NOTAS PARA UN CURSO DE

TEORÍA DE GALOIS

Nieves Rodríguez González Purificación López López
Emilio Villanueva Nóvoa

2021

II

Índice general

1. Complementos de teoría de grupos **3**
- 1.1. Generalidades . . . 3
- 1.2. Grupos finitos. Teoremas de Sylow . . . 12
- 1.3. El grupo simétrico. Grupos resolubles . . . 26
- 1.4. Ejercicios . . . 37

2. Complementos de teoría de anillos **43**
- 2.1. Generalidades . . . 43
- 2.2. Dominios Euclídeos. Divisibilidad . . . 48
- 2.3. Anillos de Polinomios . . . 56
- 2.4. Factorización de polinomios . . . 59
- 2.5. Ejercicios . . . 71

3. Extensiones de cuerpos **75**
- 3.1. Extensiones finitas . . . 75
- 3.2. Extensiones algebraicas . . . 80
- 3.3. Construcciones con regla y compás . . . 87
- 3.4. Ejercicios . . . 93

4. Extensiones separables y normales **99**
- 4.1. Extensión de encajes . . . 99
- 4.2. Cuerpos de escisión . . . 103
- 4.3. Clausura algebraica de un cuerpo . . . 110
- 4.4. Separabilidad . . . 115
- 4.5. Teorema del elemento primitivo . . . 127
- 4.6. Extensiones normales. Clausura normal . . . 130
- 4.7. Ejercicios . . . 135

5. Teoría de Galois **139**
- 5.1. Extensiones de Galois. Teorema fundamental de la teoría de Galois . . . 139
- 5.2. El Teorema fundamental del Álgebra . . . 146
- 5.3. Cuerpos finitos. Raíces de la unidad . . . 148
- 5.4. Resolubilidad por radicales . . . 157
- 5.5. La ecuación general de grado n . . . 177

5.6. Ejercicios 187

6. Complementos **191**
6.1. Constructibilidad de polígonos regulares. Teorema de Gauss-Wantzel . . 191
6.2. La trascendencia de π 194

Indicaciones para los ejercicios **201**

Prólogo

Salvo en lo concerniente a resolubilidad en característica positiva, el material utilizado para la elaboración de este manual está constituido esencialmente por las notas de clase utilizadas por los autores en los últimos años para el desarrollo de la docencia de la asignatura *Álgebra* de la Licenciatura en Matemáticas de la USC. El objetivo final de la materia es la obtención del Gran Teorema de Galois sobre resolubilidad por radicales de ecuaciones algebraicas, y con estas notas se pretende facilitar el acceso al contenido del curso. Para seguirlo es muy recomendable haber cursado previamente una materia introductoria de Álgebra en la que hayan sido tratados con el detalle necesario gran parte de los tópicos fundamentales contemplados sucintamente en el Capítulo 2, y cuya presencia en este manual se justifica por la intención de los autores de facilitar la lectura del mismo.

La deficitaria formación algebraica de los alumnos en temas de naturaleza más elemental hace imprescindible iniciar el curso con un estudio de grupos finitos que incluya la teoría de Sylow, algunos detalles sobre los grupos de permutaciones y la resolubibilidad. En esto consiste el Capítulo 1. El tratamiento de las generalidades de las teorías de grupos y anillos que hacemos a lo largo de los dos primeros capítulos es muy esquemático, y refleja también la recomendable actitud de brevedad necesaria en el desarrollo docente de la materia para poder abarcar el contenido de la misma en el tiempo asignado, ya que el plan de estudios confina a esta asignatura en un cuatrimestre de docencia. Esta exigua duración del curso y el tiempo que es necesario dedicar al desarrollo de las ya mencionadas nociones básicas constituyen el principal motivo de que el profesor abandone pronto la idea de presentar la resolubilidad en su completa generalidad, es decir, en característica arbitraria.

También se ha pretendido que, de algún modo, estas notas sean testimonio de lo realizado a lo largo de los últimos años en la docencia de esta materia y por ello presentamos por separado la resolubilidad en característica cero, ya que en ninguna ocasión, durante el período de referencia, ha habido la opción de desarrollarla en característica positiva. No obstante, alguna vez y de modo esporádico, ha sido posible esbozar un estudio de separabilidad en característica p y el mencionado carácter testimonial nos ha llevado a incluir ese material por la enorme importancia que tienen las peculiaridades de dicha teoría para la formación de un matemático. Una vez hecho esto, la resolubilidad en característica positiva se obtiene con un pequeño esfuerzo adicional y ésta es la razón por la que, finalmente, se ha decidido incluirla con el quizá desmesurado optimismo de

que alguna vez sea posible incorporarla al curso, lo que sin duda no sería utópico en una materia con docencia anual.

No hemos sabido resistir la tentación de completar el manual con los métodos de resolución de las ecuaciones de tercer y cuarto grado obtenidos a partir de la teoría general, y de añadir además un apéndice dedicado a una prueba relativamente sencilla de la trascendencia de π (sección 6.2) que completa el estudio del probLema de la cuadratura del círculo (3.30) ya tratado en el capítulo 2.

Quien esté interesado solamente en la versión en característica cero puede pasar directamente del corolario 4.29 al Lema 4.53, y en el párrafo de resolubilidad por radicales puede omitir todas las referencias al caso de característica positiva, finalizando la teoría con el Teorema de Abel (5.46). Por coherencia, el estudio sobre la resolubilidad de la ecuación general de grado n se verá entonces restringido al caso de característica nula.

Cada capítulo termina con una colección de ejercicios y al final del texto hay una sección con indicaciones para resolverlos. La bibliografía contiene algunos de los libros cuyo estilo nos ha parecido más próximo al tratamiento que se hace de la materia en este manual. Los autores no son ajenos a la opinión de que una formación matemática idónea es connatural con la consulta y estudio de los excelentes libros existentes, tanto en ésta como en otras materias, y recomiendan el uso de los mismos al abordar los temas tratados y la resolución de los probLema s allí propuestos.

Estas notas, que nacieron con vocación de ser una referencia sobre las exigencias mínimas sobre el contenido de un curso cuatrimestral -objetivo estrictamente cubierto, como se ha dicho, con lo relativo a característica cero- han sido finalmente completadas hasta lo que se puede considerar una declaración de principios sobre lo que los autores estiman imprescindible para un curso obligatorio de Álgebra, dedicado a Teoría de Galois, en una Titulación Superior de Matemáticas.

Capítulo 1

Complementos de teoría de grupos

El Teorema fundamental de teoría de Galois establece un antiisomorfismo de retículos entre el de subgrupos de un grupo de automorfismos de un cuerpo y el de subextensiones de la formada por este cuerpo y el subcuerpo fijo de dicho grupo. Esta biyección es usada sistemáticamente para la obtención del gran Teorema de Galois sobre la resolubilidad por radicales de una ecuación algebraica $f(X) = 0$, lo que constituye el objetivo central del curso. Esta resolubilidad quedará establecida en términos de las propiedades algebraicas del grupo de automorfismos del cuerpo de escisión de f sobre su cuerpo de coeficientes. El estudio de dichas propiedades algebraicas es la motivación de este capítulo

1.1. Generalidades

Aunque los conocimientos básicos necesarios forman parte del contenido de asignaturas de Álgebra previas (Álgebra Lineal, Introducción al Álgebra), con objeto de dotar a estas notas de un cierto grado de suficiencia para el seguimiento del curso y facilitar su lectura, se dedica esta primera sección a la exposición sucinta (y en gran medida informal) de las primeras cuestiones de la teoría de grupos.

Definición 1.1. Un *grupo* $(G, \cdot)$ es un conjunto no vacío G en el que existe una operación

$$\cdot : G \times G \to G$$

que satisface las siguientes propiedades:

i) La operación es asociativa, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, cualesquiera que sean x, y, z elementos de G. Por ello, en lo sucesivo se escribirá $(x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$. También,

cuando ello no suponga ambigüedad, se suprimirá el $\cdot$ para designar la operación, es decir, se pondrá xy en lugar de $x \cdot y$, (en concordancia con ello, diremos también que G es un grupo en lugar de $(G, \cdot)$ es un grupo).

ii) Existe un elemento neutro $e \in G$. Es decir, $\exists\ e \in G \mid ex = xe = x$, $\forall x \in G$ (el elemento neutro es único, pues si e' es neutro también, se tiene $e = ee' = e'$)

iii) Para cada $x \in G$ existe un $x^{-1} \in G$ tal que $xx^{-1} = x^{-1}x = e$. El elemento x^{-1} se denomina inverso (u opuesto) de x. (Tal inverso es único pues si $xy = e$, se tiene $y = x^{-1}xy = x^{-1}e = x^{-1}$ por la propiedad asociativa).

Recuérdese que si $x, y \in G$ entonces $(xy)^{-1} = y^{-1}x^{-1}$ (ya que, por la unicidad del inverso, de $y^{-1}x^{-1}xy = y^{-1}y = e$ se deduce $(xy)^{-1} = y^{-1}x^{-1}$.

Se dirá que un grupo G es *abeliano* si satisface la propiedad conmutativa, es decir, si $xy = yx$, $\forall x, y \in G$. Frecuentemente se reserva para estos grupos el símbolo $+$ para denotar la operación, el 0 para el neutro y con $-x$ se indicará el opuesto de x.

Observación 1.2. Si en un conjunto G está definida una operación asociativa, se dirá que un elemento $x \in G$ es idempotente si $x^2 = xx = x$. En este caso, $x^n := x\overset{n)}{\cdots}x = x$ para todo número natural n. Pues bien, si G es un grupo, el único elemento idempotente de G es el neutro ($x^2 = x \Rightarrow x = x^{-1}xx = x^{-1}x = e$).

Definición 1.3. Un subconjunto no vacío H de un grupo G se dirá que es un *subgrupo* de G si la operación de G induce en H una estructura de grupo con el mismo elemento neutro. Es decir,

i) $xy \in H, \forall x, y \in H$.

ii) $e \in H$

iii) $x^{-1} \in H$, $\forall x \in H$.

Observación 1.4. Un subconjunto no vacío H de un grupo G es un subgrupo de G si, y solo si, se satisface la propiedad

$$x, y \in H \Rightarrow x^{-1}y \in H.$$

En efecto, si H es subgrupo de G es evidente que la condición se cumple. Recíprocamente, para $x \in H \neq \emptyset$, dado que $x, x \in H$, se sigue que $e = x^{-1}x \in H$. Entonces para

$x \in H$, se tiene $x, e \in H$ y así $x^{-1} = x^{-1}e \in H$. Finalmente, para $x, y \in H$ se tiene $x^{-1}, y \in H$ por lo ya demostrado, y entonces $xy = \left(x^{-1}\right)^{-1} y \in H$.

Si $\{H_i \mid i \in I\}$ es una familia de subgrupos del grupo G entonces $\bigcap_{i\in I} H_i$ es también subgrupo de G. En efecto, de $x, y \in \bigcap_{i\in I} H_i$ se deduce inmediatamente $x^{-1}y \in \bigcap_{i\in I} H_i$ ya que, para cada $i \in H_i$, se tiene $x^{-1}y \in H_i$ al ser cada H_i un subgrupo de G.

Con la determinación de la naturaleza de los subgrupos de $(\mathbb{Z}, +)$ se inicia la teoría de divisibilidad en $\mathbb{Z}$. Si H es un tal subgrupo y si $s \neq 0$ es el menor entero positivo que está en H entonces $H = s\mathbb{Z}$, es decir, H consiste en el conjunto de los múltiplos de s (Si $t \in H$, el algoritmo de Euclides proporciona enteros q, r con $0 \leqslant r < s$ tales que $t = qs + r$, con lo que se obtiene $r = t - qs \in H$ ya que $qs \in H$; de ello se deduce que $r = 0$ por la selección de s.

Definición 1.5. Si G es un grupo y $\backsim$ es una relación binaria en G, se dirá que $\backsim$ es compatible por la izquierda con la operación de G si

$$x \backsim y \Rightarrow zx \backsim zy, \forall z \in G.$$

De modo análogo se define relación binaria en G compatible por la derecha con la operación de G.

Proposición 1.6. *Sea G un grupo.*

i) Si H es un subgrupo de G la relación binaria en G, ${}_H\backsim$ definida por

$$x_H \backsim y :\Leftrightarrow x^{-1}y \in H$$

es de equivalencia y compatible por la izquierda con la operación de G. Análogamente, la relación

$$x \backsim_H y :\Leftrightarrow xy^{-1} \in H$$

es de equivalencia y compatible por la derecha con la operación del grupo. La clase de equivalencia de cada $x \in G$ módulo la relación ${}_H\backsim$ (respectivamente, la relación $\backsim_H$) es $[x]_{H\backsim} = xH$ (respectivamente, $[x]_{\backsim_H} = Hx$).

ii) Si $\backsim$ es una relación de equivalencia en G, compatible por un lado con la operación del grupo, entonces la clase de equivalencia, $H = [e]_{\backsim}$, del elemento neutro, e, es un subgrupo.

iii) $H_{H\backsim} = H$ y ${}_{H_\backsim}\backsim = \backsim$. (Análogamente, $H_{\backsim_H} = H$ y $\backsim_{H_\backsim} = \backsim$).

Demostración. *i*) $x_H \backsim y$, $z \in G \Rightarrow (zx)^{-1}zy = x^{-1}z^{-1}zy = x^{-1}y \in H \Leftrightarrow zx_H \backsim zy$. Además $y \in [x]_{H^\backsim} \Leftrightarrow x_H \backsim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow\ y \in xH$. Para la prueba de *ii*) obsérvese que si $x, y \in H_\backsim = [e]_\backsim$, es decir, de $x \backsim e$ e $y \backsim e$, resulta $x^{-1}y \backsim x^{-1}e \backsim x^{-1}x = e$ por la compatibilidad por la izquierda de $\backsim$ con la operación del grupo, y por tanto $H_\backsim$ es un subgrupo de G (1.4). Además, $x \in H_{H^\backsim} \Leftrightarrow x_H \backsim e \Leftrightarrow x \in eH = H$ por lo ya demostrado. También $x_{H_\backsim} \backsim y \Leftrightarrow x^{-1}y \in H_\backsim \Leftrightarrow x^{-1}y \sim e \Leftrightarrow y \backsim x \Leftrightarrow x \backsim y$, con lo que también queda demostrado *iii*). □

Observación 1.7. Designaremos con

$$G/H = \{xH \mid x \in G\}$$

y con

$$H \setminus G = \{Hx \mid x \in G\}$$

las particiones de G correspondientes a las anteriores relaciones de equivalencia.

Como $\#H = \#xH$, $\forall x \in G$ (la aplicación $H \overset{t_x}{\to} xH$ definida por $t_x(h) = xh$ es biyectiva) y como $G = \coprod_{xH \text{ diferentes}} xH$ se tiene que $\#G = \#H\#\left(G/H\right)$.

De modo análogo se obtiene $\#G = \#H\#\left(H \setminus G\right)$.

Definición 1.8. Pondremos

$$(G : H) = \#\left(G/H\right).$$

y se denominará *índice* (por la izquierda) de H en G a este número, que será divisor del orden de G si éste es finito.

Definición 1.9. Si $(G, \cdot)$ y $(L, *)$ son grupos, una aplicación $f\colon G \to L$ es un *homomorfismo de grupos* si

$$f(xy) = f(x) * f(y),\ \forall x, y \in G.$$

Un homomorfismo biyectivo se llamará *isomorfismo*.

Así, un homomorfismo $f\colon G \to L$ es un isomorfismo si, y solo si, existe una aplicación inversa $f^{-1}\colon L \to G$ (que resulta ser también homomorfismo de grupos). Con la notación $L \simeq G$ se indicará que L y G son grupos isomorfos, es decir, que existe un isomorfismo entre ellos.

Observación 1.10. Si $f\colon G \to L$ es un homomorfismo de grupos y e_G y e_L son los correspondientes neutros entonces $f(e_G) = e_L$ ($f(e_G) = f(e_G e_G) = f(e_G) * f(e_G) \Rightarrow f(e_G) = e_L$ por (1.2), y entonces, $f(x^{-1}) = [f(x)]^{-1}$, para todo $x \in G$ ($e_L = f(e_G) = f(xx^{-1}) = f(x) * f(x^{-1})$ y se aplica la unicidad del inverso).

También, si H es un subgrupo de G, entonces $f(H)$ es subgrupo de L. En efecto,

$x = f(h),\ y = f(k)$ con $h, k \in H \Rightarrow x^{-1} * y = [f(h)]^{-1} * f(k) = f(x^{-1}y) \in H$.

Si K es subgrupo de L, entonces $f^{-1}(K) = \{x \in G \mid f(x) \in K\}$ es subgrupo de G ya que se verifica que:

$$x,\ y \in f^{-1}(K) \Leftrightarrow f(x),\ f(y) \in K \Rightarrow [f(x)]^{-1} * f(y) = f(x^{-1}y) \in K$$
$$\Rightarrow x^{-1}y \in f^{-1}(K))(1{,}4).$$

Definición 1.11. Para el homomorfismo $f\colon G \to L$ se definen dos subgrupos importantes:

i) *Imagen* de f, es el subgrupo $f(G)$ de L y se escribirá $\mathrm{Im}(f) = f(G)$.

ii) El *núcleo* de f, denotado con $\mathrm{Ker}(f)$, se define como $\mathrm{Ker}(f) = f^{-1}(\{e_L\})$.

(Obsérvese que $\{e_L\}$ es subgrupo de L y se aplica (1.10)).

Además $\mathrm{Ker}(f)$ es un subgrupo de G con la siguiente propiedad:
Si $x \in G$ e $y \in \mathrm{Ker}(f)$, como

$$f(xyx^{-1}) = f(x) * f(y) * f(x^{-1}) = f(x) * e_L * [f(x)]^{-1} = e_L,$$

se sigue que $xyx^{-1} \in \mathrm{Ker}(f)$.

La importancia de esta propiedad merece distinguir con un nombre especial a los subgrupos de un grupo que la satisfacen.

Definición 1.12. Si G es un grupo y H es un subgrupo de G, se dice que H es subgrupo *normal* (o invariante) de G si satisface cualquiera de las propiedades equivalentes siguientes:

i) $xHx^{-1} \subset H$, $\forall x \in G$

ii) $xHx^{-1} = H$, $\forall x \in G$

iii) $xH = Hx$, $\forall x \in G$.

iv) ${}_H\backsim = \backsim_H$.

La prueba de la equivalencia de las anteriores condiciones es fácil.

i) $\Rightarrow$ *ii)* Si *i)* se satisface para todo $x \in G$, se tiene también $x^{-1}H\left(x^{-1}\right)^{-1} = x^{-1}Hx \subset H$ y, por tanto, $x\left(x^{-1}Hx\right)x^{-1} = H \subset x^{-1}Hx$.

ii) $\Rightarrow$ *iii)* En virtud de la hipótesis, dado un $x \in G$, $\forall h \in H\ \exists k \in H$ tal que $xhx^{-1} = k$ y, por tanto, $xh = kx$, con lo que se obtiene $xH \subset Hx$. También, usando que $x^{-1}Hx = H$, se tiene que $\forall h \in H\ \exists k \in H$ tal que $x^{-1}hx = k$ y entonces $Hx \subset xH$.

iii) $\Leftrightarrow$ *iv)* Es evidente que dos relaciones son iguales si, y solo si, determinan la misma clase de equivalencia para cada elemento, es decir, si, y solo si, determinan la misma partición en el conjunto donde están definidas.

iii) $\Rightarrow$ *i)* Si $x \in G$ y $h \in H$ existe un $k \in H$ tal que $xh = kx$ y, por tanto, $xhx^{-1} = k$. Resulta así que $xHx^{-1} \subset H$.

Definición 1.13. Si G es un grupo se define el *centro* de G, Z_G, como el conjunto de elementos de G que conmutan con todos los elementos de G,

$$Z_G := \{a \in G \mid ab = ba,\ \forall b \in G\}.$$

Es muy fácil comprobar que el centro de G es un grupo abeliano, y que todo subgrupo de Z_G es normal en G.

Si G es un grupo abeliano todos sus subgrupos son normales. Por ejemplo todos los subgrupos de $(\mathbb{Z}, +)$ son normales. Existen grupos en los que sucede precisamente lo contrario:

Definición 1.14. Se dice que un grupo G es *simple* si sus únicos subgrupos normales son $\{e\}$ y el propio G. Es decir, G es simple si no tiene subgrupos normales propios.

Si H es un subgrupo de G de índice 2, entonces H es normal en G ($G/H = \{H, xH\}$ ya que $(G : H) = 2$, y por la misma razón $H\backslash G = \{H, Hx\}$; por lo tanto $xH = Hx$, $\forall x \in G$, pues $G = H \sqcup xH = H \sqcup Hx$ si $x \notin H$).

Si H es subgrupo normal de G, el conjunto cociente

$$G/H := \{xH \mid x \in G\}$$

adquiere estructura de grupo con la operación $(xH)(yH) := xyH$, cuyo elemento neutro es $eH = H$, y que la aplicación $\varphi_H \colon G \to G/H$ definida por $\varphi_H(x) = xH$ es homomorfismo de grupos al que llamaremos *homomorfismo canónico de paso al cociente módulo* H. El núcleo de φ_H es el grupo H, y es evidente la siguiente afirmación: H es subgrupo normal de G si, y solo si, existe un grupo L y un homomorfismo de grupos $f \colon G \to L$ cuyo núcleo es H.

Se recordará que una aplicación si $f \colon G \to L$ admite siempre una descomposición $f = f_3 \circ f_2 \circ f_1$

$$\begin{array}{ccc} G & \stackrel{f}{\to} & L \\ \downarrow f_1 & & \uparrow f_3 \\ G/\backsim_f & \stackrel{f_2}{\to} & f(G) \end{array},$$

(descomposición canónica) en donde $\backsim_f$ es la relación de equivalencia en G definida por $x \backsim_f y :\Leftrightarrow f(x) = f(y)$, y $G/\backsim_f$ denota, como es habitual, el conjunto cociente, es decir, aquél cuyos elementos son las clases de equivalencia de los de G para la relación $\backsim_f$; la aplicación f_2 es la biyección definida por $f_2\big([x]_{\backsim_f}\big) = f(x)$; y, finalmente, f_3 es la inclusión.

Supongamos ahora que $f\colon G \to L$ es un homomorfismo de grupos. Entonces, si $H = \mathrm{Ker}\,(f)$, resulta que $x \backsim_f y :\Leftrightarrow f(x) = f(y) \Leftrightarrow e_L = [f(x)]^{-1} * f(x) = [f(x)]^{-1} * f(y) = f(x^{-1}y) \Leftrightarrow x^{-1}y \in H \Leftrightarrow x_H \backsim y$, es decir que $\backsim_f = {}_H\backsim = \backsim_H$, ya que H es subgrupo normal de G. Por tanto, $G/\backsim_f = G/H$ y además $f_1\colon G \to G/H$ es el homomorfismo canónico de paso al cociente módulo H, pues $f_1(x) = [x]_{\backsim_f} = [x]_{{}_H\backsim} = xH = \varphi_H(x)$, cualquiera que sea $x \in G$. La biyección f_2 es ahora un isomorfismo de grupos pues es biyectiva y además

$$f_2\left((xH)(yH)\right) = f_2(xyH) = f(xy) = f(x) * f(y) = f_2(xH) * f_2(yH).$$

La inclusión f_3 es evidentemente homomorfismo. Así, los términos que intervienen en la factorización canónica de un homomorfismo de grupos son grupos y homomorfismos de grupos. Los Teoremas de isomorfía de grupos serán consecuencia de la existencia del isomorfismo f_2.

Observación 1.15. Si $f\colon G \to L$ es un homomorfismo de grupos y H es un subgrupo normal de G, entonces $f(H)$ es un subgrupo normal de $f(G)$. En efecto, $f(H)$ es subgrupo de $f(G)$ (1.10), y dados $f(x) \in f(G)$ y $f(h) \in f(H)$ se verifica que $f(x)f(h)\,[f(x)]^{-1} = f(xhx^{-1}) \in f(H)$.

También, si K es un subgrupo normal de L, $f^{-1}(K)$ es subgrupo normal de G ya que $f^{-1}(K)$ es subgrupo de G (1.10), y si $x \in G$ e $y \in f^{-1}(K)$, entonces $f(y) \in K$ y $f(x)f(y)\,[f(x)]^{-1} = f(xhx^{-1}) \in K$ de lo que se sigue que $xhx^{-1} \in f^{-1}(K)$.

Teorema 1.16. *Sea G un grupo y H, K subgrupos normales de G tales que $H \subset K$. Entonces se verifica que:*

i) K/H es subgrupo normal de G/H.

ii) $(G/H)\,/\,(K/H) \simeq G/K$.

Demostración. i) $K/H = \varphi_H(K)$ donde $\varphi_H\colon G \to G/H$ es el homomorfismo canónico (que es sobreyectivo) y se aplica (1.15) para obtener el resultado buscado.

ii) Existe un homomorfismo sobreyectivo $f\colon G/H \to G/K$ que está definido me-

diante $f(xH) = xK$, para cada $x \in G$. Ahora

$$\begin{aligned}\mathrm{Ker}(f) &= \{xH \in G/H \mid f(xH) = K\} = \{xH \in G/H \mid xK = K\} \\ &= \{xH \in G/H \mid x \in K\} = K/H,\end{aligned}$$

y la descomposición canónica de f proporciona el isomorfismo anunciado ya que f es sobreyectiva. □

Definición 1.17. Si G es un grupo y H un subgrupo de G, se define el subgrupo *normalizador* de H en G como

$$N_G(H) := \{x \in G \mid xH = Hx\},$$

y $N_G(H)$ es el mayor subgrupo de G en el que H es normal.

Es fácil comprobar que $N_G(H)$ es un subgrupo de G que contiene a H ya que:
$x, y \in N_G(H) \Rightarrow x^{-1}, y \in N_G(H) \Rightarrow x^{-1}yH = x^{-1}Hy = Hx^{-1}y$; además $hH = Hh = H$ para todo $h \in H$.

Teorema 1.18. *Si G es un grupo y H, K son subgrupos de G tales que $K \subset N_G(H)$, entonces*

i) $HK := \{xy \mid x \in H, y \in K\}$ es un subgrupo de G en el que H es normal.

ii) $H \cap K$ es subgrupo normal de K y existe un isomorfismo

$$HK/H \simeq K/H \cap K.$$

Demostración. i) Es evidente que $H \subset KH$. Ahora, para $x_1, x_2 \in H$ e $y_1, y_2 \in K$ se tiene $(x_1y_1)^{-1}\, x_2y_2 = y_1^{-1}x_1^{-1}x_2y_2 = x_3y_1^{-1}y_2$ (para un cierto $x_3 \in H$, pues $y_1^{-1}H = Hy_1^{-1}$ al ser $y_1^{-1} \in K \subset N_G(H)$). Por tanto, $(x_1y_1)^{-1}\, x_2y_2 \in HK$ y así HK es subgrupo de G.

Además dado que $H, K \subset N_G(H)$ resulta, de modo evidente, $HK \subset N_G(H)$.

ii) Para $x \in H \cap K$ y $k \in K$ se tiene $kxk^{-1} \in H \cap K$, pues H es normal en $N_G(H)$. Para la obtención del isomorfismo anunciado sea

$$f\colon K \xrightarrow{i} HK \xrightarrow{\varphi_H} HK/H,$$

donde i es la inclusión y φ_H el homomorfismo canónico de paso al cociente. El homomorfismo f está entonces definido por $f(k) = kH$ y, para cualquier $xyH \in HK/H$ (con $x \in H$ e $y \in K$), se tiene $xyH = yH$ (pues dado que $K \subset N_G(H)$, resulta la existencia de un $x' \in H$ tal que $xy = yx'$ y, así, $xyH = yx'H = yH$). Por lo tanto, f es sobreyectivo y además $\mathrm{Ker}(f) = H \cap K$ ($f(k) = kH = H$ con $k \in K \Leftrightarrow k \in H \cap K$). De la descomposición canónica de f resulta el isomorfismo buscado. □

Para $H = r\mathbb{Z} \subset \mathbb{Z}$, el grupo cociente $\mathbb{Z}/r\mathbb{Z}$ es el de las clases de restos de enteros módulo r. Es buen ejercicio comprobar que si r y s son enteros, d es su máximo común divisor y m su mínimo común múltiplo, entonces $r\mathbb{Z} \cap s\mathbb{Z} = m\mathbb{Z}$ y $r\mathbb{Z} + s\mathbb{Z} = d\mathbb{Z}$. Por aplicación del segundo Teorema de isomorfía se obtiene

$$d\mathbb{Z}/s\mathbb{Z} = (r\mathbb{Z}+s\mathbb{Z})/s\mathbb{Z} \simeq r\mathbb{Z}/(r\mathbb{Z}\cap s\mathbb{Z}) = r\mathbb{Z}/m\mathbb{Z}.$$

Teorema 1.19. *(Teorema de la correspondencia)*

Sean G un grupo y H un subgrupo normal de G. Existe una biyección que conserva las inclusiones entre el retículo de subgrupos (subgrupos normales) de G/H y el de subgrupos (subgrupos normales) de G que contienen a H.

Demostración. Sean $\mathfrak{S} = \{K' \mid K' \text{ es un subgrupo de } G/H\}$ y $\mathfrak{T} = \{K \mid K \text{ es subgrupo de } G \text{ que contiene a } H\}$. Si $\varphi_H : G \to G/H$ designa el homomorfismo canónico de paso al cociente, la aplicación $\Theta : \mathfrak{S} \to \mathfrak{T}$ definida por $\Theta(K') = \varphi_H^{-1}(K')$ (1.10) tiene por inversa a la aplicación $\Phi : \mathfrak{T} \to \mathfrak{S}$ dada por $\Phi(K) = \varphi_H(K)$ (1.10). Como consecuencia de (1.15) se obtiene que K' es subgrupo normal de G/H si, y solo si, $\Theta(K')$ es subgrupo normal de G que contiene a H. □

Si $(G_i)_{i\in I}$ es una familia de grupos, es muy fácil comprobar que el producto cartesiano $\prod_{i\in I} G_i$ es un grupo con la operación $(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i y_i)_{i\in I}$, definida componente a componente.

Para cada $j \in I$, la proyección $\pi_j : \prod_{i\in I} G_i \to G_j$, $\pi_j((x_i)_{i\in I}) = x_j$, es un homomorfismo sobreyectivo de grupos. Se satisface además la siguiente propiedad universal:

Proposición 1.20. *Si H es un grupo y para cada $i \in I$ está definido un homomorfismo de grupos $f_i : H \to G_i$, existe un único homomorfismo de grupos $f : H \to \prod_{i\in I} G_i$ tal que $\pi_j \circ f = f_j$, para cada $j \in J$.*

Demostración. La única aplicación $f\colon H \to \prod_{i\in I} G_i$ que satisface la condición $\pi_j \circ f = f_j$ para cada $j \in J$, está definida por la fórmula $f(h) = (f_i(h))_{i\in I}$, y es muy fácil comprobar que f es homomorfismo de grupos. □

Definición 1.21. El grupo $\prod_{i\in I} G_i$ será llamado *grupo producto directo de la familia de grupos* $(G_i)_{i\in I}$ y los homomorfismos $\pi_j\colon \prod_{i\in I} G_i \to G_j$ recibirán el nombre de *proyecciones canónicas.*

1.2. Grupos finitos. Teoremas de Sylow

El conocimiento de la estructura de un grupo pasa por el estudio del retículo de sus subgrupos y, para un grupo finito, una cuestión fundamental consiste en averiguar el número de subgrupos de un cierto orden. Las técnicas necesarias para iniciar este estudio comenzarán con el

Teorema 1.22. *(Teorema de Lagrange)*

Si G es un grupo finito y H es un subgrupo de G, entonces el orden de H divide al orden de G. Además

$$\#G = \#H(G : H),$$

en donde $(G : H)$ indica el índice de H en G, es decir, el número de clases de equivalencia de H en G.

Demostración. Es el contenido de la observación 1.7. □

Corolario 1.23. *Si K y H son subgrupos de G y además $K \subset H$, entonces*

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

Demostración. La expresión que se obtiene fácilmente mediante la aplicación del Teorema de Lagrange a los pares de grupos $K \subset H$, $H \subset G$ y $K \subset G$. □

Como caso particular, si r y s son enteros, $m = m.c.m(r, s)$ y $d = m.c.d(r, s)$, del isomorfismo $d\mathbb{Z}/s\mathbb{Z} \simeq r\mathbb{Z}/m\mathbb{Z}$ ya mencionado antes, se obtiene el conocido resultado $md = rs$. En efecto, por aplicación del anterior corolario a las inclusiones

$$s\mathbb{Z} \subset d\mathbb{Z} \subset \mathbb{Z} \quad \text{y} \quad m\mathbb{Z} \subset r\mathbb{Z} \subset \mathbb{Z},$$

resulta $(\mathbb{Z} : s\mathbb{Z}) = (\mathbb{Z} : d\mathbb{Z})(d\mathbb{Z} : s\mathbb{Z})$ y $(\mathbb{Z} : m\mathbb{Z}) = (\mathbb{Z} : r\mathbb{Z})(r\mathbb{Z} : m\mathbb{Z})$ y entonces

$$\frac{m}{r} = (r\mathbb{Z} : m\mathbb{Z}) = \#\left(r\mathbb{Z}/m\mathbb{Z}\right) = \#\left(d\mathbb{Z}/s\mathbb{Z}\right) = (d\mathbb{Z} : s\mathbb{Z}) = \frac{s}{d}.$$

Si G es un grupo y $x \in G$ consideraremos frecuentemente el homomorfismo de grupos $\varphi_x \colon \mathbb{Z} \to G$ definido por $\varphi_x(n) = x^n$. La imagen $\varphi_x(\mathbb{Z}) = \langle x \rangle$ es el subgrupo de G generado por x.

Definición 1.24. El grupo G es *cíclico* si existe un $x \in G$ tal que $\langle x \rangle = G$. El elemento x se dirá que es generador del grupo G.

El núcleo de φ_x es un subgrupo de $\mathbb{Z}$ y, por lo tanto, $\mathrm{Ker}\,(\varphi_x) = n\mathbb{Z}$ para algún $n \in \mathbb{Z}$. Entonces

$$\langle x \rangle = \varphi_x(\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$$

y, por lo tanto, todo grupo cíclico es isomorfo a algún $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ (con $n \neq 0$ en el caso finito) o a $\mathbb{Z}$ (que corresponde al caso $n = 0$).

Definición 1.25. El entero $n = \#\langle x \rangle$ recibe los nombres de *orden* o *período* de x y se denotará con $n = |x|$. Obsérvese que el período de x es también el menor entero positivo n tal que $x^n = e$; cada entero m tal que $x^m = e$ es un elemento de $\mathrm{Ker}(\varphi_x)$ y, por lo tanto, es múltiplo de $|x|$.

Una aplicación inmediata del Teorema de Lagrange proporciona:

Proposición 1.26. *Todo grupo finito de orden primo es cíclico y cada elemento diferente del neutro es un generador del grupo.*

Proposición 1.27. *Todo subgrupo y todo grupo cociente de un grupo cíclico son cíclicos.*

Demostración. Si $S \subset G$ es un conjunto generador de G, es decir, si todo elemento x de G es un producto finito de elementos del conjunto $S \cup S^{-1}$, y si $f \colon G \to G'$ es un homomorfismo de grupos, es evidente que todo elemento de $f(G)$ es un producto finito de elementos de $f(S) \cup f(S)^{-1}$. Así, la imagen mediante un homomorfismo de un sistema de generadores es un sistema de generadores de la imagen. En particular, es grupo cíclico la imagen de un grupo cíclico mediante un homomorfismo. También, si H es un subgrupo de G y si $G = \langle x \rangle = \varphi_x(\mathbb{Z})$, entonces $H = \varphi_x\left(\varphi_x^{-1}(H)\right)$ es un grupo cíclico ya que lo es $\varphi_x^{-1}(H)$ al ser subgrupo de $\mathbb{Z}$. □

Proposición 1.28. *Si $G = \langle x \rangle$ es un grupo cíclico de orden n, un elemento $y = x^r \in G$ $(1 < r < n)$ es generador de G si, y solo si, r es primo con n.*

Demostración. En efecto, r y n son coprimos si, y solo si, existen $t, q \in \mathbb{Z}$ tales que $1 = tr + qn$. Entonces $x = x^{tr+qn} = (x^r)^t = y^t$ si r y n son primos entre sí, y en ese caso se tiene $\langle x \rangle \subset \langle y \rangle \subset \langle x \rangle$. Recíprocamente, si $\langle y \rangle = \langle x \rangle$ se tiene $x = y^t$ para algún entero t, y entonces $x = x^{rt}$ con lo que resulta $x^{1-rt} = e$, es decir, $1 - rt \in \mathrm{Ker}\,(\varphi_x) = n\mathbb{Z}$. Por lo tanto, r y n son coprimos si $y = x^r$ genera $\langle x \rangle$. □

Proposición 1.29. *Si G y H son grupos finitos, $\#G = n$ y $\#H = m$, entonces el producto directo $G \times H$ es cíclico si, y solo si, G y H son cíclicos y n y m son primos entre sí.*

Demostración. En efecto, si (a, b) es generador del grupo $G \times H$ entonces a es generador de G y b lo es de H (1.27). Como $|(a, b)| = mcm(|a|, |b|) = |a|\,|b|$, necesariamente $n = |a|$ y $m = |b|$ son primos entre sí. Recíprocamente, si $\langle a \rangle = G$ y $\langle b \rangle = H$, el orden $|(a, b)| = mcm(|a|, |b|) = |a|\,|b|$, al ser $|a|$ y $|b|$ primos entre sí, y por lo tanto $G \times H = \langle (a, b) \rangle$ □

Proposición 1.30. *Si $G = \langle x \rangle$ es cíclico de orden n y d es divisor de n, entonces existe un único subgrupo de G de orden d.*

Demostración. Ciertamente, si $n = dr$ el elemento x^r es de período d y por tanto $\#\langle x^r \rangle = d$. Si H es subgrupo de G de orden d entonces H es cíclico (1.27) generado por algún $h = x^t \in H$ con $1 \leqslant t \leqslant n$. Como $\left|x^t\right| = d$ se tiene $x^{td} = e$, y entonces $td \in n\mathbb{Z}$. Pero $td = ns \Rightarrow t = rs$ con lo que $h = x^t = (x^r)^s$ y así resulta $H = \langle h \rangle \subset \langle x^r \rangle$. Por lo tanto $H = \langle x^r \rangle$, al ser ambos grupos del mismo orden d. □

Teorema 1.31. *(Teorema de Cauchy para grupos abelianos)*

Si G es un grupo abeliano finito de orden n y p es un número primo divisor de n, entonces G contiene un elemento de orden p o, equivalentemente, G tiene algún subgrupo de orden p.

Demostración. La prueba será realizada por inducción en $n = \#G$, siendo p divisor primo de n. El caso $n = p$ es trivial, pues por el Teorema de Lagrange, G es necesariamente cíclico y cualquier elemento (diferente del elemento neutro) es un generador de G. Sea $n > p$ y supóngase que el Teorema es válido para todos los grupos abelianos de orden $t < n$, con $p \mid t$.

Si $a \in G \setminus \{e\}$, entonces $m = |a| > 1$ y, por el Teorema de Lagrange, $m \mid n$, es decir, existe $r \in \mathbb{Z}$ tal que $n = mr$. Como p es divisor primo de n, entonces $p \mid m$ o $p \mid r$.

Si $m = kp$, entonces $b = a^k \in G$ tiene período p y el resultado estaría probado en ese caso.

Si $p \mid r$ considérese el grupo $G' = G/\langle a\rangle$ de orden $r < n$. Por inducción, existe un elemento $\overline{b} = b\langle a\rangle \in G'$ de período p. Si s es el período de $b \in G$ se tiene que $\overline{b}^s = b^s\langle a\rangle = e\langle a\rangle = \langle a\rangle$ y, por lo tanto, $p \mid s$. Como $s = |b|$ nos encontramos en el caso anterior, es decir, el elemento $c = b^{\frac{s}{p}} \in G$ es de período p. □

Corolario 1.32. *Si p es número primo, $r \geqslant 1$ un entero y p^r divide al orden del grupo finito abeliano G, entonces G tiene un subgrupo de orden p^r.*

Demostración. Por el Teorema de Cauchy anterior, G admite un subgrupo H de orden p y a partir de aquí se procede por inducción en r. Sea $r > 1$ y supóngase que los grupos finitos abelianos cuyo orden es divisible por p^{r-1} admiten un subgrupo de orden p^{r-1}. El grupo cociente G/H tiene orden $\dfrac{n}{p}$ y, por tanto, admite un subgrupo K' de orden p^{r-1}. Por el Teorema de la correspondencia existe un subgrupo K de G que contiene a H y tal que $K/H \simeq K'$. El Teorema de Lagrange permite afirmar ahora que K es de orden p^r. □

Corolario 1.33. *Si m es divisor del orden de un grupo finito abeliano G, entonces G admite un subgrupo de orden m.*

Demostración. Si $m = p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}$ es la factorización de m en potencias de primos y si H_i es subgrupo de G de orden $p_i^{r_i}$, entonces el subgrupo H_1H_2 es de orden $p_1^{r_1}p_2^{r_2}$. En efecto, H_1H_2 es subgrupo de G al ser G abeliano y $H_1H_2/H_2 \simeq H_1/H_1 \cap H_2$. Teniendo en cuenta que $H_1 \cap H_2 = \{e\}$, como son dos subgrupos de órdenes primos

entre sí, resulta $H_1H_2/H_2 \simeq H_1$, con lo cual se obtiene $\#(H_1H_2) = p_1^{r_1}p_2^{r_2}$, en virtud del Teorema de Lagrange. Con argumentación similar, usando recurrencia en j, resulta $\#(H_1H_2\cdots H_j) = p_1^{r_1}p_2^{r_2}\cdots p_j^{r_j}$, para cada $j = 1, 2, \ldots, t$. □

Observación 1.34. Obsérvese que tomando $m = n = \#G$ en la prueba del corolario anterior resulta el Teorema de estructura de los grupos abelianos finitos que, en esencia, afirma que $G = H_1H_2\cdots H_t$. El grupo $G = H_1H_2\cdots H_t$ es isomorfo al producto directo $H_1 \times H_2 \times \cdots \times H_t$, pues la aplicación $f\colon\ H_1 \times H_2 \times \cdots \times H_t \to H_1H_2\cdots H_t$ definida por $f(x_1, x_2, \ldots, x_t) = x_1x_2\cdots x_t$ es un homomorfismo (G es abeliano) sobreyectivo y, por tanto, isomorfismo al ser ambos grupos finitos del mismo orden. La unicidad de los subgrupos $H_1, H_2, \ldots, H_t$ puede ser obtenida como consecuencia de consideraciones posteriores (1.51).

Si G es un grupo no abeliano, la condición $d \mid \#G$ no es suficiente, en general, para que exista un subgrupo de G de orden d. Por ejemplo el grupo alternado A_5 tiene orden 60 pero no tiene ningún subgrupo de orden 30 pues cualquier tal subgrupo debería ser normal en A_5 al tener índice 2, lo cual es imposible ya que el grupo A_5 es simple (véase el ejercicio 28 de este capítulo). No obstante un resultado análogo al Teorema de Cauchy, pero para grupos finitos no necesariamente conmutativos, puede ser probado utilizando la teoría de G-conjuntos.

Definición 1.35. Una acción u operación (por la izquierda) de un grupo G sobre un conjunto A es cualquier aplicación

$$\begin{aligned} *\colon G \times A &\to A \\ (g, a) &\mapsto g * a \end{aligned}$$

que satisfaga las condiciones:

1) $(gg') * a = g * (g' * a)$, $\forall g, g' \in G$ y $\forall a \in A$

2) $e * a = a$, $\forall a \in A$.

También se dirá que A es un G-conjunto por la izquierda.

De modo análogo se define acción por la derecha $*\colon A \times G \to A, (a, g) \mapsto a * g$, con las obvias propiedades análogas a las 1) y 2) anteriores. En lo sucesivo, salvo mención expresa de otra cosa, G-conjunto será sinónimo de G-conjunto por la izquierda.

Observación 1.36. A es un *G-conjunto* si, y solo si, existe un homomorfismo de grupos $G \to S_A$, en donde S_A denota el grupo de permutaciones de A. En efecto, para la acción $*$ de G sobre A se define la aplicación $T_*\colon G \to S_A$ mediante $T_*(g)(a) := g * a$, pues para cada $g \in G$, la aplicación $T_*(g)\colon A \to A$ es biyectiva con inversa $T_*(g^{-1})$, y se comprueba fácilmente que T_* es homomorfismo de grupos como consecuencia de las propiedades 1) y 2) de la anterior definición. Recíprocamente, es fácil comprobar que si $T\colon G \to S_A$ es un homomorfismo de grupos, la aplicación ${}^*{}_T\colon G \times A \to A$ definida por ${}^*{}_T(g, a) := T(g)(a)$ dota a A de estructura de G-conjunto. Es fácil también obtener que ${}^*{}_{T_*} = *$ y que $T_{*_T} = T$. Cada homomorfismo $T\colon G \to S_A$ se denomina también una *representación de G por un grupo de automorfismos de A* y, por tanto, para cada conjunto A, existen tantas de tales representaciones como acciones diferentes de G sobre A.

Ejemplos 1.37.

1.- Sea G un grupo y A un conjunto cualquiera. La aplicación $*\colon G \times A \to A$ definida por $g * a = a$, $\forall a \in A$ y $\forall g \in G$ es una acción de G sobre A que se denomina *acción trivial.*

2.- La acción de un grupo G sobre sí mismo $*\colon G \times G \to G$ definida por $g * g' := gg'$ se denomina *traslación por la izquierda* y se dice entonces que G actúa por la izquierda sobre sí mismo por *traslación.*

3.- Otra acción $*\colon G \times G \to G$ de cualquier grupo G sobre sí mismo, que tendrá especial interés en lo que sigue, es la *conjugación,* definida mediante $g * a := gag^{-1}$.

4.- Si G es un grupo y H un subgrupo de G entonces G actúa por la izquierda (derecha) sobre el conjunto de las clases $G/H := \{gH \mid g \in G\}$, $(H\backslash G := \{Hg \mid g \in G\})$ mediante $g * (g'H) := gg'H$ $((Hg') * g := Hg'g)$. Esta acción recibe también el nombre de *traslación* por la izquierda (derecha).

5.- Si G es un grupo y designamos con $\mathfrak{S}_G$ el conjunto de subgrupos de G, entonces la aplicación $*\colon G \times \mathfrak{S}_G \to \mathfrak{S}_G$, dada por $g * H := gHg^{-1}$, está bien definida y constituye una acción (por la izquierda) de G sobre $\mathfrak{S}_G$. En efecto, si H es subgrupo de G también lo es el subconjunto gHg^{-1}, pues para $x = ghg^{-1}$ e $y = gkg^{-1}$, con $h, k \in H$ y

$g \in G$, resulta $xy^{-1} = ghg^{-1}\left(gkg^{-1}\right)^{-1} = ghg^{-1}gk^{-1}g^{-1} = ghk^{-1}g^{-1} \in gHg^{-1}$ pues $hk^{-1} \in H$ ya que H es subgrupo de G. Además las condiciones 1) y 2) de la definición anterior se satisfacen como consecuencia de las igualdades: $gg' * H = (gg')\,H\,(gg')^{-1} = gg'Hg'^{-1}g^{-1} = g\left(g'Hg'^{-1}\right)g^{-1} = g * (g' * H)$ y $e * H = eHe^{-1} = H$.

Usaremos el ejemplo 2 anterior para la prueba del

Teorema 1.38. *(Teorema de Cayley)*

Todo grupo G es isomorfo a un subgrupo del grupo S_G de sus permutaciones.

Demostración. La representación $T\colon G \to S_G$ definida por $T(a)(g) = ag$, correspondiente a la acción de traslación por la izquierda de G sobre sí mismo, (1.36), es un homomorfismo inyectivo. En efecto,

$a \in \operatorname{Ker} T \Leftrightarrow T(a) = id_G\colon G \to G \Leftrightarrow T(a)(g) = ag = g, \forall g \in G \Leftrightarrow a = e$.

Por lo tanto T_* establece así un isomorfismo de G con $T(G)$. □

Según este resultado, para conocer la estructura de todos los grupos finitos sería suficiente con estudiar el retículo de subgrupos de los grupos de permutaciones. Sin embargo esto no constituye ninguna ventaja en la práctica pues el orden del grupo de permutaciones es el factorial del orden del grupo objeto de estudio y ello supone, en general, una mayor dificultad a la hora de establecer la naturaleza del retículo de sus subgrupos. Por ello es necesario desarrollar técnicas y herramientas algo más sofisticadas.

