo H' de orden p^{k+1} tal que $H \lhd H'$.

35. Si H es un p-subgrupo normal de un grupo finito G, entonces H está contenido en todos los p-subgrupos de Sylow de G.

36. El grupo diédrico D_n (el grupo de los movimientos que dejan invariante un polígono regular de n lados) tiene orden $2n$ y está generado por dos elementos g y s tales que $g^n = s^2 = 1$, $sgs = g^{-1}$. Calcular el centro y el grupo de automorfismos del grupo D_n.

37. Si p es un número primo, todo grupo no abeliano de orden $2p$ es isomorfo al grupo D_p.

38. Si p y q son números primos distintos, entonces

    a) Ningún grupo G de orden pq es simple, y si además $p < q$ y q no es congruente con 1 módulo p, entonces G es cíclico.

    b) Ningún grupo G de orden p^2q es simple.

    c) Ningún grupo G de orden p^3q es simple.

39. Los únicos grupos simples de orden menor que 60 son los de orden primo.

40. Si para cada número primo que divide al orden de un grupo finito G éste tiene un único subgrupo de Sylow, entonces G es isomorfo al producto directo de sus subgrupos de Sylow.

41. Clasificar, salvo isomorfismos, los grupos de orden ≤ 10.

42. Todo grupo de orden menor que 60 es resoluble.

43. Si p y q son números primos distintos, entonces todos los grupos de orden pq, p^2q y p^3q son resolubles.

44. Hallar resoluciones de los grupos cíclicos $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$ y $\mathbb{Z}/30\mathbb{Z}$; de los grupos abelianos $(\mathbb{Z}/15\mathbb{Z})^*$ y $(\mathbb{Z}/32\mathbb{Z})^*$; de los grupos simétricos S_2, S_3 y S_4; y de los grupos diédricos D_3, D_4 y D_5.

45. Si un grupo finito G tiene un único p-subgrupo de Sylow para cada número primo p que divide a su orden, entonces G es resoluble.

46. Si $n \geq 5$, el único subgrupo propio de S_n de índice menor que n es A_n. (*Indicación:* Si H es un subgrupo de índice d en un grupo G, la acción de G en G/H define un morfismo $G \to S_d$.)

47. Las proyectividades de una recta proyectiva sobre un cuerpo con 5 elementos definen un subgrupo P de índice 6 del grupo S_6; luego existe un automorfismo $\tau : S_6 \to S_6$ tal que $\tau(P) = \{\sigma \in S_6 : \sigma(6) = 6\}$, y éste es un automorfismo externo del grupo S_6.

Capítulo 2

Operaciones fundamentales del Álgebra

2.1. Producto tensorial de módulos

Sean M y N dos A-módulos. Consideremos el A-módulo libre $M\square N := \overset{M\times N}{\oplus} A$. Sea $\{m\square n\}_{(m,n)\in M\times N}$ la base estándar de $M\square N$, es decir, $m\square n = (a_{(m',n')})_{(m',n')\in M\times N}$ es el elemento de $M\square N$ definido por $a_{(m',n')} = 0$ si $(m',n') \neq (m,n)$ y $a_{(m,n)} = 1$.

Sea R el submódulo de $M\square N$ generado por los elementos de la forma

$$\begin{array}{l} (m+m')\square n - m\square n - m'\square n \\ m\square(n+n') - m\square n - m\square n' \\ (am)\square n - a(m\square n) \\ m\square(an) - a(m\square n) \end{array} \qquad (*)$$

para todo $m, m' \in M$, $n \in N$ y $a \in A$.

1. Definición: Llamaremos producto tensorial de M y N sobre el anillo A, al A-módulo cociente $(M\square N)/R$ y lo denotaremos $M \otimes_A N$. Cada clase $\overline{m\square n} \in (M\square N)/R = M \otimes_A N$ la denotaremos $m \otimes n$.

De acuerdo con la definición de R tenemos que

$$\boxed{\begin{array}{l} (m+m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n+n') = m \otimes n + m \otimes n' \\ am \otimes n = a(m \otimes n) \\ m \otimes an = a(m \otimes n) \end{array}}$$

propiedades que se expresan diciendo "el producto tensorial es A-bilineal". En realidad, el formalismo seguido, ha sido para llegar a definir "el producto" ($\otimes$) de elementos de M por N, con estas propiedades y sin más relaciones que las generadas por las relaciones de M y N y estas propiedades.

Dado que los elementos $\{m\square n\}_{(m,n)\in M\times N}$ forman una base de $M\square N$, entonces los elementos $\{m \otimes n\}_{(m,n)\in M\times N}$ forman un sistema generador de $M \otimes_A N$. Por las propiedades de bilinealidad recién escritas,

Si $M = \langle m_i \rangle_{i\in I}$ y $N = \langle n_j \rangle_{j\in J}$, entonces $M = \langle m_i \otimes n_j \rangle_{(i,j)\in I\times J}$.

2. Definición: Sea P un A-módulo. Diremos que una aplicación $f: M \times N \to P$ es A-bilineal si

$$f(m+m',n) = f(m,n) + f(m',n)$$
$$f(m,n+n') = f(m,n) + f(m,n')$$
$$f(am,n) = af(m,n)$$
$$f(m,an) = af(m,n)$$

El conjunto de las aplicaciones A-bilineales de $M\times N$ en P se denota $\mathrm{Bil}_A(M,N;P)$. La condición de que una aplicación $f: M \times N \to P$ sea A-bilineal expresa que la aplicación $f_m: N \to P$, $f_m(n) = f(m,n)$, es un morfismo de A-módulos para cada elemento $m \in M$. Obtenemos así, un isomorfismo natural

$$\mathrm{Bil}_A(M,N;P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$$

La aplicación natural $\pi: M \times N \to M \otimes N$, $(m,n) \mapsto m \otimes n$, es bilineal.

3. Propiedad universal del producto tensorial: *La aplicación $f: M \times N \to P$ es una aplicación bilineal si y sólo si existe un único morfismo de A-módulos $\phi: M \otimes_A N \to P$, de modo que el siguiente diagrama*

$$\begin{array}{ccc} M\times N & \xrightarrow{f} & P \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \phi} & \\ M\otimes_A N & & \end{array}$$

es conmutativo. Con concisión,

$$\mathrm{Hom}_A(M\otimes_A N, P) = \mathrm{Bil}_A(M,N;P), \quad \phi \mapsto \phi\circ\pi$$

Demostración. Sea $f: M \times N \to P$ una aplicación A-bilineal, entonces el morfismo de A-módulos

$$\varphi: M\square N \to P,\ \varphi(\sum_i a_i(m_i \square n_i)) = \sum_i a_i f(m_i,n_i)$$

se anula sobre los generadores del submódulo R, anteriormente definido en $(*)$. Por lo tanto, induce el morfismo de A-módulos $\phi: M\otimes_A N \to P$, $m\otimes n \mapsto f(m,n)$. Este morfismo cumple que $f = \phi\circ\pi$ y si un morfismo ϕ' cumple esta igualdad entonces $\phi'(m\otimes n) = f(m,n)$ y coincide con ϕ, pues los elementos $m\otimes n$ generan $M\otimes N$.

Por último, es una simple comprobación ver que dado un morfismo de A-módulos $\phi: M\otimes N \to P$ entonces $f = \phi\circ\pi$ es una aplicación bilineal de $M\times N$ en P.

□

Este teorema nos dice que definir un morfismo de A-módulos $\phi: M\otimes_A N \to P$, es asignar a cada $m\otimes n \in M\otimes_A N$ un elemento $\phi(m\otimes n)\in P$ de modo que $\phi((am+m')\otimes n) = a\phi(m\otimes n) + \phi(m'\otimes n)$ y $\phi(m\otimes(an+n')) = a\phi(m\otimes n) + \phi(m\otimes n')$.

4. Observación: Análoga construcción puede hacerse para cualquier familia finita $M_1,\dots,M_n$ de A-módulos, obteniéndose un A-módulo $M_1\otimes_A\cdots\otimes_A M_n$ con una propiedad universal similar. Para definir un morfismo de A-módulos $f: M_1\otimes_A\cdots\otimes_A M_n\to P$, bastará definir las imágenes $f(m_1\otimes\cdots\otimes m_n)$ de modo que

$$f(m_1\otimes\cdots\otimes(a_im_i+n_i)\otimes\cdots\otimes m_n)=a_if(m_1\otimes\cdots\otimes m_i\otimes\cdots\otimes m_n)+f(m_1\otimes\cdots\otimes n_i\otimes\cdots\otimes m_n)$$

5. Teorema: *Existen isomorfismos naturales*

1. $(M\otimes_A N)\otimes_A P=M\otimes_A(N\otimes_A P)$, $(m\otimes n)\otimes p\mapsto m\otimes(n\otimes p)$.
2. $M\otimes_A N=N\otimes_A M$, $m\otimes n\mapsto n\otimes m$.
3. $A\otimes_A M=M$, $a\otimes m\mapsto am$.
4. $(\oplus_i M_i)\otimes_A N=\oplus_i(M_i\otimes N)$, $(m_i)\otimes n\mapsto(m_i\otimes n)$.
5. $M\otimes_A A/I=M/IM$, $m\otimes\bar{a}\mapsto\overline{am}$.
6. $\mathrm{Hom}_A(M\otimes_A N,P)=\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, $\phi\mapsto\varphi$, *donde* $\varphi(m)(n):=\phi(m\otimes n)$.

Demostración. Dejamos al lector que defina los morfismos inversos. Veamos, sólo, que el morfismo de 1. está bien definido: Para cada p el morfismo $M\otimes_A N\times p\to M\otimes_A(N\otimes_A P)$, $(m\otimes n)\times p\mapsto m\otimes(n\otimes p)$ está bien definido. Luego tenemos un morfismo $(M\otimes_A N)\times P\to M\otimes_A(N\otimes_A P)$, que es bilineal e induce el morfismo definido en 1. □

6. Definición: Si $f: A\to B$ es un morfismo de anillos, se dice que B es una A-álgebra. Usualmente denotaremos $f(a)=a$.

Sea B una A-álgebra y N un B-módulo. Entonces, N es de modo natural un A-módulo: $a\cdot n:=f(a)\cdot n$, para todo $a\in A$ y $n\in N$. Sea M un A-módulo y N un B-módulo. Cada elemento $b\in B$ define un endomorfismo $1\otimes b: M\otimes_A N\to M\otimes_A N$, $m\otimes n\underset{\text{def}}{\mapsto} m\otimes bn$. Podemos definir así, una estructura de B-módulo en $M\otimes_A N$ que viene dada por el siguiente producto

$$b\cdot(\sum_i m_i\otimes n_i):=\sum_i m_i\otimes bn_i$$

7. Teorema: *Sea $A\to B$ un morfismo de anillos, M un A-módulo y N,P dos B-módulos. Existen isomorfismos naturales*

1. $(M\otimes_A N)\otimes_B P=M\otimes_A(N\otimes_B P)$, $(m\otimes n)\otimes p\mapsto m\otimes(n\otimes p)$.
2. $\mathrm{Hom}_B(M\otimes_A N,P)=\mathrm{Hom}_A(M,\mathrm{Hom}_B(N,P))$.

Demostración. 1. Para cada $p\in P$, tenemos el morfismo $(M\otimes_A N)\times\{p\}\to M\otimes_A(N\otimes_B P)$, $(m\otimes n,p)\mapsto m\otimes(n\otimes p)$. La aplicación B-bilineal $(M\otimes_A N)\times P\to M\otimes_A(N\otimes_B P)$, $(m\otimes n,p)\mapsto m\otimes(n\otimes p)$, induce el morfismo $(M\otimes_A N)\otimes_B P\to M\otimes_A(N\otimes_B P)$, $(m\otimes n)\otimes p\mapsto m\otimes(n\otimes p)$.

Tenemos la aplicación A-bilineal $M\times(N\otimes_B P)\to(M\otimes_A N)\otimes_B P$, $(m,n\otimes p)\mapsto(m\otimes n)\otimes p$, que induce el morfismo $M\otimes_A(N\otimes_B P)\to M\otimes_A N)\otimes_B P$, $m\otimes(n\otimes p)\mapsto(m\otimes n)\otimes p$.

Ambos morfismos son inversos entre sí.

2. Basta comprobar que vía la igualdad $\mathrm{Hom}_A(M\otimes_A N,P)=\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))$, el submódulo $\mathrm{Hom}_B(M\otimes_A N,P)$ es igual al submódulo $\mathrm{Hom}_A(M,\mathrm{Hom}_B(N,P))$.

□

Sea $f: A\to B$ un morfismo de anillos. Se dice que $M\otimes_A B$ es el cambio de anillo base de M por $A\to B$.

Notación: Denotaremos $M\otimes_A B = M_B$.

8. Proposición : *Sean $A\to B$ y $B\to C$ morfismos de anillos, M y M' A-módulos. Existen isomorfismos naturales*

1. $(M\otimes_A M')\otimes_A B = M_B\otimes_B M'_B$, $(m\otimes m')\otimes b\mapsto (m\otimes b)\otimes(m'\otimes 1)$.

2. $(M_B)_C = M_C$, *(i.e.,* $(M\otimes_A B)\otimes_B C = M\otimes_A C$, $(m\otimes b)\otimes c\mapsto m\otimes bc$*).*

Demostración. 1. $M_B\otimes_B M'_B = (M\otimes_A B)\otimes_B M'_B = M\otimes_A (B\otimes_B M'_B) = M\otimes_A M'_B = (M\otimes_A M')\otimes_A B$.

2. $(M\otimes_A B)\otimes_B C = M\otimes_A (B\otimes_B C) = M\otimes_A C$. □

2.2. Producto tensorial de álgebras

Ahora, nuestro objetivo es definir el producto tensorial de A-álgebras.

1. Definición : Dadas dos A-álgebras B y C, diremos que un morfismo de anillos $\phi: B\to C$ es un morfismo de A-álgebras si $\phi(a)=a$, para todo $a\in A$. Denotaremos $\mathrm{Hom}_{A-alg}(B,C)$ al conjunto de todos los morfismos de A-álgebras de B en C.

2. Ejemplo : $\mathbb{C}$ es una $\mathbb{R}$-álgebra del modo obvio. Dado un anillo A, $A[x_1,\dots,x_n]$ es una A-álgebra: $A\to A[x_1,\dots,x_n]$, $a\mapsto a$.

3. Ejercicio : Calcular $\mathrm{Hom}_{A-alg}(A[x_1,\dots,x_n],B)$.

Si B y C son A-álgebras, el A-módulo $B\otimes_A C$ tiene una estructura de A-álgebra natural: El producto es el morfismo $B\otimes_A C\times B\otimes_A C\to B\otimes_A C$, $(b\otimes c,b'\otimes c')\mapsto bb'\otimes cc'$ inducido por el correspondiente morfismo $B\otimes_A C\otimes B\otimes_A C\to B\otimes_A C$. Con este producto $B\otimes_A C$ es un anillo. Por último, el morfismo $A\to B\otimes_A C$, $a\mapsto a\otimes 1=1\otimes a$ es un morfismo de anillos.

4. Proposición : *Sean B,C y D A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc}\mathrm{Hom}_{A-alg}(B\otimes_A C,D) & \longleftrightarrow & \mathrm{Hom}_{A-alg}(B,D)\times\mathrm{Hom}_{A-alg}(C,D)\\ \phi & \longmapsto & (\phi_1,\phi_2),\ \textit{donde}\ \ \phi_1(b):=\phi(b\otimes 1),\phi_2(c):=\phi(1\otimes c)\\ \phi & \longleftarrow & (\phi_1,\phi_2)\end{array}$$

$\phi(b\otimes c):=\phi_1(b)\phi_2(c)$

5. Proposición: *Sean B y C A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc} \mathrm{Hom}_{A-alg}(B,C) & = & \mathrm{Hom}_{C-alg}(B_C,C) \\ \phi & \longmapsto & \phi' \text{ donde } \phi'(b\otimes c) := \phi(b)\cdot c \\ \phi'_{|B} & \longleftarrow\!\shortmid & \phi' \end{array}$$

$$\phi'_{|B}(b) := \phi'(b\otimes 1)$$

2.3. Espectro primo de un anillo

1. Notación: Dado un anillo A denotaremos $\mathrm{Spec}A$, que denominaremos espectro primo de A, al conjunto de los ideales primos de A. Al elemento $x \in \mathrm{Spec}A$ cuando lo pensemos como ideal primo incluido en A, lo denotaremos $\mathfrak{p}_x$ (o $\mathfrak{m}_x$ si $\mathfrak{p}_x$ es maximal).

2. Ejemplos: $\mathrm{Spec}\mathbb{Z} = \{(p),\ p \in \mathbb{N} \text{ primo y } (0)\}$. $\mathrm{Spec}k[x] = \{(p(x)),\ p(x) \text{ mónico irreducible y el ideal } (0)\}$. $\mathrm{Spec}\mathbb{C}[x] = \{(x-\alpha),\ \alpha \in \mathbb{C} \text{ y el ideal } (0)\}$

Cada morfismo de anillos $f: A \to B$ induce el morfismo $f^*: \mathrm{Spec}B \to \mathrm{Spec}A$, $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$.

3. Notación: Dado un ideal $I \subseteq A$ denotamos $(I)_0 := \{x \in \mathrm{Spec}A : I \subseteq \mathfrak{p}_x\}$.

Consideremos el morfismo de paso al cociente $\pi: A \to A/I$. La aplicación, $\mathrm{Spec}A/I \to \mathrm{Spec}A$, $\mathfrak{q} \mapsto \pi^{-1}(\mathfrak{q})$ es inyectiva y de imagen $(I)_0$, es decir,

$$\mathrm{Spec}A/I = (I)_0,\ \mathfrak{q} \mapsto \pi^{-1}(\mathfrak{q})$$

y la aplicación inversa es $(I)_0 = \mathrm{Spec}A/I$, $\mathfrak{p} \mapsto \pi(\mathfrak{p}) = \bar{\mathfrak{p}}$.

4. Lema: *Sean $I_1, I_2 \subseteq A$ dos ideales. Se cumple*

1. $(I)_0 = \emptyset$ *si y sólo si* $I = A$.
2. $(I_1 + I_2)_0 = (I_1)_0 \cap (I_2)_0$.
3. $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0$

Demostración. Sólo ofrece alguna dificultad 3. Obviamente $(I_1)_0 \cup (I_2)_0 \subseteq (I_1 \cdot I_2)_0$. Si $x \notin (I_1)_0 \cup (I_2)_0$, entonces existen $f_1 \in I_1$ y $f_2 \in I_2$ de modo que $f_1, f_2 \notin \mathfrak{p}_x$, luego $f_1 \cdot f_2 \notin \mathfrak{p}_x$ y $x \notin (I_1 \cdot I_2)_0$. Luego $(I_1 \cdot I_2)_0 \subseteq (I_1)_0 \cup (I_2)_0$ y tenemos la igualdad. □

5. Ejercicio: Calcular $\mathrm{Spec}\mathbb{R}[x]/((x^2+1)\cdot x)$.

6. Ejercicio: Calcular $\mathrm{Spec}\mathbb{Z}/(12)$.

2.4. Localización de anillos

1. Definición: Sea A y $S \subseteq A$ un subconjunto. Diremos que S es un sistema multiplicativo de A si cumple

1. $1 \in S$.

2. Si $s, s' \in S$ entonces $s \cdot s' \in S$.

2. Ejemplo: $\mathbb{Z}\setminus\{0\}$ es un sistema multiplicativo de $\mathbb{Z}$.

3. Definición: Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. La localización de A por S, A_S, es el conjunto

$$A_S := \left\{ \frac{a}{s},\ a \in A \text{ y } s \in S : \begin{array}{l} \dfrac{a}{s} = \dfrac{a'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones} \\ \dfrac{s_1 a}{s_1 s}, \dfrac{s_2 a'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \end{array} \right\}^1$$

Con la suma y producto ordinarios de fracciones

$$\frac{a}{s} + \frac{a'}{s'} := \frac{s'a + sa'}{ss'}$$
$$\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

A_S es un anillo. El elemento unidad de A_S es la fracción $\frac{1}{1}$. Si $s \in S$ entonces la fracción $\frac{s}{1}$ es invertible, de inverso $\frac{1}{s}$. La fracción $\frac{0}{s} = \frac{0 \cdot s}{1 \cdot s} = \frac{0}{1}$ es el elemento nulo de A_S.

4. Ejercicio: Probar que una fracción $\frac{a}{s} = 0 \in A_S$ si y sólo si existe $s' \in S$ tal que $s' \cdot a = 0$ (en A).

5. Definición: Si A es un anillo íntegro, obviamente $A_{A\setminus\{0\}}$ es un cuerpo y diremos que es el cuerpo de fracciones de A.

6. Ejemplos: 1. $\mathbb{Q} = \mathbb{Z}_{\mathbb{Z}\setminus\{0\}}$,

2. $\mathbb{Q}(x) := \mathbb{Q}[x]_{\mathbb{Q}[x]\setminus\{0\}}$

3. $k(x) := k[x]_{k[x]\setminus\{0\}} = \{p(x)/q(x),\ p(x), q(x) \in k[x], q(x) \neq 0\}$, o con mayor generalidad, el cuerpo de funciones racionales en n-variables con coeficientes en k,

$$k(x_1, \ldots, x_n) := k[x_1, \ldots, x_n]_{k[x_1,\ldots,x_n]\setminus\{0\}} = \{p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n), \\ p(x_1, \ldots, x_n), 0 \neq q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]\}$$

7. Definición: Al morfismo natural de anillos $A \to A_S$, $a \mapsto \frac{a}{1}$ se le denomina morfismo de localización por S.

8. Ejercicio: Probar que el núcleo del morfismo de localización $A \to A_S$, es igual al ideal de elementos de A anulados por algún S.

9. Ejercicio: Probar que $(\mathbb{Z}[x])_{\mathbb{Z}\setminus\{0\}} = \mathbb{Q}[x]$.

[1] Observemos que $\frac{a}{s} = \frac{a}{s}$, que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'}{s'} = \frac{a}{s}$, y que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{a'}{s'} = \frac{a''}{s''}$ entonces $\frac{a}{s} = \frac{a''}{s''}$.

10. Proposición: *Sea $S \subseteq A$ un sistema multiplicativo y $i: A \to A_S$ el morfismo de localización. Entonces, la aplicación*

$$i^*: \operatorname{Spec} A_S \to \operatorname{Spec} A$$

es inyectiva y de imagen los ideales primos de A disjuntos con S. Si $\mathfrak{p}$ es un ideal primo de A disjunto con S entonces $\mathfrak{p} \cdot A_S$ es el ideal primo de A_S tal que $i^{-1}(\mathfrak{p} \cdot A_S) = \mathfrak{p}$.

Demostración. Sea $\mathfrak{q}$ un ideal primo de A_S. Entonces, $\mathfrak{p} := i^{-1}(\mathfrak{q}) = \{a \in A : a/1 \in \mathfrak{q}\}$. Dado $a/s \in \mathfrak{q}$ entonces $a/1 \in \mathfrak{q}$, luego $a \in \mathfrak{p}$. Por tanto, $\mathfrak{p} \cdot A_S = \mathfrak{q}$. Si $s \in S$ pertenece a $\mathfrak{p}$, entonces $s/1 \in \mathfrak{q}$, luego $1/1 \in \mathfrak{q}$ y $\mathfrak{q} = A_S$ lo cual es imposible. Por último, dejamos que el lector compruebe que si $\mathfrak{p}$ es un ideal primo de A disjunto con S entonces $\mathfrak{p} \cdot A_S$ es el ideal primo de A_S tal que $i^{-1}(\mathfrak{p} \cdot A_S) = \mathfrak{p}$. □

11. Notación: Dado $x \in \operatorname{Spec} A$ denotamos $A_x := A_{A \setminus \mathfrak{p}_x}$.

Por la proposición anterior, $\{y \in \operatorname{Spec} A : \mathfrak{p}_y \subseteq \mathfrak{p}_x\} = \operatorname{Spec} A_x$, $\mathfrak{p}_y \mapsto \mathfrak{p}_y \cdot A_x$.

Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$M_S = \left\{ \frac{m}{s},\ m \in M \text{ y } s \in S : \frac{m}{s} = \frac{m'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones } \frac{s_1 m}{s_1 s}, \frac{s_2 m'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \right\}^2$$

Con las operaciones (bien definidas)

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$$
$$\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$$

12. Ejercicio: Probar que $0 = m/s \in M_S$ si y sólo si existe $t \in S$ de modo que $tm = 0$.

M_S tiene estructura de A_S-módulo y diremos que es la localización de M por S. La aplicación canónica

$$M \to M_S,\ m \mapsto \frac{m}{1}$$

es un morfismo de A-módulos y diremos que es el morfismo de localización. Dado un morfismo $f: M \to N$ de A-módulos, induce de modo natural la aplicación (bien definida)

$$f_S: M_S \to N_S,\ \frac{m}{s} \underset{\text{def}}{\mapsto} \frac{f(m)}{s}$$

que es morfismo de A_S-módulos. Es inmediato comprobar que la localización de morfismos es compatible con composiciones.

13. Proposición: *Sea $S \subseteq A$ un sistema multiplicativo, M un A-módulo y $N \subseteq M$ un submódulo. Entonces, N_S es un submódulo de M_S y $M_S/N_S = (M/N)_S$.*

[2] Observemos que $\frac{m}{s} = \frac{m}{s}$, que si $\frac{m}{s} = \frac{m'}{s'}$ entonces $\frac{m'}{s'} = \frac{m}{s}$, y que si $\frac{m}{s} = \frac{m'}{s'}$ y $\frac{m'}{s'} = \frac{m''}{s''}$ entonces $\frac{m}{s} = \frac{m''}{s''}$.

Demostración. Veamos que el morfismo natural $N_S \to M_S$, $n/s \mapsto n/s$ es inyectivo, pues si $n/s = 0$ en M_S, existe $t \in S$ tal que $tn = 0$, luego $n/s = 0$ en N_S.

Veamos que el núcleo del epimorfismo natural $M_S \to (M/N)_S$, $m/s \mapsto \bar{m}/s$ es N_S: Si $\bar{m}/s = 0$, existe $t \in S$ tal que $t\bar{m} = 0$, luego $tm \in N$ y $tm/ts \mapsto \overline{tm}/ts = \bar{m}/s$. □

2.4.1. Radical de un anillo

14. Definición: Sea A un anillo. Diremos que $a \in A$ es nilpotente si existe un número natural $n > 0$, tal que $a^n = 0$. Llamaremos radical de un anillo A, que denotaremos $\operatorname{rad} A$, al conjunto de todos los elementos de A que son nilpotentes.

15. Ejercicio: Calcular $\operatorname{rad} \mathbb{Q}[x]/(x^3)$.

16. Ejercicio: Probar que $\operatorname{rad} A$ es un ideal.

17. Proposición: *Sea A un anillo y $S \subseteq A$ un sistema multiplicativo. Entonces, $A_S = \{0\} \iff 0 \in S$.*

Demostración. Si $0 \in S$, entonces $\frac{a}{s} = \frac{0 \cdot a}{0 \cdot s} = \frac{0}{0}$, para todo $a \in A$ y $s \in S$. Luego, $A_S = \{0\}$, pues sólo tiene un único elemento.

Si $A_S = \{0\}$, entonces $\frac{1}{1} = \frac{0}{1}$, luego existe $s \in S$ tal que $s \cdot 1 = s \cdot 0$, luego $0 = s \in S$.

□

18. Proposición: *El radical de un anillo es igual a la intersección de todos los ideales primos del anillo, es decir,*

$$\operatorname{rad} A = \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$$

Demostración. Dado $a \in A$, definamos el sistema multiplicativo $S = \{1, a, a^2, \ldots, a^n, \ldots\}$. Entonces, a es nilpotente si y sólo si $0 \in S$; $0 \in S$ si y sólo si $A_S = 0$; $A_S = 0$ si y sólo si $\operatorname{Spec} A_S = \emptyset$; $\operatorname{Spec} A_S = \emptyset$ si y sólo si $S \cap \mathfrak{p}_x \neq \emptyset$ para todo $x \in \operatorname{Spec} A$. Por último, $S \cap \mathfrak{p}_x \neq \emptyset$ si y sólo si $a \in \mathfrak{p}_x$.

□

19. Definición: Se dice que un anillo A es reducido si $\operatorname{rad} A = 0$.

20. Ejercicio: Sea A un anillo. Probar que $A/\operatorname{rad} A$ es un anillo reducido.

2.4.2. Teorema chino de los restos

21. Proposición: *1. Sea $f : M \to M'$ un morfismo de A-módulos. Si $f_x : M_x \to M'_x$, $f_x(m/s) := f(m)/s$ es un isomorfismo para todo $x \in \operatorname{Spec}_{max} A$, entonces f es un isomorfismo.*

2. Sea M un A-módulo. Si $M_x = 0$ para todo $x \in \operatorname{Spec}_{max} A$, entonces $M = 0$.

Demostración. 1. Sea $m \in \operatorname{Ker} f$ e $I := \{a \in A : am = 0\}$. Si $I = A$ entonces $m = 1 \cdot m = 0$. Supongamos que $I \neq A$. Sea $\mathfrak{m}_x$ un ideal maximal tal que $I \subseteq \mathfrak{m}_x$. Tenemos que $m/1 \in \operatorname{Ker} f_x = 0$, luego existe $s \in A \setminus \mathfrak{m}_x$ tal que $sm = 0$, es decir, $s \in I \subseteq \mathfrak{m}_x$. Contradicción. Por tanto, $\operatorname{Ker} f = 0$.

Sea $m' \in M'$ e $I := \{a \in A : a \cdot m' \in \operatorname{Im} f\}$. Si $I = A$ entonces $m' \in \operatorname{Im} f$. Supongamos que $I \neq A$. Sea $\mathfrak{m}_x$ un ideal maximal tal que $I \subseteq \mathfrak{m}_x$. Por hipótesis, $m'/1 \in \operatorname{Im} f_x$, es decir, existen $m \in M$ y $s \in A \setminus \mathfrak{m}_x$ tal que $m'/1 = f_x(m/s) = f(m)/s$, es decir, $(sm' - f(m))/s = 0$. Por tanto, existe $s' \in A \setminus \mathfrak{m}_x$ tal que $s'sm' - s'f(m) = 0$, luego $s's \in I \subseteq \mathfrak{m}_x$ y $s's \in A \setminus \mathfrak{m}_x$. Contradicción. Luego, $m' \in \operatorname{Im} f$.

2. El morfismo $0 \to M$ es isomorfismo al localizar en todo punto $x \in \operatorname{Spec}_{max} A$, luego es isomorfismo.

□

22. Teorema chino de los restos: *Sean $I, I' \subseteq A$ ideales tales que $I + I' = A$. Entonces,*

$$A/I \cdot I' = A/I \times A/I', \ \bar{a} \mapsto (\bar{a}, \bar{a})$$

Demostración. $\emptyset = (A)_0 = (I + I')_0 = (I)_0 \cap (I')_0$. Por tanto, dado $x \in \operatorname{Spec}_{max} A$, o $I \nsubseteq \mathfrak{m}_x$, o bien $I' \nsubseteq \mathfrak{m}_x$. Supongamos que $I \nsubseteq \mathfrak{m}_x$, por tanto existe $i \in I \cap (A \setminus \mathfrak{m}_x)$, luego $I_x = A_x$, porque $i/1 \in I_x \subseteq A_x$ es invertible. Por tanto,

$$(A/I \cdot I')_x = A_x/(I_x \cdot I'_x) = A_x/I'_x \text{ y } (A/I \times A/I')_x = (A/I)_x \times (A/I')_x = A_x/A_x \times A_x/I'_x = A_x/I'_x$$

y por la proposición 2.4.21, $A/I \cdot I' = A/I \times A/I'$.

□

2.4.3. Teorema de Gauss

23. Definición: Diremos que un elemento propio (no nulo ni invertible) de un anillo íntegro es irreducible si no es producto de dos elementos no invertibles del anillo.

24. Definición: Un anillo íntegro se dice que es un dominio de factorización única si todo elemento propio del anillo es producto de elementos irreducibles, de modo único salvo orden y factores invertibles.

25. Ejemplo: Los dominios de ideales principales son dominios de factorización única.

DFU significará dominio de factorización única.

26. Proposición: *Si A es DFU y $a \in A$ es irreducible, entonces $(a) \subset A$ es un ideal primo.*

Demostración. Sea $b \cdot c \in (a)$. Existe $d \in A$ tal que $b \cdot c = a \cdot d$. Si consideramos las descomposición en factores irreducibles de b, c y d, y recordamos que A es DFU, tenemos que a aparece (salvo multiplicación por un invertible) en la descomposición en producto de factores irreducibles de b o c. Luego, a divide a b o c. En conclusión, $(a) \subset A$ es un ideal primo.

□

27. Definición: Un polinomio $P(x) \in A[x]$ se dice *primitivo* cuando sus coeficientes no admiten un divisor común no invertible, es decir, si $P(x) = a \cdot Q(x)$ con $a \in A$, entonces a es invertible.

28. Lema: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Sean $P(x), Q(x) \in A[x]$ dos polinomios primitivos. Entonces,*

1. *$P(x)\cdot Q(x)$ es primitivo.*

2. *Si existen $a,b\in A$ tales que $a\cdot P(x)=b\cdot Q(x)$, entonces $b=a\cdot u$, para cierto invertible $u\in A$. Por tanto, si $P(x)=\frac{b}{a}\cdot Q(x)$ en $\Sigma[x]$, entonces $\frac{b}{a}=u\in A$ es un invertible de A.*

Demostración. 1. Supongamos que $P(x)\cdot Q(x)=a\cdot R(x)$, con $R(x)\in A[x]$ y $a\in A$ no invertible. Sea $p\in A$ irreducible que divida a a. Haciendo cociente en $A[X]$ por $p\cdot A[x]$, tenemos que

$$\overline{P(x)}\cdot\overline{Q(x)}=0\in(A/pA)[x]$$

lo cual es contradictorio, porque $(A/pA)[x]$ es íntegro y $\overline{P(x)}$ y $\overline{Q(x)}$ son no nulos.

2. Sea p un elemento irreducible que divida a a. Haciendo cociente en $A[X]$ por $p\cdot A[x]$, tenemos que $0=\bar{b}\cdot\overline{Q(x)}$, luego $\bar{b}=0$ y p divide a b. Dividiendo a a y b a la vez por p y repitiendo sucesivamente este proceso obtendremos que a divide a b, y por simetría que b divide a a. Luego, $b=a\cdot u$, para cierto invertible $u\in A$. □

29. Teorema : *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio no constante primitivo, $P(x)\in A[x]$, es irreducible en $A[x]$ si y sólo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $P(x)$ es irreducible en $\Sigma[x]$. Si $P(x)=P_1(x)\cdot P_2(x)$, con $P_1(x),P_2(x)\in A[x]$, entonces como $P(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $P_1(x)$ o $P_2(x)$ ha de ser de grado cero, digamos $P_1(x)=a$. Como $P(x)$ es primitivo $P_1(x)=a\in A$ es invertible. En conclusión, $P(x)$, es irreducible en $A[x]$.

Supongamos que $P(x)$ es irreducible en $A[X]$. Supongamos que $P(x)=\tilde{P}_1(x)\cdot\tilde{P}_2(x)$, siendo $\tilde{P}_1(x),\tilde{P}_2(x)\in\Sigma[x]$. Eliminando denominadores podemos suponer que

$$P(x)=\frac{a}{b}P_1(x)\cdot P_2(x)$$

con $P_1(x),P_2(x)\in A[x]$, primitivos. Por el lema 2.4.28, $\frac{a}{b}=u\in A$, luego $P(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

30. Teorema (Gauss): *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

Demostración. Sea $\Sigma=A_{A\setminus\{0\}}$ el cuerpo de fracciones. Sea $P(x)\in A[x]$ y escribamos $P(x)=a\cdot Q(x)$, con $a\in A$ y $Q(x)\in A[x]$ primitivo. Sea

$$Q(x)=\widetilde{Q}_1(x)\cdots\widetilde{Q}_r(x)$$

la descomposición en irreducibles en $\Sigma[x]$. Eliminando denominadores y sacando el máximo común divisor en los numeradores, es claro que se puede escribir:

$$Q(x)=\frac{b}{c}\cdot Q_1(x)\cdots Q_r(x)\qquad(*)$$

con $Q_i(x) = \frac{a_i}{b_i}\widetilde{Q}_i \in A[x]$ primitivos.

• Por el lema 2.4.28, $\frac{b}{c} = u \in A$ es un invertible de A.

• Cada $Q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por el teorema 2.4.29.

Descomponiendo $a = p_1 \cdots p_s$ en producto de irreducibles en A, se obtiene una descomposición de

$$P(x) = a \cdot Q(x) = u \cdot p_1 \cdots p_s Q_1(x) \cdots Q_r(x)$$

en $A[x]$.

Unicidad: Si $P(x) = q_1 \cdots q_l P_1(x) \cdots P_t(x)$, entonces cada $P_i(x)$ es irreducible en $\Sigma[x]$ por el teorema 2.4.29. Por tanto, los polinomios $P_i(x)$ (una vez reordenados) difieren de los $Q_i(x)$ en invertibles de A. Tachando los términos polinómicos comunes se obtiene, salvo invertibles de A, la igualdad $q_1 \cdots q_l = p_1 \cdots p_s$, de donde salvo permutación de los factores es $q_i = p_i$ (salvo invertibles de A).

□

Como corolario del teorema anterior, se obtiene el siguiente teorema.

31. Teorema : *Los anillos $\mathbb{Z}[x_1,\ldots,x_n]$ y $k[x_1,\ldots,x_n]$ (k un cuerpo) son dominios de factorización única.*

2.5. Biografía de Gauss

GAUSS BIOGRAPHY

At the age of seven, Carl Friedrich Gauss started elementary school, and his potential was noticed almost immediately. His teacher, Büttner, and his assistant, Martin Bartels, were amazed when Gauss summed the integers from 1 to 100 instantly by spotting that the sum was 50 pairs of numbers each pair summing to 101.

In 1788 Gauss began his education at the Gymnasium with the help of Büttner and Bartels, where he learnt High German and Latin. After receiving a stipend from the Duke of Brunswick-Wolfenbüttel, Gauss entered Brunswick Collegium Carolinum in 1792. At the academy Gauss independently discovered Bode's law, the binomial theorem and the arithmetic-geometric mean, as well as the law of quadratic reciprocity and the prime number theorem.

In 1795 Gauss left Brunswick to study at Göttingen University. Gauss's teacher there was Kästner, whom Gauss often ridiculed. His only known friend amongst the students was Farkas Bolyai. They met in 1799 and corresponded with each other for many years.

Gauss left Göttingen in 1798 without a diploma, but by this time he had made one of his most important discoveries - the construction of a regular 17-gon by ruler and compasses This was the most major advance in this field since the time of Greek mathematics and was published as Section VII of Gauss's famous work, Disquisitiones Arithmeticae.

Gauss returned to Brunswick where he received a degree in 1799. After the Duke of Brunswick had agreed to continue Gauss's stipend, he requested that Gauss submit a doctoral dissertation to the University of Helmstedt. He already knew Pfaff, who was chosen to be his advisor. Gauss's dissertation was a discussion of the fundamental theorem of algebra.

With his stipend to support him, Gauss did not need to find a job so devoted himself to research. He published the book Disquisitiones Arithmeticae in the summer of 1801. There were seven sections, all but the last section, referred to above, being devoted to number theory.

In June 1801, Zach, an astronomer whom Gauss had come to know two or three years previously, published the orbital positions of Ceres, a new "small planet" which was discovered by G Piazzi, an Italian astronomer on 1 January, 1801. Unfortunately, Piazzi had only been able to observe 9 degrees of its orbit before it disappeared behind the Sun. Zach published several predictions of its position, including one by Gauss which differed greatly from the others. When Ceres was rediscovered by Zach on 7 December 1801 it was almost exactly where Gauss had predicted. Although he did not disclose his methods at the time, Gauss had used his least squares approximation method.

In June 1802 Gauss visited Olbers who had discovered Pallas in March of that year and Gauss investigated its orbit. Olbers requested that Gauss be made director of the proposed new observatory in Göttingen, but no action was taken. Gauss began corresponding with Bessel, whom he did not meet until 1825, and with Sophie Germain.

Gauss married Johanna Ostoff on 9 October, 1805. Despite having a happy personal life for the first time, his benefactor, the Duke of Brunswick, was killed fighting for the Prussian army. In 1807 Gauss left Brunswick to take up the position of director of the Göttingen observatory.

Gauss arrived in Göttingen in late 1807. In 1808 his father died, and a year later Gauss's wife Johanna died after giving birth to their second son, who was to die soon after her. Gauss was shattered and wrote to Olbers asking him to give him a home for a few weeks,

to gather new strength in the arms of your friendship - strength for a life which is only valuable because it belongs to my three small children.

Gauss was married for a second time the next year, to Minna the best friend of Johanna, and although they had three children, this marriage seemed to be one of convenience for Gauss.

Gauss's work never seemed to suffer from his personal tragedy. He published his second book, Theoria motus corporum coelestium in sectionibus conicis Solem ambientium, in 1809, a major two volume treatise on the motion of celestial bodies. In the first volume he discussed differential equations, conic sections and elliptic orbits, while in the second volume, the main part of the work, he showed how to estimate and then to refine the estimation of a planet's orbit. Gauss's contributions to theoretical astronomy stopped after 1817, although he went on making observations until the age of 70.

Much of Gauss's time was spent on a new observatory, completed in 1816, but he still found the time to work on other subjects. His publications during this time in-

clude Disquisitiones generales circa seriem infinitam, a rigorous treatment of series and an introduction of the hypergeometric function, Methodus nova integralium valores per approximationem inveniendi, a practical essay on approximate integration, Bestimmung der Genauigkeit der Beobachtungen, a discussion of statistical estimators, and Theoria attractionis corporum sphaeroidicorum ellipticorum homogeneorum methodus nova tractata. The latter work was inspired by geodesic problems and was principally concerned with potential theory. In fact, Gauss found himself more and more interested in geodesy in the 1820s.

Gauss had been asked in 1818 to carry out a geodesic survey of the state of Hanover to link up with the existing Danish grid. Gauss was pleased to accept and took personal charge of the survey, making measurements during the day and reducing them at night, using his extraordinary mental capacity for calculations. He regularly wrote to Schumacher, Olbers and Bessel, reporting on his progress and discussing problems.

Because of the survey, Gauss invented the heliotrope which worked by reflecting the Sun's rays using a design of mirrors and a small telescope. However, inaccurate base lines were used for the survey and an unsatisfactory network of triangles. Gauss often wondered if he would have been better advised to have pursued some other occupation but he published over 70 papers between 1820 and 1830.

In 1822 Gauss won the Copenhagen University Prize with Theoria attractionis... together with the idea of mapping one surface onto another so that the two are similar in their smallest parts. This paper was published in 1825 and led to the much later publication of Untersuchungen über Gegenstände der Höheren Geodäsie (1843 and 1846). The paper Theoria combinationis observationum erroribus minimis obnoxiae (1823), with its supplement (1828), was devoted to mathematical statistics, in particular to the least squares method.

From the early 1800s Gauss had an interest in the question of the possible existence of a non-Euclidean geometry. He discussed this topic at length with Farkas Bolyai and in his correspondence with Gerling and Schumacher. In a book review in 1816 he discussed proofs which deduced the axiom of parallels from the other Euclidean axioms, suggesting that he believed in the existence of non-Euclidean geometry, although he was rather vague.

... the vain effort to conceal with an untenable tissue of pseudo proofs the gap which one cannot fill out.

Gauss confided in Schumacher, telling him that he believed his reputation would suffer if he admitted in public that he believed in the existence of such a geometry.

In 1831 Farkas Bolyai sent to Gauss his son János Bolyai's work on the subject. Gauss replied

to praise it would mean to praise myself.

Again, a decade later, when he was informed of Lobachevsky's work on the subject, he praised its "genuinely geometric" character, while in a letter to Schumacher in 1846, states that he

had the same convictions for 54 years.

indicating that he had known of the existence of a non-Euclidean geometry since he was 15 years of age (this seems unlikely).

Gauss had a major interest in differential geometry, and published many papers on the subject. Disquisitiones generales circa superficies curva (1828) was his most renowned work in this field. In fact, this paper rose from his geodesic interests, but it contained such geometrical ideas as Gaussian curvature. The paper also includes Gauss's famous theorema egregrium:

If an area in E^3 can be developed (i.e. mapped isometrically) into another area of E^3, the values of the Gaussian curvatures are identical in corresponding points.

The period 1817-1832 was a particularly distressing time for Gauss. He took in his sick mother in 1817, who stayed until her death in 1839, while he was arguing with his wife and her family about whether they should go to Berlin. He had been offered a position at Berlin University and Minna and her family were keen to move there. Gauss, however, never liked change and decided to stay in Göttingen. In 1831 Gauss's second wife died after a long illness.

In 1831, Wilhelm Weber arrived in Göttingen as physics professor filling Tobias Mayer's chair. Gauss had known Weber since 1828 and supported his appointment. Gauss had worked on physics before 1831, publishing Über ein neues allgemeines Grundgesetz der Mechanik, which contained the principle of least constraint, and Principia generalia theoriae figurae fluidorum in statu aequilibrii which discussed forces of attraction. These papers were based on Gauss's potential theory, which proved of great importance in his work on physics. He later came to believe his potential theory and his method of least squares provided vital links between science and nature.

In 1832, Gauss and Weber began investigating the theory of terrestrial magnetism after Alexander von Humboldt attempted to obtain Gauss's assistance in making a grid of magnetic observation points around the Earth. Gauss was excited by this prospect and by 1840 he had written three important papers on the subject: Intensitas vis magneticae terrestris ad mensuram absolutam revocata (1832), Allgemeine Theorie des Erdmagnetismus (1839) and Allgemeine Lehrsätze in Beziehung auf die im verkehrten Verhältnisse des Quadrats der Entfernung wirkenden Anziehungs- und Abstossungskräfte (1840). These papers all dealt with the current theories on terrestrial magnetism, including Poisson's ideas, absolute measure for magnetic force and an empirical definition of terrestrial magnetism. Dirichlet's principle was mentioned without proof.

Allgemeine Theorie... showed that there can only be two poles in the globe and went on to prove an important theorem, which concerned the determination of the intensity of the horizontal component of the magnetic force along with the angle of inclination. Gauss used the Laplace equation to aid him with his calculations, and ended up specifying a location for the magnetic South pole.

Humboldt had devised a calendar for observations of magnetic declination. However, once Gauss's new magnetic observatory (completed in 1833 - free of all magnetic metals) had been built, he proceeded to alter many of Humboldt's procedures, not pleasing Humboldt greatly. However, Gauss's changes obtained more accurate results with less effort.

Gauss and Weber achieved much in their six years together. They discovered Kirchhoff's laws, as well as building a primitive telegraph device which could send messages over a distance of 5000 ft. However, this was just an enjoyable pastime for Gauss. He was more interested in the task of establishing a world-wide net of magnetic observation points. This occupation produced many concrete results. The Magnetischer Verein and its journal were founded, and the atlas of geomagnetism was published, while Gauss and Weber's own journal in which their results were published ran from 1836 to 1841.

In 1837, Weber was forced to leave Göttingen when he became involved in a political dispute and, from this time, Gauss's activity gradually decreased. He still produced letters in response to fellow scientists' discoveries usually remarking that he had known the methods for years but had never felt the need to publish. Sometimes he seemed extremely pleased with advances made by other mathematicians, particularly that of Eisenstein and of Lobachevsky.

Gauss spent the years from 1845 to 1851 updating the Göttingen University widow's fund. This work gave him practical experience in financial matters, and he went on to make his fortune through shrewd investments in bonds issued by private companies.

Two of Gauss's last doctoral students were Moritz Cantor and Dedekind. Dedekind wrote a fine description of his supervisor

... usually he sat in a comfortable attitude, looking down, slightly stooped, with hands folded above his lap. He spoke quite freely, very clearly, simply and plainly: but when he wanted to emphasise a new viewpoint ... then he lifted his head, turned to one of those sitting next to him, and gazed at him with his beautiful, penetrating blue eyes during the emphatic speech. ... If he proceeded from an explanation of principles to the development of mathematical formulas, then he got up, and in a stately very upright posture he wrote on a blackboard beside him in his peculiarly beautiful handwriting: he always succeeded through economy and deliberate arrangement in making do with a rather small space. For numerical examples, on whose careful completion he placed special value, he brought along the requisite data on little slips of paper.

Gauss presented his golden jubilee lecture in 1849, fifty years after his diploma had been granted by Helmstedt University. It was appropriately a variation on his dissertation of 1799. From the mathematical community only Jacobi and Dirichlet were present, but Gauss received many messages and honours.

From 1850 onwards Gauss's work was again nearly all of a practical nature although he did approve Riemann's doctoral thesis and heard his probationary lecture. His last known scientific exchange was with Gerling. He discussed a modified Foucault pendulum in 1854. He was also able to attend the opening of the new railway link between Hanover and Göttingen, but this proved to be his last outing. His health deteriorated slowly, and Gauss died in his sleep early in the morning of 23 February, 1855.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

2.6. Cuestionario

1. ¿Si M y N son A-módulos finito generados, es $M \otimes_A N$ finito generado?

2. Sea $m \in M$ y $0 \in N$. ¿Es $m \otimes 0 = 0$?

3. ¿Es $(am) \otimes n = m \otimes (an)$?

4. Sea $2 \otimes \bar{1} \in \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. ¿Es $2 \otimes \bar{1} = 0$?

5. ¿Es $f : A[x] \otimes_A A[y] \to A[x,y]$, $f(p_1(x) \otimes q_1(y) + \cdots + p_n(x) \otimes q_n(y)) := p_1(x) \cdot q_1(y) + \cdots + p_n(x) \cdot q_n(y)$ un morfismo de A-módulos bien definido? ¿Es f epiyectivo?

6. ¿Es $(M \otimes_A N) \otimes_A P$ isomorfo a $M \otimes_A N \otimes_A P$?

7. ¿Es $A^n \otimes_A A/I$ isomorfo a $(A/I)^n$?

8. ¿Es $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C}$ isomorfo a $\mathbb{C}[x]$?

9. Sea $A = \mathbb{Z}/3\mathbb{Z}$ y $M = A^3$ ¿Cuántos elementos tiene $M \otimes_A M$? ¿Es $M \otimes_A M = \{m \otimes m'\}_{m,m' \in M}$?

10. Calcular $(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z})$.

11. ¿Es $\mathbb{Q}[x]/(x^2+1) \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$?

12. ¿Es $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$? ¿Es $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$?

13. ¿Es $A_{\{1\}} = A$?

14. Sea $s \in A$ invertible y $S = \{1, s, s^2, \ldots, s^n, \ldots\}$ ¿Es $A_S = A$?

15. Sea A un anillo íntegro y $S \subset A \setminus \{0\}$ un sistema multiplicativo ¿Es el morfismo de localización $A \to A_S$ inyectivo?

16. Sean $\{\mathfrak{p}_i\}_{i \in I}$ el conjunto de los ideales primos minimales del anillo A ¿Es $\cap_{i \in I} \mathfrak{p}_i = \operatorname{rad} A$?

17. Descomponer $2x^2 + 8x + 6 \in \mathbb{Z}[x]$ en producto de irreducibles.

18. ¿Es $k[x,y]$ un dominio de ideales principales?

19. Si A es un dominio de ideales principales ¿Es $A[x]$ un dominio de factorización única? ¿Es $A[x]$ un dominio de ideales principales?

20. ¿Es $\mathbb{Z}[i][x]$ un dominio de factorización única?

2.7. Problemas

1. Probar que si M y N son A-módulos libres entonces $M \otimes_A N$ es un A-módulo libre. Probar que si $\{m_i\}_{i\in I}$ y $\{n_j\}_{j\in J}$ son bases de dos A-módulos libres M y N, probar que $\{m_i \otimes n_j\}_{(i,j)\in I\times J}$ es una base del A-módulo libre $M \otimes_A N$.

2. Sea $A \to B$ un morfismo de anillos. Probar que si $\{m_i\}_{i\in I}$ es un sistema de generadores de un A-módulo M, entonces $\{m_i \otimes 1\}_{i\in I}$ es un sistema de generadores del B-módulo $M \otimes_A B$. Además, si $\{e_i\}_{i\in I}$ es una base de un A-módulo libre L, probar que $\{e_i \otimes 1\}_{i\in I}$ es una base del B-módulo libre $L \otimes_A B$.

3. Si E es un k-espacio vectorial y L es una extensión de cuerpos de k, entonces $\dim_L(E \otimes_k L) = \dim_k E$.

4. Sea $\{e_1,\dots,e_n\}$ una base de un k-espacio vectorial E. Si $(x_1,\dots,x_n)$ son las coordenadas de un vector $e \in E$ en tal base, determinar las coordenadas de $e\otimes 1 \in E \otimes_k L$ en la base $\{e_1 \otimes 1,\dots,e_n \otimes 1\}$

5. Sea $f : E \to E'$ una aplicación lineal entre dos k-espacios vectoriales. Si $A = (a_{ij})$ es la matriz de f en sendas bases $\{e_1,\dots,e_n\}$ y $\{e'_1,\dots,e'_m\}$ de E y E', determinar la matriz de $f \otimes \mathrm{Id} : E \otimes_k L \to E' \otimes_k L$ en las bases $\{e_1\otimes 1,\dots,e_n\otimes 1\}$ y $\{e'_1\otimes 1,\dots,e'_m\otimes 1\}$.

6. Probar que si $0 \to M_1 \to M_2 \to M_3 \to 0$ es una sucesión exacta de A-módulos y N es un A-módulo libre, entonces

$$0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$$

   es una sucesión exacta de A-módulos.

7. Probar que si $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ es una sucesión exacta de A-módulos y N es un A-módulo, entonces

$$M_1 \otimes_A N \xrightarrow{f\otimes \mathrm{Id}} M_2 \otimes_A N \xrightarrow{g\otimes \mathrm{Id}} M_3 \otimes_A N \to 0$$

   es una sucesión exacta de A-módulos.

8. Sea E' un subespacio vectorial de un k-espacio vectorial E. Para todo k-espacio vectorial V, probar que $(E/E') \otimes_k V = (E \otimes_k V)/(E' \otimes_k V)$.

9. Sea $f : E' \to E$ una aplicación k-lineal, V un k-espacio vectorial y consideremos la aplicación lineal $f \otimes 1 : E' \otimes_k V \to E \otimes_k V$. Probar que $\mathrm{Im}(f \otimes \mathrm{Id}) = (\mathrm{Im}\, f) \otimes_k V$ y $\mathrm{Ker}(f \otimes \mathrm{Id}) = (\mathrm{Ker}\, f) \otimes_k V$.

10. Probar que $A/I \otimes_A A/J = A/(I + J)$.

11. Sean I y J dos ideales de un anillo A. Si $I + J = A$, demostrar que para todo A-módulo M, tenemos un isomorfismo natural $M/IJM = (M/IM) \oplus (M/JM)$.

12. Probar que $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$, donde $d = \mathrm{m.c.d.}(m,n)$.

13. Sea $A \to B$ un morfismo de anillos. Probar que $A[x_1,\ldots,x_n] \otimes_A B = B[x_1,\ldots,x_n]$.

14. Sea $A \to B$ un morfismo de anillos. Probar que

$$\big(A[x_1,\ldots,x_n]/(p_1,\ldots,p_r)\big) \otimes_A B \;=\; B[x_1,\ldots,x_n]/(p_1,\ldots,p_r)\;.$$

(los polinomios con coeficientes en A, vía el morfismo $A \to B$ los consideramos como polinomios con coeficientes en B)

15. Si E y F son k-espacios vectoriales y $\dim_k E < \infty$, probar que $\mathrm{Hom}_k(E,F) = E^* \otimes_k F$.

16. Sea E un k-espacio vectorial de dimensión finita. Si $T^q_p(E)$ denota el espacio vectorial de los tensores de tipo (p,q) sobre E, probar la existencia de un isomorfismo natural

$$T^q_p(E) = E^* \otimes_k \overset{p}{\cdots} \otimes_k E^* \otimes_k E \otimes_k \overset{q}{\cdots} \otimes_k E\;.$$

17. Probar que el núcleo del morfismo de localización $A \to A_S$ es el ideal

$$\{a \in A : sa = 0 \text{ para algún } s \in S\}.$$

18. Dar un ejemplo en el que el morfismo de localización $A \to A_S$ no sea inyectivo.

19. ¿Es cierto que el cuerpo de fracciones de $\mathbb{Z}[x]$ es isomorfo a $\mathbb{Q}(x)$?

Si $\alpha \in \mathbb{C}$, ¿es cierto que el cuerpo de fracciones de $\mathbb{Z}[\alpha]$ es isomorfo a $\mathbb{Q}(\alpha)$?

20. Sea M un A-módulo y $S \subset A$ un sistema multiplicativo. Probar que $M \otimes_A A_S = M_S$. Sea $f : A \to B$ un morfismo de anillos y denotemos $f(S) := \{f(s) \in B : s \in S\}$. Probar que $B_S = B_{f(S)}$.

21. Sean $S, S' \subset A$ dos sistemas multiplicativos, denotemos $S \cdot S' = \{ss' :\ s \in S, s' \in S'\}$. Probar que $(A_S)_{S'} = A_{S \cdot S'}$.

Capítulo 3

Raíces de un polinomio. Extensiones finitas de cuerpos

3.1. Introducción

Antes de hablar del cuerpo de los números racionales sumamos, restamos, multiplicamos y dividimos estos números y después somos conscientes de que estamos en un ámbito, $\mathbb{Q}$, donde estas operaciones son posibles y frecuentes. Cuando estamos considerando raíces $\alpha_1, \alpha_2, \alpha_3, \ldots$ de un polinomio, las afirmaciones como podrían ser "$\alpha_1 = \alpha_2^3 - 2\alpha_1 + 1/\alpha_3$" son posibles porque estamos en un ámbito, los cuerpos, donde las operaciones anteriores son posibles. Los cuerpos aparecen de modo natural en el estudio de las raíces de un polinomio.

Cuando a un estudiante de primaria se le habla de las raíces de un polinomio $p(x) \in \mathbb{Q}[x]$, se le habla de las raíces racionales (o enteras) de $p(x)$, a lo sumo de las raíces reales. Así, para un niño, $x^2 + 1$ no tiene raíces. Un estudiante del grado de matemáticas dirá que tiene raíces complejas y que todo polinomio $p(x)$ con coeficientes complejos descompone de modo único en producto de factores simples,

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n),\ \lambda, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$$

Es decir, dirá: "el cuerpo de los números complejos, $\mathbb{C}$, es un cuerpo algebraicamente cerrado" (teorema que probaremos).

Si consideramos cualquier otro cuerpo, k (por ejemplo, $k = \mathbb{Z}/3\mathbb{Z}$), existe un único cuerpo (salvo isomorfismos), $\bar{k}$, mínimo conteniendo a k de modo que todo polinomio $p(x)$ con coeficientes en k (y $\bar{k}$) descompone en producto de factores simples

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n),\ \lambda, \alpha_1, \ldots, \alpha_n \in \bar{k}$$

Además, para cada $\alpha \in \bar{k}$ existe un polinomio $p(x) \in k[x]$ tal que $p(\alpha) = 0$.

Podemos decir que $\bar{k}$ es el conjunto (cuerpo) de todas las raíces de todos los polinomios $p(x) \in k[x]$. Los niños no entienden qué son las raíces imaginarias de $p(x) \in \mathbb{Q}[x]$. Nadie les ha definido ni construido $\mathbb{C}$ (ni $\bar{\mathbb{Q}}$). Nosotros tenemos la tarea de definir-construir $\bar{k}$.

3.2. Extensiones de cuerpos. Elementos algebraicos

1. Definición: Una extensión de cuerpos es un morfismo de anillos $k \to K$, donde k y K son cuerpos. También se dice que K es una extensión de cuerpos de k o que K es una k-extensión de cuerpos.

Obsérvese que todo morfismo de anillos $k \to K$, entre cuerpos, es inyectivo pues el núcleo es un ideal, que ha de ser el ideal (0) y no el ideal $k = (1)$, porque el elemento unidad de k se aplica en el elemento unidad de K.

2. Definición: Diremos que una extensión de cuerpos $k \hookrightarrow K$ es una extensión finita de cuerpos si K es un k-espacio vectorial de dimensión finita. Llamaremos grado de K sobre k a $\dim_k K$.

3. Ejemplo: La inclusión $\mathbb{R} \subset \mathbb{C}$ es una extensión finita de cuerpos de grado 2.

4. Proposición: *La k-álgebra $k[x]/(x^n + a_1x^{n-1} + \ldots + a_n)$ es un k-espacio vectorial de base $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$.*

Demostración. Sea $q(x) = x^n + a_1x^{n-1} + \ldots + a_n$. Dado un polinomio $p(x)$ existen dos polinomios únicos $c(x)$ y $r(x)$, de modo que $p(x) = c(x) \cdot q(x) + r(x)$ y que $\operatorname{gr} r(x) < \operatorname{gr} q(x)$. Por lo tanto, existe un único polinomio $r(x)$ de grado menor que n de modo que $\overline{r(x)} = \overline{p(x)}$ en $k[x]/(q(x))$.

Es decir, la aplicación lineal $k \oplus k \cdot x \oplus \cdots \oplus k \cdot x^{n-1} \to k[x]/(q(x))$, $r(x) \mapsto \overline{r(x)}$ es un isomorfismo.

□

Sea $k \hookrightarrow K$ una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in K$. Denotamos $k(\alpha_1, \ldots, \alpha_n)$ a la mínima k-subextensión de K que contiene a $\alpha_1, \ldots, \alpha_n$. Explícitamente,

$$k(\alpha_1, \ldots, \alpha_n) = \{\frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} \in K : p(x_1, \ldots, x_n), q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \text{ y } q(\alpha_1, \ldots, \alpha_n) \neq 0\}$$

5. Definición: Dado una extensión de cuerpos $k \hookrightarrow K$. Diremos que $\alpha \in K$ es algebraica sobre k si existe un polinomio $0 \neq p(x) \in k[x]$ tal que $p(\alpha) = 0$.

6. Ejemplos: $\sqrt{2} \in \mathbb{R}$ es un elemento $\mathbb{Q}$-algebraico, porque es raíz de $x^2 - 2 \in \mathbb{Q}[x]$. El número $\pi \in \mathbb{R}$ no es $\mathbb{Q}$-algebraico, como probó Lindemann en 1882. El número $e \in \mathbb{R}$ no es $\mathbb{Q}$-algebraico, como probó Hermite en 1873.

Si $\alpha \in K$ es algebraica entonces

$$\boxed{k(\alpha) = k[x]/(p(x))},$$

donde $p(x)$ es el polinomio mónico con coeficientes en k de grado mínimo que anula a α. En efecto, el núcleo del morfismo $\phi\colon k[x] \to K$, $\phi(q(x)) := q(\alpha)$ es el ideal formado por todos los polinomios que anulan a α y este ideal está generado por el polinomio $p(x)$ (que podemos suponer mónico) de grado mínimo que anula a α. Además, $p(x)$ ha de ser irreducible, luego $k[x]/(p(x))$ es un cuerpo. Por tanto, $\operatorname{Im}\phi \simeq k[x]/(p(x)$ es un cuerpo y ha de coincidir con $k(\alpha)$. Es decir, $k(\alpha) = k[x]/(p(x))$.

7. Observación: Si $\alpha \in K$ es k-algebraica observemos que $k(\alpha) = \{q(\alpha) \in K, q(x) \in k[x]\} =: k[\alpha]$.

8. Proposición: *Sea $k \hookrightarrow K$ una extensión de cuerpos y $\alpha \in K$. Entonces, α es algebraica sobre k, si y sólo si* $\dim_k k(\alpha) < \infty$.

Demostración. Si α es algebraica y $p(x)$ es el polinomio mínimo anulador de α, entonces $\dim_k k(\alpha) = \operatorname{gr} p(x) < \infty$ (véase 3.2.4). Recíprocamente, si $\dim_k k(\alpha) = n < \infty$ entonces $1, \alpha, \ldots, \alpha^n$ son k-linealmente dependientes, luego existe un polinomio de grado n que anula a α. □

9. Ejemplo: Sea $\sqrt{2} \in \mathbb{C}$, entonces $\mathbb{Q}[\sqrt[2]{2}] \subseteq \mathbb{C}$ es una $\mathbb{Q}$-extensión finita de cuerpos de grado 2, porque $\mathbb{Q}[\sqrt[2]{2}] = \mathbb{Q}[x]/(x^2 - 2)$.

10. Proposición: *Si $k \to K$ es una extensión finita de cuerpos de grado n y $K \to \Sigma$ es una extensión finita de grado m, entonces $k \to \Sigma$ es una extensión finita de grado $n \cdot m$. En particular, la composición de extensiones finitas es una extensión finita.*

Demostración. Se tienen igualdades de espacios vectoriales $\Sigma = K \oplus \overset{m}{\ldots} \oplus K$, y $K = k \oplus \overset{n}{\ldots} \oplus k$, luego $\Sigma = k \oplus \overset{n \cdot m}{\ldots} \oplus k$ y se concluye. □

Si $\alpha_1, \ldots, \alpha_n \in K$ son elementos k-algebraicos entonces $k(\alpha_1, \ldots, \alpha_n)$ es un extensión finita de k, porque es composición de las extensiones finitas de cuerpos $k \hookrightarrow k(\alpha_1) \hookrightarrow k(\alpha_1, \alpha_2) \hookrightarrow \cdots \hookrightarrow k(\alpha_1, \ldots, \alpha_n)$. En particular, dado $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, entonces $p(\alpha_1, \ldots, \alpha_n) \in k(\alpha_1, \ldots, \alpha_n)$ es k-algebraico.

11. Definición: Se dice que una extensión de cuerpos $k \hookrightarrow K$ es algebraica si todos los elementos de K son algebraicos sobre k.

12. Proposición: *Si $k \hookrightarrow K$ y $K \hookrightarrow K'$ son extensiones algebraicas entonces $k \hookrightarrow K'$ es algebraica.*

Demostración. Dado $\alpha \in K'$, existe un polinomio $p(x) = \sum_i a_i x^i \in K[x]$ tal que $p(\alpha) = 0$. La extensión $k \hookrightarrow k(a_1, \ldots, a_n, \alpha)$ es finita, luego $k \hookrightarrow k(\alpha)$ también y α es algebraica sobre k. □

3.3. Teorema de Kronecker. Cierre algebraico

1. Proposición: *Sean $k \hookrightarrow K$ y $k \hookrightarrow K'$ dos extensiones de cuerpos. Entonces, existe una k-extensión de cuerpos L, de modo que tenemos morfismos de k-extensiones $K \hookrightarrow L$ y $K' \hookrightarrow L$.*

Demostración. Sea $\mathfrak{m}$ un ideal maximal de $K \otimes_k K'$ y sea $L := (K \otimes_k K')/\mathfrak{m}$. L es una k-extensión de cuerpos y tenemos los morfismos naturales de k-extensiones de cuerpos $K \to (K \otimes_k K')/\mathfrak{m}$, $\lambda \mapsto \overline{\lambda \otimes 1}$, $K' \to (K \otimes_k K')/\mathfrak{m}$, $\lambda' \mapsto \overline{1 \otimes \lambda'}$. □

2. Definición: Sea L una k-extensión de cuerpos $K, K' \hookrightarrow L$ dos k-subextensiones Denotaremos $K \cdot K'$ y diremos que es el compuesto de K y K' en L, al mínimo subcuerpo de L que contiene a K y K'.

3. Teorema de Kronecker: *Sea $p(x) \in k[x]$ un polinomio de grado $n > 0$. Existe una extensión finita K de k en la que $p(x)$ descompone en factores simples, es decir, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que*

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n), \qquad \lambda \in k$$

Si K' es otra extensión de cuerpos k y existen elementos $\beta_1, \ldots, \beta_n \in K'$ tales que $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$, entonces en toda k-extensión L que contenga a K y K' se tiene que $\alpha_i = \beta_i$, para todo i (reordenando las β_i si es necesario). Se dice que $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$.

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x - \alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K_1 = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K_1[x]$ tenemos que $p(x) = (x - \alpha_1) \cdot p_2(x)$. Por hipótesis de inducción, existe una extensión finita $K_1 \hookrightarrow K$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Luego en K, que es una extensión finita de k,

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n)$$

Si $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$ (en L), como $0 = p(\alpha_1) = \lambda \cdot (\alpha_1 - \beta_1) \cdots (\alpha_1 - \beta_n)$, reordenando las β_i, podemos suponer que $\beta_1 = \alpha_1$. Dividiendo por $x - \alpha_1$, tendremos que $\lambda \cdot (x - \beta_2) \cdots (x - \beta_n) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Por inducción sobre n, reordenado $\beta_2, \ldots, \beta_n$, tendremos que $\beta_i = \alpha_i$, para todo $i \geq 2$.

□

4. Definición: Diremos que un cuerpo $\bar{k}$ es algebraicamente cerrado si no admite extensiones de cuerpos finitas (o algebraicas), es decir, todo polinomio con coeficientes en $\bar{k}$ tiene todas sus raíces en $\bar{k}$.

5. Teorema: *Dado un cuerpo k, existe una única extensión de cuerpos $k \hookrightarrow \bar{k}$, salvo isomorfismos, que es algebraica y tal que $\bar{k}$ es algebraicamente cerrado. Diremos que $\bar{k}$ es el cierre algebraico de k.*

Demostración. Sea P el conjunto de polinomios irreducibles de $k[x]$. Para cada $p \in P$ sea por Kronecker K_p un cuerpo que contenga a todas las raíces del polinomio p. Para cada subconjunto finito $\{p_1, \ldots, p_n\}$ de P consideremos la k-álgebra $K_{p_1} \otimes \ldots \otimes K_{p_n}$, y para cada inclusión $\{p_1, \ldots, p_n\} \subseteq \{p_1, \ldots, p_n, \ldots, p_m\}$ consideremos el morfismo obvio $K_{p_1} \otimes \ldots \otimes K_{p_n} \to K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m}$. Identifiquemos $K_{p_1} \otimes \ldots \otimes K_{p_n}$ con su imagen en cada $K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m}$ y sea

$$A := \bigcup_{\{p_1, \ldots, p_n\}} K_{p_1} \otimes \ldots \otimes K_{p_n}$$

Sea $\bar{k}$ el cociente de A por cualquier ideal maximal. Obviamente, $\bar{k}$ es una extensión algebraica de k, pues está generado algebraicamente por las imágenes de las extensiones K_p. Sea $\bar{k} \hookrightarrow K$ una extensión algebraica de cuerpos y $\alpha \in K$. K es una extensión algebraica de k, así pues α es algebraica sobre k. Sea $p = p(x) \in k[x]$ el polinomio mínimo anulador de α. K_p contiene todas las raíces de $p(x)$, luego $\bar{k}$ también, $\alpha \in \bar{k}$ y $K = \bar{k}$.

Si k' es una extensión algebraica de k, entonces $(\bar{k} \otimes_k k')/\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal, es una extensión algebraica de $\bar{k}$ y k'. Por tanto, $(\bar{k} \otimes_k k')/\mathfrak{m} = \bar{k}$ y ésta contiene a k'. Si k' es algebraicamente cerrado entonces $\bar{k} = k'$.

□

3.4. Teorema de las funciones simétricas

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = c(x-\alpha_1)\cdots(x-\alpha_n)$. Desarrollando el último término e igualando coeficientes de los x^i se obtiene las fórmulas de Cardano:

$$\begin{aligned} a_0 &= c \\ a_1 &= -c\cdot(\alpha_1 + \cdots + \alpha_n) \\ &\cdots \\ a_i &= (-1)^i c \cdot \sum_{1\le j_1<\cdots<j_i\le n} \alpha_{j_1}\cdots\alpha_{j_i} \\ &\cdots \\ a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n \end{aligned}$$

1. Definición: Llamaremos *funciones simétricas elementales* (o polinomios simétricos elementales) en las letras $x_1,\ldots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\ldots,x_n]$ $(i = 1,\ldots,n)$ definidos por:

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ &\cdots \\ s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\ &\cdots \\ s_n &= x_1\cdots x_n \end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

Sea S_n el grupo de las permutaciones de n letras. Consideremos la operación de S_n en $A[x_1,\ldots x_n]$ siguiente:

$$\sigma(P(x_1,\ldots,x_n)) := P(x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

para cada $\sigma \in S_n, P(x_1,\ldots,x_n) \in A[x_1,\ldots x_n]$.

2. Definición: Diremos que un polinomio $P(x_1,\ldots,x_n) \in A[x_1,\ldots x_n]$ es simétrico cuando $\sigma(P) = P$ para toda $\sigma \in S_n$. Al conjunto de las funciones simétricas las denotaremos $A[x_1,\ldots x_n]^{S_n}$.

3. Teorema de las funciones simétricas: *Se verifica la igualdad:*

$$A[x_1,\ldots,x_n]^{S_n} = A[s_1,\ldots,s_n]$$

Es decir, un polinomio en $x_1,\dots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y sólo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Procedemos por inducción sobre el número n de variables. Para $n = 1$ es trivial. Sea $P(x_1,\dots,x_n) \in A[x_1,\dots,x_n]^{S_n}$. Descomponiendo P en la suma de sus componentes homogéneas, podemos suponer que P es homogéneo de grado m. Haciendo cociente por x_n se obtiene que $P(x_1,\dots,x_{n-1},0)$ es un polinomio homogéneo de grado m en $n-1$ variables e invariante por las permutaciones de éstas, luego $P(x_1,\dots,x_{n-1},0) = Q'(s'_1,\dots,s'_{n-1})$, siendo s'_i la i-ésima función simétrica en las $n-1$ primeras variables. Observemos que en $Q'(s'_1,\dots,s'_{n-1})$ cada sumando $\lambda_{(m_1,\dots,m_{n-1})} {s'}_1^{m_1}\cdots {s'}_{n-1}^{m_{n-1}}$ es un polinomio homogéneo en $x_1,\dots,x_{n-1}$ de grado $m_1+2m_2+\cdots+(n-1)m_{n-1}$. Podemos suponer que $\lambda_{(m_1,\dots,m_{n-1})} = 0$, cuando $m_1+2m_2+\cdots+(n-1)m_{n-1} \neq m$. Por tanto, $Q'(s_1,\dots,s_{n-1})$ es un polinomio en $x_1,\dots,x_n$ homogéneo de grado m. Sea $H(x_1,\dots,x_n) = P(x_1,\dots,x_n) - Q'(s_1,\dots,s_{n-1})$. Se verifica que H es simétrico y homogéneo de grado m y se anula para $x_n = 0$ (ya que $s_i = s'_i \, mod \, x_n$), luego es múltiplo de x_n y por ser simétrico es múltiplo de $x_1\cdots x_n = s_n$, es decir, $H(x_1,\dots,x_n) = s_n \cdot H'(x_1,\dots,x_n)$ y, por tanto, $H'(x_1,\dots,x_n)$ es simétrico también y homogéneo de grado $gr(H') = gr(H) - n = gr(P) - n < gr(P)$, luego por recurrencia sobre el grado m de P se concluye que $H'(x_1,\dots,x_n) = \widetilde{Q}(s_1,\dots,s_n)$. Sustituyendo en la definición de H y despejando se obtiene:

$$P(x_1,\dots x_n) = Q'(s_1,\dots,s_{n-1}) + s_n \cdot \widetilde{Q}(s_1,\dots,s_n)$$

con lo que se concluye. □

3.5. Aplicaciones

3.5.1. Teorema Fundamental del Álgebra

1. Teorema fundamental del Álgebra: *El cuerpo de los números complejos es un cuerpo algebraicamente cerrado.*

Demostración. Dado un polinomio cualquiera, $0 \neq p(x) \in \mathbb{C}[x]$, tenemos que probar que tiene una raíz en $\mathbb{C}$. Basta probar que todo polinomio con coeficientes reales tiene una raíz compleja, porque el producto de $p(x)$ por su conjugado, $q(x) = p(x)\cdot\overline{p(x)}$ es un polinomio con coeficientes reales y si α es una raíz de $q(x)$, entonces α o su conjugada es una raíz de $p(x)$. Si $q(x) \in \mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} q(x) = -\lim_{x\to-\infty} q(x), \quad (\text{y } |\lim_{x\to+\infty} q(x)| = +\infty)$$

Luego por el teorema de Bolzano existe un $\alpha \in \mathbb{R}$ tal que $q(\alpha) = 0$. Supongamos que $\text{gr}\, q(x) = r = 2^n \cdot m$, con m impar. Para probar que $q(x)$ tiene una raíz compleja procedamos por inducción sobre n. Para $n = 0$ lo hemos probado. Supongamos $n > 0$.

Sean $\alpha_1,\dots,\alpha_r$ las raíces de $q(x)$ y fijado $\lambda\in\mathbb{R}$ sean $\beta_{ij}:=\alpha_i+\alpha_j+\lambda\alpha_i\cdot\alpha_j$. El polinomio $h(x):=\prod_{i<j}(x-\beta_{ij})\in\mathbb{R}[x]$, porque los coeficientes de $h(x)$ son funciones simétricas en $\alpha_1,\dots,\alpha_n$, luego por el teorema de las funciones simétricas, los coeficientes de $h(x)$ son polinomios en los coeficientes de $q(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2}=2^{n-1}\cdot m\cdot(r-1)=2^{n-1}\cdot m'$ con m' impar. Por inducción sobre n, cierto $\beta_{rs}=\alpha_r+\alpha_s+\lambda\alpha_r\cdot\alpha_s\in\mathbb{C}$. Variando el λ fijado (tómese $\binom{r}{2}+1$ distintos), existirán $\lambda\neq\lambda'$, para los que existen r,s, de modo que

$$\alpha_r+\alpha_s+\lambda\alpha_r\cdot\alpha_s,\ \alpha_r+\alpha_s+\lambda'\alpha_r\cdot\alpha_s\in\mathbb{C}.$$

Luego $a:=\alpha_r+\alpha_s$ y $b:=\alpha_r\cdot\alpha_s\in\mathbb{C}$. Como α_r y α_s son las raíces de $(x-\alpha_r)(x-\alpha_s)=x^2-ax+b$, tenemos que $\alpha_r,\alpha_s=(a\pm\sqrt{a^2-4b})/2\in\mathbb{C}$. □

3.5.2. Fórmulas de Newton y Girard

Sea $k[[t]]=\{a_0+a_1t+\cdots+a_nt^n+\cdots,\ a_i\in k\}$ el "anillo de series formales en t con coeficientes en k". Dadas dos series, $s_1(t)=\sum_{i=0}^{\infty}a_it^i$, $s_2(t)=\sum_{i=0}^{\infty}b_it^i$, se define

$$\begin{array}{lcl} s_1(t)+s_2(t) & := & \sum_{i=0}^{\infty}(a_i+b_i)t^i \\ s_1(t)\cdot s_2(t) & := & \sum_{i=0}^{\infty}(\sum_{j=0}^{i}a_j\cdot b_{i-j})t^i \end{array}$$

y resulta que $k[[t]]$ es un anillo íntegro. Es fácil ver que $s(t)=\sum_{i=0}^{\infty}a_it^i$ es invertible si y sólo si $a_0\neq0$. Por tanto, si $s(t)=\sum_{i=m}^{\infty}a_it^i$, con $a_m\neq0$, entonces $s(t)=t^m\cdot\tilde{s}(t)$, con $\tilde{s}(t)$ invertible. Luego,

$$\begin{aligned} k((t)):=k[[t]]_{k[[t]]\setminus\{0\}} &= \{s(t)/t^m,\ m\in\mathbb{N},s(t)\in k[[t]]\} \\ &= \{\frac{b_m}{t^m}+\cdots+\frac{b_1}{t}+a_0+a_1t+\cdots+a_nt^n+\cdots,m\in\mathbb{N},b_j,a_i\in k\} \end{aligned}$$

Sea $P(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n=a_0(x-\alpha_1)\cdots(x-\alpha_n)\in k[x]$.

2. Teorema: *Sea $P'(x)$ la derivada de $P(x)$ y $\sigma_i=\alpha_1^i+\cdots+\alpha_n^i$ las potencias simétricas en las raíces de $P(x)$. Se verifica:*

1. $\frac{P'(x)}{P(x)}=\frac{1}{x-\alpha_1}+\cdots+\frac{1}{x-\alpha_n}$.

2. *Fórmula de Girard:*

$$\frac{P'(x)}{P(x)}=\frac{\sigma_0}{x}+\frac{\sigma_1}{x^2}+\cdots+\frac{\sigma_i}{x^{i+1}}+\cdots\in k((\frac{1}{x}))$$

3. Fórmulas de Newton:

$$\begin{aligned}
0 &= a_1 + \sigma_1 a_0 \\
0 &= 2a_2 + \sigma_1 a_1 + a_0 \sigma_2 \\
0 &= 3a_3 + \sigma_1 a_2 + \sigma_2 a_1 + \sigma_3 a_3 \\
&\cdots \\
0 &= n a_n + a_{n-1}\sigma_1 + \cdots + a_0 \sigma_n \\
&\text{———————} \\
0 &= a_n \sigma_1 + \cdots + a_0 \sigma_{n+1} \\
&\cdots \\
0 &= a_n \sigma_i + \cdots + a_0 \sigma_{n+i} \\
&\cdots
\end{aligned}$$

Demostración. 1. $P'(x) = \sum_i a_0(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)$, luego

$$P'(x)/P(x) = (\sum_i a_0(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n))/(a_0(x-\alpha_1)\cdots(x-\alpha_n)) = \sum_i 1/(x-\alpha_i)$$

2. Sustituyendo $\frac{1}{x-\alpha_i} = \frac{1}{x}\frac{1}{1-\frac{\alpha_i}{x}} = \frac{1}{x}\sum_j (\frac{\alpha_i}{x})^j$ en la identidad anterior y agrupando en las potencias de $\frac{1}{x}$ se concluye.

3. Resulta de igualar coeficientes en las potencias de x en la identidad $P'(x) = P(x)\cdot\sum_i \frac{\sigma_i}{x^{i+1}}$.

□

3.5.3. Raíces múltiples. Discriminante de un polinomio

Sea $p(x) \in k[x]$ y K una k-extensión que contenga todas las raíces de $p(x)$. Agrupando los factores simples con la misma raíz, tenemos (en $K[x]$) que

$$p(x) = \lambda\cdot(x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}, \quad \text{con } \alpha_i \neq \alpha_j \text{ para todo } i \neq j$$

Si $n_i > 1$, se dice que α_i es una raíz múltiple de $p(x)$ de multiplicidad n_i.

3. Proposición: *Sea $p(x) \in k[x]$ un polinomio no nulo y K una extensión de cuerpos de k. Entonces, $\alpha \in K$ es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$ (la derivada "formal" de $p(x)$).*

Demostración. Tenemos que α es una raíz de $p(x)$, entonces $p(x) = (x-\alpha)\cdot q(x)$ (en $K[x]$) y $p'(x) = q(x) + (x-\alpha)\cdot q'(x)$. Por tanto, α es una raíz de $p'(x)$ si y sólo si es raíz de $q(x)$, es decir, si y sólo si α es una raíz múltiple de $p(x)$. □

El máximo común divisor de dos polinomios se puede calcular mediante el algoritmo de Euclides, por tanto, no cambia si hacemos un cambio de cuerpo base. Consideremos una k-extensión de cuerpos K donde $p(x)$ y $q(x)$ descompongan es factores simples, podemos escribir $p(x) = \lambda\cdot(x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}$ y $q(x) = \mu\cdot(x-\alpha_1)^{m_1}\cdots(x-\alpha_r)^{m_r}$, con $n_i, m_i \geq 0$ y $\alpha_i \neq \alpha_j$, para todo $i \neq j$. Entonces

$$m.c.d(p(x), q(x)) = (x-\alpha_1)^{min(n_1,m_1)}\cdots(x-\alpha)^{min(n_r,m_r)} \in k[x]$$

Los polinomios $p(x)$ y $q(x)$ son primos entre sí si y sólo si no tienen raíces comunes (estamos considerando todas las raíces de $p(x)$ y $q(x)$ en K).

Un polinomio $p(x)$ no tiene raíces múltiples si y sólo si $p(x)$ y $p'(x)$ son primos entre sí.

4. Definición: Sea $p(x) = x^n + a_1x^{n-1} + \cdots + a_n = (x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$ un polinomio. Llamaremos discriminante de $p(x)$, que denotaremos $\Delta(p(x))$, a

$$\Delta(p(x)) := \prod_{i<j}(\alpha_i - \alpha_j)^2$$

Observemos que $\Delta(p(x))$ es una función simétrica de las raíces $\alpha_1,\ldots,\alpha_n$, luego por el teorema de las funciones simétricas es un polinomio en $a_1,\ldots,a_n$, luego pertenece a k.

Observemos que $\Delta(p(x)) = 0$ si y sólo si $p(x)$ tiene raíces múltiples.

5. Teorema: *Sea $p(x) = x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$ un polinomio. El discriminante de $p(x)$ es igual a*

$$\Delta(p(x)) = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

Demostración. Sea el determinante de Vandermonde

$$V(x_1,\ldots,x_n) = \begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

Si hacemos $x_i = x_j$ (es decir, $x_i - x_j = 0$), este determinante se anula, luego V es múltiplo de $\prod_{i<j}(x_i - x_j)$. V es un polinomio homogéneo de grado $n\cdot(n-1)/2$. Además el coeficiente que acompaña a $x_1^0 \cdot x_2^1 \cdots x_n^{n-1}$ es igual a 1. $\prod_{i<j}(x_i - x_j)$ es homogéneo de grado $n\cdot(n-1)/2$ y el coeficiente que acompaña a $x_1^0 \cdot x_2^1 \cdots x_n^{n-1}$ es igual a ± 1. Luego, $V = \pm\prod_{i<j}(x_i - x_j)$. Por tanto, $V^2 = \Delta(p(x))$. Ahora bien

$$V^2 = \left| \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} \circ \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_1 & \cdots & x_1^{n-1} \end{pmatrix} \right| = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ \sigma_{n-1} & \sigma_n & \cdots & \sigma_{2(n-1)} \end{vmatrix}$$

□

6. Corolario: *El discriminante de $x^2 + a_1x + a_2$ es $a_1^2 - 4a_2$.*

Demostración. Por la fórmula de Girard, $\sum_i \sigma_i/x^{i+1} = (2x + a_1)/(x^2 + a_1x + a_2) = 2/x - a_1/x^2 + (-2a_2 + a_1^2)/x^3 + \cdots$. Luego,

$$\Delta(x^2 + a_1x + a_2) = \begin{vmatrix} 2 & -a_1 \\ -a_1 & -2a_2 + a_1^2 \end{vmatrix} = a_1^2 - 4a_2$$

□

7. Corolario: *El discriminante de* $x^3+a_1x^2+a_2x+a_3$ *es* $-4a_1^3+a_1^2a_2^2+18a_1a_2a_3-4a_2^3-27a_3^2$.

Demostración. $\sum_i \sigma_i/x^{i+1} = (3x^2+2a_1x+a_2)/(x^3+a_1x^2+a_2x+a_3) = 3/x-a_1/x^2+(a_1^2-3a_2)/x^3+(-a_1^3+3a_1a_2-3a_3)/x^4+(a_1^4-4a_1^2a_2+4a_1a_3+2a_2^2)/x^5+\cdots$. Luego,

$$\begin{aligned}\Delta(x^3+a_1x^2+a_2x+a_3) &= \begin{vmatrix} 3 & -a_1 & a_1^2-2a_2 \\ -a_1 & a_1^2-2a_2 & -a_1^3+3a_1a_2-3a_3 \\ a_1^2-2a_2 & -a_1^3+3a_1a_2-3a_3 & a_1^4-4a_1^2a_2+4a_1a_3+2a_2^2 \end{vmatrix} \\ &= -4a_1^3a_3+a_1^2a_2^2+18a_2a_1a_3-4a_2^3-27a_3^2\end{aligned}$$

□

3.6. k-álgebras finitas.

Ni el producto directo de extensiones finitas de cuerpos, ni (en general) el producto tensorial de extensiones finitas de cuerpos es un cuerpo. Por ello, el marco de las extensiones finitas de cuerpos es excesivamente estrecho y es necesario introducir el concepto de k-álgebra finita.

1. Definición: Diremos que una k-álgebra A, es una k-álgebra finita, si A es un k-espacio vectorial de dimensión finita.

2. Ejemplo: Las k-extensiones finitas de cuerpos son k-álgebras finitas.

3. Ejemplo: $A=k[x]/(x^n+a_1x^{n-1}+\ldots+a_n)$ es una k-álgebra finita de base $\{1,\bar{x},\ldots,\bar{x}^{n-1}\}$, por la proposición 3.2.4.

4. Proposición: *Toda k-álgebra finita e íntegra es cuerpo.*

Demostración. Sea A una k-álgebras finita íntegra. Dado $a\in A$ no nula, la homotecia $A\xrightarrow{\cdot a} A, b\mapsto b\cdot a$ es inyectiva, por ser A íntegra. Por tanto, por dimensiones, es isomorfismo. Luego a es invertible y A es cuerpo. □

5. Proposición: *El espectro primo de una k-álgebra finita A es un número finito de ideales maximales. Además,*

$$\#\operatorname{Spec} A \le \dim_k A$$

Demostración. Si hacemos cociente por un ideal primo obtenemos una k-álgebra finita íntegra, luego es un cuerpo por la proposición anterior. Por tanto, todos los ideales primos son maximales.

Sean $\{\mathfrak{m}_1,\ldots,\mathfrak{m}_n\}$ ideales maximales distintos de A. Como $(\mathfrak{m}_1+(\mathfrak{m}_2\cdots\mathfrak{m}_n))_0=(\mathfrak{m}_1)_0\cap(\mathfrak{m}_2\cdots\mathfrak{m}_n)_0=\{\mathfrak{m}_1\}\cap\{\mathfrak{m}_2,\ldots,\mathfrak{m}_n\}=\emptyset$, entonces $\mathfrak{m}_1+(\mathfrak{m}_2\cdots\mathfrak{m}_n)=A$. Por el teorema chino de los restos $A/(\mathfrak{m}_1\cdots\mathfrak{m}_n)=A/\mathfrak{m}_1\times A/(\mathfrak{m}_2\cdots\mathfrak{m}_n)=\cdots=A/\mathfrak{m}_1\times\cdots\times A/\mathfrak{m}_n$, luego

$$\dim_k A\ge\dim_k A/(\mathfrak{m}_1\cdots\mathfrak{m}_n)=\sum_{i=1}^{n}\dim_k A/\mathfrak{m}_i\ge n$$

Luego, $\dim_k A\ge\#\operatorname{Spec} A$.

□

6. Definición: Se dice que un anillo es local cuando sólo contiene un único ideal maximal.

Sea $p(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r} \in k[x]$ la descomposición en factores irreducibles distintos. Por el teorema chino de los restos

$$k[x]/(p(x)) = k[x]/(p_1(x)^{n_1}) \times \overset{r}{\cdots} \times k[x]/(p_r(x)^{n_r})$$

$k[x]/(p_1(x)^{n_1})$ es una k-álgebra finita <u>local</u>, porque $\operatorname{Spec} k[x]/(p_1(x)^{n_1}) = (p_1(x)^{n_1})_0 = (p_1(x))_0 = \{(p_1(x))\}$.

7. Proposición: *Toda k-álgebra finita es un producto cartesiano de un número finito de k-álgebras finitas locales.*

Demostración. $\operatorname{Spec} A = \{x_1, \ldots, x_n\}$, donde los ideales primos $\mathfrak{p}_{x_i}$ son maximales. Veamos que el morfismo

$$A \to A_{x_1} \times \cdots \times A_{x_n},\ a \mapsto (a/1, \ldots, a/1),$$

es un isomorfismo. Observemos que si $x_i \neq x_j$, entonces $(A_{x_i})_{x_j} = 0$, porque $\operatorname{Spec}(A_{x_i})_{x_j} = \emptyset$ ya que se corresponde con los ideales primos de A que están contenidos en $\mathfrak{p}_{x_i}$ y $\mathfrak{p}_{x_j}$. Por otra parte, $(A_{x_i})_{x_i} = A_{x_i}$. Por lo tanto, $A \to A_{x_1} \times \cdots \times A_{x_n}$ es isomorfismo porque es isomorfismo al localizar en todo punto x_i. □

Veamos cómo son los ideales primos de un producto cartesiano de anillos.

Sea $A = A_1 \times \cdots \times A_n$ un producto cartesiano de anillos. Denotemos

$$1_i := (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0) \in A.$$

Dado un ideal $I \subseteq A$ y $a = (a_1, \ldots, a_n) \in I$ observemos que $a \cdot 1_i \in I$ y que $a = \sum_i a \cdot 1_i$, por tanto $I = I \cdot 1_1 \oplus \cdots \oplus I \cdot 1_n$. Si denotamos por $I_i = \{a_i \in A_i : (0, \ldots, 0, \overset{i}{a_i}, 0, \ldots, 0) \in I\}$, tenemos que $I = I_1 \times \cdots \times I_n$. Además,

$$A/I = (A_1 \times \cdots \times A_n)/(I_1 \times \cdots \times I_n) = A_1/I_1 \times \cdots \times A_n/I_n$$

El producto directo de dos anillos no nulos $A_1 \times A_2$ nunca es un anillo íntegro pues $(1,0) \cdot (0,1) = (0,0)$. Si $\mathfrak{p} = I_1 \times \cdots \times I_n$ es un ideal primo de $A = A_1 \times \cdots \times A_n$, entonces como $A/\mathfrak{p} = A_1/I_1 \times \cdots \times A_n/I_n$ es un anillo íntegro, se ha de cumplir que $\mathfrak{p} = A_1 \times \cdots \times A_{i-1} \times \mathfrak{p}_i \times A_{i+1} \times \cdots \times A_n$, con $\mathfrak{p}_i \subseteq A_i$ ideal primo, y recíprocamente todo ideal de esta forma es un ideal primo de A. En conclusión,

$$\begin{array}{rcl} \operatorname{Spec}(A_1 \times \cdots \times A_n) & = & \operatorname{Spec} A_1 \coprod \cdots \coprod \operatorname{Spec} A_i \coprod \cdots \coprod \operatorname{Spec} A_n \\ A_1 \times \cdots \times A_{i-1} \times \mathfrak{p}_i \times A_{i+1} \times \cdots \times A_n & \longmapsto & \mathfrak{p}_i \end{array}$$

Observemos, además, que $\boxed{A/\mathfrak{p} = A_i/\mathfrak{p}_i}$. Si $A = A_1 \times \cdots \times A_n$ es un producto directo de n álgebras locales entonces A contiene exactamente n ideales maximales. Por tanto, toda k-álgebra finita A descompone en producto directo de exactamente $\#\operatorname{Spec} A$ álgebras finitas locales.

Si un anillo es producto cartesiano de anillos, $A = A_1 \times \cdots \times A_n$, entonces es fácil comprobar que $\mathrm{rad}(A) = \mathrm{rad}(A_1) \times \cdots \times \mathrm{rad}(A_n)$. Por lo tanto, A es reducido si y sólo si $A_1, \ldots, A_n$ es reducido.

Las k-álgebras finitas locales sólo tienen un ideal primo que ha de coincidir con el radical de la k-álgebra finita. Si A es una k-álgebra finita local reducida, entonces sólo tiene un ideal primo y éste es igual al ideal cero, luego A es un cuerpo.

8. Proposición: *Sea A una k-álgebra finita. Entonces, A es reducida si y sólo si es producto cartesiano de cuerpos.*

Demostración. Si $A = K_1 \times \cdots \times K_n$ es producto cartesiano de cuerpos, entonces $\mathrm{rad}(A) = \mathrm{rad}(K_1) \times \cdots \times \mathrm{rad}(K_n) = 0 \times \cdots \times 0 = 0$ y A es reducida.

Supongamos que A es reducida. Sea $A = A_1 \times \cdots \times A_n$ la descomposición de A en producto directo de k-álgebras finitas locales. Como $\mathrm{rad}(A) = 0$, entonces $\mathrm{rad}(A_i) = 0$ y A_i es un cuerpo, para todo i. □

9. Ejercicio: Sea $p(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r} \in k[x]$, con $p_i(x)$ irreducibles y primos entre sí, la descomposición de un polinomio en producto de factores irreducibles. Probar que $A = k[x]/(p(x))$ es reducida si y sólo si $n_1 = \cdots = n_r = 1$.

3.7. Teorema de Kronecker para k-álgebras finitas

1. Definición: Dada una k-álgebra A, decimos que $x \in \mathrm{Spec}\, A$ es un punto racional si $A/\mathfrak{p}_x = k$.

2. Definición: Sea A una k-álgebra finita. Diremos que A es racional si todos los puntos de su espectro son racionales. Diremos que una extensión de cuerpos $k \hookrightarrow K$ racionaliza a una k-álgebra A si $A \otimes_k K$ es una K-álgebra racional.

3. Ejemplo: Dada $\alpha \in k$, entonces $k[x]/((x-\alpha)^n)$ es una k-álgebra racional.

4. Ejercicio: Sea $A = k[x]/(p(x))$. Probar que A es racional si y sólo si $p(x)$ descompone en producto de factores simples $(x - \alpha_i)$ (repetidos o no). Probar que $A \otimes_k K$ es una K-álgebra racional si y sólo si K contiene todas las raíces de $p(x)$.

5. Proposición: *Si A es una k-álgebra finita local racional y $k \hookrightarrow K$ es una extensión finita de cuerpos, entonces $A \otimes_k K$ es una K-álgebra finita local K-racional. Por tanto, si A es una k-álgebra finita k-racional entonces $A \otimes_k K$ es una K-álgebra finita K-racional (y $\#\mathrm{Spec}\, A = \#\mathrm{Spec}(A \otimes_k K)$).*

Demostración. Si $\mathfrak{p} \subset A$ es un ideal primo tal que $A/\mathfrak{p} = k$, entonces el ideal $\mathfrak{p} \otimes_k K \subset A \otimes_k K$ cumple que

$$(A \otimes_k K)/(\mathfrak{p} \otimes_k K) = (A/\mathfrak{p}) \otimes_k K = k \otimes_k K = K$$

Por ser $\mathfrak{p} \subset A$ el único ideal primo de A, sus elementos son nilpotentes. Por tanto, los elementos de $\mathfrak{p} \otimes_k K \subset A \otimes_k K$ son nilpotentes. Luego,

$$\mathrm{Spec}(A \otimes_k K) = \{\text{Ideales primos de } A \otimes_k K \text{ que contienen a } \mathfrak{p} \otimes_k K\} = \{\mathfrak{p} \otimes_k K\}$$

En conclusión, $A \otimes_k K$ es una K-álgebra finita local K-racional.

□

6. Teorema (Kronecker) : *Si $k \hookrightarrow A$ es una k-álgebra finita, existe una extensión finita de cuerpos $k \hookrightarrow K$, de modo que $A \otimes_k K$ es una K-álgebra finita racional.*

Demostración. Procedemos por inducción sobre la dimensión de A, siendo el caso de dimensión uno inmediato. Sea $\mathfrak{m} \subset A$ un ideal maximal y $\pi : A \to A/\mathfrak{m} = K$ el morfismo de paso al cociente. El núcleo del epimorfismo inducido $A_K \to K$, $a \otimes \lambda \mapsto \pi(a) \cdot \lambda$ es un punto K-racional de A_K. Por el teorema de descomposición se tiene que A_K descompone

$$A_K = A' \times A''$$

con A' una K-álgebra finita local y racional. Ahora,

$$\dim_K A'' < \dim_K A_K = \dim_k A$$

luego por inducción existe una extensión finita $K \to \Sigma$ tal que $A'' \otimes_K \Sigma$ es Σ-racional. Entonces $A \otimes_k \Sigma$ es Σ-álgebra finita Σ-racional; en efecto:

$$A \otimes_k \Sigma = (A \otimes_k K) \otimes_K \Sigma = (A' \times A'') \otimes_K \Sigma = (A' \otimes_K \Sigma) \times (A'' \otimes_K \Sigma)$$

que es una Σ-álgebra racional. □

3.8. Biografía de Kronecker

KRONECKER BIOGRAPHY

Leopold Kronecker's parents were well off, his father, Isidor Kronecker, being a successful business man while his mother was Johanna Prausnitzer who also came from a wealthy family. The families were Jewish, the religion that Kronecker kept until a year before his death when he became a convert to Christianity. Kronecker's parents employed private tutors to teach him up to the stage when he entered the Gymnasium at Liegnitz, and this tutoring gave him a very sound foundation to his education. Kronecker was taught mathematics at Liegnitz Gymnasium by Kummer, and it was due to Kummer that Kronecker became interested in mathematics. Kummer immediately recognised Kronecker's talent for mathematics and he took him well beyond what would be expected at school, encouraging him to undertake research. Despite his Jewish upbringing, Kronecker was given Evangelical religious instruction at the Gymnasium which certainly shows that his parents were openminded on religious matters.

Kronecker became a student at Berlin University in 1841 and there he studied under Dirichlet and Steiner. He did not restrict himself to studying mathematics, however, for he studied other topics such as astronomy, meteorology and chemistry. He was especially interested in philosophy studying the philosophical works of Descartes, Leibniz, Kant, Spinoza and Hegel. After spending the summer of 1843 at the University of Bonn, which he went to because of his interest in astronomy rather than mathematics, he then went to the University of Breslau for the winter semester of

1843-44. The reason that he went to Breslau was certainly because of his interest in mathematics because he wanted to study again with his old school teacher Kummer who had been appointed to a chair at Breslau in 1842.

Kronecker spent a year at Breslau before returning to Berlin for the winter semester of 1844-45. Back in Berlin he worked on his doctoral thesis on algebraic number theory under Dirichlet's supervision. The thesis, On complex units was submitted on 30 July 1845 and he took the necessary oral examination on 14 August. Dirichlet commented on the thesis saying that in it Kronecker showed:

... unusual penetration, great assiduity, and an exact knowledge of the present state of higher mathematics. It may come as a surprise to many Ph.D. students to hear that

Kronecker was questioned at his oral on a wide range of topics including the theory of probability as applied to astronomical observations, the theory of definite integrals, series and differential equations, as well as on Greek, and the history of philosophy.

Jacobi had health problems which caused him to leave Königsberg, where he held a chair, and return to Berlin. Eisenstein, whose health was also poor, lectured in Berlin around this time and Kronecker came to know both men well. The direction that Kronecker's mathematical interests went later had much to do with the influence of Jacobi and Eisenstein around this time. However, just as it looked as if he would embark on an academic career, Kronecker left Berlin to deal with family affairs. He helped to manage the banking business of his mother's brother and, in 1848, he married the daughter of this uncle, Fanny Prausnitzer. He also managed a family estate but still found the time to continue working on mathematics, although he did this entirely for his own enjoyment.

Certainly Kronecker did not need to take on paid employment since he was by now a wealthy man. His enjoyment of mathematics meant, however, that when circumstances changed in 1855 and he no longer needed to live on the estate outside Liegnitz, he returned to Berlin. He did not wish a university post, rather he wanted to take part in the mathematical life of the university and undertake research interacting with the other mathematicians.

In 1855 Kummer came to Berlin to fill the vacancy which occurred when Dirichlet left for Göttingen. Borchardt had lectured at Berlin since 1848 and, in late 1855, he took over the editorship of Crelle's Journal on Crelle's death. In 1856 Weierstrass came to Berlin, so within a year of Kronecker returning to Berlin, the remarkable team of Kummer, Borchardt, Weierstrass and Kronecker was in place in Berlin.

Of course since Kronecker did not hold a university appointment, he did not lecture at this time but was remarkably active in research publishing a large number of works in quick succession. These were on number theory, elliptic functions and algebra, but, more importantly, he explored the interconnections between these topics. Kummer proposed Kronecker for election to the Berlin Academy in 1860, and the proposal was seconded by Borchardt and Weierstrass. On 23 January 1861 Kronecker was elected to the Academy and this had a surprising benefit.

Members of the Berlin Academy had a right to lecture at Berlin University. Although Kronecker was not employed by the University, or any other organisation for that matter, Kummer suggested that Kronecker exercise his right to lecture at the

University and this he did beginning in October 1862. The topics on which he lectured were very much related to his research: number theory, the theory of equations, the theory of determinants, and the theory of integrals. In his lectures:

He attempted to simplify and refine existing theories and to present them from new perspectives. For the best students his lectures were demanding but stimulating.

However, he was not a popular teacher with the average students:

Kronecker did not attract great numbers of students. Only a few of his auditors were able to follow the flights of his thought, and only a few persevered until the end of the semester.

Berlin was attractive to Kronecker, so much so that when he was offered the chair of mathematics in Göttingen in 1868, he declined. He did accept honours such as election to the Paris Academy in that year and for many years he enjoyed good relations with his colleagues in Berlin and elsewhere. In order to understand why relations began to deteriorate in the 1870s we need to examine Kronecker's mathematical contributions more closely.

We have already indicated that Kronecker's primary contributions were in the theory of equations and higher algebra, with his major contributions in elliptic functions, the theory of algebraic equations, and the theory of algebraic numbers. However the topics he studied were restricted by the fact that he believed in the reduction of all mathematics to arguments involving only the integers and a finite number of steps. Kronecker is well known for his remark:

God created the integers, all else is the work of man.

Kronecker believed that mathematics should deal only with finite numbers and with a finite number of operations. He was the first to doubt the significance of non-constructive existence proofs. It appears that, from the early 1870s, Kronecker was opposed to the use of irrational numbers, upper and lower limits, and the Bolzano-Weierstrass theorem, because of their non-constructive nature. Another consequence of his philosophy of mathematics was that to Kronecker transcendental numbers could not exist.

In 1870 Heine published a paper On trigonometric series in Crelle's Journal, but Kronecker had tried to persuade Heine to withdraw the paper. Again in 1877 Kronecker tried to prevent publication of Cantor's work in Crelle's Journal, not because of any personal feelings against Cantor (which has been suggested by some biographers of Cantor) but rather because Kronecker believed that Cantor's paper was meaningless, since it proved results about mathematical objects which Kronecker believed did not exist. Kronecker was on the editorial staff of Crelle's Journal which is why he had a particularly strong influence on what was published in that journal. After Borchardt died in 1880, Kronecker took over control of Crelle's Journal as the editor and his influence on which papers would be published increased.

The mathematical seminar in Berlin had been jointly founded in 1861 by Kummer and Weierstrass and, when Kummer retired in 1883, Kronecker became a codirector of the seminar. This increased Kronecker's influence in Berlin. Kronecker's international fame also spread, and he was honoured by being elected a foreign member of the Royal

Society of London on 31 January 1884. He was also a very influential figure within German mathematics:

He established other contacts with foreign scientists in numerous travels abroad and in extending to them the hospitality of his Berlin home. For this reason his advice was often solicited in regard to filling mathematical professorships both in Germany and elsewhere; his recommendations were probably as significant as those of his erstwhile friend Weierstrass.

Although Kronecker's view of mathematics was well known to his colleagues during the 1870s and 1880s, it was not until 1886 that he made these views public. In that year he argued against the theory of irrational numbers used by Dedekind, Cantor and Heine giving the arguments by which he opposed:

... the introduction of various concepts by the help of which it has frequently been attempted in recent times (but first by Heine) to conceive and establish the "irrationals" in general. Even the concept of an infinite series, for example one which increases according to definite powers of variables, is in my opinion only permissible with the reservation that in every special case, on the basis of the arithmetic laws of constructing terms (or coefficients), ... certain assumptions must be shown to hold which are applicable to the series like finite expressions, and which thus make the extension beyond the concept of a finite series really unnecessary.

Lindemann had proved that π is transcendental in 1882, and in a lecture given in 1886 Kronecker complimented Lindemann on a beautiful proof but, he claimed, one that proved nothing since transcendental numbers did not exist. So Kronecker was consistent in his arguments and his beliefs, but many mathematicians, proud of their hard earned results, felt that Kronecker was attempting to change the course of mathematics and write their line of research out of future developments. Kronecker explained his programme based on studying only mathematical objects which could be constructed with a finite number of operation from the integers in Über den Zahlbergriff in 1887.

Another feature of Kronecker's personality was that he tended to fall out personally with those who he disagreed with mathematically. Of course, given his belief that only finitely constructible mathematical objects existed, he was completely opposed to Cantor's developing ideas in set theory. Not only Dedekind, Heine and Cantor's mathematics was unacceptable to this way of thinking, and Weierstrass also came to feel that Kronecker was trying to convince the next generation of mathematicians that Weierstrass's work on analysis was of no value.

Kronecker had no official position at Berlin until Kummer retired in 1883 when he was appointed to the chair. But by 1888 Weierstrass felt that he could no longer work with Kronecker in Berlin and decided to go to Switzerland, but then, realising that Kronecker would be in a strong position to influence the choice of his successor, he decided to remain in Berlin.

Kronecker was of very small stature and extremely self-conscious about his height. An example of how Kronecker reacted occurred in 1885 when Schwarz sent him a greeting which included the sentence:

He who does not honour the Smaller, is not worthy of the Greater.