Proposición 1.39. *Sean G un grupo finito y H un subgrupo cuyo índice en G es el menor número primo p que divide al orden de G. Entonces H es normal en G.*

Demostración. Como el conjunto de las clases por la izquierda G/H tiene $p = (G : H)$ elementos, su grupo de permutaciones es S_p cuyo orden es $p!$. La acción de traslación de G por la izquierda sobre G/H (ejemplo 4 anterior) determina un homomorfismo de grupos $T\colon G \to S_p$, (1.36), cuyo núcleo deberá tener a un divisor de $p!$ como índice en G, ya que $G/\operatorname{Ker} T \simeq \operatorname{Im} T$ que es subgrupo de S_p. Además, $xH = H$, $x \in H$ si x es un elemento de $\operatorname{Ker} T$. Entonces

$$(G : H)\,(H : \operatorname{Ker} T) = (G : \operatorname{Ker} T)\,,$$

y así $p\,(H : \operatorname{Ker} T)$ es divisor de $p!$, lo cual significa que $(H : \operatorname{Ker} T)$ es divisor de $(p-1)!$. Por lo tanto, o bien $(H : \operatorname{Ker} T) = 1$, en cuyo caso $H = \operatorname{Ker} T$ ya sería subgrupo normal de G, o bien cada divisor primo q de $(H : \operatorname{Ker} T)$ será también divisor de $(p-1)!$ por lo cual $q < p$. Estos divisores primos de $(H : \operatorname{Ker} T)$ lo son también del orden de G y ello contradice la hipótesis de minimalidad de p entre tales divisores. En conclusión, necesariamente se tiene $(H : \operatorname{Ker} T) = 1$, es decir, $H = \operatorname{Ker} T$. □

El concepto de *órbita* será muy utilizado en lo que sigue.

Definición 1.40. Sea $*\colon G \times A \to A$ una acción del grupo G sobre el conjunto A y sea $a \in A$. Se denominará *G-órbita* de a (o simplemente *órbita* de a si la referencia a G es innecesaria) al conjunto

$$\mathfrak{O}_G(a) := \{x * a \in A \mid x \in G\}.$$

También se define el *subgrupo de isotropía* (o *estabilizador*) de $a \in A$ mediante

$$G_a := \{x \in G \mid x * a = a\}$$

que es efectivamente un subgrupo de G.

Usaremos frecuentemente la siguiente Proposición.

Proposición 1.41. *Si A es un G-conjunto y $a \in A$ entonces*

$$\#\mathfrak{O}_G(a) = (G : G_a)\,.$$

Además la relación binaria en A definida por

$$a \sim b :\Leftrightarrow \exists x \in G \text{ tal que } b = x * a$$

es de equivalencia y establece una partición de A en clases de equivalencia que son precisamente las diferentes G-órbitas de elementos de A por la acción de G.

Demostración. Si $x, y \in G$ se tiene:

$$x * a = y * a \Leftrightarrow y^{-1}x * a = a \Leftrightarrow y^{-1}x \in G_a \Leftrightarrow xG_a = yG_a.$$

Por lo tanto, se puede afirmar que hay tantos elementos diferentes $y * a$ como clases distintas yG_a, lo que justifica la primera afirmación de la Proposición. Para probar la segunda bastará con demostrar que las órbitas constituyen una partición de A. Es evidente que cada elemento $a = e*a$ pertenece a su órbita, y por lo tanto $A = \cup_{a\in A}\mathfrak{O}_G(a)$. Además $\mathfrak{O}_G(a) \cap \mathfrak{O}_G(b) \neq \emptyset$ si, y solo si, existen $x, y \in G$ tales $x * a = y * b$, lo cual equivale, a su vez, a que exista un $z \in G$ tal que $a = z * b$ y, por ello, a que $a \in \mathfrak{O}_G(b)$ (y también que exista $z' \in G$ tal que $b = z' * a$, o sea $b \in \mathfrak{O}_G(a)$). Ahora bien

$$a \in \mathfrak{O}_G(b) \Leftrightarrow \mathfrak{O}_G(a) \subset \mathfrak{O}_G(b),$$

ya que $x * a = x * (z * b) = xz * b \in \mathfrak{O}_G(b)$, si $a = z * b \in \mathfrak{O}_G(b)$. Entonces se tiene

$$\mathfrak{O}_G(a) \cap \mathfrak{O}_G(b) \neq \emptyset \Leftrightarrow \mathfrak{O}_G(a) = \mathfrak{O}_G(b).$$

es decir, A es la unión disjunta de las diferentes ó rbitas de sus elementos. □

En el ejemplo 5 anterior, si H es un subgrupo de G, el grupo de isotropía de H es $G_H = \{a \in G \mid aHa^{-1} = H\}$ que es el subgrupo normalizador de H, es decir, el mayor subgrupo de G en el que H es normal (1.17). Por lo tanto, a la vista de la Proposición 1.41, $\#\mathfrak{O}_G(H) = (G : G_H) = 1$ si, y solamente si, H es normal en G.

La acción de G sobre sí mismo por conjugación (ejemplo 3 anterior) proporcionará una fórmula muy útil en relación con el orden de un grupo finito G. Para la acción

$$\begin{aligned} *\colon G \times G &\to G \\ (x, a) &\mapsto x * a := xax^{-1}, \end{aligned}$$

el grupo de isotropía de un elemento $a \in G$ es

$$G_a = \{x \in G \mid xax^{-1} = a\} = \{x \in G \mid xa = ax\}$$

que se denomina también el *normalizador* de $\{a\}$ en G. Nótese que las órbitas no son vacías ($a \in \mathfrak{O}_G(a)$, $\forall a \in G$) y que una órbita $\mathfrak{O}_G(a)$ contiene solamente un elemento precisamente si $\mathfrak{O}_G(a) = \{a\}$, es decir, si, y solo si, $x * a = xax^{-1} = a$, $\forall x \in G$. Por lo tanto

$$\mathfrak{O}_G(a) = \{a\} \Leftrightarrow a \in Z_G.$$

Cada órbita $\mathfrak{O}_G(a)$ se denominará *clase de conjugación* del elemento a y cualquier elemento de $\mathfrak{O}_G(a)$ será un representante de la clase de conjugación de a.

Se ha probado así la siguiente Proposición que establece la que conoceremos desde ahora como *fórmula de las clases* para el orden de un grupo finito.

Proposición 1.42. *Si G es un grupo finito entonces*

$$\#G = \#Z_G + \sum_{i=1}^{r} (G : G_{a_i}),$$

donde $\{a_1, \ldots, a_r\}$ es un conjunto de representantes de las diferentes clases de conjugación que tienen más de un elemento.

Corolario 1.43. *Si p es un número primo y G es un grupo de orden p^n para algún $n \geqslant 1$, entonces $p \mid \#Z_G$ y $\#Z_G \neq p^{n-1}$.*

Demostración. En la fórmula de las clases, los sumandos correspondientes a representantes de clases de conjugación que tienen más de un elemento son todos divisores de p^n y por tanto múltiplos de p. Como $\#G = p^n$ resulta $p \mid \#Z_G$, que constituye la primera afirmación del corolario. Para obtener la segunda, si $\#Z_G = p^{n-1}$ sea $a \in G \setminus Z_G$. Entonces $Z_G \subsetneqq G_a \subsetneqq G$, ya que, por la selección que hemos hecho de a, existe un $g \in G$ tal que $ag \neq ga$ lo que proporciona $g \in G \setminus G_a$ y $a \in G_a \setminus Z_G$. Ello es imposible pues, por el Teorema de Lagrange, el orden de G_a, que ahora es estrictamente mayor que $p^{n-1} = \#Z_G$, deberá ser una potencia de p (al ser divisor de p^n) estrictamente menor que p^n. □

Corolario 1.44. *Si p es número primo todo grupo de orden p^2 es abeliano.*

Podemos proceder ahora a la prueba de la anunciada generalización, para grupos no abelianos, del Teorema de Cauchy.

Teorema 1.45. *Sea G un grupo finito y p un número primo. Si p^m divide al orden de G, entonces existe un subgrupo de G de orden p^m.*

Demostración. Sea $n = \#G$, que es divisible por p^m, y procedamos inductivamente en n. Para $n = 1$ el resultado es trivial. Sea $n > 1$ y supóngase válido el resultado para todos los grupos de orden menor que n.

Distingamos las dos posibilidades: $p \mid \#Z_G$ y $p \nmid \#Z_G$.

En el primer caso el Teorema de Cauchy para grupos abelianos proporciona la existencia de un subgrupo H de Z_G que es de orden p y es normal en G por ser subgrupo de

Z_G.El grupo cociente G/H es de orden $\frac{n}{p} < n$ y, por inducción, admitirá un subgrupo K' de orden p^{m-1}. El Teorema de la correspondencia proporciona ahora un subgrupo K de G que contiene a H tal que $K/H \simeq K'$. Por lo tanto $\#K = p^m$ y el resultado estaría probado en este caso.

Si, por el contrario, $p \nmid \#Z_G$, por la fórmula de las clases debe de existir un elemento $a \in G$ con $(G : G_a)$ no divisible por p . Para este elemento a se tiene $G_a \subsetneq G$ (inclusión estricta ya que $(G : G_a) > 1$) y, por el Teorema de Lagrange, $\#G = \#G_a\,(G : G_a)$, lo que significa que p^m es divisor del orden de G_a que es estrictamente menor que el de G. La hipótesis de inducción proporciona ya un subgrupo de G_a de orden p^m. □

Definición 1.46. Sean G un grupo finito y p un número primo.

1) Se dirá que G es un *p-grupo* si el orden de G es una potencia de p.

2) Si H es un subgrupo de G de orden una potencia de p se dirá que H es un p-subgrupo de G. Si p^m es la mayor potencia de p que divide al orden de G y si H es un subgrupo de G que tiene orden p^m se dirá que H es un p-subgrupo de Sylow de G. Es decir, los p-subgrupos de Sylow de G son los p-subgrupos de G de orden mayor posible.

Observación 1.47. Si H es p-subgrupo de Sylow de G entonces lo son también todos sus conjugados xHx^{-1} $(x \in G)$ y, por lo tanto, G actúa por conjugación en el conjunto de sus p-subgrupos de Sylow, para cada primo p que divide al orden de G. En conclusión, G tiene un único p-subgrupo de Sylow H si, y solo si, H es p-subgrupo de Sylow normal en G.

Proposición 1.48. *Si p es un número primo y G es un p-grupo de orden p^r existe entonces una cadena de subgrupos*

$$G_0 = \{e\} \subset G_1 \subset \cdots \subset G_r = G,$$

de tal modo que cada G_i es subgrupo normal de G_{i+1} y G_i/G_{i-1} es cíclico de orden p, para todo $i = 1, \ldots, r$.

Demostración. Es consecuencia del Teorema anterior ya que basta tomar G_{r-1} un subgrupo de G de orden p^{r-1} y, recurrentemente, G_i subgrupo de G_{i+1} de orden p^i para

$i = 0, 1, \ldots, r-1$. Por el Teorema de Lagrange el índice $(G_i + 1 : G_i) = p$, que es el menor número primo que divide al orden de G_{i+1} y, por (1.39), G_i es normal en G_{i+1}. Todos los cocientes G_{i+1}/G_i son grupos de orden primo y por ello cíclicos. □

La Proposición anterior establece que todo p-grupo es resoluble, concepto que será definido en la próxima sección.

Teorema 1.49. *(Teorema de Sylow)*

Sea p un número primo y G un grupo finito de orden $n = p^m r$, con r no divisible por p. Entonces:

a) Existen p-subgrupos de Sylow de G.

b) Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow de G.

c) Todos los p-subgrupos de Sylow de G son conjugados .

d) El número, s_p, de p-subgrupos de Sylow de G es divisor de r y, por tanto, del orden de G. Además s_p es congruente con 1 módulo p ($s_p \equiv 1 (mód\ p)$), es decir, $s_p = 1 + kp$ para algún entero k.

Demostración. Del Teorema anterior se sigue a) si allí se toma p^m como la mayor potencia de p que divide al orden de G.

Para la demostración de las restantes afirmaciones sea

$$\mathfrak{P} := \{P \mid P \text{ es } p\text{-subgrupo de Sylow de } G\}.$$

Por la observación 1.47 se puede considerar que G actúa por conjugación en $\mathfrak{P}$. Sea $P \in \mathfrak{P}$ fijado arbitrariamente, su grupo de isotropía, $G_P = \{x \in G \mid xPx^{-1} = P\}$, resulta ser el normalizador de P en G. El orden de la G-órbita de P es el índice de G_P en G, es decir, $\#\mathfrak{O}_G(P) = (G : G_P)$ (1.41). Se tienen las inclusiones de grupos

$$\{e\} \subset P \subset G_P \subset G$$

y, por aplicación reiterada del Teorema de Lagrange, las igualdades

$$p^m r = \#G = \#G_P\,(G : G_P) = \#P\,(G_P : P)\,(G : G_P) = p^m\,(G_P : P)\,(G : G_P),$$

es decir,

$$(G_P : P)\,(G : G_P) = (G_P : P)\,\#\mathfrak{O}_G(P) = r,$$

de lo que se deduce que p no es divisor de $\#\mathfrak{O}_G(P)$ (en otro caso p dividiría a r), y además que $\#\mathfrak{O}_G(P)$ es divisor de r y también de $\#G$.

Para la prueba de b), sea H un p-subgrupo de G y sea $p^\alpha = \#H$ (obviamente $\alpha \leqslant m$). El subgrupo H actúa también por conjugación en la G-órbita de P

$$\begin{aligned} H \times \mathfrak{O}_G(P) &\to \mathfrak{O}_G(P) \\ (h, Q) &\mapsto hQh^{-1}, \end{aligned}$$

ya que si $Q = xPx^{-1}$, entonces $hQh^{-1} = h\left(xPx^{-1}\right)h^{-1} = (hx)\,P\,(hx)^{-1} \in \mathfrak{O}_G(P)$. Se tiene ahora que

$$\mathfrak{O}_G(P) = \mathfrak{O}_H(P_1) \sqcup \cdots \sqcup \mathfrak{O}_H(P_t),$$

en donde $\{P_1, \ldots, P_t\} \subset \mathfrak{O}_G(P)$ es un conjunto de representantes de las diferentes H-órbitas $\mathfrak{O}_H(P_i)$ de elementos de $\mathfrak{O}_G(P)$ y, por lo tanto,

$$\#\mathfrak{O}_G(P) = \sum_{i=1}^{t} \#\mathfrak{O}_H(P_i) = \sum_{i=1}^{t} (H : H_{P_i}), \quad (*)$$

donde $H_{P_i} = \{h \in H \mid hP_ih^{-1} = P_i\}$ denota el grupo de isotropía de P_i para la acción de H.

Por el Teorema de Lagrange $\#H = \#H_{P_i}\,(H : H_{Pi})$ y $\#H = p^\alpha$, es decir,

$$(H : H_{Pi}) = p^{\beta_i}, \qquad (**)$$

con $\beta_i \leqslant \alpha$, para cada $i = 1, \ldots, t$. Puesto que $p \nmid \#\mathfrak{O}_G(P)$, de $(*)$ y $(**)$ se deduce que existe algún sumando en $(*)$ no divisible por p, o sea, $\exists i \in \{1, \ldots, t\}$ tal que $\beta_i = 0$ o, lo que es lo mismo, tal que $H = H_{P_i}$. Obviamente H_{P_i} es un subgrupo de G_{P_i} (G_{P_i} es el normalizador en G del grupo P_i) y, por lo tanto, HP_i es subgrupo de G y existe un isomorfismo de grupos (1.18)

$$HP_i/P_i \simeq H/H \cap P_i.$$

De esto se obtiene que

$$\#\,(HP_i) = \frac{\#H\#P_i}{\#(H \cap P_i)},$$

en virtud del Teorema de Lagrange, y de ello resulta que HP_i es un p-subgrupo de G al ser potencias de p todos los términos del segundo miembro de la igualdad anterior. Como $P_i \subset HP_i$, de la maximalidad del orden de P_i resulta $P_i = HP_i$, que admite a H como subgrupo y la afirmación b) queda probada.

La prueba de c) se puede obtener de lo ya demostrado. En efecto, si P y Q son dos p-subgrupos de Sylow de G hágase jugar a Q el papel que ha jugado H en la prueba de b); se encontrará un $P_i \in \mathfrak{O}_G(P)$ tal que $Q \subset P_i$ y, por lo tanto, $Q = P_i$ por ser ambos grupos finitos del mismo orden.

La demostración de d) es también consecuencia de lo ya dicho. Ahora sabemos que $\mathfrak{O}_G(P) = \mathfrak{P}$ para cualquier P (por el apartado b)). También se ha visto que $s_p = \#\mathfrak{P}$ es divisor de r. Haciendo $H = P$ en la prueba de b) se tiene

$$s_p = \sum_{i=1}^{t} (P : P_{P_i}),$$

en donde $\{P_1, \ldots, P_t\}$ es un conjunto de representantes de las P-órbitas $\mathfrak{O}_P(P_i)$ diferentes de elementos de $\mathfrak{P}$, y además existe algún sumando $(P : P_{Pi}) = p^{\beta_i}$ de valor 1, lo cual sucede solamente si $P = P_i$ (que corresponde al caso, $H = P \subset P_i$ de la prueba de b)). Por lo tanto, en la suma anterior solamente hay un sumando que vale 1 y los restantes son potencias de p, con lo que la afirmación d) queda demostrada. □

Observación 1.50. Ahora se puede afirmar:

$$s_p = 1 \Leftrightarrow \mathfrak{P} = \{P\} \Leftrightarrow P \text{ es subgrupo normal de } G.$$

Corolario 1.51. *(Teorema de estructura de grupos abelianos finitos)*

Si G es un grupo abeliano de orden $n = p_1^{r_1} \cdots p_t^{r_t}$, con $p_1, \ldots, p_t$ primos diferentes, entonces $G = H_1 \cdots H_t \simeq H_1 \times \cdots \times H_t$ en donde cada H_i es el único p_i-subgrupo de Sylow de G, para cada $i = 1, \ldots, t$.

Demostración. La existencia de los grupos H_i (para cada $i = 1, \ldots, t$) puede obtenerse como consecuencia inmediata del Teorema de Sylow anterior (aunque en el caso abeliano no es necesario recurrir a herramientas tan sofisticadas (véase (1.34)), y la unicidad se

sigue de la conmutatividad de G y de la observación 1.50. El resto de la prueba es el contenido de la observación 1.34. □

1.3. El grupo simétrico. Grupos resolubles

Uno de los resultados finales de estas notas y su principal objetivo lo constituye el Teorema de Galois sobre la resolubilidad por radicales de ecuaciones algebraicas. Este Teorema establece que dicha resolubilidad es posible para una tal ecuación si, y solo si, un cierto grupo asociado a la misma es un grupo resoluble. Por ello es importante dedicar nuestra atención al examen de algunos resultados básicos de la teoría de grupos resolubles. La no resolubilidad de los grupos de permutaciones S_n, si $n \geqslant 5$, será definitiva para la prueba del Teorema que afirma que la ecuación general de grado $n \geqslant 5$ no es resoluble por radicales.

Dedicaremos unas líneas a recordar las principales cuestiones y notaciones de la teoría de grupos de permutaciones. Recuérdese que si X es un conjunto, el grupo S_X de las permutaciones de X es el conjunto de las biyecciones X en X. La operación de S_X es la composición de aplicaciones.

Definición 1.52. Si $X = \{1, 2, \ldots, n\}$ es el conjunto de n elementos se designará con S_n el grupo de sus permutaciones, que recibe el nombre de *grupo simétrico* de n elementos.

S_n es un grupo de orden $n!$ y no es abeliano si $n \geqslant 3$ (comprobación muy sencilla). Si $\sigma \in S_n$ se escribirá

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Si un elemento $j \in \{1, 2, \ldots, n\}$ es fijo para σ, es decir, tal que $\sigma(j) = j$, el símbolo j será suprimido en la expresión anterior. Por ejemplo para $n = 5$ la permutación $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 5, \sigma(4) = 4$ y $\sigma(5) = 2$ se escribirá

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 5 \\ 3 & 1 & 5 & 2 \end{pmatrix}.$$

Con esta notación es fácil obtener que si $m \leqslant n$ entonces S_m se identifica con el subgrupo de aquellos $\sigma \in S_n$ que dejan fijos $n - m$ elementos determinados.

Definición 1.53. Si $\sigma \in S_n$ es tal que existen $a_1, \ldots, a_r \in \{1, \ldots, n\}$ de forma que $\sigma(a_i) = a_{i+1}$ para $i = 1, \ldots, r-1$, $\sigma(a_r) = a_1$, y $\forall j \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_r\}$ $\sigma(j) = j$, se dirá que σ es un r-ciclo y se escribirá

$$\sigma = (a_1\ a_2\ \ldots\ a_r).$$

Los 2-ciclos se denominan trasposiciones.

Obsérvese que si σ es un r-ciclo su período es r.

Definición 1.54. Dos permutaciones $\sigma, \tau \in S_n$ se dice que son disjuntas si, para cada $j \in \{1, \ldots, n\}$, $\sigma(j) \neq j \Rightarrow \tau(j) = j$ (o, lo que es equivalente, $\tau(j) \neq j \Rightarrow \sigma(j) = j$). Es muy fácil comprobar que permutaciones disjuntas conmutan.

Proposición 1.55. *Toda permutación $\sigma \in S_n$ es producto de ciclos disjuntos.*

Demostración. Tómese $k \in \{1, 2, \ldots, n\}$ y fórmese el conjunto $\{\sigma^i(k) \mid i \geqslant 0\}$. Se observará que, como nuestro conjunto $\{1, 2, \ldots, n\}$ es finito y σ es biyectiva, existe un entero $m \geqslant 0$ tal que $\sigma^m(k) = \sigma^i(k)$, para algún $0 \leqslant i < m$. Si r es el menor de tales enteros, necesariamente se tiene $\sigma^r(k) = k$, pues de la igualdad $\sigma^r(k) = \sigma^j(k)$, para algún $0 \leqslant j < r$, resultaría $\sigma^{r-j}(k) = k$, contradiciendo la minimalidad de r si $0 < j$. A continuación, para obtener la descomposición anunciada, comenzamos escribiendo

$$\sigma_1 = \begin{pmatrix} a & \sigma(a) & \ldots & \sigma^{r_1-1}(a) \\ \sigma(a) & \sigma^2(a) & \ldots & \sigma^{r_1}(a) = a \end{pmatrix} = \begin{pmatrix} a & \sigma(a) & \ldots & \sigma^{r_1-1}(a) \end{pmatrix},$$

que es un r_1-ciclo, donde a es el primer elemento, según el orden natural en $\{1, 2, \ldots, n\}$, que no es fijo para σ. Se procede a construir

$$\sigma_2 = \begin{pmatrix} b & \sigma(b) & \ldots & \sigma^{r_2-1}(b) \\ \sigma(b) & \sigma^2(b) & \ldots & \sigma^{r_2}(b) = b \end{pmatrix} = \begin{pmatrix} b & \sigma(b) & \ldots & \sigma^{r_2-1}(b) \end{pmatrix},$$

tomando b el primer elemento, según el orden mencionado, que no pertenezca al conjunto de elementos $\left\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{r_1-1}(a)\right\}$ y que no es fijo para σ. Recursivamente se construyen sucesivas $\sigma_3, \ldots, \sigma_t, \ldots$ donde

$$\sigma_t = \begin{pmatrix} k & \sigma(k) & \ldots & \sigma^{r_t-1}(k) \\ \sigma(k) & \sigma^2(k) & \ldots & \sigma^{r_t}(k) = k \end{pmatrix} = \begin{pmatrix} k & \sigma(k) & \ldots & \sigma^{r_t-1}(k) \end{pmatrix},$$

siendo k es el primer elemento de $\{1, 2, \ldots, n\}$, según el consabido orden natural, que no ha sido movido por ninguno de los ciclos ya construidos $\sigma_3, \ldots, \sigma_{t-1}$, y que no es fijo para σ. Los sucesivos conjuntos

$$\left\{a, \sigma(a), \ldots, \sigma^{r_1-1}(a)\right\}, \left\{b, \sigma(b), \ldots, \sigma^{r_2-1}(b)\right\}, \ldots, \left\{k, \sigma(k), \ldots, \sigma^{r_t-1}(k)\right\}, \ldots$$

son disjuntos y, por lo tanto, son disjuntos también cada uno de los pares de ciclos correspondientes. El proceso se detendrá cuando se hayan agotado los elementos de $\{1, 2, \ldots, n\}$ que no son fijos para σ. Es obvio que $\sigma = \sigma_l \cdots \sigma_2 \sigma_1$ donde σ_l es el último ciclo que es posible construir con el proceso anteriormente descrito. □

Observación 1.56. Cada ciclo es un producto de trasposiciones aunque no de modo único:

$$\begin{aligned}\sigma = (a_1\ a_2\ \ldots\ a_r) &= (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_3)(a_1\ a_2) \\ &= (a_1\ a_2)(a_2\ a_3) \cdots (a_{r-2}\ a_{r-1})(a_{r-1}\ a_r).\end{aligned}$$

Por lo tanto, cada permutación $\gamma \in S_n$ admite al menos una factorización en trasposiciones. El número de tales trasposiciones no está determinado de modo único pero sí lo está su paridad, tal y como se establece a continuación.

Proposición 1.57. *Si id es el elemento neutro de S_n y si $id = \tau_1 \tau_2 \cdots \tau_r$ es una descomposición de id como producto de trasposiciones, entonces r es par. Como consecuencia, la paridad del número de trasposiciones en que se puede descomponer una permutación $\sigma \in S_n$ está determinada por σ.*

Demostración. Si Λ designa un subconjunto arbitrario de $\{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$, para cada entero B de la forma $B = \prod_{(i,j)\in\Lambda} (j - i)$ y cada permutación $\sigma \in S_n$, se define $B^\sigma := \prod_{(i,j)\in\Lambda} (\sigma(j) - \sigma(i))$. Es fácil comprobar que $B^{\sigma\tau} = (B^\tau)^\sigma$. También $(-B)^\sigma = -B^\sigma$, cualquiera que sea $\sigma \in S_n$, pues la expresión $-B$ $(-B^\sigma)$ se puede obtener a partir de la de B (B^σ) modificando solo en el signo de uno de sus factores, por ejemplo el $k-r$ $(\sigma(k)-\sigma(r))$. La mayor dificultad de la prueba consiste en demostrar que si τ es una trasposición y $A = \prod_{1\leqslant i<j\leqslant n} (j-i)$, entonces $A^\tau = -A$. Para ello pongamos $\tau = (h\ k)$ (con $h < k$) y observemos cómo varían los factores de A con la actuación de τ para obtener A^τ:

a) Cada factor $j - i$, con $i \neq h$ y $j \neq k$, permanece en A^τ sin variación, es decir, los únicos factores $j-i$ que resultan afectados al calcular A^τ son de alguno de los siguientes tipos:

b) $i < h < k$, con $j = h$ o $j = k$ y entonces $\tau(h) - \tau(i) = k - i$ y $\tau(k) - \tau(i) = h - i$, produciéndose un cambio de posición de los factores $k - i$ y $h - i$

c) $h < k < j$, donde ahora $i = h$ o $i = k$, resultando $\tau(j) - \tau(h) = j - k$ y $\tau(j) - \tau(k) = j - h$, con lo que se reproduce lo obtenido en b).

d) $h < i < k = j$ con lo que el factor $i - h$ es cambiado en el factor $\tau(i) - \tau(h) = i - k$, pero también el factor $k - i$ es cambiado en el factor $\tau(k) - \tau(i) = h - i$, resultando así que se produce solamente un cambio de orden y la modificación del signo de dos factores. Estos cambios no afectan al valor del producto.

e) Finalmente, $i = h < j = k$, y entonces el factor $j - i$ de A se transforma en $\tau(j) - \tau(i) = i - j$.

Esto agota todas las posibilidades y significa que $A^\tau = -A$.

Por lo tanto, si $id = \tau_1 \cdots \tau_r$, se tiene que $A = A^{id} = A^{\tau_1 \cdots \tau_r} = (-A)^{\tau_1 \cdots \tau_{r-1}} = [(-1)A]^{\tau_1 \cdots \tau_{r-1}} = \cdots = (-1)^r A$ de lo que resulta que r es necesariamente par.

Ahora, si $\sigma = \tau_1 \cdots \tau_t = \varepsilon_1 \cdots \varepsilon_s$ son dos factorizaciones de $\sigma \in S_n$ en trasposiciones, resulta que $id = \tau_1 \cdots \tau_t \varepsilon_s \cdots \varepsilon_1$ con lo cual t y s son ambos pares o ambos impares ya que su suma ha de ser par. □

Definición 1.58. Se denomina *signatura* de la permutación σ al valor $\varepsilon(\sigma) = (-1)^k$, siendo k es el número de trasposiciones de una descomposición de σ (como consecuencia de la anterior Proposición la signatura está definida sin ambigüedad). Se designa con A_n el conjunto de permutaciones que se descomponen en un número par de trasposiciones (permutaciones *pares*). A_n es un subgrupo de índice 2 de S_n y recibe el nombre de *grupo alternado* de n elementos ($\sigma \in A_n \Leftrightarrow \varepsilon(\sigma) = 1$). Las $\sigma \in S_n \setminus A_n$ son las permutaciones *impares*.

A_n es el núcleo del homomorfismo $\varepsilon\colon S_n \to \{-1, 1\}$ que asocia a cada permutación su signatura ($\{-1, 1\}$ es subgrupo del grupo multiplicativo $\mathbb{R}^*$ de números reales no nulos).

Lema 1.59. *Sea p un número primo y $\sigma \in S_p$. Entonces $|\sigma| = p$ si, y solo si, σ es un p-ciclo.*

Demostración. Es evidente que si σ es un p-ciclo entonces $|\sigma| = p$. Recíprocamente, sea $\sigma \in S_p$ de período p y sea $\sigma = \sigma_1\sigma_2$ una factorización en permutaciones disjuntas (1.55), con $\sigma_1 = (a_1 a_2 \dots a_r)$ un $r-$ciclo y $\sigma_2 \in S_{p-r}$, con $1 < r \leqslant p$. Necesariamente se tiene $r = p$, ya que, en otro caso (es decir, si $1 < r < p$), se tendría $\sigma^r = \sigma_1^r\sigma_2^r = \sigma_2^r \in S_{p-r}$ al ser σ_1 y σ_2 disjuntas. Ello no es posible pues de $\sigma^r \in S_{p-r}$ se obtiene, por el Teorema de Lagrange, que $|\sigma^r| = p$ (σ^r tiene el mismo período p que σ por (1.28)) es un divisor primo de $(p-r)! = \#S_{p-r}$, lo que es falso si $r > 0$. Por lo tanto, $r = p$ y la permutación σ_2 es la identidad con lo que $\sigma = \sigma_1$ que es un p-ciclo. □

Nótese que la condición de que p es número primo es crucial en la afirmación anterior. En efecto, si $n = 12$ y $\sigma = \sigma_1\sigma_2$ con $\sigma_1 = (1\ 2\ 3)$ y $\sigma_2 = (4\ 5\ 6\ 7)$, resulta $|\sigma| = 3{\cdot}4 = 12$ y sin embargo σ no es un 12-ciclo. Más generalmente, si $n = pq$ con p y q primos diferentes, y si $\sigma = \sigma_1\sigma_2 \in S_n$ con σ_1 un p-ciclo y σ_2 un q-ciclo, σ_1 y σ_2 disjuntos, resulta que $|\sigma| = n$ y σ no es un n-ciclo (solamente actúa sobre $p + q$ elementos y $p + q < n = pq$).

Obsérvese también que si $\sigma \in S_n$ y $|\sigma| = p$ para un número primo p, entonces $\sigma \in S_p \subset S_n$ y, por lo tanto, σ es un p-ciclo.

Proposición 1.60. *Si p es un número primo y H es un subgrupo de S_p que contiene un p-ciclo y una trasposición, entonces $H = S_p$.*

Demostración. Si el p-ciclo es $\sigma = (a_1\ a_2\ \dots\ a_p) \in H$ y la trasposición es $\tau = (a_i\ a_j)$, poniendo

$$\rho = \begin{pmatrix} 1 & 2 & \dots & p \\ a_1 & a_2 & \dots & a_p \end{pmatrix}$$

resulta $\sigma' = \rho^{-1}\sigma\rho = (12\dots p) \in H' := \rho^{-1}H\rho$ y también $\tau' = \rho^{-1}\tau\rho = (i\ j) \in H'$. Ahora, $H' = S_p$ si, y solo si, $H = S_p$, pues los grupos H y H' tienen el mismo orden.

Como p es primo y $r = j - i < p$, entonces $\gamma = (\sigma')^r$ es también un p-ciclo (el Lema anterior permite afirmar que σ' es p-ciclo al tener período p y $\gamma \in H'$. Además $\gamma(i) = i + r = \tau'(i) = j$ y así se tiene $\gamma = (i\ \gamma(i)\ \gamma^2(i)\ \dots\ \gamma^{p-1}(i))$ y $\tau' = (i\ \gamma(i))$. De una nueva renumeración

$$\varsigma = \begin{pmatrix} 1 & 2 & \dots & p \\ i & \gamma(i) & \dots & \gamma^{p-1}(i) \end{pmatrix}$$

resulta que $\sigma'' = \varsigma^{-1}\gamma\varsigma = (1\ 2\ \ldots\ p)$ y $\tau'' = \varsigma^{-1}\tau'\varsigma = (1\ 2)$ son elementos del subgrupo $H'' = \varsigma^{-1}H'\varsigma$. También, $H' = S_p \Leftrightarrow H'' = S_p$, y todo lo dicho hasta aquí nos permite suponer que $\sigma = (1\ 2\ \ldots\ p)$ y que $\tau = (1\ 2)$.

Ahora $\sigma\tau\sigma^{-1} = (2\ 3)$, $\sigma(2\ 3)\sigma^{-1} = (3\ 4)$,..., $\sigma(p-2\ p-1)\sigma^{-1} = (p-1\ p)$ son elementos de H'' y, por lo tanto, $(i\ i+1) \in H''$, $\forall i \in \{1,\ldots,p-1\}$. Como $(i\ i+2) = (i\ i+1)(i+1\ i+2)(i\ i+1)$, para cada $i = 1,\ldots,p-2$, resulta, por recurrencia, que cada trasposición

$$(i\ i+s) = (i\ i+s-1)\,(i+s-1\ i+s)\,(i\ i+s-1)$$

es un elemento de H''. Como S_p está generado por las trasposiciones se tiene $H'' = S_p$. □

El concepto de grupo resoluble, que estudiamos a continuación, será esencial en la teoría de Galois de ecuaciones algebraicas.

Definición 1.61. Una cadena de subgrupos

$$G_r = \{e\} \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_0 = G$$

se dirá que es una cadena (o *torre*) *normal* si cada G_{i-1} es normal en G_i. El grupo G se dice que es *resoluble* si existe una torre normal como la anterior en la que cada grupo cociente G_{i-1}/G_i es abeliano. Una tal torre se llamará *abeliana* y se dirá también que es una torre de resolubilidad para G.

Ejemplos 1.62.

1.- Si G es abeliano, entonces G es resoluble; la consideración de la cadena $\{e\} \subset G$ es suficiente argumento.

2.- Todo p-grupo es un grupo resoluble (1.48).

3.- El grupo de las permutaciones de tres elementos S_3 es resoluble. La cadena

$$\{e\} \subset A_3 = \langle(1\ 2\ 3)\rangle \subset S_3$$

proporciona la resolubilidad ya que $\langle(1\ 2\ 3)\rangle$ es de índice 2 en S_3.

Como ya queda dicho, todo grupo abeliano es resoluble, pero como consecuencia de (1.48) y de (1.51) obtendremos, como corolario de la siguiente Proposición, un resultado para grupos finitos resolubles que será crucial en la prueba del gran Teorema de Galois.

Proposición 1.63. *Si G es un grupo abeliano finito existe una torre*

$$G_r = \{e\} \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_0 = G$$

tal que cada cociente G_{i-1}/G_i es cíclico de orden primo.

Demostración. Sea $G = H_1 \cdots H_t$ (1.51), donde cada H_i es el único p_i-subgrupo de Sylow de G. Ahora, para cada $i = 1, 2, \ldots, t$, el grupo

$$(H_1 \cdots H_i) \,/\, (H_1 \cdots H_{i-1}) \simeq H_i$$

tiene una torre de subgrupos

$$0 \subset G'_{i,r_i} \subset G'_{i,r_i-1} \subset \cdots \subset G'_{i,0} = H_i$$

tal que cada cociente $G'_{i,s-1}/G'_{i,s}$ es cíclico de orden p_i, para todo $s = 1, \ldots, r_i$ (1.48). Por aplicación del Teorema de la correspondencia al homomorfismo de paso al cociente $\varphi_i \colon (H_1 \cdots H_i) \to (H_1 \cdots H_i) \,/\, (H_1 \cdots H_{i-1})$ se obtiene una torre

$$H_1 \cdots H_{i-1} \subset G_{i,r_i} \subset G_{i,r_i-1} \subset \cdots \subset G_{i,0} = H_1 \cdots H_i$$

de las mismas características que la anterior ya que, en virtud del primer Teorema de isomorfía (1.16), se verifica que $G_{i,s-1}/G_{i,s} \equiv G'_{i,s-1}/G'_{i,s}$, para todo $s = 1, \ldots, r_i$. Se consigue una torre de resolubilidad para G por concatenación de las sucesivas torres obtenidas para cada $i = 1, \ldots, t$. □

Corolario 1.64. *Si G es un grupo finito resoluble existe una torre normal*

$$G_r = \{e\} \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_0 = G$$

en la que cada cociente G_{i-1}/G_i es cíclico de orden primo.

Demostración. Por hipótesis existe una torre normal

$$H_t = \{e\} \subset H_{t-1} \subset H_{t-2} \subset \cdots \subset H_0 = G$$

con cada H_{i-1}/H_i grupo finito abeliano. Usando la Proposición 1.63 y el Teorema de la correspondencia es posible intercalar grupos entre cada dos consecutivos de la torre original obteniendo

$$H_{i+1} = H_{i,n_i} \subset H_{i,n_i-1} \subset H_{i,n_i-2} \subset \cdots \subset H_{i,0} = H_i$$

de modo que los cocientes de grupos sucesivos sean grupos de orden primo. La concatenación de las torres parciales así obtenidas proporciona lo anunciado. □

Proposición 1.65. *Sea H un subgrupo del grupo G.*

1. *Si G es resoluble, entonces H es resoluble.*
2. *Si H es normal en G son equivalentes las afirmaciones*
   a) *G es resoluble.*
   b) *H y G/H son resolubles.*

Demostración. 1. La cadena

$$G_r = \{e\} \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_0 = G \ \ (*)$$

que establece la resolubilidad de G, proporciona otra

$$G_0 \cap H = \{e\} \subset G_{r-1} \cap H \subset G_{r-2} \cap H \subset \cdots \subset G_0 \cap H = H$$

en la que cada grupo es normal en el siguiente, cada cociente

$$G_{i-1} \cap H / G_i \cap H$$

es subgrupo de G_{i-1}/G_i y, por tanto, es abeliano.

b) $\Rightarrow$ *a)* Como consecuencia del apartado *a)* solo hay que probar que G/H es resoluble. Ahora, si $\varphi : G \to G/H$ es el homomorfismo canónico de paso al cociente, a partir de la cadena $(*)$ de resolubilidad para G, se obtiene la torre

$$\varphi(\{e\}) = \{H\} \subset \varphi(G_{r-1}) \subset \cdots \subset \varphi(G_1) \subset \varphi(G) = G/H$$

que establece la resolubilidad de G/H, pues cada grupo es normal en el siguiente por el Teorema de la correspondencia y además

$$\varphi\left(G_{i-1}\right)/\varphi\left(G_i\right)$$

es abeliano al ser un grupo cociente de subgrupos de G_{i-1}/G_i que lo es por hipótesis.

$a) \Rightarrow b)$ Sean

$$H_s = \{e\} \subset H_{s-1} \subset \cdots \subset H_0 = H \qquad (*)$$

y

$$G_t'' = \{H\} \subset G_{t-1}'' \subset G_{t-2}'' \subset \cdots \subset G_0'' = G/H \ \ (**)$$

las cadenas que establecen las resolubilidades respectivas de H y de G/H. Por el Teorema de la correspondencia existe una cadena

$$H = G_t \subset G_{t-1} \subset G_{t-2} \subset \cdots$$

definida mediante $G_i := \phi^{-1}(G_i'')$, que satisface as condiciones de normalidad requeridas y además $G_i/G_{i-1} \simeq G_i''/G_{i-1}''$, lo que proporciona la conmutatividad de cada grupo cociente. La concatenación de las cadenas $(*)$ y $(**)$ proporciona la cadena

$$\{e\} = H_s \subset H_{s-1} \subset \cdots \subset H_0 = H = G_t \subset G_{t-1} \subset G_{t-2} \subset \cdots \subset G_o = G,$$

que establece la resolubilidad de G. □

Definición 1.66. Si G es un grupo y x, y son elementos de G se define el *conmutador* del par (x, y) como

$$[x, y] = xyx^{-1}y^{-1} \in G,$$

y se denotará con $G^{(1)}$, o con $[G : G]$, el subgrupo de G generado por todos los conmutadores de pares de elementos de G. El subgrupo $G^{(1)}$ recibe el nombre de *subgrupo conmutador o subgrupo derivado* de G, y también *abelianizador* de G. De modo recursivo se define la *serie derivada* de un grupo G que está formada por la cadena de subgrupos

$$\cdots \subset G^{(i+1)} := \left[G^{(i)} : G^{(i)}\right] \subset \cdots \subset G^{(2)} := \left[G^{(1)} : G^{(1)}\right] \subset G^{(1)} \subset G := G^{(0)}$$

Nótese que en la anterior definición todo se trivializa si el grupo G es conmutativo pues en ese caso $[x, y] = e, \forall x, y \in G$.

Lema 1.67. *Sea G un grupo. Entonces*

1. *$G^{(1)}$ es subgrupo normal de G y el cociente $G/G^{(1)}$ es abeliano.*

2. *Si H es un subgrupo normal de G son equivalentes:*

   a) *El cociente G/H es abeliano.*

   b) *$G^{(1)} \subset H$.*

Demostración. 1. $G^{(1)} := \langle \{[x, y] / x, y \in G\} \rangle$. Nótese que $[x, y]^{-1} = [y, x]$ y que, por lo tanto, cada elemento de $G^{(1)}$ se expresa como un producto finito de conmutadores. Un pequeño truco de cálculo proporciona la normalidad de $G^{(1)}$:

$$g\,[a_1, b_1] \cdots [a_n, b_n]\, g^{-1} = \left[ga_1g^{-1}, gb_1g^{-1}\right] \cdots \left[ga_ng^{-1}, gb_ng^{-1}\right].$$

La conmutatividad de $G/G^{(1)}$ resulta de que como $ab\,(ba)^{-1} = aba^{-1}b^{-1} \in G^{(1)}$ se tiene que

$$aG^{(1)}bG^{(1)} = abG^{(1)} = baG^{(1)} = bG^{(1)}aG^{(1)}.$$

2. En efecto, para $a, b \in G$ se verifica que

$$aHbH = abH = baH = bHaH \Leftrightarrow ab(ba)^{-1} = [a, b] \in H,$$

y, por lo tanto, G/H es abeliano si, y solo si, H contiene a todos los conmutadores. □

Como consecuencia del Lema anterior, en la serie derivada de un grupo G cada subgrupo es normal en el siguiente y el cociente de ambos es abeliano. Por consiguiente, si existe un n tal que $G^{(n)}$ es conmutativo, la serie derivada termina en el grupo trivial $\{e\} = G^{(n+1)}$ después de un número finito de pasos y dicha serie es una cadena que establece la resolubilidad de G. El recíproco también es cierto ya que si G es un grupo resoluble y

$$G_r = \{e\} \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_1 \subset G_0 = G$$

es una torre abeliana, en virtud del apartado *b*) del Lema 1.67, se tiene que $G^{(1)} \subset G_1$ y entonces $G^{(2)} \subset G_1^{(1)}$ (pues es evidente que si H es subgrupo de K entonces $H^{(1)}$ es subgrupo de $K^{(1)}$). Como G_1/G_2 es abeliano, el Lema 1.67 nos permite afirmar que $G_1^{(1)} \subset G_2$, con lo que resulta $G^{(2)} \subset G_2$. De forma recurrente se prueba que $G^{(i)} \subset G_i$ para todo i, y por tanto necesariamente $G^{(r)} = \{e\}$.

Proposición 1.68. *Un grupo G es resoluble si, y solamente si, su serie derivada alcanza el grupo trivial después de un número finito de pasos, es decir, existe un número natural r tal que $G^{(r)} = \{e\}$.*

Obsérvese que para un grupo finito G su serie derivada es necesariamente estacionaria, es decir, existe un $k \in \mathbb{N}$ tal que $G^{(k)} = G^{(k+1)}$ (y por tanto $G^{(i)} = G^{(j)}$ para todos $i, j \geqslant k$). La no resolubilidad de G, cuando G es finito, significa entonces que su serie derivada estaciona en un grupo $G^{(k)} \neq \{e\}$. Si G es infinito no resoluble su serie derivada puede no ser estacionaria.

Los últimos resultados de esta sección se dedican al estudio de la resolubilidad de los grupos de permutaciones.

Proposición 1.69. *S_4 y A_4 son grupos resolubles.*

Demostración. Ya que $(S_4 : A_4) = 2$ la resolubilidad de S_4 es equivalente a la de A_4 en virtud de la Proposición 1.65, así que probaremos solamente que el grupo alternado A_4 es resoluble.

Sea V un 2-subgrupo de Sylow de A_4, es decir V es de orden 4 y $(A_4 : V) = 3$. Los elementos de V son todos permutaciones pares ($V \subset A_4$) y todas son de período 2. En efecto, cada permutación $\sigma \in V$ ($\sigma \neq id$) no puede tener período 3 (ya que tal período ha de ser divisor de $4 = \#V$) ni ser un 4-ciclo ya que en ese caso sería una permutación impar (1.56). Por tanto, el período de σ es necesariamente 2. Ahora bien, los únicos elementos de período 2 de S_4 son trasposiciones, que no son elementos de V al ser permutaciones impares, o producto de dos trasposiciones disjuntas, que son permutaciones pares. Solamente hay tres de tales elementos, a saber

$$(1\ 2)\,(3\ 4)\,, (1\ 3)\,(2\ 4)\,, (1\ 4)\,(2\ 3)\,.$$

Por ello, $V = \{id, (1\ 2)\,(3\ 4)\,, (1\ 3)\,(2\ 4)\,, (1\ 4)\,(2\ 3)\}$ y V es el único 2-subgrupo de Sylow de A_4, que es por tanto normal en A_4 (1.50). Como A_4/V es de orden 3 y V de orden 4 ambos son grupos abelianos. Se concluye que, A_4 es un grupo resoluble. □

Este resultado, junto con la resolubilidad de S_2 y S_3 (como subgrupos que son de S_4), nos permitirá afirmar que existe una fórmula, que contiene solamente expresiones radicales y algebraicas de los datos, para resolver la ecuación algebraica general de grado $\leqslant 4$, sin necesidad de obtener dicha fórmula de modo explícito.

Proposición 1.70. *Si $n \geqslant 5$, el grupo S_n no es resoluble.*

Demostración. La prueba se realizará por reducción al absurdo. Se demostrará que si

$$\{id\} = H_m \subset \cdots \subset H_{i+1} \subset H_i \subset \cdots \subset H_1 \subset H_0 = S_n$$

es una torre abeliana de S_n y $n \geqslant 5$, cada subgrupo H_i contiene a todos los 3-ciclos, lo que es imposible pues $\{id\} = H_m$.

Sea (abc) un 3-ciclo y elíjanse $d, e \in \{1, 2, \ldots, n\} \setminus \{a, b, c\}$, lo cual es posible al ser $n \geqslant 5$. Sean $\alpha = (c\ d\ b)$ y $\beta = (b\ a\ e)$. Como H_0/H_1 es abeliano, el conmutador $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1} = (a\ b\ c)$ es un elemento de H_1 (1.67). Sea ahora $i > 1$ y supongamos que todos los 3-ciclos son elementos de H_i. Procedemos de forma idéntica al caso $i = 1$ teniendo en cuenta que $\alpha, \beta \in H_i$ por ser 3-ciclos, y resulta que $(a\ b\ c) = [\alpha, \beta] \in H_{i+1}$ por ser H_i/H_{i+1} abeliano. □

La no resolubilidad de los grupos de permutaciones S_n para $n \geqslant 5$ será crucial a la hora de probar la no resolubilidad por radicales de la ecuación general de grado $n \geqslant 5$.

1.4. Ejercicios

1. Sea G un grupo, n un entero y $a \in G$. Definimos las potencias de a como sigue:
   a) $a^0 := e$, el elemento neutro de G,
   b) $a^n = a \overset{n)}{\cdots} a$ si $n > 0$,
   c) $a^n = a^{-1} \overset{-n)}{\cdots} a^{-1}$ si $n < 0$.

   Dados $m, n \in \mathbb{Z}$ demuéstrese que
   a) $(a^n)^{-1} = \left(a^{-1}\right)^n = a^{-n}$.
   b) $a^m \cdot a^n = a^{m+n}$.
   c) $(a^m)^n = a^{mn}$.

2. Sea H un subgrupo del grupo G. Demuéstrese que para cada $a \in G$ el conjunto $aHa^{-1} := \{aha^{-1} \mid h \in H\}$ es un subgrupo de G del mismo cardinal que H.