Here Schwarz was joking about the small man Kronecker and the large man Weierstrass. Kronecker did not see the funny side of the comment, however, and never had any further dealings with Schwarz (who was Weierstrass's student and Kummer's son-in-law). Others however displayed more tact and, for example, Helmholtz who was a professor in Berlin from 1871, managed to stay on good terms with Kronecker.

The Deutsche Mathematiker-Vereinigung was set up in 1890 and the first meeting of the Association was organised in Halle in September 1891. Despite the bitter antagonism between Cantor and Kronecker, Cantor invited Kronecker to address this first meeting as a sign of respect for one of the senior and most eminent figures in German mathematics. However, Kronecker never addressed the meeting, since his wife was seriously injured in a climbing accident in the summer and died on 23 August 1891. Kronecker only outlived his wife by a few months, and died in December 1891.

We should not think that Kronecker's views of mathematics were totally eccentric. Although it was true that most mathematicians of his day would not agree with those views, and indeed most mathematicians today would not agree with them, they were not put aside. Kronecker's ideas were further developed by Poincaré and Brouwer, who placed particular emphasis upon intuition. Intuitionism stresses that mathematics has priority over logic, the objects of mathematics are constructed and operated upon in the mind by the mathematician, and it is impossible to define the properties of mathematical objects simply by establishing a number of axioms.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

3.9. Cuestionario

1. ¿Es $\mathbb{Q} \hookrightarrow \mathbb{C}$ una extensión finita de cuerpos?
2. ¿Es $\pi \in \mathbb{R}$ un elemento $\mathbb{R}$-algebraico?
3. ¿Es $i \in \mathbb{C}$ un elemento $\mathbb{Q}$-algebraico?
4. ¿Cuál es la dimensión sobre k de la k-álgebra $(k[x]/(x^3+1) \otimes_k k[x]/(x^2+1)) \times k[x]/(x^2+x+1)$?
5. ¿Es $\sqrt{2}+8\cdot\sqrt{3}\cdot\sqrt[5]{3}^2-15$ $\mathbb{Q}$-algebraico? ¿y, $\mathbb{Q}(\sqrt{2})$-algebraico?
6. ¿Es $\mathbb{C}$ el cierre algebraico de $\mathbb{R}$?¿Es $\mathbb{C}$ el cierre algebraico de $\mathbb{Q}$?
7. Sean α_1, α_2 y α_3 las raíces de $x^3 - x + 1 \in \mathbb{Q}[x]$. Calcular $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in \mathbb{Q}$.
8. Expresar $x_1^3 + x_2^3 + x_3^3$ como polinomio en las funciones simétricas elementales de las variables x_1, x_2, x_3.
9. Calcular mediante la fórmula de Girard, las potencias simétricas σ_n de las raíces de $x^4 - 1$, para todo $n \in \mathbb{N}$.

10. Calcular el discriminante de $x^4 - 1$.

11. Si dos polinomios mónicos tienen las mismas potencias simétricas σ_n, para todo n entonces ¿son iguales?

12. ¿Tiene $x^3 - 1 \in \mathbb{Q}[x]$ raíces múltiples?¿Tiene $x^3 - 1 \in \mathbb{Z}/3\mathbb{Z}[x]$ raíces múltiples?

13. Explicitar el isomorfismo de k-álgebras $k[x]/(x-\alpha) \simeq k$.

14. Sea $k \hookrightarrow K$ una extensión de cuerpos y A una k-álgebra finita ¿Es $A \otimes_k K$ una K-álgebra finita?

15. Sea A una k-álgebra finita íntegra y $B \subseteq A$ una k-subálgebra ¿Es B una k-álgebra finita íntegra?

16. Sea $k \hookrightarrow K$ una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in K$ elementos k-algebraicos ¿Es
$$k(\alpha_1, \ldots, \alpha_n) = \{p(\alpha_1, \ldots, \alpha_n) \in K, \text{ con } p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]\}?$$

17. Sean A_1 y A_2 dos k-álgebras finitas ¿Es $A_1 \times A_2$ una k-álgebra finita? Si A_1 y A_2 son dos k-álgebras finitas íntegras ¿Es $A_1 \times A_2$ una k-álgebra finita íntegra?

18. ¿Es $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ una $\mathbb{R}$-álgebra íntegra?

19. Si A_1 y A_2 son dos k-álgebras finitas íntegras ¿Es $A_1 \otimes_k A_2$ una k-álgebra finita íntegra?

20. Decir cuáles de estas álgebras son íntegras, cuáles cuerpos y cuáles son reducidas: $\mathbb{R}[x]/(x^2+1)$, $\mathbb{C}[x]/(x^2+1)$, $\mathbb{R}[x]$, $\mathbb{R}[x]/(x+1)^3$.

21. Sea $A = \mathbb{Q}[x]/((x-2)(x^3-2)) \times \mathbb{Q}[x]/(x-2)$. Calcular $\#\operatorname{Spec} A$ y $\dim_{\mathbb{Q}} A$.

22. Descomponer $\mathbb{Q}[x]/(x^4-2x^3+2x^2-2x+1)$ en producto directo de $\mathbb{Q}$-álgebras finitas locales.

23. Sean A_1 y A_2 dos anillos no nulos ¿Puede ser $A_1 \times A_2$ un anillo local?

24. ¿Existe algún isomorfismo entre las $\mathbb{R}$-álgebras $\mathbb{R}[x]/(x^2)$ y $\mathbb{R} \times \mathbb{R}$?

25. Dar todos los ejemplos posibles (salvo isomorfismos) de $\mathbb{Q}$-álgebras finitas de dimensión 33 que descompongan en producto directo de 33 $\mathbb{Q}$-álgebras finitas locales.

26. Sea $A = \mathbb{Q}[x]/((x-2)(x^3-2)) \times \mathbb{Q}[x]/(x-2)$. Dar una $\mathbb{Q}$-extensión finita de cuerpos K, tal que $A \otimes_{\mathbb{Q}} K$ sea una K-álgebra finita racional.

27. Sea A una k-álgebra finita y $k \hookrightarrow K$ una extensión de cuerpos tal que $A \otimes_k K$ sea una K-álgebra finita racional ¿Si $K \hookrightarrow \Sigma$ es una extensión de cuerpos, entonces $A \otimes_k \Sigma$ es una Σ-álgebra finita racional?

28. Sea k un cuerpo algebraicamente cerrado y A una k-álgebra finita. ¿Es A una k-álgebra finita racional?

3.10. Problemas

1. Sea $A = \mathbb{Q}[x]/(2x^3+4x^2-x-2)$ y sea $\alpha = \bar{x}$. ¿Son $\alpha+2$ y $\alpha-2$ invertibles en A?.

2. Sea $K = \mathbb{Q}[x]/(x^3-x-1)$ y sea $\alpha = \bar{x}$. Racionalizar $1/(\alpha+2)$ y determinar si $(2+\alpha)^3$ es la unidad. ¿Tiene el polinomio x^2-2 alguna raíz en K?. Calcular un polinomio no nulo con coeficientes racionales $p(x)$ que admita la raíz $\beta = \alpha^2+1$.

3. Si $a, b \in \mathbb{Q}$, demostrar que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ precisamente cuando a/b sea un cuadrado en $\mathbb{Q}$.

4. Probar que $\mathbb{Q}(\sqrt[n]{2})$ tiene grado n sobre $\mathbb{Q}$.

5. Demostrar que $\mathbb{Q}(\sqrt[3]{2})$ es una extensión de grado 3 de $\mathbb{Q}$. ¿Está $\sqrt{2}$ en $\mathbb{Q}(\sqrt[3]{2})$?
   Demostrar que $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$. ¿Está $\sqrt[3]{2}$ en $\mathbb{Q}(\sqrt[4]{2})$?

6. Determinar si las siguientes igualdades son ciertas:

$$\begin{aligned} \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) &= \mathbb{Q}(\sqrt[4]{2}, i) \\ \mathbb{Q}(2^{-1/2}, i) &= \mathbb{Q}(i\sqrt{2}) \\ \mathbb{Q}(2^{-1/2}, i) &= \mathbb{Q}(i+\sqrt{2}) \end{aligned}$$

7. Determinar las relaciones de inclusión entre los siguientes subcuerpos de $\mathbb{C}$:
$$\mathbb{Q}\ ,\ \mathbb{Q}(1/2)\ ,\ \mathbb{Q}(\sqrt{2})\ ,\ \mathbb{Q}(\sqrt[3]{2})\ ,\ \mathbb{Q}(i)\ ,\ \mathbb{Q}(i+\sqrt{2})\ ,\ \mathbb{Q}(\sqrt{-2})$$

8. Sea $p(x)$ un polinomio irreducible de grado n con coeficientes en un cuerpo k. Si el grado de una extensión finita L de k no es múltiplo de n, entonces $p(x)$ no tiene raíces en L.

9. Demostrar que x^3-3 no tiene raíces en $k = \mathbb{Q}(\sqrt{2})$. Concluir que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ es una extensión de grado 6 de $\mathbb{Q}$ y hallar una base sobre $\mathbb{Q}$.

   Sea $\alpha = \sqrt{2}+\sqrt[3]{3}$. Probar que el grado de un polinomio irreducible en $\mathbb{Q}[x]$ que admita la raíz α es $[\mathbb{Q}(\alpha):\mathbb{Q}] = 1, 2, 3,$ ó 6. Analizando las relaciones de dependencia lineal entre las sucesivas potencias de α, concluir que α es raíz de un polinomio irreducible de grado 6 con coeficientes racionales. Calcular tal polinomio.

10. Sea $K = \mathbb{F}_2[x]/(x^3+x+1)$ y sea $\alpha = \bar{x}$. Probar que K es un cuerpo con 8 elementos

$$K = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$$

    Calcular las raíces de x^3+x+1 en K, y las raíces de x^3+x^2+1 en K.

11. Construir un cuerpo con 4 elementos y otro con 9 elementos.

12. Calcular el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan las raíces complejas del polinomio x^3-1. Análogamente para x^3+1, x^4-1, x^4+1, x^5-1, x^5+1 y x^6-1.

13. Hallar el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan todas las raíces complejas del polinomio x^3-2. Análogamente para los polinomios

$$x^4-2\ ,\ x^4+2\ ,\ x^4-x^2+1\ ,\ x^4+x^2-2,\ x^3-4x^2+5$$

14. Calcular un polinomio irreducible con coeficientes en $\mathbb{Q}(i)$ que admita la raíz $\sqrt[4]{2}$. Análogamente sustituyendo $\mathbb{Q}(i)$ por $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$.

15. Sea K una extensión de grado 2 de un cuerpo k. Si la característica de k no es 2, probar que $K=k(\sqrt{a}$ para algún $a\in k$. ¿Es cierto también cuando $\operatorname{car} k=2$?

16. Hallar un polinomio $p(x)\in\mathbb{Q}[x]$ tal que $\mathbb{Q}(i)\oplus\mathbb{Q}(\sqrt[3]{2})\ \simeq\ \mathbb{Q}[x]/(p(x))$.

17. ¿Existe algún polinomio $p(x)\in\mathbb{Q}[x]$ tal que $\mathbb{Q}(i)\oplus\mathbb{Q}(i)\ \simeq\ \mathbb{Q}[x]/(p(x))$?

18. Sean $\alpha_1,\ldots,\alpha_n$ raíces complejas de ciertos polinomios no nulos $p_1(x),\ldots,p_n(x)\in\mathbb{Q}[x]$. Demostrar que $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ es una $\mathbb{Q}$-álgebra finita de grado acotado por el producto de los grados de los polinomios $p_1(x),\ldots,p_n(x)$.

19. Una extensión finita $k\to L$ es trivial (i.e., $[L:k]=1$) si y sólo si $L\otimes_k L$ es cuerpo. (*Indicación:* Considerar el morfismo natural $L\otimes_k L\to L$).

20. Sean L,L' dos k-extensiones de cuerpos de k, de grados n y m respectivamente. Probar que si n y m son primos entre sí, entonces $L\otimes_k L'$ es un cuerpo.

21. Si L y L' son dos extensiones no triviales (i.e., de grado mayor que 1) de un cuerpo k, ¿puede ocurrir que $L'\otimes_k L$ no sea un cuerpo? ¿y que $L'\otimes_k L$ sí sea un cuerpo?.

22. Probar que toda extensión finita L de $\mathbb{C}$ es trivial: $\mathbb{C}\simeq L$. Concluir que toda $\mathbb{C}$–álgebra finita reducida de grado n es isomorfa a $\mathbb{C}\oplus\overset{n}{\ldots}\oplus\mathbb{C}$. ¿Es cierto que toda $\mathbb{C}$–álgebra finita es trivial?

23. Probar que toda extensión finita de $\mathbb{R}$ es isomorfa a $\mathbb{R}$ ó a $\mathbb{C}$. Concluir que toda $\mathbb{R}$–álgebra finita reducida es isomorfa a $\mathbb{R}\oplus\overset{n}{\ldots}\oplus\mathbb{R}\oplus\mathbb{C}\oplus\overset{m}{\ldots}\oplus\mathbb{C}$ para ciertos $n,m\in\mathbb{N}$.

24. Sea $k=\mathbb{Q}(\sqrt[5]{5})$. Probar que el polinomio mínimo anulador de $e^{\frac{2\pi i}{5}}$ con coeficientes en k es $x^4+x^3+x^2+x+1$.

    Determinar el número de automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de x^5-5.

25. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. Probar que α es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$. Probar que si α es una raíz de $p(x)$ de multiplicidad $m\geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad $m-1$, cuando la característica de k es cero. Probar que si α es una raíz de $p(x)$ de multiplicidad $m\geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad mayor o igual que $m-1$, cuando la característica de k es positiva.

26. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k, de característica nula. Probar que si m es la multiplicidad de una raíz α del polinomio $d(x) = \text{m.c.d.}\big(p(x), p'(x)\big)$, entonces α es una raíz de $p(x)$ de multiplicidad $m+1$.

    ¿Es cierto este enunciado en los cuerpos de característica positiva?

27. Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo. Probar que si $p(x)$ tiene alguna raíz múltiple, entonces su derivada $p'(x)$ es nula.

    Si $p(x)$ tiene una raíz simple ¿es cierto que todas sus raíces son simples?. Si $p(x)$ tiene una raíz múltiple ¿es cierto que todas sus raíces son múltiples?

28. Hallar las raíces múltiples de los siguientes polinomios con coeficientes racionales, así como sus respectivas multiplicidades ¿y si los coeficientes están en $\mathbb{F}_2$? ¿y en $\mathbb{F}_3$? ¿y en $\mathbb{F}_5$?

$$x^4 + 4x^2 + 1 \quad , \quad 4x^4 - 4x^3 - 3x^2 + 2x + 1$$

Capítulo 4

Teoría de Galois

4.1. Introducción

Dado un polinomio $p(x) \in k[x]$, consideremos una extensión de cuerpos $k \hookrightarrow L$, de modo que $p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n)$, con $\alpha_1, \ldots, \alpha_n \in L$.

¿Pueden obtenerse las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$ mediante expresiones con radicales de elementos de k?

Sea $k(\alpha_1, \ldots, \alpha_n) \subseteq L$ el mínimo subcuerpo de L que contiene a $\alpha_1, \ldots, \alpha_n$ (y k), que se denomina el cuerpo de descomposición de $p(x)$. Consideremos el epimorfismo $k[x_1, \ldots, x_n] \xrightarrow{\phi} k(\alpha_1, \ldots, \alpha_n) \subset L$, $\phi(q(x_1, \ldots, x_n)) := q(\alpha_1, \ldots, \alpha_n)$. Entonces,

$$k(\alpha_1, \ldots, \alpha_n) = k[x_1, \ldots, x_n]/I,$$

con $I = \{q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \colon q(\alpha_1, \ldots, \alpha_n) = 0\}$. Los automorfismos de k-álgebras de $k(\alpha_1, \ldots, \alpha_n)$, han de permutar las raíces de $p(x)$, es más, están en correspondencia biunívoca con las permutaciones de las raíces tales que si unas cuantas raíces verifican una relación algebraica entonces sus permutadas verifican la misma relación. La teoría de Galois clásica demuestra que el grupo (de Galois) de los automorfismos del cuerpo de descomposición de $p(x)$ es resoluble si y sólo si las raíces de $p(x)$ se pueden obtener mediante radicales, y en el caso resoluble da el procedimiento para obtener las raíces.

Breve reseña histórica: Una tablilla babilónica del 1600 antes de Cristo plantea problemas que se reducen al problema de resolver ecuaciones de segundo grado, y da métodos para resolverlas, si bien no usaban aún ninguna notación algebraica. Los antiguos griegos resolvieron ecuaciones de segundo grado por medios geométricos. Incluso desarrollaron métodos aplicables a ecuaciones de tercer grado, mediante el corte de cónicas, de nuevo sin ninguna formulación algebraica.

Ya en el Renacimiento italiano, parece ser que Scipio del Ferro resolvió las ecuaciones cúbicas (ya con notación algebraica). En 1535, en una competición pública, Tartaglia frente a Fior (discípulo de Ferro) demostró haber redescubierto el método de resolución de las ecuaciones cúbicas, pero se negó a contar los detalles. Se los contó bajo secreto de juramento a Cardano, el cual publicó en su Ars Magna. El Ars Magna contenía también un método, debido a Ferrari, para resolver la ecuación de cuarto grado, reduciéndola a una cúbica.

A partir de entonces mucho matemáticos intentaron resolver las ecuaciones de quinto grado. Euler fracasó en el intento de resolverlas, pero encontró nuevos métodos para resolver las cuárticas. Lagrange en 1770 mostró que el método de resolución de las cúbicas y cuárticas dependía de encontrar ciertas funciones en las raíces que fueran invariantes por ciertas permutaciones de éstas; y mostró que este método fallaba con las quínticas. Abel en 1824 probó que la ecuación general de quinto grado no es resoluble por radicales. Por último, Galois ("desenterrado" para la Historia en 1843 por Liouville), resolvió con éxito el problema de determinar cuándo las raíces de una ecuación polinómica pueden resolverse por radicales.

4.2. k-álgebras finitas triviales

1. Definición: Diremos que una k-álgebra finita A es trivial si existe un isomorfismo de k-álgebras

$$A \simeq k \times \ldots \times k.$$

2. Proposición: *Sea A una k-álgebra finita. A es trivial si y sólo si es racional y reducida.*

Demostración. Si A es trivial es obviamente racional y reducida. Si A es reducida es producto directo de cuerpos, si es además racional estos cuerpos han de ser iguales a k, es decir, A es trivial. □

3. Teorema: *Sea $p(x) \in k[x]$. Entonces, $k[x]/(p(x))$ es una k-álgebra finita trivial si y sólo si todas las raíces de $p(x)$ son de multiplicidad 1 y están en k.*

Demostración. Si $p(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, con $\alpha_i \in k$, para todo i y $\alpha_i \neq \alpha_j$ cuando $i \neq j$, entonces por el teorema chino de los restos

$$k[x]/(p(x)) = k[x]/(x-\alpha_1) \times \overset{n}{\cdots} \times k[x]/(x-\alpha_n) = k \times \overset{n}{\cdots} \times k$$

es una k-álgebra trivial.

Recíprocamente, sea $p(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ la descomposición de en factores irreducibles ($p_i(x)$ primo con $p_j(x)$, para todo $i \neq j$) y supongamos que

$$k[x]/(p(x)) = k[x]/(p_1(x)^{n_1}) \times \cdots \times k[x]/(p_r(x)^{n_r})$$

es trivial. Como es reducida $n_i = 1$, para todo i. Como es racional los polinomios irreducibles $p_i(x)$ son de grado 1. Luego, $p(x) = \lambda \cdot (x-\alpha_1)\cdots(x-\alpha_r)$, con $\alpha_i \in k$, para todo i y $\alpha_i \neq \alpha_j$ cuando $i \neq j$.

□

4. Ejercicio: Probar:

1. Si A es una k-álgebra finita trivial, entonces A_K es una K-álgebra trivial, para toda extensión $k \to K$.

2. El producto tensorial de dos k-álgebras finitas triviales es una k-álgebra finita trivial.

5. Proposición : *El cociente de una k-álgebra finita trivial por un ideal es una k-álgebra finita trivial.*

Demostración. Dado un ideal $I \subseteq k \times \overset{n}{\cdots} \times k$, tenemos que $I = I_1 \times \cdots \times I_n$, donde los ideales $I_i \subseteq k$ o son nulos o iguales a k. Por tanto,

$$(k \times \overset{n}{\cdots} \times k)/I = (k/I_1) \times \cdots \times (k/I_n)$$

es una k-álgebra trivial

□

6. Ejercicio : Probar que dos k-álgebras finitas, A y B son triviales si y sólo si $A \times B$ es trivial.

7. Proposición : *Las subálgebras de una k-álgebra finita trivial son triviales.*

Demostración. Sea $B \subseteq k^n$ una k-subálgebra. Como k^n es reducida, B es reducida, luego es producto cartesiano de k-extensiones de cuerpos. Escribamos $B = K_1 \times \cdots \times K_r$. Consideremos la aplicación $K_i \overset{i}{\hookrightarrow} K_1 \times \cdots \times K_r$, $\lambda_i \mapsto (0,\ldots,0,\overset{i}{\lambda_i},0,\ldots,0)$. Sea $\pi_j \colon k^n \to k$ una proyección en un factor j-ésimo conveniente, tal que $\pi_j \circ i \neq 0$. $\mathrm{Ker}(\pi_j \circ i)$ es un ideal de K_i, luego es el ideal 0. Luego $K_i \hookrightarrow k$, $K_i = k$ y B es trivial. □

Dado un punto racional $x \in \mathrm{Spec}\, A$ tenemos el morfismo de paso al cociente $A \to A/\mathfrak{p}_x = k$. Recíprocamente, dado un morfismo $\phi \colon A \to k$, entonces $\mathfrak{p}_x := \mathrm{Ker}\,\phi$ es un punto racional. En conclusión,

$$\mathrm{Hom}_{k-alg}(A,k) = \{\text{Puntos racionales de } A\} \subseteq \mathrm{Spec}\, A$$

8. Proposición : *Una k-álgebra finita A es racional si y sólo si* $\#\mathrm{Hom}_{k-alg}(A,k) = \#\mathrm{Spec}\, A$.

9. Proposición : *Sea A una k-álgebra finita. Entonces,*

1. *A es una k-álgebra finita trivial si y sólo si* $\#\mathrm{Spec}\, A = \dim_k A$.
2. *A es una k-álgebra finita trivial si y sólo si* $\boxed{\#\mathrm{Hom}_{k-alg}(A,k) = \dim_k A}$.

Demostración. Por 3.6.7, A es producto cartesiano de k-álgebras finitas locales

$$A = A_1 \times \ldots \times A_r \times \ldots \times A_n$$

donde podemos suponer que $A_1,\ldots,A_r$ son racionales y $A_{r+1},\ldots,A_n$ no son racionales. Tenemos que $\dim_k A = \dim_k A_1 + \cdots + \dim_k A_n$, $\#\mathrm{Spec}\, A = n$ y $\#\mathrm{Hom}_{k-alg}(A,k) = r$.

Por tanto, $\dim_k A = \#\mathrm{Spec}\, A$ si y sólo si $\dim_k A_i = 1$ para todo i, es decir, si y sólo si es trivial.

Si A es trivial, entonces $r = n = \dim_k A$. Recíprocamente, si $r = \dim_k A$, entonces $n = r$ y $\dim_k A_i = 1$ para todo i, es decir, A es trivial.

□

4.3. k-álgebras finitas separables

1. Definición: Se dice que una k-álgebra finita A es separable si existe una extensión cuerpos $k \hookrightarrow K$ tal que $A \otimes_k K = \prod_i K$. En este caso se dice que A es trivializada por K.

Las k-álgebras finitas triviales son k-álgebras finitas separables.

2. Teorema: *La k-álgebra $k[x]/(p(x))$ es separable si y sólo si $p(x)$ no tiene raíces múltiples, es decir, $p(x)$ y $p'(x)$ son primos entre sí.*

Demostración. Si $k[x]/(p(x))$ es separable es separable entonces existe una extensión de cuerpos $k \hookrightarrow K$ de modo que $k[x]/(p(x)) \otimes_k K = K[x]/(p(x))$ es K-trivial, luego todas las raíces de $p(x)$ están en K y tienen multiplicidad 1. Luego, $p(x)$ no tiene raíces múltiples.

Supongamos ahora que todas las raíces de $p(x)$ son de multiplicidad 1. Sea K una k-extensión de cuerpos que contenga a dichas raíces. Entonces, $k[x]/(p(x)) \otimes_k K = K[x]/(p(x))$ es K-trivial.

□

3. Proposición: *Sea A una k-álgebra finita separable. Si K trivializa a A y $K \hookrightarrow \Sigma$ es una extensión de cuerpos, entonces Σ trivializa a A.*

Demostración. $A \otimes_k \Sigma = (A \otimes_k K) \otimes_K \Sigma = K^n \otimes_K \Sigma = \Sigma^n$. □

4. Proposición: *Se cumple:*

- $A \times B$ es separable si y sólo si A y B lo son.

- El producto tensorial (sobre k) de k-álgebras separables es una k-álgebra separable.

- Toda subálgebra y cociente de una k-álgebra separable es separable.

Demostración. Al lector. □

5. Fórmula de los puntos: *Sea A una k-álgebra y $k \to K$ una extensión de cuerpos. Entonces,*

$$\mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \{\textit{Puntos } K\textit{-racionales de } A \otimes_k K\}$$

En particular,

$$\boxed{\#\mathrm{Hom}_{k-alg}(A,K) \leq \dim_k A}$$

Demostración. Por la proposición 2.2.5, $\mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{K-alg}(A \otimes_k K, K)$ y como sabemos

$$\mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \{\text{Puntos } K\text{-racionales de } A \otimes_k K\}.$$

Además,

$$\#\mathrm{Hom}_{k-alg}(A,K) \leq \#\mathrm{Spec}(A \otimes_k K) \leq \dim_K(A \otimes_k K) = \dim_k A$$

□

Si $A = k[x]/(p(x))$, tenemos la igualdad

$$\begin{array}{rcl} \mathrm{Hom}_{k-alg}(k[x]/(p(x)),K) & = & \{\alpha \in K\colon p(\alpha)=0\} \\ \phi & \longmapsto & \phi(\bar{x}) \\ \phi_\alpha & \longmapsto & \alpha \\ \phi_\alpha(\overline{q(x)}) := q(\alpha) & & \end{array}$$

Si $A = A_1 \times A_2$, todo morfismo de k-álgebras $f\colon A_1 \times A_2 \to K$ factoriza a través de la proyección en A_1 o la proyección en A_2: Tenemos $\mathrm{Ker}\, f = I_1 \times I_2 \subseteq A_1 \times A_2$. Como $A/\mathrm{Ker}\, f = A_1/I_1 \times A_2/I_2$ es íntegro, pues se inyecta en K, tenemos que $I_1 = A_1$, luego f factoriza a través de la proyección en A_2 ó $I_2 = A_2$, luego f factoriza a través de la proyección en A_1. En conclusión,

$$\mathrm{Hom}_{k-alg}(A_1 \times A_2, K) = \mathrm{Hom}_{k-alg}(A_1,K) \coprod \mathrm{Hom}_{k-alg}(A_2,K)$$

6. Ejercicio: Calcular $\mathrm{Hom}_{\mathbb{Q}-alg}(\mathbb{Q}[x]/(x^2-2) \times \mathbb{Q}[x]/((x^2-2)^2), \mathbb{C})$.

7. Proposición: *Una extensión de cuerpos $k \hookrightarrow K$ trivializa a una k-álgebra finita A si y sólo si*

$$\boxed{\#\mathrm{Hom}_{k-alg}(A,K) = \dim_k A}$$

Demostración. $A \otimes_k K$ es una K-álgebra trivial si y sólo si

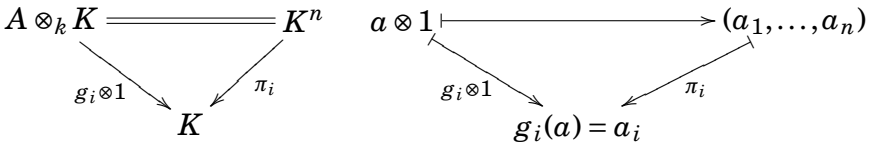
$$\#\mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \dim_K A_K,$$

es decir, si y sólo si $\#\mathrm{Hom}_{k-alg}(A,K) = \dim_k A$. □

8. Observación: Sea A una k-álgebra separable de grado n, $k \hookrightarrow K$ una extensión que trivializa a A y $\mathrm{Hom}_{k-alg}(A,K) = \{g_1,\ldots,g_n\}$. Explicitemos el isomorfismo $A \otimes_k K = K \times \overset{n}{\cdots} \times K$. Tenemos,

$$\{g_1,\ldots,g_n\} = \mathrm{Hom}_{k-alg}(A,K) = \mathrm{Hom}_{K-alg}(A \otimes_k K, K) = \mathrm{Hom}_{K-alg}(K^n,K) = \{\pi_1,\ldots,\pi_n\}$$

donde π_i es la proyección en el factor i. De los diagramas conmutativos



se deduce, que el isomorfismo $A \otimes_k K = K^n$, asigna $a \otimes \lambda$ en $(g_1(a)\cdot\lambda,\ldots,g_n(a)\cdot\lambda)$.

9. Teorema: *Sea k un cuerpo con infinitos elementos y A una k-álgebra finita separable. Existe un elemento $a \in A$ tal que $A = k[a]$. En este caso se dice que A es primitiva y que a es un elemento primitivo de A.*

Demostración. Sea $k \to K$ una extensión de cuerpos que trivialice a A. Si $\dim_k A = n$, entonces A tiene n puntos K-racionales. Escribamos $\{\phi_1,\ldots,\phi_n\} = \mathrm{Hom}_{k-\text{álg}}(A,K)$. Consideremos en A los subespacios vectoriales $H_{ij} := \mathrm{Ker}(\phi_i - \phi_j) \underset{\neq}{\subset} A$, $i \neq j$. Sea $a \in A$ un elemento que no pertenezca a ninguno de dichos subespacios vectoriales. Entonces, las restricciones de ϕ_i y ϕ_j a $k[a]$ son distintas, para todo $i \neq j$. Por tanto, $\#\mathrm{Hom}_{k-alg}(k[a],K) \geq n$, luego $\dim_k k[a] \geq n$ y $A = k[a]$. □

10. Definición: Sea A una k-álgebra finita. Se dice que un elemento $a \in A$ es separable (sobre k) si $k[a]$ es una k-álgebra separable (es decir, si el polinomio anulador mínimo de a no tiene raíces múltiples).

11. Proposición: *Una k-álgebra finita A, es separable si y sólo si todos sus elementos son separables.*

Demostración. Toda subálgebra de una k-álgebra separable es separable, luego todo elemento de una k-álgebra separable es separable.

Recíprocamente, veamos que si todo elemento es separable el álgebra es separable. Sean $a_1,\dots,a_n \in A$ tales que $A = k[a_1,\dots,a_n]$, entonces A es un cociente de $k[a_1]\underset{k}{\otimes}\cdots\underset{k}{\otimes} k[a_n]$, luego es separable. □

12. Proposición: *Sea A una k-álgebra finita y $k \to K$ una extensión de cuerpos. Entonces A es separable sobre k si y sólo si A_K es separable sobre K.*

Demostración. Si A es separable, sea Σ una extensión trivializante de A y Σ' un compuesto de K y Σ, entonces $(A \otimes_k K) \otimes_K \Sigma' = A \otimes_k \Sigma'$ es Σ'-trivial y $A \otimes_k K$ es K-separable.

Si A_K es K-separable, sea Σ una K-extensión trivializante de A_K. Entonces, $A \otimes_k \Sigma = A_K \otimes_K \Sigma$ es Σ-trivial y A es k-separable.

□

13. Proposición: *Una k-álgebra finita A es separable si y sólo si A_K es reducida, para toda extensión de cuerpos, $k \to K$.*

Demostración. Sea A una k-álgebra separable. Sea Σ una k-extensión trivializante de A. A es reducida porque $A \hookrightarrow A \otimes_k \Sigma = \Sigma^n$ es una subálgebra de un álgebra reducida. Como A_K es una K-álgebra separable entonces es reducida.

Recíprocamente, si A es reducida por todo cambio de cuerpo base, considerando un cambio de cuerpo base $k \to K$ racionalizante, se obtiene que A_K es K-racional y reducida, luego trivial. □

Consideremos el morfismo de anillos

$$\varphi\colon \mathbb{Z} \to k,\ \varphi(n) = \begin{cases} 1 + \overset{n}{\dots} + 1 & \text{si } n > 0 \\ -\varphi(-n) & \text{si } n < 0 \\ 0 & \text{si } n = 0 \end{cases}$$

14. Definición: Si $\operatorname{Ker}\varphi = 0$, se dice que k es un cuerpo de característica cero. En este caso, tendremos una inyección canónica $\mathbb{Q} \hookrightarrow k$. Si $\operatorname{Ker}\varphi \neq 0$, entonces $\operatorname{Ker}\varphi = p\mathbb{Z}$, con p primo, porque $\mathbb{Z}/p\mathbb{Z}$ es íntegro pues se inyecta en el anillo íntegro k. En este caso se dice que k es de característica p y tenemos una inyección canónica $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$.

15. Teorema: *Sea k un cuerpo de característica cero. Una k-álgebra finita A es separable si y sólo si es reducida.*

Demostración. Si A es separable es reducida por 4.3.13.

Si A es reducida entonces es producto directo de cuerpos. En característica cero las extensiones finitas de cuerpos son separables, porque todos sus elementos son separables: En efecto, el polinomio anulador $p(x)$ de un elemento es un polinomio irreducible,

luego primo con su derivada $p'(x)$ (en característica cero $p'(x) \neq 0$), luego sin raíces múltiples.

□

4.4. Extensiones de Galois

1. Definición: Diremos que una extensión finita de cuerpos $k \to K$ es de *Galois* si se trivializa a si misma, esto es

$$K \underset{k}{\otimes} K \simeq K \times \cdots \times K$$

Se llama *grupo* de la extensión K al grupo de automorfismos de k-álgebras de K. En resumen, diremos que $k \to K$ *es una extensión de Galois de grupo* G, si es de Galois y $G = \mathrm{Aut}_{k-alg} K$.

Si $k \to K$ es de Galois, entonces $K \underset{k}{\otimes} K \simeq K \times \overset{n}{\cdots} \times K$, y $n = \dim_K(K \underset{k}{\otimes} K) = \dim_k K =$ grado de la extensión K.

2. Ejemplo: $\mathbb{Q}[\sqrt{2}]$ es una $\mathbb{Q}$-extensión de Galois, porque

$$\begin{aligned}\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}] &= \mathbb{Q}[x]/(x^2-2) \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}] = \mathbb{Q}[\sqrt{2}][x]/(x^2-2) \\ &= \mathbb{Q}[\sqrt{2}][x]/(x-\sqrt{2}) \times \mathbb{Q}[\sqrt{2}][x]/(x+\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}]\end{aligned}$$

En general, una k-extensión de cuerpos $K = k[x]/(p(x))$ es de Galois si y sólo si todas las raíces de $p(x)$ son de multiplicidad 1 y están en K.

3. Proposición: *Una extensión $k \to K$ es de Galois si y sólo si el grado de la extensión coincide con el número de automorfismos,*

$$\dim_k K = \mathrm{Aut}_{k-alg} K$$

Demostración. Sabemos por la proposición 4.3.7, que K se trivializa a sí misma si y sólo tiene tantos endomorfismos (de k-álgebras) como grado. Como todo endomorfismo de k-álgebras de K es un automorfismo, se concluye. □

Sea $A = k[x]/(p(x))$ una k-álgebra separable (todas las raíces de $p(x)$ son de multiplicidad 1). Si $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $p(x)$, la extensión mínima trivializante de A es $k(\alpha_1, \ldots, \alpha_n)$. Además, $K = k(\alpha_1, \ldots, \alpha_n)$ es una extensión de Galois: $k(\alpha_i)$ está trivializada por K, para todo i, luego $B = k[\alpha_1] \otimes_k \cdots \otimes_k k[\alpha_n]$ está trivializada por K, luego K que es un cociente de B, está trivializada por K y es de Galois.

4. Teorema: *Sea $k \hookrightarrow A$ una k-álgebra finita separable. Existe una extensión mínima de cuerpos que trivializa a A. Además, es única salvo isomorfismos y es de Galois.*

Demostración. Sea $k \hookrightarrow K$ una extensión que trivialice a A. Tenemos que

$$\#\mathrm{Hom}_{k-alg}(A, K) = \dim_k A = n.$$

Sea $\{\phi_1, \ldots, \phi_n\} = \mathrm{Hom}_{k-alg}(A, K)$ y $\phi \colon A \otimes_k \overset{n}{\cdots} \otimes_k A \to K$, el morfismo de k-álgebras definido por $\phi(a_1 \otimes_k \ldots \otimes_k a_n) := \phi_1(a_1) \cdot \ldots \cdot \phi_n(a_n)$. Sea $\Sigma := \mathrm{Im}\,\phi$, que es una extensión

que trivializa a A, porque $\#\mathrm{Hom}_{k-alg}(A,\Sigma) = n$. Σ es un cociente de $A \otimes_k \ldots \otimes_k A$, que está trivializado por Σ, luego Σ trivializa a Σ, es decir, es de Galois. De nuevo, si una extensión trivializa a A, trivializa a $A \otimes_k \ldots \otimes_k A$ y trivializará a Σ, en particular, la contiene. De aquí se obtiene la unicidad y minimalidad de Σ. □

5. Definición: Sea $k \hookrightarrow A$ una k-álgebra finita separable. Denominaremos envolvente de Galois de A sobre k, a la extensión mínima de cuerpos trivializante de A. Si $A = k[x]/(p(x))$, (con $p(x)$ sin raíces múltiple) la extensión mínima que trivializa a A, es el mínimo cuerpo que contiene a las raíces de $p(x)$. Cuerpo que denominaremos cuerpo de descomposición de $p(x)$, que es una extensión de Galois de k.

6. Teorema: *Sea $k \to K$ una extensión finita separable. Las siguientes condiciones son equivalentes:*

1. *K es una extensión Galois de k.*
2. *Si $p(x) \in k[x]$ es un polinomio irreducible que tiene una raíz en K, entonces todas las raíces de $p(x)$ están en K. (Definición clásica de extensión de Galois).*
3. *("Agujero único en el cierre algebraico") Existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de K.*

Demostración. 1. $\Rightarrow$ 2. Sea K una extensión de Galois de k, y sea $p(x) \in k[x]$ un polinomio irreducible que tiene una raíz en K. Dar una raíz equivale a dar un morfismo

$$k[x]/(p(x)) \to K$$

necesariamente inyectivo, pues $k[x]/(p(x))$ es cuerpo, ya que $p(x)$ es irreducible. Tensando por K obtenemos

$$K[x]/(p(x)) = k[x]/(p(x)) \underset{k}{\otimes} K \hookrightarrow K \underset{k}{\otimes} K$$

y como $K \underset{k}{\otimes} K$ es trivial, $K[x]/(p(x))$ también, es decir $p(x)$ tiene todas sus raíces en K.

2. $\Rightarrow$ 1. $K = k[\alpha_1, \ldots, \alpha_n]$ es cociente de un producto tensorial de álgebras del tipo $k[\alpha] = k[x]/(p(x))$, con $p(x)$ irreducible y sin raíces múltiples. $K \underset{k}{\otimes} k[\alpha] = K[x]/(p(x))$ y $\alpha \in K$ es una raíz de $p(x)$. Por la hipótesis, todas las raíces de $p(x)$ están en K, luego $K \underset{k}{\otimes} k[\alpha] = K[x]/(p(x))$ es trivial. Por tanto $K \otimes_k K$ es trivial, porque es cociente de un producto tensorial de álgebras triviales.

1. $\Leftrightarrow$ 3. El cierre algebraico de k, $\bar{k}$, trivializa a K. Luego, por la proposición 4.3.7, $\#\mathrm{Hom}_{k-alg}(K,\bar{k}) = \dim_k K$. K es de Galois si y sólo K la trivializa. Por 4.3.7, K trivializa a K si y sólo si $\#\mathrm{Hom}_{k-alg}(K,K) = \dim_k K$. Por tanto, K trivializa a K si y sólo si $\mathrm{Hom}_{k-alg}(K,K) = \mathrm{Hom}_{k-alg}(K,\bar{k})$, es decir, si y sólo si existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de K.

□

7. Corolario: *Una extensión finita de cuerpos separable $k \hookrightarrow K$ es de Galois si y sólo si es el cuerpo de descomposición de un polinomio.*

Demostración. Supongamos que K es de Galois. Como K es una extensión finita, existen $\alpha_1,\dots,\alpha_n \in K$ de modo que $K = k(\alpha_1,\dots,\alpha_n)$. Sea $p_i(x)$ el polinomio mínimo anulador de α_i. Por la proposición anterior todas las raíces de $p_i(x)$ pertenecen a K. Por tanto, el cuerpo de descomposición de $p(x) = p_1(x)\cdots p_n(x)$ está incluido en K y coincide con K. □

8. Definición: Sea $p(x) \in k[x]$ un polinomio de raíces distintas y $\{\alpha_1,\dots,\alpha_n\}$ sus raíces. Diremos que $G = \mathrm{Aut}_{k-alg}\, k(\alpha_1,\dots,\alpha_n)$ es el grupo de Galois de $p(x)$.

Observemos que todo $g \in G = \mathrm{Aut}_{k-alg}\, k(\alpha_1,\dots,\alpha_n)$ queda determinado por los valores $g(\alpha_1),\dots,g(\alpha_n)$ y que además g ha de permutar las raíces de $p(x)$. Es decir, podemos pensar G como un subgrupo del grupo de permutaciones de las raíces de $p(x)$.

Sea k un cuerpo y $a_1,\dots,a_n$ variables libres. Consideremos el cuerpo $k(a_1,\dots,a_n)$, y el polinomio con coeficientes en este cuerpo:

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

que se denomina *polinomio general de grado n sobre k*.

Las raíces $\alpha_1,\dots,\alpha_n$ del ecuación general de grado n son algebraicamente independientes: Dado $0 \neq f(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$, entonces $0 \neq \prod_{\sigma\in S_n} f(x_{\sigma(1)},\dots,x_{\sigma(n)}) = q(s_1,\dots,s_n)$ por el teorema fundamental de las funciones simétricas. Por tanto, $0 \neq q(-a_1,\dots,(-1)^n a_n) = \prod_{\sigma\in S_n} f(\alpha_{\sigma(1)},\dots,\alpha_{\sigma(n)})$ y $f(\alpha_1,\dots,\alpha_n) \neq 0$.

El cuerpo de descomposición de $p(x)$ es $k(a_1,\dots,a_n)(\alpha_1,\dots,\alpha_n) = k(\alpha_1,\dots,\alpha_n)$. El grupo de Galois de $p(x)$ es un subgrupo de S_n. Por otra parte, S_n opera en $k(\alpha_1,\dots,\alpha_n)$ de modo natural permutando las α_i, que son automorfismos de $k(a_1,\dots,a_n)$-álgebras. Luego, *el grupo del polinomio general de grado n es* S_n.

4.4.1. Extensiones ciclotómicas

Sea

$$\mu_n := \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i\,sen\,\frac{2k\pi}{n} \in \mathbb{C},\ 0 \le k < n\},$$

el conjunto de todas las raíces n-ésimas de la unidad, que es un subgrupo (multiplicativo) de $\mathbb{C}^*$, de orden n.

El morfismo, $\mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{m} \mapsto e^{m\cdot 2\pi i/n}$ es un isomorfismo de grupos. Vía este isomorfismo, el conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con el conjunto $R_n \subset \mu_n$, de todas las raíces n-ésimas primitivas de la unidad ($R_n = \{\varepsilon \in \mu_n$ tales que $\varepsilon^m \neq 1$ para cada $m < n\}$). El conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con los invertibles de $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} \in \mathbb{Z}/n\mathbb{Z},\ m.c.d.(m,n) = 1\}$. Luego,

$$R_n = \{e^{m\cdot 2\pi i/n} = cos\,\frac{2m\pi}{n} + i\,sen\,\frac{2m\pi}{n},\ \text{con}\ \ 0 < m < n \text{ y } m.c.d.(m,n) = 1\}$$

9. Definición: Para cada $n \in \mathbb{N}$ se denomina n-ésimo *polinomio ciclotómico* al polinomio mónico

$$\Phi_n(x) = \prod_{m<n,\, m.c.d.(m,n)=1} (x - e^{m\cdot 2\pi i/n})$$

Una raíz n-ésima de la unidad es primitiva si y sólo si no es d-ésima para ningún divisor estricto d de n y, por tanto,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n, d|n} \Phi_d(x)}$$

luego por recurrencia se demuestra que $\Phi_n(x) \in \mathbb{Z}[x]$ (obsérvese que $\Phi_1(x) = x - 1$).

Dejamos que el lector pruebe la siguiente proposición.

10. Proposición: *Se cumple*

1. $\Phi_1(x) = x - 1$.
2. $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = x + 1$.
3. $\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = x^2 + x + 1$.
4. $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\cdot\Phi_2(x)} = x^2 + 1$.
5. $\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$.
6. $\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_3(x)} = x^2 - x + 1$.
7. *Si* $p > 0$ *es primo,* $\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = x^{p-1} + x^{p-2} + \cdots + x + 1$.
8. *Si* $p > 0$ *es primo,* $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}}) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1$. *También,* $\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}$.
9. *Si* $p > 0$ *es primo y* r *no es divisible por* p, $\Phi_{r\cdot p^n}(x) = \frac{\Phi_r(x^{p^n})}{\Phi_r(x^{p^{n-1}})}$.
10. *Si* $r > 2$ *es impar,* $\Phi_{2r}(x) = \Phi_r(-x)$.

11. Lema: *Para cada* $Q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ *se verifica la identidad:*

$$Q(x)^p = Q(x^p)$$

Demostración. Para cada $a \in \mathbb{Z}/p\mathbb{Z}$ es $a^p = a$ y $(R(x)+S(x))^p = R(x)^p + S(x)^p$, para cada $R(x), S(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, luego

$$Q(x)^p = (a_0 + a_1 x + \cdots a_n x^n)^p = a_0^p + a_1^p x^p + \cdots a_n^p (x^p)^n = Q(x^p)$$

□

12. Teorema: *Los polinomios ciclotómicos* $\Phi_n(x) \in \mathbb{Z}[x]$ *son polinomios irreducibles.*

Demostración. Sea $\Phi_n(x) = P(x)\cdot Q(x)$ con $P(x) \in \mathbb{Z}[x]$, $\mathrm{gr}P(x) > 0$. Como se sabe, si ε es una raíz primitiva de la unidad, entonces las raíces primitivas n-ésimas de la unidad son exactamente las de la forma ε^m con $m.c.d.(m,n) = 1$. Por tanto, para ver que $P(x) = \Phi_n(x)$ basta ver que si ε es raíz de $P(x)$ y p un número primo no divisor de n, entonces ε^p es también raíz de $P(x)$. Sea pues ε una raíz de $P(x)$ tal que ε^p sea raíz de $Q(x)$. Entonces, los polinomios $P(x)$ y $Q(x^p)$ que tienen en común la raíz ε, no son primos entre sí. Luego, $P(x)^p$ y $Q(x^p)$ no son primos entre sí. Entonces, en $\mathbb{Z}/p\mathbb{Z}[x]$, $\overline{P(x)^p} = \overline{P(x)}^p$ y $\overline{Q(x^p)} = \overline{Q(x)}^p$ no son primos entre sí. Luego, $\overline{P(x)}$ y $\overline{Q(x)}$ no son primos entre sí. Luego, $\overline{\Phi_n(x)} = \overline{P(x)}\cdot\overline{Q(x)}$ tiene raíces múltiples. Sin embargo, $\overline{\Phi_n(x)}$ tiene las raíces distintas, pues todas las raíces de $x^n - 1$ son distintas ya que es primo con su derivada $\bar{n}x^{n-1} \neq 0$. Hemos llegado a contradicción. □

13. Teorema: *Sea $\mathbb{Q}(e^{2\pi i/n})$ el cuerpo de descomposición de $x^n - 1$. Entonces, se cumple que*

1. $\mathbb{Q}(e^{2\pi i/n}) = \mathbb{Q}[x]/(\Phi_n(x))$.
2. *El grupo de Galois de $\mathbb{Q}(e^{2\pi i/n})$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración. 1. $\Phi_n(x)$ es un polinomio mónico irreducible en $\mathbb{Z}[x]$, luego por el teorema de Gauss es irreducible en $\mathbb{Q}[x]$. Por tanto, $\Phi_n(x)$ es el polinomio con coeficiente en $\mathbb{Q}$ mínimo anulador de $e^{2\pi i/n}$. Luego, $\mathbb{Q}[x]/(\Phi_n(x)) = \mathbb{Q}(e^{2\pi i/n})$.

2. Si $\tau \in \mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(e^{2\pi i/n}))$, entonces $\tau(e^{2\pi i/n}) = e^{k\cdot 2\pi i/n}$, para cierto $0 < k < n$, cumpliendo $m.c.d.(k,n) = 1$ y τ queda determinado por este exponente k. Es decir, el morfismo de grupos $\mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(e^{2\pi i/n})) \to (\mathbb{Z}/n\mathbb{Z})^*$, $\tau \mapsto \bar{k}$ es inyectivo. Por órdenes, ha de ser epiyectivo, luego es un isomorfismo.

□

4.4.2. Cuerpos finitos

14. Definición: Diremos que un cuerpo es finito si tiene un número finito de elementos.

Observemos que la característica de un cuerpo finito K es un número primo $p > 0$: El morfismo $\mathbb{Z} \to K$, $n \mapsto n$, no puede ser inyectivo, el núcleo ha de ser un ideal $p\mathbb{Z}$, con $p > 0$. Además, $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$, luego $\mathbb{Z}/p\mathbb{Z}$ es íntegro y p es primo.

Por tanto, K es una $\mathbb{Z}/p\mathbb{Z}$ extensión finita de cuerpos. Sea $n = \dim_{\mathbb{Z}/p\mathbb{Z}} K$, entonces K es isomorfo como espacio vectorial a $(\mathbb{Z}/p\mathbb{Z})^n$, luego

$$\#K = p^n.$$

Consideremos el grupo conmutativo $K^* = K\setminus\{0\}$ con la multiplicación. Como $\#K^* = p^n - 1$, se tiene que para todo $\alpha \in K^*$, $\alpha^{p^n-1} = 1$. Por tanto, para todo $\alpha \in K$, $\alpha^{p^n} = \alpha$. Es decir, K coincide con el conjunto de todas las raíces del polinomio de grado p^n, $x^{p^n} - x$. Polinomio que es separable. Así pues, K es el cuerpo de descomposición de $x^{p^n} - x$ y es una $\mathbb{Z}/p\mathbb{Z}$-extensión de Galois.

Hemos probado el siguiente teorema.

15. Teorema: *Sea $p > 0$ primo y $n > 0$. Entonces, sólo existe un cuerpo finito (salvo isomorfismos) de orden p^n, que denotaremos $\mathbb{F}_{p^n}$, y es precisamente el conjunto de las raíces (en el cierre algebraico de $\mathbb{F}_p$) del polinomio $x^{p^n} - x$. Luego, $\mathbb{F}_{p^n}$ es el cuerpo de descomposición de $x^{p^n} - x$, y los cuerpos finitos son extensiones de Galois de $\mathbb{F}_p$.*

16. Proposición: $\mathbb{F}_{p^n}^* := \mathbb{F}_{p^n} \setminus \{0\}$ *es un grupo (multiplicativo) cíclico.*

Demostración. Basta ver que existe $\alpha \in \mathbb{F}_{p^n}^*$ de orden $p^n - 1$. Basta ver que el anulador del grupo conmutativo (multiplicativo) $\mathbb{F}_{p^n}^*$ es $p^n - 1$. Sea d el anulador de $\mathbb{F}_{p^n}^*$. Se verifica que d es un divisor de $p^n - 1$ y que $\alpha^d = 1$, para todo $\alpha \in \mathbb{F}_{p^n}^*$. Por tanto, $\mathbb{F}_{p^n}^*$ es un subconjunto del conjunto de raíces de $x^d - 1$, luego

$$\#\mathbb{F}_{p^n} \leq d + 1 \leq p^n$$

y por tanto $d = p^n - 1$. □

17. Corolario: *Toda extensión finita de cuerpos $k \hookrightarrow K$ separable es primitiva.*

Demostración. Si k tiene infinitos elementos, este corolario es un caso particular del teorema 4.3.9. Si k es un cuerpo finito, entonces K también lo es y sabemos que $K \setminus \{0\}$ es un grupo multiplicativo cíclico, generado por cierto $\alpha \in K$. Por tanto, $K = k[\alpha]$.

□

18. Definición: Sea K un cuerpo de característica $p > 0$. Llamaremos *automorfismo de Frobenius* al automorfismo de $\mathbb{F}_p$-álgebras

$$F : K \to K$$

definido por $F(\lambda) = \lambda^p$.

19. Teorema: *Sea $k \to K$ una extensión finita entre cuerpos finitos. Sea $k = \mathbb{F}_{p^n}$. El grupo de automorfismos,* $\mathrm{Aut}_{k-alg} K$*, es un grupo cíclico generado por la potencia n-ésima del automorfismo de Frobenius,*

$$\mathrm{Aut}_{k-alg} K = < F^n >$$

Demostración. F sobre $k = \mathbb{F}_{p^n}$ es un automorfismo de orden n (para todo n). Si K es una k-extensión de grado m, $\#K = (\#k)^m = p^{nm}$. Entonces $K = \mathbb{F}_{p^{nm}}$. El orden de F^n (como automorfismo de K) es m, por tanto

$$\#\langle F^n \rangle = m = \dim_k K$$

Por tanto, K es una extensión de Galois de grupo $\langle F^n \rangle$.

□

4.5. Equivalencia clásica de Galois

1. Proposición: *Sea $k \hookrightarrow K$ una extensión de Galois y $K' \subseteq K$ una k-subextensión. Entonces, $K' \hookrightarrow K$ es una extensión de Galois.*

Demostración. K es una K'-extensión de Galois, porque $K \otimes_{K'} K$ es una K-álgebra trivial, porque es cociente de la K-álgebra trivial $K \otimes_k K$ (considérese el epimorfismo $K \otimes_k K \to K \otimes_{K'} K, a \otimes b \mapsto a \otimes b$). □

2. Teorema de Artin: *Sea K una k-extensión de Galois de grupo G. Entonces,*

$$\boxed{K^G = k}$$

Demostración. K es una K^G-extensión de Galois de grupo G. Entonces,

$$\dim_{K^G} K = \#G = \dim_k K = \dim_k K^G \cdot \dim_{K^G} K$$

Luego, $\dim_k K^G = 1$ y $K^G = k$. □

3. Teorema: *Sea K una k-extensión de Galois de grupo de automorfismos G, $K' \subseteq K$ una k-subextensión y $H := \mathrm{Aut}_{K'-alg}(K) \subseteq \mathrm{Aut}_{k-alg}(K) = G$. Entonces, $K' = K^H$.*

Demostración. $K' \hookrightarrow K$ es una extensión de Galois de grupo H. Por el teorema de Artin, $K' = K^H$.

□

4. Proposición: *Sea $k \hookrightarrow K$ una extensión finita de Galois de grupo G, $\alpha \in K$ y $H := \{h \in G : h(\alpha) = \alpha\}$ el subgrupo de isotropía de α. El polinomio mínimo anulador de α con coeficientes en k, es el polinomio*

$$p(x) = \prod_{\bar{g} \in G/H} (x - g(\alpha))$$

En particular, G opera transitivamente[1] *sobre el conjunto de las raíces de $p(x)$.*

Demostración. Consideremos la operación natural de G en $K[x]$,

$$g(\sum_i a_i x^i) := \sum_i g(a_i) x^i, \text{ para cada } g \in G. \text{ y } \sum_i a_i x^i \in K[x]$$

Por el teorema de Artin, un polinomio $q(x) \in K[x]$ es invariante por G si y sólo si $q(x) \in k[x]$. Observemos que si $q(x) = (x - a_1) \cdots (x - a_n)$, con $a_1, \ldots, a_n \in K$, entonces $g(q(x)) = (x - g(a_1)) \cdots (x - g(a_n))$. Observemos que $G \cdot \alpha = \{g(\alpha), \bar{g} \in G/H\}$ y $g(\alpha) \neq g'(\alpha)$ si $\bar{g} \neq \overline{g'}$. Además, $G \cdot \alpha = g' \cdot G \cdot \alpha = \{g'(g(\alpha)), \bar{g} \in G/H\}$, por tanto, $g'(p(x)) = p(x)$, para todo $g' \in G$, porque tienen las mismas raíces. Luego, $p(x) \in k[x]$.

El polinomio $p(x)$ anula a α. Si $\alpha \in K$ es una raíz de un polinomio irreducible $q(x) \in k[x]$, entonces $g(\alpha)$ es una raíz de $g(q(x)) = q(x)$, para todo $g \in G$. Por tanto, el polinomio mínimo anulador de α es $p(x)$. □

[1] Sea X un G-conjunto. Se dice que G opera transitivamente sobre X si X es una sola órbita, es decir, para toda pareja $x, x' \in X$ existe un $g \in G$ de modo que $x' = gx$. Diremos que un subgrupo de permutaciones $G \subset S_n = Biy\{1, \ldots, n\}$ es transitivo si opera transitivamente en $\{1, \ldots, n\}$.

5. Teorema: *Sea K una k-extensión finita de cuerpos y $G \subseteq \mathrm{Aut}_{k-alg}(K)$ un subgrupo. Entonces, K es una K^G-extensión de Galois de grupo G.*

Demostración. Dado $a \in K$, sea $G \cdot a = \{g(a), g \in G\} = \{a_1, \ldots, a_n, a_i \neq a_j \text{ si } i \neq j\}$. Observemos que G opera en $\{a_1, \ldots, a_n\}$ permutando $a_1, \ldots, a_n$. Entonces, el polinomio $\prod_{i=1}^{n}(x - a_i) \in K^G[x]$ anula a a y es de grado menor que $\#G$. Por tanto, a es separable y K es una K^G-extensión de cuerpos separable. Además, por el teorema del elemento primitivo, existe $b \in K$ tal que $K^G[b] = K$, luego $\dim_{K^G} K \leq \#G$. Por tanto, $\dim_{K^G} K \leq \#G \leq Aut_{K^G-alg}(K)$, entonces las desigualdades son igualdades y K es una K^G-extensión de Galois de grupo G.

□

6. Teorema clásico de Galois: *Sea K una k-extensión de Galois de grupo G. La asignación*

$$[\textit{Conj. de subgrupos de } G] \to [\textit{Conj. de } k\textit{-subextensiones de } K],\ H \mapsto K^H$$

es biyectiva, cuya asignación inversa es

$$[\textit{Conj. de } k\textit{-subextensiones de } K] \to [\textit{Conj. de subgrupos de } G],\ K' \mapsto \mathrm{Aut}_{K'-alg}(K).$$

Observemos que $\mathrm{Aut}_{K'-alg}(K) = \{g \in G : g(a) = a, \textit{ para todo } a \in K'\}$.

Demostración. Las asignaciones son inversas entre sí por 4.5.3 y 4.5.5.

□

7. Corolario: *Sea K una k-extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. Entonces, K^H es una k-extensión de Galois si y sólo si H es normal en G. Por lo tanto, en el teorema clásico de Galois, el conjunto de k-subextensiones de Galois de K se corresponde biunívocamente con el conjunto de los subgrupos normales de G.*

Además, si K^H es una k-extensión de Galois, su grupo de Galois es G/H.

Demostración. Dado $g \in G$ es fácil comprobar que $g(K^H) = K^{gHg^{-1}}$.

Si K^H es una k-extensión de Galois, por el teorema de hueco único $g(K^H) = K^H$, luego $K^{gHg^{-1}} = K^H$ y $gHg^{-1} = H$. Es decir, H es normal en G.

Si H es normal en G, entonces $g(K^H) = K^{gHg^{-1}} = K^H$. Tenemos $(K^H)^{G/H} = (K^H)^G = k$, luego K^H es una k-extensión de Galois de grupo G/H.

□

8. Teorema de los irracionales naturales de Lagrange: *Sea $k \hookrightarrow K$ una extensión de Galois y $k \hookrightarrow L$ una extensión de cuerpos y consideremos un compuesto $L \cdot K$, que es una L-extensión de Galois. Entonces,* $\mathrm{Aut}_{L-alg}(L \cdot K) = \mathrm{Aut}_{L \cap K-alg}(K)$.

Demostración. K es el cuerpo de descomposición de un cierto polinomio separable $p(x) \in k[x]$, luego $L \cdot K$ es el cuerpo de descomposición del polinomio $p(x) \in L[x]$ y es una L-extensión de Galois.

Consideremos la inclusión $G' := \mathrm{Aut}_{L-alg}(L \cdot K) \hookrightarrow \mathrm{Aut}_{k-alg} K$, $g' \mapsto g'_{|K}$. Observemos que $K^{G'} = (K \cdot L)^{G'} \cap K = L \cap K$. Luego, G' se identifica con $\mathrm{Aut}_{L \cap K-alg}(K)$. □

9. Teorema de prolongación: *Sea K una k-extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. Entonces, la aplicación*

$$G/H \to \mathrm{Hom}_{k-alg}(K^H, K), \bar{g} \mapsto g_{|K^H}$$

es biyectiva.

Demostración. Dados $g, g' \in G$, se cumple que $g_{|K^H} = g'_{|K^H}$ si y sólo si $(gg'^{-1})_{|K^H} = \mathrm{Id}$, es decir, $gg'^{-1} \in \mathrm{Aut}_{K^H-alg}(K) = H$, o equivalentemente, $\bar{g} = \bar{g}'$ en G/H. Por tanto, la aplicación $G/H \to \mathrm{Hom}_{k-alg}(K^H, K)$, $\bar{g} \mapsto g_{|K^H}$ es inyectiva.

K trivializa a K^H, porque trivializa a K, luego

$$\#\mathrm{Hom}_{k-alg}(K^H, K) = \dim_k K^H = \dim_k K / \dim_{K^H} K = \#G/\#H$$

Por tanto, la aplicación inyectiva $G/H \to \mathrm{Hom}_{k-alg}(K^H, K)$, $\bar{g} \mapsto g_{|K^H}$ es biyectiva.

□

4.6. Equivalencia categorial de Galois

1. Definición: Dar una categoría $\mathscr{C}$ es dar

1. Una familia arbitraria, cuyos elementos llamaremos objetos de $\mathscr{C}$.
2. Unos conjuntos $\mathrm{Hom}_{\mathscr{C}}(M, N)$, para cada par de objetos M, N de $\mathscr{C}$, cuyos elementos f llamaremos morfismos de M en N y denotaremos por el símbolo $f : M \to N$.
3. Una aplicación

$$\mathrm{Hom}_{\mathscr{C}}(N, P) \times \mathrm{Hom}_{\mathscr{C}}(M, N) \to \mathrm{Hom}_{\mathscr{C}}(M, P), \quad (f, g) \mapsto f \circ g$$

para cada terna M, N, P de objetos de $\mathscr{C}$. Satisfaciéndose

a) $(f \circ g) \circ h = f \circ (g \circ h)$.

b) Para cada objeto M de $\mathscr{C}$, existe un morfismo $\mathrm{Id}_M : M \to M$ de modo que $f \circ \mathrm{Id}_M = f$ e $\mathrm{Id}_M \circ g = g$ para todo morfismo $f : M \to N$ y $g : N \to M$.

Un morfismo $f : M \to N$ se dice que es un isomorfismo si existe $g : N \to M$ de modo que $f \circ g = \mathrm{Id}_N$ y $g \circ f = \mathrm{Id}_M$.

2. Ejemplos:

1. La categoría $\mathscr{C}_{Conj}$ de conjuntos finitos, es la categoría cuyos objetos son los conjuntos finitos y los morfismos entre los objetos son las aplicaciones de conjuntos.
2. La categoría $\mathscr{C}_{Top}$ de espacios topológicos, es la categoría cuyos objetos son los espacios topológicos y los morfismos entre los objetos son las aplicaciones continuas.
3. La categoría $\mathscr{C}_{Mod}$ de A-módulos, es la categoría cuyos objetos son los A-módulos y los morfismos entre los objetos son los morfismos de módulos.

4. La categoría $\mathscr{C}_{AlgTrv}$ de k-álgebras finitas triviales, es la categoría cuyos objetos son las k-álgebras finitas triviales y los morfismos entre objetos son los morfismos de k-álgebras.

5. Sea G un grupo. La categoría C_{G-conj} de G-conjuntos finitos, es la categoría cuyos objetos son los G-conjuntos finitos y los morfismos entre los objetos son los morfismos de G-conjuntos.

3. Definición: Sean $\mathscr{C}$ y $\mathscr{C}'$ dos categorías. Dar un funtor covariante $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$ es asignar a cada objeto M de $\mathscr{C}$ un objeto $F(M)$ de $\mathscr{C}'$, y cada morfismo $f: M \to N$ de $\mathscr{C}$ un morfismo $F(f): F(M) \to F(N)$ de $\mathscr{C}'$, de modo que se verifique que $F(f \circ g) = F(f) \circ F(g)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Análogamente se definen los funtores contravariantes $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$, que asignan a cada objeto M de $\mathscr{C}$ un objeto $F(M)$ de $\mathscr{C}'$, y a cada morfismo $f: M \to N$ de $\mathscr{C}$ un morfismo $F(f): F(N) \to F(M)$ de $\mathscr{C}'$, de modo que verifica $F(f \circ g) = F(g) \circ F(f)$ y $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

4. Definición: Sean $F, F': \mathscr{C} \rightsquigarrow \mathscr{C}'$ dos funtores covariantes (o contravariantes). Dar un isomorfismo $\theta: F \to F'$, es dar para cada objeto M de $\mathscr{C}$ un isomorfismo $\theta_M: F(M) \to F'(M)$, de modo que para cada morfismo $f: M \to N$ el diagrama

$$\begin{array}{ccc} F(M) & \xrightarrow{F(f)} & F(N) \\ \downarrow{\scriptstyle \theta_M} & & \downarrow{\scriptstyle \theta_N} \\ F'(M) & \xrightarrow{F'(f)} & F'(N) \end{array}$$

es conmutativo.

5. Definición: Diremos que dos categorías $\mathscr{C}$ y $\mathscr{C}'$ son equivalentes (respectivamente, anti-equivalentes) si existen dos funtores covariantes (respectivamente, contravariantes) $F: \mathscr{C} \rightsquigarrow \mathscr{C}'$ y $F': \mathscr{C}' \rightsquigarrow \mathscr{C}$ tales que $F \circ F'$ es isomorfo al funtor identidad Id y $F' \circ F$ es isomorfo al functor identidad Id.

6. Teorema: *La categoría de las k-álgebras finitas triviales, $\mathscr{C}_{AlgTrv}$, es anti-equivalente a la categoría de conjuntos finitos, $\mathscr{C}_{Conj}$. Los functores que dan la anti-equivalencia son $F: \mathscr{C}_{Conj} \rightsquigarrow \mathscr{C}_{AlgTrv}$, donde $F(X) := \mathrm{Aplic}(X, k)$, para cada conjunto finito X y $F': \mathscr{C}_{AlgTrv} \rightsquigarrow \mathscr{C}_{Conj}$, donde $F'(A) := \mathrm{Hom}_{k-alg}(A, k)$, para cada k-álgebra trivial A.*

Demostración. Tenemos que probar que existen isomorfismo $\mathrm{Id} \overset{\theta}{\simeq} F \circ F'$ y que $\mathrm{Id} \overset{\theta'}{\simeq} F' \circ F$.

El morfismo natural $\theta_A: A \to (F \circ F')(A) = \mathrm{Aplic}(\mathrm{Hom}_{k-alg}(A, k), k)$, $\theta_A(a) := \tilde{a}$, con $\tilde{a}(\phi) := \phi(a)$, para cada $\phi \in \mathrm{Hom}_{k-alg}(A, k)$. θ_A es inyectivo: Dados $a = (\lambda_1, \ldots, \lambda_n) \in k^n = A$ y $a' = (\lambda'_1, \ldots, \lambda'_n) \in k^n = A$, si $a \neq a'$, existe i, tal que $\lambda_i \neq \lambda'_i$. Sea $\phi_i: A = k^n \to k$, definido por $\phi_i(\mu_1, \ldots, \mu_n) := \mu_i$. Entonces, $\theta_A(a)(\phi_i) = \lambda_i \neq \lambda'_i = \theta_A(a')(\phi_i)$, luego $\theta_A(a) \neq \theta_A(a')$. Por dimensiones, θ_A es un isomorfismo.

En conclusión, $\mathrm{Id} \overset{\theta}{\simeq} F \circ F'$.

El morfismo natural $\theta'_X: X \to (F' \circ F)(X) = \mathrm{Hom}_{k-alg}(\mathrm{Aplic}(X, k), k)$, $\theta'_X(x) := \tilde{x}$, donde $\tilde{x}(f) := f(x)$, para cada $f \in \mathrm{Aplic}(X, k)$. θ'_X es una aplicación inyectiva: Dados $x \neq x' \in X$, sea $f: X \to k$ la aplicación nula en todo punto, salvo en x donde $f(x) = 1$.

Entonces, $\theta'_X(x)(f) = f(x) = 1 \neq 0 = f(x') = \theta'_X(x')(f)$, luego $\theta'_X(x) \neq \theta'_X(x')$. Por órdenes, θ'_X es una biyección.

En conclusión, $\mathrm{Id} \overset{\theta'}{\simeq} F' \circ F$.

□

7. Definición: Sea K una k-extensión de Galois de grupo G. G opera en K de modo obvio. Diremos que una K-álgebra B es una GK-álgebra si G opera en B (como morfismos de anillos) de modo que

$$g(\lambda \cdot b) = g(\lambda) \cdot g(b), \quad \forall\, g \in G, \lambda \in K \text{ y } b \in B$$

Diremos que una aplicación $f : B \to B'$ entre GK-álgebras es un morfismo de GK-álgebras si f es un morfismo de K-álgebras y de G-conjuntos.

La categoría cuyos objetos son las GK-álgebras que sean K-álgebras finitas triviales y cuyos morfismos son los morfismos de GK-álgebras la denotaremos $\mathscr{C}_{G-AlgTrv}$.

8. Teorema: *Sea K una k-extensión de Galois de grupo G. La categoría de las GK-álgebras finitas triviales, $\mathscr{C}_{GK-Trv}$ es anti-equivalente a la categoría de G-conjuntos finitos, $\mathscr{C}_{G-Conj}$. Los funtores que dan la anti-equivalencia son*

$$F : \mathscr{C}_{G-Conj} \rightsquigarrow \mathscr{C}_{GK-Trv},\ F(X) := \mathrm{Aplic}(X, K),$$

donde G opera en $\mathrm{Aplic}(X,K)$ como sigue: $(g \cdot f)(x) := g \cdot (f(g^{-1} \cdot x))$, para toda $g \in G$, $f \in \mathrm{Aplic}(X,K)$ y $x \in X$; y

$$F' : \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{G-Conj},\ F'(A) := \mathrm{Hom}_{K-alg}(A, K),$$

donde G opera en $\mathrm{Hom}_{K-alg}(A,K)$ como sigue: $(g \cdot \phi)(a) := g \cdot (\phi(g^{-1} \cdot a))$, para toda $a \in A$, $g \in G$ y $\phi \in \mathrm{Hom}_{K-alg}(A,K)$.

Demostración. Ya hemos probado en 4.6.6 que $F \circ F'$ y $F' \circ F$ son isomorfos al functor identidad.

□

9. Lema: *Sea E un k-espacio vectorial, $G \subseteq \mathrm{Aut}_{k-lin}(E)$ un grupo de automorfismos lineales de E y E' una k-espacio vectorial. Entonces,*

$$(E \otimes_k E')^G = E^G \otimes_k E'.$$

Demostración. $E' = \oplus_I k$ como k-espacio vectorial. Es fácil comprobar que

$$(E \otimes_k E')^G = (E \otimes_k (\oplus_I k))^G = (\oplus_I E)^G = \oplus_I E^G = E^G \otimes_k E'$$

□

10. Lema: *Sea K una k-extensión de Galois de grupo G. Si B es una GK-álgebra finita. Entonces, el morfismo natural*

$$B^G \otimes_k K \to B,\ b \otimes \lambda \mapsto b \cdot \lambda,$$

es un isomorfismo.

Demostración. $B\otimes_k K = B\otimes_K(K\otimes_k K) = B\otimes_K \prod^G K = \prod^G B$. La operación de G en $B\otimes_k K$ en el primer factor se traduce en $\prod^G B$ en la operación de G en G (por la izquierda) y la operación natural en cada factor B. Como $(\prod^G B)^G = \{(g(b))_{g\in G} \in \prod^G B, \text{ con } b\in B\} = B$, entonces

$$B^G \otimes_k K = (B\otimes_k K)^G = (\prod^G B)^G = B$$

□

11. Teorema: *Sea K una k-extensión de Galois de grupo G. La categoría de las GK-álgebras finitas triviales, $\mathscr{C}_{GK-Trv}$ es equivalente a la categoría de k-álgebras finitas trivializadas por K, $\mathscr{C}_{K/k}$. Los funtores que dan la anti-equivalencia son*

$$H\colon \mathscr{C}_{K/k} \rightsquigarrow \mathscr{C}_{GK-Trv},\ H(A) := A\otimes_k K,$$

donde G opera en $\mathrm{Aplic}(X,K)$ *como sigue:* $(g\cdot f)(x) := g\cdot(f(g^{-1}\cdot x))$*, para toda $g\in G$, $f\in \mathrm{Aplic}(X,K)$ y $x\in X$; y*

$$H'\colon \mathscr{C}_{GK-Trv} \rightsquigarrow \mathscr{C}_{K/k},\ H'(B) = B^G$$

donde G opera en $\mathrm{Hom}_{K-alg}(A,K)$ *como sigue:* $(g\cdot\phi)(a) := g\cdot(\phi(g^{-1}\cdot a))$*, para toda $a\in A$, $g\in G$ y $\phi\in \mathrm{Hom}_{K-alg}(A,K)$.*

Demostración. $H'\circ H \simeq \mathrm{Id}$, porque $K^G = k$ y por el lema 4.6.9. $H\circ H' \simeq \mathrm{Id}$ por el lema 4.6.10 □

12. Teorema de Galois: *Sea $k\hookrightarrow K$ una extensión de Galois de grupo G. Denotemos $C_{K/k}$ la categoría de k-álgebras finitas trivializadas por K, y por C_{G-conj} la categoría de G-conjuntos finitos. Los funtores*

$$\begin{aligned} P&\colon C_{K/k} \rightsquigarrow C_{G-conj} \quad P(A) := \mathrm{Hom}_{k-alg}(A,K)\\ \bar{P}&\colon C_{G-conj} \rightsquigarrow C_{K/k} \quad \bar{P}(Z) := \mathrm{Hom}_G(Z,K)\end{aligned}$$

establecen una anti-equivalencia entre las categorías $C_{K/k}$ y C_{G-conj}.

Demostración. Tenemos las equivalencias

$$\begin{aligned} \mathscr{C}_{K/k} &\overset{H}{\rightsquigarrow} \mathscr{C}_{GK-Trv} \overset{F'}{\rightsquigarrow} \mathscr{C}_{G-conj}\\ \mathscr{C}_{K/k} &\overset{H'}{\leftsquigarrow} \mathscr{C}_{GK-Trv} \overset{F}{\leftsquigarrow} \mathscr{C}_{G-conj}\end{aligned}$$

Observemos que $F'\circ H = P$, porque

$$(F'\circ H)(A) = F'(A\otimes_k K) = \mathrm{Hom}_{K-alg}(A\otimes_k K, K) = \mathrm{Hom}_{k-alg}(A,K) = P(A),$$

y que $H'\circ F = \bar{P}$, porque $(H'\circ F)(X) = H'(\mathrm{Aplic}(X,K)) = \mathrm{Aplic}(X,K)^G = \mathrm{Hom}_G(X,K) = P(X)$. Recordemos que si X e Y son dos G-conjuntos y consideramos la operación de G en $\mathrm{Aplic}(X,Y)$ definida por $(g\cdot f)(x) = g\cdot(f(g^{-1}\cdot x))$, para toda $g\in G$, $f\in\mathrm{Aplic}(X,Y)$ y $x\in X$, entonces

$$\mathrm{Aplic}(X,Y)^G = \mathrm{Hom}_G(X,Y)$$

□

13. Corolario : *Sea K una k-extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. Entonces,*

$$\mathrm{Aut}_{k-alg}(K^H) = N(H)/H$$

Demostración. $\mathrm{Aut}_{k-alg}(K^H) = \mathrm{Hom}_{k-alg}(K^H, K^H) = \mathrm{Hom}_G(G/H, G/H) = N(H)/H.$

□

4.7. Biografía de Galois

GALOIS BIOGRAPHY

Evariste Galois' father Nicholas Gabriel Galois and his mother Adelaide Marie Demante were both intelligent and well educated in philosophy, classical literature and religion. However there is no sign of any mathematical ability in any of Galois' family. His mother served as Galois' sole teacher until he was 12 years old. She taught him Greek, Latin and religion where she imparted her own scepticism to her son. Galois' father was an important man in the community and in 1815 he was elected mayor of Bourg-la-Reine.

The starting point of the historical events which were to play a major role in Galois' life is surely the storming of the Bastille on 14 July 1789. From this point the monarchy of Louis 16th was in major difficulties as the majority of Frenchmen composed their differences and united behind an attempt to destroy the privileged establishment of the church and the state.

Despite attempts at compromise Louis 16th was tried after attempting to flee the country. Following the execution of the King on 21 January 1793 there followed a reign of terror with many political trials. By the end of 1793 there were 4595 political prisoners held in Paris. However France began to have better times as their armies, under the command of Napoleon Bonaparte, won victory after victory.

Napoleon became first Consul in 1800 and then Emperor in 1804. The French armies continued a conquest of Europe while Napoleon's power became more and more secure. In 1811 Napoleon was at the height of his power. By 1815 Napoleon's rule was over. The failed Russian campaign of 1812 was followed by defeats, the Allies entering Paris on 31 March 1814. Napoleon abdicated on 6 April and Louis XVIII was installed as King by the Allies. The year 1815 saw the famous one hundred days. Napoleon entered Paris on March 20, was defeated at Waterloo on 18 June and abdicated for the second time on 22 June. Louis XVIII was reinstated as King but died in September 1824, Charles X becoming the new King.

Galois was by this time at school. He had enrolled at the Lycée of Louis-le-Grand as a boarder in the 4 th class on 6 October 1823. Even during his first term there was a minor rebellion and 40 pupils were expelled from the school. Galois was not involved and during 1824-25 his school record is good and he received several prizes. However in 1826 Galois was asked to repeat the year because his work in rhetoric was not up to the required standard.

February 1827 was a turning point in Galois' life. He enrolled in his first mathematics class, the class of M. Vernier. He quickly became absorbed in mathematics and his director of studies wrote

It is the passion for mathematics which dominates him, I think it would be best for him if his parents would allow him to study nothing but this, he is wasting his time here and does nothing but torment his teachers and overwhelm himself with punishments.

Galois' school reports began to describe him as singular, bizarre, original and closed. It is interesting that perhaps the most original mathematician who ever lived should be criticised for being original. M. Vernier reported however

Intelligence, marked progress but not enough method.

In 1828 Galois took the examination of the École Polytechnique but failed. It was the leading University of Paris and Galois must have wished to enter it for academic reasons. However, he also wished to enter this school because of the strong political movements that existed among its students, since Galois followed his parents example in being an ardent republican.

Back at Louis-le-Grand, Galois enrolled in the mathematics class of Louis Richard. However he worked more and more on his own researches and less and less on his schoolwork. He studied Legendre's Géométrie and the treatises of Lagrange. As Richard was to report:

This student works only in the highest realms of mathematics.

In April 1829 Galois had his first mathematics paper published on continued fractions in the Annales de mathématiques. On 25 May and 1 June he submitted articles on the algebraic solution of equations to the Académie des Sciences. Cauchy was appointed as referee of Galois' paper.

Tragedy was to strike Galois for on 2 July 1829 his father committed suicide. The priest of Bourg-la-Reine forged Mayor Galois' name on malicious forged epigrams directed at Galois' own relatives. Galois' father was a good natured man and the scandal that ensued was more than he could stand. He hanged himself in his Paris apartment only a few steps from Louis-le-Grand where his son was studying. Galois was deeply affected by his father's death and it greatly influenced the direction his life was to take.

A few weeks after his father's death, Galois presented himself for examination for entry to the École Polytechnique for the second time. For the second time he failed, perhaps partly because he took it under the worst possible circumstances so soon after his father's death, partly because he was never good at communicating his deep mathematical ideas. Galois therefore resigned himself to enter the École Normale, which was an annex to Louis-le-Grand, and to do so he had to take his Baccalaureate examinations, something he could have avoided by entering the École Polytechnique.

He passed, receiving his degree on 29 December 1829. His examiner in mathematics reported:

This pupil is sometimes obscure in expressing his ideas, but he is intelligent and shows a remarkable spirit of research.

His literature examiner reported:

This is the only student who has answered me poorly, he knows absolutely nothing. I was told that this student has an extraordinary capacity for mathematics. This astonishes me greatly, for, after his examination, I believed him to have but little intelligence.

Galois sent Cauchy further work on the theory of equations, but then learned from Bulletin de Férussac of a posthumous article by Abel which overlapped with a part of his work. Galois then took Cauchy's advice and submitted a new article On the condition that an equation be soluble by radicals in February 1830. The paper was sent to Fourier, the secretary of the Paris Academy, to be considered for the Grand Prize in mathematics. Fourier died in April 1830 and Galois' paper was never subsequently found and so never considered for the prize.

Galois, after reading Abel and Jacobi's work, worked on the theory of elliptic functions and abelian integrals. With support from Jacques Sturm, he published three papers in Bulletin de Férussac in April 1830. However, he learnt in June that the prize of the Academy would be awarded the Prize jointly to Abel (posthumously) and to Jacobi, his own work never having been considered.

July 1830 saw a revolution. Charles 10th fled France. There was rioting in the streets of Paris and the director of École Normale, M. Guigniault, locked the students in to avoid them taking part. Galois tried to scale the wall to join the rioting but failed. In December 1830 M. Guigniault wrote newspaper articles attacking the students and Galois wrote a reply in the Gazette des Écoles, attacking M. Guigniault for his actions in locking the students into the school. For this letter Galois was expelled and he joined the Artillery of the National Guard, a Republican branch of the militia. On 31 December 1830 the Artillery of the National Guard was abolished by Royal Decree since the new King Louis-Phillipe felt it was a threat to the throne.

Two minor publications, an abstract in Annales de Gergonne (December 1830) and a letter on the teaching of science in the Gazette des Écoles (2 January 1831) were the last publications during his life. In January 1831 Galois attempted to return to mathematics. He organised some mathematics classes in higher algebra which attracted 40 students to the first meeting but after that the numbers quickly fell off. Galois was invited by Poisson to submit a third version of his memoir on equation to the Academy and he did so on 17 January.

On 18 April Sophie Germain wrote a letter to her friend the mathematician Libri which describes Galois' situation.

.. the death of M. Fourier, have been too much for this student Galois who, in spite of his impertinence, showed signs of a clever disposition. All this has done so much that he has been expelled form École Normale. He is without money... . They say he will go completely mad. I fear this is true.

Late in 1830 19 officers from the Artillery of the National Guard were arrested and charged with conspiracy to overthrow the government. They were acquitted and on 9 May 1831 200 republicans gathered for a dinner to celebrate the acquittal. During the dinner Galois raised his glass and with an open dagger in his hand appeared to

make threats against the King, Louis-Phillipe. After the dinner Galois was arrested and held in Sainte-Pélagie prison. At his trial on 15 June his defence lawyer claimed that Galois had said

To Louis-Phillipe, if he betrays

but the last words had been drowned by the noise. Galois, rather surprisingly since he essentially repeated the threat from the dock, was acquitted.

The 14th of July was Bastille Day and Galois was arrested again. He was wearing the uniform of the Artillery of the National Guard, which was illegal. He was also carrying a loaded rifle, several pistols and a dagger. Galois was sent back to Sainte-Pélagie prison. While in prison he received a rejection of his memoir. Poisson had reported that:

His argument is neither sufficiently clear nor sufficiently developed to allow us to judge its rigour.

He did, however, encourage Galois to publish a more complete account of his work. While in Sainte-Pélagie prison Galois attempted to commit suicide by stabbing himself with a dagger but the other prisoners prevented him. While drunk in prison he poured out his soul

Do you know what I lack my friend? I confide it only to you: it is someone whom I can love and love only in spirit. I have lost my father and no one has ever replaced him, do you hear me...?

In March 1832 a cholera epidemic swept Paris and prisoners, including Galois, were transferred to the pension Sieur Faultrier. There he apparently fell in love with Stephanie-Felice du Motel, the daughter of the resident physician. After he was released on 29 April Galois exchanged letters with Stephanie, and it is clear that she tried to distance herself from the affair.

The name Stephanie appears several times as a marginal note in one of Galois' manuscripts.

Galois fought a duel with Perscheux d'Herbinville on 30 May, the reason for the duel not being clear but certainly linked with Stephanie.

I beg patriots and my friends not to reproach me for dying otherwise than for my country. I die victim of an infamous coquette. It is in a miserable brawl that my life is extinguished.

You can see a note in the margin of the manuscript that Galois wrote the night before the duel. The note reads

There is something to complete in this demonstration. I do not have the time. (Author's note).

It is this which has led to the legend that he spent his last night writing out all he knew about group theory. This story appears to have been exaggerated.

Galois was wounded in the duel and was abandoned by d'Herbinville and his own seconds and found by a peasant. He died in Cochin hospital on 31 May and his funeral

was held on 2 June. It was the focus for a Republican rally and riots followed which lasted for several days.

Galois' brother and his friend Chevalier copied his mathematical papers and sent them to Gauss, Jacobi and others. It had been Galois' wish that Jacobi and Gauss should give their opinions on his work. No record exists of any comment these men made. However the papers reached Liouville who, in September 1843, announced to the Academy that he had found in Galois' papers a concise solution

...as correct as it is deep of this lovely problem: Given an irreducible equation of prime degree, decide whether or not it is soluble by radicals.

Liouville published these papers of Galois in his Journal in 1846.

The theory that Galois outlined in these papers is now called Galois theory.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

4.8. Cuestionario

1. ¿Son reducidas las k-álgebras finitas triviales? ¿Son íntegras las k-álgebras finitas triviales?

2. ¿Son triviales las k-álgebras finitas racionales reducidas?

3. Si A es una k-álgebra finita racional, entonces ¿$A/\operatorname{rad} A$ es una k-álgebra trivial?

4. ¿Cuáles de las siguientes $\mathbb{Q}$-álgebras son triviales?:

$$\mathbb{Q}[x]/(x^3-1),\ \mathbb{Q}[x]/(x^2-1)\times\mathbb{Q}[x]/(x-1),\ \mathbb{Q}[x]/((x-1)^2\cdot(x-2)^2).$$

5. Sean A y B una k-álgebra finitas. Si $A\otimes_k B$ es k-trivial, entonces ¿A y B son k-triviales?

6. Dar un ejemplo de $\mathbb{Q}$-álgebra finita no separable.

7. Dar un ejemplo de una $\mathbb{Q}$-álgebra finita separable no trivial.

8. Sea k un cuerpo de característica $p>0$ (p primo). Dados $a,b\in k$ ¿Es $(a+b)^p = a^p+b^p$? ¿Cuántas raíces distintas tiene el polinomio $x^p-a\in k[x]$?

9. ¿Es $\mathbb{Q}[x]/(x^3-2)$ una $\mathbb{Q}$-álgebra separable?¿Es $\mathbb{F}_3[x]/(x^3-2)$ una $\mathbb{F}_3$-álgebra separable?

10. ¿Son las k-álgebras finitas separables reducidas?

11. Sea A una k-álgebra finita separable y k un cuerpo algebraicamente cerrado. ¿Es A una k-álgebra trivial?

12. Sea A una k-álgebra finita separable y k' es cierre algebraico de k ¿Es $A\otimes_k k'$ una k'-álgebra trivial?

13. Sea $A = \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt[3]{2})$. Calcular $\mathrm{Hom}_{\mathbb{Q}-alg}(\mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$ ¿Es $(\sqrt{2}, \sqrt[3]{2})$ un elemento primitivo de A?

14. ¿Es $\mathbb{Q}(\sqrt[3]{2})$ una $\mathbb{Q}$-extensión de Galois?

15. Calcular $\mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}[\sqrt{2}])$.

16. ¿Es $\mathbb{C}$ una $\mathbb{R}$-extensión de Galois?

17. ¿Es $\mathbb{Q}[e^{2\pi i/33}]$ una $\mathbb{Q}$-extensión de Galois?

18. Sea $k \hookrightarrow K$ una extensión de Galois. Sea $K \hookrightarrow \Sigma$ una extensión finita ¿Es el agujero de K en Σ único (las inclusiones de k en K y en Σ se suponen fijadas)?

19. ¿Para qué $n > 0$ es $\mathbb{Q}(\sqrt[n]{2})$ una extensión de Galois de $\mathbb{Q}$? ¿Es $\mathbb{Q}(\sqrt[4]{2})$ una extensión de Galois de $\mathbb{Q}(\sqrt{2})$?

20. ¿Es $\mathbb{Q}[\sqrt[4]{2}]$ una $\mathbb{Q}$-extensión de Galois? Dar un ejemplo de extensiones de Galois $k \to L'$ y $L' \to L$ de grado 2 tales que $k \to L$ no sea extensión de Galois.

21. Sea $n \neq m$. ¿Es $\Phi_n(x)$ primo con $\Phi_m(x)$?

22. ¿Calcular $\Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_3(x) \cdot \Phi_4 \cdot \Phi_6(x) \cdot \Phi_{12}(x)$?

23. ¿Cuál es el grado de $\Phi_{24}(x)$?

24. ¿A qué grupo abeliano es isomorfo el grupo de Galois de la $\mathbb{Q}$-extensión $\mathbb{Q}(e^{2\pi i/24})$?

25. Sean $p(x), q(x) \in \mathbb{F}_p[x]$ dos polinomios irreducibles de grado n ¿Son $\mathbb{F}_p[x]/(p(x))$ y $\mathbb{F}_p[x]/(q(x))$ cuerpos isomorfos?

26. Sea $p(x) \in \mathbb{F}_p[x]$ un polinomio sin raíces múltiples ¿Existe un $n \in \mathbb{N}$, tal que $p(x)$ divida a $x^{p^n} - x$?

27. ¿Cuántos subcuerpos distintos contiene $\mathbb{F}_{p^{10}}$?

28. ¿Calcular el grupo de Galois de la $\mathbb{F}_2$-extensión de Galois $\mathbb{F}_2[x]/(x^4 + x + 1)$?

29. ¿Cuántos subcuerpos distintos contiene $\mathbb{Q}(e^{2\pi i/9})$?

30. ¿Es $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$? Calcular el polinomio mínimo anulador de $\sqrt{2} + \sqrt{3}$ con coeficientes en $\mathbb{Q}$.

31. Calcular el polinomio mínimo anulador de $i + \sqrt{2}$ con coeficientes en $\mathbb{R}$.

32. ¿Son todas los subcuerpos de $\mathbb{Q}(e^{2\pi i/9})$ $\mathbb{Q}$-extensiones de Galois?

33. ¿Es el grupo de Galois de $x^3 - 2 \in \mathbb{Q}[x]$ isomorfo a S_3? ¿Cuántas $\mathbb{Q}$-extensiones de Galois contiene el cuerpo de descomposición de $x^3 - 2$?

4.9. Problemas

1. Si $A = \mathbb{Q}(\sqrt[3]{2})$, hallar una extensión finita L de $\mathbb{Q}$ tal que $A \otimes_{\mathbb{Q}} L = \oplus L$.

   Igualmente cuando $A = \mathbb{Q}(\sqrt[4]{2})$ y $A = \mathbb{Q}(i) \oplus \mathbb{Q}(\sqrt[3]{2})$.

2. Sean $k \hookrightarrow K$ y $K \hookrightarrow L$ extensiones finitas de cuerpos. Probar que si $k \hookrightarrow L$ es separable entonces $K \hookrightarrow L$ es separable.

3. Sea k un cuerpo de característica positiva p y sea $k \to L$ una extensión finita separable. Si $\alpha \in L$ demostrar que $k(\alpha) = k(\alpha^p)$.

4. Sea k un cuerpo de característica nula. Si A y B son dos k-álgebras finitas reducidas, probar que $A \otimes_k B$ también es una k-álgebra finita reducida.

5. Sea $k = \mathbb{F}_2(t)$ el cuerpo de las funciones racionales en una indeterminada con coeficientes en $\mathbb{F}_2$. Demostrar que polinomio $p(x) = x^2 - t$ es irreducible en $k[x]$.

   Si $\alpha = \sqrt{t}$ es una raíz de $p(x)$, probar que $x^2 - t = (x - \alpha)^2$.

   Concluir que la extensión finita $k \to k(\sqrt{t})$ no es separable.

6. Sea k un cuerpo de característica $p > 0$ y $k \hookrightarrow K$ una extensión de cuerpos de grado n. Si n es primo con p, probar que K es una k-extensión separable.

7. Demostrar que toda extensión separable $k \to L$ de grado 2 es de Galois.

   Demostrar que toda extensión de grado 2 de un cuerpo de característica distinta de 2 es una extensión de Galois.

   ¿Puede tener un cuerpo de característica 2 una extensión de Galois de grado 2?

8. Determinar los automorfismos de los cuerpos $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[5]{2})$ y $\mathbb{Q}(\sqrt[6]{2})$.

9. Determinar los automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de $x^3 - 3$. Análogamente para $x^2 - 2$, $x^4 - 4$.

10. El grupo de Galois sobre $\mathbb{C}$ de cualquier polinomio separable con coeficientes complejos es trivial: $G = 1$.

11. Si un polinomio separable con coeficientes reales tiene todas sus raíces reales, entonces su grupo de Galois sobre $\mathbb{R}$ es trivial: $G = 1$. Por el contrario, si tiene alguna raíz imaginaria, entonces su cuerpo de descomposición sobre $\mathbb{R}$ es $L = \mathbb{C}$, y su grupo de Galois es $G = \{\mathrm{id}, \tau\}$, donde τ denota la conjugación compleja.

12. Determinar cuáles de las siguientes extensiones de $\mathbb{Q}$ son de Galois y, en caso afirmativo, determinar su grupo de automorfismos:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad , \quad \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \quad , \quad \mathbb{Q}(i\sqrt{2}, \sqrt[3]{3}) \quad , \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

13. Sean $k \to L'$ y $L' \to L$ dos extensiones de Galois. Si todo automorfismo de L' sobre k puede extenderse a un automorfismo de L, probar que $k \to L$ es una extensión de Galois.

    (*Indicación:* Considerar el morfismo de restricción $\mathrm{Aut}_{k-alg}L \to \mathrm{Aut}_{k-alg}L'$.)

14. Sean $k \to L$ y $k \to L'$ dos extensiones de Galois de un mismo cuerpo k, de grupos G y G' respectivamente. Si $L \otimes_k L'$ es un cuerpo, demostrar que es una extensión de Galois de k y que su grupo de Galois es isomorfo a $G \times G'$.

15. Si $k \to L$ y $k \to L'$ son dos extensiones de Galois de un mismo cuerpo k, probar que cualquier compuesto $L'L$ también es una extensión de Galois de k. Concluir que todos los compuestos de L con L' son isomorfos, y que $L \otimes_k L'$ descompone en suma directa de extensiones de k isomorfas entre sí.

16. Sea $k \hookrightarrow K$ una extensión de cuerpos. Probar que si L y L' son k-extensiones de Galois incluidas en K, entonces $L \cap L'$ es una k-extensión de Galois ¿Depende la subextensión $L \cap L'$ de L, del cuerpo K escogido?

17. Determinar el cuerpo de descomposición L sobre $\mathbb{Q}$ del polinomio $p(x) = x^4 - 4$ y su grupo de Galois. Análogamente para el polinomio $p(x) = (x^2 - 2)(x^2 + 1)$.

18. Sea $p_2(x) = ax^2 + bx + c \in k[x]$ un polinomio separable de grado 2. Si $p_2(x)$ tiene alguna raíz en k, entonces su grupo de Galois sobre k es $G = \{\mathrm{id}\}$.

    Si $p_2(x)$ no tiene raíces en k, lo que equivale a que sea irreducible en $k[x]$, entonces su grupo de Galois sobre k es $G = S_2$.

19. Determinar el grupo de automorfismos de $\mathbb{Q}(\sqrt[8]{2}, i)$ sobre $\mathbb{Q}$. ¿Es $\mathbb{Q}(\sqrt[8]{2}, i)$ una extensión de Galois de $\mathbb{Q}$?

20. Determinar el menor subcuerpo de $\mathbb{C}$ que contenga a $\alpha = \sqrt{2} + \sqrt[3]{2}$ y sea una extensión de Galois de $\mathbb{Q}$. Calcular su grupo de Galois. Determinar el grado del polinomio irreducible de α sobre $\mathbb{Q}$.

21. Calcular el grupo de Galois del polinomio $(x^3 + 3)(x^2 + 3)$.

22. Sea k un cuerpo de característica nula y sea $k \to L$ una extensión de Galois de grupo G. Si $H = \{\tau_1, \ldots, \tau_n\}$ es un subgrupo de G, probar que es epiyectiva la aplicación k-lineal

$$s : L \to L^H \quad , \quad s(\alpha) = \tau_1(\alpha) + \ldots + \tau_n(\alpha) \, .$$

23. Hallar todos los cuerpos intermedios del cuerpo de descomposición L sobre $\mathbb{Q}$ del polinomio $x^3 - 2$. Análogamente para el polinomio $(x^2 - 2)(x^2 + 1)$ y el polinomio $x^4 - 4$.

24. Demostrar que $\sqrt{3}$ no está en la extensión $\mathbb{Q}(i, \sqrt[4]{2})$.

    Determinar un polinomio irreducible con coeficientes en $\mathbb{Q}(\sqrt{3})$ que admita la raíz $\sqrt[4]{2}$.

25. Sea $\mathbb{Q} \to L$ una extensión de Galois. Si su grupo de Galois es el grupo de Klein $K_4 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, probar que $L = \mathbb{Q}(\alpha, \beta)$, donde $\alpha^2, \beta^2 \in \mathbb{Q}$.

26. Sea $k \hookrightarrow K$ una extensión de Galois de grupo G. Sean H_1, H_2 dos subgrupos de G y denotemos $\langle H_1, H_2 \rangle \subseteq G$ el mínimo subrgupo de G que contiene a H_1 y H_2. Probar

    a) $K^{H_1} \cdot K^{H_2} = K^{H_1 \cap H_2}$.

    b) $K^{H_1} \cap K^{H_2} = K^{\langle H_1, H_2 \rangle}$.

27. Sea $k \hookrightarrow K$ una extensión de Galois de grupo G. Sean H_1, H_2 dos subgrupos de G y supongamos que H_1 es normal en G. Probar que $K^{H_1} \cdot K^{H_2}$ es una K^{H_2}-extensión de Galois de grupo $H_2/(H_1 \cap H_2)$ y que éste es un subgrupo del grupo de Galois de la k-extensión de Galois K^{H_1}.

28. Si $k \to L$ es una extensión finita separable, probar que sólo hay un número finito de cuerpos intermedios. (*Indicación:* Probarlo para la envolvente de Galois de L).

29. Sea k un cuerpo infinito. Si una extensión finita $k \to k(\alpha, \beta)$ es separable, probar que existen $a, b \in k$ tales que $k(\alpha + b\beta) = k(\alpha + a\beta)$. Concluir que $k(\alpha, \beta) = k(\alpha + a\beta)$, y que toda extensión finita separable de k está generada por un elemento.

30. Sea $k \to L$ una extensión de Galois de grado n. Si su grupo de Galois es cíclico, probar las siguientes afirmaciones:

    a) Para cada divisor d de n, existe un único cuerpo intermedio de grado d sobre k.

    b) Si L_1 y L_2 son dos cuerpos intermedios, entonces $L_1 \subseteq L_2$ si y sólo si $[L_1 : k]$ divide a $[L_2 : k]$.

31. Sea $k \to L$ una extensión de Galois de grupo G y sean K_1, K_2 dos cuerpos intermedios. Demostrar que si existe un isomorfismo de k-álgebras $f : K_1 \to K_2$, entonces existe algún automorfismo $\sigma \in G$ tal que $\sigma(K_1) = K_2$.

32. Sea $k \to L$ una extensión de Galois de grupo G y sean K_1, K_2 dos cuerpos intermedios. Demostrar que $K_1 \simeq K_2$ si y sólo si los subgrupos de G correspondientes a K_1 y K_2 son conjugados.

33. Si $k \to L'$ y $L' \to L$ son extensiones de Galois, entonces $k \to L$ es extensión de Galois:

$$L' \otimes_k L = L' \otimes_k L' \otimes_{L'} L = (\oplus L') \otimes_{L'} L = \oplus L$$
$$L \otimes_k L = L \otimes_{L'} (L' \otimes_k L) = L \otimes_{L'} (\oplus L) = \oplus (L \otimes_{L'} L) = \oplus (\oplus L)$$

    ¿Qué parte del razonamiento es falaz?

34. Sea σ el automorfismo de $\mathbb{Q}(e^{2\pi i/5})$ tal que $\sigma(e^{2\pi i/5}) = e^{8\pi i/5}$. Probar que $\mathbb{Q}(\sqrt{5})$ es el cuerpo de elementos invariantes por σ.

35. Determinar el grupo de Galois de $x^6 - 8$ sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(e^{2\pi i/3})$, $\mathbb{Q}(\sqrt[3]{2})$ y $\mathbb{Q}(\sqrt[4]{2})$.

36. Para cada automorfismo τ del cuerpo $\mathbb{Q}(e^{2\pi i/8})$, calcular el grado sobre $\mathbb{Q}$ del cuerpo de invariantes $\mathbb{Q}(e^{2\pi i/8})^\tau = \{\alpha \in \mathbb{Q}(e^{2\pi i/8}) \colon \tau(\alpha) = \alpha\}$.

    ¿Existe algún automorfismo de $\mathbb{Q}(e^{2\pi i/8})$ que sólo deje fijos los números racionales?

37. Determinar el número de extensiones de $\mathbb{Q}$ de grado 2 contenidas en $\mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 13$. Igualmente para las de grado 3.

38. Determinar todas las extensiones de $\mathbb{Q}$ contenidas en $\mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 9$.

39. Determinar los números racionales b tales que $\sqrt{b} \in \mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 9$.

40. Demostrar que $\sqrt{-3}$ no pertenece a la $\mathbb{Q}$-extensión $\mathbb{Q}(\sqrt{-2}, i)$ y concluir de ello que $\mathbb{Q}(\sqrt{-3}, \sqrt{-2}, i)$ es una $\mathbb{Q}$-extensión de Galois de $\mathbb{Q}$ de grado 8.

41. Probar que el grupo de Galois de $L = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$ tiene 7 subgrupos de orden 2, y que $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ es la única extensión real de grado 4 contenida en L. Concluir que $\sqrt[4]{3}$ no está en L y que $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 16.

42. Probar que el grupo de Galois de $L = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ tiene 11 subgrupos de orden 2, y que $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2})$ es la única extensión real de grado 8 contenida en L.

    Si $\sqrt[8]{3} \in L$, probar que $\mathbb{Q}(\sqrt{2}, i) \to L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es una extensión cíclica de grado 4 y, aplicando el teorema fundamental de las ecuaciones cíclicas, obtener la contradicción $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, i)$.

    Concluir que $\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 32.

43. Demostrar que $\mathbb{Q} \to \mathbb{Q}(\sqrt[8]{3}, i)$ no es una extensión de Galois, y que $\sqrt{2}$ no está en $\mathbb{Q}(\sqrt[8]{3}, i)$.

44. Expresar con radicales reales una raíz compleja α del polinomio $x^4 + 2$. Determinar si es cierto que $i \in \mathbb{Q}(\alpha)$ ó si $\sqrt{2} \in \mathbb{Q}(\alpha)$. Más aún, hallar todas las extensiones de $\mathbb{Q}$ de grado 2 contenidas en el cuerpo $\mathbb{Q}(\alpha)$

45. Determinar si $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ es una extensión de Galois de $\mathbb{Q}$.

46. Hallar un polinomio con coeficientes racionales $p(x)$ que no tenga raíces racionales, pero tal que cada automorfismo $\tau \in G$ de su grupo de Galois deje fija alguna raíz de $p(x)$. (*Indicación:* Elegir una extensión de Galois $\mathbb{Q} \to L$ cuyo grupo de Galois G no sea cíclico, y para cada automorfismo $\tau_i \in G$ elegir $\alpha_i \in L - \mathbb{Q}$ tal que $\tau_i(\alpha_i) = \alpha_i$. El producto de los polinomios irreducibles de estos irracionales α_i sirve).

47. Sea $p(x) \in \mathbb{Q}[x]$ un polinomio irreducible de grado n. Probar que en su grupo de Galois G hay un automorfismo que no deja fija ninguna raíz.

    (*Indicación:* Si H_i es el subgrupo de G formado por los automorfismos que dejan fija la raíz i–ésima, entonces $|H_i| = |G|/n$ y por tanto $H_1 \cup \ldots \cup H_n \neq G$.)

48. Sea $q(x) \in k[x]$ un polinomio separable cuyas raíces, en su cuerpo de descomposición, formen un cuerpo. Demostrar que k es un cuerpo de característica positiva p y que $q(x) = x^{p^n} - x$ para algún número natural $n \geq 1$.

49. Calcular las raíces y el grupo de Galois del polinomio $x^4 - x^2 + 1$ con coeficientes en $\mathbb{F}_5$.

50. Probar que el producto de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ es $x^{25} - x$.

51. Probar que todo polinomio irreducible de grado 2 con coeficientes en $\mathbb{F}_p$ tiene sus raíces en el cuerpo $\mathbb{F}_{p^2}$, y que todo elemento de $\mathbb{F}_{p^2}$ es raíz de un polinomio irreducible de grado 1 ó 2. Concluir que el número de polinomios mónicos irreducibles de grado 2 con coeficientes en $\mathbb{F}_p$ es $(p^2 - p)/2$. ¿Cuál es el número de polinomios irreducibles en $\mathbb{F}_p[x]$ de grado 2?

52. Hallar el número de polinomios mónicos irreducibles de grado 3 con coeficientes en $\mathbb{F}_p$. Análogamente para los de grado 4, 6 y 8.

53. Sea $p \neq 2$ un número primo. Probar que el núcleo del morfismo de grupos $\mathbb{F}_p^* \to \mathbb{F}_p^*$ $\bar{a} \mapsto \bar{a}^2$ es $\{\pm 1\}$ y concluir que tenemos un isomorfismo de grupos $\mathbb{F}_p^*/\mathbb{F}_p^{*2} = \{\pm 1\}$.

    Probar que la proyección canónica $\mathbb{F}_p^* \to \mathbb{F}_p^*/\mathbb{F}_p^{*2} = \{\pm 1\}$ transforma cada clase $\bar{a} \in \mathbb{F}_p^*$ en el símbolo de Legendre $\left(\frac{a}{p}\right)$ y concluir que éste es multiplicativo: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

54. Sean $p < q$ dos números primos distintos. Probar que p es resto cuadrático módulo q si y sólo si p genera en $\mathbb{F}_q^*$ un subgrupo de índice par.

55. Probar que el polinomio $(x^2 + 1)(x^2 - 2)(x^2 + 2)$ tiene raíz en $\mathbb{F}_p$ para todo número primo p, aunque carezca de raíces racionales.

56. Sean p, q dos números primos distintos. Probar que las siguientes condiciones son equivalentes:

    a) $x^q - 1$ tiene alguna raíz $x \neq 1$ en $\mathbb{F}_{p^n}$.

    b) $x^q - 1$ tiene q raíces distintas en $\mathbb{F}_{p^n}$.

    c) $p^n - 1$ es múltiplo de q.

57. Sean p, q dos números primos distintos. Probar que p genera el grupo cíclico $(\mathbb{Z}/q\mathbb{Z})^*$ si y sólo si el polinomio $x^{q-1} + \ldots + x + 1$ es irreducible en $\mathbb{F}_p[x]$.

58. Sea $p > 3$ un número primo y ε_{12} una raíz primitiva 12-ésima de $\bar{1} \in \mathbb{F}_p$. Probar que

$$\sqrt{3} = \varepsilon_{12}^3(2\varepsilon_{12}^4 + 1) = \varepsilon_{12}^3 + 2\varepsilon_{12}^7 \in \mathbb{F}_p(\varepsilon_{12}) \, .$$

y concluir (sin usar la Ley de reciprocidad cuadrática) que 3 es resto cuadrático módulo p si y sólo si $p \equiv 1$ ó -1 (mód. 12).