3. Demuéstrese que si G es un grupo en el que para cada $a \in G$ se tiene $a^2 = e$ (elemento neutro de G), entonces G es abeliano.

4. Dados H, K subgrupos de un grupo G se define el conjunto $HK := \{hk | h \in H, k \in K\}$. Demuéstrese que, HK es subgrupo de G si, y solo si, $HK = KH$.

5. Sea $V = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

   a) Pruébese que V es subgrupo normal de A_4.

   b) Demuéstrese que $W := \langle (1\ 2)(3\ 4) \rangle$ es subgrupo normal de V y que no es normal en A_4.

6. Sean H subgrupo de G y K subgrupo de L.

   a) Demuéstrese que $H \times K$ es subgrupo de $G \times L$.

   b) Demuéstrese que $H \times K$ es normal en $G \times L$ si, y solo si, H es normal en G y K es normal en L.

7. Sean G y H grupos, $a \in G$ y $b \in H$ elementos de orden finito. Demuéstrese que $(a, b) \in G \times H$ es un elemento de orden $mcm(|a|, |b|)$.

8. Sea G un grupo y $a, b \in G$ tales que $(|a|, |b|) = 1$. Demuéstrese que si $ab = ba$, entonces $|ab| = |a|\,|b|$.

9. Sean $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ elementos de $GL_2(\mathbb{R})$. Demuéstrese que A tiene orden 4, que B es de orden 3 y que AB es de orden 0.

10. Sea G un grupo y $a, b \in G$. Demuéstrense las siguientes identidades

    a) $|a| = \left|a^{-1}\right| = \left|bab^{-1}\right|$.

    b) $|ab| = |ba|$.

11. Sea $G = \langle a \rangle$ un grupo cíclico de orden n. Demuéstrese que:

    a) $\left|a^j\right| = \dfrac{n}{(n, j)}$.

    b) Si r es un entero positivo que divide a n, entonces G contiene exactamente un subgrupo de orden r.

12. Sea $G = \langle a \rangle$ un grupo cíclico de orden 154 y sea H un subgrupo de G generado por $\left\{a^{28}, a^{88}\right\}$. Pruébese que existe un entero k tal que $H = \langle a^k \rangle$.

13. Sean G y H grupos cíclicos de órdenes m y n, respectivamente. Demuéstrese que, el grupo $G \times H$ es cíclico si, y solo si, $(m, n) = 1$.

14. Sea G un grupo, $G \neq \{e\}$. Pruébese que, G no tiene otros subgrupos que G y $\{e\}$ si, y solo si, G es cíclico de orden primo.

15. Sea G un grupo abeliano finito de orden $n = p^r q$ con p primo no divisor de q y $r \geqslant 1$. Demuéstrese que si H es el subgrupo de G de orden p^r, existe según lo establecido en (1.32), se tiene

$$H = \{x \in G \mid |x| \text{ es una potencia de } p\}.$$

16. Sean $f\colon G \to H$ un homomorfismo de grupos y $a \in G$ un elemento de orden finito. Demuéstrese que $|f(a)|$ divide a $|a|$ y que si, además f es inyectivo, entonces $|f(a)| = |a|$.

17. Sea G un grupo finito. Demuéstrese :

    a) Si G es de orden 4, entonces G es isomorfo a $\mathbb{Z}_4$ o al grupo de Klein.

    b) Si $\#G \leqslant 5$, entonces G es abeliano.

18. Se consideran los subgrupos $5\mathbb{Z}$ y $35\mathbb{Z}$ de $\mathbb{Z}$. Demuéstrese que $5\mathbb{Z}/35\mathbb{Z} \simeq \mathbb{Z}_7$.

19. Si G es un grupo finito, abeliano de orden n y m es entero positivo coprimo con n, entonces la aplicación $f\colon G \to G$ definida por $f(a) = a^m$ es un automorfismo de G.

20. Demuéstrese que $(\mathbb{Q}, +)$ no es isomorfo a $(\mathbb{Z}, +)$. ¿Es $(\mathbb{Q}^*, .)$ isomorfo a $(\mathbb{Z}, +)$?

21. Sea $G = S_3 \times \mathbb{Z}_5$. ¿Es G un grupo cíclico? ¿Cuántos 5-subgrupos de Sylow tiene G? ¿Es cíclico todo 5-subgrupo de Sylow de G? ¿Cuántos 3-subgrupos de Sylow tiene G?

22. Sean G un grupo y H y K subgrupos de G.

    Se considera la aplicación $\Phi\colon H \times K \to G$ definida por $\Phi(a, b) = ab$. Demuéstrese que son equivalentes las afirmaciones:

    a) Φ es isomorfismo.

    b) H y K son subgrupos normales de G y cada elemento $x \in G$ se expresa de forma única como $x = ab$ con $a \in H$ y $b \in K$.

    c) H y K son subgrupos normales de G, $H \cap K = \{e\}$ y $HK = G$.

23. Sea G un grupo de orden 65. Demuéstrese que existen subgrupos normales H y K de G tales que $G = HK$. Como consecuencia demuéstrese que G es cíclico.

24. Demuéstrese que todo grupo de orden 35 es cíclico.

25. Pruébese que un grupo de orden 56 o 132 no es simple.

26. Sean H y K grupos y $G = H \times K$. Demuéstrese que G es resoluble si, y solo si, son resolubles H y K.

27. Demuéstrese que un grupo G de orden 30 no es simple. ¿Es resoluble? Como consecuencia demuéstrese que si un grupo de orden 60 no es simple entonces es resoluble. Como aplicación obténgase que A_5 es grupo simple.

28. Sea G un grupo simple de orden 168.

    a) Calcúlense el número de 7-subgrupos de Sylow de G.

    b) Si P es un 7-subgrupo de Sylow de G, determínese el orden de $N_G(P)$.

    c) Utilizando lo anterior, demuéstrese que G no tiene subgrupos de orden 14.

29. Sean, p un número primo, G un grupo finito, H un subgrupo normal de G y P un p-subgrupo de Sylow de G. Demuéstrese que

    a) $H \cap P$ es p-subgrupo de Sylow de H.

    b) HP/H es p-subgrupo de Sylow de G/H.

30. *a*) Sean p, q enteros positivos, p primo y $q < p$. Demuéstrese que si G es un grupo de orden pq existe un único subgrupo H de G tal que $\#H = p$ y que H es subgrupo normal de G.

    b) Demuéstrese que si G es un grupo de orden 42, entonces G tiene un subgrupo normal de orden 21.

31. Demuéstrese que si $p \neq 2$ es un número primo, todo grupo de orden $2p$ es cíclico o bien isomorfo al grupo diédrico D_{2p}. Si $p = 3$ demostrar que $D_{2p} \simeq S_3$.

32. Demuéstrese que todo grupo G de orden 12 es resoluble.

33. Sean p, q números primos.

    a) Demuéstrese que todo grupo G de orden pq es resoluble.

    b) Demuéstrese que todo grupo de orden p^2q es resoluble.

34. Se consideran los grupos $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D_{2,4}$ y $\mathbb{Z}_4 \times \mathbb{Z}_2$.

    a) Justifíquese que cada dos de ellos no son isomorfos.

    b) Razónese cuáles son cíclicos y cuáles son resolubles.

    c) ¿Alguno de estos grupos tiene subgrupos de orden 4?

35. Sea G un grupo finito y p un número primo.

    a) Demuéstrese que G es un p-grupo si, y solo si, todo elemento de G tiene de período una potencia de p.

b) Demuéstrese que al menos existen dos grupos no isomorfos de orden p^2.

36. Sea G un grupo de orden 10.

a) Demuéstrese que G tiene un subgrupo normal H de orden 5 y al menos un subgrupo K de orden 2.

b) Demuéstrese también que si G es abeliano entonces G es isomorfo a $G/H \times G/K$ y que, como consecuencia, G es cíclico.

37. *a*) Sean p, q números primos. Pruébese que un grupo G de orden pq es resoluble. ¿Es abeliano?

b) Sea G un grupo tal que para cada par de subgrupos H, K de G se verifica que $H \subset K$ o $K \subset H$. Demuéstrese que G es un p-grupo para algún primo p.

38. Si n es un entero positivo descríbase el grupo $Aut(\mathbb{Z}_n)$.

39. *a*) Sea p un número primo. Demuéstrese

1) Si G es un p-grupo entonces p divide al orden de Z_G.
2) Como consecuencia de 1) todo p-grupo tiene un subgrupo normal de orden p.

b) Sea $G = S_3 \times \mathbb{Z}_4$. Justificar razonadamente las afirmaciones

1) G es un grupo resoluble.
2) Existe un único 3-subgrupo de Sylow de G.
3) G tiene exactamente tres subgrupos de orden 8.

40. Sea G un grupo de orden 440. Demuéstrese que

a) G no es simple.

b) G tiene un subgrupo normal de orden 55.

41. Demuéstrese que si $n \geqslant 3$ el grupo alternado A_3 está generado por los 3-ciclos.

42. Usando el ejercicio anterior demuéstrese que A_n es el subgrupo derivado de S_n, si $n \geqslant 3$.

Capítulo 2

Complementos de teoría de anillos

Se desarrollan aquí de forma muy esquemática los aspectos de la teoría de anillos que van a ser utilizados en lo que sigue. Una parte importante del contenido del capítulo debe ser conocido para quien haya estudiado un curso elemental de Álgebra.

2.1. Generalidades

Se dedica esta primera sección a las nociones de anillo, módulo e ideal, los Teoremas de isomorfía para anillos y el Teorema de la correspondencia en el contexto de anillos, módulos e ideales.

Definición 2.1. Un *anillo* A es un grupo abeliano $(A,+)$ en el que hay definida una segunda operación $\cdot : A\times A \to A$ (multiplicación) de modo que se satisfacen las siguientes condiciones

i) La multiplicación es asociativa $(ab)c = a(bc)$, $\forall a,b,c \in A$ (a partir de ahora se pondrá $abc = (ab)c = a(bc)$).

ii) Existe un elemento neutro 1 para la multiplicación: $1a = a1 = a, \forall a \in A$.

iii) La multiplicación es distributiva respecto de la suma:

$$a(b+c) = ab + ac, \quad (a+b)c = ac + bc, \quad \forall a,b,c \in A.$$

De aquí se deduce que $a0 = 0, \forall a \in A$, ya que $a0 = a(0+0) = a0 + a0 \Rightarrow a0 = 0$, al ser $a0$ idempotente en el grupo $(A,+)$; de forma análoga se obtiene $0a = 0, \forall a \in A$.

Se dirá que el anillo A es *conmutativo* si la operación de multiplicar es conmutativa: $ab = ba, \forall a,b \in A$.

Definición 2.2. Un elemento $u \in A$ se dirá que es una *unidad* si tiene inverso para la multiplicación. El conjunto de unidades de A se denotará con A^* o con $U(A)$. Se dirá que el anillo $A \neq 0$ es un *anillo de división* si cada elemento no nulo tiene inverso para la multiplicación. Un *cuerpo* es un anillo de división conmutativo.

A^* es un grupo respecto de la multiplicación de A. El anillo A es de división precisamente si $A^* = A \setminus \{0\}$.

Definición 2.3. Si A es un anillo, un *subanillo* B de A es un subgrupo del grupo aditivo $(A, +)$ tal que $ab \in B$, $\forall a, b \in B$ y $1 \in B$. En otras palabras B es anillo con las mismas operaciones de A y con el mismo neutro para la multiplicación.

Definición 2.4. Si A y B son anillos, una aplicación $f\colon A \to B$ es un *homomorfismo de anillos* si lo es de los grupos abelianos $(A, +)$ y $(B, +)$ y además

i) $f(aa') = f(a)f(a')$, $\forall a, a' \in A$, y

ii) $f(1_A) = 1_B$.

Un *isomorfismo* es un homomorfismo biyectivo.

Son afirmaciones de comprobación inmediata:

Si $f\colon A \to B$ es un homomorfismo de anillos y A' es subanillo de A, entonces $f(A')$ es subanillo de B.

Si $f\colon A \to B$ es un homomorfismo de anillos y B' es subanillo de B, entonces $f^{-1}(B')$ es subanillo de A.

Definición 2.5. Sea A un anillo conmutativo.

i) Un elemento no nulo $a \in A$ se dice que es un *divisor de cero* si existe un $b \in A$, $b \neq 0$, tal que $ab = ba = 0$.

ii) El anillo A se dirá que es un *dominio de integridad* (o simplemente un dominio) si no posee divisores de cero.

Un cuerpo A es un dominio de integridad, pues si $a, b \in A$ son tales que $ab = 0$ y $a \neq 0$, entonces $b = a^{-1}ab = a^{-1}0 = 0$.

Definición 2.6. Si A es un anillo, un grupo abeliano M se dirá que es un *A-módulo* por la izquierda si existe una operación

$$\cdot\colon A \times M \to M$$

$$(a, m) \mapsto am$$

que satisface las siguientes condiciones

i) $1m = m,\ \ \forall m \in M.$

ii) $(ab)m = a(bm),\ \ \forall a, b \in A, \forall m \in M.$

iii) $a(m+n) = am + an,\ \ \forall a \in A$ y $\forall m, n \in M.$

iv) $(a+b)m = am + bm,\ \ \forall a, b \in A$ y $\forall m \in M.$

Como consecuencia, se tiene de modo inmediato que $0_A m = 0_M$ y $a0_M = 0_M$, $\forall a \in A$ y $\forall m \in M$, en donde se ha escrito 0_A (0_M) para indicar el elemento neutro de la suma en A (M).

Definición 2.7. N es un *A-submódulo* del A-módulo por la izquierda M, si N es un subgrupo de $(M, +)$ y tal que $an \in N$, $\forall a \in A$ y $\forall n \in N$. Es decir, N es también un A-módulo por la izquierda.

Es muy fácil demostrar que N es un submódulo del A-módulo M si, y solo si, $ax + by \in N$, $\forall a, b \in A$ y $\forall x, y \in N$.

Si N es un A-submódulo del A-módulo por la izquierda M, el grupo abeliano M/N adquiere estructura de A-módulo por la izquierda con la operación $a(m+N) := am+N$ (que está bien definida, pues para $m + N = m' + N$ se tiene $m - m' \in N$ y, por tanto, $a(m - m') = am - am' \in N$, es decir, $am + N = am' + N, \forall a \in A$).

Análogas consideraciones para estructuras por la derecha. El propio anillo A es un ejemplo de A-módulo por la derecha y por la izquierda.

Definición 2.8. Si A es un anillo, los A-submódulos del A-módulo por la izquierda (derecha) A serán denominados ideales por la izquierda (derecha) de A. Los ideales biláteros de A, que llamaremos ideales, son los ideales por ambos lados.

Si $f\colon A \to B$ es un homomorfismo de anillos, el núcleo de f considerado como homomorfismo de grupos abelianos es ahora un ideal bilátero.

Si I es un ideal bilátero de A la operación $(a+I)(b+I) := ab+I$ está bien definida y dota al grupo abeliano cociente A/I de estructura de anillo, y el homomorfismo canónico de paso al cociente $\varphi_I\colon A \to A/I$ es homomorfismo de anillos. Si $f\colon A \to B$ es un homomorfismo de anillos el núcleo de f considerado como homomorfismo de grupos abelianos es ahora un ideal bilátero. De hecho un subconjunto I del anillo A es ideal bilátero de A si, y solo si, es núcleo de un homomorfismo de anillos $f\colon A \to B$, para algún anillo B. Para un homomorfismo de anillos $f\colon A \to B$ los homomorfismos que aparecen en la descomposición canónica de f como homomorfismo de grupos abelianos son también homomorfismos de anillos. Un isomorfismo de anillos es un homomorfismo biyectivo.

Definición 2.9. Si M y M' son A-módulos por la izquierda, una aplicación $f\colon M \to M'$ es un homomorfismo de A-módulos si lo es de grupos abelianos y además $f(am) = af(m), \forall a \in A$ y $\forall m \in M$. Equivalentemente, la aplicación $f\colon M \to M'$ es homomorfismo de A-módulos si $f(ax + by) = af(x) + bf(y), \quad \forall a, b \in A$ y $\forall x, y \in M$.

Si $f\colon M \to M'$ es un homomorfismo de A-módulos y N es un A-submódulo de M entonces $f(N)$ lo es de M'. También, si N' es A-submódulo de M' entonces $f^{-1}(N')$ es A-submódulo de M. Los conceptos de núcleo e imagen de f como homomorfismo de A-módulos son los mismos que los correspondientes como homomorfismo de grupos abelianos, y las anteriores son afirmaciones de comprobación inmediata, como lo es también que si $f\colon A \to B$ es homomorfismo de A-módulos, los homomorfismos que aparecen en la descomposición canónica de f como homomorfismo de grupos abelianos son también homomorfismos de A-módulos.

Un isomorfismo de A-módulos es un homomorfismo biyectivo.

Teorema 2.10. *Sean A un anillo, M un A-módulo por la izquierda y N, L A-submódulos de M tales que $L \subset N$. Entonces*

i) N/L es un A-submódulo de M/N.

ii) Existe un isomorfismo de A-módulos por la izquierda

$$M/N \simeq (M/L) \,/\, (N/L)\,.$$

Demostración. La prueba consiste en comprobar que los homomorfismos que aparecen en la demostración correspondiente al Teorema análogo de grupos son ahora también homomorfismos de A-módulos. □

Teorema 2.11. *Sean A un anillo e I y J ideales de A tales que $I \subset J$. Entonces*

i) J/I es ideal del anillo A/I.

ii) Existe un isomorfismo de anillos

$$A/J \simeq (A/I) \,/\, (J/I)\,.$$

Demostración. La prueba consiste en comprobar que los homomorfismos que aparecen en la demostración correspondiente al Teorema análogo de grupos son ahora también homomorfismos de anillos. □

Si $(N_i)_{i\in I}$ es una familia de submódulos de un A-módulo por la izquierda M es fácil comprobar que

$$\cap_{i\in I} N_i \quad \text{y} \quad \sum_{i\in I} N_i := \{\sum_{i\in I} x_i \mid x_i \in N_i,\ x_i = 0 \text{ para casi todo } i \in I\}$$

son también submódulos de M. La intersección $\cap_{i\in I} N_i$ es el mayor submódulo de M que está contenido en todos los N_i y la suma $\sum_{i\in I} N_i$ es el menor submódulo de M que contiene a todos los N_i.

Teorema 2.12. *Sean A un anillo, M un A-módulo por la izquierda y N, L A-submódulos de M. Entonces existe un isomorfismo*

$$(N + L)/N \simeq L/N \cap L.$$

Demostración. La prueba consiste en comprobar que los homomorfismos que aparecen en la demostración correspondiente al Teorema análogo de grupos son ahora también homomorfismos de A-módulos. □

Teorema 2.13. *(Teorema de la correspondencia)*

Sea A un anillo (M un A-módulo) y J un ideal de A (N un submódulo de M). Existe una biyección que conserva las inclusiones entre el retículo de ideales de A/J (submódulos de M/N) y el de ideales de A que contienen a J (submódulos de M que contienen a N).

Demostración. Para un homomorfismo de anillos $f\colon A \to B$ el conjunto $f(A)$ es un subanillo de B y son válidas consideraciones semejantes a las de la observación 1.10: si I es ideal de A el conjunto $f(I)$ es ideal de $f(A)$; la imagen inversa $f^{-1}(J)$ de un ideal J de B es ideal de A que contiene al núcleo de f. También, si $\varphi\colon M \to N$ es homomorfismo de A-módulos y L (respectivamente, T) es submódulo de M (respectivamente, N), entonces $\varphi(L)$ (respectivamente, $\varphi^{-1}(T)$) es submódulo de N (respectivamente, submódulo de M que contiene al núcleo de φ). (Compárese con (1.19)). □

Si M es un A-módulo por la izquierda y S un subconjunto de M, el menor submódulo de M que contiene a S, que denotaremos con AS y lo denominaremos submódulo de M generado por S, está determinado por cualquiera de las dos propiedades siguientes:

a) AS es la intersección de todos los submódulos de M que contienen a S.

b) AS es el conjunto de todas las combinaciones lineales de elementos de S, es decir,

$$AS = \Big\{x = \sum_i a_i x_i \mid x_i \in S \text{ y } a_i \in A \text{ casi todos nulos}\Big\}.$$

Si $S = \{x_1, \ldots, x_n\}$, entonces $AS = Ax_1 + \cdots + Ax_n$, en donde se ha escrito Ax_i en lugar de $A\{x_i\}$.

Si $a_1, \ldots, a_n$ son elementos del anillo conmutativo A con $(a_1, \ldots, a_n)$ se indicará el ideal generado por el conjunto $\{a_1, \ldots, a_n\}$, es decir, el A-submódulo de A generado por dicho conjunto.

Se comprueba fácilmente que si $(N_i)_{i\in I}$ es una familia de submódulos de M entonces $\sum_{i\in I} N_i$ es el submódulo generado por el conjunto $\cup_{i\in I} N_i$.

Para cada anillo A existe un único homomorfismo de anillos $c\colon \mathbb{Z} \to A$. En efecto, la condición $c(1) = 1_A$ determina la imagen de cualquier número natural n ($c(n) = 1_A + \overset{n)}{\cdots} + 1_A$) y, por lo tanto, de cualquier número entero ($c(-n) = -c(n)$). El núcleo de este homomorfismo está generado (como subgrupo de $\mathbb{Z}$ que es) por el menor entero positivo que contiene y $\mathrm{Ker}(c) = n\mathbb{Z} = (n)$.

Definición 2.14. Con las notaciones anteriores si $\mathrm{Ker}(c) = n\mathbb{Z}$, el número natural n recibe el nombre de característica de A ($Caract(A) = n$), y es entonces el menor entero positivo n tal que $n1_A := 1_A + \overset{n)}{\cdots} + 1_A = 0$. Además, si m es un entero tal que $m1_A = 0$, entonces m es múltiplo de n. Nótese que $Caract(A) = |1_A|$ es el período de 1_A en el grupo abeliano $(A, +)$.

Si A es un dominio de integridad entonces la característica de A es nula o un número primo. En efecto, si $Caract(A) = n \neq 0$ y si $n = ab$ con $a \neq 1 \neq b$, entonces $n1_A = (a1_A)(b1_A) = 0$ y así $(a1_A) = 0$ o $(b1_A) = 0$ contradiciendo la minimalidad de n respecto de la condición $n1_A = 0$.

Si A es un dominio, A contiene (una réplica isomorfa) al anillo $\mathbb{Z}$ o al cuerpo $\mathbb{Z}/p\mathbb{Z}$, y si además A es cuerpo, entonces contiene (una réplica isomorfa) al cuerpo $\mathbb{Q}$ o a $\mathbb{Z}/p\mathbb{Z}$. El subanillo $\mathrm{Im}(c)$ es el menor subanillo de A (todos los subanillos contienen a 1_A). Si A es cuerpo, los cuerpos $\mathbb{Q}$, si $Caract(A) = 0$, o $\mathbb{Z}/p\mathbb{Z}$, si $Caract(A) = p$, son, en cada caso, el menor subcuerpo de A, y recibe el nombre de (*sub*)*cuerpo primo* de A.

2.2. Dominios Euclídeos. Divisibilidad

A partir de ahora, y salvo mención explícita de otra cosa, los anillos considerados aquí serán siempre conmutativos.

En esta sección se revisan los elementos de la teoría de divisibilidad en dominios de ideales principales.

Todo subanillo de un dominio de integridad es también un dominio de integridad, y en particular todo subanillo de un cuerpo es un dominio de integridad. Esto agota todas las posibilidades pues de hecho se tiene:

Proposición 2.15. *Un anillo conmutativo A es un dominio de integridad si, y solo si, A es subanillo de un cuerpo. Cada dominio A es subanillo de un cuerpo $Q(A)$, que se denomina cuerpo de fracciones de A y que satisface la siguiente propiedad universal:*

Si B es otro anillo conmutativo y $f\colon A \to B$ es un homomorfismo de anillos tal que $f(s)$ es unidad en B, para todo $s \in A \setminus \{0\}$, entonces f se extiende de modo único a un homomorfismo $f'\colon Q(A) \to B$.

Demostración. Si A es dominio se considera en el conjunto $A \times (A \setminus \{0\})$ la relación binaria definida por

$$(a, s) \sim (b, t) \Leftrightarrow at = bs,$$

que es una relación de equivalencia.

El conjunto cociente $Q(A) = [A \times (A \setminus \{0\})] / \sim$ es el cuerpo de fracciones de A. Cada clase de equivalencia $[(a, s)] \in Q(A)$ se escribirá ahora $[(a, s)] = \dfrac{a}{s}$ y con esta notación se tiene $0 = \dfrac{0}{s}$ y $1 = \dfrac{s}{s}$ cualquiera que sea s elemento no nulo de A. Es fácil comprobar ahora que con las operaciones definidas por

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$
$$\frac{a}{s}\frac{b}{t} := \frac{ab}{st}$$

el conjunto $Q(A)$ adquiere estructura de cuerpo (el inverso de $\dfrac{a}{s}$ es $\dfrac{s}{a}$ si $\dfrac{a}{s} \neq \dfrac{0}{s}$, es decir, si $a \neq 0$).

El dominio A se identifica ahora con el subanillo de $Q(A)$ formado por los elementos $x \in Q(A)$ que admiten la expresión $x = \dfrac{a}{1}$. Cada elemento $a \in A$ se identifica con $\dfrac{a}{1}$. Si ahora $f\colon A \to B$ es homomorfismo de anillos, definimos $f'\colon Q(A) \to B$ mediante $f'\left(\dfrac{a}{s}\right) := f(s)^{-1} f(a)$ (por hipótesis $f(s)$ tiene inverso en B). Es fácil comprobar que la anterior es una buena definición para f' y que $f'(\dfrac{a}{1}) = f(a)$. Para probar la unicidad de f' supóngase que $g\colon Q(A) \to B$ satisface nuestros requerimientos, entonces

$$g(\frac{a}{s}) = g(\frac{a}{1}\frac{1}{s}) = g(\frac{a}{1})g(\frac{1}{s}) = g(\frac{a}{1})g(\left[\frac{s}{1}\right]^{-1}) = g(\frac{a}{1})(g\left[\frac{s}{1}\right])^{-1} = f(a)f\,(s)^{-1} = f'(\frac{a}{s}).$$

□

En particular $Q(A)$ es el menor cuerpo que contiene a A como subanillo. Es decir, si K es un cuerpo y $f\colon A \to K$ es una inclusión o un homomorfismo inyectivo de anillos, entonces existe $f'\colon Q(A) \to B$ cuya restricción a A es $f'|_A = f$.

Definición 2.16. Sea A un dominio de integridad, se dice que A es un *dominio de ideales principales* (DIP en lo sucesivo) si todo ideal I de A es principal, es decir, $I = (a) = Aa = \{xa \mid x \in A\}$ para un cierto $a \in I$.

Ejemplos 2.17.

1.- Si K es un cuerpo sus únicos ideales son 0 y $K = (1)$.

2.- En el anillo $\mathbb{Z}$ de los enteros los ideales son precisamente los subgrupos y son de la forma $n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$, es decir, el conjunto de los múltiplos de un entero n.

Definición 2.18. Sea A un dominio de integridad. Se dirá que A es un *dominio euclídeo* (DE) si existe una aplicación

$$\partial\colon A \setminus \{0\} \to \mathbb{Z}^+$$

tal que

1.- $\partial(a) \leqslant \partial(ab), \forall a, b \in A \setminus \{0\}$.

2.- (Algoritmo de la división euclídea) Dados $a, b \in A$, con $b \neq 0$, existen $q, r \in A$ tales que

$$a = bq + r,$$

en donde $\partial(r) < \partial(b)$ si $r \neq 0$.

Ejemplos 2.19.

1.- $\mathbb{Z}$ es dominio euclídeo con la aplicación $\partial\colon \mathbb{Z} \setminus \{0\} \to \mathbb{Z}^+$ definida por $\partial(n) = |n|$ (valor absoluto).

2.- Si K es un cuerpo, el anillo de polinomios $K[X]$ es un dominio euclídeo con la aplicación $\partial\colon K[X] \setminus \{0\} \to \mathbb{Z}^+$ definida por $\partial(f) = grado\ de\ f$.

Proposición 2.20. *Todo dominio euclídeo es un dominio de ideales principales.*

Demostración. Sea I un ideal de A y sea $\mathfrak{t}$ el menor entero positivo en el conjunto $\partial(I) \subset \mathbb{N}$ (recuérdese que el conjunto $\mathbb{N}$ está bien ordenado con su orden natural, es decir, que cada subconjunto no vacío de $\mathbb{N}$ tiene primer elemento). Sea $b \in I$ tal que $\partial(b) = \mathfrak{t}$ y sea a cualquier elemento de I. Existen $q, r \in A$ tales que

$$a = bq + r,$$

en donde $\partial(r) < \partial(b) = \mathfrak{t}$, si $r \neq 0$. Como $r = a - bq \in I$, r es necesariamente nulo pues en otro caso se entraría en contradicción con la selección de b. □

Definición 2.21. Sea A un dominio de integridad.

1.- Si $a, b \in A$, se dice que a *divide* a b (y se escribirá $a \mid b$) si existe un $c \in A$ tal que $b = ac$.

2.- Si $a, b \in A \setminus \{0\}$, se dirá que a y b son *asociados* si $a \mid b$ y $b \mid a$.

3.- Un elemento $a \in A$ es *irreducible* si $a \notin A^*$ y además

$$a = bc \text{ con } b, c \in A \Rightarrow b \in A^* \text{ o } c \in A^*.$$

Obsérvese que la relación de divisibilidad puede ser interpretada en términos de ideales:

$$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subset (a).$$

Por lo tanto,

$$a \text{ y } b \text{ son asociados } \Leftrightarrow (a) = (b).$$

Además, $a = ub$ y $b = va$ proporcionan que $a(1 - uv) = 0$, y, siendo A dominio de integridad, resulta que $u, v \in U(A)$. Es decir, que los elementos asociados a uno dado se obtienen de éste multiplicándolo por unidades.

Obsérvese también que la relación "ser asociado" es una relación de equivalencia en A, y que si a y b son asociados entonces a es irreducible si, y solo si, b es irreducible.

La irreducibilidad de un elemento depende del anillo en que se esté considerando. Es decir, si A es subanillo de B, un elemento a de A puede ser irreducible en A pero no en B (3 y -3 son irreducibles en $\mathbb{Z}$ pero no en $\mathbb{Q}$).

Definición 2.22. i) Un ideal $\mathfrak{p}$ de un anillo conmutativo A se dice que es *primo* si es propio (es decir, $\mathfrak{p} \neq A$) y para $a, b \in A \setminus \mathfrak{p}$ se tiene que $ab \notin \mathfrak{p}$.

ii) Un ideal propio $\mathfrak{m}$ de un anillo conmutativo A se dice que es *maximal* si es elemento maximal del conjunto de ideales propios de A respecto a la relación de orden definida por la inclusión.

Proposición 2.23. *En un anillo conmutativo A son equivalentes*

i) $\mathfrak{p}$ *es un ideal primo de* A.

ii) El anillo $A/\mathfrak{p}$ *es un dominio de integridad.*

Demostración. i) $\Rightarrow$ *ii)* Sean $\overline{a} = a + \mathfrak{p}$ y $\overline{b} = b + \mathfrak{p}$ elementos no nulos de $A/\mathfrak{p}$, o, lo que es equivalente, a y b elementos de A que no están en $\mathfrak{p}$. Entonces, por la definición de ideal primo, se tiene $ab \notin \mathfrak{p}$, es decir $\overline{a}\overline{b} \neq 0$ en $A/\mathfrak{p}$.

ii) $\Rightarrow$ *i)* $A/\mathfrak{p} \neq 0$ (es decir, $\mathfrak{p}$ es ideal propio) y si a y b son elementos de A que no están en $\mathfrak{p}$ se tiene que $\overline{a} = a + \mathfrak{p}$ y $\overline{b} = b + \mathfrak{p}$ son elementos no nulos de $A/\mathfrak{p}$, y como $A/\mathfrak{p}$ es un dominio se sigue que $\overline{a}\overline{b} \neq 0$, es decir, $ab \notin \mathfrak{p}$. □

Proposición 2.24. *En un anillo conmutativo A son equivalentes*

i) $\mathfrak{m}$ *es ideal maximal de* A.

ii) El anillo $A/\mathfrak{m}$ *es un cuerpo.*

Demostración. i) $\Rightarrow$ *ii)* Si $\overline{a} = a + \mathfrak{m}$ es no nulo en $A/\mathfrak{m}$, es decir, si $a \notin \mathfrak{m}$, se tiene $\mathfrak{m} \subsetneq \mathfrak{m} + Aa$ y, por tanto, $\mathfrak{m} + Aa = A$, es decir, para un cierto $b \in A$ y un cierto $m \in \mathfrak{m}$ se verifica que $1 = m + ab$, y entonces $1 - ab = m \in \mathfrak{m}$, es decir $\overline{a}\overline{b} = \overline{1}$.

ii) $\Rightarrow$ *i)* $A/\mathfrak{m} \neq 0$ (es decir, $\mathfrak{m}$ es ideal propio). Si además I es un ideal de A que contiene propiamente a $\mathfrak{m}$, existirá un $a \in I$ tal que $a \notin \mathfrak{m}$. El elemento $\overline{a} = a + \mathfrak{m}$ no es nulo y tiene entonces un inverso $\overline{b} = b + \mathfrak{m}$ para la multiplicación. Como $1 - ab \in \mathfrak{m}$ se tiene $1 - ab \in I$ y entonces $1 \in I$ ya que $ab \in I$. Es decir, necesariamente $I = A$. □

Como consecuencia de ambas proposiciones se obtiene de forma inmediata que todo ideal maximal de un anillo conmutativo es un ideal primo.

Definición 2.25. Un *dominio de integridad* A es un dominio de factorización única (DFU) si:

a) Cada elemento no nulo $a \in A$ admite una factorización

$$a = up_1^{r_1} \cdots p_t^{r_t}$$

en donde u es una unidad en A y $p_1, \ldots, p_t$ son irreducibles, cada dos no asociados.

b) Tal factorización es esencialmente única; es decir, si

$$a = vq_1^{s_1} \cdots q_l^{s_l}$$

es otra factorización en irreducibles de a, entonces $l = t$ y, después de una reordenación, p_i y q_i son asociados y $r_i = s_i$, para cada $i = 1, \ldots, t$.

La siguiente Proposición establece un resultado fundamental.

Proposición 2.26. *Si A es un DIP y $0 \neq a \in A$, son equivalentes*

i) (a) es ideal primo de A.

ii) a es irreducible en A.

iii) (a) es ideal maximal de A.

Demostración. i) $\Rightarrow$ ii) El elemento a no es unidad pues el ideal (a) es propio por ser primo, y si $a = bc \in (a)$, entonces $b \in (a)$ o $c \in (a)$. En el caso $b \in (a)$, se tiene $b = ua$, para algún $u \in A$, y así $a = bc = auc$, de lo que resulta $a(1 - uc) = 0$ y, por tanto, $1 = uc$, al ser A dominio de integridad. Similar resultado se obtiene si se supone $c \in (a)$.

ii) $\Rightarrow$ iii) Sea I un ideal de A estrictamente mayor que (a). Como A es un DIP existe un $b \in A$ tal que $I = (b)$ y de $(a) \subsetneq (b)$ resulta $a = bc$ para un cierto $c \in A$. Como a es irreducible y $(a) \neq (b)$ resulta que b es unidad en A y $I = A$.

iii) $\Rightarrow$ i) Todo ideal maximal es primo. □

Por ejemplo, en el anillo $\mathbb{Z}$ si $p \in \mathbb{Z}^+$ se tiene que, p es número primo $\Leftrightarrow$ (p) es ideal primo de $\mathbb{Z} \Leftrightarrow (p)$ es ideal maximal de $\mathbb{Z}$.

Proposición 2.27. *Todo DIP es un DFU.*

Demostración. Se probará en primer lugar que todo elemento no nulo de A admite una tal factorización. Si $a, b \in A$ son asociados, a admite una factorización en irreducibles si, y solo si, b la admite también. Veamos que el conjunto

$$\mathfrak{S} = \{(a) \subsetneq A \mid 0 \neq a \text{ no admite factorización en irreducibles}\}$$

es vacío. Supongamos que $\mathfrak{S} \neq \emptyset$ y que

$$(a_1) \subset (a_2) \subset \cdots \subset (a_i) \subset \cdots$$

es una cadena de ideales en $\mathfrak{S}$. Entonces $\cup_i(a_i)$ es un ideal propio de A (en otro caso 1 sería un elemento de algún (a_i)) y, por lo tanto, $\cup_i(a_i) = (b)$ ya que A es un DIP. Entonces $b \in (a_i)$ para algún i y así $(b) = (a_i) \in \mathfrak{S}$ con lo cual $\mathfrak{S}$ resulta un conjunto inductivo si no es vacío y, en ese caso, existen elementos maximales en $\mathfrak{S}$ en virtud del Lema de Zorn. Sea (a) maximal en $\mathfrak{S}$, entonces a no es irreducible y existe una factorización $a = bc$ en donde ni b ni c son unidades. Ahora $(a) \subsetneq (b)$ y $(a) \subsetneq (c)$, y por la maximalidad de (a) los elementos b y c admiten sendas factorizaciones en irreducibles cuyo producto es una factorización en irreducibles para a. Por lo tanto, $\mathfrak{S} = \emptyset$ y cada elemento no nulo $a \in A$ admite una factorización en irreducibles.

Sean

$$a = up_1^{r_1}p_2^{r_2}\cdots p_t^{r_t} = vq_1^{s_1}q_2^{s_2}\cdots q_l^{s_l} \quad (*)$$

dos factorizaciones en irreducibles de a. Como (p_1) es un ideal primo de A (2.26), algún q_i es elemento de (p_1). Después de una reordenación, se puede suponer $q_1 \in (p_1)$ y, por tanto, $(q_1) = (p_1)$, por la maximalidad de (q_1). Así p_1 y q_1 son asociados y si $r_1 \geqslant 1$, al ser A dominio de integridad, resulta $up_1^{r_1-s_1}p_2^{r_2}\cdots p_t^{r_t} = v'q_2^{s_2}\cdots q_l^{s_l}$, en donde v' es una unidad. Si $r_1 > s_1$, de la anterior igualdad se deduce como antes que p_1 es asociado a algún q_j con $j \in \{2, 3, \ldots, l\}$, resultando así asociados los irreducibles q_1 y q_j lo cual es contrario a la naturaleza de las factorizaciones. Si $r_1 < s_1$ se tiene $up_2^{r_2}\cdots p_t^{r_t} = v''q_1^{s_1-r_1}q_2^{s_2}\cdots q_l^{s_l}$ (con v'' unidad de A) y de forma análoga se deduce que p_1 es asociado a otro p_i, $i \in \{2, 3, \ldots, t\}$. Por lo tanto, $r_1 = s_1$ y así se obtiene $up_2^{r_2}\cdots p_t^{r_t} = v'q_2^{s_2}\cdots q_l^{s_l}$. Repitiendo el proceso para irreducibles sucesivos se llega a una expresión en la que han desaparecido todos los irreducibles de uno de los dos miembros de la igualdad inicial (*). Ese es el momento final de la prueba ya que ello es solamente posible en el caso de que hayan desaparecido también todos los irreducibles del otro miembro de dicha igualdad, pues de otro modo resultaría que un producto de irreducibles es una unidad. Entonces el número de factores que son potencia de irreducibles es el mismo en las dos factorizaciones y, como se ha visto, los factores irreducibles de una de ellas son asociados a los correspondientes de la otra y aparecen además con los mismos exponentes. □

Definición 2.28. Si A es un dominio de integridad y $a_1, \ldots, a_n \in A$, se dice que d es un *máximo común divisor* de los elementos $a_1, \ldots, a_n$, y se escribirá $d = mcd(a_1, \ldots, a_n)$ si verifica:

1) $d \mid a_i$, $\forall i \in \{1, \ldots, n\}$, y además

2) si $c \in A$ es tal que $c \mid a_i$ $\forall i \in \{1, \ldots, n\}$, entonces $c \mid d$.

Se dirá que a,$b \in A$ son primos entre sí (o que a y b son coprimos) si $1 = mcd(a, b)$

Obsérvese que un máximo común divisor, si existe, está definido salvo unidades, es decir, que $d = mcd(a_1, \ldots, a_n) \Leftrightarrow du = mcd(a_1, \ldots, a_n), \forall u \in A^*$.

Proposición 2.29. *Si A es un DIP, $a_1, \ldots, a_n \in A$ y $d = mcd(a_1, \ldots, a_n)$, entonces $(d) = (a_1) + \cdots + (a_n) = (a_1, \ldots, a_n)$.*

Demostración. El ideal $(a_1) + \cdots + (a_n) = (a_1, \ldots, a_n)$ está generado por un elemento $d \in A$ ya que el anillo A es un DIP, y entonces $(a_1), \ldots, (a_n) \subset (d)$ o, lo que es lo mismo, $a_i \in (d)$, $\forall i \in \{1, \ldots, n\}$; es decir, $d \mid a_i$ $\forall i \in \{1, \ldots, n\}$. Si $c \in A$, la condición $c \mid a_i$ $\forall i \in \{1, \ldots, n\}$ equivale a que $a_i \in (c)$ $\forall i \in \{1, \ldots, n\}$, y en ese caso se tiene $(d) = (a_1) + \cdots + (a_n) \subset (c)$, es decir, $c \mid d$. □

Corolario 2.30. *(Teorema de Bézout) Si A es un DIP y $a, b \in A$, entonces a y b son coprimos si, y solo si, existen $r, s \in A$ tales que $1 = ra + sb$.*

Definición 2.31. Si A es un dominio de integridad y $a_1, \ldots, a_n \in A$ se dice que m es un mínimo común múltiplo de $a_1, \ldots, a_n$, y se escribirá $m = mcm(a_1, \ldots, a_n)$, si

1) $a_i \mid m$, $\forall i \in \{1, \ldots, n\}$, y además,

2) si $c \in A$ es tal que $a_i \mid c$ $\forall i \in \{1, \ldots, n\}$, entonces $m \mid c$.

Proposición 2.32. *Si A es un DIP, $a_1, \ldots, a_n \in A$ y $m = mcm(a_1, \ldots, a_n)$, entonces $(m) = \cap_{i=1}^{n}(a_i)$.*

Demostración. El ideal $\cap_{i=1}^{n}(a_i)$ está generado por un elemento $m \in A$ ya que el anillo A es un DIP. Además $\cap_{i=1}^{n}(a_i)$ está constituido por los elementos de A que son múltiplos de a_i $\forall i \in \{1, \ldots, n\}$, por lo que un elemento de A es múltiplo de a_i, $\forall i \in \{1, \ldots, n\}$ si, y solo si, es múltiplo de m. □

Obsérvese que, como en el caso del máximo común divisor, el mínimo común múltiplo está determinado salvo unidades.

Recuérdese que si A es un DE con aplicación euclídea $\partial\colon A\setminus\{0\}\to\mathbb{Z}^+$, existe un algoritmo para el cálculo del máximo común divisor de $D,d\in A$.

Si $D=dq+d_1$ con $\partial(d_1)<\partial(d)$ o bien $d_1=0$, en cuyo caso $mcd(D,d)=d$ y se habrá finalizado ya. Si no es así, de nuevo $d=d_1q_1+d_2$ con $\partial(d_2)<\partial(d_1)<\partial(d)$ o $d_2=0$. Recurrentemente se construyen $d_{i-1}=d_iq_i+d_{i+1}$ con $\partial(d_{i+1})<\partial(d_i)<\cdots<\partial(d_1)<\partial(d)$ y existe entonces un t tal que $d_t=0$. Si d_t es el primer resto nulo, entonces $d_{t-1}=mcd(D,d)$. La prueba consiste en observar que $(D,d)=(d,d_1)=(d_1,d_2)=\cdots=(d_{t-2},d_{t-1})=(d_{t-1})$.

2.3. Anillos de Polinomios

Dedicaremos ahora nuestra atención a recordar algunas cuestiones sobre anillos de polinomios. No se darán demostraciones de resultados que supondremos ya conocidos.

Si S es un conjunto (el conjunto de indeterminadas) denotaremos con $\mathbb{N}\langle S\rangle$ el monoide conmutativo libre sobre S cuyos elementos son las aplicaciones $\nu\colon S\to\mathbb{N}$ de soporte finito (es decir, tales que $\nu(X)=0$, para casi todo $X\in S$). En el monoide $\mathbb{N}\langle S\rangle$ la operación (multiplicación) está definida por

$$(\nu\mu)(X):=\nu(X)+\mu(X),\forall X\in S,$$

y, si $X\in S$ y n es un número natural, se denota con $X^n\in\mathbb{N}\langle S\rangle$ la aplicación $\nu\colon S\to\mathbb{N}$ tal que $\nu(X)=n$ y $\nu(Y)=0$, para todo $Y\in S\setminus\{X\}$. Con esta notación y con la definición de producto en $\mathbb{N}\langle S\rangle$, se tiene que

$$X^nX^m=X^{n+m}\ \text{ y que } X^0=e,\ \forall X\in S,$$

donde e es el neutro de $\mathbb{N}\langle S\rangle$, es decir, la aplicación constante $e(X)=0,\forall X\in S$. Si $X_1,X_2,\ldots,X_r\in S$, la aplicación $\nu=X_1^{n_1}X_2^{n_2}\cdots X_r^{n_r}:S\to\mathbb{N}$ es tal que $\nu(X_i)=n_i$, para $i=1,2,\ldots,r$, y $\nu(Y)=0$ para todo $Y\notin\{X_1,X_2,\ldots,X_r\}$. Obsérvese que cada $\nu\in\mathbb{N}\langle S\rangle$ admite una única expresión $\nu=\prod_{X\in S}X^{\nu(X)}$ (en la que casi todos los factores son iguales a e, los correspondientes a aquellos $X\in S$ para los cuales $\nu(X)=0$) como consecuencia de la finitud del soporte de cada $\nu\in\mathbb{N}\langle S\rangle$. A los elementos de $\mathbb{N}\langle S\rangle$ se les denominará *monomios* en S.

Si ahora A es un anillo conmutativo y N un monoide (multiplicativo) conmutativo denotaremos con $A[N]$ el A-módulo libre de base N. Los elementos de $A[N]$ son las aplicaciones $f\colon N\to A$ también de soporte finito (es decir, tales que $f(\nu)=0$ para casi todo $\nu\in N$). Si $\nu\in N$ y $a\in A$ se denota con $a\nu$ al elemento $f\in A[N]$ tal que $f(\nu)=a$ y $f(\mu)=0$, para todo $\mu\in N$, $\mu\neq\nu$. La suma en $A[N]$, que dota a $A[N]$ de estructura de grupo abeliano, está definida por

$$(f+g)(\nu):=f(\nu)+g(\nu),$$

y el producto por elementos de A mediante

$$(af)(\nu) := af(\nu), \text{ para } a \in A \text{ y } \nu \in N.$$

Es fácil comprobar que con estas operaciones $A[N]$ satisface todas las condiciones necesarias para ser el A-módulo libre sobre N. Cada elemento $f \in A[N]$ tiene una única expresión

$$f = \sum_{\nu \in N} f(\nu)\nu$$

con solamente un número finito de sumandos no nulos (es decir, $f(\nu) = 0$, para casi todo $\nu \in N$). Nótese que el 0 de $A[N]$ es el elemento 0ν, para cualquier $\nu \in N$.

El A-módulo libre $A[N]$ tiene además estructura de anillo conmutativo como consecuencia de que N es monoide conmutativo. En efecto, se define una multiplicación en $A[N]$ mediante:

$$(fg)(\gamma) := \sum_{\mu\nu=\gamma} f(\nu)\, g(\mu),$$

expresión en la que solamente hay un número finito de sumandos no nulos, ya que casi todos los $f(\nu)$ y casi todos los $g(\mu)$ son nulos. El elemento neutro de este producto es la aplicación de $N \to A$ que con nuestra notación se escribirá $1e$ (en donde e es el elemento neutro de N, y 1 es el de la multiplicación de A). Este elemento se denotará con $1 = 1e$. Se comprobará que $A[N]$ es un anillo conmutativo y que la aplicación $\varphi\colon A \to A[N]$, definida por $\varphi(a) = ae$, es homomorfismo de anillos.

Si ahora se toma $N = \mathbb{N}\langle S\rangle$, al anillo $A[\mathbb{N}\langle S\rangle]$ se le denotará con $A[S]$ y se le llamará *anillo de polinomios con indeterminadas en* S (o sobre S) *y coeficientes en* A. Cada elemento tiene ahora una única expresión

$$f = \sum_{\nu \in \mathbb{N}\langle S\rangle} a_\nu \nu = \sum_{\nu \in \mathbb{N}\langle S\rangle} a_\nu \prod_{X \in S} X^{\nu(X)} \qquad (*),$$

en donde se ha puesto $a_\nu = f(\nu)$ y, por supuesto, $a_\nu = 0$ para casi todo $\nu \in \mathbb{N}\langle S\rangle$. Esta expresión se puede hacer más explícita teniendo en cuenta que en ella solamente intervienen un número finito de sumandos no nulos y un número finito de expresiones X^ν diferentes de e (ahora $e = X^0$ para cualquier $X \in S$)

$$f = \sum_{\nu \in \mathbb{N}\langle S\rangle} a_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \quad (**).$$

Las $X_1, \ldots, X_n \in S$ son las variables que intervienen de modo efectivo (es decir, con algún exponente no nulo) en alguno de los sumandos de (*). En aquellos sumandos de (*) en las que no interviene, X_i aparecerá elevada a exponente 0 en el correspondiente sumando de (**). La expresión (**) es ya más familiar y el elemento f es un polinomio con coeficientes en A y con indeterminadas en S.