59. Sea $q \neq 2$ un número primo y ε_{4q} una raíz primitiva $4q$-ésima de la unidad. Probar que $\sqrt{q} \in \mathbb{F}_p(\varepsilon_{4q})$.

60. Si $\mathbb{F}_q$ es un cuerpo finito de característica distinta de 2, probar que el número de cuadrados en $\mathbb{F}_q$ es $(q+1)/2$. Concluir que todo elemento a de un cuerpo finito descompone en suma de dos cuadrados.

(*Indicación:* Si Q es el conjunto de cuadrados, probar que $Q \cap (a - Q)$ no es vacío).

61. Demostrar que la norma $N : \mathbb{F}_{p^n}^* \to \mathbb{F}_p^*$, $N(a) = F(a)F^2(a)\ldots F^n(a)$, es un morfismo de grupos epiyectivo, donde F denota el automorfismo de Frobënius $F(\alpha) = \alpha^p$.

(*Indicación:* Estudiar el orden del núcleo de la norma).

62. Sean a, b números enteros y sea p un número primo. Si $-4a^3 - 27b^2$ no es un resto cuadrático módulo p, probar que la congruencia $x^3 + ax \equiv b$ (módulo p) admite alguna solución entera.

Capítulo 5

Aplicaciones de la teoría de Galois

Observación: En este capítulo supondremos siempre que los cuerpos son de característica cero. Por tanto, todas las extensiones finitas de cuerpos consideradas serán separables.

5.1. Resolución de ecuaciones polinómicas por radicales

Sea $p(x) \in k[x]$ un polinomio y G el grupo de Galois del cuerpo de descomposición de $p(x)$. El objetivo de esta sección es probar que las raíces de $p(x)$ se pueden obtener como combinaciones algebraicas y toma de radicales sucesivas de elementos de k si y sólo si G es resoluble.

1. Teorema de independencia lineal de Artin: *Sea $k \to K$ una extensión de Galois de grupo $G = \{g_1, \ldots, g_n\}$. Se verifica que $g_1, \ldots, g_n \in \mathrm{End}_k(K)$ son K-linealmente independientes.*

Demostración. Como $k \to K$ es de Galois, $K \underset{k}{\otimes} K = K \times \overset{n}{\ldots} \times K$, y los automorfismos de K se corresponden con las proyecciones de $K \times \overset{n}{\ldots} \times K$ en cada uno de los factores, que son claramente K-linealmente independientes. □

2. Definición : Diremos que una extensión $k \to K$ es *cíclica* si es de Galois de grupo cíclico.

3. Proposición : *Sea $k \hookrightarrow K$ una extensión de cuerpos de grado n y supongamos k contiene todas las raíces n-ésimas de la unidad. Entonces, $k \to K$ es una extensión cíclica si y sólo existe $a \in k$ de modo que $K = k(\sqrt[n]{a})$.*

Demostración. Si $K = k(\sqrt[n]{a})$. K es una extensión de Galois porque es el cuerpo de descomposición del polinomio $x^n - a$. El grupo de Galois, G, de K es un subgrupo de $\mathbb{Z}/n\mathbb{Z}$: Dado $g \in \mathrm{Aut}_{k-alg}(k(\sqrt[n]{a})) = G$, tenemos que $g(\sqrt[n]{a}) = \epsilon^i \sqrt[n]{a}$, para cierto $0 \leq i < n$ y la aplicación $G \to \mathbb{Z}/n\mathbb{Z}$, $g \mapsto \bar{i}$ es un morfismo inyectivo de grupos. G es cíclico porque es un subgrupo de un grupo cíclico.

Supongamos que $k \hookrightarrow K$ sea una extensión de Galois de grupo cíclico $G = \langle \sigma \rangle$. Sea $\epsilon \in k$ una raíz n-ésima primitiva de la unidad. Si existe $0 \neq R \in K$ tal que $\sigma(R) = \epsilon R$, entonces

1. $R^n \in k$, porque $\sigma(R^n) = \sigma(R)^n = R^n$, luego $R^n \in K^{\langle \sigma \rangle} = k$.

2. $K = k(R)$, porque $k(R) = K^H$, donde $H = \{h \in G : h(R) = R\} = \{\mathrm{Id}\}$, luego $k(R) = K$.

3. Si denotamos $a = R^n \in k$, $K = k(\sqrt[n]{a})$.

Existe R: Tenemos que demostrar que ϵ es un valor propio de σ. Obviamente $x^n - 1$ anula a σ y por el teorema de independencia lineal de Artin, $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ son linealmente independientes, luego $x^n - 1$ es el polinomio mínimo anulador de σ y ϵ es un valor propio de σ. □

4. Observación: Sea $k \hookrightarrow K$ una extensión de Galois de grupo $G = \langle \sigma \rangle$ y $R \in K$. En la demostración del corolario anterior se ha visto que $R = \sqrt[n]{a}$, para algún $a \in k$, si y sólo si $\sigma(R) = \epsilon R$, siendo ϵ una raíz n-ésima de la unidad.

Calculemos un vector propio de σ, R, de valor propio ϵ. Observemos que $x^n - 1 = (x-\epsilon)\cdot(1+\epsilon^{-1}\cdot x+\cdots+\epsilon^{-(n-1)}x^{n-1})$. Por tanto, $\mathrm{Im}(1+\epsilon^{-1}\cdot\sigma+\cdots+\epsilon^{-(n-1)}\sigma^{n-1}) \subseteq \mathrm{Ker}(\sigma-\epsilon)$ (de hecho son iguales). Sea $\alpha \in K$, tal que $R := (1+\epsilon^{-1}\cdot\sigma+\cdots+\epsilon^{-(n-1)}\sigma^{n-1})(\alpha) \neq 0$, entonces $\sigma(R) = \epsilon \cdot R$.

5. Definición: Supongamos que $k \hookrightarrow K$ sea una extensión de Galois cíclica de grupo $G = \langle \sigma \rangle$. Sea $n = \dim_k K$ y $\epsilon \in k$ una raíz n-ésima de la unidad y $\alpha \in K$. Llamaremos resolvente de Lagrange de α por ϵ, que denotaremos $R(\alpha, \epsilon)$, a

$$R(\alpha,\epsilon) := \sum_{i=0}^{n-1} \epsilon^i \sigma^i(\alpha)$$

Observemos que $\sigma(R(\alpha,\epsilon)) = \epsilon^{-1} \cdot R(\alpha,\epsilon)$. Por tanto, $\sigma(R(\alpha,\epsilon)^n) = R(\alpha,\epsilon)^n$, luego $R(\alpha,\epsilon)^n \in k$.

6. Definición: Diremos que una extensión de cuerpos $k \to K$ es *radical* si $K \simeq k(\sqrt[n]{a})$.

7. Definición: Diremos que una extensión $k \to K$ es una extensión por radicales de k si $K = k(\alpha_1, \ldots, \alpha_n)$ de modo que $\alpha_i^{m_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$, para cierto m_i y todo i. Es decir, $k \to K$ es una extensión por radicales de k si admite una cadena de subextensiones

$$k \to K_1 \to K_2 \to \cdots \to K_r = K$$

tal que $K_i \to K_{i+1}$ es radical.

Obviamente el compuesto de extensiones de k por radicales es una extensión de k por radicales.

8. Teorema: *Sea $k \to K$ una extensión de Galois de grupo G de grado n. Supongamos que k contiene todas las raíces n-ésimas de la unidad. Entonces, $k \to K$ es una extensión por radicales si y sólo si el grupo G es resoluble.*

Demostración. Observemos que si $H_1 \subset H_2 \subseteq G$ son dos subgrupos, entonces H_1 es normal en H_2 si y sólo si $K^{H_2} \hookrightarrow K^{H_1}$ es una extensión de Galois (de grupo H_2/H_1): En efecto, $K^{H_2} \hookrightarrow K$ es una extensión de Galois de grupo H_2. Por el corolario 4.5.7, $K^{H_2} \hookrightarrow K^{H_1}$ es una extensión de Galois (de grupo H_2/H_1) si y sólo si H_1 es normal en H_2.

Sea $\{\mathrm{Id}\} = G_1 \subset G_2 \subset \cdots \subset G_r = G$ una cadena de subgrupos de G. Entonces, $k = K^{G_r} \subset K^{G_{r-1}} \subset \cdots \subset K^{G_2} \subset K^{G_1} = K$ es una resolución por extensiones radicales de K si y sólo si $K^{G_i} \hookrightarrow K^{G_{i-1}}$ es una extensión de Galois de grupo cíclico, para todo i, que equivale a decir que G_{i-1} es normal en G_i y G_i/G_{i-1} es cíclico, para todo i.

□

9. Teorema: *Sea $k \to K$ una extensión finita de cuerpos. Entonces, K está incluida en una extensión de k por radicales si y sólo si el grupo de la envolvente de Galois de K es resoluble.*

Demostración. Sea Σ la envolvente de Galois de K. Recordemos que si $\bar{k}$ es el cierre algebraico de k y $\{\phi_1, \ldots, \phi_n\} = \mathrm{Hom}_{k-alg}(K, \bar{k})$, entonces $\Sigma = \phi_1(K) \cdots \phi_n(K)$. Por tanto, K está incluida en una extensión por radicales si y sólo si Σ lo está.

En conclusión, podemos suponer que K es de Galois.

Sea $\dim_k K = n$ y ϵ una raíz n-ésima primitiva de la unidad. Es obvio que K está incluida en una extensión de k por radicales si y sólo si $K(\epsilon)$ está incluida en una extensión de $k(\epsilon)$ por radicales.

$K \cap k(\epsilon)$ es una k-extensión de Galois de grupo cíclico (pues es una subextensión de $k(\epsilon)$). Por el teorema 4.5.8, la sucesión

$$1 \to \mathrm{Aut}_{k(\epsilon)-alg}(K(\epsilon)) \to \mathrm{Aut}_{k-alg}(K) \to \mathrm{Aut}_{k-alg}(K \cap k(\epsilon)) \to 1$$

es exacta. Por tanto, $\mathrm{Aut}_{k-alg}(K)$ es un grupo resoluble si y sólo si $\mathrm{Aut}_{k(\epsilon)-alg}(K(\epsilon))$ es resoluble.

En conclusión, podemos suponer que $\epsilon \in k$.

Si el grupo de Galois de K es resoluble, por el teorema anterior K es una extensión por radicales (luego está incluida en una extensión por radicales).

Si K está incluida en una extensión K', que sea una extensión por radicales, entonces está incluida en una extensión K'' de Galois que es una extensión por radicales. Luego el grupo de Galois de K'' es resoluble, por el teorema anterior. Luego el grupo de Galois de K es resoluble, porque es un cociente del de K''.

□

10. Definición: Diremos que un polinomio $p(x) \in k[x]$ es resoluble por radicales si todas sus raíces están incluidas en una extensión de k por radicales.

11. Corolario: *Un polinomio $p(x) \in k[x]$ es resoluble por radicales si y sólo si el grupo de Galois del polinomio es resoluble.*

12. Teorema: *La ecuación general de grado n es resoluble por radicales para $n \leq 4$ y no es resoluble por radicales para $n > 4$.*

Demostración. Se deduce de que el grupo simétrico S_n es resoluble si y sólo si $n \leq 4$. □

13. Observación: El teorema de las funciones implícitas del Análisis nos dice que en general las raíces de un polinomio se pueden expresar como funciones diferenciables de los coeficientes del polinomio: Consideremos la función real en $n+1$ variables

$$P(x,a_1,\dots,a_n) = x^n + a_1x^{n-1} + \cdots + a_n$$

Sea $(\alpha_1,c_1,\dots,c_n) \in \mathbb{R}^{n+1}$ tal que $P(\alpha_1,c_1,\dots,c_n) = 0$ y que $\frac{\partial P}{\partial x}(\alpha_1,c_1,\dots,c_n) \neq 0$. Por el teorema de las funciones implícitas, existe una función diferenciable $f(a_1,\dots,a_n)$ definida en un entorno abierto de $(c_1,\dots,c_n)$ de modo que

$$P(f(a_1,\dots,a_n),a_1,\dots,a_n) = 0$$
$$f(c_1,\dots,c_n) = \alpha_1$$

En general, para las raíces imaginarias, deberemos considerar $P(x,a_1,\dots,a_n)$ como función (compleja) holomorfa y el teorema de las funciones implícitas en el caso holomorfo.

5.1.1. Resolución de las ecuaciones de grados 2, 3 y 4

Fórmula de Lagrange.

Sea $k \to K$ una extensión cíclica de grado n, supongamos que k contiene a las raíces n-ésimas de la unidad y fijemos una raíz n-ésima primitiva de la unidad, ϵ. Dado $\alpha \in K$, veamos cómo expresarlo en función de radicales de elementos de k (obtenidos a partir de α y el grupo de Galois de K).

Sea $R(\alpha,\epsilon^j)$ la resolvente de Lagrange de α por ϵ^j. La suma de las raíces r-ésimas de la unidad es cero, ya que el coeficiente de x^{r-1} de $x^r - 1$ es nulo. Ahora es fácil comprobar que

$$\boxed{\alpha = \frac{1}{n}\sum_{j=0}^{n-1} R(\alpha,\epsilon^j)}$$

Igualdad que se conoce como *fórmula de Lagrange*. Recordemos que $R(\alpha,\epsilon^j)^n \in k$.

Este teorema se generaliza de forma sencilla al caso en el que el grupo es producto directo de grupos abelianos.

14. Teorema: *Sea K una extensión de Galois de grupo $G = \mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_r\mathbb{Z}$, de orden n. Sea $\{\sigma_1,\dots\sigma_r\}$ un sistema de generadores de G de órdenes $n_1,\dots,n_r$, respectivamente, y $\varepsilon_1,\dots,\varepsilon_r$ raíces primitivas $n_1,\dots,n_r$-ésimas de la unidad. Dado $\alpha \in K$, denotemos*

$$R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r}) := \sum_{i_1<n_1,\dots,i_r<n_r} \varepsilon_1^{i_1j_1}\cdots\varepsilon_r^{i_rj_r}(\sigma_1^{i_1}\circ\cdots\circ\sigma_r^{i_r})(\alpha)$$

$R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$ son radicales d-ésimos ($d = m.c.m.(n_1,\dots,n_r)$) y se cumple la fórmula:

$$\alpha = \frac{1}{n_1\cdots n_r}\sum_{j_1<n_1,\dots,j_r<n_r} R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$$

Demostración. Se cumple que $R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r}) \stackrel{*}{=} R(R(\alpha,\varepsilon_1^{j_1}),\varepsilon_2^{j_2}\dots,\varepsilon_r^{j_r})$. Procedamos por inducción sobre r. Entonces,

$$\alpha = \frac{1}{n_1}\sum_{j_1<n_1} R(\alpha,\varepsilon_1^{j_1}) = \frac{1}{n_1}\sum_{j_1<n_1}\left(\frac{1}{n_2\cdots n_r}\sum_{j_2<n_2,\dots,j_r<n_r} R(R(\alpha,\varepsilon_1^{j_1}),\varepsilon_2^{j_2},\dots,\varepsilon_r^{j_r})\right)$$
$$= \frac{1}{n_1\cdots n_r}\sum_{j_1<n_1,\dots,j_r<n_r} R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$$

Denotemos $G_i = \langle\sigma_i\rangle$. Denotemos $R = R(\alpha,\varepsilon_1^{j_1},\dots,\varepsilon_r^{j_r})$. Por la igualdad $\stackrel{*}{=}$, $R^{n_1} \in K^{G_1}$. Como la definición de la resolvente R no depende del orden con el que se tomen los σ_i, tenemos que $R^{n_i} \in K^{G_i}$. Por tanto, $R^d \in \cap_i K^{G_i} = K^{\langle G_1,\dots,G_r\rangle} = K^G = k$.

□

15. Resolución de la ecuación de segundo grado, $x^2 + a_1x + a_2 = 0$.

Sea $x^2 + a_1x + a_2$ el polinomio general de segundo grado, de raíces x_1, x_2. Entonces, $k = \mathbb{Q}(a_1,a_2) \hookrightarrow \mathbb{Q}(x_1,x_2) = K$ es un extensión cíclica de grupo $S_2 = \mathbb{Z}/2\mathbb{Z}$, generado por la permutación $\sigma = (1,2)$, $\sigma(x_1) = x_2$. Calculemos $x_1 \in K$.

Calculamos las resolventes de Lagrange. Tenemos

$$R(x_1,1) = x_1 + x_2 = -a_1$$
$$R(x_1,-1) = x_1 - x_2$$

y $R(x_1,-1)^2 = (x_1-x_2)^2 = (x_1+x_2)^2 - 4x_1x_2 = a_1^2 - 4a_2$. Por tanto,

$$x_1,x_2 = \frac{1}{2}(R(x_1,1) + R(x_1,-1)) = \frac{-a_1 \pm \sqrt{a_1^2-4a_2}}{2}$$

16. Resolución de la cúbica, $x^3 + a_1x^2 + a_2x + a_3 = 0$**.**

Sea $x^3 + a_1x^2 + a_2x + a_3$ el polinomio general de tercer grado, de raíces x_1, x_2, x_3. Entonces, $k = \mathbb{Q}(a_1,a_2,a_3) \hookrightarrow \mathbb{Q}(x_1,x_2,x_3) = K$ es un extensión de Galois de grupo S_3. Calculemos $x_1 \in K$.

S_3 es un grupo resoluble: el alternado $A_3 = <(1,2,3)> \approx \mathbb{Z}/3\mathbb{Z}$ es un subgrupo normal y $S_3/A_3 = <\overline{(1,2)}> \approx \mathbb{Z}/2\mathbb{Z}$.

Notación: En lo que sigue, denotaremos $\sigma = (1,2,3)$ y $\tau = (1,2)$.

La extensión $k \subset K^{A_3}$ es de Galois de grado 2 de grupo $S_3/A_3 = <\overline{(1,2)}> \approx \mathbb{Z}/2\mathbb{Z}$, es decir, generado por la permutación τ y la extensión $K^{A_3} \subset K$ es de Galois de grado 3 y grupo $A_3 = <\sigma> \approx \mathbb{Z}/3\mathbb{Z}$.

Por la fórmula de Lagrange, las raíces $x_1, x_2, x_3 \in K$ se expresan en función de radicales cúbicos de elementos de K^{A_3} de la siguiente forma:

$$x_1 = \frac{1}{3}(R(x_1,1) + R(x_1,\varepsilon) + R(x_1,\varepsilon^2))$$

donde ε es una raíz cúbica de la unidad y

$$R(x_1,1) = x_1 + x_2 + x_3 = -a_1$$
$$R(x_1,\varepsilon) = x_1 + \varepsilon x_2 + \varepsilon^2 x_3 = R_1$$
$$R(x_3,\varepsilon^2) = x_1 + \varepsilon^2 x_2 + \varepsilon x_3 = R_2$$

Luego basta calcular los radicales cúbicos $R_1 = R(x_1, \varepsilon)$ y $R_2 = R(x_1, \varepsilon^2)$.

$R_1^3 \in K^{A_3}$ y K^{A_3} es una k-extensión de Galois de grupo $\langle \tau \rangle$. Aplicando la resolvente de Lagrange,

$$R_1^3 = \frac{1}{2}(R(R_1^3, 1) + R(R_1^3, -1)) = \frac{1}{2}(R_1^3 + \tau(R_1^3)) + \frac{1}{2}(R_1^3 - \tau(R_1^3))$$

Calculando resulta:

$$\frac{1}{2}(R_1^3 + \tau(R_1^3)) = \frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2}$$
$$\frac{1}{2}(R_1^3 - \tau(R_1^3)) = \frac{3}{2}\sqrt{-3\Delta} = \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}$$

Como $\tau(R_1) = \varepsilon R_2$, entonces $\tau(R_1^3) = R_2^3$. Por lo tanto, $R_2^3 = \frac{1}{2}(R_1^3 + \tau(R_1^3)) - \frac{1}{2}(R_1^3 - \tau(R_1^3))$.

En conclusión, resulta:

$$x_i = \frac{1}{3}\Big(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\Big)$$

donde los dos radicales cúbicos no son independientes, ya que puede comprobarse que $R_1 \cdot R_2 = a_1^2 - 3a_2$.

17. Resolución de la cuártica, $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$**.**

Sea $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ el polinomio general de cuarto grado, de raíces x_1, x_2, x_3, x_4. Entonces, $k = \mathbb{Q}(a_1, a_2, a_3, a_4) \hookrightarrow \mathbb{Q}(x_1, x_2, x_3, x_4) = K$ es un extensión de Galois de grupo S_4. Calculemos $x_1 \in K$.

Sea $K_4 = <(1,2)(3,4), (1,3)(2,4) \subset S_4$ el grupo de Klein.

$K^{K_4} \subset K$ es una extensión de Galois de grupo $K_4 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generado por las permutaciones $\sigma_1 = (1,2)(3,4)$ y $\sigma 2 = (1,3)(2,4)$.

Apliquemos la fórmula de Lagrange generalizada al caso no cíclico (como es K_4). Las resolventes de x_1 respecto de $K_4 = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle$ son:

$$R(x_1, 1, 1) = x_1 + x_2 + x_3 + x_4 = -a_1$$
$$R(x_1, 1, -1) = x_1 + x_2 - x_3 - x_4 = R_1$$
$$R(x_1, -1, 1) = x_1 - x_2 + x_3 - x_4 = R_2$$
$$R(x_1, -1, -1) = x_1 - x_2 - x_3 + x_4 = R_3$$

donde R_1, R_2, R_3 son radicales cuadráticos sobre K^{K_4}, es decir, $R_1^2, R_2^2, R_3^2 \in K^{K_4}$ (y verifican la relación $R_1R_2R_3 = -a_1^3 + 4a_1a_2 - 8a_3$). Como se puede comprobar es: $R_i^2 = a_1^2 - 4a_2 + 4\theta_i$, donde

$$\theta_1 = x_1x_2 + x_3x_4$$
$$\theta_2 = x_1x_3 + x_2x_4$$
$$\theta_3 = x_1x_4 + x_2x_3$$

Por tanto,

$$\boxed{x_i = \frac{1}{4}(-a_1 + \sqrt{a_1^2 - 4a_2 + 4\theta_1} + \sqrt{a_1^2 - 4a_2 + 4\theta_2} + \sqrt{a_1^2 - 4a_2 + 4\theta_3})}$$

donde el producto de cada dos de estos radicales cuadráticos determinan el tercero, pues el producto de los tres es $-a_1^3 + 4a_1a_2 - 8a_3$.

Tenemos que calcular $\theta_1, \theta_2, \theta_3 \in K^{K_4}$. El grupo de Galois de K^{K_4}, S_4/K_4, opera transitivamente sobre $\theta_1, \theta_2, \theta_3$. Por tanto, son las raíces de una cúbica con coeficientes en k, a saber:

$$(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 - a_2x^2 + (a_1a_3 - 4a_4)x - (a_1^2a_4 - 4a_2a_4 + a_3^2)$$

Esta cúbica es a la que se denomina *cúbica resolvente*. Como hemos resuelto ya las ecuaciones cúbicas, tenemos calculadas $\theta_1, \theta_2, \theta_3$.

18. Observación: $K^{K_4} = k(\theta_1, \theta_2, \theta_3)$.

5.1.2. Grupo de Galois de las cúbicas y las cuárticas

Los cálculos anteriores se han realizado para los polinomios genéricos, pero obviamente son válidos para cualquier polinomio.

Si un polinomio de grado 2, $x^2 + a_1x + a_2$, es irreducible, su grupo de Galois es S_2 y, en caso contrario es trivial. Es reducible si y sólo si tiene raíces en k y esto sucede cuando $\sqrt{a_1^2 - 4a_2} \in k$.

19. Proposición: *Sea $p(x) \in k[x]$ un polinomio separable de grado n. El grupo de Galois $G \subseteq S_n$ de $p(x)$ está incluido en el grupo alternado A_n si y sólo si el discriminante Δ de $p(x)$ es un cuadrado en k. Es decir,*

$$G \subseteq A_n \iff \sqrt{\Delta} \in k$$

Demostración. Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$, recordemos que

$$\sqrt{\Delta} = \prod_{i<j}(\alpha_i - \alpha_j) \in k(\alpha_1, \ldots, \alpha_n).$$

Además, dado $\sigma \in G \subseteq S_n$, $\sigma(\sqrt{\Delta}) = \text{sign}(\sigma) \cdot \sqrt{\Delta}$. Entonces, $\sqrt{\Delta} \in k = k(\alpha_1, \ldots, \alpha_n)^G$ $\iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$, para todo $\sigma \in G \iff \text{sign}(\sigma) = 1$, para todo $\sigma \in G \iff G \subseteq A_n$. □

Consideremos un polinomio irreducible de grado 3, $x^3 + a_1x^2 + a_2x + a_3$. Como el grupo de Galois, G opera transitivamente sobre el conjunto de las raíces, su orden es múltiplo de 3, luego G es igual a A_3 ó S_3. Tenemos que $\Delta = a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2$. Si $\sqrt{\Delta} \in k$ entonces $G = A_3$. Si $\sqrt{\Delta} \notin k$ entonces $G = S_3$.

Consideremos un polinomio irreducible de grado 4, $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$. Como las cuatro raíces son distintas, es fácil comprobar que las tres raíces de su cúbica resolvente también son distintas entre sí. $G \cap K_4$ son los automorfismos que dejan fijas las tres raíces, $\theta_1, \theta_2, \theta_3$ de la cúbica resolvente, luego $k(\alpha_1, \ldots, \alpha_4)^{G \cap K_4} = k(\theta_1, \theta_2, \theta_3) =$

K'. Observemos que $G/(G\cap K_4)\subseteq S_4/K_4 = S_3$. Denotemos $d = \#(G/(G\cap K_4))$, que es el grado de la extensión $k\hookrightarrow K'$. Tenemos que $d = 6,3,2,1$.

Como la cuártica se supone irreducible, el orden de su grupo de Galois, G, es múltiplo de 4.

Si $d = 6$, entonces el orden de G es 12 o 24. Si es 12 entonces $A_4 = G$ y $K_4\subseteq G$. Por tanto, $G\cap K_4 = K_4$, luego el orden de G es 24. En conclusión, si $d = 6$, $G = S_4$.

Si $d = 3$, entonces el orden de G es 12 y $G = A_4$.

Si $d = 2$, entonces el orden de G es 4 (cuando $G\cap K_4$ es de orden 2, que no actúa transitivamente sobre las raíces de la cuártica, luego ésta es reducible sobre K') y $G = \mathbb{Z}/4\mathbb{Z}$, ó el orden de G es 8 y contiene a K_4 (que actúa transitivamente sobre las raíces de la cuártica, luego ésta es irreducible sobre K'), luego $G = D_4$ (el grupo diédrico).

Si $d = 1$, entonces $G = K_4$.

5.2. Construcciones con regla y compás

5.2.1. Extensiones por radicales cuadráticos

Dado $a\in k$, la extensión $k\hookrightarrow k(\sqrt{a})$ tiene grado 1 o 2 según que $\sqrt{a}$ pertenezca a k o no. Recíprocamente, si $k\hookrightarrow K$ es una extensión de grado 2, entonces $K = k(\alpha)$, donde α es una raíz de un polinomio con coeficientes en k, irreducible de grado 2. La bien conocida fórmula de las raíces de los polinomios de grado 2, prueba que $K = k(\sqrt{a})$, para cierto $a\in k$.

1. Definición: Diremos que una extensión finita de cuerpos $k\hookrightarrow K$ es una extensión por radicales cuadráticos si $K = k(\alpha_1,\dots,\alpha_n)$, donde $\alpha_i^2\in k(\alpha_1,\dots,\alpha_{i-1})$, para todo $1\le i\le n$.

De la discusión anterior se sigue que el grado de una extensión por radicales cuadráticos es una potencia de 2. Además, es obvio que el compuesto de un número finito de extensiones por radicales cuadráticos de k es una extensión por radicales cuadráticos de k. Por tanto, si K es una k-extensión por radicales cuadráticos su envolvente de Galois Σ es una extensión por radicales cuadráticos: Sea $\bar{k}$ el cierre algebraico de k y $\{\phi_1,\dots,\phi_n\} = \mathrm{Hom}_{k-alg}(K,\bar{k})$, entonces $\phi_i(K)$ son extensiones por radicales cuadráticos, pues son isomorfas a K, y $\Sigma = \phi_1(K)\cdots\phi_n(K)$ es una extensión por radicales cuadráticos.

2. Teorema: *Sea $k\hookrightarrow K$ una extensión de Galois. K es una extensión por radicales cuadráticos de k si y sólo si es de grado una potencia de 2.*

Demostración. Sólo tenemos que probar el recíproco. Como $\#G = 2^n$, entonces G es resoluble y existe una serie normal $\{1\}\subset G_1\subset\cdots\subset G_n = G$ de factores isomorfos a $\mathbb{Z}/2\mathbb{Z}$. Esta sucesión de grupos por toma de invariantes se corresponde con una sucesión de subcuerpos $K\supset K^{G_1}\supset\cdots\supset K^{G_n} = k$, cada uno de grado 2 sobre el anterior. Por tanto, $K^{G_i} = K^{G_{i-1}}(\alpha_i)$, donde $\alpha_i^2\in K^{G_i}$. Luego, $K = k(\alpha_1,\dots,\alpha_n)$ es una extensión por radicales cuadráticos. □

3. Ejercicio: Sea $K = k(x_1,\dots,x_4)$ el cuerpo descomposición del polinomio general de grado 4. Sea $H = \langle(1,2,3)\rangle\subset S_4$. Probar que el grado de la k-extensión K^H es 2^3 y que

la envolvente de Galois de K^H es K que es de grado 24. Probar que K^H no es una extensión por radicales cuadráticos.

4. Proposición: *Una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si y sólo si está incluida en una extensión por radicales cuadráticos.*

Demostración. Supongamos que K está incluida en una extensión $k \hookrightarrow \Sigma$ por radicales cuadráticos. La envolvente de Galois de Σ es una extensión por radicales cuadráticos. Luego podemos suponer que Σ es de Galois. Su grupo de Galois G es un 2-grupo. Sea $H \subset G$ tal que $\Sigma^H = K$. Existe una cadena de grupos $H \subset H_1 \subset H_2 \subset \cdots \subset H_n = G$ de modo que $|H_{i+1}/H_i| = 2$, para todo i (ver demostración del primer teorema de Sylow 1.8.4). Tenemos la cadena $k \hookrightarrow K^{H_{n-1}} \hookrightarrow \cdots \hookrightarrow K^{H_1} \hookrightarrow K$ que muestra que $k \hookrightarrow K$ es una extensión de cuerpos por radicales cuadráticos. □

5. Corolario: *Una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si y sólo si su envolvente de Galois es de grado 2^n.*

Demostración. Si K es una extensión por radicales cuadráticos, su envolvente de Galois es una extensión por radicales cuadráticos, luego es de grado 2^n. Si la envolvente de Galois de K es de grado 2^n, entonces es una extensión por radicales cuadráticos y K también.

□

6. Definición: Diremos que un elemento $\alpha \in K$ de una extensión de cuerpos de k es un irracional cuadrático de k, si existe una extensión por radicales cuadráticos de k que contiene a α.

7. Ejercicio: Si α es un irracional cuadrático sobre k, pruébese que $k(\alpha)$ es una extensión de k por radicales cuadráticos.

Si un polinomio es irreducible y una raíz es un irracional cuadrático entonces todas las raíces son irracionales cuadráticos, ya que si α y β son raíces de $p(x)$, entonces $k(\alpha) = k[x]/(p(x)) = k(\beta)$.

8. Teorema: *Todas las raíces de un polinomio con coeficientes en k son irracionales cuadráticos si y sólo si su grupo de Galois es un grupo de orden una potencia de 2.*

Demostración. Si todas las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$ son irracionales cuadráticos, entonces $k(\alpha_1, \ldots, \alpha_n)$ es una extensión (de Galois) por radicales cuadráticos, luego su grupo de Galois es un grupo de orden una potencia de 2.

Si el grupo de Galois del polinomio es un grupo de orden una potencia de 2, entonces su cuerpo de descomposición es una extensión por radicales cuadráticos de k y las raíces del polinomio son irracionales cuadráticos.

□

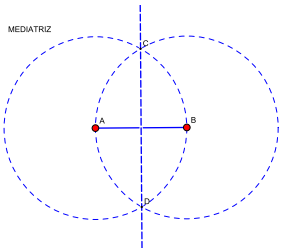
5.2.2. Construcciones con regla y compás

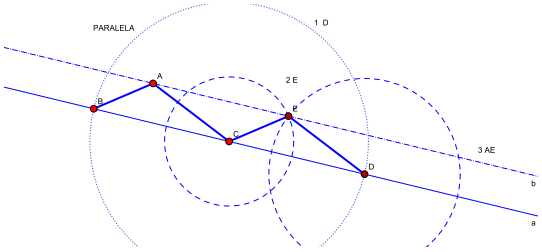
Consideremos en el plano euclídeo un conjunto de puntos $\mathbb{P}$, de cardinal mayor o igual que dos. El conjunto $\mathscr{C}(\mathbb{P})$ de los puntos del plano euclídeo constructibles con regla y compás a partir de $\mathbb{P}$ se define inductivamente mediante la aplicación reiterada (un número finito de veces) de las construcciones 2.,3. y 4.:

1. Diremos que los puntos de $\mathbb{P}$ son constructibles.
2. Diremos que las rectas que pasan por un par de puntos constructibles son constructibles.
3. Diremos que las circunferencias de centro un punto constructible y radio la distancia entre dos puntos constructibles son constructibles.
4. Diremos que los puntos de corte entre dos líneas constructibles (rectas o circunferencias) son constructibles.
5. $\mathscr{C}(\mathbb{P})$ es el conjunto de todos los puntos constructibles (con regla y compás a partir de $\mathbb{P}$).

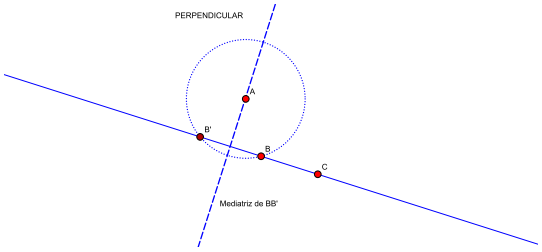
Es bien conocido que las siguiente construcciones pueden realizarse con regla y compás:

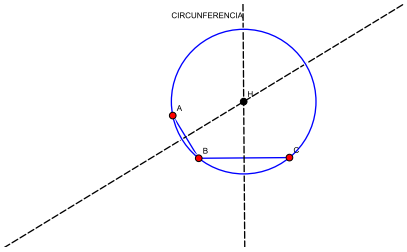
- Trazar la perpendicular por su punto medio a un segmento dado.
- Dados tres puntos no alineados A,B,C, trazar la paralela a la recta BC que pasa por A.



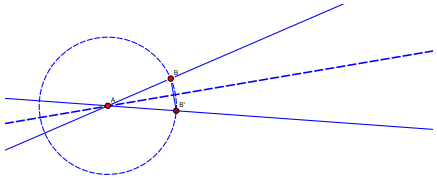


- Dados tres puntos no alineados A,B,C, trazar la perpendicular a la recta BC que pasa por A.
- Trazar la circunferencia que pasa por tres puntos no alineados A, B y C





- Trazar la bisectriz de un ángulo dado.



Escojamos dos puntos de $\mathbb{P}$ como sistema de referencia, uno el origen de coordenadas $(0,0)$ y el otro el $(0,1)$. Identifiquemos el plano euclídeo con $\mathbb{C}$. Los puntos escogidos se corresponden con el 0 y 1 de $\mathbb{C}$. Los puntos de $\mathbb{C}(\mathbb{P})$ se corresponden con ciertos

números complejos. A partir de ahora identificamos los puntos del plano euclídeo con los correspondientes números complejos.

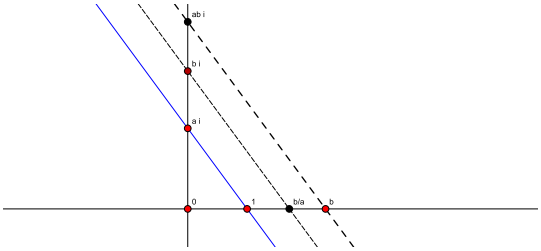
9. Lema: *La condición necesaria y suficiente para que un número complejo $a+bi$ sea constructible es que lo sean su parte real a y su parte imaginaria b.*

Demostración. Es consecuencia directa de la posibilidad de trazar paralelas y perpendiculares con regla y compás. □

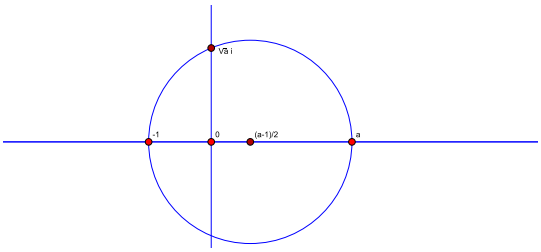
10. Lema: *Los números complejos constructibles $\mathscr{C}(\mathbb{P})$, forman un subcuerpo de $\mathbb{C}$, estable por toma de raíces cuadradas.*

Demostración. La suma y diferencia de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales y este caso es trivial.

El producto y cociente de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales. En la siguiente figura construimos el producto y cociente de a y b.



Para concluir hay que demostrar que la raíz cuadrada de cualquier número complejo constructible también lo es. Si el número es real, basta considerar la siguiente figura:



En el caso de un número complejo arbitrario, se construye la bisectriz del ángulo que determina con el 1 y se traza en ella el segmento de longitud igual a la raíz cuadrada del módulo del número complejo dado.

□

11. Teorema: *Sea k el mínimo subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{P}$. La condición necesaria y suficiente para que un número complejo sea constructible con regla y compás a partir de $\mathbb{P}$ es que sea un irracional cuadrático de k.*

Demostración. Si α es un irracional cuadrático, entonces $k(\alpha)$ es una extensión de k por radicales cuadráticos. Por el lema anterior, α es constructible.

Para demostrar el recíproco, obsérvese que los coeficientes de las ecuaciones de las rectas y circunferencias son funciones racionales de las coordenadas de los puntos que las determinan, según las construcciones 2 y 3. Además, las coordenadas de la intersección de dos líneas (círculos o rectas), se expresan en función de los coeficientes de las ecuaciones como irracionales cuadráticos. Procediendo inductivamente concluimos que las coordenadas de cualquier punto constructible son irracionales cuadráticos sobre k. Es decir, si $a+bi$ es constructible, es un irracional cuadrático sobre k.

□

12. Definición: Se dice que un número primo $p \in \mathbb{Z}$ es un primo de Fermat si $p = 2^n + 1$, para cierto $n \in \mathbb{N}$.

13. Proposición: *Si 2^n+1 es primo, entonces n es igual a una potencia de 2.*

Demostración. Escribamos $n = 2^m \cdot m'$, con m' impar y sea $a = 2^{2^m}$. Entonces, $2^n + 1 = 2^{2^m \cdot m'} + 1 = a^{m'} + 1$ que es divisible por $a+1$. Entonces, si 2^n+1 es primo, $m' = 1$. □

Los únicos primos de Fermat conocidos son $3 = 2+1$, $5 = 2^2+1$, $17 = 2^4+1$, $257 = 2^8+1$ y $65537 = 2^{16}+1$.

14. Proposición: *El polígono de n lados es constructible con regla y compás a partir de $\mathbb{P} = \{0,1\}$, si y sólo si $n = 2^{n_0} \cdot p_1 \cdots p_r$, con $n_0 \geq 0$, $r \geq 0$ y $p_1, \ldots, p_r$ números primos de Fermat distintos.*

Demostración. El polígono de n lados es constructible con regla y compás si y sólo si $e^{2\pi i/n}$ es constructible con regla y compás. Por los teoremas 5.2.8, 5.2.11, el polígono de n lados es constructible con regla y compás si y sólo si $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/n})$ es una potencia de 2. Ahora bien, si $n = 2^m \cdot p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de n en producto de potencias de primos distintos, entonces,

$$\begin{aligned}\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/n}) &= |(\mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/2^m\mathbb{Z})^*| \cdot |(\mathbb{Z}/p_1^{n_1}\mathbb{Z})^*| \cdots |(\mathbb{Z}/p_r^{n_r}\mathbb{Z})^*| \\ &= 2^{m-1} \cdot p_1^{n_1-1}(p_1-1) \cdots p_r^{n_r-1}(p_r-1),\end{aligned}$$

que es una potencia de dos si y sólo si n es producto de una potencia de 2 y de números primos de Fermat distintos. □

Construyamos el pentágono regular. Tenemos que construir $\xi = e^{2\pi i/5}$, que es raíz de

$$\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$$

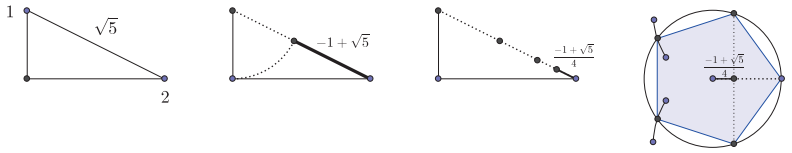
$\mathbb{Q}(\xi)$ es una $\mathbb{Q}$-extensión de Galois de grado 4, de grupo cíclico $G = \langle\sigma\rangle$, $\sigma(\xi) = \xi^2$. Consideremos las dos extensiones por un radical cuadrático

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\xi)^{\langle\sigma^2\rangle} = \mathbb{Q}(\xi + \xi^4) \hookrightarrow \mathbb{Q}(\xi)$$

El polinomio mínimo anulador de $\xi + \xi^4$ es

$$(x - (\xi + \xi^4)) \cdot (x - \sigma(\xi + \xi^4)) = (x - (\xi + \xi^4)) \cdot (x - (\xi^2 + \xi^3)) = x^2 + x - 1$$

Luego, $\xi + \xi^4 = (-1 + \sqrt{5})/2$. Observemos que si $\xi = a + bi$, entonces $2a = \xi + \xi^4 = (-1 + \sqrt{5})/2$ y $a = (-1 + \sqrt{5})/4$. Dibujemos el pentágono regular



Comentemos tres problemas irresolubles famosos de la Grecia clásica.

15. Duplicación del cubo: En el año 429 a. C., Pericles, gobernador de Atenas por esa época, muere víctima de la peste que atacaba muy severamente a la ciudad. A raíz de este suceso, algunos de los habitantes deciden ir a la ciudad de Delfos, para hacer consultas al Oráculo de Apolo y saber cómo poder detener la epidemia. La respuesta a la consulta del Oráculo fue que debían elaborar un nuevo altar en forma de cubo cuyo volumen duplicara el del altar entonces existente.

Si el altar existente es un cubo de lado de longitud $a \in \mathbb{Q}$, su volumen es a^3. Para construir un altar de volumen $2a^3$, hay que construir un cubo de lado de longitud $\sqrt[3]{2} \cdot a$. Este problema se resuelve con regla y compás si y sólo si $\sqrt[3]{2}$ es un irracional cuadrático sobre $\mathbb{Q}$, que no lo es, pues $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$.

16. Cuadratura del círculo: ¿Es posible, dado un círculo, construir con regla y compás un cuadrado del mismo área (y por tanto ser capaces de "conocer" el área del círculo)? Si el círculo es de radio $a \in \mathbb{Q}$, su área es $a^2 \cdot \pi$. El cuadrado de área $a^2 \cdot \pi$, es el cuadrado de lado de longitud $a \cdot \sqrt{\pi}$. Este problema se resuelve con regla y compás si y sólo si $\sqrt{\pi}$ es un irracional cuadrático sobre $\mathbb{Q}$, que no lo es, pues como demostró Lindemann, π es trascendente, es decir, $\dim_{\mathbb{Q}} \mathbb{Q}(\pi) = \infty$ (luego $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{\pi}) = \infty$).

17. Trisección de un ángulo: ¿Es posible, dado un ángulo cualquiera, dividirlo en tres ángulos iguales, con regla y compás? Dar un ángulo α es dar el número complejo $e^{\alpha \cdot i}$ y trisecarlo con regla y compás es construir el número complejo $e^{\alpha/3 \cdot i}$. Por ejemplo, si consideramos el ángulo $\pi/3$, es decir, el número complejo $e^{\pi/3 \cdot i}$, entonces $e^{\pi/9 \cdot i}$ no es un irracional cuadrático sobre $\mathbb{Q}(e^{\pi/3 \cdot i})$, porque $\dim_{\mathbb{Q}(e^{\pi/3 \cdot i})} \mathbb{Q}(e^{\pi/9 \cdot i}) = 3$.

5.3. Biografía de Abel

ABEL BIOGRAPHY

Niels Abel's life was dominated by poverty and we begin by putting this in context by looking briefly at the political problems which led to economic problems in Norway. At the end of the 18th century Norway was part of Denmark and the Danish tried to remain neutral through the Napoleonic wars. However a neutrality treaty in 1794 was considered a aggressive act by Britain and, in 1801, the British fleet destroyed most of the Da-

nish fleet in a battle in the harbour at Copenhagen.

Despite this Denmark-Norway avoided wars until 1807 when Britain feared that the Danish fleet might be used by the French to invade. Using the philosophy that attack is the best form of defence, the English attacked and captured the whole Danish fleet in October 1807.

Denmark then joined the alliance Britain Britain. The continental powers blockaded Britain, and as a counter to this Britain blockaded Norway. The twin blockade was a catastrophe to Norway preventing their timber exports, which had been largely to Britain, and preventing their grain imports from Denmark. An economic crisis in Norway followed with the people suffering hunger and extreme poverty. In 1813 Sweden attacked Denmark from the south and, at the treaty of Kiel in January 1814, Denmark handed over Norway to Sweden. An attempt at independence by Norway a few months later led to Sweden attacking Norway in July 1814. Sweden gained control of Norway, setting up a complete internal self-government for Norway with a government in Christiania (which is called Oslo today). In this difficult time Abel was growing up in Gjerstad in south-east Norway.

Abel's father, Sören Georg Abel, had a degree in theology and philology and his father (Niels Abel's grandfather) was a Protestant minister at Gjerstad near Risor. Sören Abel was a Norwegian nationalist who was active politically in the movement to make Norway independent. Sören Abel married Ane Marie Simonson, the daughter of a merchant and ship owner, and was appointed as minister at Finnoy. Niels Abel, the second of seven children, was one year old when his grandfather died and his father was appointed to succeed him as the minister at Gjerstad. It was in that town that Abel was brought up, taught by his father in the vicarage until he reached 13 years of age. However, these were the 13 years of economic crisis for Norway described above and Abel's parents would have not been able to feed their family that well. The problems were not entirely political either for

[Abel's] father was probably a drunkard and his mother was accused of having lax morals.

Abel's father was, however, important in the politics of Norway and, after Sweden gained control of Norway in 1814, he was involved in writing a new constitution for Norway as a member of the Storting, the Norwegian legislative body. In 1815 Abel and his older brother were sent to the Cathedral School in Christiania. The founding of the University of Christiania had taken away the good teachers from the Cathedral School to staff the University when it opened for teaching in 1813. What had been a good school was in a bad state when Abel arrived. Uninspired by the poor school, he proved a rather ordinary pupil with some talent for mathematics and physics.

When a new mathematics teacher Bernt Holmboë joined the school in 1817 things changed markedly for Abel. The previous mathematics teacher had been dismissed for punishing a boy so severely that he had died. Abel began to study university level mathematics texts and, within a year of Holmboë's arrival, Abel was reading the works of Euler, Newton, Lalande and d'Alembert. Holmboë was convinced that Abel had great talent and encouraged him greatly taking him on to study the works of Lagrange and Laplace. However, in 1820 tragedy struck Abel's family when his father died.

Abel's father had ended his political career in disgrace by making false charges against his colleagues in the Storting after he was elected to the body again in 1818. His habits of drinking to excess also contributed to his dismissal and the family was therefore in the deepest trouble when he died. There was now no money to allow Abel to complete his school education, nor money to allow him to study at university and, in addition, Abel had the responsibility of supporting his mother and family.

Holmboë was able to help Abel gain a scholarship to remain at school and Abel was able to enter the University of Christiania in 1821, ten years after the university was founded. Holmboë had raised money from his colleagues to enable Abel to study at the university and he graduated in 1822. While in his final year at school, however, Abel had begun working on the solution of quintic equations by radicals. He believed that he had solved the quintic in 1821 and submitted a paper to the Danish mathematician Ferdinand Degen, for publication by the Royal Society of Copenhagen. Degen asked Abel to give a numerical example of his method and, while trying to provide an example, Abel discovered the mistake in his paper. Degen had given Abel some important advice that was to set him working on an area of mathematics,

... whose development would have the greatest consequences for analysis and mechanics. I refer to elliptic integrals. A serious investigator with suitable qualifications for research of this kind would by no means be restricted to the many beautiful properties of these most remarkable functions, but could discover a Strait of Magellan leading into wide expanses of a tremendous analytic ocean.

At the University of Christiania Abel found a supporter in the professor of astronomy Christopher Hansteen, who provided both financial support and encouragement. Hansteen's wife began to care for Abel as if he was her own son. In 1823 Abel published papers on functional equations and integrals in a new scientific journal started up by Hansteen. In Abel's third paper, Solutions of some problems by means of definite integrals he gave the first solution of an integral equation.

Abel was given a small grant to visit Degen and other mathematicians in Copenhagen. While there he met Christine Kemp who shortly afterwards became his fiancée. Returning to Christiania, Abel tried to get the University of Christiania to give him a larger grant to enable him to visit the top mathematicians in Germany and France. He did not speak French of German so, partly to save money, he was given funds to remain in Christiania for two years to give him the chance to become fluent in these languages before travelling. Abel began working again on quintic equations and, in 1824, he proved the impossibility of solving the general equation of the fifth degree in radicals. He published the work in French and at his own expense since he wanted an impressive piece of work to take with him when he was on his travels. As Ayoub writes

He chose a pamphlet as the quickest way to get it into print, and in order to save on the printing costs, he reduced the proof to fit on half a folio sheet [six pages].

By this time Abel seems to have known something of Ruffini's work for he had studied Cauchy's work of 1815 while he was an undergraduate and in this paper there is a reference to Ruffini's work. Abel's 1824 paper begins

Geometers have occupied themselves a great deal with the general solution of algebraic equations and several among them have sought to prove the impossibility. But, if I am not mistaken, they have not succeeded up to the present.

Abel sent this pamphlet to several mathematicians including Gauss, who he intended to visit in Göttingen while on his travels. In August 1825 Abel was given a scholarship from the Norwegian government to allow him to travel abroad and, after taking a month to settle his affairs, he set out for the Continent with four friends, first visiting mathematicians in Norway and Denmark. On reaching Copenhagen, Abel found that Degen had died and he changed his mind about taking Hansteen's advice to go directly to Paris, preferring not to travel alone and stay with his friends who were going to Berlin. As he wrote in a later letter

Now I am so constituted that I cannot endure solitude. Alone, I am depressed, I get cantankerous, and I have little inclination to work.

In Copenhagen Abel was given a letter of introduction to Crelle by one of the mathematicians there. Abel met Crelle in Berlin and the two became firm friends. This proved the most useful part of Abel's whole trip, particularly as Crelle was about to begin publishing a journal devoted to mathematical research. Abel was encouraged by Crelle to write a clearer version of his work on the insolubility of the quintic and this resulted in Recherches sur les fonctions elliptiques which was published in 1827 in the first volume of Crelle's Journal, along with six other papers by Abel. While in Berlin, Abel learnt that the position of professor of mathematics at the University of Christiania, the only university in Norway, had been given to Holmboë. With no prospects of a university post in Norway, Abel began to worry about his future.

Crelle's Journal continued to be a source for Abel's papers and Abel began to work to establish mathematical analysis on a rigorous basis. He wrote to Holmboë from Berlin:

My eyes have been opened in the most surprising manner. If you disregard the very simplest cases, there is in all of mathematics not a single infinite series whose sum had been rigorously determined. In other words, the most important parts of mathematics stand without foundation. It is true that most of it is valid, but that is very surprising. I struggle to find a reason for it, an exceedingly interesting problem.

It had been Abel's intention to travel with Crelle to Paris and to visit Gauss in Göttingen on the way. However, news got back to Abel that Gauss was not pleased to receive his work on the insolubility of the quintic, so Abel decided that he would be better not to go to Göttingen. It is uncertain why Gauss took this attitude towards Abel's work since he certainly never read it - the paper was found unopened after Gauss's death. Ayoub gives two possible reasons:

... the first possibility is that Gauss had proved the result himself and was willing to let Abel take the credit. ... The other explanation is that he did not attach very much importance to solvability by radicals...

The second of these explanations does seem the more likely, especially since Gauss had written in his thesis of 1801 that the algebraic solution of an equation was no

better than devising a symbol for the root of the equation and then saying that the equation had a root equal to the symbol.

Crelle was detained in Berlin and could not travel with Abel to Paris. Abel therefore did not go directly to Paris, but chose to travel again with his Norwegian friends to northern Italy before crossing the Alps to France. In Paris Abel was disappointed to find there was little interest in his work. He wrote back to Holmboë:

The French are much more reserved with strangers than the Germans. It is extremely difficult to gain their intimacy, and I do not dare to urge my pretensions as far as that; finally every beginner had a great deal of difficulty getting noticed here. I have just finished an extensive treatise on a certain class of transcendental functions to present it to the Institute which will be done next Monday. I showed it to Mr Cauchy, but he scarcely deigned to glance at it.

The contents and importance of this treatise by Abel is described,

It dealt with the sum of integrals of a given algebraic function. Abel's theorem states that any such sum can be expressed as a fixed number p of these integrals, with integration arguments that are algebraic functions of the original arguments. The minimal number p is the genus of the algebraic function, and this is the first occurrence of this fundamental quantity. Abel's theorem is a vast generalisation of Euler's relation for elliptic integrals.

Two referees, Cauchy and Legendre, were appointed to referee the paper and Abel remained in Paris for a few months,

... emaciated, gloomy, weary and constantly worried. He ... could only afford to eat one meal a day.

He published some articles, mainly on the results he had already written for Crelle's Journal, then with no money left and his health in a very poor state, he returned to Berlin at the end of 1826. In Berlin, Abel borrowed some money and continued working on elliptic functions. He wrote a paper in which

... he radically transformed the theory of elliptic integrals to the theory of elliptic functions by using their inverse functions ...

Crelle tried to persuade Abel to remain in Berlin until he could find an academic post for him and he even offered Abel the editorship of Crelle's Journal. However, Abel wanted to get home and by this time he was heavily in debt. He reached Christiania in May 1827 and was awarded a small amount of money by the university although they made sure they had the right to deduct a corresponding amount from any future salary he earned. To make a little more money Abel tutored schoolchildren and his fiancée was employed as a governess to friends of Abel's family in Froland.