Proposición 2.33. *La aplicación* $\lambda\colon S \to A[S]$ *definida por* $\lambda(X) = 1X^1$ *y el homomorfismo* $\varphi\colon A \to A[S]$ *definido por* $\varphi(a) = ae$ *verifican la siguiente propiedad*

universal: si $\psi\colon A \to B$ *es un homomorfismo de anillos conmutativos y* $\chi\colon S \to B$ *es una aplicación, entonces existe un único homomorfismo de anillos* $\psi^{\chi}\colon A[S] \to B$ *tal que* $\psi^{\chi} \circ \lambda = \chi$ *y* $\psi^{\chi} \circ \varphi = \psi$ *(propiedad universal del anillo de polinomios* $A[S]$ *).*

Demostración. Utilizando la naturaleza de monoide conmutativo libre de $N\langle S\rangle$ y la de A-módulo libre de $A[S]$ se encuentra el homomorfismo de A-módulos $\psi^{\chi}\colon A[S] \to B$ definido mediante

$$\psi^{\chi}\Big(\sum_{\nu\in\mathbb{N}\langle S\rangle} a_{\nu}\prod_{X\in S} X^{\nu(X)}\Big) = \sum_{\nu\in\mathbb{N}\langle S\rangle} \psi(a_{\nu})\prod_{X\in S}[\lambda(X)]^{\nu(X)},$$

y es muy fácil probar que es homomorfismo de anillos. □

El homomorfismo ψ^{χ} será denominado evaluación en χ.

Si ahora S es el conjunto finito $S = \{X_1, \ldots, X_n\}$ se escribirá $A[S] = A[X_1, \ldots, X_n]$ y cada polinomio en las variables $X_1, \ldots, X_n$ con coeficientes en A, es decir cada $f \in A[X_1, \ldots, X_n]$, tiene una expresión canónica

$$f = \sum_{(\nu)=(\nu_1,\ldots,\nu_n)} a_{\nu_1,\ldots,\nu_n} X_1^{\nu_1}\cdots X_n^{\nu_n}$$

con $(\nu) = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$ y $a_{\nu_1,\ldots,\nu_n} \in A$ casi todos nulos. Cada $X_1^{\nu_1}\cdots X_n^{\nu_n}$ es un monomio y la canonicidad de la expresión anterior indica que los coeficientes están determinados de modo único por los monomios cuando se han escrito solamente monomios diferentes. No se olvide que el conjunto de los monomios es una base de $A[X_1, \ldots, X_n]$ como A-módulo libre. Diferentes expresiones no canónicas de f pueden ser obtenidas a partir de la canónica descomponiendo uno o varios de sus coeficientes en suma de nuevos elementos de A.

Definición 2.34. Para un monomio $M_{(\upsilon)}(X_1, \ldots, X_n) = X_1^{\nu_1}\cdots X_n^{\nu_n}$ se define el grado como el entero $\partial(M_{(\upsilon)}) = \nu_1 + \cdots + \nu_n$. Para el polinomio $f = \sum_{(\nu)=(\nu_1,\ldots,\nu_n)} a_{\nu_1,\ldots,\nu_n} M_{(\upsilon)}$ se define el *grado* como $\partial(f) = \max_{a_{(\upsilon)}\neq 0} \partial\left(M_{(\upsilon)}\right)$. Un polinomio se dice que es *homogéneo* si todos sus monomios (es decir, aquellos que aparecen en su expresión canónica con coeficiente no nulo) tienen el mismo grado.

Observación 2.35. Si A es subanillo del anillo B se puede considerar $A[S]$ como subanillo de $B[S]$. En efecto, a partir de $\chi = id_S$ y de $\psi\colon A \hookrightarrow B$ la inclusión, el homomorfismo $\psi^{\chi}\colon A[S] \to B[S]$ obtenido como en (2.33) es inyectivo.

Si $S \subset T$ es una inclusión de conjuntos y A es anillo conmutativo resulta también una inclusión de anillos $A[S] \subset A[T]$. Además si $T = S \sqcup L$, entonces $A[T] = A[S][L]$. En particular, $A[X,Y] = A[X][Y]$.

2.4. Factorización de polinomios

La mayor parte de estas notas se dedicarán a estudiar cuestiones que conciernen a polinomios en una variable, es decir, elementos de $A[X]$ y, frecuentemente, A será además un cuerpo.

Definición 2.36. Si $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ con $a_n \neq 0$, entonces $\partial(f) = n$ es el *grado* de f y a_n es su *coeficiente principal*; a_0 será llamado *término independiente* de f. El polinomio f se dirá que es *mónico* si su coeficiente principal es 1. Los polinomios no nulos de grado cero son identificados con las constantes, es decir, los elementos de A no nulos.

Si $f = \sum_{i=0}^{r} a_iX^i$ y $g = \sum_{j=0}^{s} b_jX^j$ son polinomios con coeficientes en cualquier dominio de integridad K y con $a_r \neq 0 \neq b_s$ (es decir, $\partial(f) = r$ y $\partial(g) = s$), entonces $\partial(fg) = r + s$, pues $a_rb_s \neq 0$ y

$$fg = \sum_{k=0}^{r+s} \Big(\sum_{i+j=k} a_ib_j \Big) X^k.$$

Si K es un cuerpo y $f = aX + b \in K[X]$ es un polinomio lineal (es decir, de grado 1) entonces f es irreducible. En efecto, las unidades de $K[X]$ son los polinomios de grado 0, y una factorización $f = gh$, con $g, h \in K[X]$, proporciona $\partial(g) = 0$ o $\partial(h) = 0$, en virtud de lo anterior

Proposición 2.37 (Algoritmo de la división de polinomios)**.** *Si A es un anillo conmutativo, $f, g \in A[X]$ son polinomios no nulos y el coeficiente principal de g es una unidad de A, entonces existen únicos $q, r \in A[X]$ tales que*

$$f = gq + r \text{ con } \partial r < \partial g, \text{ si } r \neq 0.$$

Se dice que q y r son, respectivamente, cociente y resto de la división del polinomio f entre el polinomio g.

Demostración. Se puede suponer $\partial(f) \geqslant \partial(g)$ pues de lo contrario bastará tomar $q = 0$ y $r = f$.

Sean entonces $f = a_n X^n + \cdots + a_1 X + a_0$ y $g = b_m X^m + \cdots + b_1 X + b_0$ con $b_m \in U(A)$, $a_n \neq 0$ y $n \geqslant m$. Poniendo $h_1 = a_n b_m^{-1} X^{n-m}$ se tiene que el polinomio

$$f_1 = f - gh_1 = c_{r_1} X^{r_1} + \text{ términos de menor grado,}$$

es de grado $r_1 < n$ o el polinomio nulo. Si $f_1 \neq 0$ y $r_1 \geqslant m$ tomemos $h_2 = c_{r_1} b_m^{-1} X^{r_1 - m}$ y pongamos

$$f_2 = f_1 - gh_2 = d_{r_2} X^{r_2} + \text{ términos de menor grado}$$

que es de grado $r_2 < r_1$ si no es el polinomio nulo. Obsérvese que $f = f_1 + gh_1 = f_2 + gh_2 + gh_1 = g(h_1 + h_2) + f_2$. Se reitera el proceso obteniendo polinomios f_i de grados descendentes $r_i < r_{i-1} < \cdots < r_2 < r_1 < n$, proceso que se interrumpe al llegar a un polinomio $f_t = 0$ o con $\partial(f_t) < m$. Se tiene $f = g(h_1 + h_2 + \cdots + h_t) + f_t$, y así basta entonces con poner $q = h_1 + h_2 + \cdots + h_t$ y $r = f_t$.

Si $f = q'g + r' = qg + r$ también con $\partial(r') \leqslant \partial(g)$, se tiene $(q - q')g = r - r'$. Como g no es divisor de cero en $A[X]$ al tener coeficiente principal una unidad de A, entonces $q = q'$ si, y solo si, $r = r'$. Si fuese $q - q' \neq 0$, se tendría, $\partial(g) < \partial\left[g(q - q')\right] = \partial(r - r') \leqslant máx\{\partial(r), \partial(r')\}$ ya que el coeficiente principal de g es una unidad. Resultaría así $\partial(g) < máx\{\partial(r), \partial(r')\}$, lo cual no es posible. Por tanto, $q = q'$ y así también $r = r'$. □

Si K es un cuerpo, la aplicación $\partial\colon K[X] \setminus \{0\} \to \mathbb{Z}^+$, que satisface las condiciones de (2.18), proporciona al anillo de polinomios $K[X]$ la estructura de dominio euclídeo. Por lo tanto, $K[X]$ es un dominio de ideales principales y entonces un dominio de factorización única (2.27). Las unidades del anillo $K[X]$ son los elementos no nulos de K y cada polinomio $f(X) \in K[X]$ admite una expresión $f = p_1^{r_1} \cdots p_t^{r_t}$ (esencialmente única) como producto de factores irreducibles en $K[X]$.

Recíprocamente, si para un anillo conmutativo A el anillo de polinomios $A[X]$ es un DIP, entonces A es un cuerpo. El homomorfismo $h\colon A[X] \to A$ consistente en la evaluación en $0 \in A$, es decir, $h(f) = f(0)$ para $f \in A[X]$, es sobreyectivo ($a = h(a)$, $\forall a \in A$) y tiene por núcleo el ideal (X) ($h(f) = f(0) = 0 \Leftrightarrow X$ divide a f). Por lo tanto, $A \simeq A[X]/(X)$. Ahora, en el caso de que $A[X]$ es un DIP el anillo A es un cuerpo ya que el ideal (X) es maximal, pues X es irreducible y se aplica (2.26). Para probar la irreducibilidad de X obsérvese que A es dominio de integridad al ser subanillo de $A[X]$ y, como ya se ha dicho, $A \simeq A[X]/(X)$. En particular, $\mathbb{Z}[X]$ no es un DIP.

Definición 2.38. Los elementos irreducibles en el DFU $K[X]$ se llamarán *polinomios irreducibles* en $K[X]$ (también se dirá que son irreducibles sobre K). Los polinomios no irreducibles se dirá que son *reducibles*.

Como $K[X]$ es un DIP si K es un cuerpo, se obtiene de forma inmediata un importante

Corolario 2.39. *Si K es un cuerpo y $f \in K[X]$, son equivalentes las afirmaciones*

i) (f) *es ideal primo de* $K[X]$.

ii) f *es irreducible en* $K[X]$.

iii) (f) *es ideal maximal de* $K[X]$.

Demostración. Es consecuencia inmediata de (2.26) □

Definición 2.40. Sean A un subanillo de B, $b \in B$, $\psi\colon A \to B$ la inclusión y la aplicación $b\colon \{X\} \to B$ definida por $b(X) = b$, el único homomorfismo obtenido por la propiedad universal del anillo de polinomios (2.33), $\psi^b\colon A[X] \to B$, se denominará evaluación en b, y para cada $f \in A[X]$ el elemento $\psi^b(f) := f(b)$ será el valor numérico de f en b. Se dirá que $b \in B$ es un *cero*, o una *raíz*, de $f \in A[X]$ si $f(b) = 0$.

Proposición 2.41. *(Teorema del resto)*

Sean A un anillo conmutativo, $f \in A[X]$ un polinomio no nulo y $\alpha \in A$. El resto de la división de f entre $X - \alpha$ es $f(\alpha)$.

Demostración. Como el coeficiente principal de $X - \alpha$ es unidad en A, existen únicos $q, r \in A[X]$ tales que $f = (X - \alpha)q + r$, con $\partial r < \partial(X - \alpha) = 1$ (si $r \neq 0$). Como la evaluación en α es un homomorfismo, se tiene que $f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Pero $\partial r = 0$, es decir, $r \in A$ y, por lo tanto, $r(\alpha) = r = f(\alpha)$. □

Corolario 2.42. *(Teorema del factor)*

Sea A un anillo conmutativo, $f \in A[X]$ un polinomio no nulo y $\alpha \in A$. Entonces $X - \alpha$ divide a f en $A[X]$ si, y solamente si, α es un cero de f.

El anterior corolario admite una generalización en el caso de que A sea un dominio de integridad.

Proposición 2.43. *Si A es un dominio de integridad, $f \in A[X]$ es un polinomio no nulo y $\alpha_1, \ldots, \alpha_r \in A$ son ceros distintos de f, entonces el polinomio $\prod_{i=1}^{r} (X - \alpha_i)$ divide a f en $A[X]$.*

Demostración. Por inducción en r. Para $r = 1$ es el Teorema del factor. Supuesto $r > 1$ y que el resultado es válido para $r - 1$ el polinomio $\prod_{i=1}^{r-1} (X - \alpha_i)$ divide a f en $A[X]$, es decir,

$$f = q \prod_{i=1}^{r-1} (X - \alpha_i)$$

para un $q \in A[X]$. Como A es dominio de integridad

$$f(\alpha_r) = q(\alpha_r) \prod_{i=1}^{r-1} (\alpha_r - \alpha_i) = 0$$

implica $q(\alpha_r) = 0$, que por el Teorema del factor proporciona $q = (X - \alpha_r) h$ para un cierto $h \in A[X]$. Se tiene así

$$f = h \prod_{i=1}^{r} (X - \alpha_i). \qquad \square$$

Corolario 2.44. *Si A es un dominio de integridad y $f \in A[X]$ es un polinomio de grado $n \geqslant 0$, entonces*

1) El número de ceros diferentes de f en A es a lo sumo n.

2) Si f tiene n ceros diferentes $\alpha_1, \ldots, \alpha_n \in A$, entonces

$$f = c(X - \alpha_1) \cdots (X - \alpha_n),$$

en donde $c \in A$ es el coeficiente principal de f.

Demostración. 1) Si $\alpha_1, \ldots, \alpha_r \in A$ son los ceros distintos de f en A

$$f = h \prod_{i=1}^{r} (X - \alpha_i),$$

con $h \in A[X]$ por el corolario anterior. Como A es dominio de integridad $n = \partial(f) = \partial(h) + \partial\Big(\prod_{i=1}^{r} (X - \alpha_i)\Big) = \partial(h) + r \geqslant r$.

2) Como consecuencia de 1)

$$f = h \prod_{i=1}^{n} (X - \alpha_i),$$

con $\partial(h) = 0$, es decir, $h = c \in A$ es el coeficiente principal de f. $\square$

Los anteriores resultados no son válidos si A no es un dominio de integridad. Por ejemplo, $\overline{1}, \overline{3}, \overline{5} \in \mathbb{Z}_6$ son ceros distintos del polinomio $f = \overline{3}X + \overline{3} \in \mathbb{Z}_6[X]$.

En relación con la estructura de dominio euclídeo de $K[X]$ es importante poder disponer de criterios que permitan averiguar si un polinomio dado es irreducible. Obsérvese, en primer lugar, que todo polinomio lineal $f = aX + b \in K[X]$ es irreducible en $K[X]$. El recíproco no es cierto en general como establece la siguiente Proposición.

Proposición 2.45. *Si K es un cuerpo son equivalentes las afirmaciones:*

i) Todo polinomio irreducible en $K[X]$ es lineal.

ii) Todo $f \in K[X]$ con $\partial(f) \geqslant 1$ tiene al menos un cero en K.

Demostración. *i)* $\Rightarrow$ *ii)* Sea $f \in K[X]$ con $\partial(f) \geqslant 1$, y sea $f = f_1 \cdots f_r$ la factorización de f en irreducibles ($K[X]$ es un DFU), que por hipótesis son lineales. Cada $f_i = a_i X + b_i$ admite como cero a $-b_i a_i^{-1} \in K$, que también es un cero de f.

ii) $\Rightarrow$ *i)* Si $f \in K[X]$ y si $\partial(f) > 1$, f admite un cero $\alpha \in K$, en virtud de la hipótesis, y es divisible por $X - \alpha$ en $K[X]$ (2.42), es decir, $f = (X - \alpha)g$ con $\partial(g) = \partial(f) - 1 > 0$. Los polinomios $X - \alpha$ y g no son unidades de $K[X]$, al ser de grado mayor que cero, y entonces f no es irreducible. □

Los cuerpos que satisfacen las condiciones de la Proposición anterior se dice que son *algebraicamente cerrados*.

Como se ve, la naturaleza del cuerpo de coeficientes también incide en la posible irreducibilidad de un polinomio. Se demostrará (5.16) que todo polinomio no constante con coeficientes en $\mathbb{C}$ se descompone en factores lineales en $\mathbb{C}[X]$. Según esto los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los lineales, sin embargo un polinomio no lineal $f \in \mathbb{R}[X]$ puede ser irreducible en $\mathbb{R}[X]$ (basta tomar $f = aX^2 + bX + c$ con $\triangle(f) = b^2 - 4ac < 0$ (2.46)).

Proposición 2.46. *Si K es un cuerpo y $f \in K[X]$ con $\partial(f) = 2$ o $\partial(f) = 3$, entonces f irreducible en $K[X]$ si, y solo si, f no tiene ceros en K.*

Demostración. Si $f = gh$ es una factorización en $K[X]$ y ambos factores son no constantes entonces necesariamente alguno de ellos es lineal y, por tanto, tiene un cero en K.

Recíprocamente, si f tiene un cero α en K, f es divisible por $X - \alpha$ (2.42) y el cociente es de grado al menos 1, por lo que f resulta factorizado en no unidades de $K[X]$. □

Observación 2.47. Solamente con objeto de facilitar la formulación de ejemplos y ejercicios, admitiremos por el momento como verdadero el resultado que afirma que todo polinomio no constante con coeficientes números reales tiene al menos un cero complejo. Esto es consecuencia del Teorema fundamental del Álgebra que será probado más adelante en (5.16).

Proposición 2.48. *Los polinomios irreducibles en* $\mathbb{R}[X]$ *son de grado 1 o 2. Un polinomio* $f = aX^2 + bX + c \in \mathbb{R}[X]$ *, con* $a \neq 0$*, es irreducible en* $\mathbb{R}[X]$ *si, y solo si,* $\triangle(f) = b^2 - 4ac < 0$.

Demostración. Si $f \in \mathbb{R}[X]$ y $\alpha = a + bi \in \mathbb{C} \setminus \mathbb{R}$ es un cero de f, entonces $\overline{\alpha} = a - bi$ también lo es. La conjugación

$$(-) : \mathbb{C} \to C$$
$$\alpha = a + bi \mapsto \overline{\alpha} = a - bi$$

es un automorfismo y $\overline{a} = a$ para todo $a \in \mathbb{R}$.

Si $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{R}[X]$, se tiene $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$, y entonces

$$0 = \overline{0} = \overline{f(\alpha)} = \overline{a_n\alpha^n + \cdots + a_1\alpha + a_0} = \overline{a_n\alpha}^n + \cdots + \overline{a_1\alpha} + \overline{a_0}$$
$$= a_n\overline{\alpha}^n + \cdots + a_1\overline{\alpha} + a_0 = f(\overline{\alpha}).$$

Si f es irreducible en $\mathbb{R}[X]$ y no lineal, entonces f es divisible en $\mathbb{C}[X]$ por el polinomio $(X - \alpha)(X - \overline{\alpha})$ pues f admite al menos un cero complejo no real, α, ya que en otro caso f no sería irreducible en $\mathbb{R}[X]$.

Como el polinomio $(X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha}$ tiene coeficientes reales, se tiene necesariamente $f = c(X - \alpha)(X - \overline{\alpha})$ con $c \in \mathbb{R}$. □

Proposición 2.49. *Si* $f \in \mathbb{R}[X]$ *es de grado impar, entonces* f *admite, al menos, un cero real.*

Demostración. Cada cero $\alpha \in \mathbb{C} \setminus \mathbb{R}$ de f determina que f es divisible en $\mathbb{C}[X]$ por $(X - \alpha)(X - \overline{\alpha})$ y, por tanto, existe un $g \in \mathbb{C}[X]$ tal que $f = g(X - \alpha)(X - \overline{\alpha})$.

Como $(X-\alpha)(X-\overline{\alpha})$ tiene sus coeficientes reales lo mismo le sucede a g (unicidad del cociente y del resto de la división euclídea en $\mathbb{C}[X]$ (2.37)). Reiterando el proceso, resulta que si f no tiene ninguna raíz real entonces

$$f = c\prod_{i=1}^{m}\left[X^2-(\alpha_i+\overline{\alpha_i})X+\alpha_i\overline{\alpha_i}\right],$$

donde c es el coeficiente principal de f y los α_i son complejos no reales. Por lo tanto, si $f\in\mathbb{R}[X]$ no tiene ceros reales su grado es par. □

El estudio de la irreducibilidad en $\mathbb{Q}[X]$ es considerablemente más complicado. De hecho veremos que existen polinomios irreducibles de cualquier grado (2.61). Nuestro próximo objetivo es establecer ciertos criterios que permitirán reconocer la irreducibilidad de algunos polinomios con coeficientes racionales. No serán criterios que permitan decidir sobre la irreducibilidad de cualquier polinomio, pero serán muy útiles.

Definición 2.50. Si $f=\sum_0^n a_iX^i\in\mathbb{Z}[X]$ es no nulo, se define el contenido de f como

$$cont(f) := mcd(a_0,\ldots,a_n).$$

Se dirá que f es primitivo si $cont(f)=1$.

Observación 2.51. Sea $0\neq f=a_nX^n+\cdots+a_0\in\mathbb{Z}[X]$. Entonces:

a) Si $0\neq a\in\mathbb{Z}$ se tiene

$$cont(af)=a\,cont(f)$$

b) Existe un polinomio primitivo $g\in\mathbb{Z}[X]$ con $\partial(f)=\partial(g)$ tal que $f=cont(f)g$.

En efecto, basta con considerar que si $f=a_nX^n+\cdots+a_1X+a_0$ y $c=cont(f)$, el polinomio $g=\dfrac{a_n}{c}X^n+\cdots+\dfrac{a_1}{c}X+\dfrac{a_0}{c}\in\mathbb{Z}[X]$ satisface los condiciones exigidas.

Recíprocamente si $0\neq f\in\mathbb{Z}[X]$ es tal que $f=cf_1$, con $f_1\in\mathbb{Z}[X]$ primitivo, entonces $c=cont(f)$.

c) Si p es un número primo y $\varphi_p\colon\mathbb{Z}\to\mathbb{Z}_p$ es el homomorfismo canónico, la propiedad universal del anillo de polinomios (2.33) permite obtener el homomorfismo $\overline{\varphi_p}\colon\mathbb{Z}[X]\to\mathbb{Z}_p[X]$ definido para $h=\sum_0^n a_iX^i$ mediante $\overline{\varphi_p}(h)=\overline{h}:=\sum_0^n\overline{a_i}X^i$. El homomorfismo $\overline{\varphi_p}$ recibirá el nombre de *homomorfismo de reducción módulo p*.

Como el polinomio $h=\sum_0^n a_iX^i\in\mathbb{Z}[X]$ es primitivo si, y solo si, sus coeficientes a_i no tienen ningún divisor primo común, entonces para cada número primo p existe un

$i \in \{0, 1, \ldots, n\}$ tal que p no divide a a_i. Se puede afirmar así que: h es primitivo si, y solo si, $\overline{\varphi_p}(h) \neq 0$ para todo primo p.

Proposición 2.52. *(Lema de Gauss)*

Si $f, g \in \mathbb{Z}[X]$ son polinomios primitivos entonces su producto fg es primitivo también.

Demostración. Para cada primo p se tiene que $\overline{\varphi_p}(fg) = \overline{\varphi_p}(f)\overline{\varphi_p}(g) \neq 0$, ya que f y g son primitivos (2.51) c) y $\mathbb{Z}_p[X]$ es un dominio de integridad. □

Corolario 2.53. *Si $f, g \in \mathbb{Z}[X]$, entonces $cont(fg) = cont(f)cont(g)$.*

Demostración. Por (2.51) b) Se puede escribir $f = cont(f)f_1$, $g = cont(g)g_1$, con f_1 y g_1 polinomios primitivos, y por (2.51) a) se tiene que

$$cont(fg) = cont(f)cont(g)cont(f_1g_1) = cont(f)cont(g).$$

en virtud del Lema de Gauss. □

Lema 2.54. *Sea $f \in \mathbb{Z}[X]$. Si f admite una factorización $f = gh$ con $g, h \in \mathbb{Q}[X]$, entonces existen $g_1, h_1 \in \mathbb{Z}[X]$ con $\partial(g) = \partial(g_1)$, $\partial(h) = \partial(h_1)$ y tales que $f = g_1h_1$.*

Demostración. Para la factorización $f = gh$ con $f, g \in \mathbb{Q}[X]$ seleccionamos $c, d \in \mathbb{Z}$ tales que $cg = g', dh = h'$ son polinomios con coeficientes enteros y, por lo tanto, $cdf = g'h'$ y $\partial(g) = \partial(g')$ y $\partial(h) = \partial(h')$. Existe entonces un entero $n \geqslant 1$ tal que $nf = g'h'$ con $g', h' \in \mathbb{Z}[X]$ y con $\partial(g) = \partial(g')$ y $\partial(h) = \partial(h')$. El conjunto de números naturales m para los cuales existen $g_m, h_m \in \mathbb{Z}[X]$ con $\partial(g) = \partial(g_m)$, $\partial(h) = \partial(h_m)$ y tales que $mf = g_mh_m$ es, por tanto, no vacío y admite entonces un primer elemento (el orden natural es un buen orden para $\mathbb{N}$). Sea t el menor número natural tal que existen $g_t, h_t \in \mathbb{Z}[X]$ con $\partial(g) = \partial(g_t)$, $\partial(h) = \partial(h_t)$ y con $tf = g_th_t$. Probaremos que $t = 1$ con lo que el Lema quedará demostrado.

En efecto, si $t \neq 1$ existe un número primo p tal que $t = pr$, con $r < t$ otro número natural. El número primo p no es divisor de todos los coeficientes de g_t ni de todos los coeficientes de h_t, ya que si p divide a todos los coeficientes de g_t existe un

$g_2 \in \mathbb{Z}[X]$ con $\partial(g_2) = \partial(g_t)$ y con $g_t = pg_2$, con lo cual resulta $prf = pg_2h_t$ y, por tanto, $rf = g_2h_t$, lo que contradice la minimalidad de t. Lo mismo sucede si se supone que p divide a todos los coeficientes de h_t. Ahora utilizando la reducción módulo p se tiene $\overline{\varphi_p}(tf) = \overline{\varphi_p}(g_t)\overline{\varphi_p}(h_t) = 0$ en $\mathbb{Z}_p[X]$ ya que tf tiene sus coeficientes múltiplos de p. Como $\mathbb{Z}_p[X]$ es dominio de integridad resulta $\overline{\varphi_p}(g_t) = 0$ o $\overline{\varphi_p}(h_t) = 0$, lo que contradice la afirmación ya probada de que p no divide a todos los coeficientes de g_t ni de h_t. □

Teorema 2.55. *Sea $f \in \mathbb{Z}[X]$ con $\partial(f) \geqslant 1$. Son equivalentes las afirmaciones*

i) Si f es irreducible en $\mathbb{Z}[X]$.

ii) Si f es primitivo e irreducible en $\mathbb{Q}[X]$.

Demostración. $i) \Rightarrow ii)$

Si f es irreducible en $\mathbb{Z}[X]$, de $f = cont(f)f_1$ se obtiene $cont(f) = 1$. Supongamos que $f = gh$, siendo $g, h \in \mathbb{Q}[X]$. Por el Lema 2.54 existen $g_1, h_1 \in \mathbb{Z}[X]$ con $\partial(g) = \partial(g_1)$, $\partial(h) = \partial(h_1)$ y tales que $f = g_1h_1$. De la irreducibilidad de f en $\mathbb{Z}[X]$ se obtiene que $g_1 = \pm 1$ o $h_1 = \pm 1$, y así $\partial(g) = \partial(g_1) = 0$ o bien $\partial(h) = \partial(h_1) = 0$, es decir, uno de los factores g o h es una unidad en $\mathbb{Q}[X]$.

$ii) \Rightarrow i)$

Si f es irreducible en $\mathbb{Q}[X]$ y si $f = gh$ con $g, h \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$, necesariamente uno de los factores g o h es una unidad en $\mathbb{Q}[X]$ y entonces un número entero. Si $g = c \in \mathbb{Z}$ entonces $f = ch$ y, como $1 = cont(f) = cont(ch) = ccont(h)$, resulta $g = c = \pm 1$, es decir, g es una unidad en $\mathbb{Z}[X]$. □

Obsérvese que se ha probado que para polinomios primitivos la irreducibilidad sobre $\mathbb{Z}$ es equivalente a la irreducibilidad sobre $\mathbb{Q}$.

La condición de que f es primitivo es fundamental en la afirmación anterior. El polinomio $f = 2X + 4$ es irreducible en $\mathbb{Q}[X]$ y no lo es en $\mathbb{Z}[X]$.

El anillo $\mathbb{Z}[X]$ no es un DIP sin embargo es un DFU. Como consecuencia del resultado anterior se tiene el

Corolario 2.56. *$\mathbb{Z}[X]$ es un DFU. Sus elementos irreducibles son números primos o polinomios primitivos que son irreducibles en $\mathbb{Q}[X]$.*

Demostración. De una hipotética factorización en $\mathbb{Z}[X]$ de un número primo, argumentando con los grados de los factores se obtiene una factorización en $\mathbb{Z}$ de dicho número primo. Por tanto, todo número primo es un elemento irreducible en $\mathbb{Z}[X]$.

Además $\mathbb{Z}[X]$ es un dominio de integridad al serlo $\mathbb{Z}$. Si $f \in \mathbb{Z}[X]$ y $f = cont(f)f_1$, la factorización en irreducibles de $\mathbb{Q}[X]$ del polinomio primitivo $f_1 = up_1^{r_1} \cdots p_t^{r_t}$ (en donde u es un número racional no nulo) proporciona, mediante su multiplicación por el producto de todos los denominadores de los polinomios p_i y el de u, una expresión $cf_1 = vq_1^{r_1} \cdots q_t^{r_t}$ en donde ahora los q_i $(i = 1, \ldots, t)$ son polinomios con coeficientes enteros, $c, v \in \mathbb{Z}$ y donde, para cada i, se tiene $\partial q_i = \partial p_i$ al ser q_i y p_i asociados en $\mathbb{Q}[X]$. Se obtiene $cont(cf_1) = c = v \prod_i cont(q_i)^{r_i}$ (2.51 , b) y 2.53) y también la igualdad

$$cf_1 = vq_1^{r_1} \cdots q_t^{r_t} = v(\prod_i cont(q_i)^{r_i}) q_1'^{r_1} \cdots q_t'^{r_t},$$

en donde, para cada i, se ha puesto $q_i = cont(q_i)q_i'$ con q_i' primitivo (e irreducible en $\mathbb{Z}[X]$ por ser asociado a p_i en $\mathbb{Q}[X]$). Por lo tanto resulta $f_1 = q_1'^{r_1} \cdots q_t'^{r_t}$. El producto de la factorización de $cont(f)$ en primos en $\mathbb{Z}$ y de la anterior factorización de f_1 resulta la de f. La unicidad es consecuencia inmediata de la unicidad de la factorización en $\mathbb{Q}[X]$. □

Es oportuno preguntarse acerca de la naturaleza de los ceros racionales de polinomios con coeficientes enteros ya que ello está relacionado con su posible irreducibilidad.

Proposición 2.57. *Sean $f = a_r X^r + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ y n, m enteros primos entre sí. Si el número racional $\frac{n}{m}$ es raíz de f, entonces n divide a a_0 y m divide a a_r.*

Demostración.
$f(\frac{n}{m}) = a_r \left(\frac{n}{m}\right)^r + \cdots + a_1 \frac{n}{m} + a_0 = 0 \Rightarrow m^r a_0 + \cdots + a_r n^r = 0 \Rightarrow n \mid m^r a_0$ y $m \mid a_r n^r$.
Por tanto, $n \mid a_0$ y $m \mid a_r$ ya que n y m son primos entre sí. □

Corolario 2.58. *Los ceros racionales de un polinomio mónico con coeficientes enteros son números enteros.*

A continuación usaremos los homomorfismos de reducción $\overline{\varphi_p}$ para el reconocimiento de polinomios con coeficientes enteros que son irreducibles sobre $\mathbb{Q}$.

Proposición 2.59. *(Criterio de reducción)*

Sea $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ *con* $\partial(f) \geqslant 1$ *y sea* p *un número primo que no divide al coeficiente principal* a_n*. Si* $\overline{\varphi_p}(f) = \overline{a_n}X^n + \cdots + \overline{a_1}X + \overline{a_0} \in \mathbb{Z}_p[X]$ *es irreducible sobre* $\mathbb{Z}_p$*, entonces* f *es irreducible sobre* $\mathbb{Q}$*.*

Demostración. Si f es reducible en $\mathbb{Q}[X]$ existen $g_1, h_1 \in \mathbb{Q}[X]$ tales que $f = g_1h_1$ con $\partial(g_1) \geqslant 1$ y $\partial(h_1) \geqslant 1$. Por el Lema 2.54 existen $g, h \in \mathbb{Z}[X]$ con $\partial(g) = \partial(g_1)$ y $\partial(h) = \partial(h_1)$ tales que $f = gh$. Ahora, si el número primo p no divide a a_n tampoco divide al coeficiente principal de g ni al de h y se verifica que $\partial(f) = \partial(\overline{\varphi_p}(f))$, $\partial(\overline{\varphi_p}(g)) = \partial(g) \geqslant 1$ y $\partial(\overline{\varphi_p}(h)) = \partial(h) \geqslant 1$, por lo que f resulta reducible en $\mathbb{Z}_p[X]$. □

Proposición 2.60. *(Criterio de Eisenstein)*

Sea $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ *con* $\partial(f) \geqslant 1$*. Si existe un número primo* p *tal que* $p \mid a_i$ *para* $i = 0, 1, \ldots, n-1$*,* $p \nmid a_n$ *y* $p^2 \nmid a_0$*, entonces* f *es irreducible en* $\mathbb{Q}[X]$*.*

Demostración. Si $f = a_nX^n + \cdots + a_1X + a_0$ es reducible en $\mathbb{Q}[X]$ se pueden encontrar $g, h \in \mathbb{Z}[X]$ con $\partial(g) = r \geqslant 1$ y $\geqslant \partial(h) = s \geqslant 1$ tales que $f = gh$. Ahora, por hipótesis, $\overline{\varphi_p}(f) = \overline{a_n}X^n = \overline{\varphi_p}(g)\overline{\varphi_p}(h)$ y entonces $\partial\ (\overline{\varphi_p}(g)) = r$ y $\partial\ (\overline{\varphi_p}(h)) = s$. En el DFU $\mathbb{Z}_p[X]$ el elemento X es irreducible y, por lo tanto, $\overline{\varphi_p}(g) = \overline{b_r}X^r$ y $\overline{\varphi_p}(h) = \overline{c_s}X^s$, como consecuencia de la unicidad de la factorización en irreducibles de $\overline{\varphi_p}(f)$ (X es necesariamente, el único factor irreducible tanto de $\overline{\varphi_p}(g)$ como de $\overline{\varphi_p}(h)$). Ahora, si b_0 y c_0 son los términos independientes respectivos de g y de h, resulta que $a_0 = b_0c_0$ ha de ser múltiplo de p^2 pues son nulas las clases de b_0 y de c_0 módulo p, ya que los polinomios $\overline{\varphi_p}(g)$ y $\overline{\varphi_p}(h)$ carecen de término independiente. Esto contradice la hipótesis y, por lo tanto, tal factorización de f no es posible. □

Como consecuencia se tiene que existen polinomios irreducibles de cualquier grado en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$, pues, si p es un número primo, el polinomio $X^n + p$ es irreducible en ambos anillos para cualquier número natural n.

Observación 2.61. Si A es anillo conmutativo y $h \in A[X]$ es un polinomio cualquiera, la propiedad universal del anillo de polinomios (2.33) permite asegurar que existe un

único homomorfismo de anillos $\Gamma_h\colon A[X] \to A[X]$ tal que $\Gamma_h(X) = h$ y $\Gamma_h(d) = d$, $\forall d \in A$.

Si a es una unidad de A y se consideran los polinomios $g = aX + b \in A[X]$ y $f = a^{-1}X - a^{-1}b \in A[X]$ se obtiene que los homomorfismos Γ_g y Γ_f son isomorfismos mutuamente inversos. En efecto, bastará demostrar que $(\Gamma_g \circ \Gamma_f)(X) = X$ y que $(\Gamma_f \circ \Gamma_g)(X) = X$:

$$(\Gamma_g \circ \Gamma_f)(X) = \Gamma_g\left(a^{-1}X - a^{-1}b\right) = a^{-1}g - a^{-1}b = a^{-1}(aX + b) - a^{-1}b = X.$$

Nótese que todo homomorfismo de anillos $\Gamma\colon A[X] \to A[X]$ tal que $\Gamma\,|_A = id_A$ está solamente ligado a la selección de una imagen $\Gamma(X) = g \in A[X]$ que determina dicha aplicación (2.33). Para $f = a_nX^n + \cdots + a_1X + a_0$ se tiene $\Gamma(f) = a_ng^n + \cdots + a_1g + a_0$. Por lo tanto, si A es un dominio de integridad, para que Γ sea sobreyectiva ha de ser necesariamente $\partial(g) = 1$, pues en otro caso ninguna de las imágenes $\Gamma(f) \in A[X]$ puede ser de grado 1. Además, si $\Gamma(X) = g = aX + b$, para que exista Γ^{-1} es necesario que a sea una unidad de A. En efecto, si $\Gamma^{-1}(X) = cX + d$ (también polinomio lineal para que Γ^{-1} sea sobreyectiva), entonces $\left(\Gamma^{-1} \circ \Gamma\right)(X) = X = c(aX + b) + d$, lo que proporciona $ca = 1$ y $cb + d = 0$.

Por lo tanto, si A es un dominio de integridad, todo isomorfismo $\Gamma : A[X] \to A[X]$ tal que $\Gamma\,|_A = id_A$ está ligado a la elección de un polinomio lineal $\Gamma(X) = aX + b$ con a una unidad de A. Tales isomorfismos se denominarán *cambios de variable.*

Nótese también que si $\varphi\colon A \to B$ es un isomorfismo de anillos y $a \in A$, entonces $\varphi(a)$ es unidad en B si, y solo si, a es unidad en A.

$$\varphi(a)\,\varphi(b) = \varphi(ab) = 1_B = \varphi(1_A) \Leftrightarrow ab = 1_A$$

Como consecuencia, para el mismo isomorfismo $\varphi\colon A \to B$ se tiene también que $\varphi(a)$ es irreducible en B si, y solo si, a es irreducible en A. En efecto, si $\varphi(a) = b_1b_2$ en B, y si $a_1, a_2 \in A$ son tales que $\varphi(a_1) = b_1$ y $\varphi(a_2) = b_2$, entonces $\varphi(a) = \varphi(a_1)\,\varphi(a_2) = \varphi(a_1a_2)$, por lo que $a = a_1a_2$ al ser φ un isomorfismo. Como a es irreducible en A, alguno de los factores a_1 o a_2 es unidad en A, y por lo tanto también es unidad en B

alguno de los factores b_1 o b_2. El recíproco se obtiene utilizando el isomorfismo inverso $\varphi^{-1}\colon B \to A$.

Proposición 2.62. *(Criterio de cambio de variable)*

Si $g = aX + b \in A[X]$ y $a \in A^*$, un polinomio $f \in A[X]$ es irreducible si, y solo si, $\Gamma_g(f)$ lo es también.

Corolario 2.63. *Sea p un número primo. El polinomio $f = X^{p-1} + \cdots + X + 1 \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$.*

Demostración. $X^p - 1 = (X-1)f$. Tomando $g = X + 1$ resulta

$$\begin{aligned} X\Gamma_g(f) &= \Gamma_g[(X-1)f] = \Gamma_g(X^p - 1) = (X+1)^p - 1 \\ &= \binom{p}{0}X^p + \binom{p}{1}X^{p-1} + \cdots + \binom{p}{p-1}X + \binom{p}{p} - 1, \text{ y ello implica} \end{aligned}$$

$$\Gamma_g(f) = \binom{p}{0}X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-1} \in \mathbb{Z}[X],$$

que es un polinomio irreducible en $\mathbb{Q}[X]$ por el criterio de Eisenstein (2.60), pues para $i = 1, \ldots, p-1$ el número combinatorio $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$ es múltiplo de p, y $\binom{p}{p-1} = p$ no lo es de p^2. Aplicando ahora el criterio de cambio de variable resulta que $f = X^{p-1} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$ pues su contenido es 1. □

2.5. Ejercicios

1. Sea J un ideal del anillo conmutativo A.
   a) Demuéstrese que
   $$J[X] := \{f = a_n X^n + \cdots + a_1 X + a_0 \in A[X] \mid a_n, \ldots, a_1, a_0 \in J\}$$
   es un ideal de $A[X]$ y que los anillos $A[X]/J[X]$ y $(A/J)[X]$ son isomorfos.
   b) Utilizando el apartado anterior demuéstrese que J es ideal primo de A si, y solo si, $J[X]$ es ideal primo de $A[X]$.
   c) ¿Puede ser $J[X]$ ideal maximal de $A[X]$?
2. Demuéstrese que un polinomio $f \in \mathbb{Z}[X]$ no tiene raíces enteras si $f(0)$ y $f(1)$ son números impares.

3. Determínense todos los enteros positivos n para los que el polinomio X^2+2 divide a $X^5-10X+12$ en $\mathbb{Z}_n[X]$.

4. Demuéstrese que los anillos $\mathbb{Z}[X]/(n,X)$ y $\mathbb{Z}_n$ son isomorfos.

5. *a*) Demuéstrese que si $f(X)$ es irreducible en $\mathbb{Z}_2[X]$ y $\partial(f)>1$, entonces el número de coeficientes no nulos de f es impar.
   b) Calcúlense todos los polinomios irreducibles en $\mathbb{Z}_2[X]$ de grado menor o igual que 4.

6. Sean $J=(X^3+\overline{2}X+\overline{1})\subset\mathbb{Z}_3[X]$ y $F=\mathbb{Z}_3[X]/J$.
   a) Demuéstrese que todo elemento del anillo cociente F admite un único representante de grado $\leqslant 2$.
   b) Demuéstrese que F es un cuerpo.
   c) Calcúlese el número de elementos de F.

7. Factorícense en irreducibles el polinomio $7X^4-28$ en cada uno de los anillos siguientes: $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}[X]$ y $\mathbb{Z}_2[X]$.

8. Imitando la prueba del criterio de Eisenstein pruébese el siguiente, que denominaremos de (Eisenstein)*. Sea $f=a_nX^n+\cdots+a_1X+a_0\in\mathbb{Z}[X]$ y p un número primo tal que $p\mid a_i$ si $i=1,\ldots,n$, $p\nmid a_0$ y $p^2\nmid a_n$, entonces f es irreducible en $\mathbb{Q}[X]$.

9. Factorícense en irreducibles en $\mathbb{Q}[X]$ los polinomios:
   $X^7-2X^5+14X^2-8X+22$, $4X^3-X^2+7$, X^4+4, $X^5-2X^3+X^2-4X+3$, X^4-3X^2+9, $3X^5-6X^3-21X^2-15X+100$, $(X^2-7)(X^6-1)$ y $X^3-X+(3n+2)$ con $n\in\mathbb{Z}$.

10. Sea $f=X^5-6X^4+2X^3+5X^2-X-2\in\mathbb{Z}[X]$.
    a) Descompóngase en producto de irreducibles en $\mathbb{Z}_2[X]$ la reducción de f módulo 2.
    b) Utilizando el apartado anterior demuéstrese que f es irreducible en $\mathbb{Z}[X]$.

11. Sea $f=-5X^6+12X^4+3X^2-18X+7\in\mathbb{Z}[X]$
    a) Descompóngase en producto de irreducibles en $\mathbb{Z}_2[X]$ la reducción de f módulo 2.
    b) Descompóngase en producto de irreducibles en $\mathbb{Z}_3[X]$ la reducción de f módulo 3.
    c) Descompóngase f en producto de irreducibles en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.

12. *a*) Sea $J = \{f \in \mathbb{Z}[X] \mid f(0) = 0\}$. Demuéstrese que J es un ideal principal de $\mathbb{Z}[X]$.¿Es J ideal primo de $\mathbb{Z}[X]$? ¿Es ideal maximal de $\mathbb{Z}[X]$?

    b) Demuéstrese que el polinomio $X^4 + 6X^2 + 7$ es irreducible en $\mathbb{Q}[X]$.

13. *a*) ¿Para qué valores de $n \in \mathbb{Z}$ es $X^3 + X^2 + nX + 2$ irreducible sobre $\mathbb{Q}$?

    b) Pruébese que $X^3 + mX + n$ es irreducible en $\mathbb{Z}[X]$ cuando m y n son impares.

    c) Sea $f(X) \in \mathbb{Z}[X]$ un polinomio mónico tal que $f(0) = p$ es un número primo. Pruébese que $f(X)$ tiene a lo sumo tres raíces racionales.

14. Sabiendo que $1 + i$ es un cero del polinomio $f(X) = X^4 - X^3 + X^2 + 2 \in \mathbb{R}[X]$, descompóngase f en producto de irreducibles en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

Capítulo 3

Extensiones de cuerpos

3.1. Extensiones finitas

Definición 3.1. Sea K un cuerpo. Una *extensión* de K es un cuerpo F del cual K es subcuerpo que será denominado cuerpo base de la extensión. Con $F : K$ se indicará que F es una extensión de K. En este caso F puede ser considerado como espacio vectorial sobre K. La dimensión de este K-espacio se denominará *grado* de la extensión y se denotará $\dim_K F = [F : K]$. La extensión se dirá que es finita si dicha dimensión es finita.

Una *torre de cuerpos* (o de extensiones) es una familia de extensiones $K_{i+1} : K_i$, $i \geqslant 1$, que también se indicará con

$$K_1 \subset K_2 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots$$

La torre se dirá que es *finita* si intervienen en ella solamente un número finito de cuerpos.

Ejemplos 3.2.

1.- $[\mathbb{C} : \mathbb{R}] = 2$, ya que cada $\alpha \in \mathbb{C}$ admite una única expresión $\alpha = a + bi$ con $i^2 = -1$ y $a, b \in \mathbb{R}$, lo cual significa que $\{1, i\}$ constituye una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial.

2.- $\mathbb{C} : \mathbb{Q}$ y $\mathbb{R} : \mathbb{Q}$ son extensiones no finitas. Obviamente $[\mathbb{R} : \mathbb{Q}] \leqslant [\mathbb{C} : \mathbb{Q}]$, y si $[\mathbb{R} : \mathbb{Q}]$ fuese finito $\mathbb{R}$ resultaría numerable (al ser producto cartesiano de un número

finito de conjuntos numerables).

3.- Para una extensión $F : K$ se tiene trivialmente que $[F : K] = 1$ si, y solo si, $F = K$.

Teorema 3.3. *(Teorema del grado)*

Sea $K \subset F \subset E$ una torre de cuerpos. Entonces son equivalentes las afirmaciones:

i) $F : K$ y $E : F$ son finitas.

ii) $E : K$ es finita.

Además, en ese caso se tiene $[E : K] = [E : F]\,[F : K]$.

Demostración. ii) $\Rightarrow$ i)

F es un K-subespacio de E y, por lo tanto, $[F : K] \leqslant [E : K]$. Además, una K-base $\{z_1, \ldots, z_t\}$ de E es también un sistema de generadores de E como F-espacio vectorial y por ello $E : F$ es finita.

i) $\Rightarrow$ ii)

Sean $\{x_1, \ldots, x_n\}$ una K-base de F y $\{y_1, \ldots, y_r\}$ una F-base de E. Entonces $\{x_i y_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant r\}$ es una K base de E. En efecto, para $\alpha \in E$ existen $b_1, \ldots, b_r \in F$ tales que $\alpha = \sum_1^r b_j y_j$. Para cada $j \in \{1, \ldots, r\}$ existen $a_{1,j}, \ldots, a_{n,j} \in K$, tales que $b_j = \sum_1^n a_{i,j} x_i$, y

$$\alpha = \sum_{j=1}^{r} \Big(\sum_{i=1}^{n} a_{i,j} x_i \Big) y_j = \sum_{i,j} a_{ij}\,(x_i y_j)\,,$$

lo cual quiere decir que $\{x_i y_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leq r\}$ es un sistema de generadores de E como K-espacio. Dicho conjunto de generadores es además linealmente independiente sobre K, ya que si $\sum_{i,j} a_{i,j}\,(x_i y_j) = 0$ con $a_{i,j} \in K$, entonces los elementos $a_{i,j} x_i \in F$ son tales que $\sum_j \left(\sum_i a_{i,j} x_i\right) y_j = 0$. La F-independencia lineal de los y_j proporciona entonces que $\sum_i a_{i,j} x_i = 0$ para cada j, y de la K-independencia lineal de los x_i resulta $a_{i,j} = 0$ para todo par i, j. Por lo tanto, $\{x_i y_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leq r\}$ constituye una K-base de E. □

Observaciones 3.4. 1) Nótese que la anterior demostración es constructiva en el sentido de que se obtiene directamente una K-base de E multiplicando los elementos de una

F-base de E por los de una K-base de F. Este método constructivo será utilizado muy frecuentemente en lo que sigue.

2) Nótese también que la igualdad $[E:K]=[E:F]\,[F:K]$ es válida en el caso de extensiones arbitrarias, en el sentido de que $[E:K]$ no es finito si, y solo si, $[E:F]$ o $[F:K]$ es no finito, y que así ambos miembros de dicha igualdad son infinitos.

3) Recuérdese el Teorema de Lagrange para grupos que establece si $H\subset L\subset G$ es una torre de grupos entonces $(G:H)=(G:L)\,(L:H)$, lo que constituye una fórmula similar a la del Teorema del grado. Esto no es algo casual, como se comprobará al estudiar el Teorema fundamental de teoría de Galois para extensiones finitas.

4) Nótese finalmente que, por aplicación directa de la fórmula del Teorema del grado, si $E:K$ es finita de grado primo entonces no existen extensiones intermedias entre E y K.

Definición 3.5. Sean $F:K$ una extensión de cuerpos y A un subconjunto de F. Con $K[A]$ se denotará el menor subanillo de F que contiene a A y a K, es decir, la intersección de todos los subanillos de F que contienen a A y a K. Con $K(A)$ se denotará el menor subcuerpo de F que contiene a A y a K. $K(A)$ es, entonces, el menor subcuerpo de F que contiene al subanillo $K[A]$. Se tiene una torre $K\subset K(A)\subset F$ y se dirá que $K(A)$ es el subcuerpo de F *generado* por A sobre K. También se dirá que $K(A):K$ es la subextensión de $F:K$ generada por A. En particular, si $A=\{x_1,\ldots,x_n\}$, se escribirá $K(A)=K(x_1,\ldots,x_n)$, y también $K[A]=K[x_1,\ldots,x_n]$. La extensión $K(x_1,\ldots,x_n):K$ se dirá que es *finitamente generada,* y $\{x_1,\ldots,x_n\}$ se dirá que es un conjunto de *generadores* de dicha extensión. Se dirá que $K(x):K$ es una extensión *simple*, o que $K(x)$ es una extensión simple de K.

El cuerpo $K(A)$ es el cuerpo, $Q(K[A])$, de fracciones de $K[A]$ (2.15).

Proposición 3.6. *Sea $F:K$ una extensión de cuerpos y sea $A=\{x_1,\ldots,x_n\}\subset F$. Sea $\varphi_{x_1,\ldots,x_n}\colon K[X_1,\ldots,X_n]\to F$ el único homomorfismo de anillos tal que $\varphi_{x_1,\ldots,x_n}|_K=id_K$ y tal que $\varphi_{x_1,\ldots,x_n}(X_i)=x_i$ para cada $i=1,\ldots,n$ (evaluación en $\{x_1,\ldots,x_n\}$ (2.33)). Entonces*

$$K[x_1,\ldots,x_n]=\{f(x_1,\ldots.,x_n)\mid f\in K[X_1,\ldots,X_n]\}=\mathrm{Im}\,(\varphi_{x_1,\ldots,x_n})\ \ y$$

cada elemento $\alpha \in K(x_1, \ldots, x_n)$ *es de la forma*

$$\alpha = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} = f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n)^{-1}$$

con $f, g \in K[X_1, \ldots, X_n]$ *y* $g(x_1, \ldots, x_n) \neq 0$.

Demostración. Si B es un subanillo de F que contieneal conjunto $A = \{x_1, \ldots, x_n\}$ y al cuerpo K, entonces el único homomorfismo $\psi\colon K[X_1, \ldots, X_n] \to B$ tal que $\psi(a) = a, \forall a \in K$, y tal que $\psi(X_i) = x_i$, para $i = 1, 2, \ldots, n$, (2.33) está definido por

$$\psi\Big(\sum_{r_1,\ldots,r_n} a_{r_1,\ldots,r_n} X_1^{r_1} \cdots X_n^{r_r}\Big) = \sum_{r_1,\ldots,r_n} a_{r_1\ldots,r_n} x_1^{r_1} \cdots x_n^{r_r}.$$

Por la unicidad de ψ, se tiene necesariamente que $\varphi_{x_1,\ldots,x_n} = j \circ \psi$, denotando con $j\colon B \hookrightarrow F$ la inclusión. Así se obtiene que $A, K \subset \operatorname{Im}(\varphi_{x_1,\ldots,x_n}) \subset B$ y, por tanto, $\operatorname{Im}(\varphi_{x_1,\ldots,x_n})$ es el menor subanillo de F que contiene a A y a K. Por otra parte, es evidente que

$$\{f(x_1, \ldots, x_n) \mid f \in K[X_1, \ldots, X_n]\} = \operatorname{Im}(\varphi_{x_1,\ldots,x_n}).$$

Si E es un subcuerpo de F que contiene a K y a A, entonces E contiene a $K[x_1, \ldots, x_n]$ y al inverso de cada uno de sus elementos no nulos. Por lo tanto,

$$f(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n)^{-1} \in E \text{ si } f, g \in K[X_1, \ldots, X_n] \text{ y } g(x_1, \ldots, x_n) \neq 0.$$

Ahora, para $\alpha = \dfrac{f_1(x_1, \ldots, x_n)}{g_1(x_1, \ldots, x_n)}$ y $\beta = \dfrac{f_2(x_1, \ldots, x_n)}{g_2(x_1, \ldots, x_n)}$ (con $g_1(x_1, \ldots, x_n)$ y $g_2(x_1, \ldots, x_n)$ no nulos) se tiene

$$\begin{aligned}
\alpha - \beta &= \frac{f_1(x_1, \ldots, x_n)\, g_2(x_1, \ldots, x_n) - f_2(x_1, \ldots, x_n)\, g_1(x_1, \ldots, x_n)}{g_1(x_1, \ldots, x_n)\, g_2(x_1, \ldots, x_n)} \\
&= \frac{(f_1 g_2 - f_2 g_1)(x_1, \ldots, x_n)}{(g_1 g_2)(x_1, \ldots, x_n)}, \\
\alpha\beta^{-1} &= \frac{(f_1 g_2)(x_1, \ldots, x_n)}{(g_1 f_2)(x_1, \ldots, x_n)} \text{ si } \beta \neq 0,
\end{aligned}$$

es decir, dicho conjunto es subcuerpo de F y, por lo tanto, es el menor subcuerpo de F que contiene a K y a A. □

Obsérvese que una parte importante del razonamiento anterior puede ser obviada a la luz de la Proposición 2.15.

En particular si $\alpha \in F$,

$$K[\alpha] = \{f(\alpha) \mid f \in K[X]\} \quad \text{y}$$
$$K(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[X] \text{ y } g(\alpha) \neq 0\right\}.$$

Si $F : K$ es una extensión y si se denota con $\langle x_1, \ldots, x_n\rangle_K$ el K-subespacio de F generado por los elementos $x_1, \ldots, x_n \in F$, es decir, el conjunto de las combinaciones lineales con coeficientes en K de dichos elementos, entonces se tiene trivialmente que

$$\langle x_1, \ldots, x_n\rangle_K \subset K[x_1, \ldots, x_n] \subset F$$

ya que, si $\alpha = a_1x_1 + \cdots + a_nx_n \in \langle x_1, \ldots, x_n\rangle_K$, se tiene $\alpha = \varphi_{x_1,\ldots,x_n}(f) \in K[x_1, \ldots, x_n]$, en donde $f = a_1X_1 + \cdots + a_nX_n$. Por lo tanto, si los elementos $x_1, \ldots, x_n \in F$ generan F como K-espacio, también se tiene $K[x_1, \ldots, x_n] = F$.

Si K y F son subcuerpos de un mismo cuerpo E, $K[F] = F[K]$ es el menor subanillo de E que contiene a K y a F. Sus elementos son expresiones $\sum_i a_ib_i$ con solamente un número finito de sumandos no nulos, donde $a_i \in K$ y $b_i \in F$, ya que el conjunto de tales expresiones es un subanillo de E que contiene a K y a F, y todo subanillo de E que contenga a K y a F debe contener también a dichas expresiones. El menor subcuerpo de E que contiene a K y a F es ahora el conjunto de elementos de la forma $\alpha = \dfrac{\sum_i a_ib_i}{\sum_j a'_jb'_j}$ con numerador y denominador (éste último no nulo) elementos de $F[K]$. La comprobación es muy fácil, es una simple aplicación de (2.15), pues de nuevo, KF es el cuerpo de fracciones de $K[F] = F[K]$.

Definición 3.7. A dicho subcuerpo de E se le denotará con $KF = FK$ y se le denominará *composición* de K y F.

Observación 3.8. Sean $F : K$ y $E : K$ tales que E, F son subcuerpos de un cuerpo L, y tal que existe un subconjunto A de L con $E = K(A)$. Entonces $EF = F(A)$. En efecto, $F \subset EF$ y $A \subset E \subset EF$, y así $F(A) \subset EF$. También $E = K(A) \subset F(A)$ y $F \subset F(A)$ proporciona $EF \subset F(A)$. Esta propiedad será usada frecuentemente en el caso en que A es un conjunto finito. Si E y F son subcuerpos de un cuerpo L, ambos extensiones de K, y $E = K(\alpha_1, \ldots, \alpha_n)$, entonces $EF = F(\alpha_1, \ldots, \alpha_n)$.

3.2. Extensiones algebraicas

Definición 3.9. Sea $F : K$ una extensión de cuerpos. Un elemento $\alpha \in F$ se dice que es *algebraico sobre* K si existe un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$, es decir, si α es un *cero* de algún polinomio no nulo f con coeficientes en K.

Si $\alpha \in F$ no es algebraico sobre K se dirá que es trascendente sobre K.

Se dirá que la extensión $F : K$ es *algebraica* si todo elemento $\alpha \in F$ es algebraico sobre K, y se dirá que es *trascendente* en caso contrario.

Ejemplos 3.10.

1.- Cada $\alpha \in K$ es algebraico sobre K ya que dicho elemento es cero del polinomio $X - \alpha \in K[X]$.

2.- La extensión $\mathbb{C} : \mathbb{R}$ es algebraica, pues si $\alpha = a + bi \in \mathbb{C}$, y $\overline{\alpha} = a - bi$ denota su conjugado, entonces

$$\begin{aligned} f(X) &= (X - \alpha)(X - \overline{\alpha}) \\ &= X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} = X^2 - 2aX + a^2 + b^2 \end{aligned}$$

es un polinomio no nulo con coeficientes reales y $f(\alpha) = 0$.

3.- La extensión $\mathbb{R} : \mathbb{Q}$ es trascendente. C. Hermite (1873) y F. von Lindemann (1882) probaron, respectivamente, que los números reales e y π son transcendentes sobre $\mathbb{Q}$. En la sección 6.2 daremos una prueba de la trascendencia de π.

4.- i, $\sqrt{7}$, $\sqrt[3]{5}$, son elementos de $\mathbb{C}$ algebraicos sobre $\mathbb{Q}$, y por lo tanto sobre $\mathbb{R}$.

En efecto, i es un cero de $X^2 + 1$, $\sqrt{7}$ lo es de $X^2 - 7$ y $\sqrt[3]{5}$ de $X^3 - 5$, todos ellos polinomios no nulos con coeficientes racionales.

5.- También $\alpha = \sqrt{2} + i \in \mathbb{C}$, que es algebraico sobre $\mathbb{R}$, lo es también sobre $\mathbb{Q}$, pues

$$\alpha - i = \sqrt{2} \Rightarrow \alpha^2 - 2i\alpha - 1 = 2 \Rightarrow 2i\alpha = \alpha^2 - 3 \Rightarrow -4\alpha^2 = \left(\alpha^2 - 3\right)^2 \Rightarrow \alpha^4 - 2\alpha^2 + 9 = 0,$$

y α es cero del polinomio no nulo $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$.

6.- Con $K[X_1, \ldots, X_n]$ se denota el anillo de polinomios en las n variables (o indeterminadas) $X_1, \ldots, X_n$, y con $K(X_1, \ldots, X_n)$ el *cuerpo de funciones racionales* en las mismas variables. Cada una de las indeterminadas X_i es trascendente sobre K.

Observaciones 3.11. 1) Si $\varphi_\alpha \colon K[X] \to F$ es la evaluación en α, entonces α es algebraico sobre K si, y solo si, $\mathrm{Ker}(\varphi_\alpha) \neq 0$ si, y solo si, φ_α no es inyectivo.

2) Si $\alpha \in F$ es algebraico sobre algún subcuerpo K' de K, entonces α es también algebraico sobre K ya que $K'[X] \subset K[X]$.

3) Si α es un cero de $f \in K[X]$ lo es también de $c^{-1}f$ siendo $c \in K - \{0\}$. En particular, si c es el coeficiente principal de f, existe un polinomio mónico del cual α es un cero.

4) Sea $F : K$ una extensión y $\alpha \in F$.

a) α es trascendente sobre K si, y solo si, $\mathrm{Ker}(\varphi_\alpha) = 0$ y entonces $\mathrm{Im}\,\varphi_\alpha = K[\alpha]$ es isomorfo al anillo de polinomios $K[X]$. Obsérvese que $K[X]$ no es cuerpo en ningún caso, y, como consecuencia, si $K[\alpha] = K(\alpha)$, es decir, si $K[\alpha]$ es un cuerpo, entonces necesariamente $\mathrm{Ker}(\varphi_\alpha)$ es un ideal no nulo (y maximal), con lo cual existe $f \in \mathrm{Ker}(\varphi_\alpha)$, $f \neq 0$ tal que $f(\alpha) = 0$, equivalentemente, α es algebraico sobre K.

b) Si α es algebraico sobre K, es decir, si $\mathrm{Ker}(\varphi_\alpha) \neq 0$, entonces $\mathrm{Im}\,\varphi_\alpha = K[\alpha] \approx K[X]/\mathrm{Ker}(\varphi_\alpha)$ es un dominio de integridad al ser subanillo del cuerpo F y, por lo tanto, $\mathrm{Ker}(\varphi_\alpha) = \{g \in K[X] \mid g(\alpha) = \varphi_\alpha(g) = 0\}$ es un ideal primo no nulo del anillo $K[X]$. Como $K[X]$ es un DIP, el ideal $\mathrm{Ker}(\varphi_\alpha)$ está generado por un polinomio irreducible g, es decir, $\mathrm{Ker}(\varphi_\alpha) = (g)$. Ahora, si c es el coeficiente principal de g considerando el polinomio mónico $f := c^{-1}g$ resulta que $(f) = (g)$.

Recuérdese que para un dominio de ideales principales A, dos elementos a y b del anillo A generan el mismo ideal si, y solamente si, a y b son asociados (2.21), es decir, si existe una unidad u de A tal que $a = ub$. En nuestro caso, $A = K[X]$, si dos polinomios mónicos f y h generan el mismo ideal de $K[X]$, se tiene $f = h$, pues las unidades de $K[X]$ son los elementos no nulos de K; al ser f y h asociados, deberá ser $f = uh$ con $u \in K$, y así $u = 1$ por la igualdad entre los coeficientes principales de los polinomios f y uh.

Por lo tanto, para nuestro elemento $\alpha \in F$ algebraico sobre K existe un único polinomio mónico $f \in K[X]$ tal que $\mathrm{Ker}(\varphi_\alpha) = (f)$. Como el ideal $\mathrm{Ker}(\varphi_\alpha)$ es primo, el polinomio f es irreducible. Recuérdese que en un DIP, un elemento p es irreducible si, y solo si, el ideal (p) es primo (2.26). Recuérdese también que en un DIP un ideal no nulo I es primo si, y solamente si, I es maximal (2.26).

Podemos probar ahora el siguiente

Teorema 3.12. *Sean $F : K$ es una extensión de cuerpos y $\alpha \in F$ algebraico sobre K.*

Entonces

i) $K[\alpha] = \operatorname{Im}\varphi_\alpha \simeq K[X]/(f)$ *en donde* f *es un polinomio mónico irreducible de grado* $\geqslant 1$.

ii) $K[\alpha] = K(\alpha)$.

iii) Para un $g \in K[X]$, $g(\alpha) = 0 \Leftrightarrow f$ *divide a* g *en* $K[X]$.

iv) f *es el único polinomio mónico irreducible en* $K[X]$ *tal que* $f(\alpha) = 0$.

v) f *es el polinomio mónico de menor grado en* $K[X]$ *tal que* $f(\alpha) = 0$.

Demostración. La afirmación *i)* es inmediata consecuencia de nuestras consideraciones previas.

La *ii)* es consecuencia de la Proposición 3.6 y del hecho de que, siendo ahora el anillo $K[\alpha] \simeq K[X]/(f)$ un cuerpo, $K[\alpha]$ es el menor subcuerpo de F que contiene a K y a α. Por lo tanto, $K[\alpha] = K(\alpha)$.

La *iii)* es inmediata, ya que un polinomio $g \in K[X]$ es tal que $\varphi_\alpha(g) = g(\alpha) = 0$ si, y solamente si, $g \in \operatorname{Ker}(\varphi_\alpha) = (f)$, es decir si, y solo si, g es múltiplo de f en $K[X]$.

La afirmación *iv)* resulta del hecho de que si g es irreducible en $K[X]$ y además $g \in (f)$, necesariamente se tiene $g = hf$ con h una unidad de $K[X]$ (es decir, con $h \in K^*$), ya que g es irreducible. Por tanto, si además g es mónico resulta $h = 1$ con lo cual $f = g$.

La *v)* se obtiene de que $g \in (f) \Rightarrow \partial(f) \leqslant \partial(g)$ ya que el grado de un producto de polinomios, con coeficientes en un dominio de integridad, es la suma de los grados de los factores. □

Definición 3.13. Sean $F : K$ una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K. El único polinomio mónico f irreducible en $K[X]$ tal que $f(\alpha) = 0$ se llamará el *polinomio irreducible de* α *sobre* K y se denotará $f = Irr(\alpha, K)$. A la vista de *v)* anterior, a $Irr(\alpha, K)$ se le denomina también *polinomio mínimo de* α sobre K.

Proposición 3.14. *Sean* $F : K$ *una extensión de cuerpos y* $\alpha \in F$ *un elemento algebraico sobre* K. *Entonces*

i) $[K(\alpha) : K] = \partial(Irr(\alpha, K))$.

ii) Si $\partial(Irr(\alpha, K)) = n$, *el conjunto* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *es una base de* $K(\alpha)$ *como* K*-espacio vectorial.*

Demostración. i) Es evidente consecuencia de *ii*). Para probar *ii*) obsérvese que si $\beta = g(\alpha) \in \mathrm{Im}(\varphi_\alpha) = K(\alpha)$ con $g \in K[X]$, entonces $g = fq + r$, donde $q, r \in K[X]$ y además $r = 0$ o bien $\partial(r) < \partial(f) = n$ (recuérdese que $K[X]$ es un dominio euclídeo cuya norma euclídea es el grado). Se tiene así que $\beta = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, y como $r = a_t X^t + \cdots + a_1 X + a_0$ con las $a_i \in K$ y $t = \partial(r) < n$, resulta $\beta = r(\alpha) = a_t\alpha^t + \cdots + a_1\alpha + a_0$. Por lo tanto, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es un sistema de generadores de $K(\alpha)$ como K-espacio.

Para probar la independencia lineal sobre K de estos elementos, si

$$b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0, \text{ con } b_0, b_1, \ldots, b_{n-1} \in K,$$

el polinomio $h = b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 \in K[X]$ es tal que $h(\alpha) = 0$, y, por lo tanto, $h \in (f)$; pero ello solamente es posible si $h = 0$, pues en otro caso sería $n - 1 \geqslant \partial(h) \geqslant \partial(f) = n$. □

Ejemplos 3.15.

1.- $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$ pues es cero del polinomio $X^2 - 2 \in \mathbb{Q}[X]$ que es irreducible en $\mathbb{Q}[X]$ e $Irr(\sqrt{2}, \mathbb{Q}) = X^2 - 2$. Según lo que establece la Proposición 3.14, $\{1, \sqrt{2}\}$ constituye una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$ y, por lo tanto, cada elemento $\beta \in \mathbb{Q}(\sqrt{2})$ admite una única expresión $\beta = a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$.

2.- Sea $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$. Entonces $(\alpha^2 - 1)^2 = 3$ y α es un cero del polinomio $X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$. Este polinomio es irreducible en $\mathbb{Q}[X]$ (criterio de Eisenstein para el primo $p = 2$) y entonces $Irr(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = X^4 - 2X^2 - 2$, con lo cual resulta que $\{1, \sqrt{1 + \sqrt{3}}, 1 + \sqrt{3}, (1 + \sqrt{3})\sqrt{(1 + \sqrt{3})}\}$ constituye una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{1 + \sqrt{3}})$.

3.- Sea ω la raíz cuarta real positiva de 2. Por el criterio de Eisenstein (para $p = 2$) el polinomio $X^4 - 2$ es irreducible en $\mathbb{Q}[X]$ y tiene a ω como raíz. Por tanto, ω es algebraico sobre $\mathbb{Q}$, $Irr(\omega, \mathbb{Q}) = X^4 - 2$ y $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. Entonces $\{1, \omega, \omega^2, \omega^3\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$, y cada elemento β de $\mathbb{Q}(\omega)$ admite una única expresión $\beta = a + b\omega + c\omega^2 + d\omega^3$

con $a, b, c, d \in \mathbb{Q}$. ¿Cuál es la expresión de $\gamma = 1+\omega-2\omega^6 \in \mathbb{Q}(\omega)$ como $\mathbb{Q}$-combinación lineal de la citada base? El siguiente cálculo determina la respuesta.

$$\begin{aligned}\gamma &= 1+\omega-2\omega^6 = \varphi_\omega(1+X-2X^6)\\ &= \varphi_\omega\left[\left(X^4-2\right)\left(-2X^2\right)+\left(-4X^2+X+1\right)\right]\\ &= \varphi_\omega\left(X^4-2\right)\varphi_\omega\left(-2X^2\right)+\varphi_\omega\left(-4X^2+X+1\right) = -4\omega^2+\omega+1.\end{aligned}$$

Una forma alternativa de proceder consiste en utilizar que $\omega^4 = 2$ para reducir los exponentes en la expresión original de γ. En efecto, de $\omega^4 = 2$ se deduce que $\omega^6 = 2\omega^2$, y entonces $\gamma = 1+\omega-2\omega^6 = 1+\omega-4\omega^2$.

Proposición 3.16. *Toda extensión finita es algebraica.*

Demostración. Sea $F : K$ una extensión finita. Se trata de probar que cada $\alpha \in F$ es algebraico sobre K.

Se tiene $K \subset K(\alpha) \subset F$ y, en virtud del Teorema del grado, $[K(\alpha) : K]$ divide a $[F : K]$ y entonces $K(\alpha) : K$ es finita. Si $[K(\alpha) : K] = n$, y si los $n+1$ elementos $1, \alpha, \ldots, \alpha^n \in K(\alpha)$ son diferentes, entonces son necesariamente K-linealmente dependientes y existen $a_0, a_1, \ldots, a_n \in K$, no todos nulos, tales que $a_0+a_1\alpha+\cdots+a_n\alpha^n = 0$. El polinomio no nulo $f(X) = a_nX^n+\cdots+a_1X+a_0 \in K[X]$ es tal que $f(\alpha) = 0$. Si, por el contrario, existen $i \neq j$, con $0 \leqslant i < j \leqslant n$, tales que $\alpha^i = \alpha^j$, entonces $\alpha^{j-i} = 1$, lo que indica que α es un cero del polinomio $X^{j-i}-1 \in K[X]$. En cualquier caso resulta que α es algebraico sobre K. □

Corolario 3.17. *Sea $F : K$ una extensión y sea $\alpha \in F$ un elemento algebraico sobre K, la extensión $K(\alpha) : K$ es algebraica.*

Demostración. Por la Proposición 3.14 la extensión $K(\alpha) : K$ es finita y por la Proposición 3.16 es algebraica. □

Proposición 3.18. *Para una extensión $F : K$ son equivalentes las afirmaciones*

i) $F : K$ es finita.

ii) $F : K$ es finitamente generada por elementos algebraicos sobre K.

Demostración. $i) \Rightarrow ii)$

Si $\{x_1, \ldots, x_n\}$ es una K-base de F también se tiene $F = K[x_1, \ldots, x_n]$ (véase el comentario posterior a la Proposición 3.6). Además, como consecuencia de la Proposición 3.16, cada x_i es algebraico sobre K y $F = K(x_1, \ldots, x_n)$ al ser F cuerpo.

$ii) \Rightarrow i)$

Sea $F = K(\alpha_1, \ldots, \alpha_n)$ con α_i algebraico sobre K, para cada $i = 1, \ldots, n$, y, por tanto, algebraico sobre $K(\alpha_1, \ldots, \alpha_{i-1})$, ya que $K \subset K(\alpha_1, \ldots, \alpha_{i-1})$. Se tiene así una torre de cuerpos

$$\begin{aligned} K &\subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) \subset K(\alpha_1, \alpha_2)(\alpha_3) \subset \cdots \\ &\subset K(\alpha_1, \ldots, \alpha_{i-1}) \subset K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = F, \end{aligned}$$

en la que cada paso es una extensión simple generada por un elemento algebraico y, por lo tanto, finita, en virtud de la Proposición 3.14. Ahora $[F : K]$ es el producto de los grados de cada una de dichas extensiones y $F : K$ es una extensión finita. □

Ya ha sido dicho que la extensión $\mathbb{R} : \mathbb{Q}$ es trascendente y, en particular, $\mathbb{R} : \mathbb{Q}$ no es finita. Obsérvese que ello quizás resulte poco intuitivo si queremos pensar en la dimensión de espacios vectoriales como algo que tiene que ver única y exclusivamente con "lo ancho", "lo largo", "lo alto", etc. La naturaleza de la dimensión tiene mucho que ver también con la posibilidad de elegir coordenadas, es decir, con la naturaleza del cuerpo de coeficientes.

En particular todo espacio vectorial V de dimensión finita sobre $\mathbb{R}$ es también espacio vectorial sobre $\mathbb{Q}$ por restricción de escalares, pero con esa estructura V no es finito dimensional como $\mathbb{Q}$-espacio.

Teorema 3.19. *Para una torre de cuerpos $K \subset F \subset E$, son equivalentes las afirmaciones*

i) $F : K$ y $E : F$ son algebraicas.

ii) $E : K$ es algebraica.

Demostración. $ii) \Rightarrow i)$

Es evidente usando 2) de (3.11) y el hecho de que cada elemento de F es un elemento de E.

$i) \Rightarrow ii)$

Sean $\alpha \in E$ y $f = Irr(\alpha, F) = \sum_0^n a_i X^i$ (con $a_n = 1$). Entonces α es algebraico sobre $K(a_0, \ldots, a_n)$ ya que $f \in K(a_0, \ldots, a_n)[X]$ y $f(\alpha) = 0$. Así, en la torre

$$K \subset K(a_0, \ldots, a_n) \subset K(a_0, \ldots, a_n)(\alpha),$$

la extensión $K(a_0, \ldots, a_n) : K$ es finita por la Proposición 3.18, al ser $a_0, \ldots, a_n \in F$ y $F : K$ algebraica, y $K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)$ lo es también en virtud de la Proposición 3.14. Por tanto, $K(a_0, \ldots, a_n)(\alpha) : K$ es finita, por el Teorema 3.12, y algebraica, por la Proposición 3.16. Cada elemento de $K(a_0, \ldots, a_n)(\alpha)$ es algebraico sobre K y, en particular, α también lo es. Por lo tanto, $E : K$ es algebraica. □

Corolario 3.20. *Sea $F : K$ una extensión y sea*

$$\overline{K}^F := \{\alpha \in F \mid \alpha \text{ es algebraico sobre } K\}.$$

Entonces $\overline{K}^F$ es cuerpo, la extensión $\overline{K}^F : K$ es algebraica y $\overline{K}^F$ contiene a cada cuerpo E tal que $K \subset E \subset F$ y tal que $E : K$ es algebraica. El cuerpo $\overline{K}^F$ no tiene extensiones algebraicas propias dentro de F.

Demostración. Es evidente que $K \subset \overline{K}^F \subset F$. Además si $\alpha, \beta \in \overline{K}^F$ se tiene obviamente que $\alpha - \beta$, $\alpha\beta$ y $\alpha\beta^{-1}$ (si $\beta \neq 0$) son elementos de $K(\alpha, \beta)$, que es una extensión algebraica de K en virtud de las Proposición 3.18, por lo cual dichos elementos de F son algebraicos sobre K y entonces pertenecen a $\overline{K}^F$. Por lo tanto, $\overline{K}^F$ es cuerpo y la extensión $\overline{K}^F : K$ es obviamente algebraica. Es claro que cualquier subextensión de $F : K$ constituida por elementos algebraicos sobre K debe estar contenida en $\overline{K}^F$ por la propia definición de $\overline{K}^F$. Además, si $E : \overline{K}^F$ es algebraica y $E \subset F$, resulta que $E : K$ es algebraica por el Teorema 3.19 y, en virtud de lo anterior, se tiene $E \subset \overline{K}^F$. □

Definición 3.21. A $\overline{K}^F$ se le denominará *clausura algebraica de K en F.*

Ejemplo 3.22. En la extensión $\mathbb{R} : \mathbb{Q}$ el cuerpo $\overline{\mathbb{Q}}^{\mathbb{R}}$ es una extensión algebraica de $\mathbb{Q}$ pero no finita. De hecho, para cada $n > 0$ es posible elegir $\alpha \in \overline{\mathbb{Q}}^{\mathbb{R}}$ tal que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ y, por lo tanto, $\mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}^{\mathbb{R}}$ y $\left[\overline{\mathbb{Q}}^{\mathbb{R}} : \mathbb{Q}\right] \geqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. En efecto, para cualquier

número primo $p > 0$, el polinomio $X^n - p \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$ (criterio de Eisenstein) y tomando $\alpha = \sqrt[n]{p} \in \mathbb{R}$, que es algebraico sobre $\mathbb{Q}$ por ser un cero de $X^n - p$, se tiene $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial(Irr(\alpha, \mathbb{Q})) = n$. Así, $\alpha \in \overline{\mathbb{Q}}^{\mathbb{R}}$ y $\left[\overline{\mathbb{Q}}^{\mathbb{R}} : \mathbb{Q}\right] \geqslant n$, para todo $n > 0$.

3.3. Construcciones con regla y compás

Finaliza esta sección con la aplicación de los conocimientos hasta ahora adquiridos sobre extensiones de cuerpos a la solución de ciertos problemas geométricos clásicos. Por ejemplo, se estudiará ahora la posibilidad de trisecar un ángulo utilizando solamente la regla y el compás, y se verá que el ángulo $\frac{\pi}{3}$ no es trisecable, o, lo que es equivalente, que el polígono regular de dieciocho lados no es constructible (con solamente los citados útiles de dibujo). La posibilidad de construir el polígono regular de n lados quedará establecida en su total generalidad con el Teorema de Gauss-Wantzel que será probado en la parte final del curso.

Los problemas geométricos que se resolverán en esta sección tienen su origen en el trabajo de los geómetras de la Grecia clásica, y dedicaremos nuestra atención también a la *duplicación del cubo* y a *la cuadratura del círculo,* problemas que han llegado a ser famosos y que han permanecido sin resolver durante mucho tiempo.

Nos gusta pensar que los geómetras griegos consideraban a la recta y a la circunferencia como las únicas figuras geométricas *perfectas* y que ese es quizás el motivo por el cual todas sus argumentaciones geométricas eran consideradas (filosófica y estéticamente) perfectas si estaban basadas en el uso exclusivo de dichas figuras básicas. En ello estaría el origen de las restricciones impuestas sobre el uso exclusivo de la regla (sin graduación) y el compás.

Utilizando solamente la regla y el compás se pueden realizar gran cantidad de construcciones geométricas. Por ejemplo, se puede trazar (construir) la mediatriz de un segmento dado o la bisectriz de un ángulo dado, y se puede trazar la perpendicular o la paralela a una recta dada, que pasen por un punto dado. Estas construcciones son muy conocidas de los cursos elementales de geometría euclídea y no las detallaremos aquí. Los griegos conocían que, en la medida que las restricciones se relajasen, ciertos problemas podrían ser resueltos. De todos modos la perfección estaba condicionada al uso de esos dos únicos útiles de dibujo.

En lo que sigue, los términos *construir* o *constructible* serán sinónimos de *construir* o *constructible con regla y compás.* También conviene precisar en qué términos debe ser establecido lo que se entiende por que una determinada figura sea constructible *a partir de los datos.* Por ejemplo, en la constructibilidad de la mediatriz de un segmento deberá ser considerado como dato el propio segmento, o, lo que es equivalente, los dos puntos que lo determinan; en el problema de la bisectriz de un ángulo los datos están constituidos por éste último o, equivalentemente, por el vértice y dos puntos, uno sobre cada lado, etc. Por ello un problema de constructibilidad será planteado como el

estudio de la posibilidad de obtener una figura geométrica (o un conjunto de puntos que la determinen de modo único) a partir de un conjunto de puntos conocido.

Con estas ideas intuitivas podemos plantear una

Formulación geométrica

Sea entonces P un conjunto de puntos del plano euclídeo $\mathbb{R}^2$. Se supondrá siempre que $\#\mathsf{P} \geqslant 2$. Las únicas *operaciones elementales* permitidas en un problema de constructibilidad son de dos tipos:

Tipo I. Trazar la recta determinada por dos puntos de P.

Tipo II. Trazar una circunferencia con centro en un punto de P y cuyo radio es la distancia entre algún par de puntos de P.

Definición 3.23. Sea $\mathsf{P} \subset \mathbb{R}^2$.

a) Se dice que un punto $A \in \mathbb{R}^2$ es constructible *en un paso* a partir de P si A está contenido en la intersección de dos rectas, o de una recta y una circunferencia, o de dos circunferencias, todas ellas obtenidas a partir de P mediante operaciones elementales de los tipos I y II.

b) Se dirá que un punto A es *constructible* a partir de P si existe una sucesión finita de puntos $A_1, A_2, \ldots, A_n = A$ del plano $\mathbb{R}^2$ tales que

i) A_1 es constructible en un paso a partir de P.

ii) A_i es constructible en un paso a partir de $\mathsf{P} \cup \{A_1, A_2, \ldots, A_{i-1}\}$, para cada $i = 2, \ldots, n$.

Formulación algebraica

Procedemos ahora a dar una formulación algebraica de la constructibilidad que será utilizada para dar respuesta a los tres problemas clásicos.

Como ya se ha dicho, consideraremos que el conjunto de datos P está constituido por al menos dos puntos, y que, tras una apropiada elección de coordenadas en $\mathbb{R}^2$, $\{(0,0),(1,0)\} \subset \mathsf{P}$.

Ya que son constructibles la paralela y la perpendicular a una recta dada que pasan por un punto dado, es evidente que el punto (x, y) es constructible a partir de P si, y solo si, son constructibles a partir de P los puntos $(0, y)$ y $(x, 0)$.

Sea $A \in \mathbb{R}^2$ constructible a partir de $\mathsf{P} \subset \mathbb{R}^2$ y sea $A_1, A_2, \ldots, A_n = A$ la sucesión de puntos del plano que existe por la constructibilidad de A. Para cada $i = 1, 2, \ldots, n$, sea $A_i = (x_i, y_i)$ y $K_i = K_{i-1}(x_i, y_i)$. Llamando $K_0 = \mathbb{Q}(\mathsf{P})$ al cuerpo generado finitamente sobre $\mathbb{Q}$ por las coordenadas de todos los puntos de P, resulta una torre de cuerpos

$$\begin{aligned} \mathbb{Q} \;&\subset\; K_0 = \mathbb{Q}(\mathsf{P}) \subset K_1 = K_0(x_1, y_1) \subset K_2 = K_1(x_2, y_2) \subset \cdots \\ &\subset\; K_n = K_0(x_1, \ldots, x_n, y_1, \ldots, y_n). \quad (*) \end{aligned}$$

Teorema 3.24. *Con las notaciones anteriores se tiene* $[K_n : K_0] = 2^r$ *para algún* $r \geqslant 0$.

La prueba del Teorema 3.24 será consecuencia inmediata de la aplicación del Teorema del grado (3.3) a la torre $(*)$ y del Lema siguiente

Lema 3.25. *Con las notaciones anteriores, para cada* $i = 1, \ldots, n$, *se tiene*

$$[K_{i-1}(x_i) : K_{i-1}] \leqslant 2 \quad y \quad [K_{i-1}(y_i) : K_{i-1}] \leqslant 2.$$

Demostración. La demostración consistirá en probar que si $A_i = (x_i, y_i)$ es constructible en un paso a partir de $\mathsf{P} \cup \{A_1, A_2, \ldots, A_{i-1}\}$, entonces x_i e y_i son ceros de polinomios de grado $\leqslant 2$ con coeficientes en K_{i-1}. Para ello deben ser estudiados todos los casos posibles.

Caso I. El punto A_i es la intersección de dos rectas diferentes r y r', determinadas ambas por pares de puntos de $\mathsf{P} \cup \{A_1, A_2, \ldots, A_{i-1}\}$. Los coeficientes de las ecuaciones de ambas rectas son elementos de K_{i-1} ya que, por ejemplo, si r es la recta determinada por los puntos (α_1, β_1), $(\alpha_2, \beta_2) \in \mathsf{P} \cup \{A_1, A_2, \ldots, A_{i-1}\}$, entonces

$$\begin{vmatrix} X & Y & 1 \\ \alpha_1 & \beta_1 & 1 \\ \alpha_2 & \beta_2 & 1 \end{vmatrix} = 0$$

es la ecuación de r.

Ahora, si $r \equiv aX + bY + c = 0$ y $r' \equiv a'X + b'Y + c' = 0$, se tiene

$$x_i = \frac{\begin{vmatrix} -c & b \\ -c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}}, \; y_i = \frac{\begin{vmatrix} a & -c \\ a' & -c' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}}$$

y, por lo tanto, $x_i, y_i \in K_{i-1}$, en este caso.

Caso II. El punto A_i está en la intersección de una recta $aX + bY + c = 0$, con $a, b, c \in K_{i-1}$, y una circunferencia de ecuación $(X - \alpha)^2 + (Y - \beta)^2 - \rho^2 = 0$, con (α, β) como centro, $\rho^2 = (\alpha_1 - \alpha_2)^2 + (\beta_1 - \beta_2)^2$, donde $(\alpha, \beta), (\alpha_1, \beta_1), (\alpha_2, \beta_2) \in$

$\mathsf{P} \cup \{A_1, A_2, \ldots, A_{i-1}\}$, con lo cual $\alpha, \beta, \alpha_1, \beta_1, \alpha_2, \beta_2 \in K_{i-1}$. Por lo tanto, las coordenadas x_i, y_i del punto A_i deberán satisfacer simultáneamente ambas ecuaciones. Supóngase que $b \neq 0$ (en otro caso debería ser $a \neq 0$ y la argumentación a partir de ese momento sería análoga) con lo cual $y_i = -b^{-1}c - b^{-1}ax_i$ y, por lo tanto, $(x_i - \alpha)^2 + \left(-b^{-1}c - b^{-1}ax_i - \beta\right)^2 - \rho^2 = 0$. Resulta así que x_i es raíz de un polinomio de grado $\leqslant 2$ con coeficientes en K_{i-1}. Lo análogo se prueba para y_i de modo idéntico.

Caso III. El punto A_i está en la intersección de dos circunferencias (de ecuaciones $f_i(X, Y) = 0$, $i = 1, 2$) como la anterior. Este caso III se reduce al anterior observando que cada una de las circunferencias tiene la misma intersección con la otra que con el eje radical $\mathfrak{r}$ de ambas, de ecuación $f_1(X, Y) - f_2(X, Y) = 0$, cuyos coeficientes están en K_{i-1}. □

Demostración. (del Teorema)

Basta con observar que

$$[K_{i-1}(x_i, y_i) : K_{i-1}(y_i)] \leqslant [K_{i-1}(x_i) : K_{i-1}] \leqslant 2,$$

como consecuencia del Lema 3.25, y que, por lo tanto,

$$[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(y_i)]\,[K_{i-1}(y_i) : K_{i-1}]$$

es $1, 2$ o 4. □

A partir de ahora, por simplicidad, supondremos que $\mathsf{P} = \{(0, 0), (1, 0)\}$. También a partir de ahora, *constructible* (respectivamente, *constructibilidad*) será sinónimo de *constructible a partir de* P (respectivamente, *constructibilidad a partir de* P).

Definición 3.26. Se dirá que un número real α es constructible si es constructible el punto $(\alpha, 0) \in \mathbb{R}^2$.

Teorema 3.27. *El conjunto $\mathfrak{C}$ de números reales constructibles es una extensión algebraica de $\mathbb{Q}$ contenida en $\mathbb{R}$ y es cerrado para la extracción de raíces cuadradas de números constructibles positivos.*

Demostración. Ya que nuestro conjunto de datos P está constituido por los puntos $(0,0)$ y $(1,0)$ es inmediato obtener que todos los números enteros son constructibles. El número entero n es constructible ya que lo es el punto $(n,0)$ utilizando el compás para yuxtaponer segmentos. Con el mismo método de obtiene que la suma y diferencia de números constructibles es constructible, y el Teorema de Thales permite construir cualquier número racional. También el Teorema de Thales permite la construcción del producto de números constructibles y el inverso de cualquier número constructible no nulo. Por lo tanto, $\mathfrak{C}$ es una extensión de $\mathbb{Q}$ contenida en $\mathbb{R}$. Además, si $a \geqslant 0$ es constructible lo es también $1+a$, y son constructibles la perpendicular r al eje de abscisas en el punto $(1,0)$ y la circunferencia C de radio $\dfrac{1+a}{2}$ cuyo centro es el pie de la mediatriz del segmento $[(0,0),(1+a,0)]$. El Teorema de la altura correspondiente a la hipotenusa de un triángulo rectángulo establece entonces que, si $B \in r \cap C$, la distancia entre B y $(1,0)$ es $\sqrt{a}$. Por lo tanto, $\sqrt{a}$ es también constructible y así $\mathfrak{C}$ es cerrado para la extracción de raíces cuadradas de números constructibles positivos. Finalmente, si $(x,0)$ es constructible, el Teorema 3.24 permite obtener un cuerpo F, extensión finita (y por tanto algebraica) de $K_0 = \mathbb{Q}$, que contiene al elemento x que será, entonces, algebraico sobre $\mathbb{Q}$. □

Teorema 3.28. *(Teorema fundamental sobre constructibilidad)*

Sea $\mathsf{P} = \{(0,0),(1,0)\} \subset \mathbb{R}^2$. *Un número real* α *es constructible a partir de* P *si, y solamente si, existe una torre de subcuerpos de* $\mathbb{R}$

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$$

tales que $\alpha \in K_m$ *y* $[K_i : K_{i-1}] \leqslant 2$, *para* $i = 1,2,\ldots,m$. *En particular si* α *es un número real constructible, entonces* $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ *es una potencia de* 2.

Demostración. Si $\alpha \in \mathbb{R}$ es constructible el punto $A = (\alpha, 0)$ lo es también, y teniendo en cuenta que ahora $\mathbb{Q}(\mathsf{P}) = K_0$ es el cuerpo $\mathbb{Q}$ al ser $\mathsf{P} = \{(0,0),(1,0)\}$, la aplicación del Lema 3.25 proporciona la torre de cuerpos anunciada, ya que con las notaciones de la prueba de dicho Teorema, $\alpha \in K_m$.

El recíproco será obtenido por inducción en m.

Para $m = 0$ se tiene $\alpha \in \mathbb{Q}$ por hipótesis, y todo número racional es constructible (3.27).

Sea $m > 0$ y supongamos que son constructibles los elementos de K_{m-1}. Sea $\alpha \in K_m$ del que se puede suponer $\alpha \notin K_{m-1}$. Entonces, necesariamente, se tiene $K_m = K_{m-1}(\alpha)$ e $Irr(\alpha, K_{m-1}) = X^2 + bX + c$, en donde b, c son constructibles por ser elementos de K_{m-1}. Como $\delta = b^2 - 4c \in K_{m-1}$ es constructible, lo es también $\alpha = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$, en virtud del Teorema 3.27.

La última afirmación es consecuencia de que $\mathbb{Q}(\alpha) \subset K_m$ y, por lo tanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide a $[F_m : \mathbb{Q}]$ que es una potencia de 2. □

Duplicación de cubo:

Existe una leyenda según la cual, con ocasión de una plaga en Atenas, los atenienses recurrieron al Oráculo quien, a través de la Pitonisa, les comunicó que la solución de sus problemas pasaba por duplicar el tamaño del altar de Apolo, que estaba formado por un roca tallada en forma cúbica. Pusieron manos a la obra aquellas buenas gentes y construyeron otro altar cúbico cuya arista era de longitud doble de la del antiguo altar. Como la plaga persistía, indignados, reclamaron al Oráculo el cual les dijo que no habían interpretado bien sus instrucciones, ya que aquellas consistían en construir un altar con volumen doble del existente.

Teorema 3.29. *La duplicación del cubo es imposible utilizando solamente la regla y el compás.*

Demostración. Si $(0, 0)$ y $(1, 0)$ son extremos de una arista del cubo inicial, se trata de construir otro cubo cuya arista tenga por extremos $(0, 0)$ y $(b, 0)$ tal que $b^3 = 2$ o, lo que es equivalente, que $b = \sqrt[3]{2}$. Ahora bien $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ ya que $Irr(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$, y así, por el Teorema fundamental sobre constructibilidad, $\sqrt[3]{2}$ no es constructible pues 3 no es una potencia de 2. □

Cuadratura del círculo:

Teorema 3.30. *(Lindemann) La cuadratura del círculo es imposible, es decir, es imposible construir con regla y compás un cuadrado cuya área sea igual a la de un círculo dado.*

Demostración. Si el círculo es de radio 1 (lo cual se puede suponer con un sistema de coordenadas apropiado), el lado l del cuadrado solución será tal que $l^2 = \pi$. Entonces, si l fuese constructible lo sería π, que, en virtud del Teorema 3.28, debería ser algebraico sobre $\mathbb{Q}$. □

Trisección del ángulo:

Teorema 3.31. *La trisección del ángulo no es posible en general. Es decir, existen ángulos que no son trisecables con regla y compás.*

Demostración. La prueba consistirá en demostrar que el ángulo $\frac{\pi}{3}$ no es trisecable o, lo que es equivalente, que el ángulo $\frac{\pi}{9}$ no es constructible. Ahora bien, un ángulo θ es constructible si, y solamente si, es constructible el número real $\cos\theta$ (y por lo tanto si, y solo si, $sen\theta = \sqrt{1-\cos^2\theta}$ es constructible).

Obsérvese que como $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, si $\theta = \frac{\pi}{9}$ y se pone $\alpha = \cos\frac{\pi}{9}$, entonces $\frac{1}{2} = 4\alpha^3 - 3\alpha$. Si el ángulo $\theta = \frac{\pi}{9}$ es constructible también lo será el número real $\beta = 2\alpha$, pero como $Irr(\beta, \mathbb{Q}) = X^3 - 3X - 1$ (pues este polinomio no tiene raíces racionales) resulta $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, lo que establece una contradicción con el Teorema fundamental sobre constructibilidad, ya que 3 no es potencia de 2. □

Las recetas proporcionadas en los cursos de dibujo técnico para dibujar un polígono regular de dieciocho lados permiten, por tanto, solamente la obtención aproximada de dicho polígono.

3.4. Ejercicios

1. Sea $F : K$ una extensión de cuerpos tal que $[F : K]$ es primo. Pruébese que $F : K$ es una extensión simple.

2. Sea $A = \{\sqrt{7},\ 2+\sqrt{3},\ e+3,\ \sqrt[5]{7},\ i+3,\ \sqrt{-1+\sqrt{2}},\ cos\left(\frac{2\pi}{5}\right) + isen\left(\frac{2\pi}{5}\right)\}$.

   Determínese el polinomio irreducible sobre $\mathbb{Q}$ de los elementos de A que son algebraicos sobre $\mathbb{Q}$.

3. Sea $E : K$ una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n$ elementos de E.

   a) Demuéstrese que para $2 \leqslant i \leqslant n$,

$$K[\alpha_1, \ldots, \alpha_n] = K[\alpha_1, \ldots, \alpha_{i-1}][\alpha_i, \alpha_{i+1}, \ldots, \alpha_n]$$

y que

$$K(\alpha_1,\ldots,\alpha_n) = K(\alpha_1,\ldots,\alpha_{i-1})(\alpha_i,\ldots,\alpha_n).$$

b) Demuéstrese que si $\alpha_1,\ldots,\alpha_n$ son algebraicos sobre K entonces

$$K[\alpha_1,\ldots,\alpha_n] = K(\alpha_1,\ldots,\alpha_n).$$

4. a) Demuéstrese que $\mathbb{Q}(i,\sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$ y que $[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}] = 4$.
   b) Calcúlese el polinomio mínimo de $i+\sqrt{2}$ sobre los siguientes cuerpos:
   i) $\mathbb{Q}(i)$; ii) $\mathbb{Q}(\sqrt{2})$ y iii) $\mathbb{Q}(i\sqrt{2})$.