Hansteen received a major grant to investigate the Earth's magnetic field in Siberia and a replacement was needed to teach for him at the University and also at the Military Academy. Abel was appointed to this post which improved his position a little.

In 1828 Abel was shown a paper by Jacobi on transformations of elliptic integrals. Abel quickly showed that Jacobi's results were consequences of his own and added a note to this effect to the second part of his major work on elliptic functions. He had

been working again on the algebraic solution of equations, with the aim of solving the problem of which equations were soluble by radicals (the problem which Galois solved a few years later). He put this to one side to compete with Jacobi in the theory of elliptic functions, quickly writing several papers on the topic.

Legendre saw the new ideas in the papers which Abel and Jacobi were writing and said

Through these works you two will be placed in the class of the foremost analysts of our times.

Abel continued to pour out high quality mathematics as his health continued to deteriorate. He spent the summer vacation of 1828 with his fiancée in Froland. The masterpiece which he had submitted to the Paris Academy seemed to have been lost and so he wrote the main result down again

The paper was only two brief pages, but of all his many works perhaps the most poignant. He called it only "A theorem": it had no introduction, contained no superfluous remarks, no applications. It was a monument resplendent in its simple lines - the main theorem from his Paris memoir, formulated in few words.

Abel travelled by sled to visit his fiancée again in Froland for Christmas 1828. He became seriously ill on the sled journey and despite an improvement which allowed them to enjoy Christmas, he soon became very seriously ill again. Crelle was told and he redoubled his efforts to obtain an appointment for Abel in Berlin. He succeeded and wrote to Abel on the 8 April 1829 to tell him the good news. It was too late, Abel had already died. Ore [3] describes his last few days:

... the weakness and cough increased and he could remain out of bed only the few minutes while it was being made. Occasionally he would attempt to work on his mathematics, but he could no longer write. Sometimes he lived in the past, talking about his poverty and about Fru Hansteen's goodness. Always he was kind and patient. ...

He endured his worst agony during the night of April 5. Towards morning he became more quiet and in the forenoon, at eleven o'clock, he expired his last sigh.

After Abel's death his Paris memoir was found by Cauchy in 1830 after much searching. It was printed in 1841 but rather remarkably vanished again and was not found until 1952 when it turned up in Florence. Also after Abel's death unpublished work on the algebraic solution of equations was found. In fact in a letter Abel had written to Crelle on 18 October 1828 he gave the theorem:

If every three roots of an irreducible equation of prime degree are related to one another in such a way that one of them may be expressed rationally in terms of the other two, then the equation is soluble in radicals.

This result is essentially identical to one given by Galois in his famous memoir of 1830. In this same year 1830 the Paris Academy awarded Abel and Jacobi the Grand Prix for their outstanding work.

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

5.4. Cuestionario

Recordemos que suponemos que los cuerpos considerados son de característica cero.

1. ¿Son las extensiones de Galois de grado primo, cíclicas?
2. ¿Son las extensiones de grado dos, extensiones de Galois cíclicas?
3. Dado $1+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, calcular $R(1+\sqrt{2},-1)$.
4. Sea k un cuerpo que contiene a las raíces 31-ésimas de la unidad y $k \hookrightarrow K$ una extensión de Galois de grado 31. ¿Es $K = k(\sqrt[31]{a})$ para cierto $a \in k$?
5. Si k es un cuerpo de característica cero que contiene a las raíces 10-ésimas de la unidad y $k \hookrightarrow K$ es una extensión de Galois de grado 10. Entonces ¿$k \hookrightarrow K$ es una extensión por radicales?
6. ¿Es el cuerpo de descomposición de x^5-2 una extensión de $\mathbb{Q}$ por radicales?
7. Sea $p(x) = x^3+a_1x^2+a_2x+a_3 \in k[x]$ irreducible y α una raíz de $p(x)$ ¿Es el grupo de Galois de $p(x)$ de orden 3 si y sólo si $k(\alpha)$ es el cuerpo de descomposición de $p(x)$?
8. ¿Cuáles son las raíces de x^3+px+q? Hacer un cambio de variable lineal para que la cúbica $x^3+a_1x^2+a_2x+a_3$ sea de la forma de la cúbica anterior.
9. Calcular la cúbica resolvente de la cuártica.
10. Si $p(x)$ es una cuártica de grupo de Galois S_4 ¿Es el grupo de Galois de su cúbica resolvente isomorfo a S_3?
11. ¿Cuáles de las siguientes $\mathbb{Q}$-extensiones son extensiones de $\mathbb{Q}$ por radicales cuadráticos?: $\mathbb{Q}[\sqrt[4]{2}]$, $\mathbb{Q}[\sqrt[3]{2}]$ y $\mathbb{Q}[\sqrt{2}\cdot\sqrt{5}\cdot\sqrt{7}+\sqrt{\sqrt{5}+1}]$.
12. ¿Cuáles de las siguientes $\mathbb{Q}$-extensiones son extensiones de $\mathbb{Q}$ por radicales cuadráticos?: $\mathbb{Q}(e^{2\pi i/3})$, $\mathbb{Q}(e^{2\pi i/7})$ y $\mathbb{Q}(e^{2\pi i/15})$.
13. Sea $\mathbb{P} = \{0,1\}$. ¿Pertenecen, 33, i y $33+i$ al conjunto de puntos construidos con regla y compás a partir de $\mathbb{P}$?
14. ¿Es constructible $\sqrt[3]{2}$ con regla y compás a partir de $\mathbb{P} = \{0,1\}$?
15. ¿Es constructible $\frac{\sqrt[2]{8+\sqrt[3]{2}}}{\sqrt{5}+\sqrt[3]{2}}$ con regla y compás a partir de $\mathbb{P} = \{0,1,\sqrt[3]{2}\}$?
16. Dado un heptágono regular ¿Se puede construir con regla y compás un polígono regular de 56 lados?
17. Dado un heptágono regular ¿Se puede construir con regla y compás un polígono regular de 168 lados?

5.5. Problemas

1. Sea A una k-álgebra separable, K una k-extensión de cuerpos trivializante de A y $\{g_1,\dots,g_n\} = \mathrm{Hom}_{k-alg}(A,K)$. Dado $a \in A$ consideremos el endomorfismo k-lineal $h_a : A \to A$, $h_a(a') := aa'$. Probar que $N(a) = g_1(a)\cdots g_n(a)$ es igual al determinante de h_a. Probar que $Tr(a) = g_1(a) + \ldots + g_n(a)$ es igual a la traza de h_a.

2. Consideremos la extensión de Galois $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^{nm}}$. Dado $a \in \mathbb{F}_{p^{nm}}$, probar que $N(a) = a^{\frac{p^{nm}-1}{p^m-1}}$. Probar que $N : \mathbb{F}_{p^{nm}} \to \mathbb{F}_{p^m}$ es epiyectivo.

3. Dada la extensión de Galois $\mathbb{Q} \in \mathbb{Q}(e^{2\pi i/3})$, calcular $N(1+2e^{2\pi i/3})$.

4. Probar que un número complejo $z \in \mathbb{C}$ es de módulo 1 si y sólo existe otro número complejo z' de modo que $z = z'/\overline{z'}$.

5. Probar que si K y K' son k-extensiones por radicales entonces todo compuesto $K \cdot K'$ es una extensión por radicales.

6. Probar que si $k \hookrightarrow K$ es una extensión finita separable por radicales, entonces la envolvente de Galois es una extensión por radicales.

7. Sea $p(x) = x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{C}(a_1,a_2,a_3)[x]$ la polinomio general de grado 3. ¿Es $\mathbb{C}(a_1,a_2,a_3) \hookrightarrow \mathbb{C}(a_1,a_2,a_3)[x]/(p(x)) =: K$ una extensión por radicales? ¿Es la envolvente de Galois de K una extensión por radicales?

8. Determinar el grupo de Galois de la cúbica $x^3 + 2x + 1$ sobre el cuerpo $\mathbb{Q}(e^{2\pi i/7})$.

9. Si el discriminante de una cúbica $p(x) \in k[x]$ (no necesariamente irreducible) es un cuadrado en k, probar que el grupo de Galois G de $p(x)$ sobre k es $G = A_3$ ó $G = \{1\}$.

10. Sea K una extensión de $\mathbb{Q}$. Probar que $x^3 - 3x + 1$ es irreducible en $K[x]$ o tiene todas sus raíces en K. (*Indicación:* El discriminante es $\Delta = 9^2$).

11. Si el grupo de Galois sobre $\mathbb{Q}$ de una cúbica es A_3, probar que tiene tres raíces reales.

12. Una ecuación cúbica con coeficientes reales tiene una única raíz real cuando el discriminante es negativo, y tiene todas sus raíces reales cuando el discriminante es positivo.

13. Si Δ es el discriminante de una cúbica irreducible con coeficientes racionales, probar que su cuerpo de descomposición es $\mathbb{Q}(\sqrt{\Delta}, \alpha)$ donde α es cualquier raíz compleja.

14. Estudiar el grupo de Galois de una cúbica binómica $x^3 - a$ sobre un cuerpo k de característica 0, según que las raíces cúbicas de la unidad estén o no en k.

15. Calcular el grupo de Galois de la cúbica binómica genérica $x^3 - a$ sobre los números racionales (i.e., sobre el cuerpo $\mathbb{Q}(a)$ de funciones racionales en una indeterminada). ¿Y sobre el cuerpo de los números complejos?

16. El grupo de Galois sobre $\mathbb{Q}$ de una ecuación bicuadrada irreducible $x^4 + ax^2 + b$ es

    a) El grupo de Klein K_4 si b es un cuadrado.

    b) El grupo cíclico C_4 si b no es un cuadrado, pero $a^2b - 4b^2$ sí lo es.

    c) El grupo diédrico D_4 en cualquier otro caso.

17. Sea α una raíz de una cuártica irreducible $p(x) \in \mathbb{Q}[x]$. Demostrar que no existen cuerpos intermedios propios entre $\mathbb{Q}$ y $\mathbb{Q}(\alpha)$ si y sólo si el grupo de Galois de $p(x)$ es el grupo simétrico S_4 o el grupo alternado A_4.

18. Si una cuártica irreducible tiene exactamente dos raíces reales, probar que su grupo de Galois sobre $\mathbb{Q}$ es el grupo simétrico S_4 o el diédrico D_4.

19. El grupo de Galois sobre $\mathbb{Q}$ de una recíproca irreducible $x^4 + ax^3 + bx^2 + ax + 1$ es

    a) El grupo de Klein K_4 si $b^2 + 4b + 4 - 4a^2$ es un cuadrado.

    b) El grupo cíclico C_4 cuando $b^2 + 4b + 4 - 4a^2$ no es un cuadrado, pero sí lo es $(b^2 + 4b + 4 - 4a^2)(a^2 - 4b + 8)$.

    c) El grupo diédrico D_4 en cualquier otro caso.

20. Calcular el grupo de Galois de la cuártica bicuadrada genérica $x^4 + ax^2 + b$ sobre los números racionales.

21. Calcular el grupo de Galois de la cuártica recíproca genérica $x^4 + ax^3 + bx^2 + ax + 1$ sobre los números racionales.

22. Sea G el grupo de Galois de una cuártica separable $p_4(x)$ con coeficientes en un cuerpo k. Si $p_4(x)$ no es irreducible en $k[x]$, probar las siguientes afirmaciones:

    a) Si $p_4(x)$ tiene más de dos raíces en k, entonces $G = \{\mathrm{Id}\}$.

    b) Si $p_4(x)$ tiene dos raíces en k, entonces $G = S_2 = \{\mathrm{Id}, (1,2)\}$.

    c) $p_4(x)$ tiene una raíz en k, entonces $G = A_3$ ó $G = S_3$, según que el discriminante de $p_4(x)$ sea un cuadrado en k o no lo sea.

    d) Si $p_4(x)$ no tiene raíces en k, entonces $G = \{\mathrm{Id}, (1,2)(3,4)\}$ ó

    $$G = \{\mathrm{Id}, (1,2), (3,4), (1,2)(3,4)\}$$

23. Calcular el grupo de Galois sobre $\mathbb{Q}$ de las cuárticas: $x^4 - 4x^2 + 2$, $x^4 + 6x^2 + 1$, $x^4 - 3x + 1$, $2x^4 + x^3 - x^2 + 2x - 1$, $x^4 + 1$, $12x^4 + 8x^3 + 1$, $x^4 - 3x^3 + 4x^2 - 2x + 1$, $x^4 - 3x^3 - 3x^2 + 10x - 3$.

24. Hallar una cuártica con coeficientes racionales cuyo grupo de Galois sea $G = \{\mathrm{Id}, (1,2)(3,4)\}$ y otra cuyo grupo de Galois sea $G = \{\mathrm{Id}, (1,2), (3,4), (1,2)(3,4)\}$.

25. Determinar si las raíces de la unidad $e^{\frac{2\pi i}{7}}$, $e^{\frac{2\pi i}{8}}$, $e^{\frac{2\pi i}{9}}$, $e^{\frac{2\pi i}{10}}$, $e^{\frac{2\pi i}{11}}$, $e^{\frac{2\pi i}{12}}$, $e^{\frac{2\pi i}{13}}$, $e^{\frac{2\pi i}{14}}$, $e^{\frac{2\pi i}{15}}$ y $e^{\frac{2\pi i}{16}}$ son irracionales cuadráticos sobre $\mathbb{Q}$.

26. Determinar si $\sqrt{2}+\sqrt[3]{3}$, $\sqrt[4]{2}$ y $\sqrt[5]{2}$ son irracionales cuadráticos sobre $\mathbb{Q}$.

Solución de los problemas del curso

Solución de los problemas del capítulo primero

P1. a. $\Rightarrow$ b.) $\phi(g_1 \cdot g_2) = (g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1} = g_1^{-1} \cdot g_2^{-1} = \phi(g_1) \cdot \phi(g_2)$. b. $\Rightarrow$ a.) $g_1^{-1} \cdot g_2^{-1} = \phi(g_1) \cdot \phi(g_2) = \phi(g_1 \cdot g_2) = (g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}$, luego G es conmutativo.

a. $\Rightarrow$ c.) $\phi(g_1 g_2) = (g_1 g_2)^2 = g_1 g_2 g_1 g_2 = g_1^2 g_2^2 = \phi(g_1)\phi(g_2)$. c. $\Rightarrow$ a.) $g_1 g_2 g_1 g_2 = g_1^2 g_2^2$, luego $g_2 g_1 = g_1 g_2$.

a. $\Rightarrow$ d.) $\phi((g_1, g_2) \cdot (g_1', g_2')) = g_1 g_1' g_2 g_2' = g_1 g_2 g_1' g_2' = .\phi((g_1, g_2))\phi((g_1', g_2'))$. d. $\Rightarrow$ a.) $g_1 g_1' g_2 g_2' = g_1 g_2 g_1' g_2'$, luego $g_1' g_2 = g_2 g_1'$.

P2. $\tau_a(bb') = abb'a^{-1} = aba^{-1}ab'a^{-1} = \tau_a(b) \cdot \tau_a(b')$, luego τ_a es morfismo de grupos. Como $\tau_{ab}(c) = abcb^{-1}a^{-1} = \tau_a(\tau_b(c))$, entonces $\tau_a \circ \tau_b = \tau_{ab}$ y $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, es un morfismo de grupos.

P3. Si $h_1, h_2 \in N(H)$ entonces $\tau_{h_1 h_2}(H) = \tau_{h_1}(\tau_{h_2}(H)) = \tau_{h_1}(H) = H$ y $h_1 h_2 \in N(H)$. Si $h \in N(H)$, entonces $\tau_h(H) = H$, luego $\tau_{h^{-1}}(H) = \tau_h^{-1}(H) = H$ y $h^{-1} \in N(H)$. En conclusión, $N(H)$ es grupo. $H \subseteq H' \subseteq G$ es normal en H', si y sólo si para todo $h \in H'$, $hHh^{-1} = H$, por tanto $H' \subseteq N(H)$ y $N(H)$ es el mayor subgrupo de G que contiene a H como subgrupo normal. Si $\phi\colon G \to G'$ es un isomorfismo de grupos y H es normal en $H' \subseteq G$ entonces $\phi(H)$ es normal en $\phi(H')$. Por tanto, $\phi(N(H)) = N(\phi(H))$. En particular, $aN(H)a^{-1} = \tau_a(N(H)) = N(\tau_a(H)) = N(aHa^{-1})$.

P4. $Z(G)$ es el núcleo del morfismo $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, luego es normal.

P5. Sea $\sigma \in S_n$, $\sigma \neq \mathrm{Id}$. Sea a_1 tal que $a_2 := \sigma(a_1) \neq a_1$. Sea $a_3 \neq a_1, a_2$ y $\tau = (a_2, a_3)$. Entonces, $\tau\sigma\tau^{-1}(a_1) = a_3$, luego $\tau\sigma\tau^{-1} \neq \sigma$ y $\sigma \notin Z(G)$. En conclusión, el centro del grupo simétrico S_n es trivial cuando $n \geq 3$.

P6. El núcleo del epimorfismo de grupos $\pi\colon H \rtimes K \to H \cdot K$, $\pi((h,k)) = hk$, son las parejas (h,k) tales que $hk = 1$, luego $k = h^{-1} \in H \cap K$. En conclusión, $\mathrm{Ker}\,\pi = \{(h, h^{-1}),\ h \in H \cap K\} \simeq H \cap K$. Por el teorema de isomorfía y de Lagrange, $|H \cap K||HK| = |H \rtimes K| = |H \times K| = |H||K|$.

P7. Dados $h \in H$ y $k \in K$, $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{1\}$, luego $hkh^{-1}k^{-1} = 1$ y $hk = kh$.

P8. Por el teorema de Lagrange no puede haber más subgrupos de G que G y el trivial $\{1\}$. Por tanto, el subgrupo generado por cualquier elemento distinto de 1 es igual a G.

P9. Dado $g \in G$, $g \neq 1$, el subgrupo generado $\langle g \rangle$ ha de ser G. Por tanto, G es cíclico y no es $\mathbb{Z}$ porque éste contiene subgrupos propios. Luego, $G \simeq \mathbb{Z}/n\mathbb{Z}$, para $n > 0$. Si n no es primo, sea $d > 1$ un divisor de n. Entonces, $\langle \bar{d} \rangle$ es un subgrupo propio de $\mathbb{Z}/n\mathbb{Z}$ (de orden n/d). Luego, n ha de ser primo.

P10. Observemos que $g^2 = 1$ si y sólo si $g = g^{-1}$. Si $g \neq g^{-1}$, para toda $g \in G \backslash \{1\}$, entonces G es la unión disjunta de parejas $\{g, g^{-1}\}$ junto con $\{1\}$ y su orden sería impar, lo que contradice las hipótesis.

P11. Dado $g \in G$, el subgrupo generado por g ha de ser finito, porque si no es isomorfo a $\mathbb{Z}$, que contiene un número infinito de subgrupos. El conjunto de los subgrupos de G generados por un sólo elemento (subgrupos cíclicos), es finito digamos que son $\{\langle g_1 \rangle, \ldots, \langle g_r \rangle\}$. Dado $g \in G$, para algún i, $\langle g \rangle = \langle g_i \rangle$. Por tanto, $\cup_{i=1}^{r} \langle g_i \rangle = G$ y G es finito.

P12. Observemos que $g_1 H g_1^{-1} = g_2 H g_2^{-1} \iff (g_1^{-1} g_2) H (g_1^{-1} g_2)^{-1} = H \iff g_1 g_2^{-1} \in N(H) \iff \bar{g}_1 = \bar{g}_2 \in G/N(H)$. Por tanto, el número de conjugados distintos de H es $|G/N(H)|$. Como no son disjuntos tenemos que el orden de la unión de todos los conjugados de H es menor estricto que $|G/N(H)||H| \leq |G/H||H| = |G|$, luego existe algún elemento de G que no está contenido en ninguno de los subgrupos conjugados de H.

P13. Se tiene que $g' \in I_{x'} \iff g' \cdot x' = x' \iff g' \cdot g \cdot x = g \cdot x \iff g^{-1} \cdot g' \cdot g \cdot x = x \iff g^{-1} \cdot g' \cdot g \in I_x \iff g' \in g \cdot I_x \cdot g^{-1}$. Es decir, $I_{x'} = g \cdot I_x \cdot g^{-1}$.

P14. $\phi(G \cdot x) = G \cdot \phi(x)$. El endomorfismo de una órbita es un epimorfismo luego es biyectivo, luego es un automorfismo.

P15. Si $\phi : G/H \to G/K$ es un isomorfismo de G-conjuntos, entonces el grupo de isotropía de $\bar{1} \in G/H$, que es $\bar{1}$, ha de ser igual al grupo de isotropía de $\phi(\bar{1}) = \bar{g} \in G/K$, que es gKg^{-1}. Es decir, $H = gKg^{-1}$. Recíprocamente, si $H = gKg^{-1}$, entonces $\phi : G/H \to G/K$, $\phi(\bar{t}) := \overline{tg}$ es un isomorfismo de G-conjuntos.

P17. Todo automorfismo de G-conjuntos $\phi : G/H \to G/H$, está determinado por $\phi(\bar{1})$, ya que $\phi(\bar{t}) = \phi(t \cdot \bar{1}) = t \cdot \phi(\bar{1})$. Tenemos, pues, un morfismo inyectivo

$$\mathrm{Aut}_{G-conj}(G/H) \hookrightarrow G/H,\ \phi \mapsto \phi(\bar{1}).$$

Veamos ahora cuándo $G/H \to G/H$, $\bar{t} \mapsto t \cdot \bar{g}$ es un morfismo bien definido de G-conjuntos: tiene que cumplirse que $t \cdot H \cdot \bar{g} = t \cdot \bar{g}$, es decir, $H \cdot \bar{g} = \bar{g}$, que equivale a decir que $HgH \subseteq gH$, que equivale a $gHg^{-1} \subseteq H$. Si además ϕ es un automorfismo entonces $\phi^{-1}(\bar{1}) = \overline{g^{-1}}$, que estará bien definido si $g^{-1}Hg \subseteq H$ (que equivale a $gHg^{-1} \subseteq H$). En conclusión, ϕ es un automorfismo de G-conjuntos (bien definido) si y sólo si $g \in N(H)$, que equivale a decir que $\bar{g} \in N(H)/H$.

P18. En la solución del problema 15 hemos visto que el número de subgrupos conjugados de H es $\#(G/N(H))$.

P19. $G/H = \{\bar{1}, \bar{g}\}$, para todo $g \notin H$. Entonces, $G = H \amalg gH$, para todo $g \notin H$. Si consideramos la biyección $F\colon G \to G$, $F(g) = g^{-1}$, tenemos que

$$G = F(G) = F(H) \coprod F(gH) = H \coprod Hg^{-1}, \text{ para todo } g \notin H.$$

Si $g \notin H$ entonces $g^{-1} \notin H$, luego $G = H \amalg Hg$ si $g \notin H$. Por tanto, $gH = Hg$, si $g \notin H$, luego $gHg^{-1} = H$ si $g \notin H$. Obviamente, $gHg^{-1} = H$ si $g \in H$.

En conclusión, H es normal en G.

Demos otra demostración. Consideremos G/H como H conjunto: $h \cdot \bar{g} = \overline{hg}$. Como $G/H = \{\bar{1}, \bar{g}\}$ y $H \cdot \bar{1} = \bar{1}$, se tiene que $H \cdot \bar{g} = \bar{g}$. Es decir, $G/H = (G/H)^H = N(H)/H$, luego $N(H) = G$ y H es normal en G.

P20. Consideremos la acción de G por traslaciones a la izquierda en G/H, es decir, el morfismo $\phi\colon G \to \mathrm{Biy}(G/H)$, $\phi(g) := L_g$ ($L_g(\bar{t}) = \overline{gt}$). Sea $\#G = p_1^{n_1} \cdots p_r^{n_r}$, con p_i primos y $p_1 < \cdots < p_r$. Entonces, $\#\mathrm{Biy}(G/H) = p_1!$ y $\mathrm{Im}\,\phi = p_1$. Como $\mathrm{Ker}\,\phi \subseteq H$, entonces $\mathrm{Ker}\,\phi = H$ y H es normal.

P21. Los elementos de A_4 de orden 2 son los del grupo de Klein. Por el teorema de Cauchy o porque el orden del grupo de Klein es 4, existen elementos de orden 3 en el subgrupo G de orden 6, que podemos decir que es $(1,2,3)$ (tomando en vez del subgrupo considerado un conjugado suyo). Como $\langle(1,2,3)\rangle$ es de índice 2 en G, ha de ser normal en G. Ahora bien, $N_{A_4}(\langle(1,2,3)\rangle) = \langle(1,2,3)\rangle$, luego $N_G(\langle(1,2,3)\rangle) = \langle(1,2,3)\rangle$, contradicción.

P22. El automorfismo de G conjugar por $g \in G$, τ_g es igual al automorfismo identidad si y sólo si $\tau_g(t) = t$, para todo $t \in G$, es decir, si y sólo si $gtg^{-1} = t$, que equivale a que $gt = tg$, para todo $t \in G$. En conclusión, $\tau_g = \mathrm{Id} \iff g \in Z(G)$, luego el núcleo del morfismo de grupos $G \to \mathrm{Aut}(G)$ que define la conjugación es el centro $Z(G)$ del grupo G.

Si $G/Z(G) = \langle\bar{g}\rangle$ entonces dados $t, t' \in G$, tenemos que $t = g^n z$ y $t' = g^m z'$ (para ciertos $n, m \in \mathbb{Z}$ y $z, z' \in Z(G)$). Por tanto, $tt' = g^n z g^m z' = g^n g^m z z' = g^{n+m} z z'$ y $t't = g^m z' g^n z = g^m g^n z' z = g^{n+m} z z'$, luego $tt' = t't$ y G es conmutativo.

P23. $Z(G) \subset G$ es no trivial por la proposición 1.7.11, luego $G/Z(G)$ es de orden 1 o p. En cualquier caso $G/Z(G)$ es cíclico y, por el problema 22 G es abeliano.

P24. Sea H el máximo subgrupo incluido estrictamente en G. Sea $t \in G$, $t \notin H$. Entonces, como $\langle t\rangle \not\subseteq H$, tendremos que $H \underset{\neq}{\subset} \langle t\rangle$, luego $G = \langle t\rangle$. Por tanto, $G \simeq \mathbb{Z}/n\mathbb{Z}$. Si $n = r \cdot s$ con r y s primos entre sí, entonces $G \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$, que tiene subgrupos incomparables: $0 \times \mathbb{Z}/s\mathbb{Z}$ y $\mathbb{Z}/r\mathbb{Z} \times 0$. Por tanto, $G \simeq \mathbb{Z}/p^n\mathbb{Z}$. (Observemos que los subgrupos de $\mathbb{Z}/p^n\mathbb{Z}$, que son $\langle\overline{p^i}\rangle$, y no existen pares incomparables).

P25. Sea H un p-subgrupo de Sylow. Consideremos la acción de G en G/H por traslaciones por la izquierda. Entonces, $(G/H)^G = \emptyset$, salvo que $G/H = \{\bar{1}\}$. Entonces, o G es un p-grupo, o bien

$$|G/H| \equiv 0 \mod p$$

y esta igualdad es imposible (pues $|G/H| = |G|/|H|$ es primo con p).

P26. Sea H un subgrupo normal de orden p de un p-grupo G. Consideremos la acción por conjugación de G en H. Entonces, $p = |H| \equiv |H^G|$ (módulo p) y $H^G = H$ (observemos que $1 \in H^G$). Por tanto, $H \subseteq Z(G)$.

P27. Sea H un subgrupo normal de un p-grupo G. Consideremos la acción por conjugación de G en H. Como $1 \in H^G$, entonces $|H^G| \neq 0$. Además, $p^i = |H| \equiv |H^G|$ (módulo p). Entonces, $H \subseteq Z(G) = H^G$ no es trivial.

P28. $|Z(G)| \neq p^2$ porque en tal caso $G/Z(G)$ es cíclico y G sería abeliano. Luego, $|Z(G)| = p$. Por el problema 27, se concluye.

P29. Hagamos operar H en G/H por traslaciones a la izquierda. Se cumple la igualdad $(G/H)^H = N(H)/H$ y $|H| = |(G/H)^H| \mod p$, luego $|N(H)/H| \neq 1$.

P30. Los 3-subgrupos de Sylow de S_3 son $\{\langle(1,2,3)\rangle\}$, los 2-subgrupos de Sylow de S_3 son

$$\{\langle(1,2)\rangle, \langle(2,3)\rangle, \langle(1,3)\rangle\}.$$

Los 3-subgrupos de Sylow de S_4 son $\{\langle(1,2,3)\rangle, \langle(1,2,4)\rangle, \langle(1,3,4)\rangle, \langle(2,3,4)\rangle\}$. Los 2-subgrupos de Sylow de S_4, que son 3, son

$$\{\langle(1,2,3,4),(1,3)\rangle, \langle(1,3,2,4),(1,2)\rangle, \langle(1,2,4,3),(1,4)\rangle\}.$$

Los 5-subgrupos de Sylow de S_5, que son 6, son

$$\{\langle(1,2,3,4,5)\rangle, \langle(1,2,3,5,4)\rangle, \langle(1,2,4,3,5)\rangle, \langle(1,2,4,5,3)\rangle, \langle(1,2,5,3,4)\rangle, \langle(1,2,5,4,3)\rangle\}$$

Los 3-subgrupos de Sylow de S_5, que son 10, son

$$\{\langle(1,2,3)\rangle, \langle(1,2,4)\rangle, \langle(1,2,5)\rangle, \langle(1,3,4)\rangle, \langle(1,3,5)\rangle,$$
$$\langle(1,4,5)\rangle, \langle(2,3,4)\rangle, \langle(2,3,5)\rangle, \langle(2,4,5)\rangle, \langle(3,4,5)\rangle\}$$

Los 2-subgrupos de Sylow de S_5, son 15: para cada S_4 le corresponden 3 2-subgrupos de Sylow.

P31. El único subgrupo normal propio de S_3 es $A_3 = \langle(1,2,3)\rangle$, porque si el subgrupo contiene un dos ciclo, los contiene todos, luego es S_3.

Si el subgrupo normal de S_4 contiene un dos ciclo entonces ha de ser S_4. Si contiene, a un producto de dos ciclos disjuntos entonces contiene al grupo de Klein, K_4. Observemos que $S_4/K_4 \simeq S_3$, que contiene un único subgrupo normal. Luego, en este caso el subgrupo es K_4 ó A_4. Si el grupo no contiene ningún elemento de orden 2, entonces su orden ha de ser primo con 2, es decir, es de orden 3, ha de ser el grupo generado por un tres ciclo, que no es normal.

El único subgrupo normal propio de A_4 es el grupo de Klein.

P32. G contiene un p-subgrupo. Basta ver que todo grupo G de orden p^n contiene un grupo de orden p^i (con $i \leq n$). $Z(G)$ es un subgrupo propio, abeliano, entonces contiene un subgrupo H de orden p, que es normal en G. Por inducción sobre n, G/H contiene un subgrupo, F, de orden p^{i-1}. Si $\pi\colon G \to G/H$ es el morfismo de paso al cociente, entonces $\pi^{-1}(F)$ es el subgrupo de orden p^i buscado.

P33. El número n de subgrupos de orden 25 es justamente el número de 5-subgrupos de Sylow. Sabemos que n divide a 4 y $n \equiv 1 \mod 5$, luego $n = 1$. Por tanto, sólo hay un 5-subgrupo de Sylow, luego es normal.

P34. Léase la demostración del primer teorema de Sylow, teorema 1.8.4.

P35. H está contenido en un p-subgrupo de Sylow. Conjugando obtenemos que H está contenido en todos los p-subgrupos de Sylow de G.

P36. Observemos que $sg^r s = g^{-r}$. Por tanto, $s(sg^r)s = sg^{-r}$ y $g(sg^r)g^{-1} = sg^{r-2}$. Luego, si n es impar $Z(D_n) = \{1\}$ y si n es par $Z(D_n) = \langle g^{n/2} \rangle$.

Observemos que $(sg^r)^2 = 1$. Por tanto, los elementos de orden n son los generadores de $\langle g \rangle = \mathbb{Z}/n\mathbb{Z}$. Además, sg^r opera por conjugación en $\langle g \rangle = \mathbb{Z}/n\mathbb{Z}$ multiplicando por -1 (igual que s). En conclusión,

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Aut}(D_n),\ (\bar{r}, \bar{s}s) \mapsto F_{(\bar{r},\bar{s})},\ \text{donde } F_{(\bar{a},\bar{b})}(s) := sg^a \text{ y } F_{(\bar{a},\bar{b})}(g) := g^b$$

y definimos $(\bar{a}, \bar{b}) * (\bar{u}, \bar{v}) = (\bar{a} + \bar{b} \cdot \bar{u}, \bar{b} \cdot \bar{v})$.

P37. Sea $|G| = 2p$. El número de p-subgrupos de Sylow divide a 2 y es congruente con $1 \mod p$. Luego sólo hay un p-subgrupo de Sylow y es normal. Sea H el p-grupo de Sylow, que es de orden p, luego es cíclico. $H = \langle g \rangle$, $g^p = 1$. Sea s un elemento de orden 2. Obviamente, $H \cap \langle s \rangle = \{1\}$. Por tanto, $H \cdot \langle s \rangle = G$. Si s conmuta con g, entonces G sería abeliano y llegaríamos a contradicción. Por tanto, el automorfismo de $H = \mathbb{Z}/p\mathbb{Z}$, conjugar por s, ha de ser de orden 2, luego es multiplicar por un invertible de $\mathbb{Z}/p\mathbb{Z}$ que al cuadrado es 1, luego es multiplicar por -1. En conclusión, $sgs = g^{-1}$ y el grupo es isomorfo a D_p.

P38. a. Podemos suponer que $p < q$. Entonces el número de q-subgrupos de Sylow divide a p y es congruente con $1 \mod q$, luego sólo hay uno y es normal. Si q no es congruente con 1 módulo p, entonces sólo hay un p-subgrupo de Sylow, y resulta ser normal. Si H es p-subgrupo de Sylow y H' el q-subgrupo de Sylow, tenemos que $G = H \times H' = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}$.

b. Si $q < p$, entonces el p-subgrupo de Sylow es normal. Supongamos $p < q$. Si el q-subgrupo de Sylow no es normal, entonces hay p^2 q-subgrupos de Sylow y $p^2 \equiv 1 \mod q$. Por tanto, existen $p^2 \cdot (q-1)$ elementos de orden q. Luego el complementario de estos elementos ha de ser el único p-subgrupo de Sylow, que es por tanto normal.

c. Si $q < p$, entonces el p-subgrupo de Sylow es normal. Supongamos $p < q$. Si el q-subgrupo de Sylow no es normal, entonces hay dos casos que considerar: 1. Hay p^2 q-subgrupos de Sylow y $p^2 \equiv 1 \mod q$. Por tanto, $p^2 - 1 = (p-1)(p+1)$ es divisible por q. Luego, $q = p + 1$. El único caso posible es $p = 2$ y $q = 3$. Si 2-subgrupo de Sylow no es normal, entonces hay 3 2-subgrupos de Sylow. G opera sobre el conjunto de los 2-subgrupos de Sylow, es decir, tenemos un morfismo $G \to S_3$. El núcleo de este morfismo es el subgrupo normal buscado.

2. p^3 q-subgrupos de Sylow. Luego el número de elementos de orden q es igual a $p^3(q-1) = p^3q - p^3$. Luego, sólo puede haber un p-subgrupo de Sylow, y éste será normal.

P39. Si H es un p-grupo de orden p^n, con $n > 1$, entonces existen subgrupos de orden p^{n-1} y éstos son normales. Luego los grupos de orden p^n, pq, p^2q, p^3q ($n > 1$, p, q primos distintos) no son simples. Sea $|G| = 2^2 \cdot 3^2 = 36$ y supongamos que G es simple. Entonces el número de 3-subgrupos de Sylow es 4. Sean H_3 y H_3' dos 3-subgrupos de Sylow distintos. Los subgrupos de orden 3 de H_3 son normales en H_3 (idem para H_3'). Si $P = H_3 \cap H_3' \neq \{1\}$, entonces el normalizador de P en G, $N(P)$, contiene a H_3 y H_3', luego es G (y P sería normal) ó es un subgrupo de índice 2 (y $N(P)$ sería normal). Hemos llegado a contradicción. Si $|G| = 2 \cdot 3 \cdot 5$ y G es simple entonces el número de 3-subgrupos de Sylow es 10 (luego hay 20 elementos de orden 3) y el número de 5-subgrupos de Sylow es 6 (luego hay 24 elementos de orden 5), pero $20 + 24 > 30$ y llegamos a contradicción.

P40. Sea $|G| = p_1^{n_1} \cdots p_r^{n_r}$ la descomposición de $|G|$ como producto de potencias de primos. Los p_i-subgrupos de Sylow, H_i, son normales. Luego, $H_1 \cdots H_r$ es un subgrupo de G y $H_1 \cdots H_r = H_1 \times \cdots \times H_r$ (procédase por inducción sobre r). Por órdenes, $G = H_1 \times \cdots \times H_r$.

P41. Los grupos de orden $1, 2, 3, 5, 7$ son cíclicos. Si $|G| = 4$, entonces G es conmutativo por el problema 23. Entonces, $G = \mathbb{Z}/4\mathbb{Z}$ ó $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Si $|G| = 6$, entonces el 3-subgrupo $H_3 = \mathbb{Z}/3\mathbb{Z}$ de Sylow es normal. Sea $H_2 = \mathbb{Z}/2\mathbb{Z} = \langle \sigma \rangle$ un 2-subgrupo de Sylow. H_2 opera en $\mathbb{Z}/3\mathbb{Z}$ por conjugación. Si la acción es trivial entonces $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si no, σ opera multiplicando por -1, en este caso $G = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_3$.

Si $|G| = 8$, entonces si es conmutativo es isomorfo a $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ó $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si no es conmutativo existe un elemento, g de orden 4. Entonces, $\langle g \rangle = \mathbb{Z}/4\mathbb{Z}$ es de índice 2, luego es normal. Si existe un elemento, s, de orden 2 no contenido en $\langle g \rangle$. La operación por conjugación de s en $\langle g \rangle = \mathbb{Z}/4\mathbb{Z}$ ha de ser la multiplicación por -1, luego

$$G = \langle g \rangle \rtimes \mathbb{Z}/2\mathbb{Z} = D_4$$

Si no existe un elemento, de orden 2 fuera de $\langle g \rangle$, entonces G contiene 6 elementos de orden 4, 1 de orden 2 (s^2) y el elemento neutro. Sea $s' \notin \langle s \rangle$. Entonces, s' es de orden 4, $\langle s \rangle \cap \langle s' \rangle = \langle s^2 = s'^2 \rangle$ y s' opera por conjugación en $\langle g \rangle = \mathbb{Z}/4\mathbb{Z}$ multiplicando por -1. Entonces, G es isomorfo a $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (donde $(0, \bar{1})$ opera en el primer factor multiplicando por -1) cociente el subgrupo normal $\langle (\bar{2}, \bar{2}) \rangle$. ($G$ resulta ser el subgrupo multiplicativo del álgebra de los cuaterniones formado por $\{1, -1, i, -i, j, -j, k. - k\}$, $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$)

Sea $|G| = 9$. G es conmutativo por el problema 23.Entonces, $G = \mathbb{Z}/9\mathbb{Z}$ ó $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Sea $|G| = 10$. Si G es conmutativo entonces $G = \mathbb{Z}/10\mathbb{Z}$. Si G no es conmutativo, sea $H_5 = \mathbb{Z}/5\mathbb{Z}$ un 5-subgrupo de Sylow (que es normal por ser de índice 2) y $H_2 =$

$\mathbb{Z}/2\mathbb{Z} = \langle s \rangle$ un 5-subgrupo de Sylow. El elemento s opera en H_5 por conjugación multiplicando por -1. Luego, $G = \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_5$.

P42. Si son de orden primo, son cíclicos luego resolubles. Si no son de orden primo contienen algún subgrupo normal. Por inducción sobre el orden, el subgrupo normal y el conúcleo son resolubles, luego el grupo es resoluble.

P43. Por el problema 38, contienen un subgrupo normal. El subgrupo y el conúcleo es de orden una potencia de un primo o un producto de potencias de dos primos (con exponentes menores que los de partida). Por inducción sobre el orden, son resolubles, luego el grupo es resoluble.

P44. $\langle \bar{0} \rangle \subset \langle \bar{9} \rangle \subset \langle \bar{3} \rangle \subset \mathbb{Z}/27\mathbb{Z}$.

$\langle \bar{0} \rangle \subset \langle \bar{9} \rangle \subset \langle \bar{3} \rangle \subset \mathbb{Z}/18\mathbb{Z}$.

$\{\bar{1}\} \subset \{\bar{1}, \bar{4}\} \subset \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\} \subset (\mathbb{Z}/15\mathbb{Z})^*$.

$\{\bar{1}\} \subset \{\bar{1}, \overline{17}\} \subset \{\bar{1}, \bar{9}, \overline{17}, \overline{25}\} \subset \langle \bar{3} \rangle \subset (\mathbb{Z}/32\mathbb{Z})^*$.

$\{\mathrm{Id}\} \subset S_2$.

$\{\mathrm{Id}\} \subset A_3 \subset S_3$.

$\{\mathrm{Id}\} \subset \{\mathrm{Id}, (1,2)(3,4)\} \subset K_4 \subset A_4 \subset S_4$.

$\{\mathrm{Id}\} \subset \langle (1,2,3) \rangle \subset D_3$.

$\{\mathrm{Id}\} \subset \langle (1,3)(2,4) \rangle \subset \langle (1,2,3,4) \rangle \subset D_4$.

$\{\mathrm{Id}\} \subset \langle (1,2,3,4,5) \rangle \subset D_5$.

P45. Sea $|G| = p_1^{n_1} \cdots p_r^{n_r}$ la descomposición de $|G|$ como producto de potencias de primos. Los p_i-subgrupos de Sylow, H_i, son normales. Luego, $G = H_1 \times \cdots \times H_r$. Como cada H_i es resoluble, G es resoluble.

P46. El núcleo del morfismo $S_n \to \mathrm{Biy}(S_n/H) = S_d$ es un subgrupo normal, luego ha de ser A_n (no puede ser S_n, pues S_n no opera trivialmente en S_n/H, ni puede ser $\{1\}$, porque $|S_n| = n! > d! = |S_d|$). La imagen del morfismo es isomorfa a $S_n/A_n = \mathbb{Z}/2\mathbb{Z}$ y es un grupo que opera transitivamente en S_n/H, luego $|S_n/H| = 2$ y $H = A_n$.

P47. La recta proyectiva sobre $\mathbb{F}_5$ tiene 6 puntos. Las proyectividades de la recta proyectiva está determinada por la imagen de 3 puntos. Así pues, P es un subgrupo de S_6 de orden $6 \cdot 5 \cdot 4$, que es de índice 6. P no deja ningún punto de la recta proyectiva fijo, luego no es ninguno de los S_5 obvios de S_6. Consideremos la acción de S_6 por traslaciones por la izquierda en S_6/P. Identifiquemos S_6/P con $\{1,2,3,4,5,6\}$ de modo que $\bar{1}$ se identifique con el elemento 6. Tenemos pues un morfismo $\tau : S_6 \to \mathrm{Biy}(S_6/P) = S_6$, que ha de ser un isomorfismo. $\tau(P)$ deja fijo $\bar{1}$, es decir, el 6. Por tanto, $\tau(P) = S_5$. Por último, τ no puede ser una conjugación, porque las conjugaciones (y sus inversas) permutan los subgrupos S_5 obvios de S_6.

Solución de los problemas del capítulo segundo

P1. Escribamos $M = \oplus^I A$ y $N = \oplus^J A$. Entonces,

$$M \otimes_A N = (\oplus^I A) \otimes_A N = \oplus^I (A \otimes_A N) = \oplus^I N = \oplus^I (\oplus^J A) = \oplus^{I \times J} A$$

Dado $i \in I$, si denotamos $e_i = (0, \overset{i}{\dots}, 1, 0, \cdots) \in \oplus^I A$. Vía estos isomorfismos se tiene que $e_i \otimes e_j \mapsto e_{(i,j)}$.

P2. Dado $m \otimes b \in M \otimes_A B$, tendemos que $m = \sum_i a_i m_i$, luego $m \otimes b = \sum_i m_i \otimes a_i b = \sum_i a - ib \cdot (m \otimes 1) \in \langle m_i \otimes 1 \rangle_{i \in I}$. Luego, $\{m_i \otimes 1\}_{i \in I}$ es un sistema generador del B-módulo $M \otimes_A B$.

Si $L = \oplus^I A$, entonces $L \otimes_A B = (\oplus^I A) \otimes_A B = \oplus^I A \otimes_A B = \oplus^I B$, es un B-módulo libre. Dado $i \in I$, si denotamos $e_i = (0, \overset{i}{\dots}, 1, 0, \cdots) \in \oplus^I A$. Vía estos isomorfismos se tiene que $e_i \otimes 1 \mapsto e_i$.

P3. Es consecuencia inmediata del problema 2.

P4. Las coordenadas de $e \otimes 1$ en la base $\{e_i \otimes 1\}_{1 \le i \le n}$ son $(x_1, \dots, x_n)$: $e \otimes 1 = (\sum_i x_i e_i) \otimes 1 = \sum_i x_i \cdot (e_i \otimes 1)$.

P5. La matriz asociada a $f \otimes \mathrm{Id}$ es $A = (a_{ij})$: $(f \otimes \mathrm{Id})(e_i \otimes 1) = f(e_i) \otimes 1 = \sum_j a_{ji} e'_j \otimes 1 = \sum_j a_{ji} (e'_j \otimes 1)$.

P6. Dado un conjunto de A-módulos $\{M_j\}_{j \in J}$ y de submódulos $\{N_j \subseteq M_j\}_{j \in J}$, tenemos el submódulo $\oplus_{j \in J} N_j \subseteq \oplus_{j \in J} M_j$, $(n_j)_{j \in J} \mapsto (n_j)_{j \in J}$. Además, $(\oplus_{j \in J} M_j)/\oplus_{j \in J} N_j = \oplus_{j \in J} M_j/N_j$, $\overline{(m_j)_{j \in J}} \mapsto (\bar{m}_j)_{j \in J}$.

Dado un conjunto I y un A-módulo M denotemos $M^{(I)} = \oplus_I M$. Dado un morfismo de módulos $f : M \to N$, sea $f^{(I)} : M^{(I)} \to M'^{(I)}$, $f^{(I)}((m_i)_{i \in I}) = (f(m_i))_{i \in I}$. Se cumple que $\mathrm{Ker}\, f^{(I)} = (\mathrm{Ker}\, f)^{(I)}$, $\mathrm{Im}\, f^{(I)} = (\mathrm{Im}\, f)^{(I)}$ y $\mathrm{Coker}\, f^{(I)} = (\mathrm{Coker}\, f)^{(I)}$.

El problema es consecuencia de que si $N = \oplus_I A$, entonces $M \otimes_A N = M^{(I)}$ y dado un morfismo $f : M \to M'$, entonces $f \otimes \mathrm{Id} : M \otimes N \to M' \otimes N$ se identifica con $f^{(I)}$.

P7. El morfismo $g \otimes \mathrm{Id}$ es epiyectivo: Sea $m_3 \otimes n \in M_3 \otimes N$. Sea $m_2 \in M_2$ tal que $g(m_2) = m_3$. Entonces, $(g \otimes \mathrm{Id})(m_2 \otimes n) = m_3 \otimes n$.

$\mathrm{Im}(f \otimes \mathrm{Id}) \subseteq \mathrm{Ker}(g \otimes \mathrm{Id})$: $(g \otimes \mathrm{Id}) \circ (f \otimes \mathrm{Id}) = (g \circ f) \otimes \mathrm{Id} = 0 \otimes \mathrm{Id} = 0$.

Tenemos pues un epimorfismo

$$\overline{g \otimes \mathrm{Id}} : (M_2 \otimes N)/\mathrm{Im}(f \otimes \mathrm{Id}) \to M_3 \otimes N,\ \overline{g \otimes \mathrm{Id}}(\overline{m_2 \otimes n}) = (g \otimes \mathrm{Id})(m_2 \otimes n) = g(m_2) \otimes n.$$

Veamos que es un isomorfismo: Sea $s : M_3 \otimes N \to (M_2 \otimes N)/\mathrm{Im}(f \otimes \mathrm{Id})$, definido por $s(m_3 \otimes n) = \overline{m_2 \otimes n}$, donde m_2 es cualquier elemento de M_2 tal que $g(m_2) = m_3$ (si $g(m'_2) = m_3$, entonces $m_2 = m'_2 + m'$, con $m' \in \mathrm{Ker}\, g = \mathrm{Im}\, f$, luego $\overline{m_2 \otimes n} = \overline{m'_2 \otimes n} + \overline{m' \otimes n} = \overline{m'_2 \otimes n}$). Es claro que $s \circ \overline{g \otimes \mathrm{Id}} = \mathrm{Id}$ y que $\overline{g \otimes \mathrm{Id}} \circ s = \mathrm{Id}$.

En conclusión, $(M_2 \otimes N)/\mathrm{Im}(f \otimes \mathrm{Id}) = M_3 \otimes N$ y $\mathrm{Im}(f \otimes \mathrm{Id}) = \mathrm{Ker}(g \otimes \mathrm{Id})$.

P8. Si tensamos la sucesión exacta

$$0 \to E' \to E \to E/E' \to 0$$

por $\otimes_k V$, obtenemos la sucesión exacta

$$0 \to E' \otimes_k V \to E \otimes_k V \to (E/E') \otimes_k V \to 0$$

Luego, $(E/E') \otimes_k V = (E \otimes_k V)/(E' \otimes_k V)$.

P9. Si tensamos las sucesiones exactas

$$0 \to \operatorname{Ker} f \to E' \to \operatorname{Im} f \to 0, \quad 0 \to \operatorname{Im} f \to E$$

por $\otimes_k V$, obtenemos las sucesiones exactas

$$0 \to (\operatorname{Ker} f) \otimes_k V \to E' \otimes_k V \to (\operatorname{Im} f) \otimes_k V \to 0, \quad 0 \to (\operatorname{Im} f) \otimes_k V \to E \otimes_k V$$

De las que se deduce que $(\operatorname{Im} f) \otimes_k V = \operatorname{Im}(f \otimes \operatorname{Id})$ y que $(\operatorname{Ker} f) \otimes_k V = \operatorname{Ker}(f \otimes \operatorname{Id})$.

P10. Si N y $N' \subseteq M$ son dos A-submódulos y denotamos $\bar{N} = \{\bar{n} \in M/N', \forall n \in N\}$, entonces $(M/N')/\bar{N} = M/(N+N')$. En efecto, el núcleo del epimorfismo $M/N' \to M/(N+N')$, $\bar{m} \mapsto \bar{m}$, es $\bar{N}$, porque si $\bar{m} = 0$ en $M/(N+N')$, entonces $m \in N+N'$, luego existen $n \in N$ y $n' \in N'$ tales que $m = n+n'$ y $\bar{m} = \overline{n+n'} = \bar{n}$ en M/N'. Por tanto, $(M/N')/\bar{N} = M/(N+N')$. Luego, $A/I \otimes_A A/J = (A/I)/J \cdot (A/I) = (A/I)/\bar{J} = A/(I+J)$

Demos otra demostración. Los morfismos $A/I \otimes_A A/J \to A/(I+J)$, $\bar{a} \otimes \bar{b} \mapsto \overline{ab}$ y $A/(I+J) \to A/I \otimes_A A/J$, $\bar{a} \mapsto \bar{a} \otimes 1$, están bien definidos y son inversos entre sí.

P11. Por el teorema chino de los restos $A/(IJ) = A/I \times A/J$. Por tanto,

$$\begin{aligned} M/IJM &= M \otimes_A (A/(IJ)) = M \otimes_A (A/I \times A/J) = (M \otimes_A A/I) \oplus (M \otimes_A A/J) \\ &= M/IM \oplus M/JM \end{aligned}$$

P12.

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(n\mathbb{Z} + m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$$

P13. Los morfismos $A[x_1,\dots,x_n] \otimes_A B \to B[x_1,\dots,x_n]$, $p(x) \otimes b \mapsto b \cdot p(x)$ y $B[x_1,\dots,x_n] \to A[x_1,\dots,x_n] \otimes_A B$, $\sum_\alpha b_\alpha \otimes x^\alpha \mapsto \sum_\alpha x^\alpha \otimes b_\alpha$ son inversos entre sí.

P14. Denotemos $R = A[x_1,\dots,x_n]$. Entonces,

$$\begin{aligned} R/(p_1,\dots,p_r) \otimes_A B &= (R/(p_1,\dots,p_r) \otimes_R R) \otimes_A B \\ &= R/(p_1,\dots,p_r) \otimes_R B[x_1,\dots,x_n] \\ &= B[x_1,\dots,x_n]/(p_1,\dots,p_r) \cdot B[x_1,\dots,x_n] \\ &= B[x_1,\dots,x_n]/(p_1,\dots,p_r) \end{aligned}$$

P15. Sea $I: E^* \otimes F \to \mathrm{Hom}_k(E,F)$, el morfismo definido por $I(w \otimes f)(e) := w(e) \cdot f$, para todo $e \in E$ (y todo $w \in E^*$ y $f \in F$). Sea $\{e_i\}_{i\in I}$ una base de E, $\{w_i\}_{i\in I}$ la base dual de E^* y sea $\{f_j\}$ una base de F. Entonces, $\{w_i \otimes f_j\}_{(i,j)\in I\times J}$ es una base de $E^* \otimes F$. Se tiene que $I(w_i \otimes f_j)(e_k) = 0$, para $k \neq i$ y $I(w_i \otimes f_j)(e_i) = f_j$, para $k = i$; es decir, $\{I(w_i \otimes f_j)\}_{(i,j)\in I\times J}$ es la base estándar de $\mathrm{Hom}_k(E,F)$ (fijadas las bases de E y F). Por tanto, I es un isomorfismo.