5. Pruébese que:

$$\left[\mathbb{Q}\left(\sqrt{3+4i}) + \sqrt{3-4i}\right) : \mathbb{Q}\right] = 1 \text{ y } \left[\mathbb{Q}\left(\sqrt{1+\sqrt{3}} + \sqrt{1-\sqrt{3}}\right) : \mathbb{Q}\right] \neq 1.$$

6. Sea $F:K$ una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K tal que $Irr(\alpha,K)$ tiene grado impar. Pruébese que α^2 es algebraico sobre K y que $K(\alpha) = K(\alpha^2)$.

7. a) Determínese el grado de la extensión $\mathbb{Q}(\alpha) : \mathbb{Q}$ en los siguientes casos: *i)* $\alpha = 2+\sqrt{3}$ y *ii)* $\alpha = 1+\sqrt[3]{2}+\sqrt[3]{4}$.
   b) Calcúlese el polinomio mínimo de $\sqrt[3]{2}+\sqrt[3]{4}$ sobre $\mathbb{Q}$.

8. Sea $F = \mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ con $\alpha_i^2 \in \mathbb{Q}$,$\forall i = 1,\ldots,n$. Pruébese que $\sqrt[3]{2} \notin F$.

9. Hállese el grado de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{5},i) : \mathbb{Q}$.

10. Sea $F:K$ una extensión finita y $f \in K[X]$ un polinomio irreducible sobre K con $\partial(f) > 1$. Demuéstrese que si $mcd(\partial(f),[F:K]) = 1$, entonces f no tiene ceros en F.

11. Sea $F = K(\alpha,\beta)$, siendo α y β elementos algebraicos sobre K de grados n y m, respectivamente. Si m y n son coprimos, pruébese que $[K(\alpha,\beta):K] = nm$ y que $Irr(\alpha,K)$ es irreducible sobre $K(\beta)$. ¿Cuál es el grado de la extensión $K(a) \cap K(\beta) : K$?

12. Sean $E:K$ y $F:K$ extensiones finitas de grados n y m respectivamente, ambos E y F subcuerpos de un cuerpo Ω. Demuéstrese que si n y m son primos entre si, entonces $[EF:K] = nm$.

13. a) Pruébese:
    $i)$ $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$; $ii)$ $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right]=4$ y $iii)$ $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{3}-\sqrt{2}\right)$.
    b) Calcúlese el polinomio irreducible de $\sqrt{3}-\sqrt{2}$ sobre $\mathbb{Q}\left(\sqrt{3}\right)$.
    c) Sea $\alpha=\sqrt[5]{2}$. Calcúlese $Irr(\alpha,\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right))$.

14. a) Determínese una base de $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)$ como $\mathbb{Q}$-espacio.
    b) Dedúzcase que $\sqrt[6]{2}\in\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)$ y que $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)$ es una extensión simple de $\mathbb{Q}$.
    c) Demuéstrese que $Irr\left(\sqrt{2}+\sqrt[3]{2},\mathbb{Q}\right)=X^6-6X^4-4X^3+12X^2-24X-4$.

15. Sea α una raíz de $X^3+2X+2\in\mathbb{Q}[X]$.
    a) Exprésense los elementos α^{-1}, $(\alpha^2+\alpha+1)^{-1}$ y $u=\alpha^6+2\alpha^4+2\alpha^3+6\alpha$ como $\mathbb{Q}$-combinación lineal de una $\mathbb{Q}$-base de $\mathbb{Q}\left(\alpha\right)$.
    b) Determínese $Irr\left(u,\mathbb{Q}\right)$ e $Irr(\alpha^{-1},\mathbb{Q})$.

16. Sean $F:K$, $f\in K\left[X\right]$ mónico e irreducible de grado 3 y $\alpha,\beta,\gamma\in F$ tres ceros distintos de f. Pruébese que:
    a) $[K(\alpha):K]=3$.
    b) β es raíz de un polinomio de grado 2 con coeficientes en $K(\alpha)$.
    c) $K\left(\alpha,\beta,\gamma\right)=K\left(\alpha,\beta\right)$.
    d) La extensión $K\left(\alpha,\beta,\gamma\right):K$ es de grado 3 o 6.

17. Sea $F=\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)$.
    a) Calcúlense los polinomios irreducibles de $\sqrt{1+\sqrt{3}}$ sobre $\mathbb{Q}$ y sobre $\mathbb{Q}\left(\sqrt{3}\right)$.
    b) Calcúlese $[F:\mathbb{Q}]$.

18. Sea $E:K$ y $\alpha,\beta\in E$ elementos algebraicos sobre K.
    a) Demuéstrese que $\partial\left(Irr(\alpha,K)\right)=\partial\left(Irr(\alpha^{-1},K)\right)$.
    b) Si $[K(\alpha):K]=3$ y $[K(\beta):K]=8$, demuéstrese que $Irr(\alpha,K)=Irr(\alpha,K(\beta))$.

19. Sea $f=X^6-2\in\mathbb{Q}[X]$ y sea β un cero de f en $\mathbb{C}$. Expresar β^{-1} como combinación lineal de una $\mathbb{Q}$-base de $\mathbb{Q}\left(\beta\right)$ y calcular $Irr(\beta^{-1},\mathbb{Q})$.

20. a) Sabiendo que $1+i$ es un cero del polinomio $f=X^4-X^3+X^2+2$, descompóngase f en producto de irreducibles en $\mathbb{Q}\left[X\right]$ y en $\mathbb{C}\left[X\right]$.
    b) Demuéstrese que $\{\sqrt{2},\sqrt[3]{2},\sqrt[5]{2}\}$ es un conjunto linealmente independiente sobre $\mathbb{Q}$.

21. Sea $f = 2X^3 + 10X + 4$.

    a) Justifíquese en cuál de los anillos $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y $\mathbb{Q}(\sqrt[5]{2})[X]$ el polinomio f es irreducible.

    b) Sea $\alpha \in \mathbb{C}$ un cero de f. Calcúlese $Irr(1+\alpha, \mathbb{Q})$ e $Irr(\alpha^{-1}, \mathbb{Q})$.

22. a) Sea $f = X^4 - 2X^3 + 5X^2 - 4X + 6 \in \mathbb{Q}[X]$. Sabiendo que $f(i\sqrt{2}) = 0$, calcúlese la descomposición de f en producto de irreducibles en cada uno de los siguientes anillos: $\mathbb{Z}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}(\sqrt{3})[X]$.

    b) Justifíquese si $i \in \mathbb{Q}[\alpha]$ en los siguientes casos:

    l) $\alpha = \sqrt{-2}$.

    2) $\alpha \in \mathbb{C}$ y $\alpha^3 + \alpha + 1 = 0$.

23. Sea $\alpha \in \mathbb{C}$ un cero del polinomio $X^3 + X + 1 \in \mathbb{Q}[X]$.

    a) Pruébese que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2) \subsetneq \mathbb{Q}(\alpha\sqrt{2})$.

    b) Usando el apartado anterior pruébese que $Irr(\alpha\sqrt{2}, \mathbb{Q}) = X^6 + 4X^4 + 4X^2 - 8$.

24. a) Sean $F : K$ una extensión finita y $E : K$ una extensión arbitraria tales que E y F son subcuerpos de un mismo cuerpo Ω. Demuéstrese que $EF : E$ es también extensión finita.

    b) Con las mismas condiciones de a), demuéstrese que si además $E : K$ es finita también lo es la extensión $EF : K$.

    c) Pruébese que lo enunciado en a) permanece válido si se sustituye la condición "extensión finita" por "extensión algebraica".

    d) Análogamente, pruébese que si en b) se sustituye la condición "extensión finita" por "extensión algebraica" el enunciado resultante también es válido.

25. Sea $F : K$ una extensión de cuerpos y $u, v \in F$. Demuéstrese que son equivalentes las afirmaciones:

    i) u es trascendente sobre K y v es trascendente sobre $K(u)$.

    ii) El conjunto $\{u, v\}$ es trascendente sobre K, es decir, si $f \in K[X, Y]$, la condición $f(u, v) = 0$ solo es posible si $f = 0$.

26. Sea $F : K$ una extensión de cuerpos y $\{u_1, \ldots, u_t\} \subset F$ un conjunto trascendente sobre K (es decir, que, para $f \in K[X_1, \ldots, X_t]$, la condición $f(u_1, \ldots, u_t) = 0$ solo es posible si $f = 0$). Demuéstrese que, en este caso, $K(u_1, \ldots, u_t)$ es el cuerpo de funciones racionales en t variables sobre K, es decir, el cuerpo de fracciones del anillo de polinomios en t variables.

27. Sea $F = K(u_1, \ldots, u_n)$ una extensión no algebraica finitamente generada de cuerpos. Demuéstrese que existe un entero $t \in \{1, \ldots, n\}$ tal que $\{u_1, \ldots, u_t\}$ es trascendente sobre K y tal que la extensión $F : K(u_1, \ldots, u_t)$ es finita.

28. Sea A es un anillo conmutativo no finito.

    a) Demuéstrese que $\#A = \#A[X]$.

    b) Conclúyase que si $\{M_t\}_{t\in\mathbb{N}}$ es una familia de A-módulos libres de rango 1, entonces $\#(\oplus_{t\in\mathbb{N}} M_t) = \#A$.

    c) El mismo resultado se tiene si la familia $\{M_t\}_{t\in\mathbb{N}}$ está constituida por A-módulos libres de rango finito.

    d) Si A es dominio de integridad, demuéstrese que $\#A = \#K$ siendo K el cuerpo de fracciones de A.

29. Sea K un cuerpo infinito. Demuéstrese que si F es una extensión algebraica de K, entonces $\#F = \#K$. Como consecuencia de lo establecido en el ejercicio anterior, demuéstrese que no existe un conjunto finito de números reales $u_1, \ldots, u_n$ tal que la extensión $\mathbb{R} : \mathbb{Q}(u_1, \ldots, u_n)$ sea algebraica. En particular, para cada número natural $n > 0$ existe un conjunto $\{t_1, \ldots, t_n\} \subset \mathbb{R}$ que es trascendente sobre $\mathbb{Q}$.

Capítulo 4

Extensiones separables y normales

4.1. Extensión de encajes

Recuérdese que si $f\colon A \to B$ es un homomorfismo de anillos, $\mathrm{Ker}(f)$ es un ideal de A, y que f es inyectivo si, y solo si, $\mathrm{Ker}(f) = 0$. Nuestros homomorfismos son todos propios, es decir, tales que $f(1) = 1$, por lo tanto, si B es un cuerpo $f(1) = 1 \neq 0$. Ahora, como en un cuerpo K solamente existen dos ideales (el 0 y K), cada homomorfismo de cuerpos $f\colon K \to F$ es necesariamente inyectivo, es decir, $\mathrm{Ker}(f) = 0$, pues, por lo ya dicho, $\mathrm{Ker}(f) \neq K$ al ser $1 \notin \mathrm{Ker}(f)$.

Los homomorfismos de cuerpos serán denominados aquí *encajes,* e *isomorfismos* si son biyectivos.

Definición 4.1. Sean $F : K$ y $E : L$ extensiones de cuerpos y $\sigma\colon K \to L$ un encaje. Un encaje $\tau\colon F \to E$ se dirá que *extiende* a σ si $\tau|_K = \sigma$, es decir, si es conmutativo el diagrama

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & L \end{array}$$

en el que las flechas verticales indican las inclusiones. También se dirá que τ es un *encaje sobre* σ. Si $K = L$ y $\sigma = id_K$ se dirá que τ es un *encaje sobre* K, y si además $F = E$ y τ es isomorfismo se dirá que τ es un K-*automorfismo* de F.

Observaciones 4.2.

1) Nótese que si τ es un encaje sobre σ, si $x_1, \ldots, x_n \in F$ y si $k_1, \ldots, k_n \in K$, entonces $\tau(k_1x_1 + \cdots + k_nx_n) = \sigma(k_1)\tau(x_1) + \cdots + \sigma(k_n)\tau(x_n)$ (es decir, τ es σ-*semilineal*). Nótese también que en el caso de que τ es un encaje sobre K la anterior igualdad se simplifica un poco y aparece como $\tau(k_1x_1 + \cdots + k_nx_n) = k_1\tau(x_1) + \cdots + k_n\tau(x_n)$, es decir, τ es una aplicación lineal entre los K-espacios F y E.

2) Por la propiedad universal del anillo de polinomios (2.33), si $\sigma\colon K \to L$ es un encaje, existe un único homomorfismo de anillos $\overline{\sigma}\colon K[X] \to L[X]$ tal que $\overline{\sigma}(a) = \sigma(a)$, para todo $a \in K$, y tal que $\overline{\sigma}(X) = X$. Entonces, para $f = \sum_0^n a_iX^i$ se tiene $f^\sigma := \overline{\sigma}(f) = \sum_0^n \sigma(a_i)X^i$. El homomorfismo $\overline{\sigma}$ es también inyectivo, pues $\overline{\sigma}(f) = \sum_0^n \sigma(a_i)X^i = 0 \Leftrightarrow \sigma(a_i) = 0$, para $i = 0, 1, \ldots, n \Leftrightarrow a_i = 0$, para $i = 0, 1, \ldots, n$, por ser σ inyectivo, y por lo tanto $f = \sum_0^n a_iX^i = 0$.

Nótese que

$$f \in K[X] \text{ es mónico} \Leftrightarrow f^\sigma \in L[X] \text{ es mónico,}$$

y que $\partial(f) = \partial(f^\sigma)$. Además si σ es isomorfismo lo es también $\overline{\sigma}$, y

$$f \in K[X] \text{ es irreducible en } K[X] \Leftrightarrow f^\sigma \in L[X] \text{ es irreducible en } L[X].$$

3) Sean σ y τ como en la Definición 4.1 con la condición adicional de que σ y τ son isomorfismos. Entonces,

3.a) $F : K$ es finita $\Leftrightarrow E : L$ es finita.

Ello es consecuencia de que τ es isomorfismo σ-semilineal y, por tanto, $\dim_K F = \dim_L E$.

3.b) Si $f \in K[X]$ y $u \in F$, entonces

$$u \text{ es un cero } f \Leftrightarrow \tau(u) \text{ es un cero de } f^\sigma$$

Para $f = \sum_0^n a_i X^i \in K[X]$, ya que τ es isomorfismo se verifica que:

$$\begin{aligned} u \in F \text{ es un cero de } f &\Leftrightarrow f(u) = \sum_0^n a_i u^i = 0 \\ &\Leftrightarrow 0 = \tau(f(u)) = \sum_0^n \sigma(a_i)\,\tau(u)^i = f^\sigma(\tau(u)) \\ &\Leftrightarrow \tau(u) \text{ es un cero de } f^\sigma. \end{aligned}$$

3.c) Como consecuencia de 2), 3.a) y 3.b) de (4.2), para $u \in F$ se tiene que:

$$\begin{aligned} &u \text{ es algebraico sobre } K, \text{ con } f = Irr(u, K) \\ \Leftrightarrow\ &\tau(u) \text{ es algebraico sobre L, con } f^\sigma = Irr(\tau(u), L). \end{aligned}$$

De las observaciones anteriores resulta:

Proposición 4.3. *Si $F : K$ y $\tau\colon F \to F$ es un K-automorfismo de F, entonces:*

i) Si $u \in F$ es un cero de $f \in K[X]$, también lo es $\tau(u)$.

ii) Si $u \in F$ es algebraico sobre K, también lo es $\tau(u)$ e $Irr(\tau(u), K) = Irr(u, K)$.

Demostración. Basta fijar $E = F$ y $K = L$ en 3.a) y 3.b) de (4.2), con $\sigma = id_K$. □

Teorema 4.4. *(Teorema de extensión de encajes para extensiones simples)*

Sean, como antes, $F : K$ y $E : L$ extensiones y $\sigma\colon K \to L$ un isomorfismo. Sean $\alpha \in F$ algebraico sobre K y $\beta \in E$ algebraico sobre L. Entonces son equivalentes las afirmaciones siguientes:

i) Existe un encaje $\tau\colon K(\alpha) \to L(\beta)$ sobre σ tal que $\tau(\alpha) = \beta$.

ii) $Irr(\beta, L) = Irr^\sigma(\alpha, K)$.

Además, si tal $\tau\colon K(\alpha) \to L(\beta)$ existe, es un isomorfismo sobre σ.

Demostración. ii) $\Rightarrow$ i)

Si $\overline{\sigma}\colon K[X] \to L[X]$ es el isomorfismo inducido por $\sigma\colon K \to L$, en virtud de la propiedad universal del anillo de polinomios, se tiene el diagrama conmutativo de homomorfismos de anillos

$$\begin{array}{ccc} K[X] & \stackrel{\overline{\sigma}}{\to} & L[X] \\ \uparrow & & \uparrow \\ K & \stackrel{\sigma}{\to} & L \end{array}$$

en el que las flechas verticales son las inclusiones naturales y $\overline{\sigma}(X) = X$.

El isomorfismo $\overline{\sigma}$ es tal que $\overline{\sigma}(Irr(\alpha, K)) = Irr^{\sigma}(\alpha, K) = Irr(\beta, L)$, por la hipótesis. Por lo tanto, $\overline{\sigma}(\mathrm{Ker}(\varphi_\alpha)) = \overline{\sigma}(Irr(\alpha, K)) = (Irr(\beta, L)) = \mathrm{Ker}(\varphi_\beta)$. Entonces existe un isomorfismo $\tau\colon K[\alpha] \to L[\beta]$ tal que es conmutativo el diagrama

$$\begin{array}{ccccc} \mathrm{Ker}(\varphi_\alpha) & \hookrightarrow & K[X] & \stackrel{\varphi_\alpha}{\longrightarrow} & K[\alpha] \\ \downarrow & & \downarrow \overline{\sigma} & & \downarrow \tau \\ \mathrm{Ker}(\varphi_\beta) & \hookrightarrow & L[X] & \stackrel{\varphi_\beta}{\longrightarrow} & L[\beta] \end{array}$$

en el cual las flechas horizontales de la izquierda son la inclusiones y $\tau(f(\alpha)) = f^{\sigma}(\beta)$. En particular para el polinomio $f = X$ resulta $\tau(X(\alpha)) = \tau(\alpha) = X(\beta) = \beta$.

Entonces se tiene el diagrama conmutativo

$$\begin{array}{ccccc} K & \to & K[X] & \stackrel{\varphi_\alpha}{\longrightarrow} & K[\alpha] \\ \downarrow & & \downarrow \overline{\sigma} & & \downarrow \tau \\ L & \to & L[X] & \stackrel{\varphi_\beta}{\longrightarrow} & L[\beta] \end{array}$$

en el que las composiciones de los morfismos horizontales son, respectivamente, las inclusiones $K \hookrightarrow K[\alpha]$ (la superior) y $L \hookrightarrow L[\beta]$ (la inferior). Como $K[\alpha] = K(\alpha)$ y $L[\beta] = L(\beta)$ (Teorema 3.12 apartado ii)) se tiene la afirmación i).

$i) \Rightarrow ii)$

Es 3.c) de (4.2) para $u = \alpha$. □

Existe una prueba alternativa de $ii) \Rightarrow i)$ usando que

$$[K(\alpha) : K] = \partial(Irr(\alpha, K)) = \partial(Irr(\beta, L)) = [L(\beta) : L] = n,$$

y que, si $\sigma\colon K \to L$ es un isomorfismo, existe un único isomorfismo σ-semilineal $\tau\colon K(\alpha) \to L(\beta)$ tal que $\tau(\alpha^i) = \beta^i$ para $i = 0, 1, \ldots, n-1$, es decir, que transforma la K-base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de $K(\alpha)$ en la L-base $\{1, \beta, \ldots, \beta^{n-1}\}$ de $L(\beta)$. Por tanto, si $x \in K(\alpha)$ es de la forma $x = \sum_{i=0}^{n-1} a_i\alpha^i = h(\alpha)$, con $h = \sum_{i=0}^{n-1} a_i X^i$, entonces

$$\tau(x) = \tau(h(\alpha)) = \tau\Big(\sum_{i=0}^{n-1} a_i\alpha^i\Big) = \sum_{i=0}^{n-1} \sigma(a_i)\beta^i = h^\sigma(\beta).$$

La prueba finalizará demostrando que además τ es homomorfismo de anillos.

Si $f = Irr(\alpha, K)$, sean $x, y \in K(\alpha)$ y $h, g \in K[X]$ tales que $\partial(h), \partial(g) \leqslant n-1$ con $x = h(\alpha)$ e $y = g(\alpha)$. Si $hg = kf + l$ con $\partial(l) < \partial(f)$ (algoritmo de Euclides en $K[X]$), se tiene $(hg - l)(\alpha) = 0$, es decir, $hg - l \in (f)$ y $l(\alpha) = h(\alpha)\, g(\alpha) = xy$. Entonces$f^\sigma = Irr(\beta, L)$, por hipótesis, y $(hg - l)^\sigma = h^\sigma g^\sigma - l^\sigma \in (f^\sigma)$ (ya que $\overline{\sigma}\colon K[X] \to L[X]$ es homomorfismo de anillos).

Por tanto, $(hg - l)^\sigma(\beta) = (h^\sigma g^\sigma - l^\sigma)(\beta) = h^\sigma(\beta) g^\sigma(\beta) - l^\sigma(\beta) = 0$, es decir, $\tau(xy) = \tau(l(\alpha)) = l^\sigma(\beta) = h^\sigma(\beta) g^\sigma(\beta) = \tau(x)\,\tau(y)$.

4.2. Cuerpos de escisión

Uno de los objetivos de este capítulo es probar que todo cuerpo K posee una extensión algebraica $\overline{K}$ tal que todo polinomio no constante $f \in K[X]$ escinde en factores lineales en $\overline{K}[X]$ o, equivalentemente, que cada polinomio no constante con coeficientes en K tiene al menos un cero en $\overline{K}$. Este objetivo se logrará de forma paulatina. En primer lugar se probará que para un polinomio no constante $f \in K[X]$ existe una extensión simple $K(\alpha) : K$ tal que $f(\alpha) = 0$. Después se demostrará que existe una extensión finita $F : K$ tal que f escinde en factores lineales en $F[X]$. En la sección siguiente se procederá a la prueba de la existencia de $\overline{K}$.

Para nuestras argumentaciones necesitaremos un Lema de carácter técnico.

Lema 4.5. *Sea $\sigma\colon K \to F'$ un encaje de cuerpos. Entonces existe una extensión $F : K$ y un isomorfismo $\tau\colon F \to F'$ que extiende a σ (τ es un encaje sobre σ).*

Demostración. $\sigma(K)$ es un subcuerpo de F'. Se considera la unión disjunta conjuntista $F := K \bigsqcup [F' \setminus \sigma(K)]$ y se define la aplicación $\tau\colon F \to F'$ mediante

$$\tau(a) := a \text{ si } a \in F' \setminus \sigma(K) \text{ y } \tau(a) = \sigma(a) \text{ si } a \in K.$$

La comprobación de que τ es biyectiva es inmediata y es un ejercicio para el lector. También es obvio que $\tau|_K = \sigma$. Definiendo, para $a, b \in F$

$$a \triangle b := \tau^{-1}[\tau(a) + \tau(b)]$$

y

$$a * b := \tau^{-1}\left[\tau\left(a\right)\tau\left(b\right)\right]$$

se tiene $\tau\left(a\triangle b\right) := \tau\left(a\right) + \tau\left(b\right)$ y $\tau\left(a * b\right) := \tau\left(a\right)\tau\left(b\right)$ con lo cual, si $(F, \triangle, *)$ es un cuerpo, la aplicación τ es un isomorfismo sobre σ. En ese caso, además, para $x, y \in K$ resultará que

$$x\triangle y := \tau^{-1}\left[\tau\left(x\right) + \tau\left(y\right)\right] = \tau^{-1}\left[\sigma\left(x\right) + \sigma\left(y\right)\right] = \tau^{-1}\left[\sigma\left(x + y\right)\right] = x + y$$

y análogamente $x * y = xy$. Entonces si F es un cuerpo, sus operaciones son compatibles con las de K, es decir, F es una extensión de K. Por lo tanto el Lema quedará probado si se demuestra que con las operaciones $\triangle, *$ el conjunto F es cuerpo. Ahora, por ejemplo, para la operación $\triangle$ se tiene asegurada la asociatividad en virtud de las igualdades

$$\begin{aligned} a\triangle(b\triangle c) &= a\triangle\tau^{-1}\left(\tau\left(b\right) + \tau\left(c\right)\right) = \tau^{-1}\left[\tau\left(a\right) + \tau\left(\tau^{-1}\left[\tau\left(b\right) + \tau\left(c\right)\right]\right)\right] \\ &= \tau^{-1}\left[\tau\left(a\right) + \left(\tau\left(b\right) + \tau\left(c\right)\right)\right] = \tau^{-1}\left[\left(\tau\left(a\right) + \tau\left(b\right)\right) + \tau\left(c\right)\right] = (a\triangle b)\triangle c, \end{aligned}$$

que son consecuencia de la definición de la operación $\triangle$ aplicada varias veces y de la asociatividad de $+$ en F'. De forma análoga se prueba la asociatividad de $*$ y que $(F, \triangle)$ es grupo abeliano. También se prueba de modo análogo que $\left(F \setminus \{0\}, *\right)$ es grupo abeliano. La distributividad de $*$ respecto $\triangle$ se establece mediante las igualdades

$$\begin{aligned} a * (b\triangle c) &= \tau^{-1}\left[\tau\left(a\right)\tau\left(b\triangle c\right)\right] = \tau^{-1}\left[\tau\left(a\right)\left[\tau\left(b\right) + \tau\left(c\right)\right]\right] \\ &= \tau^{-1}\left[\tau\left(a\right)\tau\left(b\right) + \tau\left(a\right)\tau\left(c\right)\right] = \tau^{-1}\left[\tau\left(a * b\right) + \tau\left(a * c\right)\right] = \left(a * b\right) \triangle \left(a * c\right), \end{aligned}$$

que resultan de las definiciones de las nuevas operaciones y de la distributividad en F'. □

Observaciones 4.6.

1) Bajo las hipótesis del Lema anterior, si $a_0, a_1, \ldots, a_n \in K$ y $\alpha \in F$ es tal que $\tau(\alpha) = \alpha' \in F'$, se tiene

$$\begin{aligned}&\sigma(a_n)(\alpha')^n + \cdots + \sigma(a_1)\alpha' + \sigma(a_0) = 0\\ &\qquad \Leftrightarrow \tau^{-1}\left(\sigma(a_n)(\alpha')^n + \cdots + \sigma(a_0)\right) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0.\end{aligned}$$

Lo anterior es inmediata consecuencia de que tanto τ como τ^{-1} son isomorfismos de cuerpos y de que $\tau|_K = \sigma$ (y también de que $\tau^{-1}|_{\sigma(K)} = \sigma^{-1}$).

2) Nótese que la observación anterior establece implícitamente que si $\sigma\colon K \to F'$ es un encaje tal que para el polinomio $f = a_nX^n + \cdots + a_1X + a_0 \in K[X]$ existe un $\alpha' \in F'$ con $f^\sigma(\alpha') = \sigma(a_n)(\alpha')^n + \cdots + \sigma(a_1)\alpha' + \sigma(a_0) = 0$, entonces existe un $\alpha \in F$ con $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Es decir, si se puede encontrar un encaje (como σ) de K en otro cuerpo (como F') en el cual un polinomio $f^\sigma \in \sigma(K)[X]$ tiene un cero (en nuestro caso α'), se habrá encontrado una extensión F de K en la cual el polinomio $f \in K[X]$ tiene un cero (el elemento $\alpha = \tau^{-1}(\alpha')$).

Proposición 4.7. *Si $f \in K[X]$ es irreducible existe una extensión simple $K(\alpha) : K$ con $f(\alpha) = 0$ y además $[K(\alpha) : K] = \partial(f)$.*

Demostración. Recuérdese que en un dominio de ideales principales un elemento es irreducible si, y solo si, genera un ideal maximal (2.26). El ideal (f) es maximal en $K[X]$ y $F' := K[X]/(f)$ es un cuerpo. Si $\pi\colon K[X] \to K[X]/(f)$ es el homomorfismo de anillos canónico, se considera la composición σ de los homomorfismos

$$\begin{array}{ccccccc} K & \hookrightarrow & K[X] & \xrightarrow{\pi} & K[X]/(f) = F' \\ a & \mapsto & a & \mapsto & a + (f) = \overline{a} = \sigma(a). \end{array}$$

Entonces $\sigma\colon K \to F'$ es un encaje. Además, poniendo $\alpha' := \pi(X)$, la sobreyectividad de π proporciona $F' = \sigma(K)(\alpha')$. Ahora, si $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, de

la definición de π resulta que

$$\begin{aligned} 0 &= \pi(f) = \pi(X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) \\ &= \pi(X)^n + \pi(a_{n-1})\,\pi(X)^{n-1} + \cdots + \pi(a_1)\,\pi(X) + \pi(a_0) \\ &= \left(\alpha'\right)^n + \sigma(a_{n-1})\left(\alpha'\right)^{n-1} + \cdots + \sigma(a_1)\,\alpha' + \sigma(a_0), \end{aligned}$$

es decir, que $f^\sigma(\alpha') = 0$. La aplicación del Lema 4.5 y de la observación anteriores proporciona ahora una extensión $F : K$ y un isomorfismo $\tau\colon F \to F'$ sobre σ de tal modo que $f(\alpha) = 0$, en donde $\alpha \in F$ es tal que $\tau(\alpha) = \alpha'$. Del isomorfismo $\tau^{-1}\colon F' \to F$ se obtiene además que $F = K(\alpha)$. Ahora, como ya se sabe, $[K(\alpha) : K] = \partial(Irr(\alpha, K)) = \partial(f)$, ya que, por hipótesis, f es irreducible en $K[X]$. □

Se puede enunciar ahora el

Teorema 4.8. *(Teorema de Kronecker)*

Si K es un cuerpo y $g \in K[X]$, con $\partial(g) \geqslant 1$, entonces existe una extensión F de K con $[F : K] \leqslant \partial(g)$, en la que g tiene un cero.

Demostración. Es consecuencia casi inmediata de la Proposición anterior. Sea f un factor irreducible de g en $K[X]$ ($K[X]$ es un DFU), es decir $g = fh$, donde $h \in K[X]$ es el producto los restantes factores irreducibles de dicha factorización. Aplicando la Proposición anterior al polinomio f se obtiene un cuerpo F, extensión de K, y un elemento $\alpha \in F$ tal que $F = K(\alpha)$, con $f(\alpha) = 0$. Como f es irreducible en $K[X]$ se tiene $[K(\alpha) : K] = \partial(Irr(\alpha), K) = \partial(f) \leqslant \partial(g)$ y además $g(\alpha) = f(\alpha)\,h(\alpha) = 0$. □

Definición 4.9. Sea K un cuerpo, $f \in K[X]$ con $\partial(f) = n \geqslant 1$ y E una extensión de K.

1.- Se dirá que f *escinde* (en factores lineales) en E si existen $\alpha_1, \ldots \alpha_n \in E$, no necesariamente distintos, tales que

$$f = c(X - \alpha_1) \cdots (X - \alpha_n)$$

en donde, obviamente, $c \in K$ es el coeficiente principal de f. Dicho de otro modo, los únicos factores irreducibles de f, como elemento del DFU $E[X]$, son lineales.

2.- Se dirá que E es *un cuerpo de escisión de f sobre K* si además se tiene

$$E = K(\alpha_1, \ldots, \alpha_n).$$

Observaciones 4.10.

1) Obsérvese que, según lo establecido, para un mismo polinomio $f \in K[X]$ se podrán encontrar diferentes cuerpos de escisión sobre K. No obstante probaremos que todos son isomorfos sobre K.

2) Nótese que si el polinomio $f \in K[X]$ escinde en la extensión E de K (como en 1) de (4.9)), entonces el cuerpo $E' = K(\alpha_1, \ldots, \alpha_n) \subset E$ es un cuerpo de escisión de f sobre K.

3) Nótese también que si f *escinde* en la extensión E de K, entonces los elementos $\alpha_1, \ldots, \alpha_n \in E$ son los únicos ceros que f tiene en cualquier extensión F de E. En efecto, si $F : E$ es una tal extensión y $\beta \in F$ es un cero de $f \in K[X] \subset E[X] \subset F[X]$, resulta $0 = f(\beta) = c(\beta - \alpha_1) \cdots (\beta - \alpha_n)$ y, por tanto, alguno de las factores $\beta - \alpha_i$ debe ser nulo o, equivalentemente, $\beta = \alpha_i$ para algún i.

4) Obviamente, si el polinomio $f \in K[X]$ es lineal, entonces f escinde en K y K es cuerpo de escisión de f sobre K, pues para $f = cX + b$ basta tomar $\alpha = -bc^{-1} \in K$ para que se tenga $f = c(X - \alpha)$. Además $K = K(\alpha)$, ya que $\alpha \in K$.

5) Si E es un cuerpo de escisión sobre K del polinomio $f \in K[X]$ y si $K \subset F \subset E$, entonces E es también un cuerpo de escisión de f sobre F, pues las condiciones de la definición anterior se cumplen para F en lugar de K, con los mismos $\alpha_1, \ldots, \alpha_n \in E$.

6) Finalmente, la condición 2) de la Definición 4.9 es obviamente equivalente a:

2′) No existe ningún cuerpo intermedio F entre E y K tal que f escinda en F.

Ejemplos 4.11.

1.- Para el polinomio $f = X^2 + 1 \in \mathbb{R}[X]$, que es irreducible en $\mathbb{R}[X]$, un cuerpo de escisión de f sobre $\mathbb{R}$ es el cuerpo $\mathbb{C} = \mathbb{R}(i)$ de los números complejos, pues $i^2 = -1$ proporciona la factorización $f = (X - i)(X + i)$.

2.- El mismo polinomio $f = X^2 + 1 \in \mathbb{C}[X]$ tiene a $\mathbb{C}$ como cuerpo de escisión sobre $\mathbb{C}$.

3.- $\mathbb{Q}(i)$ es cuerpo de escisión de $f = X^2 + 1 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$.

4.- Si $f = X^2 - 5 \in \mathbb{Q}[X]$, $\mathbb{Q}(\sqrt{5})$ es cuerpo de escisión de f sobre $\mathbb{Q}$.

El siguiente Teorema establece la existencia de cuerpos de escisión.

Teorema 4.12. *Sea K un cuerpo y $f \in K[X]$ con $\partial(f) = n \geqslant 1$. Existe una extensión $E : K$ tal que E es cuerpo de escisión de f sobre K y $[E : K] \leqslant n!$*

Demostración. La prueba se hará por inducción en n.

Para $n = 1$ es trivial, ya que se puede tomar $E = K$.

Supongamos ahora que $n > 1$ y que el resultado es cierto para cualquier polinomio de grado menor que n con coeficientes en cualquier cuerpo. Por el Teorema de Kronecker, existe una extensión $K(\alpha_1) : K$ tal que $f(\alpha_1) = 0$ y $[K(\alpha_1) : K] \leqslant n$. Ahora, $X - \alpha_1$ divide a f en $K(\alpha_1)[X]$, es decir, existe $h \in K(\alpha_1)[X]$ tal $f = (X - \alpha_1)h$. El grado de h es $n - 1 < n$, y, por hipótesis de inducción, existe $E \supset K(\alpha_1)$ que es cuerpo de escisión de h sobre $K(\alpha_1)$. Así $E = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$, con $h = c(X-\alpha_2)\cdots(X-\alpha_n)$, donde c es el coeficiente principal de h, que es el mismo que coeficiente principal de f, y además $[E : K(\alpha_1)] \leqslant (n-1)!$

Tenemos ahora $f = c(X - \alpha_1)\cdots(X - \alpha_n)$, $E = K(\alpha_1, \ldots, \alpha_n)$, y el Teorema del grado proporciona $[E : K] = [E : K(\alpha_1)][K(\alpha_1) : K] \leqslant (n-1)!\, n = n!$ □

Estableceremos ahora la "unicidad" del cuerpo de escisión de un polinomio sobre un cuerpo que contenga a sus coeficientes.

Teorema 4.13. *(Teorema de extensión de encajes para cuerpos de escisión)*

Sea $\sigma\colon K \to F$ un isomorfismo de cuerpos y $f \in K[X]$ con $\partial(f) \geqslant 1$. Sean E un cuerpo de escisión de f sobre K y L un cuerpo de escisión de $f^\sigma \in F[X]$ sobre F. Entonces existe un isomorfismo $\tau\colon E \to L$ sobre σ.

Demostración. Se probará también por inducción en $m = [E : K]$.

Si $m = 1$, $E = K$, f escinde en K, y si

$$f = c(X - \alpha_1)\cdots(X - \alpha_n)$$

con $\alpha_1, \dots \alpha_n \in K$, entonces

$$f^\sigma = \sigma(c)(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n))$$

con lo cual f^σ escinde en F y, por tanto, $L = F$ y $\tau = \sigma$ es el isomorfismo buscado.

Supongamos $m > 1$. Entonces f no escinde en K y, por lo tanto, en la factorización de f en $K[X]$

$$f = cf_1 \cdots f_r,$$

con cada f_i mónico e irreducible, algún f_i tiene grado mayor que 1 (en otro caso se tendría $f_i = X - \alpha_i$ con $\alpha_i \in K$, para cada $i = 1, \dots, r$, y entonces f escindiría en K). Supongamos que tal f_i es el polinomio f_1. Como, por hipótesis, f escinde en E, cada f_i también, ya que el conjunto de los ceros de f en E es la unión de los conjuntos de ceros de cada uno de los f_i en dicho cuerpo (consecuencia de la unicidad de la factorización de f en irreducibles en $E[X]$). Si $\alpha \in E$ es cualquier cero de f_1 y, por lo tanto, también de f, $f_1 = Irr(\alpha, K)$ y $[K(\alpha) : K] = \partial(f_1) > 1$. Entonces $f^\sigma = \sigma(c) f_1^\sigma \cdots f_r^\sigma$ con f_1^σ mónico e irreducible en $F[X]$, que escinde en L, ya que f^σ escinde en L por hipótesis. Ahora si $\beta \in L$ es un cero de f_1^σ se tiene $f_1^\sigma = Irr(\beta, F)$, y por el Teorema de extensión de encajes para extensiones simples, existe un único isomorfismo $\widetilde{\sigma}\colon K(\alpha) \to F(\beta)$ sobre σ tal que $\widetilde{\sigma}(\alpha) = \beta$. Además E es cuerpo de escisión de f sobre $K(\alpha)$ y L lo es de $f^{\widetilde{\sigma}}$ sobre $F(\beta)$. Por el Teorema del grado se tiene $[E : K(\alpha)] < [E : K] = m$ al ser $[E : K] = [E : K(\alpha)][K(\alpha) : K]$ y $[K(\alpha) : K] = \partial(f_1) > 1$, como ya se ha dicho. Es ahora cuando interviene la hipótesis de inducción, ya que $[E : K(\alpha)] < m$ permite suponer que existe un isomorfismo $\tau\colon E \to L$ sobre $\widetilde{\sigma}$ que es isomorfismo sobre σ. Así τ es isomorfismo sobre σ y el Teorema queda probado. □

Corolario 4.14. *(Unicidad del cuerpo de escisión)*

Si E y L son cuerpos de escisión de un polinomio $f \in K[X]$ sobre K, entonces E y L son K-isomorfos.

Demostración. Aplíquese el Teorema anterior al caso $K = F$ con $\sigma = id_K$. □

Corolario 4.15. *Sean E un cuerpo de escisión de un polinomio $f \in K[X]$ sobre K y $\alpha, \beta \in E$ elementos que tienen el mismo polinomio irreducible sobre K. Entonces existe un isomorfismo $\tau\colon E \to E$ sobre K (es decir, un K-automorfismo de E) tal que $\tau(\alpha) = \beta$.*

Demostración. Ya que $Irr(\alpha, K) = Irr(\beta, K)$ existe un isomorfismo $\sigma\colon K(\alpha) \to K(\beta)$ sobre K tal que $\sigma(\alpha) = \beta$, en virtud del Teorema de extensión de encajes para extensiones simples. Se aplica ahora el Teorema anterior haciendo jugar a $K(\alpha)$ el papel de K, a $K(\beta)$ el papel de F y a E los papeles de E y de L en el enunciado de dicho Teorema. Ello es lícito, ya que si E es cuerpo de escisión de f sobre K, lo es también sobre $K(\alpha)$, notando además que E es cuerpo de escisión de f^σ sobre K y sobre $K(\beta)$, ya que f tiene sus coeficientes en K y por tanto $f^\sigma = f$, pues $\sigma|_K = id_K$. □

4.3. Clausura algebraica de un cuerpo

En la sección anterior hemos visto que existe la posibilidad de encontrar extensiones finitas de un cuerpo K en las que un polinomio dado $f \in K[X]$ escinda en factores lineales (4.12) y, por lo tanto, que existen cuerpos de escisión que, además, están determinados de modo esencialmente único como extensión de K (4.14).

Se trata de obtener ahora una extensión $\overline{K}$ de un cuerpo dado K que contenga los ceros de todos los polinomios con coeficientes en $\overline{K}$ y de modo que $\overline{K} : K$ sea algebraica.

Lema 4.16. *Para un cuerpo E son equivalentes las afirmaciones:*

i) Todo elemento irreducible en $E[X]$ es un polinomio lineal.

ii) Todo $f \in E[X]$ con $\partial(f) \geqslant 1$ escinde en E.

iii) Todo $f \in E[X]$ con $\partial(f) \geqslant 1$ tiene un cero en E.

iv) El cuerpo E no tiene extensiones finitas propias.

v) El cuerpo E no tiene extensiones algebraicas propias.

Demostración. *v)* $\Rightarrow$ *iv)* Es obvio ya que toda extensión finita es algebraica.

iv) $\Rightarrow$ *v)* Sea $F : E$ algebraica y $\alpha \in F$. El elemento α es algebraico sobre E y entonces $E(\alpha) : E$ es finita por la Proposición 3.14 y, por lo tanto, $E(\alpha) = E$, como consecuencia de la hipótesis *iv)*. Cada $\alpha \in F$ es entonces un elemento de E y así $E = F$.

i) $\Rightarrow$ *ii)* Si $f \in E[X]$ con $\partial(f) \geqslant 1$ y $f = cf_1 \cdots f_r$ es su factorización en irreducibles en $E[X]$ con cada f_i mónico, entonces necesariamente cada $f_i = X - \alpha_i$ para algún $\alpha_i \in E$, en virtud de la hipótesis *i)*.

ii) $\Rightarrow$ *iii)* Dado un $f \in E[X]$ con $\partial(f) \geqslant 1$, cada $\alpha_i \in E$ que interviene en la factorización $f = c(X - \alpha_1) \cdots (X - \alpha_n)$ en $E[X]$ es un cero de f.

iii) $\Rightarrow$ *v)* Sean $F : E$ una extensión algebraica, α un elemento fijado arbitrariamente en F y $f = Irr(\alpha, E) \in E[X]$. En virtud de la hipótesis *iii)*, existe un $\beta \in E$ tal que $f(\beta) = 0$ y entonces f es divisible por $X - \beta$ en $E[X]$. De la irreducibilidad de f en $E[X]$ resulta $f = X - \beta$. Ahora $f(\alpha) = 0$ proporciona $\alpha = \beta \in E$. Es decir, $F = E$.

iv) $\Rightarrow$ *i)* Si $f \in E[X]$ es un polinomio irreducible $\partial(f) \geqslant 1$, por la Proposición 4.7, existe una extensión $E(\alpha) : E$ tal que $f(\alpha) = 0$ y tal que $[E(\alpha) : E] = \partial(Irr(\alpha, E))$. La extensión $E(\alpha) : E$ es finita y $f = cIrr(\alpha, E)$. Por la hipótesis *iv)* se verifica que $\alpha \in E = E(\alpha)$ y, por lo tanto, $Irr(\alpha, E) = X - \alpha$. Así $f = c(X - \alpha)$ es un polinomio lineal.

Obsérvese que la equivalencia *i)* $\Leftrightarrow$ *ii)* ya ha sido probada en (2.45). □

Definición 4.17. Se dirá que un cuerpo E es *algebraicamente cerrado* si E satisface cualquiera de las condiciones equivalentes del Lema anterior. Se dirá que E es una *clausura algebraica* de K si $E : K$ es una extensión algebraica y E es algebraicamente cerrado.

Antes de probar la existencia de clausura algebraica de un cuerpo, probaremos que, si existe, es esencialmente única. Explícitamente:

Proposición 4.18. *Sean K un cuerpo, $F : K$ una extensión algebraica y L un cuerpo algebraicamente cerrado. Si $\sigma : K \to L$ es un encaje, entonces existe un encaje $\tau : F \to L$ que extiende a σ. Si, además, $L : \sigma(K)$ es algebraica y F es algebraicamente cerrado, entonces τ es un isomorfismo. En particular, dos clausuras algebraicas de un mismo cuerpo K son K-isomorfas.*

Demostración. Sea

$$\Im = \{(E, \tau) \mid K \subset E \subset F, \tau : E \to L \text{ es un encaje sobre } \sigma\}.$$

El conjunto $\Im$ no es vacío ya que $(K, \sigma) \in \Im$. Definimos en $\Im$ una relación de orden mediante

$$(E_1, \tau_1) \leqslant (E_2, \tau_2) :\Leftrightarrow E_1 \subset E_2 \text{ y } \tau_2|_{E_1} = \tau_1,$$

con la cual el conjunto $\Im$ es inductivamente ordenado.

En efecto, si $\cdots \leqslant (E_i, \tau_i) \leqslant (E_{i+1}, \tau_{i+1}) \leqslant \cdots$ es una cadena de elementos de $\Im$ el conjunto $E' := \cup_i E_i$ es un subcuerpo de F que contiene a K y, si se define $\tau' \colon E' \to L$ mediante $\tau'(x) = \tau_i(x)$ cuando $x \in E_i$, se obtiene que τ' es un encaje sobre σ. Nótese que τ' está bien definido, ya que si $x \in E_i$ y $x \in E_k$, como necesariamente se tiene $(E_i, \tau_i) \leqslant (E_k, \tau_k)$ o bien $(E_i, \tau_i) \geqslant (E_k, \tau_k)$, resulta $\tau_k(x) = \tau_i(x)$. Entonces (E', τ') es una cota superior de dicha cadena.

Por aplicación del Lema de Zorn, nuestro conjunto $\Im$ tiene elementos maximales. Sea (E, τ) uno de ellos. Entonces, necesariamente, $E = F$. En efecto, supongamos que $E \subsetneq F$ y sea $\alpha \in F \setminus E$, que por hipótesis es algebraico sobre K (y por lo tanto sobre E), con $f = Irr(\alpha, E)$. El polinomio $f^\tau \in L[X]$ tendrá un cero $\beta \in L$, ya que L es algebraicamente cerrado, y f^τ es irreducible en $\tau(E)[X]$, ya que $\overline{\tau} \colon E[X] \to \tau(E)[X]$ es isomorfismo de anillos. Entonces $f^\tau = Irr(\beta, \tau(E))$ y, por el Teorema de extensión de encajes a extensiones simples, existe un encaje $\tau_{\alpha,\beta} \colon E(\alpha) \to \tau(E)(\beta)$ sobre τ, tal que $\tau_{\alpha,\beta}(\alpha) = \beta$. El encaje $\tau_{\alpha,\beta}$ es también encaje sobre σ (ya que extiende a τ), y, llamando j a la inclusión $\tau(E)(\beta) \hookrightarrow L$, se obtiene un encaje $\gamma := j \circ \tau_{\alpha,\beta} \colon E(\alpha) \to L$ que extiende a σ y $(E, \tau) \leqslant (E(\alpha), \gamma)$. La maximalidad de (E, τ) proporciona $E = E(\alpha)$, y así resulta $\alpha \in E$ en contradicción con la selección de α. Por lo tanto $E = F$.

Si además $L : \sigma(K)$ es algebraica y F es algebraicamente cerrado se obtiene una torre de cuerpos $\sigma(K) \subset \tau(F) \subset L$ en la cual todas las extensiones son algebraicas y $\tau(F)$ es también algebraicamente cerrado (véase observación a continuación de esta prueba). Entonces, por el apartado *iv)* del Lema 4.16, resulta $\tau(F) = L$ y τ es un isomorfismo.

Si F y L son dos clausuras algebraicas de K, se aplica lo anterior tomando como σ la inclusión de K en L, y el isomorfismo τ es un K-isomorfismo. □

Si $\tau \colon E \to E'$ es un isomorfismo de cuerpos, entonces E es algebraicamente cerrado

si, y solamente si, E' lo es también. En efecto, cada $f' \in E'[X]$ es de la forma $f' = f^\tau$ con $f \in E[X]$, y un elemento $\alpha \in E$ es un cero de f si, y solamente si, $\tau(\alpha) \in E'$ es un cero de f'. Por lo tanto, cada $f \in E[X]$ no constante tiene un cero en E si, y solo si, cada $f' \in E'[X]$ no constante tiene un cero en E'.

La prueba de la existencia será realizada en varios pasos siguiendo una demostración dada por E. Artin, y que ha sido tomada del libro *Algebra* de S. Lang [LAN] y utilizará la propiedad universal del anillo de polinomios sobre un conjunto finito de indeterminadas (2.33).

Teorema 4.19. *(Teorema de Steinitz)*

Si K es un cuerpo existe una clausura algebraica $\overline{K}$ de K, que está determinada salvo K-isomorfismos.

Demostración. En primer lugar se conseguirá una extensión de K en la que todo polinomio con coeficientes en K tendrá un cero. A continuación se probará que existe una extensión $E : K$ tal que E es algebraicamente cerrado. Finalmente, tomando $\overline{K}^E$ se obtendrá una clausura algebraica de K. La unicidad ha sido ya establecida en la Proposición 4.18.

Procedamos a demostrar la existencia.

Sean $S = \{X_f \mid f \in K[X] \text{ con } \partial(f) \geqslant 1\}$ y $K[S]$ el anillo de polinomios sobre S con coeficientes en K. En el anillo $K[S]$ el ideal

$$\mathbf{I} = \langle \{f(X_f) \mid X_f \in S\} \rangle$$

es propio. En efecto, $1 \in \mathbf{I} \Leftrightarrow \exists f_1, \ldots, f_r \in S$ y $\exists h_1, \ldots, h_r \in K[S]$ tales que

$$\sum_1^r h_i f_i(X_{f_i}) = 1.$$

Si en la expresión anterior, que involucra solo a un número finito t de variables X_f, se pone $X_{f_i} := X_i$, resulta que

$$1 \in \mathbf{I} \Leftrightarrow \sum_1^r h_i(X_1, \ldots, X_t) f_i(X_i) = 1 \quad (*).$$

Sea F una extensión finita de K en la que cada polinomio f_i tiene un cero α_i (tal extensión existe, pues basta con tomar F como cuerpo de escisión sobre K del polinomio $g = \prod_1^r f_i$). La anterior expresión (*) es una igualdad en $K[X_1, \ldots, X_t]$, que es

subanillo de $K[S]$, y la propiedad universal del anillo de polinomios nos permite obtener un homomorfismo de anillos $\psi_{\alpha_1,\ldots,\alpha_t}\colon K[X_1,\ldots,X_t] \to F$ tal que $\psi_{\alpha_1,\ldots,\alpha_t}|_K = id_K$, $\psi_{\alpha_1,\ldots,\alpha_t}(X_i) = \alpha_i$, para $i = 1,\ldots,r$, y con $\psi_{\alpha_1,\ldots,\alpha_t}(X_j) = \alpha_j$ arbitrariamente prefijado en F, para cada $j = r+1,\ldots,t$. Entonces,

$$\begin{aligned} 1 &= \psi_{\alpha_1,\ldots,\alpha_t}(1) = \psi_{\alpha_1,\ldots,\alpha_t}\Big[\sum_1^r h_i(X_1,\ldots,X_t)f_i(X_i)\Big] = \\ &= \sum_1^r h_i(\alpha_1,\ldots,\alpha_t)f_i(\alpha_i) = 0 \end{aligned}$$

lo que establece una contradicción, pues, en cualquier cuerpo, 1 y 0 son elementos diferentes.

Sea ahora $\mathfrak{m}$ un ideal maximal de $K[S]$ tal que $\mathbf{I} \subset \mathfrak{m}$ y sea $\pi\colon K[S] \to K[S]/\mathfrak{m}$ el epimorfismo canónico. El anillo $K[S]/\mathfrak{m}$ es ahora un cuerpo y obtenemos un encaje $\sigma\colon K \to K[S]/\mathfrak{m}$ definido como la composición de la inclusión $K \hookrightarrow K[S]$ con el epimorfismo π. Cada polinomio f^σ con $\partial(f) \geqslant 1$ tiene un cero en $K[S]/\mathfrak{m}$. En efecto, poniendo $\alpha_f := X_f + \mathfrak{m} \in K[S]/\mathfrak{m}$, ya que $f(X_f) \in \mathfrak{m}$, resulta que

$$\pi(f(X_f)) = f(X_f) + \mathfrak{m} = 0_{K[S]/\mathfrak{m}}$$

y, como $\pi(f(X_f)) = f^\sigma(\pi(X_f)) = f^\sigma(\alpha_f)$, se tiene que $\alpha_f \in K[S]/\mathfrak{m}$ es un cero de f^σ.

De este modo hemos construido un encaje $\sigma\colon K \to F' = K[S]/\mathfrak{m}$ tal que, para cada polinomio $f \in K[X]$, con $\partial(f) \geqslant 1$, el polinomio f^σ tiene al menos un cero en F'. Utilizando ahora el Lema 4.5, resulta que lo anterior es equivalente a probar la existencia de una extensión F_1 de K tal que cada polinomio $f \in K[X]$ de grado $\geqslant 1$ tiene al menos un cero en F_1 .

Se puede construir así, de modo inductivo, una torre de cuerpos

$$K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots$$

caracterizada por la propiedad de que cada polinomio no constante $f \in F_i[X]$ tiene al menos un cero en F_{i+1}. Si $E = \cup_i F_i$, entonces E es un cuerpo que admite a cada F_i como subcuerpo, y si $f \in E[X]$ existe un i tal que $f \in F_i[X]$ (basta tomar el índice i

suficientemente alto para que todos los coeficientes de f pertenezcan a F_i), por lo que, si $\partial(f) \geqslant 1$, el polinomio f tiene al menos un cero en $F_{i+1} \subset E$. Entonces el cuerpo E es algebraicamente cerrado y contiene a K como subcuerpo (4.16).

Sea ahora $\overline{K} = \overline{K}^E$ la extensión algebraica maximal de K en E (3.21). Por construcción $\overline{K} : K$ es una extensión algebraica y además $\overline{K}$ es algebraicamente cerrado. En efecto, si $f \in \overline{K}[X]$ es de grado $\geqslant 1$ el polinomio f tiene algún cero $\alpha \in E$ y entonces α es algebraico sobre $\overline{K}$; en la torre $K \subset \overline{K} \subset \overline{K}(\alpha)$ todas las extensiones son algebraicas y, por tanto, α es algebraico sobre K (3.19), con lo que se tiene $\alpha \in \overline{K}$, por la construcción de $\overline{K}$. □

Observación 4.20. Si $F : K$ es una extensión algebraica y $\overline{F}$ es una clausura algebraica de F, entonces $\overline{F}$ es también una clausura algebraica de K. También, si $\overline{K}$ es una clausura algebraica de K la inclusión $K \hookrightarrow \overline{K}$ se extiende a un encaje $\sigma\colon \overline{F} \to \overline{K}$ sobre K que será un isomorfismo (Proposición 4.18). Así las clausuras algebraicas de F y de K son esencialmente iguales.

A partir de ahora, a menudo, consideraremos a cada cuerpo K incluido dentro de su clausura algebraica, y si $f \in K[X]$ es un polinomio no constante nos referiremos a sus ceros dentro de $\overline{K}$.

4.4. Separabilidad

Esta sección se dedica al estudio de la multiplicidad de las raíces de polinomios con coeficientes en un cuerpo, noción que está muy relacionada con el número de encajes del cuerpo de escisión en una clausura algebraica de dicho cuerpo de coeficientes.

Definición 4.21. Sea $f \in K[X]$ un polinomio no constante y sea E_f un cuerpo de escisión de f sobre K. Entonces existen elementos distintos $\alpha_1, \ldots, \alpha_r \in E_f$ tales que

$$f = c\,(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}\,.$$

Cada m_i será denominado *la multiplicidad de la raíz* α_i *de* f. Una raíz α_i se dirá que es *simple* si $m_i = 1$. En otro caso se dirá que es *múltiple* (doble, triple, cuádruple, etc., si $m_i = 2, 3, 4$, etc.).

Observaciones 4.22.

1) La multiplicidad de cada $\alpha_i \in E_f$ está determinada por la unicidad de la factorización de f en $E_f[X]$.

2) Si $f \in K[X]$ y E_1 y E_2 son dos cuerpos de escisión de f sobre K, sabemos que existe un K-isomorfismo $\sigma\colon E_1 \to E_2$ (4.14). Por lo tanto, si

$$f = c(X-\alpha_1)^{m_1}\cdots(X-\alpha_r)^{m_r} \quad \text{y} \tag{4.1}$$

$$f = c(X-\beta_1)^{n_1}\cdots(X-\beta_t)^{n_t} \tag{4.2}$$

son las factorizaciones correspondientes de dicho polinomio en $E_1[X]$ y $E_2[X]$, respectivamente, entonces $r = t$ y, salvo una permutación de índices, se tiene $\beta_i = \sigma(\alpha_i)$ y $m_i = n_i$, para todo $i = 1, \ldots, r$. En efecto, $f^\sigma = f$ ya que $f \in K[X]$ y así resulta que

$$f^\sigma = c(X-\sigma(\alpha_1))^{m_1}\cdots(X-\sigma(\alpha_r))^{m_r} = f = c(X-\beta_1)^{n_1}\cdots(X-\beta_t)^{n_t}$$

en $E_2[X]$. De la unicidad de la factorización en $E_2[X]$ se obtiene lo anunciado.

3) Como consecuencia de lo anterior, aunque las raíces de un polinomio f dependen del cuerpo de escisión en que éstas se consideren, el número de diferentes raíces de f y los exponentes asociados a ellas, a los que hemos llamado *multiplicidades,* están determinados por f, es decir, no dependen del cuerpo de escisión en que se consideren.

Definición 4.23. 1) Se dirá que un polinomio $f \in K[X]$ es *separable* si solamente posee raíces simples.

2) Sean $F : K$ una extensión y $\alpha \in F$ algebraico sobre K. Se dirá que α es *separable* sobre K si el polinomio $Irr(\alpha, K) \in K[X]$ es separable.

3) Si $F : K$ es una extensión algebraica, se dirá que $F : K$ es *separable* si cada $\alpha \in F$ es separable sobre K.

Observación 4.24. Si $K \subset F \subset E$ es una torre de cuerpos y $\alpha \in E$ es separable sobre K, entonces lo es también sobre F. Ello es inmediata consecuencia de que $f = Irr(\alpha, F)$ divide a $g \in Irr(\alpha, K)$ en $F[X]$ y, por tanto, también en el anillo $F_g[X]$, para cualquier F_g cuerpo de escisión de g sobre F.

Definición 4.25. La aplicación $(-)' : K[X] \to K[X]$, definida por

$$(-)'(f) = f' = na_nX^{n-1} + \cdots + a_1,$$

para cada $f = a_nX^n + \cdots + a_1X + a_0$, se denominará *derivación* (o K-derivación) ordinaria. A f' se le denominará *la derivada* de f.

Nótese que se verifican las bien conocidas propiedades

$$\begin{aligned}(f+g)' &= f' + g',\\ (fg)' &= f'g + fg',\end{aligned}$$

de las que resulta que si $a \in K$ entonces $a' = 0$ y, por tanto, $(af)' = af', \forall a \in K$, lo cual establece que la derivación es también un homomorfismo de K-espacios.

La derivada se utiliza para el estudio de la multiplicidad de las raíces de polinomios.

Proposición 4.26. *Sea $f \in K[X]$ un polinomio no constante y sea E_f un cuerpo de escisión de f sobre K. Un elemento $\alpha \in E_f$ es raíz múltiple de f si, y solo si, α es raíz de f y de f'.*

Demostración. Es obvio que si $\alpha \in E_f$ es una raíz múltiple de f, $(X-\alpha)^2$ divide a f en $E_f[X]$, es decir, existe $h \in E_f[X]$ tal que $f = (X-\alpha)^2 h$, y entonces $f' = (X-\alpha)^2 h' + 2(X-\alpha)h$, lo cual proporciona $f'(\alpha) = 0$.

Recíprocamente, como α es raíz de f se tiene que $f = (X-\alpha)g$ en $E_f[X]$, con lo cual $f' = (X-\alpha)g' + g$.

Ahora, si α es raíz también de f' resulta $f'(\alpha) = (\alpha-\alpha)g'(\alpha) + g(\alpha) = 0$ y, por tanto, $X-\alpha$ divide a g en $E_f[X]$. Es decir, existe $h \in E_f[X]$ tal que $g = (X-\alpha)h$, y entonces $f = (X-\alpha)^2 h$. □

Proposición 4.27. *Sea $f \in K[X]$ un polinomio no constante. Entonces el polinomio f es separable si, y solo si, $mcd(f, f') = 1$ en el DFU $K[X]$.*

Demostración. Sea $d = mcd(f, f') \in K[X]$. Si d es de grado $\geqslant 1$, es decir si d no es una constante, todo cero de d (en $\overline{K}$) es también un cero tanto de f como de f', ya que d es divisor (en $K[X]$ y por tanto en $\overline{K}[X]$) de ambos polinomios. Por la Proposición 4.26 f tiene algún cero múltiple y entonces no es separable.

Recíprocamente, si $d = 1$, el Teorema de Bézout (2.30) afirma que en el DIP $K[X]$ existen elementos g, h tales que $1 = fg + f'h$. Si f no fuese separable, f y f' tendrían alguna raíz común $\alpha \in \overline{K}$ (4.26), con lo cual

$$1 = 1(\alpha) = f(\alpha)\, g(\alpha) + f'(\alpha)\, h(\alpha) = 0,$$

lo que constituye un absurdo. □

Corolario 4.28. *Si f es un polinomio irreducible de $K[X]$ y si $Caract(K) = 0$, entonces f es separable.*

Demostración. Si $d = mcd(f, f') \in K[X]$, d es divisor en $K[X]$ de ambos polinomios f y f' y, por tanto, $\partial(d) \leqslant \partial(f), \partial(f')$. Ahora, como $Caract(K) = 0$, $\partial(f') = \partial(f) - 1$, y así $\partial(d) < \partial(f)$, con lo cual el polinomio d es necesariamente una constante, pues f es irreducible en $K[X]$ (si d fuese un polinomio no constante sería un divisor de f y no unidad en $K[X]$). □

Corolario 4.29. *Si $Caract(K) = 0$, toda extensión algebraica de K es separable.*

Aunque la resolubilidad por radicales, que en gran medida constituye el objetivo final del curso, será desarrollada para cuerpos de característica 0, parece razonable mantener la hipótesis de característica arbitraria tan lejos como las complicaciones inherentes a ello nos lo permitan.

El resto de este párrafo se dedica de modo específico al estudio de la separabilidad en característica $p \neq 0$, hipótesis bajo la cual la teoría comienza a enriquecerse introduciendo la nueva noción de inseparabilidad. La siguiente Proposición, que proporciona además una prueba alternativa de los Corolarios (4.28) y (4.29), es básica para este tratamiento.

Proposición 4.30. *Sean K un cuerpo y f un polinomio irreducible en $K[X]$. Entonces todos los ceros de f tienen la misma multiplicidad m. Además, $m = 1$ si la característica de K es cero y, en ese caso, f es separable. Si la característica de K es un número primo p, entonces existe un número natural μ tal que $m = p^{\mu}$.*

Demostración. En primer lugar, nótese que si a es cualquier elemento no nulo de K, las raíces (y sus multiplicidades) de los polinomios f y af, son las mismas. Por ello se puede suponer que nuestro polinomio irreducible f es mónico.

Sea E un cuerpo de escisión de f sobre K y sea

$$f = (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}$$

su factorización en $E[X]$, que lo es también en $\overline{E}[X]$, en donde $\overline{E}$ es la clausura algebraica de E (y de K). Para cada α_i que interviene en tal descomposición se tiene $f = Irr(\alpha_i, K)$ y, para cada $i = 1, \ldots, r$, existe un $\sigma_i \colon K(\alpha_1) \to K(\alpha_i) \subset E \subset \overline{E}$, encaje sobre K, tal que $\sigma_i(\alpha_1) = \alpha_i$, en virtud del Teorema de extensión de encajes a extensiones simples. Tal encaje $\sigma_i \colon K(\alpha_1) \to \overline{E}$ admite una extensión a un encaje (que seguiremos denominando σ_i) $\sigma_i \colon E \to \overline{E}$, en virtud de (4.18). Como $f \in K[X]$ y $\sigma_i|_K = id_K$ se tiene

$$\begin{aligned} f &= (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r} \\ &= f^{\sigma_i} = (X - \sigma_i(\alpha_1))^{m_1} \cdots (X - \sigma_i(\alpha_r))^{m_r} = (X - \alpha_i)^{m_1} \cdots (X - \sigma_i(\alpha_r))^{m_r} \end{aligned}$$

y, por la unicidad de la factorización en $\overline{E}[X]$, se tendrá, en particular, que $m_i = m_1$. Por lo tanto, queda probada la primera parte de la Proposición.

Si $m > 1$ es la multiplicidad común de todos los ceros de f, cada raíz de f, por ejemplo la α_1, es raíz también de la derivada f'. Entonces f divide a f' en $K[X]$ pues $f = Irr(\alpha_1, K)$, lo que conduce a un absurdo pues $\partial(f') < \partial(f)$, salvo que f' sea el polinomio nulo, lo cual es imposible si $Caract(K) = 0$. Así, en el caso de característica nula se tiene necesariamente $m = 1$.

Si $Caract(K) = p \neq 0$ y $m > 1$, para $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ se tiene

$$f' = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1 = 0$$

por lo ya dicho, y entonces, si $a_i \neq 0$ deberá ser i un múltiplo de p (para que ia_i sea nulo). Ya que los monomios X^i que aparecen en f deben ser todos de exponente múltiplo de p, se puede escribir

$$\begin{aligned} f(X) &= X^{ps_n} + \cdots + a_iX^{ps_i} + \cdots + a_0 \\ &= (X^p)^{s_n} + \cdots + a_i(X^p)^{s_i} + \cdots + a_0 = g_1(X^p), \end{aligned}$$

donde $g_1 = X^{s_n} + \cdots + a_i X^{s_i} + \cdots + a_0 \in K[X]$ y $\partial(f) = p\partial(g_1)$. Nuestro polinomio g_1 es irreducible en $K[X]$, puesto que una factorización $g_1 = kh$ en $K[X]$ conduciría a $f = g_1(X^p) = k(X^p)h(X^p)$, lo cual no es posible por la irreducibilidad de f en $K[X]$, salvo que alguno de los factores k o h sea una constante. Además $\alpha \in \overline{K}$ es un cero de f (en ese caso entonces $f = Irr(\alpha, K)$) si, y solo si, α^p es un cero de g_1 (pues $g_1(\alpha^p) = f(\alpha) = 0$) y, así, $g_1 = Irr(\alpha^p, K)$. Repitiendo el proceso para el polinomio g_1, si sus raíces son múltiples, se obtendrá un polinomio $g_2 \in K[X]$, irreducible también en $K[X]$, tal que $g_1(X) = g_2(X^p)$ y del que $((\alpha^p)^p) = \alpha^{p^2}$ será raíz si, y solo si, $\alpha \in \overline{K}$ es un cero de f. Ahora $f = g_1(X^p) = g_2(X^{p^2})$ con $\partial(f) = p\partial(g_1) = p^2\partial(g_2)$. El método podrá reiterarse, obteniendo una sucesión de polinomios $f, g_1, \ldots, g_i, \ldots$ de grados estrictamente decrecientes, si cada g_i tiene raíces múltiples. Como el proceso debe finalizar tras un número finito de pasos, existe necesariamente un μ tal que g_μ solamente tiene raíces simples. De todo el proceso reiterativo resulta que si $\alpha_1, \alpha_2, \ldots, \alpha_r$ son todos los ceros de f, nuestro g_μ tiene a $\alpha_1^{p^\mu}, \alpha_2^{p^\mu}, \cdots, \alpha_r^{p^\mu}$ por únicos ceros (que además son simples). Entonces $g_\mu(X) = (X - \alpha_1^{p^\mu}) \cdots (X - \alpha_r^{p^\mu})$. Ahora, de la factorización única de f en $\overline{K}[X]$, y de las igualdades

$$\begin{aligned} f(X) = g_\mu\left(X^{p^\mu}\right) &= (X^{p^\mu} - \alpha_1^{p^\mu}) \cdots (X^{p^\mu} - \alpha_r^{p^\mu}) = (X - \alpha_1)^{p^\mu} \cdots (X - \alpha_r)^{p^\mu} \\ &= (X - \alpha_1)^m \cdots (X - \alpha_r)^m, \end{aligned}$$

se obtiene $m = p^\mu$. □

Observación 4.31. Se ha utilizado que en un anillo conmutativo A de característica p, si $a, b \in A$, se tiene que $(ab)^p = a^p b^p$ (lo que resulta de la conmutatividad de A) y que $(a+b)^p = \sum_0^p \binom{p}{r} a^{p-r} b^r = a^p + b^p$ puesto que los coeficientes $\binom{p}{r}$ de la última expresión son múltiplos de p para $r \neq 0, 1$ y $\binom{p}{0} = \binom{p}{p} = 1$. También se ha usado que $(-a)^{p^\mu} = -a^{p^\mu}$ lo cual es cierto también para $p = 2$, pues en ese caso $x = -x$, $\forall x \in A$.

Corolario 4.32. *Para una extensión $F : K$ con $Caract(K) = p \neq 0$, si $\alpha \in F$ es algebraico sobre K y $f = Irr(\alpha, K)$, entonces existe un entero $\mu \geqslant 0$ tal que α^{p^μ} es separable sobre K. Además se verifica que $[K(\alpha) : K] = p^\mu \left[K\left(\alpha^{p^\mu}\right) : K\right]$.*

Demostración. En la demostración de la Proposición anterior para el polinomio $f = Irr(\alpha, K)$, se obtiene el polinomio $g_\mu \in K[X]$ que es separable e irreducible en $K[X]$ (de una factorización de g_μ en $K[X]$ y de la igualdad $f(X) = g_\mu\left(X^{p^\mu}\right)$ resultaría una factorización de f) y además $f(\alpha) = g_\mu\left(\alpha^{p^\mu}\right) = 0$. Por lo tanto, $g_\mu = Irr(\alpha^{p^\mu}, K)$ y entonces

$$\partial f = [K(\alpha) : K] = p^\mu \partial g = p^\mu \left[K\left(\alpha^{p^\mu}\right) : K\right]. \qquad \square$$

Observación 4.33. Si K es un cuerpo de característica $p \neq 0$, lo establecido en la observación anterior permite definir un encaje $\varphi_p \colon K \to K$, $\varphi_p(a) = a^p$, denominado *endomorfismo de* Frobenius, cuya imagen denotaremos por K^p. Nótese que, si se pone $b = a^p \in K^p$ el elemento $a \in K$ es un cero del polinomio $X^p - b \in K^p[X]$, y la extensión $K : K^p$ es algebraica. Obsérvese también que el polinomio $X^p - b \in K^p[X]$ escinde en K, ya que $X^p - b = (X - a)^p$ con $X - a \in K[X]$, con lo que $X^p - b$ es un polinomio no separable.

Con las hipótesis y notaciones de la observación anterior, supóngase además que $a \notin K^p$. Se tiene entonces que $X^p - b = Irr(a, K^p)$. En efecto, si $f = Irr(a, K^p)$, el polinomio f divide a $X^p - b = (X - a)^p$ en $K^p[X]$, y por lo tanto

$$f = (X - a)^d = X^d - daX^{d-1} + \cdots + (-1)^d a^d \in K^p[X]$$

para un cierto $d \leqslant p$, con lo cual, en particular, $da = (d \cdot 1)\, a \in K^p$. Si se supone $d < p$, el elemento $d \cdot 1 = 1 + \overset{d)}{\cdots} + 1 \in K^p$ no es nulo, y entonces resulta que $a = (d \cdot 1)^{-1} da \in K^p$, en contra de la hipótesis. Se tiene entonces $d = p$ y, por tanto, $f = (X - a)^p = X^p - b$ y f es un polinomio irreducible en $K^p[X]$ pero no separable. Esto es exclusivo de los cuerpos de característica no nula y la extensión $K : K^p$ es prototipo de las que llamaremos extensiones algebraicas *puramente inseparables.*

Se puede construir una torre de extensiones algebraicas

$$\cdots \subset K^{p^\mu} \subset K^{p^{\mu-1}} \subset \cdots \subset K^{p^2} \subset K^p \subset K \subset K^{\frac{1}{p}} \subset K^{\frac{1}{p^2}} \subset \cdots \subset K^{\frac{1}{p^{\mu-1}}} \subset K^{\frac{1}{p^\mu}} \subset \cdots$$

en la cual cada cuerpo está constituido por las *raíces p-ésimas* de los elementos del anterior. Es muy fácil probar que si un paso de esta cadena es trivial (es decir, si es de grado 1), entonces todos los pasos son triviales.

Definición 4.34. Un cuerpo K de característica $p \neq 0$ se dice que es un *cuerpo perfecto* si φ_p es isomorfismo, o lo que es lo mismo, si $K = K^p$ (es decir, la anterior cadena de extensiones es trivial).

Los cuerpos finitos son perfectos ($\#K = \#\varphi_p(K)$ ya que φ_p es inyectivo), y lo son también los cuerpos algebraicamente cerrados (para cualquier $b \in K$ el polinomio $X^p - b \in K[X]$ tiene al menos un cero en K, y, por lo tanto, existe un $a \in K$ tal que $b = a^p$).

Observación 4.35. Volviendo sobre lo descrito en la prueba de (4.30) se debe constatar que el número r de diferentes encajes $\tau : K(\alpha) \to \overline{K}$ que extienden a la inclusión $K \hookrightarrow \overline{K}$ es precisamente el número r de diferentes ceros del polinomio $f^\sigma \in \overline{K}[X]$, siendo $f = Irr(\alpha, K)$, y es un divisor del grado de f. La separabilidad del polinomio f tiene que ver con el valor de r, es decir, con el número de tales encajes. Así, f es separable precisamente si $r = \partial f$.

En relación con la separabilidad estudiaremos el número de encajes $\tau\colon F \to L$ que extienden a un encaje dado $\sigma\colon K \to L$, siendo $F : K$ algebraica y L algebraicamente cerrado, y veremos que este número no depende más que de la extensión $F : K$. Para cada uno de tales encajes $\tau\colon F \to L$ se tiene que $\tau(F) : \sigma(K)$ es algebraica, así que $\tau(F) \subset \overline{\sigma(K)}^L$ (donde $\overline{\sigma(K)}^L$ (3.20) es algebraicamente cerrado, según se establece en la prueba del Teorema de Steinitz (4.19)), con lo que, para este estudio será suficiente con considerar la situación inicial en donde además $L : \sigma(K)$ es algebraica.

Para un encaje $\sigma\colon K \to L$ pongamos $\mathfrak{S}_\sigma := \{\tau\colon F \to L \mid \tau|_K = \sigma\}$. Se tiene entonces

Proposición 4.36. *Sean $\sigma\colon K \to L$ y $\sigma'\colon K \to L'$ encajes con L , L' algebraicamente cerrados y $L : \sigma(K)$, $L' : \sigma'(K)$ extensiones algebraicas. Si $F : K$ es algebraica se tiene $\#\mathfrak{S}_\sigma = \#\mathfrak{S}_{\sigma'}$.*

Demostración. Poniendo $\lambda = \sigma' \circ \sigma^{-1}\colon \sigma(K) \to \sigma'(K)$ nuestro λ se extiende a un isomorfismo $\gamma\colon L \to L'$ (4.18) y es fácil ver que, para $\tau \in \mathfrak{S}_\sigma$ el encaje $\gamma \circ \tau$ es elemento de $\mathfrak{S}_{\sigma'}$. Como la aplicación $\gamma \circ -\colon \mathfrak{S}_\sigma \to \mathfrak{S}_{\sigma'}$ es inyectiva al serlo γ, se tiene $\#\mathfrak{S}_\sigma \leqslant \#\mathfrak{S}_{\sigma'}$. Razonando con $\lambda^{-1} = \sigma \circ \sigma'^{-1}$ se obtiene de modo análogo que $\#\mathfrak{S}_{\sigma'} \leqslant \#\mathfrak{S}_\sigma$. □

La importancia de este hecho motiva la siguiente

Definición 4.37. Sea $F : K$ una extensión finita. Se denominará grado de separabilidad de dicha extensión al número de diferentes encajes $\tau\colon F \to \overline{K}$ sobre K, y se denotará con $[F : K]_s$. Dicho número es también el de extensiones a F de un encaje dado $\sigma\colon K \to L$, en donde L es un cuerpo algebraicamente cerrado cualquiera.

De modo informal se puede decir que el grado de separabilidad de la extensión algebraica $F : K$ designa el número de posibilidades de mover F dentro de $\overline{K}$ dejando los elementos de K fijos (siempre se puede suponer F dentro de $\overline{K}$, a la luz de (4.36)).

Obsérvese que según lo establecido hasta ahora, si α es algebraico y separable sobre K (por ejemplo si K es de característica nula), entonces

$$[K(\alpha) : K]_s = \#\{\text{ceros de } Irr(\alpha, K)\} = \partial\left(Irr(\alpha, K)\right) = [K(\alpha) : K].$$

Observación 4.38. Recuérdese una vez más que si $K \subset F \subset E$ es una torre de extensiones algebraicas, cada encaje $\gamma\colon F \to \overline{K} = \overline{F} = \overline{E}$ sobre un encaje dado $\sigma\colon K \to \overline{K}$ se extiende a otro $\tau\colon E \to \overline{K}$ (4.18). Además si $\{\sigma_i\}_{i\in I}$ es el conjunto de encajes de F en $\overline{K}$ sobre $\sigma\colon K \to \overline{K}$ y, si para cada $i \in I$, $\{\tau_{i,j_i}\}_{j_i\in J_i}$ es el conjunto de encajes $\tau_{i,j_i}\colon E \to \overline{K}$ que extienden a σ_i, entonces todos los τ_{i,j_i} son encajes sobre σ, y $\#J_i = \#J_{i'}$ cualesquiera que sean $i, i' \in I$ (4.36). Además cualquier $\tau\colon E \to \overline{K}$ sobre σ es uno de los τ_{i,j_i}, pues su restricción a F es un encaje sobre σ y, por tanto, $\sigma|_F = \sigma_i$ para algún i. Por tanto,

Proposición 4.39. *Con las mismas notaciones que en (4.38), si I y J_i son finitos se tiene $\#I = [F : K]_s$, $\#J_i = [E : F]_s$ para cada $i \in I$. Además $[E : K]_s = [F : K]_s\,[E : F]_s$.*

Proposición 4.40. *Sea $F : K$ una extensión finita. Entonces $[F : K]_s$ divide a $[F : K]$. El cociente $\dfrac{[F : K]}{[F : K]_s}$ recibe el nombre de grado de inseparabilidad de la extensión y se designa con $[F : K]_i$.*

Demostración. Sea $F = K(\alpha_1, \ldots, \alpha_n)$ con cada α_i algebraico sobre K. Se considera la torre

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = F$$

de la cual, en cada paso se tiene

$$[K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)]_s = \#\{\text{ceros de } Irr(\alpha_{i+1}, K(\alpha_1, \ldots, \alpha_i))\}$$

que es divisor de

$$\partial(Irr(\alpha_{i+1}, K(\alpha_1, \ldots, \alpha_i))) = [K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)] .$$

De la observación (4.38) y del Teorema del grado se obtiene que $[F : K]_s$ divide a $[F : K]$. □

Nótese que si $F = K(\alpha)$ con $\alpha \in F$ algebraico sobre K, entonces $[F : K]_i$ es la multiplicidad común de todos los ceros de $Irr(\alpha, K)$ y, por tanto, $[F : K]_i = p^\mu$, si K es de característica $p \neq 0$. Si $Caract(K) = 0$, se tiene que $[F : K]_i = 1$.

Corolario 4.41. *Sea $F : K$ una extensión finita. Entonces $F : K$ es separable sobre K si, y solo si, $[F : K]_s = [F : K]$.*

Demostración. Como consecuencia de (4.39) y del Teorema del grado, si $[F : K]_s = [F : K]$ se tiene $[K(\alpha) : K] = [K(\alpha) : K]_s$, para cada $\alpha \in F$. De (4.35) se sigue que

$$[K(\alpha) : K]_s = \#\{\text{ceros de } Irr(\alpha, K)\} = \partial\left(Irr(\alpha, K)\right),$$

es decir, $Irr(\alpha, K)$ es un polinomio separable y por lo tanto α es separable sobre K.

Recíprocamente, si $F : K$ es separable finita, $F = K(\alpha_1, \ldots, \alpha_n)$ con cada α_i algebraico y separable sobre K (y, por lo tanto, sobre $K(\alpha_1, \ldots, \alpha_{i-1})$). Como consecuencia de lo establecido hasta ahora (4.35) se tiene

$$[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})] = [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]_s$$

para cada $i = 1, \ldots, n-1$. De la multiplicatividad en torres de ambos grados ((3.3),(4.39)) se obtiene $[F : K]_s = [F : K]$.

En otras palabras, si $F = K(\alpha_1, \ldots, \alpha_n)$ con cada α_i algebraico y separable sobre K entonces $[F : K]_s = [F : K]$ y así cada $\alpha \in F$ es separable sobre K. □

Corolario 4.42. *Si $F : K$ es una extensión y si $\alpha_1, \ldots, \alpha_n \in F$ son elementos algebraicos separables sobre K, entonces la extensión $K(\alpha_1, \ldots, \alpha_n) : K$ es separable.*

Como consecuencia inmediata del corolario anterior, dada una extensión $F : K$ algebraica, el conjunto

$$F_s(K) := \{a \in F \mid a \text{ es separable sobre } K\}$$

es una extensión algebraica separable de K. Si $\alpha, \beta \in F$ son separables sobre K, también lo son los elementos $\alpha - \beta$ y $\alpha\beta^{-1}$ (si $\beta \neq 0$) pues ambos son elementos de $K(\alpha, \beta)$ que es extensión separable de K por (4.42).

De (4.41) y de (4.40) se obtiene fácilmente también el

Corolario 4.43. *Una extensión finita $F : K$ es separable si, y solo si, $[F : K]_i = 1$.*

En el otro extremo del espectro de divisores de $[F : K]$ se encuentran las extensiones puramente inseparables

Definición 4.44. Se dice que la extensión finita $F : K$ es *puramente inseparable* si $[F : K]_i = [F : K]$ o, equivalentemente, $[F : K]_s = 1$.

Sea $K \subset F \subset E$ es una torre de extensiones finitas Como consecuencia de (3.3), (4.39) y (4.40) resulta que $[E : K]_i = [F : K]_i [E : F]_i$.

Observación 4.45. Obsérvese que si K es de característica p y el grado de una extensión finita $F : K$ no es divisible por p, entonces $F : K$ es separable, ya que el grado de inseparabilidad (que siempre es una potencia de p y divisor de $[F : K]$) es ahora necesariamente 1. El recíproco no es cierto. En efecto, para cada entero $\mu > 0$ existe una extensión $F : \mathbb{Z}_p$ de grado μ que es el cuerpo de escisión sobre $\mathbb{Z}_p$ del polinomio $X^{p^\mu} - X$, que es separable (5.17) y así lo es también la extensión $F : \mathbb{Z}_p$. Basta tomar μ un múltiplo de p para obtener una extensión separable de grado divisible por p. También es separable sobre $\mathbb{Z}_p$ el cuerpo de escisión del polinomio $X^p - X - 1 \in \mathbb{Z}_p[X]$ sobre $\mathbb{Z}_p$, pues dicho polinomio no tiene ningún cero en $\mathbb{Z}_p$ (por el pequeño Teorema de Fermat (4.54)) y, por tanto, es irreducible y separable (véase (5.52)).

Proposición 4.46. *Sea $K \subset F \subset E$ una torre de extensiones finitas.*

i) $E : K$ es separable si, y solo si, son separables $E : F$ y $F : K$.

ii) $E : K$ es puramente inseparable si, y solo si, son puramente inseparables $E : F$ y $F : K$.

Entonces, en una extensión finita $F : K$ puramente inseparable cada elemento $\alpha \in F$ genera una extensión $K(\alpha) : K$ que es puramente inseparable.

Definición 4.47. En una extensión algebraica $F : K$ un elemento $\alpha \in F$ se dirá que es *puramente inseparable* sobre K si $K(\alpha) : K$ es una extensión puramente inseparable.

Si $F : K$ es una extensión algebraica y si el elemento $\alpha \in F$ es puramente inseparable sobre K, el $Irr(\alpha, K)$ tiene solamente un cero y su multiplicidad es p^μ, como consecuencia de (4.30). Así $Irr(\alpha, K) = (X - \alpha)^{p^\mu} = X^{p^\mu} - \alpha^{p^\mu}$ y $\alpha^{p^\mu} \in K$, para algún número natural μ (4.32).

Observación 4.48. Es necesario destacar que el recíproco también es cierto. Si $\alpha^{p^\nu} \in K$ para algún número natural ν, sea μ el menor de tales enteros. Entonces $Irr(\alpha, K)$ es divisor de $X^{p^\mu} - \alpha^{p^\mu}$ en $K[X]$. Por tanto, $Irr(\alpha, K) = (X - \alpha)^n$ con $n \leqslant p^\mu$. En todo caso n es la multiplicidad de la raíz α del polinomio $Irr(\alpha, K)$ y, por tanto, debe ser una potencia de la característica (4.30). Así, $n = p^\lambda$ con $\lambda \leqslant \mu$ (para que sea $n = p^\lambda \leqslant p^\mu$). De este modo se tiene $Irr(\alpha, K) = (X - \alpha)^n = (X - \alpha)^{p^\lambda} = X^{p^\lambda} - \alpha^{p^\lambda} \in K[X]$, y en consecuencia $a^{p^\lambda} \in K$, con lo cual $\lambda = \mu$ por la minimalidad de μ. Obsérvese que se ha probado que si μ es el menor número natural tal que $\alpha^{p^\mu} \in K$, entonces $Irr(\alpha, K) = X^{p^\mu} - \alpha^{p^\mu}$.

Proposición 4.49. *Si $F : K$ es una extensión de cuerpos de característica $p \neq 0$, un elemento $\alpha \in F$ es puramente inseparable sobre K si, y solo si, existe un número natural μ tal que $\alpha^{p^\mu} \in K$. Si μ es el menor de tales números naturales, entonces $Irr(\alpha, K) = X^{p^\mu} - \alpha^{p^\mu}$.*

Esto sugiere la siguiente definición

Definición 4.50. Se dice que una extensión algebraica (no necesariamente finita) $F : K$ es *puramente inseparable* si cada $a \in F$ es puramente inseparable sobre K.

Ejemplos 4.51.

1.- Si K es un cuerpo de característica $p \neq 0$ no perfecto, entonces $K : K^p$ es una extensión puramente inseparable no trivial. Si $a \in K \setminus K^p$, entonces $Irr(a, K^p) = (X - a)^p$. Las extensiones $K^{p^s} : K^{p^t}$ (con $t \leqslant s$) son todas puramente inseparables.

2.- Si K es de característica $p \neq 0$ y K no es perfecto, el cuerpo $K^{\frac{1}{p^\infty}} := \cup_{\mu \in \mathbb{Z}} K^{\frac{1}{p^\mu}}$ es una extensión algebraica no finita puramente inseparable de K y de cualquiera de los cuerpos $K^{\frac{1}{p^\nu}}$.

Observación 4.52. Para una extensión algebraica $F : K$ de característica $p \neq 0$, la extensión $F : F_s(K)$ es puramente inseparable (4.42). Si $a \in F \setminus F_s(K)$ y $f = Irr(a, K)$

el polinomio f no es separable y existe un entero $\mu \geqslant 0$ tal que a^{p^μ} es raíz simple de un cierto polinomio separable $g \in K[X]$ tal que $f = g(X^{p^\mu})$ ((4.30) y (4.32)). El polinomio $Irr(a^{p^\mu}, K)$ es divisor en $K[X]$ del polinomio g y por ello también es separable. Entonces $a^{p^\mu} \in F$ es separable sobre K y $a^{p^\mu} \in F_s(K)$.

Si α, β son puramente inseparable sobre K y $\alpha^{p^s}, \beta^{p^r} \in K$, entonces para cualquier $x \in K(\alpha, \beta)$ se tiene $x^{p^{s+r}} \in K$ y, por lo tanto, una extensión finitamente generada por elementos puramente inseparables es puramente inseparable. En particular, para una extensión algebraica en característica p, el conjunto

$$F_{pi}(K) = \{\alpha \in F \mid \alpha \text{ es puramente inseparable sobre } K\}$$

es un subcuerpo de F que contiene a K.

Se tiene así que la extensión original $F : K$ determina un diagrama

$$\begin{array}{ccc} F_s(K) & \overset{pi}{\hookrightarrow} & F \\ \uparrow^{sep} & & \uparrow^{sep} \\ K & \overset{pi}{\hookrightarrow} & F_{pi}(K) \end{array}$$

Obsérvese que $F_s(K) \cap F_{pi}(K) = K$ y que $F = F_s(K) \cup F_{pi}(K)$.

4.5. Teorema del elemento primitivo

El siguiente Lema tendrá más aplicaciones en el futuro desarrollo de la materia y ahora posibilita la prueba del Teorema del elemento primitivo.

Lema 4.53. *Si G es un subgrupo finito del grupo multiplicativo de un cuerpo K, entonces G es cíclico.*

Demostración. Sea $\#G = n = p_1^{r_1} \cdots p_t^{r_t}$ la factorización de n en factores primos. Si, para cada $i = 1, \ldots, t$, H_i es el único p_i-subgrupo de Sylow de G, entonces $G = H_1 \cdots H_t \simeq H_1 \times \cdots \times H_t$ (1.51). Ya que los órdenes de dichos grupos son primos entre si, bastará entonces con demostrar que cada H_i es un grupo cíclico. Se ha reducido así el problema al caso en que el subgrupo finito H del grupo multiplicativo del cuerpo K es un p-grupo.

Sea H un p-grupo que es subgrupo del grupo K^* y sea $h \in H$ el máximo de los períodos de los elementos de H. Dicho período es necesariamente una potencia de p,

ya que divide al orden de H. Si $h = p^m$, entonces, para cada $x \in H$ se tiene $\mid x \mid = p^s$ con $s \leqslant m$ y, por lo tanto, $x^{p^m} = \left(x^{p^s}\right)^{p^{m-s}} = 1^{p^{m-s}} = 1$. En consecuencia, todos los elementos de H son ceros (en K) del polinomio

$$X^{p^m} - 1 \in K\,[X]$$

que admite a lo sumo p^m ceros. Por lo tanto, $\#H \leqslant p^m$ y así $\#\langle h\rangle = p^m \leqslant \#H \leqslant p^m$. Es decir, $\langle h\rangle = H$, ya que $\langle h\rangle \subset H$ y ambos son grupos finitos del mismo orden p^m. □

Proposición 4.54. *(Pequeño Teorema de Fermat)*

Si p es un número primo, $\mathbb{Z}_p^*$ es un grupo cíclico. En particular, si a es cualquier número entero se tiene $a \equiv a^p (\text{mód } p)$.

Demostración. El grupo multiplicativo $\mathbb{Z}_p^*$ es cíclico, por aplicación directa del Lema anterior, y tiene orden $p-1$. Por lo tanto, $\overline{a}^{p-1} = \overline{1}$ para todo $\overline{a} \in \mathbb{Z}_p^*$, pues $|\overline{a}|$ es necesariamente divisor de $p-1 = \#\mathbb{Z}_p^*$, y $\overline{a}^p = \overline{a}$ en este caso. Además si $\overline{a} = \overline{0}$ es evidente que $\overline{a} = \overline{a^p} = \overline{a}^p = \overline{0}$. Entonces $\overline{a}^p = \overline{a}$, para todo $\overline{a} \in \mathbb{Z}_p$. □

Nótese que en la prueba de la Proposición anterior no es necesario conocer que $\mathbb{Z}_p^*$ es cíclico, pues es suficiente con tener $\overline{a}^{p-1} = \overline{1}$ para todo $\overline{a} \in \mathbb{Z}_p^*$, lo cual es evidente pues el período de $\overline{a}$ es necesariamente divisor de $p-1 = \#\mathbb{Z}_p^*$.

Teorema 4.55. *(Teorema del elemento primitivo)*

Toda extensión finita y separable F de un cuerpo K es simple, es decir, existe un $\alpha \in F$ tal que $F = K(\alpha)$. El elemento α será denominado elemento primitivo de la extensión.

Demostración. En primer lugar consideramos el caso en que K es un cuerpo finito. Si $F : K$ es finita entonces F también es finito pues $\#F = (\#K)^{[F:K]}$ y, por (4.53), F^* es cíclico. Si α genera el grupo F^* se tiene también que $F = K(\alpha)$ y la hipótesis de separabilidad no es necesaria en este caso.

Se puede suponer ahora que K es un cuerpo infinito, condición que acoge al caso de característica nula (situación en la que la hipótesis de separabilidad sería redundante también (4.29)). Una extensión $F : K$ es finita si, y solo si, es finitamente generada por

elementos algebraicos (3.18). Por lo tanto, existe una torre

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n) = F$$

en la que cada α_i es algebraico y separable sobre $K(\alpha_1, \ldots, \alpha_{i-1})$ al serlo sobre K. Si se demuestra para $n = 2$ se habrá terminado la prueba ya que $K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3) = K(\gamma_1)(\alpha_3) = K(\gamma_1, \alpha_3) = K(\gamma_2)$, para ciertos $\gamma_1, \gamma_2 \in K(\alpha_1, \alpha_2, \alpha_3)$, (que serán también separables sobre K por serlo todo elemento de F), y recurrentemente tendremos $F = K(\gamma)$, para algún $\gamma \in F$. Así, la prueba quedará completa con la demostración del Lema siguiente. □

Lema 4.56. *Sean K un cuerpo infinito y E una extensión de K. Si $\alpha, \beta \in E$ son algebraicos y separables sobre K, entonces la extensión $F = K(\alpha, \beta)$ de K es simple.*

Demostración. Por la separabilidad de α y β, los polinomios $f = Irr(\alpha, K)$ y $g = Irr(\beta, K)$ se factorizan en $\overline{K} = \overline{F}$ cada uno de ellos en factores lineales diferentes

$$\begin{aligned} f &= \prod_1^r (X - \alpha_i) \\ g &= \prod_1^s (X - \beta_j), \end{aligned}$$

donde, pongamos por caso, $\alpha = \alpha_1$ y $\beta = \beta_1$.

Como K es infinito se puede elegir $c \in K$ tal que $c \neq \dfrac{\alpha - \alpha_i}{\beta j - \beta}$, para todo $i = 1, \ldots, r$ y todo $j = 2, \ldots, s$. Si $\gamma = \alpha + c\beta \in K(\alpha, \beta)$, entonces $K \subset K(\gamma) \subset F = K(\alpha, \beta)$ y β es algebraico sobre $K(\gamma)$ al serlo sobre K. Sea $g_1 = Irr(\beta, K(\gamma))$ que escindirá en factores lineales $g_1 = (X - \beta) \prod_l (X - \delta_l)$ en $\overline{F}$ (β y las $\delta_l \in \overline{F}$ son las raíces de g_1, también de multiplicidad 1 ya que β es separable sobre $K(\gamma)$). Sea $h = f(\gamma - cX) \in K(\gamma)[X]$. Entonces $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$, y como $g \in K[X] \subset K(\gamma)[X]$ tiene a β como raíz, el polinomio g_1 divide a h y a g en $K(\gamma)[X]$. Por tanto,

$$\{\beta\} \subset \{\text{ceros de } g_1 \text{ en } \overline{F}\} \subset \{\text{ceros de } g \text{ en } \overline{F}\} \cap \{\text{ceros de } h \text{ en } \overline{F}\}.$$

Ahora, $\forall j = 2, \ldots, s$, la raíz β_j de g no es un cero de h pues, en caso contrario, se tendría $h(\beta_j) = f(\gamma - c\beta_j) = 0$ y $\gamma - c\beta_j = \alpha_i$, para algún $i \in \{1, 2, \ldots, r\}$, con lo cual $\alpha + c\beta - c\beta_j = \alpha_i$ y, de este modo, sería $c = \dfrac{\alpha - \alpha_i}{\beta_j - \beta}$, lo que contradice la selección de c.

Por lo tanto, $\{\text{ceros de } g \text{ en } \overline{F}\} \cap \{\text{ceros de } h \text{ en } \overline{F}\} = \{\beta\} = \{\text{ceros de } g_1 \text{ en } \overline{F}\}$. Entonces $g_1 = X - \beta$, y así $\beta \in K(\gamma)$, con lo que resulta $\alpha = \gamma - c\beta \in K(\gamma)$ y se tiene que $K(\alpha, \beta) \subset K(\gamma)$ y, por lo tanto, la igualdad buscada $F = K(\alpha, \beta) = K(\gamma)$. □

4.6. Extensiones normales. Clausura normal

El objetivo de esta sección es analizar más detenidamente la naturaleza de los cuerpos de escisión considerando sus posibles encajes en la clausura algebraica del cuerpo base. Este nuevo punto de vista tendrá gran importancia en el estudio de la Teoría de Galois.

Definición 4.57. Una extensión algebraica $E : K$ se dice que es *normal* si cada polinomio irreducible en $K[X]$ que tiene un cero en E escinde en E.