P16. Sea $I: E^* \otimes_k \overset{p}{\cdots} \otimes_k E^* \otimes_k E \otimes_k \overset{q}{\cdots} \otimes_k E \to T^p_q E$, el morfismo definido por

$$I(w_1 \otimes \cdots \otimes w_p \otimes e_1 \otimes \cdots \otimes e_q)(f_1,\ldots,f_p,v_1,\ldots,v_p) = w_1(f_1)\cdots w_p(f_p)\cdot v_1(e_1)\cdots v_q(e_q),$$

$\forall w_1,\ldots,w_p,v_1,\ldots,v_p \in E^*$, $\forall e_1,\ldots,e_q,f_1,\ldots,f_p \in E$. Sea $\{e_i\}_{i\in I}$ una base de E y $\{w_i\}_{i\in I}$ la base dual de E^*. Entonces,

$$I(w_{i_1} \otimes \cdots \otimes w_{i_p} \otimes e_{j_1} \otimes \cdots \otimes e_{j_q})(e_{r_1},\ldots,e_{r_p},w_{s_1},\ldots,w_{s_q}) = \delta_{i_1 r_1}\cdots\delta_{i_p r_p}\cdot\delta_{j_1 s_1}\cdots\delta_{j_q s_q}$$

Luego, $\{I(w_{i_1} \otimes \cdots \otimes w_{i_p} \otimes e_{j_1} \otimes \cdots \otimes e_{j_q})\}$ es la base estándar de $T^p_q E$ (fijada la base de E). Por lo tanto, I es un isomorfismo.

P17. $\frac{a}{1} = 0 = \frac{0}{1}$ en A_S si y sólo si existe $s \in S$ tal que $sa = 0$.

P18. Sea $S = \{\bar{1},\bar{2},\bar{4}\} \subset \mathbb{Z}/6\mathbb{Z}$. El morfismo de localización $\mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z})_S$ no es inyectivo, por el ejercicio anterior.

P19. Tenemos la inclusión $\mathbb{Z}[x] \hookrightarrow \mathbb{Q}(x)$. La imagen de todo elemento no nulo de $\mathbb{Z}[x]$ es invertible. Por la propiedad universal de la localización tenemos el morfismo de cuerpos $\mathbb{Z}[x]_{\mathbb{Z}[x]\setminus\{0\}} \to \mathbb{Q}(x)$, $\frac{p(x)}{q(x)} \mapsto \frac{p(x)}{q(x)}$, que ha de ser inyectivo. Es epiyectivo: Dada una fracción $\frac{r(x)}{s(x)} \in \mathbb{Q}(x)$, existen $n,m \in \mathbb{Z}$ tales que $r'(x) = n \cdot r(x), s'(x) = m \cdot s(x) \in \mathbb{Z}[x]$. Obviamente, $\frac{m\cdot r'(x)}{n\cdot s'(x)} \mapsto \frac{r(x)}{s(x)}$.

En conclusión, $\mathbb{Z}[x]_{\mathbb{Z}[x]\setminus\{0\}} = \mathbb{Q}(x)$.

$\mathbb{Z}[\alpha] \subset \mathbb{C}$ es un anillo íntegro, incluido en $\mathbb{Q}(\alpha)$. De nuevo, el cuerpo de fracciones de $\mathbb{Z}[\alpha]$ está incluido en $\mathbb{Q}(\alpha)$ y argumentando igual antes se tiene la igualdad.

P20. La aplicación $M \times A_S \to M_S$, $(m,a/s) \mapsto am/s$ está bien definida y es A-bilineal. Tenemos pues el morfismo $M \otimes A_S \to M_S$ $m \otimes a/s \mapsto am/s$. La aplicación $M_S \to M \otimes A_S$, $m/s \mapsto m \otimes 1/s$ está bien definida. Estas dos aplicaciones son inversas entre sí.

1. Por la propiedad universal de la localización, el morfismo $B \to B_S$, $b \mapsto \frac{b}{1}$, factoriza vía $B_{f(S)} \to B_S$, $\frac{b}{f(s)} \mapsto \frac{b}{s}$. Tenemos el morfismo $f: B \otimes_A A_S \to B_S$, $f(b \otimes \frac{a}{s}) = \frac{b}{1} \cdot \frac{f(a)}{f(s)}$.

Por la propiedad universal de la localización, el morfismo $B \to B \otimes_A A_S$, $b \mapsto b \otimes 1$, factoriza vía $g: B_{f(S)} \to B \otimes_A A_S$, $g(\frac{b}{f(s)}) = b \otimes \frac{1}{s}$.

Los morfismos f y g son inversos entre sí.

P21. $(A_S)_{S'} = A_S \otimes_A A_{S'}$. Tenemos morfismos naturales $A_S \to A_{S\cdot S'}$, $\frac{a}{s} \mapsto \frac{a}{s}$ y $A_{S'} \to A_{S\cdot S'}$, $\frac{a}{s'} \mapsto \frac{a}{s'}$. Sea $f : A_S \otimes_A A_{S'} \to A_{SS'}$, $f(\frac{a}{s} \otimes \frac{a'}{s'}) := \frac{a}{s} \cdot \frac{a'}{s'}$.

Por la propiedad universal de la localización, el morfismo $A \to A_S \otimes_A A_{S'}$, $a \mapsto a \otimes 1$, factoriza vía $g : A_{SS'} \to A_S \otimes_A A_{S'}$, $\frac{a}{ss'} \mapsto (a \otimes 1) \cdot (\frac{1}{s} \otimes \frac{1}{s'}) = \frac{a}{s} \otimes \frac{1}{s'}$.

Los morfismos f y g son inversos entre sí.

Solución de los problemas del capítulo tercero

P1. $\alpha + 2 = \overline{x+2} \in \mathbb{Q}[x]/(2x^3 + 4x^2 - x - 2) = A$ es invertible, si y sólo si $(\overline{x+2}) = A$, es decir, $(x + 2, 2x^3 + 4x^2 - x - 2) = \mathbb{Q}[x]$. Por tanto, $\alpha + 2$ es invertible en A si y sólo si $x+2$ y $2x^3+4x^2-x-2$ son primos entre sí, es decir, -2 no es raíz de $2x^3+4x^2-x-2$. Pero, $2\cdot(-2)^3+4\cdot(-2)^2-(-2)-2 = 0$, luego $\alpha+2$ no es invertible. $\alpha-2$ es invertible, porque 2 no es raíz de $2x^3 + 4x^2 - x - 2$.

P2. Los polinomios $x^3 - x - 1$ y $x + 2$ son primos entre sí y tenemos que

$$\frac{-1}{7} \cdot (x^3 - x - 1) + \frac{x^2 - 2x^2 + 3}{7} \cdot (x + 2) = 1$$

Tomando clases en $K = \mathbb{Q}[x]/(x^3 - x - 1)$, tenemos que $\frac{\alpha^2-2\alpha^2+3}{7} \cdot (\alpha + 2) = 1$, luego $\frac{1}{\alpha+2} = \frac{\alpha^2-2\alpha^2+3}{7}$.

- $(2 + \alpha)^3 = (2 + \bar{x})^3 = \overline{x^3 + 6x^2 + 12x + 8} = \overline{6x^2 + 13x + 9} \neq \bar{1}$ (pues una base de la $\mathbb{Q}$-álgebra $\mathbb{Q}[x]/(x^3 - x - 1)$ es $\bar{1}, \bar{x}, \bar{x}^2$).

- El polinomio $x^2 - 2$ tiene alguna raíz en K, si y sólo si $\sqrt{2} \in K$, es decir, $\mathbb{Q}[\sqrt{2}] \subseteq K$. Pero esta inclusión es imposible porque $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}] = 2$ no divide a $\dim_{\mathbb{Q}} K = 3$.

- Consideremos el endomorfismo $\mathbb{Q}$-lineal $K \overset{(\alpha^2+1)\cdot}{\to} K$, $\mu \mapsto (\alpha^2 + 1) \cdot \mu$. Resulta que el polinomio característico de este endomorfismo anula a $\alpha^2 + 1$. La matriz de este endomorfismo es

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

y su polinomio característico es $x^3 - 5x^2 + 8x - 5$.

P3. Supongamos que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$. Si $\sqrt{a} \in \mathbb{Q}$, entonces $\sqrt{b} \in \mathbb{Q}(\sqrt{a}) = \mathbb{Q}$, luego $\frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$ y a/b es un cuadrado en $\mathbb{Q}$. Si $\sqrt{a} \notin \mathbb{Q}$, entonces $\sqrt{b} \notin \mathbb{Q}$. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{a}) = 2$ y $\sqrt{b} = c_1 + c_2 \cdot \sqrt{a}$, con $c_1, c_2 \in \mathbb{Q}$ y $c_2 \neq 0$. Si elevamos al cuadrado, tenemos $b = (c_1^2 + c_2^2 a) + 2c_1c_2 \cdot \sqrt{a}$, luego $c_1c_2 = 0$ y $c_1 = 0$. En conclusión, $\frac{\sqrt{a}}{\sqrt{b}} = 1/c_2 \in \mathbb{Q}$ y a/b es un cuadrado en $\mathbb{Q}$.

Si $a/b = c^2$, con $c \in \mathbb{Q}$, entonces $\sqrt{a} = c \cdot \sqrt{b}$ y $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$.

P4. Por el criterio de Eisenstein, $x^n - 2$ es irreducible. Luego, $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[x]/(x^n - 2)$ y su grado es n.

P5. El polinomio x^3-2 anula a $\sqrt[3]{2}$ y es irreducible porque si lo fuese tendría raíces racionales. Por tanto, x^3-2 es el polinomio mínimo anulador de $\sqrt[3]{2}$ y $\mathbb{Q}[x]/(x^3-2) \simeq \mathbb{Q}(\sqrt[3]{2})$. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$. $\mathbb{Q}(\sqrt{2}) \not\subset \mathbb{Q}(\sqrt[3]{2})$, porque $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$ no divide a $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$.

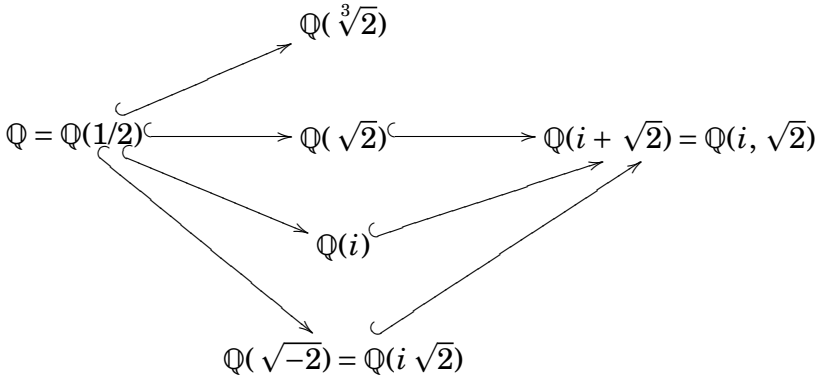
El polinomio x^4-2 es irreducible por el criterio de Eisenstein y anula a $\sqrt[4]{2}$, por tanto es su polinomio mínimo anulador. Luego, $\mathbb{Q}(\sqrt[4]{2}) \simeq \mathbb{Q}[x]/(x^4-2)$, que es un $\mathbb{Q}$-espacio vectorial de dimensión 4. $\mathbb{Q}(\sqrt[3]{2}) \not\subset \mathbb{Q}(\sqrt[4]{2})$, porque $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$ no divide a $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}) = 4$.

P6. $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$, porque $\sqrt[4]{2}, i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2}, i)$ y $\sqrt[4]{2}, i \in \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$.

$\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}[x]/(x^2+2)$, porque x^2+2 anula a $i\sqrt{2}$ y es irreducible. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(i\sqrt{2}) = 2$. $\mathbb{Q}(2^{-1/2}, i) = \mathbb{Q}(\sqrt{2}, i)$ es de grado 4 sobre $\mathbb{Q}$, porque $i \notin \mathbb{Q}(\sqrt{2})$ y tenemos la composición de extensiones $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, i)$. Luego, $\mathbb{Q}(i\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, i)$.

Una base del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}(\sqrt{2}, i)$, es $1, \sqrt{2}, i, i\sqrt{2}$. Obviamente, $\mathbb{Q}(i+\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Observemos que $(i+\sqrt{2})^2 = 1 + 2i\sqrt{2}$. Entonces, $1, i+\sqrt{2}, 1+2i\sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$ y son linealmente independientes. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(i+\sqrt{2}) = 4$ porque $\dim_{\mathbb{Q}} \mathbb{Q}(i+\sqrt{2}) \geq 3$ y divide a $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, i) = 4$. En conclusión, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i+\sqrt{2})$.

P7.



P8. Si $\alpha \in L$ es una raíz de $p(x)$, entonces $k[x]/(p(x)) \simeq k(\alpha) \hookrightarrow L$ y el grado de L sería divisible por el grado de $p(x)$.

P9. Por el problema 8 x^3-3 no tiene raíces en $\mathbb{Q}(\sqrt{2})$. Por tanto, x^3-3 es el polinomio mínimo anulador de $\sqrt[3]{3}$ con coeficientes en $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ es una extensión de cuerpos de grado 3.

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) &= \mathbb{Q}(\sqrt{2}) \cdot 1 \oplus \mathbb{Q}(\sqrt{2}) \cdot \sqrt[3]{3} \oplus \mathbb{Q}(\sqrt{2}) \cdot (\sqrt[3]{3})^2 \\ &= \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{2} \oplus \mathbb{Q} \cdot \sqrt[3]{3} \oplus \mathbb{Q} \cdot \sqrt{2} \cdot \sqrt[3]{3} \oplus \mathbb{Q} \cdot \sqrt[3]{3}^2 \oplus \mathbb{Q} \cdot \sqrt{2} \cdot \sqrt[3]{3}^2\end{aligned}$$

Tenemos que

$$\begin{aligned}
1 &= 1\cdot 1+0\cdot\sqrt{2}+0\cdot\sqrt[3]{3}+0\cdot\sqrt{2}\sqrt[3]{3}+0\cdot\sqrt[3]{3}^2+0\cdot\sqrt{2}\sqrt[3]{3}^2\\
\sqrt{2}+\sqrt[3]{3} &= 0\cdot 1+1\cdot\sqrt{2}+1\cdot\sqrt[3]{3}+0\cdot\sqrt{2}\sqrt[3]{3}+0\cdot\sqrt[3]{3}^2+0\cdot\sqrt{2}\sqrt[3]{3}^2\\
(\sqrt{2}+\sqrt[3]{3})^2 &= 2\cdot 1+0\cdot\sqrt{2}+0\cdot\sqrt[3]{3}+\cdot 2\sqrt{2}\sqrt[3]{3}+1\cdot\sqrt[3]{3}^2+0\cdot\sqrt{2}\sqrt[3]{3}^2\\
(\sqrt{2}+\sqrt[3]{3})^3 &= 3\cdot 1+2\cdot\sqrt{2}+6\cdot\sqrt[3]{3}+0\cdot\sqrt{2}\sqrt[3]{3}+0\cdot\sqrt[3]{3}^2+3\cdot\sqrt{2}\sqrt[3]{3}^2\\
(\sqrt{2}+\sqrt[3]{3})^4 &= 4\cdot 1+12\cdot\sqrt{2}+3\cdot\sqrt[3]{3}+8\cdot\sqrt{2}\sqrt[3]{3}+12\cdot\sqrt[3]{3}^2+0\cdot\sqrt{2}\sqrt[3]{3}^2\\
(\sqrt{2}+\sqrt[3]{3})^5 &= 60\cdot 1+4\cdot\sqrt{2}+20\cdot\sqrt[3]{3}+15\cdot\sqrt{2}\sqrt[3]{3}+3\cdot\sqrt[3]{3}^2+20\cdot\sqrt{2}\sqrt[3]{3}^2\\
(\sqrt{2}+\sqrt[3]{3})^6 &= 17\cdot 1+120\cdot\sqrt{2}+90\cdot\sqrt[3]{3}+24\cdot\sqrt{2}\sqrt[3]{3}+60\cdot\sqrt[3]{3}^2+18\cdot\sqrt{2}\sqrt[3]{3}^2
\end{aligned}$$

Los cuatro primeros son linealmente independientes, luego $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}+\sqrt[3]{3})\geq 4$ y divide a 6. Por tanto, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}+\sqrt[3]{3})=6$ y $\mathbb{Q}(\sqrt{2}+\sqrt[3]{3})=\mathbb{Q}(\sqrt{2},\sqrt[3]{3})$. Tenemos que

$$\begin{pmatrix}1&0&2&3&4&60\\0&1&0&2&12&4\\0&1&0&6&3&20\\0&0&2&0&8&15\\0&0&1&0&12&3\\0&0&0&3&0&20\end{pmatrix}^{-1}\cdot\begin{pmatrix}17\\120\\90\\24\\60\\18\end{pmatrix}=\begin{pmatrix}-1\\36\\-12\\6\\6\\0\end{pmatrix}$$

Luego, el polinomio anulador de $\sqrt{2}+\sqrt[3]{3}$ resulta ser $x^6-6x^4-6x^3+12x^2-36x+1$.

P10. K es un $\mathbb{F}_2$-espacio vectorial de dimensión 3, es isomorfo como $\mathbb{F}_2$-espacio vectorial a $\mathbb{F}_2^3$, que tiene $2^3=8$ elementos. $K^*=K\setminus\{0\}$ es un grupo con la multiplicación de orden 7, luego es cíclico y está generado por cualquier elemento, distinto de 1. Luego, $K^*=\{\alpha,\alpha^2,\ldots,\alpha^7=1\}$.

P11. $\mathbb{F}_2[x]/(x^2+x+1)$ y $\mathbb{F}_3[x]/(x^2+1)$.

P12. Las raíces de x^3-1 son $\{e^{2\pi i/3},e^{4\pi i/3},e^{6\pi i/3}=1\}$ y $\mathbb{Q}(e^{2\pi i/3},e^{4\pi i/3},e^{6\pi i/3})=\mathbb{Q}(e^{2\pi i/3})$. Tenemos que $x^3-1=(x-1)(x^2+x+1)$. El polinomio x^2+x+1 es irreducible de raíces $e^{2\pi i/3},e^{4\pi i/3}$. Luego el polinomio mínimo anulador de $e^{2\pi i/3}$ es x^2+x+1 y $\dim_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/3})=2$.

Observemos que α es una raíz de x^3-1 si y sólo si $-\alpha$ es una raíz de x^3+1. Luego, la $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de x^3+1 coincide con $\mathbb{Q}(e^{2\pi i/3})$. $\mathbb{Q}(e^{2\pi i/6})$ es la $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de x^6-1. Luego, $\dim_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/6})=\dim_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/3})=2$.

La $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de x^4-1, es $\mathbb{Q}(e^{2\pi i/4})$. Además, $x^4-1=(x^2-1)(x^2+1)$, x^2+1 es irreducible y $e^{2\pi i/4}$ es raíz de x^2+1. Luego, $\dim_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/4})=2$.

Observemos que $x^8-1=(x^4-1)\cdot(x^4+1)$. Las raíces de x^8-1 son las potencias de $e^{2\pi i/8}$ y $e^{2\pi i/8}$ es raíz de x^4+1 (y no de x^4-1). Observemos que $\mathbb{Q}(e^{2\pi i/4}=i)\subsetneq$

$\mathbb{Q}(e^{2\pi i/8})$. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/8}) = 2 \cdot m$, con $m > 1$. El polinomio anulador de $e^{2\pi i/8}$ divide a $x^4 + 1$ y es de grado $2 \cdot m$, luego es $x^4 + 1$. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/8}) = 4$.

Observemos que $x^5 - 1 = (x-1)\cdot(x^4 + x^3 + x^2 + x + 1)$. Además, si hacemos el cambio de variable $x = y + 1$, obtenemos

$$(x^4 + x^3 + x^2 + x + 1) = \frac{x^5 - 1}{x - 1} = \frac{(y+1)^5 - 1}{y + 1 - 1} = y^4 + 5y^3 + 10y^2 + 10y + 5,$$

que es irreducible por el criterio de Eisenstein. Por tanto, $x^4 + x^3 + x^2 + x + 1$ es irreducible y la subextensión de $\mathbb{C}$ generada por sus raíces, $\mathbb{Q}(e^{2\pi i/5})$, es de grado 4.

Observemos que α es una raíz de $x^5 + 11$ si y sólo si $-\alpha$ es raíz de $x^5 - 1$, luego la subextensión de $\mathbb{C}$ generada por sus raíces es $\mathbb{Q}(e^{2\pi i/5})$

P13. Las raíces de $x^3 - 2$ son $\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}$ y $e^{4\pi i/3} \cdot \sqrt[3]{2}$. Luego,

$$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}, e^{4\pi i/3} \cdot \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

y $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = 3 \cdot 2 = 6$.

La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 - 2$, es $\mathbb{Q}(\sqrt[4]{2}, i)$. Como $i \notin \mathbb{Q}(\sqrt[4]{2})$, entonces $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}, i) = 4 \cdot 2 = 8$.

La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 + 2$, es

$$\begin{aligned}\mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/8} \cdot \sqrt[4]{2}, e^{5\pi i/8} \cdot \sqrt[4]{2}, e^{7\pi i/8} \cdot \sqrt[4]{2}) &= \mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/8}) = \mathbb{Q}(\sqrt[4]{2}, \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot i) \\ &= \mathbb{Q}(\sqrt[4]{2}, i)\end{aligned}$$

que es una extensión de grado 8.

Consideremos el polinomio $x^4 - x^2 + 1$. Sea $y = x^2$, las raíces de $y^2 - y + 1$, son $\frac{1 \pm \sqrt{3}i}{2}$. Luego las raíces de $x^4 - x^2 + 1$ son $\pm\sqrt{\frac{1 \pm \sqrt{3}i}{2}}$. La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 - x^2 + 1$ es $\mathbb{Q}(\frac{\sqrt{3} \pm i}{2}) = \mathbb{Q}(\sqrt{3}, i)$ que es una extensión de grado 4.

Tenemos que $x^4 + x^2 - 2 = (x-1)(x+1)(x^2+2)$. Luego, La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 + x^2 - 2$ es $\mathbb{Q}(\sqrt{-2})$, que es de grado 2.

Tenemos que $x^3 - 4x^2 + 5 = (x+1)(x^2 - 5x + 5)$. Luego, La $\mathbb{Q}$-subextensión generada por las raíces de $x^3 - 4x^2 + 5$ es $\mathbb{Q}(\sqrt{5})$, que es de grado 2.

P14. Como $i \notin \mathbb{Q}(\sqrt[4]{2})$, entonces $\mathbb{Q}(i, \sqrt[4]{2})$ es una $\mathbb{Q}$-extensión de grado 8, luego es una $\mathbb{Q}(i)$-extensión de grado 4. Por tanto, el polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(i)$ es $x^4 - 2$.

$\mathbb{Q}(\sqrt[4]{2})$ es una $\mathbb{Q}(\sqrt{2})$-extensión de grado 2, luego el polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(\sqrt{2})$ es $x^2 - \sqrt{2}$.

$\mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{2})$ es una $\mathbb{Q}$-extensión de grado 12, luego es una $\mathbb{Q}(\sqrt[3]{2})$-extensión de grado 4. El polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(\sqrt[3]{2})$ es $x^4 - 2$.

P15. Sea $\alpha \in K - k$. Obviamente, $\{1, \alpha\}$ es una base del k-espacio vectorial K. Luego, existen $b, c \in k$ tales que $\alpha^2 = c \cdot 1 + b \cdot \alpha$ y $\alpha = \frac{b \pm \sqrt{b^2 - 4c}}{2}$ y $K = k(\alpha) = k(\sqrt{b^2 - 4c})$.

La $\mathbb{Z}/2\mathbb{Z}$-extensión $K = \mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$, no es extender por un radical cuadrático de 0 ó $1 \in \mathbb{Z}/2\mathbb{Z}$.

P16. $x^2 + 1$ y $x^3 - 2$ son polinomios primos entre sí, luego

$$\mathbb{Q}[x]/((x^2+1)\cdot(x^3-2)) = \mathbb{Q}[x]/(x^2+1) \times \mathbb{Q}[x]/(x^3-2) = \mathbb{Q}(i) \times \mathbb{Q}(\sqrt[3]{2})$$

P17. $x^2 + 1$ y $(x+1)^2 + 1 = x^2 + 2x + 2$ son polinomios primos entre sí, luego

$$\mathbb{Q}[x]/((x^2+1)(x^2+2x+2)) = \mathbb{Q}[x]/(x^2+1) \times \mathbb{Q}[x]/(x^2+2x+2) = \mathbb{Q}(i) \times \mathbb{Q}(i)$$

P18. Resulta del epimorfismo obvio $\mathbb{Q}(\alpha_1) \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha_n) \to \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $1 \otimes \cdots \otimes \alpha_i \otimes \cdots \otimes 1 \mapsto \alpha_i$ y de los epimorfismos $\mathbb{Q}[x]/(p_i(x)) \to \mathbb{Q}(\alpha_i)$, $\overline{q(x)} \mapsto q(\alpha_i)$.

P19. Consideremos el epimorfismo $L \otimes_k L \to L$, $l \otimes l' \mapsto l \cdot l'$. Todo morfismo entre cuerpos es inyectivo (o nulo). Por tanto, si $L \otimes_k L$ es un cuerpo entonces $L \otimes_k L = L$. Entonces, el morfismo $L \to L \otimes_k L$, $l \mapsto l \otimes 1$ es un isomorfismo, porque es el morfismo inverso. Ahora bien, si $\{e_1 = 1, \ldots, e_n\}$ es una base del k-espacio vectorial L, entonces $\{e_i \otimes e_j\}$ es una base de L. Tenemos que $\{e_i \otimes 1\}$ es una base de $L \otimes_k L$. En conclusión, L es un k-espacio vectorial de dimensión 1, luego $L = k$.

Si $L = k$, entonces $L \otimes_k L = k \otimes_k k = k$, que es cuerpo.

P20. Sea $\mathfrak{m}$ un ideal maximal de $L \otimes_k L'$. Entonces, $\dim_k(L \otimes_k L')/\mathfrak{m} \leq \dim_k(L \otimes_k L') = n \cdot m$. Por otra parte, $(L \otimes_k L')/\mathfrak{m}$ es una L-álgebra finita, luego su k-dimensión es múltiplo de $\dim_k L = n$. Igualmente, $\dim_k(L \otimes_k L')/\mathfrak{m}$ es múltiplo de m. Con todo, $\dim_k(L \otimes_k L')/\mathfrak{m} = n \cdot m = \dim_k(L \otimes_k L')$. Luego, $(L \otimes_k L')/\mathfrak{m} = L \otimes_k L'$ y $L \otimes_k L'$ es un cuerpo.

P21. $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ no es cuerpo y $\mathbb{Q}(\sqrt{2}) \otimes \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ es cuerpo.

P22. $\mathbb{C}$ es un cuerpo algebraicamente cerrado, por tanto si $\mathbb{C} \hookrightarrow K$ es una extensión finita de cuerpos, toda $\alpha \in K$ es algebraico sobre $\mathbb{C}$, luego $\alpha \in \mathbb{C}$ y $K = \mathbb{C}$. Toda k-álgebra finita reducida es producto directo de extensiones finitas de cuerpos de k. Por tanto, toda $\mathbb{C}$-álgebra finita reducida es trivial. $\mathbb{C}[x]/(x^2)$ es una $\mathbb{C}$-álgebra finita con nilpotentes, luego no trivial.

P23. Sea $\mathbb{R} \hookrightarrow K$ una extensión finita de $\mathbb{R}$. Entonces, $K \otimes_{\mathbb{R}} \mathbb{C}$ es una $\mathbb{C}$-álgebra finita racional (es más trivial). Luego, $\mathrm{Hom}_{\mathbb{R}-alg}(K, \mathbb{C}) = \mathrm{Hom}_{\mathbb{C}-alg}(K \otimes_{\mathbb{R}} \mathbb{C}, \mathbb{C}) \neq \emptyset$ y tenemos un morfismo de $\mathbb{R}$-algebras $K \hookrightarrow \mathbb{C}$. Por dimensiones, $K = \mathbb{R}$ ó $K = \mathbb{C}$. Toda k-álgebra finita reducida es producto directo de extensiones finitas de cuerpos de k. Por tanto, toda $\mathbb{R}$-álgebra finita reducida es isomorfa a $\mathbb{R} \oplus \overset{n}{\cdots} \oplus \mathbb{R} \oplus \mathbb{C} \oplus \overset{m}{\cdots} \oplus \mathbb{C}$ para ciertos $n, m \in \mathbb{N}$.

P24. $\mathbb{Q}(\sqrt[5]{5}, e^{2\pi i/5})$ es una extensión de grado 20 sobre $\mathbb{Q}$, luego es una $\mathbb{Q}(\sqrt[5]{5})$-extensión de grado 4 y el polinomio mínimo anulador de $e^{2\pi i/5}$) con coeficientes en $\mathbb{Q}(\sqrt[5]{5})$ es $x^4+x^3+x^2+x+1$.

$$\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[5]{5}, e^{2\pi i/5})) = \{\tau_{rs}\}_{1\le r\le 4; 1\le s\le 5},$$

con $\tau_{rs}(e^{2\pi i/5}) = e^{r\cdot 2\pi i/5}$ y $\tau_{rs}(\sqrt[5]{5}) = e^{s\cdot 2\pi i/5}\cdot\sqrt[5]{5}$.

P25. Escribamos $p(x) = (x-\alpha)^m\cdot q(x)$, con $q(\alpha)\neq 0$. Entonces, $p'(x) = m\cdot(x-\alpha)^{m-1}q(x) + (x-\alpha)^m\cdot q'(x) = (x-\alpha)^{m-1}\cdot(mq(x)+(x-\alpha)q'(x))$, que es de multiplicidad $m-1$ en característica cero y de multiplicidad mayor o igual que $m-1$ en característica prima (observemos que $m=0\in k$, si $m\in\mathbb{N}$ es múltiplo de la característica). Si $m=1$, entonces α no es raíz de $p'(x)$.

P26. Es inmediato por el problema 25.

P27. Las raíces múltiples de $p(x)$ son las raíces de $m.c.d.(p(x), p'(x))$. Si hay raíces múltiples, entonces $m.c.d(p(x), p'(x))$ es un polinomio de grado mayor que cero. Si $p'(x)\neq 0$, entonces $m.c.d(p(x), p'(x))$ es un polinomio de grado menor que el de $p(x)$, que lo divide. En este caso, $p(x)$ no sería irreducible y llegamos a contradicción.

Si $p'(x)=0$, entonces $m.c.d.(p(x), p'(x)) = p(x)$ y todas las raíces son de $p(x)$ son múltiples. Si $p'(x)\neq 0$, entonces $m.c.d.(p(x), p'(x)) = (1)$ y $p(x)$ no tiene raíces múltiples.

P28. Sea $p(x) = x^4+4x^2+1\in k[x]$, entonces $p'(x) = 4x^3+8x = 4x(x^2+2)$ que es primo con $p(x)$ si $k=\mathbb{Q},\mathbb{F}_5$, luego $p(x)$ no tiene raíces múltiples sobre estos cuerpos. Sobre $\mathbb{F}_3$, $x^2+2 = x^2-1 = (x+1)(x-1)$. Las raíces comunes son el ± 1. Luego, ± 1 son raíces de $p(x)$ de multiplicidad 2. Sobre $\mathbb{F}_2$, $p(x) = x^4+1 = (x+1)^4$, luego $p(x)$ tiene una única raíz, 1, que es de multiplicidad 4.

Sea $p(x) = 4x^4-4x^3-3x^2+2x+1$, entonces $p'(x) = 16x^3-12x^2-6x+2$. Sobre $\mathbb{Q}$ y $\mathbb{F}_5$ se tiene que $m.c.d(p(x), p'(x)) = 2x^2-x-1 = 2(x-1)(x+1/2)$, luego $1, 1/2$ son las raíces múltiples, de multiplicidad 2. Sobre $\mathbb{F}_2$, $p(x) = x^2-x+1 = (x+1)^2$, que tiene 1 como raíz múltiple de multiplicidad 2. Sobre $\mathbb{F}_3$, $m.c.d(p(x), p'(x)) = p'(x) = x^3-1 = (x-1)^3$ y $p(x) = (x-1)^4$, luego 1 es de multiplicidad 4.

Solución de los problemas del capítulo cuarto

P1. Sea una extensión de cuerpos $k\hookrightarrow k(\alpha)$ separable y $p(x)$ el polinomio mínimo anulador de α, con coeficientes en k. Entonces, $k(\alpha) = k[x]/(p(x))$. Si $\alpha_1,\ldots,\alpha_n$ son las raíces de $p(x)$, entonces una extensión Σ trivializa a $k(x)/(p(x)$ si y sólo si $\alpha_1,\ldots,\alpha_n\in\Sigma$.

El polinomio mínimo anulador de $\sqrt[3]{2}$ es x^3-2, cuyas raíces son $\sqrt[3]{2}$, $\sqrt[3]{2}\cdot e^{2\pi i/3}$, $\sqrt[3]{2}\cdot e^{4\pi i/3}$. La mínima extensión trivializante de $\mathbb{Q}(\sqrt[3]{2})$, es

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\cdot e^{2\pi i/3}, \sqrt[3]{2}\cdot e^{4\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

El polinomio mínimo anulador de $\sqrt[4]{2}$ es x^4-2, cuyas raíces son $\sqrt[4]{2}$, $\sqrt[4]{2}\cdot e^{2\pi i/4}$, $\sqrt[4]{2}\cdot e^{4\pi i/4}$, $\sqrt[4]{2}\cdot e^{6\pi i/4}$. La mínima extensión trivializante de $\mathbb{Q}(\sqrt[4]{2})$, es

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

Si $A = A_1 \times A_2$ y K_1 trivializa a A_1 y K_2 trivializa a A_2, entonces cualquier compuesto de K_1 y K_2 trivializa a A. Entonces,

$$\mathbb{Q}(i)\cdot\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(i, e^{2\pi i/3}, \sqrt[3]{2})$$

P2. Todos los elementos de L son separables sobre k, por tanto son separables sobre K y $K \hookrightarrow L$ es separable.

P3. $k(\alpha^p) \hookrightarrow k(\alpha)$ es separable, porque α es separable sobre k. El polinomio $x^p - \alpha^p \in k(\alpha^p)[x]$ anula a α, y tiene a α como única raíz (múltiple), pues $x^p - \alpha^p = (x-\alpha)^p$. En conclusión, el polinomio mínimo anulador de α con coeficientes en $k(\alpha^p)$, que es separable y divide a $x^p - \alpha^p$, ha de ser $x - \alpha$, es decir, $\alpha \in k(\alpha^p)$ y $k(\alpha^p) = k(\alpha)$.

P4. En característica cero, las k-álgebras finitas reducidas coinciden con las separables. Además, el producto tensorial de k-álgebras finitas separables es separable.

P5. El anillo $A = \mathbb{F}_2[t]$ es un dominio de factorización única. Por el criterio de Eisenstein $x^2 - t \in A[x]$ es irreducible. Por el lema de Gauss, $x^2 - t \in \mathbb{F}_2(t)[x] = k[x]$ es irreducible.

Tenemos que $(x-\alpha)^2 = x^2 - \alpha^2 = x^2 - t$. Por tanto, α es una raíz doble del polinomio irreducible $x^2 - t \in k[x]$, luego $k \hookrightarrow k(\alpha) = k[\sqrt{t}]$ no es separable.

P6. Dado $\alpha \in K$, el grado m de $k[\alpha]$ divide a n, luego es primo con p.

P7. $L \otimes_k L$ es una L-extensión separable de grado 2, con un punto L-racional. Por tanto, $L \otimes_k L = L \times L'$ y por grados $L' = L$. En conclusión, L es de Galois.

Toda extensión de cuerpos de grado n, con n primo con la característica es separable, pues todo el grado del polinomio mínimo anulador de todo elemento divide a n, luego su derivada es no nula y el polinomio (irreducible) es separable. Por tanto, toda extensión de cuerpos de grado dos es de Galois, en característica distinta de 2. En característica dos $\mathbb{F}_2(x) \hookrightarrow \mathbb{F}_2(\sqrt{x})$ no es separable, pero $\mathbb{F}_2(x) \hookrightarrow \mathbb{F}_2(x)[y]/(y^2 + y + x)$ es separable, luego de Galois.

P8. Dado un polinomio irreducible $p(x)$ de raíces $\alpha_1, \ldots, \alpha_n$, entonces $\mathrm{Aut}_{k-alg}\, k(\alpha_1) = \{\alpha_i : \alpha_i \in k(\alpha_1)\}$, $\tau \mapsto \tau(\alpha_1)$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt{2}) = \{\sqrt{2}, -\sqrt{2}\}$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[3]{2}) = \{\mathrm{Id}\}$, porque $e^{2\pi i/3}\cdot\sqrt[3]{2}, e^{4\pi i/3}\cdot\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[4]{2}) = \{\sqrt[4]{2}, -\sqrt[4]{2}\}$, porque $\pm\sqrt[4]{2}\cdot i \notin \mathbb{Q}(\sqrt[4]{2})$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[5]{2}) = \{\mathrm{Id}\}$, porque $e^{n\cdot 2\pi i/5}\cdot\sqrt[5]{2} \notin \mathbb{Q}(\sqrt[5]{2})$, para $n = 1,2,3,4$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[6]{2}) = \{\pm\sqrt[6]{2}\}$, porque $e^{n\cdot 2\pi i/6}\cdot\sqrt[5]{2} \notin \mathbb{Q}(\sqrt[6]{2})$, para $n = 1,2,4,5$.

P9. El cuerpo de descomposición de x^3-2 es $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/3})$. Sea $\tau \in \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ determinado por $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(e^{2\pi i/3}) = e^{4\pi i/3}$. Entonces,

$$\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathrm{Aut}_{\mathbb{Q}(e^{2\pi i/3})}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \coprod \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \circ \tau$$

Por último, $\mathrm{Aut}_{\mathbb{Q}(e^{2\pi i/3})}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \{\sigma_0, \sigma_1, \sigma_2\}$, con $\sigma_j(\sqrt[3]{2}) := e^{j\cdot 2\pi i/3} \cdot \sqrt[3]{2}$.

El cuerpo de descomposición de x^4-2 es $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$. Entonces, $\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[4]{2}, i)) = \{\tau_{rs}\}_{1\le r, s\le 2}$, con $\tau_{rs}(i) = (-1)^r \cdot i$ y $\tau_{rs}(\sqrt[4]{2}) = (-1)^s \cdot i \cdot \sqrt[4]{2}$.

P10. Dado $p(x) \in \mathbb{C}$, todas sus raíces $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, luego $\mathbb{C}(\alpha_1, \ldots, \alpha_n) = \mathbb{C}$, cuyo grupo de Galois sobre $\mathbb{C}$ es $G = \{1\}$.

P11. Efectivamente.

P12. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de $(x^2-2)\cdot(x^2-3) \in \mathbb{Q}[x]$, luego es de Galois. Además, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, por tanto, $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es de grado 2, luego $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es una $\mathbb{Q}$-extensión de grado 4. Luego el grupo G de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es de orden 4. Todo $\tau \in G$ está determinado por sus valores en $\sqrt{2}$ y en $\sqrt{3}$. Además, se cumple que $\tau(\sqrt{2}) = \pm\sqrt{2}$ y $\tau(\sqrt{3}) = \pm\sqrt{3}$. En conclusión,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq G, (\bar{i}, \bar{j}) \mapsto \tau_{\bar{i}\bar{j}}, \text{ donde } \tau_{\bar{i}\bar{j}}(\sqrt{2}) := (-1)^i \sqrt{2}, \text{ y } \tau_{\bar{i}\bar{j}}(\sqrt{3}) := (-1)^j \sqrt{3}$$

Si $k \hookrightarrow K$ es una extensión de Galois, $\alpha \in K$ y el polinomio mínimo anulador de α es $p(x)$ de raíces $\alpha_1, \ldots, \alpha_n$, entonces $\alpha_1, \ldots, \alpha_n \in K$. El polinomio anulador con coeficientes en $\mathbb{Q}$ de $\sqrt[3]{3}$ es x^3-3 y $e^{2\pi i/3} \cdot \sqrt[3]{3}$ es una raíz de x^3-3. Se cumple que $e^{2\pi i/3} \cdot \sqrt[3]{3} \notin \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, luego $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ no es Galois.

$\mathbb{Q}(i\cdot\sqrt{2}, \sqrt[3]{3}) = K$ es una $\mathbb{Q}$-extensión de grado 6, porque es un compuesto de las extensiones $\mathbb{Q}(i\cdot\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{3})$. Si fuese de Galois, entonces $e^{2\pi i/3} \cdot \sqrt[3]{3} \in K$, luego $e^{2\pi i/3} \in K$ y $i\cdot\sqrt{3} \in K$. Como $i\cdot\sqrt{3} \notin \mathbb{Q}(i\cdot\sqrt{2})$, tendríamos que $\mathbb{Q}(i\cdot\sqrt{2}, i\cdot\sqrt{3})$ es una $\mathbb{Q}$-extensión de grado 4, incluida en K, lo que es contradictorio. Luego K no es de Galois.

$\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ es el cuerpo de descomposición de x^3-2, luego es de Galois. Es una $\mathbb{Q}$-extensión de grado 6 y su grupo de Galois es un subgrupo de las permutaciones de las raíces de x^3-2, luego es isomorfo a S_3.

P13. Entonces, la sucesión

$$1 \to \mathrm{Aut}_{L'-alg} L \to \mathrm{Aut}_{k-alg} L \to \mathrm{Aut}_{k-alg} L' \to 1$$

es exacta y $\#\mathrm{Aut}_{k-alg} L = \#\mathrm{Aut}_{L'-alg} L \cdot \#\mathrm{Aut}_{k-alg} L' = \dim_{L'} L \cdot \dim_k L' = \dim_k L$ y L es una k-extensión de Galois.

P14. $(L\otimes_k L')\otimes_k (L\otimes_k L') = (L\otimes_k L)\otimes_k (L'\otimes_k L') = (\prod^n L)\otimes_k (\prod^m L') = \prod^{nm}(L\otimes_k L')$, luego $L\otimes_k L'$ es de Galois. Tenemos el morfismo natural inyectivo

$$G \times G' \to \mathrm{Aut}_k(L\otimes_k L'), (g, g') \mapsto g\otimes g'$$

Por órdenes de los grupos, concluimos que es biyectivo.

P15. El agujero de L y L' en el cierre algebraico de k, $\bar{k}$ es único. Por tanto, El agujero de $L\cdot L'$ en $\bar{k}$ es único, exactamente es el subcuerpo de $\bar{k}$ generado por L y L'. Por tanto, $L\cdot L'$ (que es separable) es de Galois y todo compuesto de L y L' es isomorfo al subcuerpo de $\bar{k}$ generado por L y L'. $L\otimes_k L'$ (que es separable) es producto directo de compuestos de L y L'.

P16. Si un polinomio irreducible tiene una raíz en $L\cap L'$, tiene todas sus raíces en L y L', luego en $L\cap L'$; por tanto $L\cap L'$ es una k-extensión de Galois.

Si consideramos otra k-extensión K' y K'' es un compuesto de K y K', entonces el agujero de L en K se identifica con el agujero de L en K'', y éste con el agujero de L en K'. Idem con L'. Por tanto, la intersección de L y L' en K es la misma que en K'', y ésta es la misma que en K'.

P17. El cuerpo de descomposición del polinomio $x^4-4=(x^2-2)(x^2+2)$ es $\mathbb{Q}(\sqrt{2},\sqrt{-2})=\mathbb{Q}(\sqrt{2},i)$, que es una $\mathbb{Q}$-extensión de grado 4, y el grupo de Galois es isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

El cuerpo de descomposición de $(x^2-2)(x^2+1)$ es $\mathbb{Q}(\sqrt{2},i)$.

P18. Obvio.

P19. $1/\sqrt{2}+1/\sqrt{2}i$ es una raíz octava primitiva de la unidad. Luego, $\mathbb{Q}(\sqrt[8]{2},i)$ es el cuerpo de descomposición de x^8-2, luego es de Galois de grado 16. Por tanto, el morfismo

$$\mathbb{Z}/8\mathbb{Z}\ltimes\mathbb{Z}/2\mathbb{Z}\to \mathrm{Aut}_{\mathbb{Q}-alg}\,\mathbb{Q}(\sqrt[8]{2},i),(\bar{r},\bar{s})\mapsto\tau_{(\bar{r},\bar{s})}$$

donde $\tau_{(\bar{r},\bar{s})}(\sqrt[8]{2})=e^{r2\pi i/8}\cdot\sqrt[8]{2}$, $\tau_{(\bar{r},\bar{s})}(i)=(-1)^s\cdot i$, es un isomorfismo. (Consideramos el morfismo de grupos $\mathbb{Z}/2\mathbb{Z}\to\mathrm{Aut}_{grp}(\mathbb{Z}/8\mathbb{Z})$, $\bar{s}\to h_{\bar{s}}$, con $h_{\bar{s}}(\bar{n})=3^s\cdot\bar{n}$).

P20. $\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})$ es el cuerpo de descomposición de x^3-2, que es una $\mathbb{Q}$-extensión de Galois de grado 6. Sea τ la conjugación compleja. Tenemos que $\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})^{\langle\tau\rangle}=\mathbb{Q}(\sqrt[3]{2})$. Si $\sqrt{2}\in\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})$ entonces $\sqrt{2}\in\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})^{\langle\tau\rangle}=\mathbb{Q}(\sqrt[3]{2})$, lo cual es imposible. Por tanto,

$$\mathbb{Q}(\sqrt{2},\sqrt[3]{2},e^{2\pi i/3})=\mathbb{Q}(\sqrt{2})\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})$$

que es una $\mathbb{Q}$-extensión de Galois de grado 12 y grupo $G=\mathbb{Z}/2\mathbb{Z}\times(\mathbb{Z}/3\mathbb{Z}\ltimes\mathbb{Z}/2\mathbb{Z})$. Explícitamente, si denotamos $\tau_{\bar{i},\bar{j},\bar{k}}=(\bar{i},\bar{j},\bar{k})\in\mathbb{Z}/2\mathbb{Z}\times(\mathbb{Z}/3\mathbb{Z}\ltimes\mathbb{Z}/2\mathbb{Z})$, tenemos que

$$\begin{aligned}\tau_{\bar{i},\bar{j},\bar{k}}(\sqrt{2})&=(-1)^i\cdot\sqrt{2}\\ \tau_{\bar{i},\bar{j},\bar{k}}(\sqrt[3]{2})&=(-1)^j\cdot\sqrt[3]{2}\\ \tau_{\bar{i},\bar{j},\bar{k}}(e^{2\pi i/3})&=e^{k\cdot 2\pi i/3}\end{aligned}$$

El subgrupo de G que deja invariante a $\sqrt{2}+\sqrt[3]{2}$ es $H=0\times 0\times\mathbb{Z}/2\mathbb{Z}$. Por tanto, $\mathbb{Q}((\sqrt{2}+\sqrt[3]{2})=\mathbb{Q}((\sqrt{2},\sqrt[3]{2})$. $\mathbb{Q}((\sqrt{2},\sqrt[3]{2})$ es una $\mathbb{Q}$-extensión de grado 6, que no es Galois, porque $e^{2\pi i/3}\cdot\sqrt[3]{2}\notin\mathbb{Q}((\sqrt{2},\sqrt[3]{2})$. Por tanto, su envolvente de Galois es $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},e^{2\pi i/3})$.

P21. El grupo de Galois de $(x^3+3)(x^2+3)$ es el grupo de Galois de $\mathbb{Q}(\sqrt[3]{3}, e^{2\pi i/3}, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, i)$, que es una $\mathbb{Q}$-extensión de grado 12. El grupo de Galois de $(x^3+3)(x^2+3)$ es $S_3 \times S_2$.

P22. Considérese la sección de s, $L^H \hookrightarrow L$, $l \mapsto \frac{1}{\#H} \cdot l$.

P23. El cuerpo de descomposición de x^3-2 es $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}, e^{4\pi i/3} \cdot \sqrt[3]{2})$, de grupo de Galois S_3. Los subgrupos de S_3, son $S_3, \langle(1,2,3)\rangle, \langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle$ y $\{\mathrm{Id}\}$, que por toma de invariantes se corresponden con las subextensiones

$$\mathbb{Q}, \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{3} \cdot i), \mathbb{Q}(e^{4\pi i/3} \cdot \sqrt[3]{2}), \mathbb{Q}(e^{2\pi i/3} \cdot \sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

El cuerpo de descomposición de $(x^2-2)(x^2+1)$ es $\mathbb{Q}(\sqrt{2}, i)$ de grupo de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Los subgrupos son $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\langle(\bar{1},\bar{0})\rangle$, $\langle(\bar{0},\bar{1})\rangle$, $\langle(\bar{1},\bar{1})\rangle$, $\{\mathrm{Id}\}$, que por toma de invariantes se corresponden con las subextensiones

$$\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2} \cdot i), \mathbb{Q}(\sqrt{2}, i)$$

El cuerpo de descomposición de x^4-4 es $\mathbb{Q}(\sqrt{2}, i)$.

P24. $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$, porque en caso contrario, $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ ha de coincidir con $\mathbb{Q}(\sqrt[4]{2})$, lo cual es imposible porque la primera $\mathbb{Q}$-extensión es de Galois y la segunda no.

Por tanto, $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$ es una $\mathbb{Q}$-extensión de grado 8. Como $i \notin \mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$, entonces $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}, i)$ es una $\mathbb{Q}$-extensión de grado 16, luego $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}, i) \neq \mathbb{Q}(\sqrt[4]{2}, i)$ y $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2}, i)$.

Por último, $\dim_{\mathbb{Q}(\sqrt{3})} \mathbb{Q}(\sqrt{3}, \sqrt[4]{2}) = 4$ y x^4-2 es irreducible sobre $\mathbb{Q}(\sqrt{3})$.

P26. a) $K^{H_1}, K^{H_2} \subseteq K^{H_1 \cap H_2}$, luego $K^{H_1} \cdot K^{H_2} \subseteq K^{H_1 \cap H_2}$. $K^{H_1} \cdot K^{H_2} = K^H$, con $H \subseteq H_1, H_2$, luego $H \subseteq H_1 \cap H_2$. Luego, $K^{H_1} \cdot K^{H_2} = K^H \supseteq K^{H_1 \cap H_2}$ y $K^{H_1} \cdot K^{H_2} = K^{H_1 \cap H_2}$.

b) $K^{\langle H_1, H_2\rangle} \subseteq K^{H_1}, K^{H_2}$, luego $K^{\langle H_1, H_2\rangle} \subseteq K^{H_1} \cap K^{H_2}$. $K^{H_1} \cap K^{H_2} = K^H$, con $H \supseteq H_1, H_2$, luego $H \supseteq \langle H_1, H_2\rangle$ y $K^{\langle H_1, H_2\rangle} \subseteq K^H = K^{H_1} \cap K^{H_2}$. Por tanto, $K^{H_1} \cap K^{H_2} = K^{\langle H_1, H_2\rangle}$.

P27. K es una K^{H_2}-extensión de Galois de grupo H_2. $K^{H_1} \cdot K^{H_2} = K^{H_1 \cap H_2}$ y $H_1 \cap H_2$ es normal en H_2, porque H_1 es normal en G. Por tanto, $K^{H_1} \cdot K^{H_2}$ es una K^{H_2} extensión de Galois de grupo $H_2/(H_1 \cap H_2)$. Por otra parte, K^{H_1} es una k-extensión de Galois de grupo G/H_1 y el morfismo $H_2/(H_1 \cap H_2) \to G/H_1$, $\bar{h}_2 \mapsto \bar{h}_2$ es inyectivo.

P28. Sea L' la envolvente de Galois de L. Las subextensiones de L' son un número finito, porque se corresponden con los subgrupos del grupo de Galois de L'. Por tanto, las subextensiones de L, que son subextensiones de L', son un número finito.

P29. Si las subextensiones $k(\alpha + a\beta)$ son todas distintas variando $a \in k$, tendríamos que el número de subextensiones de $k(\alpha, \beta)$ sería infinito, lo que contradice el problema 28. Por tanto, existen $a \neq b \in k$ tales que $k(\alpha + a\beta) = k(\alpha + b\beta)$. Luego, $(\alpha + a\beta) - (\alpha + b\beta) \in k(\alpha + a\beta)$, $\beta \in k(\alpha + a\beta)$, $\alpha \in k(\alpha + a\beta)$ y $k(\alpha + a\beta) = k(\alpha, \beta)$.

P30. a. Por el teorema de equivalencia de Galois, tenemos que demostrar que $\mathbb{Z}/n\mathbb{Z}$ sólo contiene para cada divisor d' de n un único subgrupo de orden d'. En efecto, el subgrupo es cíclico, luego está generado por un elemento de orden d'. Los elementos de $\mathbb{Z}/n\mathbb{Z}$ anulados por d', son $\overline{n/d'}, 2\cdot\overline{n/d'}, \cdots, (d'-1)\cdot\overline{n/d'}$, los cuales forman un subgrupo de orden d'. En conclusión, $\langle\overline{n/d'}\rangle$ es el único subgrupo de orden d' de $\mathbb{Z}/n\mathbb{Z}$.

b. Por el teorema de equivalencia de Galois, tenemos que demostrar que si tenemos dos subgrupos $H_1 = \langle\bar{r}\rangle$,$H_2 = \langle\bar{s}\rangle$ de $\mathbb{Z}/n\mathbb{Z}$ (con r y s divisores de n), entonces $H_1 \subseteq H_2$ si y sólo si $\#H_1 | \#H_2$. Ahora bien, $H_1 \subseteq H_2$ si y sólo si s divide a r, que equivale a decir que $n/r = \#H_1$ divide a $n/s = \#H_2$.

P31. Por el teorema de prolongación, todo morfismo de K_1 en K prolonga a automorfismo de K. Sea $i : K_2 \hookrightarrow K$ la inclusión. El morfismo $i \circ f$ prolonga al automorfismo σ buscado.

P32. Denotemos $i_1 : K_1 \hookrightarrow L$, $i_2 : K_2 \hookrightarrow L$ las inclusiones y $\sigma : K_1 \simeq K_2$ el isomorfismo. Consideremos el morfismo $i_2 \circ \sigma : L_1 \to L$. Por el teorema de prolongación existe un automorfismo $g : L \to L$, tal que $i_2 \circ \sigma = g \circ i_1$. Por tanto, $g(K_1) = K_2$. Entonces, si $K_1 = L^{H_1}$, se tiene que $L^{H_2} := K_2 = g(K_1) = L^{gH_1g^{-1}}$. Luego, $H_2 = gH_1g^{-1}$. Recíprocamente, si $H_2 = gH_1g^{-1}$, entonces $K_2 = g(K_1)$ y $K_2 \simeq K_1$.

P33. Sea $G = \mathrm{Aut}_{k-alg} L'$. Dada una extensión $L' \hookrightarrow L$ y $g \in G$, denotemos L_g, la L'-extensión $L' \overset{g}{\simeq} L' \hookrightarrow L$. $L' \otimes_k L = \oplus L$ como L-álgebras, considerando $L' \otimes_k L$ como L-álgebra vía el segundo factor. Si consideramos $L' \otimes_k L = \oplus L$ como L'-álgebra vía el primer factor de $L' \otimes_k L$ y queremos considerar $\oplus L$ como L'-álgebra vía el isomorfismo $L' \otimes_k L = \oplus L$, entonces deberíamos escribir en vez de $\oplus L$, $\oplus_{g\in G} L_g$. Por tanto, tenemos (con rigor) que $L \otimes_k L = \oplus_{g\in G}(L \otimes_{L'} L_g)$.

Si $L' = \mathbb{Q}(\sqrt{2})$ y $L = \mathbb{Q}(\sqrt[4]{2})$, entonces $G = \mathrm{Aut}_{\mathbb{Q}-alg}\mathbb{Q}(\sqrt{2}) = \{\mathrm{Id}, g\}$, con $g(\sqrt{2}) = -\sqrt{2}$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Q}(i\cdot\sqrt[4]{2}) & \xrightarrow{\sim} & \mathbb{Q}(\sqrt[4]{2}) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow[g]{\sim} & \mathbb{Q}(\sqrt{2}) \end{array} \qquad \begin{array}{c} i\cdot\sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ \\ \sqrt{2} \longmapsto -\sqrt{2} \end{array}$$

Luego, $L_g = \mathbb{Q}(i\cdot\sqrt[4]{2})$, $L \otimes_{L'} L_g = \mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(i\cdot\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ y

$$L \otimes_k L = (L \otimes_{L'} L) \times (L \otimes_{L'} L_g) = L \times L \times \mathbb{Q}(\sqrt[4]{2}, i)$$

P34. $\sigma^2(e^{2\pi i/5}) = e^{32\pi i/5} = e^{2\pi i/5}$, luego $\sigma^2 = \mathrm{Id}$. Por tanto, $H = \langle\sigma\rangle$ es un grupo de orden 2. Como $\mathbb{Q} \hookrightarrow \mathbb{Q}(e^{2\pi i/5})$ es una extensión de Galois de grado 4, entonces $\mathbb{Q}(e^{2\pi i/5})^H$ es una $\mathbb{Q}$-extensión de grado 2. Como $\frac{-1+\sqrt{5}}{2} = e^{2\pi i/5} + e^{8\pi i/5} \in \mathbb{Q}(e^{2\pi i/5})^H$, entonces $\sqrt{5} \in \mathbb{Q}(e^{2\pi i/5})^H$ y $\mathbb{Q}(e^{2\pi i/5})^H = \mathbb{Q}(\sqrt{5})$.

P35. El cuerpo de descomposición de x^6-8 sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt{2})\otimes_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/3})$, que es una $\mathbb{Q}$-extensión de grado 4, de grupo de Galois $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Sobre $\mathbb{Q}(\sqrt{2})$ es $\mathbb{Z}/2\mathbb{Z}$ y sobre $\mathbb{Q}(e^{2\pi i/3})$ es $\mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, e^{2\pi i/3})$ es una $\mathbb{Q}$-extensión de grado $3\cdot 4 = 12$, luego es una $\mathbb{Q}(\sqrt[3]{2})$-extensión de Galois de grado 4, de grupo de Galois $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(\sqrt[4]{2}, \sqrt{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/3})$ es una $\mathbb{Q}$-extensión de grado $4\cdot 2 = 8$, luego es una $\mathbb{Q}(\sqrt[4]{2})$-extensión de Galois de grado 2, de grupo de Galois $\mathbb{Z}/2\mathbb{Z}$.

P36. El grupo de Galois de $\mathbb{Q}(e^{2\pi i/8})$ sobre $\mathbb{Q}$ es $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, que son todos de grado dos salvo la identidad. Luego $\langle\tau\rangle$ es de orden 2, salvo $\tau = \mathrm{Id}$. Luego, el grado de $\mathbb{Q}(e^{2\pi i/8})^\tau$ es $4/2 = 2$, salvo para $\tau = \mathrm{Id}$, que 4.

No hay ningún automorfismo de $\mathbb{Q}(e^{2\pi i/8})$ que sólo deje fijos los números racionales.

P37. El grupo de Galois de $\mathbb{Q}(e^{2\pi i/n})$ es $(\mathbb{Z}/n\mathbb{Z})^*$. Para $n = 3$, es $\mathbb{Z}/2\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 5$ es $\mathbb{Z}/4\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 6$, es $(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})^* = (\mathbb{Z}/3\mathbb{Z})^*\times(\mathbb{Z}/2\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 7$ es $\mathbb{Z}/6\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 8$, es $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ que contiene tres subgrupos de índice dos. Para $n = 9$, es $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 10$, es $\mathbb{Z}/4\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 11$ es $\mathbb{Z}/10\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 12$, es $(\mathbb{Z}/3\mathbb{Z})^*\times(\mathbb{Z}/4\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ que contiene tres subgrupos de índice dos. Para $n = 13$ es $\mathbb{Z}/12\mathbb{Z}$, que contiene un único subgrupo de índice 2.

P38. Para $n = 5$, el grupo de Galois es $(\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$, que tiene un único subgrupo propio, $H = \langle\bar{4}\rangle = \langle\tau\rangle$, donde τ es el automorfismo conjugar. Entonces, $\mathbb{Q}(e^{2\pi i/5})^H = \mathbb{Q}(e^{2\pi i/5} + e^{-2\pi i/5}) = \mathbb{Q}(\sqrt{5})$. Para $n = 6$, el grupo de Galois es $\mathbb{Z}/2\mathbb{Z}$, que no tiene subgrupos propios. Para $n = 7$, el grupo de Galois es $(\mathbb{Z}/7\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z}$, que contiene dos subgrupos propios, $H_1 = \langle\bar{2}\rangle \simeq \mathbb{Z}/3\mathbb{Z}$ y $H_2 = \langle\bar{6}\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(e^{2\pi i/7})^{H_1} = \mathbb{Q}(e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7})$, porque si $e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7} = a \in \mathbb{Q}$, entonces $x + x^2 + x^4 - a$ anularía a $e^{2\pi i/7}$ (además, si denotamos $w = e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7}$, entonces su polinomio anulador resulta ser $x^2 + x + 2$, luego $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{-7})$). $\mathbb{Q}(e^{2\pi i/7})^{H_2} = \mathbb{Q}(e^{2\pi i/7} + e^{-2\pi i/7})$. Para $n = 8$, el grupo de Galois es $(\mathbb{Z}/8\mathbb{Z})^* = \langle\bar{1}, \bar{3}, \bar{5}, \bar{7}\rangle = \langle\bar{1}, \bar{3}\rangle\times\langle\bar{1}, \bar{5}\rangle = H_1\times H_2$. $\mathbb{Q}(e^{2\pi i/8})^{H_2} = \mathbb{Q}(e^{\pi i/2}) = \mathbb{Q}(i)$ y $\mathbb{Q}(e^{2\pi i/8})^{H_1} = \mathbb{Q}(e^{2\pi i/8} + e^{6\pi i/8})$, (además, si denotamos $w = e^{2\pi i/8} + e^{6\pi i/8}$, entonces su polinomio anulador resulta ser $x^2 + 2$, luego $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{-2})$). $H_1\times H_2 = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ contiene tres subgrupos propios (de orden 2), nos falta considerar la subextensión $\mathbb{Q}(\sqrt{-2}\cdot i) = \mathbb{Q}(\sqrt{2})$. Para $n = 9$, el grupo de Galois es $(\mathbb{Z}/9\mathbb{Z})^* = \langle\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\rangle = \langle\bar{8}\rangle\times\langle\bar{4}\rangle = H_1\times H_2$. $\mathbb{Q}(e^{2\pi i/9})^{H_1} = \mathbb{Q}(e^{2\pi i/9} + e^{-2\pi i/9})$ y $\mathbb{Q}(e^{2\pi i/9})^{H_2} = \mathbb{Q}(e^{6\pi i/9}) = \mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$.

P39. Supongamos que $\sqrt{b} \notin \mathbb{Q}$ (es decir, que b no es el cuadrado de un número racional). Entonces, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{b})$ es una extensión de grado 2. Para $n = 5$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{5})$, luego $\sqrt{b} = a_1 + a_2\sqrt{5}$, con $a_1, a_2 \in \mathbb{Q}$. Elevando al cuadrado, observamos que $a_1 = 0$ y que $b = a_2^2\cdot 5$. Para $n = 6$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-3})$ y $b = -3a_2^2$. Para $n = 7$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-7})$, luego $b = -a_2^2\cdot 7$. Para $n = 8$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-1})$, luego $b = -a_2^2$; ó

$\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-2})$, luego $b = -2 \cdot a_2^2$; ó $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{2})$, luego $b = 2 \cdot a_2^2$. Para $n = 9$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-3})$, luego $b = -3 \cdot a_2^2$.

P40. $\mathbb{Q}(\sqrt{-2}, i)$ es una extensión de Galois de grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que contiene exactamente tres subgrupos de índice 2. Luego, $\mathbb{Q}(\sqrt{-2}, i)$ contiene tres subextensiones de grado 2: $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{-2} \cdot i) = \mathbb{Q}(\sqrt{2})$. Ninguna de estas tres contiene a $\sqrt{-3}$.

P41. $L = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$ es una extensión de Galois de grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Todos los elementos de este grupo son de orden 2, salvo el elemento neutro, luego contiene 7 subgrupos de orden 2. El elemento $\sigma = (\bar{r}, \bar{s}, \bar{t}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, opere como sigue $\sigma(\sqrt{3}) := (-1)^r \cdot \sqrt{3}$, $\sigma(\sqrt{2}) = (-1)^s \cdot \sqrt{2}$, $\sigma(i) = (-1)^t \cdot i$. Si L' es real entonces es invariante por $H = 0 \times 0 \times \mathbb{Z}/2\mathbb{Z}$ y $L^H = \mathbb{Q}(\sqrt{3}, \sqrt{2})$, luego $L' = \mathbb{Q}(\sqrt{3}, \sqrt{2})$. $\mathbb{Q}(\sqrt[4]{3})$ es una $\mathbb{Q}$-extensión de grado 4, que no es de Galois, luego no coincide con $\mathbb{Q}(\sqrt{3}, \sqrt{2})$, por tanto, $\sqrt[4]{3} \notin L' = L \cap \mathbb{R}$ y $\sqrt[4]{3} \notin L$. Entonces, $L \hookrightarrow L(\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es de grado 2, luego $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es una $\mathbb{Q}$-extensión de grado 16. Además es es el compuesto de dos extensiones de Galois: $\mathbb{Q}(\sqrt[4]{3}, i)$ y $\mathbb{Q}(\sqrt{2})$, luego es de Galois.

P42. El grupo de Galois de L es $(\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$: $\sigma = (\bar{r}, \bar{s}, \bar{t}) \in (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ opera como sigue $\sigma(\sqrt[4]{3}) = i^r \cdot \sqrt[4]{3}$, $\sigma(i) = (-1)^s \cdot i$ y $\sigma(\sqrt{2}) = (-1)^t \cdot \sqrt{2}$. Puede comprobarse que $(\bar{r}, \bar{s}, \bar{t}) + (\bar{r}, \bar{s}, \bar{t}) = (\bar{r} + (-1)^s \cdot \bar{r}, 0, 0)$, que es cero si $s = 1$, ó $s = 0$ y $r = 0, 2$. En total, 11 subgrupos de orden 2. Si L' es de real, entonces es invariante por $H = 0 \times \mathbb{Z}/2\mathbb{Z} \times 0$ y $L' \subseteq L^H = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2})$.

Si $\sqrt[8]{3} \in L$ entonces $L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$. Observemos que $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$. El grupo de Galois, G, de la extensión de grado 4, $\mathbb{Q}(\sqrt{2}, i) \to L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es $\mathbb{Z}/4\mathbb{Z}$, pues es un subgrupo de $\mathbb{Z}/8\mathbb{Z}$, ya que dado $\tau \in G$, $\tau(\sqrt[8]{3}) = e^{r \cdot 2\pi i/8} \cdot \sqrt[8]{3}$, para cierto $\bar{r} \in \mathbb{Z}/8\mathbb{Z}$ (y $\tau^m(\sqrt[8]{3}) = e^{mr \cdot 2\pi i/8} \cdot \sqrt[8]{3}$). Por tanto, $G = \langle\sigma\rangle$, con $\sigma(\sqrt[8]{3}) = e^{2\pi i/4} \cdot \sqrt[8]{3}$ y el polinomio mínimo anulador de $\sqrt[8]{3}$ es $x^4 - \sqrt{3}$. Por tanto, $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$, lo cual es falso, por el problema 39.

P43. $\mathbb{Q}(\sqrt[8]{3}, i)$ fuese una $\mathbb{Q}$-extensión de Galois, entonces contendría todas las raíces de $x^8 - 3$, luego contendría a $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$. Por tanto, $\mathbb{Q}(\sqrt[8]{3}, i) = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ y llegamos a contradicción con el problema 42.

P44. Las raíces de $x^4 + 2$ son

$$\sqrt[4]{-2} = \sqrt[4]{2} \cdot \sqrt[4]{-1} = \begin{cases} \pm\sqrt[4]{2} \cdot (\sqrt{2}/2 + \sqrt{2}/2i) = \pm(1/\sqrt[4]{2} + 1/\sqrt[4]{2} \cdot i) \\ \pm i \cdot (1/\sqrt[4]{2} + 1/\sqrt[4]{2} \cdot i) \end{cases}$$

Si $i \in \mathbb{Q}(\alpha)$, entonces $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $x^4 + 2$, que coincide con $\mathbb{Q}(\sqrt[4]{2}, i)$ que es de grado 8 sobre $\mathbb{Q}$, lo cual es contradictorio. Observemos que $\sqrt{-2} \in \mathbb{Q}(\alpha)$, luego si $\sqrt{2} \in \mathbb{Q}(\alpha)$ entonces $i \in \mathbb{Q}(\alpha)$ y hemos probado que no es así.

El grupo de Galois de $\mathbb{Q}(\sqrt[4]{2}, i)$ es $G = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ y los inavariantes por $H = \langle(\bar{1}, \bar{1})\rangle$ es $\mathbb{Q}(\alpha)$. Las extensiones de grado 2 son de Galois. Buscamos subgrupos

H' de orden 4 de G, normales que contengan a H. Por ser normal ha de contener a $(-\bar{1},\bar{1}) = (0,\bar{1}) * (\bar{1},\bar{1}) * (0,\bar{1})^{-1}$. Luego $H' = \langle(\bar{1},\bar{1}),(-\bar{1},\bar{1})\rangle$ y solo hay una subextensión de grado 2: $\mathbb{Q}(\sqrt{-2})$.

P45. El polinomio mínimo anulador de $\sqrt{2+\sqrt{2}}$ es $x^4 - 4x^2 + 2$, pues anula y es irreducible por el criterio de Eisenstein. Sus raíces son $\pm\sqrt{2\pm\sqrt{2}}$. $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ es una extensión de Galois de $\mathbb{Q}$ si y sólo si $\beta = \sqrt{2-\sqrt{2}} \in \mathbb{Q}(\alpha = \sqrt{2+\sqrt{2}})$. Ahora bien, $\alpha\cdot\beta = \sqrt{2}$, luego $\beta = \sqrt{2}/\alpha \in \mathbb{Q}(\alpha)$.

De otro modo: el grupo de Galois de esta bicuadrada se puede calcular y es de orden 4.

P46. Consideremos la extensión de Galois $\mathbb{Q}(\sqrt{2},\sqrt{3})$, cuyo grupo de Galois es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. El polinomio $(x^2-2)\cdot(x^2-3)\cdot(x^2-6)$ cumple lo requerido.

P47. Sea $g \in G - (H_1 \cup \ldots \cup H_n)$. Por definición g no deja fija ninguna raíz.

P48. El cuerpo formado por las raíces es finito. Por tanto, es de característica positiva p. Luego, el cuerpo es de orden p^n, y $x^{p^n} - x$ tiene justamente como raíces los elementos del cuerpo y ha de coincidir con $q(x)$.

P49. Sea α una raíz del polinomio irreducible $y^2 - y + 1$. Veamos que $\sqrt{\alpha} \in \mathbb{F}_5(\alpha)$: Calculemos $a, b \in \mathbb{F}_5$ tales que $(a+b\alpha)^2 = \alpha$. En tal caso, $a^2+b^2\alpha^2+2ab\alpha-\alpha = 0$, luego $0 = a^2 + b^2(\alpha-1) + 2ab\alpha - \alpha = (a^2+b^2) + (b^2+2ab-1)\alpha = 0$. Por tanto, $a^2 - b^2 = 0$ y $b^2 + 2ab - 1 = 0$. Una solución es $a = 2$ y $b = -2$. Entonces el cuerpo de descomposición de $x^4 - x^2 + 1$ es $\mathbb{F}_5(\alpha)$, cuyo grupo de Galois (que está generado por el automorfismo de Frobenius) es $\mathbb{Z}/5\mathbb{Z}$.

Las raíces de $y^2 - y + 1$ son $2 \pm 3\sqrt{2}$ y las de $x^4 - x^2 + 1$, $\pm(2 - 2(2 \pm 3\sqrt{2})) = \pm(3 + \mp\sqrt{2})$.

P50. Sea $\mathbb{F}_{25}$ el único cuerpo con 25 elementos, cuyos elementos son las raíces de $x^{25} - x$. Dado un polinomio, $p(x)$ de grado 2 irreducible, entonces $\mathbb{F}_5[x]/(p(x)) = \mathbb{F}_{25}$. Luego las raíces de $p(x)$ están en $\mathbb{F}_{25}$. Recíprocamente, dada $\alpha \in \mathbb{F}_{25} - \mathbb{F}_5$, su polinomio mínimo anulador es de grado 2. En conclusión, las raíces de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ coinciden con los elementos de $\mathbb{F}_{25}$, luego el producto de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ tiene las mismas raíces que $x^{25} - x$, luego son iguales.

P51. Si $p(x)$ es un polinomio irreducible de grado 2 con coeficientes en $\mathbb{F}_p$, entonces $\mathbb{F}_p[x]/(p(x))$ es un cuerpo con p^2 elementos, luego $\mathbb{F}_p[x]/(p(x)) = \mathbb{F}_{p^2}$, luego las raíces de $p(x)$ pertenecen a $\mathbb{F}_{p^2}$. Dado $\alpha \in \mathbb{F}_{p^2}$, tenemos $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$, luego el grado de $\mathbb{F}_p(\alpha)$ sobre $\mathbb{F}_p$ es 1 ó 2. Es decir, α es raíz de un polinomio irreducible de grado 1 ó 2. Es decir, $\mathbb{F}_{p^2} - \mathbb{F}_p$ son todos los elementos de polinomio anulador de grado 2 y cada uno de estos polinomios tiene dos raíces, luego el número de polinomios irreducibles de grado 2 es igual a

$$\#(\mathbb{F}_{p^2} - \mathbb{F}_p)/2 = (p^2 - p)/2$$

Si $\{p_i(x)\}_{i\in I}$ es el conjunto de los polinomios mónicos irreducibles de grado 2, entonces el conjunto de los polinomios irreducibles de grado 2 es $\{a\cdot p_i(x)\}_{i\in I, a\in\mathbb{F}_p^*}$. Por tanto, el número de polinomios mónicos irreducibles de grado 2 con coeficientes en $\mathbb{F}_p$ es $(p_1)\cdot(p^2-p)/2 = p(p-1)^2/2$.

P52. Los elementos de polinomio mínimo anulador de grado 3 son los elementos de $\mathbb{F}_{p^3}-\mathbb{F}_p$ ($\mathbb{F}_{p^3}$ no contiene subextensiones propias). Luego el número de los polinomios mónicos irreducibles de grado 3 con coeficientes en $\mathbb{F}_p$ es igual a

$$\#(\mathbb{F}_{p^3}-\mathbb{F}_p)/3 = (p^3-p)/3$$

Los elementos de polinomio mínimo anulador de grado 4 son los elementos de $\mathbb{F}_{p^4}-\mathbb{F}_{p^2}$ ($\mathbb{F}_{p^2}$ el la única subextensión propia de $\mathbb{F}_{p^4}$). Luego el número de los polinomios mónicos irreducibles de grado 4 con coeficientes en $\mathbb{F}_p$ es igual a

$$\#(\mathbb{F}_{p^4}-\mathbb{F}_{p^2})/4 = (p^4-p^2)/4$$

Los elementos de polinomio mínimo anulador de grado 6 son los elementos de $\mathbb{F}_{p^6}-(\mathbb{F}_{p^2}\cup\mathbb{F}_{p^3})$. Luego el número de los polinomios mónicos irreducibles de grado 6 con coeficientes en $\mathbb{F}_p$ es igual a

$$(\#\mathbb{F}_{p^4}-\#(\mathbb{F}_{p^2}\cup\mathbb{F}_{p^3}))/6 = (p^6-(p^2+p^3-p))/6$$

Los elementos de polinomio mínimo anulador de grado 8 son los elementos de $\mathbb{F}_{p^8}-\mathbb{F}_{p^4}$. Luego el número de los polinomios mónicos irreducibles de grado 8 con coeficientes en $\mathbb{F}_p$ es igual a

$$(\#(\mathbb{F}_{p^8}-\#\mathbb{F}_{p^4})/4 = (p^8-p^4)/8$$

P53. El núcleo del morfismo de grupos $\mathbb{F}_p^*\to\mathbb{F}_p^*$ $\bar{a}\mapsto\bar{a}^2$ lo forman las raíces de x^2-1, que son ±1. Por tanto, la imagen de este morfismo, $\mathbb{F}_p^{*2}$, es de orden $(p-1)/2$. Luego, $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ es un grupo de orden 2, entonces isomorfo a $\{\pm1\}$. Explícitamente, $\mathbb{F}_p^*/\mathbb{F}_p^{*2}=\{\pm1\}$, $\bar{a}\mapsto\bar{a}^{(p-1)/2}$.

P54. Por el problema 53, sabemos que p es resto cuadrático módulo q si y sólo si $p^{(q-1)/2}=1$ en $\mathbb{F}_q^*$, es decir, si y sólo si el orden de p en $\mathbb{F}_q^*$ es $(q-1)/(2d)$, que equivale a decir, que p genera en $\mathbb{F}_q^*$ un subgrupo de índice $2d$.

P55. Tenemos que ver que $\mathbb{F}_p^{*2}\cap\{-\bar{1},-\bar{2},\bar{2}\}\neq\emptyset$. En efecto, no puede ser que $(-1)^{(p-1)/2} = (2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1$ en $\mathbb{F}_p^*$, porque el producto de los dos primeros es el tercero.

P56. El grupo multiplicativo $\mathbb{F}_{p^n}^*$ es isomorfo a $\mathbb{Z}/(p^n-1)$. Por tanto, las raíces q-ésimas de la unidad se identifica con los elementos de $\mathbb{Z}/(p^n-1)$ anulados por q, que son $\{0\}$ si q es primo con p^n-1, ó $\langle(p^n-1)/q\rangle$ (que son q elementos) si q divide a p^n-1.

P57. Sea ε_q una raíz de $x^{q-1}+\ldots+x+1\in\mathbb{F}_p[x]$, cuyo polinomio mínimo anulador, $q(x)$ lo divide. $\mathbb{Z}/q\mathbb{Z}$ es isomorfo al conjunto de las raíces de x^q-1 y tenemos que

$$\langle F\rangle = \mathrm{Aut}_{\mathbb{F}_p}\mathbb{F}_p(\varepsilon_q)\subseteq(\mathbb{Z}/\mathfrak{q}\mathbb{Z})^*, F\mapsto\bar{p}$$

Como $\#\mathrm{Aut}_{\mathbb{F}_p}\mathbb{F}_p(\varepsilon_q)=\mathrm{gr}\,q(x)$. Tenemos que $\bar{p}$ genera $(\mathbb{Z}/\mathfrak{q})^*$ si y sólo si $\mathrm{gr}\,q(x)=q-1$, es decir, si y sólo si $q(x)=x^{q-1}+\ldots+x+1$, es decir, si y sólo si $x^{q-1}+\ldots+x+1$ es irreducible.

P58. $\mathrm{Aut}_{\mathbb{F}_p}\mathbb{F}_p(\varepsilon_{12})=\langle F\rangle\subseteq(\mathbb{Z}/12\mathbb{Z})^*=\langle\bar{1},\bar{5},\bar{7},-\bar{1}\rangle$, $F\mapsto\bar{p}$. El polinomio de raíces primitivas 12-ésimas de la unidad es x^4-x^2+1. Si hacemos el cambio $y=x+1/x$, tenemos que $x^4-x^2+1=x^2(y^2-3)$. Por tanto, $\varepsilon_{12}+1/\varepsilon_{12}=\sqrt{3}$ (y $\varepsilon_{12}^5+1/\varepsilon_{12}^5=-\sqrt{3}$). Por tanto, $\sqrt{3}\in\mathbb{F}_p\iff F(\sqrt{3})=\sqrt{3}\iff\bar{p}=\pm\bar{1}$.

P59. El discriminante δ del polinomio x^q-1 es igual a $q^{(q-1)/2}\sqrt{-q}$. Entonces, como $\sqrt{-1},\delta\in\mathbb{F}_p(\varepsilon_{4q})$, tenemos que $\sqrt{q}\in\mathbb{F}_p(\varepsilon_{4q})$.

P60. La sucesión $1\to\pm1\to\mathbb{F}_q^*\to\mathbb{F}_q^{*2}\to1$ es exacta, luego $\#\mathbb{F}_q^{*2}=(q-1)/2$, luego el número de cuadrados en $\mathbb{F}_q$ es $(q+1)/2$. Por órdenes, Q y $a-Q$ no pueden ser disjuntos, luego existen $b_1,b_2\in Q$ tales que $a-b_1=b_2$ y $a=b_1+b_2$.

P61. $\mathbb{F}_{p^n}^*\simeq\mathbb{Z}/(p^n-1)=\mathbb{Z}/((p-1)(p^{n-1}+p^{n-2}+\cdots+1))$. Vía este isomorfismo la norma N es igual a multiplicar por $p+p^2+\cdots+p^n\equiv p^{n-1}+p^{n-2}+\cdots1$, luego el orden de la imagen es $p-1$ y N es epiyectivo.

P62. Si x^3+ax-b es irreducible en $\mathbb{F}_p[x]$, es decir, $x^3+ax\equiv b$ (módulo p) no admite alguna solución entera, entonces su grupo de Galois sobre $\mathbb{F}_p$ es $\mathbb{Z}/3\mathbb{Z}=A_3$. En este caso, si $\delta=(\alpha_1-\alpha_2)\cdot(\alpha_2-\alpha_3)\cdot(\alpha_2-\alpha_3)=\sqrt{-4a^3-27b^2}$, entonces $\mathbb{F}_p=\mathbb{F}_p(\alpha_1)^{A_3}=\mathbb{F}_p(\sqrt{-4a^3-27b^2})$ y llegamos a contradicción.

Solución de los problemas del capítulo quinto

P1. Por cambio de cuerpo base, $\otimes_k K$, $A\otimes_k K$ es isomorfo a $K\times\overset{n}{\cdots}\times K$ y la homotecia por $a\otimes1$ es igual a la homotecia por $(g_1(a),\ldots,g_n(a))$, cuyo determinante es igual $N(a)=g_1(a)\cdots g_n(a)$ y cuya traza es igual a $Tr(a)=g_1(a)+\ldots+g_n(a)$.

P2. Sea F el morfismo de Frobenius. El grupo de Galois de $\mathbb{F}_{p^m}\hookrightarrow\mathbb{F}_{p^{nm}}$ es $G=\langle F^m\rangle$. Por tanto,

$$N(a)=F^m(a)\cdot F^{2m}(a)\cdots F^{nm}(a)=a^{p^m+p^{2m}+\cdots+p^{nm}}=a^{\frac{p^{nm}-1}{p^m-1}}$$

P3. $N(1+2e^{2\pi i/3})=(1+2e^{2\pi i/3})(1+2e^{4\pi i/3})=1+4+2(e^{2\pi i/3}+e^{4\pi i/3})=5-2=3$.

P4. El número complejo z es de módulo 1 si y sólo si $N(z)=1$, que equivale a decir por el teorema 90 de Hilbert que existe otro número complejo z' de modo que $z=z'/\overline{z'}$.

P5. Si $k = K_1 \hookrightarrow K_2 \hookrightarrow \cdots \hookrightarrow K_r = K$ y $k = K'_1 \hookrightarrow K'_2 \hookrightarrow \cdots \hookrightarrow K'_s = K'$ son dos resoluciones por radicales entonces

$$k = K_1 \hookrightarrow K_2 \hookrightarrow \cdots \hookrightarrow K_r \hookrightarrow K \cdot K'_2 \hookrightarrow \cdots \hookrightarrow K \cdot K'_s = K \cdot K'$$

es una resolución por radicales de $K \cdot K'$.

P6. Sea $\bar{k}$ el cierre algebraico de k y $\{g_1, \ldots, g_r\} = \mathrm{Hom}_{k-alg}(K, \bar{k})$. Entonces, la envolvente de Galois es $g_1(K) \cdots g_r(K)$, que es una extensión por radicales porque lo son $g_i(K)$, para todo i.

P7. Si $\mathbb{C}(a_1, a_2, a_3) \hookrightarrow \mathbb{C}(a_1, a_2, a_3)[x]/(p(x))$ fuese una extensión por radicales entonces sería radical y por tanto de Galois, que no lo es porque $\mathbb{C}(a_1, a_2, a_3)[x]/(p(x))$ sólo contiene una raíz de $p(x)$. La envolvente de Galois de K es una extensión por radicales porque su grupo de Galois, S_3 es resoluble.

P8. El cuerpo de descomposición, K, de $x^3 + 2x + 1$ sobre $\mathbb{Q}$ es una extensión de Galois de grupo S_3, porque la ecuación cúbica es irreducible y su discriminante es $\sqrt{-59} \notin \mathbb{Q}$. K no contiene subextensiones de Galois de grado 3 y $\mathbb{Q}(\sqrt{-59})$ es la única subextensión de grado 2. $\mathbb{Q}(e^{2\pi i/7})$, es una $\mathbb{Q}$-extensión de Galois de grupo $\mathbb{Z}/6\mathbb{Z}$, luego todas sus subextensiones son de Galois y contiene una única subextensión de grado 2, $\mathbb{Q}(\sqrt{-7})$ (calcúlese el discriminante de $x^7 - 1$. Por tanto, $K \cap \mathbb{Q}(\sqrt{-7}) = \mathbb{Q}$ y $\mathbb{Q}((e^{2\pi i/7}) \hookrightarrow \mathbb{Q}(e^{2\pi i/7}) \cdot K$ es una extensión de Galois de grupo S_3, por el teorema de los irracionales naturales.

P9. El grupo de Galois la cúbica está incluido en A_3.

P10. El grupo de Galois de $x^3 - x + 1$ es A_3 ó {Id}, por el problema 9. Si es {Id}, entonces el cuerpo de descomposición es K y las tres raíces están en K. Si es A_3, entonces el polinomio mínimo anulador de cualquiera de las raíces es $x^3 - x + 1$ y el polinomio es irreducible.

P11. Si tuviese alguna raíz compleja, entonces el automorfismo conjugar sería distinto del morfismo identidad, y como pertenece a A_3 sería de orden 3, lo cual es imposible, pues su orden es 2.

P12. Si el discriminante es positivo, entonces es un cuadrado en $\mathbb{R}$, luego su grupo de Galois es A_3 o {Id}. Si alguna raíz fuese compleja, entonces el automorfismo conjugar (en el cuerpo de descomposición de la cúbica) sería distinto de la identidad y de orden 2, lo cual es imposible. Si el discriminante es negativo, el entonces el automorfismo conjugar (en el cuerpo de descomposición de la cúbica) sería distinto de la identidad, luego una raíz con su conjugada son imaginarias y la tercera real.

P13. $\mathbb{Q}(\sqrt{\Delta}, \alpha) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)^H$, para cierto subgrupo H del grupo de Galois de la cúbica. Si $H \cdot \sqrt{\Delta} = \sqrt{\Delta}$ entonces $H \subseteq A_3$; y si además $H \cdot \alpha_1 = \alpha_1$ entonces $H = \{\mathrm{Id}\}$. Por tanto, $\mathbb{Q}(\sqrt{\Delta}, \alpha) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

P14. Sea ε_3 una raíz cúbica primitiva de la unidad. El cuerpo de descomposición de x^3-a es $k(\sqrt[3]{a},\varepsilon_3)$. Si $\varepsilon_3\in k$, entonces el cuerpo de descomposición es $k(\sqrt[3]{a})$ y el grupo de Galois es $\mathbb{Z}/3\mathbb{Z}$, si $\sqrt[3]{a}\notin k$ ó {Id} si $\sqrt[3]{a}\in k$. Si $\varepsilon_3\notin k$, entonces el cuerpo de composición es la cúbica es de grado 6, si $\sqrt[3]{a}\notin k$, luego su grupo de Galois es S_3, ó el cuerpo de descomposición es $k(\varepsilon_3)$, si $\sqrt[3]{a}\in k$, luego su grupo de Galois es $\mathbb{Z}/2\mathbb{Z}$.

P15. Por el problema 14, el grupo de Galois sobre $\mathbb{Q}(a)$ es S_3 y sobre $\mathbb{C}(a)$ es $\mathbb{Z}/3\mathbb{Z}$.

P16. La resolvente cúbica de la cuártica es $(x-a)(x^2-4b)$ y el cuerpo de descomposición de la resolvente cúbica es $\mathbb{Q}(\sqrt{b})$, de grupo de Galois $G/(G\cap K_4)$. Si $\sqrt{b}\in\mathbb{Q}$ entonces $G\cap K_4=G$ y $G=K_4$. Supongamos que $\sqrt{b}\notin\mathbb{Q}$, luego $G=\langle\sigma=(1,2,3,4),\tau=(1,2)(3,4)\rangle$ ó $G=\langle\sigma\rangle$. Las raíces de la cuártica son $\alpha,\beta=\sigma(\alpha),-\alpha=\sigma^2(\alpha),-\beta=\sigma^3(\alpha)$. Observemos que $\alpha^2\in\mathbb{Q}(\alpha,\beta)^{G\cap K_4}$ si $G=\langle\sigma\rangle$ y que $\alpha^2\notin\mathbb{Q}(\alpha,\beta)^{K_4}$ si $G=\langle\sigma,\tau\rangle$. Es decir, y^2+ay+b es reducible sobre $\mathbb{Q}(\sqrt{b})$ si $G=\langle\sigma\rangle$ (que equivale a decir que $\sqrt{a^2-4b}\in\mathbb{Q}(\sqrt{b})$, que equivale a decir que $a^2-4b=b\cdot c^2$, que equivale a decir que ba^2-4b^2 es un cuadrado); y y^2+ay+b es irreducible sobre $\mathbb{Q}(\sqrt{b})$ si $G=\langle\sigma,\tau\rangle$ (que equivale a decir que ba^2-4b^2 no es un cuadrado).

P17. El subgrupo de S_4 que dejan fijo el 1 es S_3. Si el grupo de Galois de la cuártica es S_4 tenemos que ver que no existen subgrupos propios entre S_4 y S_3. Si el grupo de Galois de la cuártica es A_4 tenemos que ver que no existen subgrupos propios entre A_4 y $A_4\cap S_3=A_3$. Si el grupo de Galois de la cuártica es D_4 tenemos que ver que existen subgrupos propios entre D_4 y $D_4\cap S_3=\{1\}$. Si el grupo de Galois de la cuártica es $\mathbb{Z}/4\mathbb{Z}$ tenemos que ver que existen subgrupos propios entre $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/4\mathbb{Z}\cap S_3=\{1\}$. Si el grupo de Galois de la cuártica es K_4 tenemos que ver que existen subgrupos propios entre K_4 y $K_4\cap S_3=\{1\}$.

P18. El automorfismo conjugar es una transposición. Los únicos grupos de Galois de una cuártica que contienen una transposición son S_4 y D_4.

P19. La resolvente cúbica de la cuártica es $(x-2)(x^2+(2-b)x+a^2-2b)$ y el cuerpo de descomposición de la resolvente cúbica es $\mathbb{Q}(\sqrt{b^2+4b+4-4a^2})$, de grupo de Galois $G/(G\cap K_4)$. Si $\sqrt{b^2+4b+4-4a^2}\in\mathbb{Q}$ entonces $G\cap K_4=G$ y $G=K_4$. Supongamos que $\sqrt{b^2+4b+4-4a^2}\notin\mathbb{Q}$, luego $G=\langle\sigma=(1,2,3,4),\ \tau=(1,2)(3,4)\rangle$ ó $G=\langle\sigma\rangle$. Las raíces de la cuártica son $\alpha,\beta=\sigma(\alpha),1/\alpha=\sigma^2(\alpha),1/\beta=\sigma^3(\alpha)$. Observemos que $\alpha+1/\alpha\in\mathbb{Q}(\alpha,\beta)^{K_4}$ si $G=\langle\sigma\rangle$ y que $\alpha+1/\alpha\notin\mathbb{Q}(\alpha,\beta)^{K_4}$ si $G=\langle\sigma,\tau\rangle$. Es decir, $y^2+ay+(b-2)$ es reducible sobre $\mathbb{Q}(\sqrt{b^2+4b+4-4a^2})$ si $G=\langle\sigma\rangle$ (que equivale a decir que $\sqrt{a^2-4b+8}\in\mathbb{Q}(\sqrt{b^2+4b+4-4a^2})$, que equivale a decir que $a^2-4b+8=(b^2+4b+4-4a^2)\cdot c^2$, que equivale a decir que $(b^2+4b+4-4a^2)\cdot(a^2-4b+8)$ es un cuadrado); y $y^2+ay+(b-2)$ es irreducible sobre $\mathbb{Q}(\sqrt{b})$ si $G=\langle\sigma,\tau\rangle$ (que equivale a decir que $(b^2+4b+4-4a^2)\cdot(a^2-4b+8)$ no es un cuadrado).

P20. Es D_4 por el problema 16.

P21. Es D_4 por el problema 19.

P22. a. El grupo de Galois deja fijas las raíces que están en k. Las permutaciones de las cuatro raíces que dejan fijas a tres han de dejar fijas las cuatro.

b. El grupo de Galois deja fija dos raíces y no es el grupo trivial. Luego es el conjunto de permutaciones de las otras dos raíces, $G = S_2 = \{id, (1,2)\}$.

c. $p_4(x) = (x-a)p_3(x)$, con $p_3(x)$ irreducible y $a \in k$. El grupo de Galois de $p_4(x)$ es igual al grupo de Galois de $p_3(x)$. El discriminante de $p_4(x)$ es igual (compruébese) a $p_3(a)^2$ multiplicado por el discriminante de $p_3(x)$.

d. Como $p_4(x)$ no es irreducible, tenemos que $p_4(x) = p_2(x) \cdot q_2(x)$. Digamos que α_1, α_2 son las raíces de $p_2(x)$ y que α_3, α_4 son las raíces de $q_2(x)$. Si $\alpha_3 \in k(\alpha_1)$ entonces, el cuerpo de descomposición del polinomio $p_4(x)$ es $k(\alpha_1) = k(\alpha_3)$, luego $G = \{id, (1,2)(3,4)\}$. Si $\alpha_3 \notin k(\alpha_1)$, entonces el cuerpo de descomposición de $p_4(x)$ es $k(\alpha_1) \otimes_k k(\alpha_3)$ y su grupo de Galois es $G = \langle (1,2) \rangle \times \langle (3,4) \rangle$.

P23. El grupo de Galois de $x^4 - 4x^2 + 2$ es el grupo cíclico $\mathbb{Z}/4\mathbb{Z}$, por el problema 16.

El grupo de Galois de $x^4 + 6x^2 + 1$ es el grupo de Klein por el problema 16.

La cúbica resolvente de $x^4 - 3x + 1$ es $x^3 - 4x - 9$, cuyo discriminante es $4^4 - 3^7$. Luego el grupo de Galois de la cúbica es S_3 y por tanto el grupo de Galois de la cuártica es S_4.

El grupo de Galois de $2x^4 + x^3 - x^2 + 2x - 1 = (x - 1/2) \cdot (2x^3 + 2x^2 + 2)$ es el grupo de Galois de $x^3 + x^2 + 1$. El discriminante de $x^3 + x^2 + 1$ es -31. Luego el grupo de Galois de $2x^4 + x^3 - x^2 + 2x - 1$ es S_3.

El grupo de Galois de $x^4 + 1$ es $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

El polinomio $12x^4 + 8x^3 + 1 = (6x^2 + 1)(2x^2 + 1)$ no es irreducible, su cuerpo de descomposición es $\mathbb{Q}(\sqrt{-6}, \sqrt{-2}) = \mathbb{Q}(\sqrt{-6}) \otimes_{\mathbb{Q}} (\sqrt{-2})$, luego su grupo de Galois es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

El polinomio $x^4 - 3x^3 + 4x^2 - 2x + 1$ es irreducible. Su cúbica resolvente es igual a $x^3 - 4x^2 + 2x + 3 = (x-3)(x^2 - x - 1)$ cuyo cuerpo de descomposición es $\mathbb{Q}(\sqrt{5})$. Digamos que $3 = \alpha_1\alpha_3 + \alpha_2\alpha_4$. En este caso el grupo de Galois es $G = \langle (1,2,3,4), (1,3) \rangle$ (y $G \cap K_4 = K_4$), ó $G = \langle (1,2,3,4) \rangle$ (y $G \cap K_4 = \langle (1,3)(2,4) \rangle$). Observemos que $(x - \alpha_1\alpha_3) \cdot (x - \alpha_2\alpha_4) = x^2 - 3x + 1$ y que $\alpha_1\alpha_3 = (3 + \sqrt{5})/2 \in \mathbb{Q}(\sqrt{5})$. Por tanto, $\alpha_1\alpha_3$ es invariante por $G \cap K_4$, luego $G \cap K_4 = \langle (1,3)(2,4) \rangle$ y $G = \langle (1,2,3,4) \rangle$.

El grupo de Galois de $x^4 - 3x^3 - 3x^2 + 10x - 3 = (x-3)(x^3 - 3x + 1)$ es el grupo de Galois de $x^3 - 3x + 1$ (que es irreducible), cuyo discriminante es 9^2. Luego el grupo de Galois de $x^4 - 3x^3 - 3x^2 + 10x - 3$ es A_3.

P24. Por el problema 22: 1. $(x^2 + 1) \cdot ((x+3)^2 + 1)$. 2. $(x^2 + 1) \cdot (x^2 + 2)$.

P25. Una extensión de Galois es una extensión por radicales cuadráticos si y sólo si su grado es una potencia de 2. El grado de $\mathbb{Q}(e^{\frac{2\pi i}{7}})$ es 6, el de $\mathbb{Q}(e^{\frac{2\pi i}{8}})$ es $4 = 2^2$, el de $\mathbb{Q}(e^{\frac{2\pi i}{9}})$ es 6, el de $\mathbb{Q}(e^{\frac{2\pi i}{11}})$ es 10, el de $\mathbb{Q}(e^{\frac{2\pi i}{12}})$ es $4 = 2^2$, el de $\mathbb{Q}(e^{\frac{2\pi i}{13}})$ es 12, el de $\mathbb{Q}(e^{\frac{2\pi i}{14}})$ es 6, el de $\mathbb{Q}(e^{\frac{2\pi i}{15}})$ es $8 = 2^3$ y el $\mathbb{Q}(e^{\frac{2\pi i}{16}})$ es $8 = 2^3$.

P26. $\mathbb{Q}(\sqrt{2}+\sqrt[3]{3})$ es una $\mathbb{Q}$-extensión de grado 6, que no es una potencia de 2, luego $\sqrt{2}+\sqrt[3]{3}$ no es un irracional cuadrático. $\mathbb{Q}(\sqrt[5]{2})$ es una $\mathbb{Q}$-extensión de grado 5, que no es una potencia de 2, luego $\sqrt[5]{2}$ no es un irracional cuadrático. $\sqrt[4]{2}=\sqrt{\sqrt{2}}$, luego es un irracional cuadrático.

Práctica de Mathematica

Primero bajamos de internet el paquete AlgFields.txt, le indicamos al *Mathematica* dónde lo hemos guardado y lo instalamos.

```
In[1]:= SetDirectory[
         "C://Archivos de programa/Wolfram Research/Mathematica/8.0"]
Out[1]= C:\Archivos de programa\Wolfram Research\Mathematica\8.0
In[2]:= << AlgFields.txt
```

Calculemos el cociente de x^2+x+1 por el polinomio x (e indiquemos al final cuál es la variable).

```
In[3]:= PolynomialQuotient[x^2 + x + 1, x, x]
Out[3]= 1 + x
```

Calculemos el resto de dividir x^2 + x + 1 por el polinomio x.

```
In[4]:= PolynomialRemainder[x^2 + x + 1, x, x]
Out[4]= 1
```

Descompongamos x^2 + x en factores simples.

```
In[5]:= Factor[x^2 + x]
Out[5]= x (1 + x)
```

Calculemos el máximo comun divisor de x^2+x y x^3+x.

```
In[6]:= PolynomialGCD[x^2 + x, x^3 + x]
Out[6]= x
```

Calculemos el máximo comun divisor de x^2 + x y x^3 + x, y los polinomios de la identidad de Bezout.

```
In[7]:= PolynomialExtendedGCD[x^2 + x, x^3 + x, x]
```

$$\text{Out[7]= } \left\{x, \left\{\frac{1-x}{2}, \frac{1}{2}\right\}\right\}$$

Trabajemos con extensiones de Q. Definamos la extensión K=Q[a], donde a es raíz de x^3-x+3.

```
In[8]:= FDeclareField[K, {a^3 - a + 3}]
----Details of field K----
  Algebraic Numbers: {a}
  Dimension over Q: 3
  Minimal Polynomials: {3 - a + a^3}
  Root Approximations: {-1.6716998816571609697}
----
```

Factoricemos x^3-x+3 en K[x].

```
In[9]:= FFactor[x^3 - x + 3, K]
```

$$\text{Out[9]= } -(a-x)\left(-1+a^2+a\,x+x^2\right)$$

Calculemos el inverso de a^2+1 (en K).

```
In[10]:= FInvert[a^2 + 1, K]
```

$$\text{Out[10]= } \frac{4}{13}-\frac{3\,a}{13}-\frac{2\,a^2}{13}$$

Simplifiquemos a^4 + 3*a^3 + a^2 - a + 5.

```
In[11]:= FSimplifyE[a^4 + 3*a^3 + a^2 - a + 5, K]
```

$$\text{Out[11]= } -4-a+2\,a^2$$

Calculemos el polinomio mínimo anulador de a^2+1 en K (y expresemoslo como polinomio en x).

```
In[12]:= FMinPoly[a^2 + 1, x, K]
```

$$\text{Out[12]= } -13+8\,x-5\,x^2+x^3$$

Calculemos el máximo comun divisor de x^3-x+3 y x^2-a^2 en K[x].

```
In[13]:= FPolynomialExtendedGCD[x^3 - x + 3, x^2 - a^2, x, K]
```

$$\text{Out[13]= } \left\{-a+x,\ \left\{-\frac{a}{3},\ \frac{a\,x}{3}\right\}\right\}$$

Definamos la extensión L=Q[a,b] donde a es la "primera" raíz de x^3 - x + 3 y b es la "segunda" raíz de x^2 - 2.

```
In[14]:= FDeclareField[L, {a^3 - a + 3, b^2 - 2}, {1, 2}]
----Details of field L----
  Algebraic Numbers: {a, b}
  Dimension over Q: 6
  Minimal Polynomials: {3 - a + a^3, -2 + b^2}
  Root Approximations:
 {-1.6716998816571609697, 1.4142135623730950488}
----
```

Definamos la L-extensión L2=L(c) donde c es la segunda raíz de x^4 - x^2 + 3.

```
In[15]:= FDeclareExtensionField[L2, L, {c^4 - c^2 + 3}, {2}]
----Details of field L2----
  Algebraic Numbers: {a, b, c}
  Dimension over Q: 24
  Minimal Polynomials: {3 - a + a^3, -2 + b^2, 3 - c^2 + c^4}
  Root Approximations:
 {-1.6716998816571609697, 1.4142135623730950488,
  -1.0564210352811224890 5 + 0.78487285835633190582 i}
----
```

Definamos el cuerpo de descomposición de x^4 - 2, SF.

```
In[16]:= FDeclareSplittingField[SF, x^4 - 2]
----Details of field SF----
  Algebraic Numbers: {r3, r4, r5, r6}
  Dimension over Q: 8
  Minimal Polynomials:
 {-2 + r3^4, r3 + r4, r3^2 + r5^2, r5 + r6}
  Root Approximations: {-1.1892071150027210667,
  1.1892071150027210667, 0. × 10^-21 - 1.1892071150027106672 i,
  0. × 10^-21 + 1.1892071150027106672 i}
----
```

Definamos la SF-extensión que sea el cuerpo de descomposición de x^2 - 2, SF2.

```
In[17]:= FDeclareSplittingExtensionField[SF2, SF, x^2 - 2, {z1, z2}]
----Details of field SF2----
  Algebraic Numbers: {r3, r4, r5, r6, z1, z2}
  Dimension over Q: 8
  Minimal Polynomials: {-2 + r3^4, r3 + r4,
  r3^2 + r5^2, r5 + r6, r3^2 + z1, -r3^2 + z2}
  Root Approximations: {-1.1892071150027210667,
  1.1892071150027210667, 0. × 10^-21 - 1.1892071150027106672 i,
  0. × 10^-21 + 1.1892071150027106672 i,
  -1.4142135623730950488, 1.4142135623730950488}
----
```

Calculemos el grupo de Galois de SF.

```
In[18]:= FGaloisGroup[SF]
Out[18]= {{{r3, r4, r5, r6}, {r3, r4, r5, r6}},
  {{r3, r4, r5, r6}, {r3, r4, r6, r5}},
  {{r3, r4, r5, r6}, {r4, r3, r5, r6}},
  {{r3, r4, r5, r6}, {r4, r3, r6, r5}},
  {{r3, r4, r5, r6}, {r5, r6, r3, r4}},
  {{r3, r4, r5, r6}, {r5, r6, r4, r3}},
  {{r3, r4, r5, r6}, {r6, r5, r3, r4}},
  {{r3, r4, r5, r6}, {r6, r5, r4, r3}}}
```

Calculemos la cúbica resolvente de la cuártica general, es decir, si x1,x2,x3,x4 son las raíces de la cuártica x^4 - σ1x^3 + σ2x^2 -σ3x + σ4, queremos calcular la cúbica de raíces x1*x2+x3*x4, x1*x3+x2*x4, x1*x4+x2*x4 (que son los transformados de x1*x2+x3*x4 por S_4).

```
In[19]:= FGaloisResolvent[x1 * x2 + x3 * x4, {x1, x2, x3, x4}, x]

Out[19]= x^3 - x^2 σ2 - σ3^2 + x (σ1 σ3 - 4 σ4) - σ1^2 σ4 + 4 σ2 σ4
```

Calculemos la cúbica resolvente de x^4 - x^3 + 2*x + 5.

```
In[20]:= FGaloisResolvent[x1 * x2 + x3 * x4,
          {x1, x2, x3, x4}, x, x^4 - x^3 + 2 * x + 5]

Out[20]= -9 - 22 x + x^3
```

Expresemos un polinomio simétrico en n variables como polinomio en las funciones simétricas elementales σ1,...,σn.

```
In[21]:= FGaloisResolvent[x1^2 + x2^2 + x3^2 + x4^2, {x1, x2, x3, x4}, x]

Out[21]= x - σ1^2 + 2 σ2
```

Calculemos el discriminante de la cúbica general.

```
In[22]:= FGaloisResolvent[(x1 - x2) * (x1 - x3) * (x2 - x3), {x1, x2, x3}, x]

Out[22]= x^2 - σ1^2 σ2^2 + 4 σ2^3 + 4 σ1^3 σ3 - 18 σ1 σ2 σ3 + 27 σ3^2
```

Bibliografía

1. E. Artin, Teoría de Galois, Colección de Matemáticas Nuevo Límite, Vicens-Vives, España, 1970, traducción y prólogo de R. Rodríguez Vidal.

2. M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Reading Mass., Addison-Wesley Publishing Company, Massachusetts, 1969.

3. N. Bourbaki, Algèbre, chapitres 4 a 7, Elements de Mathematique, Masson, Paris, 1981.

4. J. Dorronsoro and E. Hernández, Números, grupos y anillos, Addison-Wesley/Universidad Autónoma de Madrid, Madrid, 1996.

5. L. Gaal, Classical Galois Theory, Chelsea Publishing Company, NY, 1973.

6. R. Hartshorne, Geometry: Euclid and beyond, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2000.

7. A.I. Kostrikin, Introducción al algebra, McGraw-Hill/Interamericana de España, Madrid, 1992.

8. S. Lang, Álgebra, Aguilar S.A. de ediciones, Madrid, 1971.

9. J.S. Milne, Field and Galois theory, 2002, Apuntes de clase disponible en:

   http://www.jmilne.org/math/CourseNotes/math594f.html.

10. J.A. Navarro González, Teoría de Galois, Sección de Matemáticas, vol. 5, Universidad de Extremadura, 1984.

11. J.A. Navarro González, Álgebra conmutativa básica, Manuales de Unex, vol. 19, Universidad de Extremadura, 1996.

12. R. Pastor, Lecciones de Álgebra, Nuevas Gráficas, Madrid, 1960.

13. I. Stewart, Galois Theory, Chapman and Hall mathematics series, London 1973.

14. J. Swallow, Exploratory Galois theory, Cambridge Univ. Press, New York, 2004.

Páginas web interesantes

1. Puedes encontrar interesantes biografías de matemáticos en la Universidad de Saint Andrews. Introduce en el buscador de Google: Saint Andrews y Biographies.

2. Curso online de Álgebra del MIT en www.ocw.mit.edu/courses/mathematics/ Busca el curso Algebra II.

3. Curso online de Álgebra de Harvard en www.openculture.com/freeonlinecourses/ Busca en sciences, mathematics, Abstract Algebra.

4. Busca en youtube los vídeos:

   a) Insólita historia de Évariste Galois.

   b) Último teorema de Fermat (documental de la BBC).

   c) Universo Matemático 5. Gauss, de lo real a lo imaginario.

   d) Universo Matemático 4. Fermat: El margen más famoso de la historia.

Índice alfabético

UNIVERSIDAD DE EXTREMADURA

UNIÓN EUROPEA
FONDO EUROPEO DE
DESARROLLO REGIONAL:
UNA MANERA DE HACER EUROPA

GOBIERNO DE EXTREMADURA
Consejería de Empleo, Empresa e Innovación

91