Ejemplos 4.58.

1.- La clausura algebraica $\overline{K}$ es una extensión normal de K.

2.- Si $[E : K] = 2$, entonces $E : K$ es normal.

En efecto, sea f un polinomio irreducible en $K[X]$ que tiene un cero $\alpha \in E$. Veamos que f escinde en E. El elemento α es algebraico sobre K y, como f es irreducible en $K[X]$, $f = cIrr(\alpha, K)$, donde c es el coeficiente principal de f. Ahora $\partial(f) = [K(\alpha) : K] \leqslant [E : K] = 2$, y por tanto, o f es lineal, en cuyo caso escinde en K y, como consecuencia, en E, o $f = c(X - \alpha)g$ con $g \in E[X]$ y $\partial(g) = 1$, con lo cual g escinde en E. Por tanto, f escinde en E en cualquier caso.

Recuérdese que para grupos existe un resultado con formulación semejante:

"Si H es un subgrupo del grupo G y $(G : H) = 2$, entonces H es subgrupo normal de G".

Esto no es casual, como quedará claro a la vista del Teorema Fundamental de Teoría de Galois.

En particular, como $[\mathbb{C} : \mathbb{R}] = 2$, la extensión $\mathbb{C} : \mathbb{R}$ es normal, y es normal también la extensión $\mathbb{Q}(\sqrt{n}) : \mathbb{Q}$, para todo $n \in \mathbb{N}$.

3.- Si $p > 0$ es un número primo la extensión $\left[\mathbb{Q}\left(\sqrt[3]{p}\right) : \mathbb{Q}\right]$ no es normal, pues $X^3 - p = Irr(\sqrt[3]{p}, \mathbb{Q})$, y este polinomio irreducible tiene una raíz, $\sqrt[3]{p}$, en $\mathbb{Q}\left(\sqrt[3]{p}\right)$ pero

las otras dos raíces son complejas no reales y no son elementos de $\mathbb{Q}\left(\sqrt[3]{p}\right)$.

Teorema 4.59. *Sea $E : K$ una extensión finita y sea $\overline{E}$ una clausura algebraica de E (y por lo tanto de K). Son equivalentes las afirmaciones*

i) La extensión $E : K$ es normal.

ii) E es cuerpo de escisión sobre K de algún polinomio $f \in K[X]$.

iii) Todo encaje $\sigma\colon E \to \overline{K} = \overline{E}$ sobre K es un automorfismo de E (es decir, $\sigma(E) = E$).

Demostración. i) $\Rightarrow$ ii)

Como $E : K$ es finita, existen $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = K(\alpha_1, \ldots, \alpha_n)$ (3.18). Sea $f_i = Irr(\alpha_i, K)$, para $i = 1, \ldots n$, y sea $f = \prod_1^n f_i \in K[X]$. Ya que $E : K$ es normal, cada polinomio f_i escinde en E pues tiene en E al menos una raíz, α_i. Como toda raíz β de f es raíz de algún f_i, el polinomio f escinde también en $E = K(\alpha_1, \ldots, \alpha_n)$. Ahora E está generado sobre K por las raíces de f (de hecho basta con $\alpha_1, \ldots, \alpha_n$ pues, como ya se ha dicho, las restantes están en $E = K(\alpha_1, \ldots, \alpha_n)$). Entonces E es cuerpo de escisión de f sobre K.

ii) $\Rightarrow$ iii)

Sea $f \in K[X]$ tal que E es cuerpo de escisión de f sobre K y sea $\sigma\colon E \to \overline{E}$ un encaje sobre K. Ahora $E = K(\alpha_1, \ldots, \alpha_n)$ en donde las $\alpha_1, \ldots, \alpha_n$ son todas las raíces de f en $\overline{E}$. Como $\sigma|_K = id_K$ y $f \in K[X]$ se tiene $f^\sigma = f$, y entonces $\sigma(f(\alpha_i)) = f^\sigma(\sigma(\alpha_i)) = f(\sigma(\alpha_i)) = \sigma(0) = 0$; por tanto $\sigma(\alpha_i)$ es también un cero de f en $\overline{E}$ para cada $i = 1, \ldots, n$. Así σ establece una permutación de las raíces $\alpha_1, \ldots, \alpha_n$ y, en consecuencia, $\sigma(E) \subset E$. Como σ es también homomorfismo inyectivo de K-espacios se tiene que $\dim_K \sigma(E) = \dim_K E$, con lo cual resulta $E = \sigma(E)$ ya que ambos K-espacios tienen la misma dimensión finita.

iii) $\Rightarrow$ i)

Sea $f \in K[X]$ un polinomio irreducible en $K[X]$ que tiene un cero α en E. Se trata de demostrar que f escinde en E. Sea $\beta \in \overline{E} = \overline{K}$ otro cero de f. Por el Teorema de extensión de encajes a extensiones simples, existe un isomorfismo $\tau\colon K(\alpha) \to K(\beta)$ sobre K tal que $\tau(\alpha) = \beta$, pues ambos elementos tienen el mismo polinomio irreducible

$g = c^{-1}f$ sobre K, donde c es el coeficiente principal de f. El isomorfismo τ determina un encaje γ sobre K definido como la composición de τ con la inclusión $K(\beta) \hookrightarrow \overline{E}$, es decir, $\gamma\colon K(\alpha) \xrightarrow{\tau} K(\beta) \hookrightarrow \overline{E}$. Como $E : K$ es algebraica y $\overline{E}$ es algebraicamente cerrado, nuestro γ se extiende a un $\sigma\colon E \to \overline{E}$ que es un encaje sobre K (4.18). En virtud de la hipótesis *iii*) $\sigma(E) = E$, y así $\beta = \sigma(\alpha)$ es un elemento de E pues $\alpha \in E$. Por lo tanto, cada raíz de f en $\overline{E}$ es elemento de E y f escinde en E. □

Este último Teorema establece claramente que la condición de normalidad para extensiones finitas es una nueva propiedad de los cuerpos de escisión.

Corolario 4.60. *Si $K \subset F \subset E$ es una torre de cuerpos y si $E : K$ es normal finita, entonces la extensión finita $E : F$ es también normal.*

Demostración. $E : F$ es finita por (3.3), y en virtud del apartado *ii*) del Teorema anterior, E es cuerpo de escisión de un polinomio $f \in K[X]$ sobre K y, por ello, también lo es sobre F. □

Veremos que en las hipótesis del Corolario 4.60 la extensión $F : K$ no es necesariamente normal. El apartado *iii*) del Teorema 4.59 permite establecer una condición bajo la cual sí lo es.

Corolario 4.61. *Si $K \subset F \subset E$ es una torre de cuerpos y $E : K$ es normal finita, entonces son equivalentes*

i) *$F : K$ es normal.*

ii) *Para cada automorfismo $\tau\colon E \to E$ sobre K se tiene que $\tau(F) = F$.*

Demostración. *i*) $\Rightarrow$ *ii*)

Si τ es un automorfismo de E sobre K, el encaje $\sigma\colon F \to \overline{F} = \overline{E}$ definido por

$$F \hookrightarrow E \xrightarrow{\tau} E \hookrightarrow \overline{F}$$

es necesariamente un automorfismo de F, en virtud del Teorema 4.59, ya que, por hipótesis, $F : K$ es normal. Como $\tau(F) = \sigma(F)$ se tiene el resultado.

ii) $\Rightarrow$ *i*)

Como consecuencia del apartado *iii*) del Teorema 4.59 bastará con demostrar que cada encaje $\tau\colon F \to \overline{F} = \overline{E} = \overline{K}$ sobre K es un automorfismo de F. Para un tal

encaje existe una extensión $\sigma\colon E \to \overline{F}$ ya que $E : F$ es algebraica (por ser finita) y $\overline{F}$ es algebraicamente cerrado (4.18). Como $E : K$ es normal finita, $\sigma(E) = E$ por el mencionado apartado del Teorema 4.59, y, en virtud de la hipótesis, se tiene $\sigma(F) = F = \tau(F)$. □

Ejemplos 4.62.

1.- Si $\xi = \cos\frac{2\pi}{3} + i sen\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}. \in \mathbb{C}$, entonces $\mathbb{Q}\left(\sqrt[3]{2}, \xi\right)$ es cuerpo de escisión de $X^3 - 2$ sobre $\mathbb{Q}$.

En efecto, los elementos $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, $\xi^2\sqrt[3]{2} \in \mathbb{C}$ son las raíces de dicho polinomio y todas están en la extensión $\mathbb{Q}\left(\sqrt[3]{2}, \xi\right)$ de $\mathbb{Q}$. Por lo tanto, $\mathbb{Q}\left(\sqrt[3]{2}, \xi\right) : \mathbb{Q}$ es una extensión finita (está generada por un número finito de elementos algebraicos sobre $\mathbb{Q}$) y también normal (4.59). Sin embargo la extensión intermedia $\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}$ no es normal ya que el polinomio $X^3 - 2 = Irr(\sqrt[3]{2}, \mathbb{Q})$ tiene un cero en $\mathbb{Q}\left(\sqrt[3]{2}\right)$ pero no los restantes (en caso contrario se tendría que $\xi = \left(\sqrt[3]{2}\right)^{-1}\xi\sqrt[3]{2} \in \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{R}$, lo cual es absurdo).

Es importante señalar también que si en una torre $K \subset F \subset E$ de extensiones finitas se tiene que $F : K$ y $E : F$ son extensiones normales, en general no es normal la extensión $E : K$, como se ve en el siguiente ejemplo

2.- Sean $\sqrt{2}, \sqrt[4]{2} \in \mathbb{R}$. Las extensiones $\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}$ y $\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)$ son normales y finitas y, sin embargo, la extensión finita $\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}$ no es normal.

En efecto, como $Irr(\sqrt[4]{2}, \mathbb{Q}\left(\sqrt{2}\right)) = X^2 - \sqrt{2}$ e $Irr(\sqrt{2}, \mathbb{Q}) = X^2 - 2$, se verifica que $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2 = \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right]$, y así ambas extensiones son normales. La extensión $\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}$ no es normal ya que el polinomio $X^4 - 2 = Irr(\sqrt[4]{2}, \mathbb{Q})$ no escinde en $\mathbb{Q}\left(\sqrt[4]{2}\right)$, que es un subcuerpo de $\mathbb{R}$, y no todos los ceros de $X^4 - 2$ son reales (los únicos ceros reales de dicho polinomio son $\pm\sqrt[4]{2}$).

Recuérdese que si $L \subset H \subset G$ es una torre de grupos y si L es normal en G, entonces L es normal en H, pero H puede no ser normal en G. También, aunque L sea normal en H y H sea normal en G no se tiene en general que L sea normal en G.

Estos resultados de grupos son los correspondientes análogos a los referidos en los dos anteriores ejemplos de extensiones normales de cuerpos.

Teorema 4.63. *Si $L : K$ es una extensión finita, existe una extensión $F : L$ que verifica*

i) $F : K$ es normal finita.

ii) Si $F' : K$ es otra extensión normal tal que $K \subset L \subset F' \subset F$, entonces $F = F'$.

Si además si $L : K$ es separable también lo es $F : K$. En cualquier caso, el cuerpo F está determinado salvo isomorfismos sobre L y será denominado "clausura normal de L sobre K".

Demostración. Por ser finita la extensión $L : K$, existen $\alpha_1, \ldots \alpha_n \in L$ que son algebraicos sobre K, tales que $L = K(\alpha_1, \ldots, \alpha_n)$. Para cada $i = 1, \ldots, n$, sea $f_i = Irr(\alpha_i, K)$ y sea $f = \prod_1^n f_i$. Si $F \subset \overline{L}$ es cuerpo de escisión de f sobre K, la extensión $F : K$ es finita (está generada por un número finito de elementos algebraicos sobre K, las raíces en $\overline{L}$ del polinomio f) y $F : K$ es normal, por el Teorema 4.59. Como los elementos α_i son ceros de f en L, se tiene $L = K(\alpha_1, \ldots, \alpha_n) \subset F$ y se cumple la condición i).

Sea ahora $F' : K$ normal y $F \supset F' \supset L \supset K$. Entonces, como $L = K(\alpha_1, \ldots, \alpha_n)$, cada cero de $f_i = Irr(\alpha_i, K)$ en $\overline{F} = \overline{L}$ es elemento de F' ya que, por hipótesis, $F' : K$ es normal. Así, todos los ceros de $f = \prod_i^n f_i$ están en F' y, como tales ceros son los generadores de F sobre K, se tiene $F \subset F'$ y, por tanto, la igualdad $F = F'$.

Supóngase ahora que $L : K$ separable y finita. En ese caso $L = K(\alpha)$ para algún $\alpha \in L$ separable sobre K (4.55). El cuerpo F está ahora generado por todos los ceros en $\overline{L}$ del $Irr(\alpha, K)$ que es un polinomio separable. Entonces la extensión $F : K$ es separable al ser separables sobre K todos los generadores de F pues todos ellos tienen el mismo polinomio irreducible sobre K que α (4.42).

Para probar la última afirmación sea, como antes, $F \subset \overline{L}$ cuerpo de escisión de $f = \prod_1^n f_i$ sobre K, y sea E la clausura normal de L construida dentro de otra clausura algebraica $\overline{L}'$ de L. Por la Proposición 4.18 sabemos que existe un isomorfismo $\sigma : \overline{L} \to \overline{L}'$ sobre L. Entonces $\sigma(F)$ está generado sobre K por el conjunto $\{\sigma(\beta) \mid \beta \text{ es un cero de } f \text{ en } \overline{L}\}$. Los $\alpha_1, \ldots, \alpha_n \in L$, que son elementos de dicho conjunto, son también elementos de E y, por tanto, $\sigma(\beta) \in E$, ya que $E : K$ es normal y cada $\sigma(\beta)$ es cero de algún $f_i = Irr(\alpha_i, K)$. En consecuencia, $\sigma(F) \subset E$, y como además $\sigma(F) : K$ es normal (es cuerpo de escisión, dentro de $\overline{L}'$, de $f^\sigma = f$ sobre K), resulta $\sigma(F) = E$ por la minimalidad de la clausura normal E. □

Si $F = K(\alpha_1, \ldots, \alpha_n)$ con cada α_i algebraico sobre K, entonces solamente hay un

número finito de encajes $\sigma\colon F \to \overline{K} = \overline{F}$. En efecto, cada uno de tales encajes σ está determinado por los elementos $\sigma(\alpha_i)$ que han de ser necesariamente raíces de $Irr(\alpha_i, K)$, y así son posibles solamente un número finito de tales encajes.

Proposición 4.64. *Si $F : K$ es una extensión finita y $\sigma_1 = id_F, \sigma_2, \ldots, \sigma_t$ son los diferentes encajes de F en $\overline{K} = \overline{F}$ sobre K, entonces la clausura normal de F sobre K es el cuerpo $N = \sigma_1(F)\,\sigma_2(F)\cdots\sigma_t(F)$.*

Demostración. La extensión $N : K$ es finita al serlo las $\sigma_i(F) : K$, para $i = 1, \ldots, t$. Para probar la normalidad de la extensión, sea $\tau\colon N \to \overline{K} = \overline{F} = \overline{N}$ un encaje sobre K. La composición de la restricción de τ a $\sigma_i(F)$ con σ_i es, necesariamente, uno de los encajes $\sigma_{j_i} := F \overset{\sigma_i}{\to} \sigma_i(F) \hookrightarrow N \overset{\tau}{\to} \overline{K} = \overline{F} = \overline{N}$. Por lo tanto,

$$\tau(N) = \tau(\sigma_1(F)\cdots\sigma_t(F)) = \tau(\sigma_1(F))\cdots\tau(\sigma_t(F)) = \sigma_{j_1}(F)\cdots\sigma_{j_t}(F) = N,$$

pues la composición con τ establece una permutación de $\sigma_1, \ldots, \sigma_t$, según se ha dicho. Por lo tanto, la extensión $N : K$ es normal (4.59) y $F \subset N$. Sea ahora $E : K$ normal con $F \subset E \subset N$. Entonces E contiene a cada uno de los cuerpos $\sigma_i(F)$ y $E = N$. En efecto, cada encaje $\sigma_i\colon F \to \overline{K} = \overline{F} = \overline{N} = \overline{E}$ sobre K se extiende a un encaje $\sigma_i'\colon E \to \overline{E}$ para el cual se tiene $\sigma_i'(E) = E$, en virtud de (4.59), y $\sigma_i(F) \subset \sigma_i'(E) \subset E$. □

4.7. Ejercicios

1.- Sea α la raíz séptima real de 3 y ξ una raíz séptima de 1, $\xi \neq 1$. Pruébese que $\mathbb{Q}(\xi, \alpha)$ es cuerpo de escisión para $X^7 - 3$ sobre $\mathbb{Q}$.

2.- Encuéntrese un cuerpo de escisión sobre $\mathbb{Q}$ para cada uno de los polinomios siguientes:
X^4+5X^2+6, X^7-1, X^3-3X^2+3X-2, X^4-3, X^6-8, X^6+1, $(X^2-3)(X^2-7)$, X^5-2 y $(X^3-2)(X^2-7)$.
Determínense los grados de las correspondientes extensiones.

3.- Sea $f = (X^{12} - 16)(X^2 - 3) \in \mathbb{Q}[X]$. Demuéstrese que $E = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}, i\right)$ es un cuerpo de escisión para f sobre $\mathbb{Q}$ y calcúlese $[E : \mathbb{Q}]$.

4.- Si E_f denota un cuerpo de escisión sobre $\mathbb{Q}$ de $f \in \mathbb{Q}[X]$, encuéntrese un elemento primitivo para la extensión $E_f : \mathbb{Q}$ en cada uno de los siguientes casos:
a) $f = X^4 + 1$.
b) $f = X^4 + 4$.

5.- Obténgase el grupo de Galois de cada uno de los siguientes polinomios sobre los cuerpos especificados:

a) $X^3 - X - 1 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$.

b) $X^3 - 10 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}\left(\sqrt{2}\right)$ y sobre $\mathbb{Q}\left(i\sqrt{3}\right)$.

c) $X^3 - X - 1 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}(\sqrt{-23})$.

d) $X^4 - 5 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}\left(\sqrt{5}\right)$, sobre $\mathbb{Q}\left(\sqrt{-5}\right)$ y sobre $\mathbb{Q}(i)$.

6.- Sean $E : F : K$ extensiones finitas de cuerpos.

a) Pruébese que si $E : K$ es normal, entonces $E : F$ es normal.

b) Si $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$ y $E = \mathbb{Q}(\sqrt[3]{2}, \xi)$, siendo ξ una raíz primitiva sexta de la unidad, pruébese que $E : K$ es normal y que $F : K$ no es normal.

7.- Se consideran cuerpos de escisión E_f y E_g sobre $\mathbb{Q}$ de los polinomios $f = X^6 - 2$ y $g = X^3 - 2$, respectivamente.

a) Pruébese que $Eg \subset E_f$ y calcúlese $[E_f : \mathbb{Q}]$.

b) Sea β un cero de f en $\mathbb{C}$. Expresar β^{-1} como combinación lineal de una $\mathbb{Q}$-base de $\mathbb{Q}(\beta)$ y calcúlese $Irr(\beta^{-1}, \mathbb{Q})$.

8.- Sean $f = \left(X^2 - 3\right)\left(X^3 + 1\right), g = \left(X^2 - 2X - 2\right)\left(X^2 + 1\right) \in \mathbb{Q}[X]$. Pruébese que $\mathbb{Q}\left(\sqrt{3}, i\right)$ es cuerpo de escisión sobre $\mathbb{Q}$ tanto de f como de g.

9.- Justifíquense las siguientes afirmaciones

a) El polinomio $X^5 - 9X^3 + 15X + 6 \in \mathbb{Q}[X]$ tiene al menos un cero real.

b) $X^5 - 9X^3 + 15X + 6$ es irreducible en $\mathbb{Q}\left(\sqrt[3]{2}\right)[X]$.

c) La extensión $\mathbb{Q}\left(\sqrt[3]{2}, i\right) : \mathbb{Q}$ es de grado 6 y no es normal.

10.- Sea α la raíz quinta real de 3 y ξ una raíz quinta de 1, $\xi \neq 1$. Pruébese que $\mathbb{Q}(\alpha, \xi)$ es un cuerpo de escisión de $X^5 - 3$ sobre $\mathbb{Q}$ y calcúlese $[\mathbb{Q}(\alpha, \xi) : \mathbb{Q}]$.

11.- Pruébese que si $f \in K[X]$ es irreducible de grado n y E es un cuerpo de escisión para f sobre K, entonces n divide a $[E : K]$. Plantéese un ejemplo que muestre que esto no es necesariamente cierto si f no es irreducible.

12.- Sea $f = X^4 + X^2 + 1 \in \mathbb{Q}[X]$. Demuéstrese que un cuerpo de escisión para f sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha)$, siendo $\alpha = \dfrac{-1 + i\sqrt{3}}{2}$.

13.- Sea E un cuerpo de escisión de $(X^3 - 2)(X^2 - 5)$ sobre $\mathbb{Q}(\sqrt{-3})$. Calcúlese $\left[E : \mathbb{Q}(\sqrt{-3})\right]$.

14.- Sean $L_1 = \mathbb{Q}(\sqrt{3})$ y $L_2 = \mathbb{Q}(\sqrt{\sqrt{3} + 1})$. Demuéstrese que $L_1 : \mathbb{Q}$ y $L_2 : L_1$ son normales y que $L_2 : \mathbb{Q}$ no lo es.

15.- Sea $f = X^5 - X^4 - X^3 - X^2 - X - 2 \in \mathbb{Q}[X]$.

a) Factorícese f en irreducibles en $\mathbb{Q}[X]$. Calcúlese un cuerpo de escisión E_f para f sobre $\mathbb{Q}$ y el grado de la extensión $E_f : \mathbb{Q}$.

b) Demuéstrese que si $a \in \mathbb{Z}$, f no tiene ningún cero en común con el polinomio $X^3 - 3aX + 3$.

16.- Sea $\alpha = (1+i)\sqrt[4]{5}$. Pruébese que $\mathbb{Q}(\alpha) : \mathbb{Q}\left(i\sqrt{5}\right)$ es normal. Demuéstrese que $\mathbb{Q}(\alpha) : \mathbb{Q}$ no es normal y encuéntrese una clausura normal de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

17.- Pruébese que $\mathbb{Q}\left(\sqrt{2}\right)$ y $\mathbb{Q}(i)$ son isomorfos como $\mathbb{Q}$-espacios vectoriales pero no como cuerpos.

18.- Calcúlese el número de $\mathbb{Q}$-isomorfismos entre $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\beta)$ en los siguientes casos

a) $\alpha = i\sqrt{2}$ y $\beta = i\sqrt{3}$.

b) $\alpha = e^{\frac{2\pi}{5}i}$ y $\beta = \alpha^3$.

Capítulo 5

Teoría de Galois

5.1. Extensiones de Galois. Teorema fundamental de la teoría de Galois

Esta sección está dedicada a la demostración del Teorema fundamental de la teoría de Galois para extensiones de cuerpos. Para una tal extensión $F : K$ se considera el grupo de automorfismos de F que dejan fijos los elementos de K, y el resultado fundamental establece que, bajo ciertas condiciones, existe una biyección, que invierte las inclusiones, entre el retículo de subgrupos de dicho grupo y el de cuerpos intermedios de la extensión.

Si F es un cuerpo, el conjunto $Aut(F)$ de todos los automorfismos de F es un grupo con la operación definida por la composición de aplicaciones.

Definición 5.1. Sean F un cuerpo y G un subgrupo del grupo $Aut(F)$. Se define el *cuerpo fijo por* G como

$$F^G := \{x \in F \mid \sigma(x) = x, \forall \sigma \in G\}.$$

Si $F : K$ es una extensión de cuerpos se define el *grupo de Galois de la extensión* $F : K$ como

$$Gal(F/K) := \{\sigma \in Aut(F) \mid \sigma|_K = id_K\}.$$

Observaciones 5.2.

1) F^G es efectivamente un subcuerpo de F, ya que para $x, y \in F^G$ y para cualquier elemento $\sigma \in G$, se tiene $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$, $\sigma(xy) = \sigma(x)\sigma(y) = xy$,

$\sigma(-x) = -\sigma(x) = -x$ y, si $x \neq 0$, $\sigma\left(x^{-1}\right) = (\sigma(x))^{-1} = x^{-1}$. Entonces $x - y \in F^G$ y, si $y \neq 0$, $xy^{-1} \in F^G$.

También es inmediato comprobar que $Gal(F/K)$ es un subgrupo del grupo $Aut(F)$, pues si $\sigma, \tau \in Gal(F/K)$, entonces $\forall x \in K$ se tiene $(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$ y también $\sigma(x) = x \Leftrightarrow \sigma^{-1}(\sigma(x)) = \sigma^{-1}(x) \Leftrightarrow x = \sigma^{-1}(x)$.

2) Sean $F : K$ y $F' : K'$ extensiones de cuerpos y $\alpha \in F$ un elemento algebraico sobre K. Si $\tau\colon K \to K'$ y $\sigma\colon F \to F'$ son encajes tales que $\sigma|_K = \tau$ (es decir, si σ es un encaje sobre τ), entonces $\sigma|_{K(\alpha)}\colon K(\alpha) \to F'$ está determinado por el elemento $\sigma(\alpha) \in F'$. En efecto, cada $x \in K(\alpha)$ admite una única expresión $x = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, con $a_0, a_1, \ldots, a_{n-1} \in K$, si el polinomio $Irr(\alpha, K)$ es de grado n, ya que en este caso $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ constituye una base de $K(\alpha)$ como K-espacio (3.14). Entonces $\sigma(x) = \tau(a_0) + \tau(a_1)\sigma(\alpha) + \cdots + \tau(a_{n-1})\sigma(\alpha)^{n-1}$. En particular, poniendo $K = K'$ y $F = F' = K(\alpha)$, resulta que cada automorfismo $\sigma \in Gal(K(\alpha)/K)$ está determinado por $\sigma(\alpha) \in K(\alpha)$.

3) Además $\sigma(\alpha)$ es un cero del polinomio $(Irr(\alpha, K))^{\tau} \in K'[X]$, pues si $Irr(\alpha, K) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$, entonces $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0 \Rightarrow \sigma\left(\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0\right) = \sigma(\alpha)^n + \tau(b_{n-1})\sigma(\alpha)^{n-1} + \cdots + \tau(b_0) = \sigma(0) = 0$. En particular, se obtiene que $\sigma(\alpha)$ es necesariamente un cero de $Irr(\alpha, K)$, para cada $\sigma \in Gal(K(\alpha)/K)$.

4) Nótese que, en virtud del Teorema de extensión de encajes a extensiones simples (4.4), para cada raíz $\beta \in K(\alpha)$ del $Irr(\alpha, K)$ existe un encaje $\sigma_{\alpha,\beta}\colon K(\alpha) \to K(\alpha)$ tal que $\sigma_{\alpha,\beta}(\alpha) = \beta$. Tal encaje debe ser un automorfismo de $K(\alpha)$, ya que $\sigma_{\alpha,\beta}$ es, en particular, un homomorfismo inyectivo entre K-espacios de la misma dimensión finita.

Como consecuencia de las anteriores observaciones se obtiene directamente la siguiente

Proposición 5.3. *Si $F : K$ es una extensión de cuerpos y si $\alpha \in F$ es algebraico sobre K, entonces $\#(Gal(K(\alpha)/K)) \leqslant \partial(Irr(\alpha, K)) = [K(\alpha) : K] \leqslant [F : K]$.*

La desigualdad $\#(Gal(K(\alpha)/K)) \leqslant [K(\alpha) : K]$ es estricta en general. Por ejemplo, para la extensión $\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}$ se tiene que $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = \partial(Irr\left(\sqrt[3]{2}, \mathbb{Q}\right)) = \partial\left(X^3 - 2\right) = 3$, mientras que es 1 el orden del grupo de Galois de dicha extensión. La última afirmación es consecuencia de que si $\sigma \in Gal(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q})$, entonces

$\sigma\left(\sqrt[3]{2}\right) \in \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{R}$ ha de ser necesariamente un cero real de $X^3 - 2$ (5.2), y por tanto $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$, con lo que $\sigma = id_{\mathbb{Q}\left(\sqrt[3]{2}\right)}$ (5.2). El único cero real de $X^3 - 2$ es $\sqrt[3]{2}$; los restantes ceros son $\sqrt[3]{2}\xi$ y $\sqrt[3]{2}\xi^2$, en donde $\xi = \cos\dfrac{2\pi}{3} + isen\dfrac{2\pi}{3} = e^{\frac{2\pi i}{3}}$, y ambos son números complejos no reales.

Proposición 5.4. *Sea $F : K$ una extensión normal finita.*

1) *Si $\alpha, \beta \in F$ se tiene*

$$Irr(\alpha, K) = Irr(\beta, K) \Leftrightarrow \exists \sigma \in Gal\,(F/K) \text{ tal que } \sigma\,(\alpha) = \beta.$$

2) *Si además $F : K$ es separable se tiene*

$$\#Gal\,(F/K) = [F : K]\,.$$

Demostración. La afirmación 1) resulta del Teorema de extensión de encajes a extensiones simples (4.4) y de la aplicación combinada de la Proposición 4.18 y del Corolario 4.61. En efecto,

$$Irr(\alpha, K) = Irr(\beta, K) \Leftrightarrow \exists \sigma_{\alpha,\beta} \colon K\,(\alpha) \to K\,(\beta) \ K\text{-isomorfismo tal que } \sigma_{\alpha,\beta}\,(\alpha) = \beta.$$

Ahora, para $K\,(\alpha) \overset{\sigma_{\alpha,\beta}}{\to} K\,(\beta) \hookrightarrow F \hookrightarrow \overline{F}$ existe una extensión $\sigma \colon F \to \overline{F}$ (por 4.18) que es un automorfismo de F sobre K (4.59), tal que $\sigma\,(\alpha) = \beta$. Recíprocamente, si $\sigma \in Gal\,(F/K)$ es tal que $\sigma\,(\alpha) = \beta$, la Proposición 4.3 proporciona que $Irr(\alpha, K) = Irr(\beta, K)$.

Para la demostración de 2) considérese un elemento primitivo $\alpha \in F$ de la extensión $F : K$, que existe al ser $F : K$ separable (4.55). Así, $F = K\,(\alpha)$ y $f = Irr(\alpha, K)$ es separable y $[F : K] = \partial(f) = n$. Como la extensión $F : K$ es normal el polinomio f escinde en F y, por tanto, F es cuerpo de escisión de f sobre K. Si $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ son los diferentes ceros de f en F, se tiene que $f = Irr(\alpha_i, K)$ para cada $i = 1, \ldots, n$, y, en virtud del apartado 1), para cada α_i existe un $\sigma_i \in Gal\,(F/K)$ tal que $\sigma_i\,(\alpha) = \alpha_i$. Se obtienen así n automorfismos de F sobre K diferentes, con lo cual resulta que $n = [F : K] \leqslant \#Gal\,(F/K)$. De la Proposición 5.3 se deduce directamente que $[F : K] \geqslant \#Gal\,(F/K)$, y de ahí el resultado. □

Ejemplos 5.5.

1.- $Gal(\mathbb{C}/\mathbb{R}) \simeq Z_2$.

2.- $Gal(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q})$ es el grupo de un solo elemento.

Consideramos ahora a cada subgrupo H del grupo $Gal\,(E/K)$ actuando sobre el cuerpo E mediante la acción

$$\begin{array}{rcl} H \times E & \to & E \\ (\sigma, \alpha) & \mapsto & \sigma\,(\alpha)\,. \end{array}$$

Recuérdese que si $\alpha \in E$, la H-órbita de α es el conjunto $\mathfrak{O}_H\,(\alpha) := H\alpha = \{\sigma\,(\alpha) = \sigma\alpha \mid \sigma \in H\}$ (1.40), y que si $H_\alpha := \{\sigma \in H \mid \sigma\,(\alpha) = \alpha\}$ denota el subgrupo de isotropía de α, entonces $\#\,\mathfrak{O}_H\,(\alpha) = (H : H_\alpha)$ que es un divisor de $\#H$ si este grupo es finito (1.41).

El siguiente Lema será muy usado en lo sucesivo.

Lema 5.6. *Sea $E : K$ una extensión finita y H un subgrupo de $G = Gal(E/K)$. Entonces si $\alpha \in E$, α es algebraico sobre E^H y además*

$$Irr(\alpha, E^H) = \prod_{\sigma(\alpha) \in \mathfrak{O}_H(\alpha)} (X - \sigma\,(\alpha))\,.$$

Por lo tanto,

$$\left[E^H\,(\alpha) : E^H\right] = \#\mathfrak{O}_H\,(\alpha) = (H : H_\alpha)$$

es divisor de $\#H$.

Demostración. La extensión $E : E^H$ es finita (al ser E^H un cuerpo intermedio entre E y K) y, por ello, es algebraica. Sea $\alpha \in E$ y sea $f = Irr\left(\alpha, E^H\right)$, cada $\sigma\,(\alpha)$ es necesariamente un cero de f en E si $\sigma \in H \subset Gal(E/E^H)$ y, por lo tanto, el polinomio $g = \prod_{\sigma(\alpha) \in \mathfrak{O}_H(\alpha)} (X - \sigma\,(\alpha)) \in E\,[X]$ es un divisor de f en el anillo $E\,[X]$. Por otra parte, si $\tau \in H$ se tiene $\tau H = H$ y entonces $\mathfrak{O}_H\,(\alpha) = \{\sigma\,(\alpha) \mid \sigma \in H\} = \{\tau\sigma\,(\alpha) \mid \sigma \in H\}$, con lo cual resulta que

$$g^\tau = \prod_{\sigma(\alpha) \in \mathfrak{O}_H(\alpha)} (X - \tau\sigma\,(\alpha)) = \prod_{\sigma(\alpha) \in \mathfrak{O}_H(\alpha)} (X - \sigma\,(\alpha)) = g$$

Es decir, los coeficientes del polinomio $g \in E\,[X]$ quedan fijos por cada $\tau \in H$, lo que significa que $g \in E^H\,[X]$. Ahora, como α es un cero de g y como $f = Irr\left(\alpha, E^H\right)$,

resulta que f divide a g en $E^H[X]$ y, por lo tanto, también en $E[X]$. Como ambos polinomios son mónicos, se tiene que $f = g$.

La segunda afirmación es consecuencia inmediata de lo ya demostrado. □

Proposición 5.7. *Si $E : K$ es finita y separable, para cada subgrupo H del grupo $Gal(E/K)$ se tiene*

$$\left[E : E^H\right] = \#H \quad y \quad H = Gal(E/E^H).$$

Demostración. Como $E : K$ es finita y separable, también lo es $E : E^H$, al ser E^H un cuerpo intermedio entre E y K, y, por el Teorema del elemento primitivo (4.55), existe un $\alpha \in E$ tal que $E = E^H(\alpha)$.

Por el Lema 5.6, se puede afirmar que $\left[E^H(\alpha) : E^H\right] = \#\mathfrak{O}_H(\alpha) = (H : H_\alpha)$. Como $E = E^H(\alpha)$ resulta $H_\alpha = \{\sigma \in H \mid \sigma(\alpha) = \alpha\} = \left\{id_{E^H(\alpha)}\right\} = \left\{id_E\right\}$, pues $\sigma|_{E^H} = id_{E^H}, \forall \sigma \in H$. Se tiene así que $(H : H_\alpha) = \#H$ y la primera afirmación queda probada.

Ahora, como $\#Gal(E/E^H) \leqslant \left[E : E^H\right] = \#H$ (por la Proposición 5.3 y por lo demostrado hasta ahora), y como H es subgrupo del grupo finito $Gal(E/E^H)$, se obtiene $H = Gal(E/E^H)$. □

Definición 5.8. Una extensión $E : K$ se dirá que es una *extensión de Galois* si es algebraica, normal y separable.

En lo sucesivo nos ocuparemos exclusivamente de las extensiones de Galois finitas. El estudio de las extensiones de Galois no finitas puede ser abordado utilizando la topología de Krull en el grupo G de automorfismos, en la cual el retículo de subgrupos correspondientes a subextensiones de Galois finitas constituye un sistema fundamental de entornos de la identidad, y respecto de la cual el grupo topológico G resulta cuasicompacto y totalmente disconexo. El análisis de estas extensiones rebasaría ampliamente los objetivos del curso y no se tratará aquí.

Proposición 5.9. *Sea $E : K$ una extensión finita y separable. Entonces son equivalentes las afirmaciones*

i) $E : K$ *es de Galois.*

ii) $[E : K] = \#Gal(E/K)$.

iii) $K = E^{Gal(E/K)}$.

Demostración. $i) \Rightarrow ii)$

Directamente de la Proposición 5.4 en su apartado 2).

$ii) \Rightarrow iii)$

La extensión $E : K$ es algebraica al ser finita y la torre $K \subset E^{Gal(E/K)} \subset E$ proporciona $[E : K] = \left[E : E^{Gal(E/K)}\right] \left[E^{Gal(E/K)} : K\right]$, como consecuencia del Teorema del grado. Por la Proposición 5.7 se tiene $\left[E : E^{Gal(E/K)}\right] = \#Gal(E/K)$, poniendo allí $H = Gal(E/K)$. Como, por hipótesis $[E : K] = \#Gal(E/K)$, se tiene forzosamente que $\left[E^{Gal(E/K)} : K\right] = 1$, es decir, $E^{Gal(E/K)} = K$.

$iii) \Rightarrow i)$

Probaremos que $E : K$ es normal. Sea $E = K(\alpha)$ (4.55), y sea $H = Gal(E/K)$. Por hipótesis se tiene que $E^H = K$, y así $E = E^H(\alpha)$. Por el Lema 5.6, se puede afirmar que

$$f = Irr(\alpha, E^H) = Irr(\alpha, K) = \prod_{\sigma(\alpha) \in \mathfrak{O}_H(\alpha)} (X - \sigma(\alpha)).$$

Como consecuencia se obtiene que E es cuerpo de escisión de f sobre $E^H = K$. En efecto, para cada $\sigma \in H = Gal(E/K) = Gal(K(\alpha)/K)$ el elemento $\sigma(\alpha)$ pertenece a $E = K(\alpha)$, y $\{\sigma(\alpha) \mid \sigma \in H\}$ es el conjunto de los ceros de f, a la vista de la anterior factorización de dicho polinomio. Entonces f escinde en $E = K(\alpha) = K(\{\sigma(\alpha) \mid \sigma \in H\})$, con lo que queda probado que $E : K$ es una extensión normal. □

Corolario 5.10. *Si $E : K$ es de Galois finita y $K \subset F \subset E$ es una torre de cuerpos, entonces $F = E^{Gal(E/F)}$.*

Demostración. De los resultados análogos para extensiones finitas (3.3), para extensiones normales (4.60) y para extensiones separables (4.24), resulta que $E : F$ es de Galois finita. El resultado se obtiene aplicando a esta extensión el apartado $iii)$ de la Proposición anterior. □

Aunque el siguiente resultado formará parte del enunciado del Teorema Fundamental de Teoría de Galois interesa que quede explícito para su uso futuro

Lema 5.11. *Si $K \subset F \subset E$ es una torre de extensiones normales tal que $E : K$ es también normal, entonces $Gal(E/F)$ es subgrupo normal de $Gal(E/K)$ y se tiene un*

isomorfismo:

$$Gal(F/K) \simeq Gal(E/K)/Gal(E/F).$$

Demostración. Para cada automorfismo σ de E sobre K resulta $\sigma(F) = F$ por el Corolario 4.61, y entonces $\sigma|_F$ es un automorfismo de F. De este modo se obtiene que la aplicación $r_F\colon Gal(E/K) \to Gal(F/K)$, $r_F(\sigma) = \sigma|_F$, está bien definida y es inmediato comprobar que es un homomorfismo de grupos. Además r_F es sobreyectivo ya que si $\tau\colon F \to F \subset \overline{K}$ es un automorfismo de F sobre K, el encaje $\tau\colon F \to \overline{K}$ se extiende a otro $\sigma\colon E \to \overline{K}$, (por ser $E : F$ algebraica y $\overline{K}$ algebraicamente cerrado, según establece la Proposición 4.18), que es necesariamente un automorfismo de E al ser $E : K$ normal, y así $\sigma \in Gal(E/K)$, con lo cual $r_F(\sigma) = \sigma|_F = \tau$. Por otra parte, $\operatorname{Ker}(r_F) = \{\sigma \in Gal(E/K) \mid \sigma|_F = id_F\} = Gal(E/F)$, y entonces dicho grupo es un subgrupo normal de $Gal(E/K)$.

Obsérvese que además se ha probado la última afirmación, pues la existencia del homomorfismo sobreyectivo $r_F\colon Gal(E/K) \to Gal(F/K)$ proporciona que

$$Gal(F/K) \simeq Gal(E/K)/\operatorname{Ker}(r_F) = Gal(E/K)/Gal(E/F). \qquad \square$$

Teorema 5.12. *(Teorema fundamental de la teoría de Galois)*

Sea $E : K$ una extensión finita de Galois y $G = Gal(E/K)$.

Si $\mathcal{F} = \{F \mid F$ es cuerpo intermedio entre K y $E\}$ y $\mathcal{S} = \{H \mid H$ es subgrupo de $G\}$, entonces existe una biyección, que invierte las inclusiones, $\Psi\colon \mathcal{F} \to \mathcal{S}$, definida por $\Psi(F) = Gal(E/F)$, cuya inversa es la aplicación $\Phi\colon \mathcal{S} \to \mathcal{F}$, definida mediante $\Phi(H) = E^H$.

Para cada $F \in \mathcal{F}$ la extensión $E : F$ es de Galois finita, y son equivalentes las afirmaciones

i) $F : K$ es de Galois finita.

ii) El grupo $\Psi(F) = Gal(E/F)$ es un subgrupo normal de G.

Además, si $F : K$ es de Galois se tiene

$$Gal(F/K) \simeq Gal(E/K)/Gal(E/F).$$

Demostración. Es evidente que las aplicaciones Ψ y Φ están bien definidas. Además, para $F \in \mathcal{F}$ el Corolario 5.10 afirma que $E : F$ es una extensión de Galois, y entonces $F = E^{Gal(E/F)} = E^{\Psi(F)} = \Phi(\Psi(F))$. Por otra parte, si $H \in \mathcal{S}$ la Proposición 5.7 establece que $H = Gal(E/E^H) = Gal(E/\Phi(H)) = \Psi(\Phi(H))$. Por lo tanto, dichas aplicaciones Φ y Ψ son inversas.

Si $H_1 \subset H_2$ son subgrupos de G y $x \in E^{H_2}$, para cada $\sigma \in H_1$ se tiene $\sigma(x) = x$, ya que tal σ es elemento de H_2 y, por lo tanto, $x \in E^{H_1}$.

De forma análoga, si $F_1 \subset F_2$ son cuerpos intermedios de la extensión $E : K$, entonces cada $\sigma \in Gal(E/F_2)$ es tal que $\sigma(x) = x$ para todo $x \in F_1$, ya que x es también elemento de F_2, y así $Gal(E/F_1) \supset Gal(E/F_2)$. De este modo queda probado que Φ y Ψ invierten las inclusiones.

Veamos ahora que las condiciones $i)$ y $ii)$ del enunciado son equivalentes.

$ii) \Rightarrow i)$

Sea $H = Gal(E/F)$ un subgrupo normal de $G = Gal(E/K)$, es decir, tal que $\sigma H \sigma^{-1} = H$ para todo $\sigma \in G$. Para probar que $F : K$ es de Galois veremos que esta extensión es normal (5.9), y para ello se demostrará que si $\sigma\colon E \to E$ automorfismo de E sobre K entonces $\sigma(F) = F$ lo cual es suficiente en virtud del corolario 4.61. Por la biyección ya probada bastará demostrar que para $y \in F$ se tiene que $\sigma(y) \in E^H = F$. Sea entonces $y \in F$ y sea $x = \sigma(y)$. Para cada $\rho \in H = Gal(E/F) = \sigma H \sigma^{-1}$ existe un $\tau \in H$ tal que $\rho = \sigma\tau\sigma^{-1}$ y entonces $\rho(x) = \sigma\tau\sigma^{-1}(x) = \sigma\tau\sigma^{-1}(\sigma(y)) = \sigma\tau(y) = \sigma(y) = x$, ya que $\tau \in Gal(E/F)$. Así $x = \sigma(y) \in E^H = F$. Por lo tanto, $F : K$ es de Galois.

$i) \Rightarrow ii)$

Es el Lema anterior. □

5.2. El Teorema fundamental del Álgebra

Esta sección está dedicada a la prueba del Teorema que establece que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

El siguiente resultado será admitido aquí sin prueba pues ésta es de índole no algebraica y puede ser consultada en cualquier texto de Análisis real, al ser una de las

aplicaciones clásicas del Teorema de Bolzano.

Lema 5.13. *Si $f \in \mathbb{R}[X]$ es un polinomio de grado impar, entonces f admite un cero real.*

Lema 5.14. *Si $\alpha \in \mathbb{C}$ existe $\beta \in \mathbb{C}$ tal que $\beta^2 = \alpha$.*

Demostración. Para $\alpha = a + bi$ se consideran los números reales $a' = \dfrac{a + \sqrt{a^2 + b^2}}{2}$ y $b' = \dfrac{-a + \sqrt{a^2 + b^2}}{2}$, ambos no negativos y, por lo tanto, existen $c, d \in \mathbb{R}$ tales que $c^2 = a'$, y $d^2 = b'$. Un cálculo sencillo proporciona que el número complejo $\beta = c + di$ es tal que $\beta^2 = \alpha$. □

Lema 5.15. *Cada polinomio $f = \alpha X^2 + \beta X + \gamma \in \mathbb{C}[X]$ escinde en factores lineales en $\mathbb{C}[X]$. En particular $\mathbb{C}$ no admite extensiones de grado 2.*

Demostración. La primera afirmación es consecuencia directa del Lema anterior ya que el discriminante de f, $\delta = \beta^2 - 4\alpha\gamma$, es un cuadrado en $\mathbb{C}$ y entonces

$$f = \alpha\Big(X - \frac{-\beta + \sqrt{\delta}}{2\alpha}\Big)\Big(X - \frac{-\beta - \sqrt{\delta}}{2\alpha}\Big)$$

es la factorización anunciada.

La segunda afirmación es consecuencia de la primera. En efecto, sea $L : \mathbb{C}$ una extensión de grado 2 y sea $\alpha \in L \setminus \mathbb{C}$, entonces $L = \mathbb{C}(\alpha)$, por el Teorema del grado. Como $[L : \mathbb{C}] = \partial(Irr(\alpha, \mathbb{C})) = 2$, dicho polinomio irreducible escindirá en $\mathbb{C}$, lo que constituye una contradicción. □

Teorema 5.16. *(Teorema Fundamental del Álgebra)*

El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

Demostración. Como se sabe, bastará con demostrar que $\mathbb{C}$ no tiene extensiones finitas propias (4.16). Si $F : \mathbb{C}$ es una tal extensión, entonces la clausura normal N de F sobre $\mathbb{R}$ es también una extensión finita de $\mathbb{R}$. Se obtiene así una torre de cuerpos $\mathbb{R} \subset C \subset F \subset N$ y , para probar que $F = \mathbb{C}$ será suficiente con demostrar que $N = \mathbb{C}$.

La extensión $N : \mathbb{R}$ es de Galois finita normal finita en característica 0), y entonces, como por el apartado *ii)* de la Proposición (5.9) se tiene que $\#Gal(N/\mathbb{R}) = [N : \mathbb{R}] =$

$[N:\mathbb{C}]\,[\mathbb{C}:\mathbb{R}]$, resulta que $\#Gal(N/\mathbb{R})$ es par. Pongamos $G = Gal(N/\mathbb{R})$ y sea H un 2-subgrupo de Sylow de G. Si $E = N^H$ es el cuerpo fijo de H, la extensión $N : E$ es de Galois y $H = Gal\,(N/E)$, en virtud del Teorema 5.12. Como $[N:E] = \#H$ y $[N:\mathbb{R}] = \#G$, del Teorema del grado se deduce que $[E:\mathbb{R}]$ es necesariamente un número impar. Sea $\alpha \in E$ un elemento primitivo de la última extensión, es decir, $E = \mathbb{R}\,(\alpha)$. El polinomio $f = Irr(\alpha, \mathbb{R})$ es de grado impar y, por lo tanto, necesariamente de grado 1, pues en caso contrario f no sería irreducible en $\mathbb{R}\,[X]$ al tener un cero real según se establece en el Lema 5.13. Entonces $E = \mathbb{R}$ y $H = Gal(N/N^H) = Gal(N/E) = Gal(N/\mathbb{R}) = G$ es un 2-grupo. Sea ahora $G_1 = Gal\,(N/\mathbb{C}) \subset Gal\,(N/\mathbb{R}) = G$, si el 2-grupo G_1 es distinto del grupo trivial $\{id_N\}$ (o, lo que es equivalente al ser la extensión $N : \mathbb{C}$ de Galois, si $N \neq \mathbb{C}$), G_1 admitirá un subgrupo G_2 de índice 2 según establece un conocido resultado de la teoría de Sylow (1.48). Sea ahora $E_2 = N^{G_2}$ y entonces, $\mathbb{C} \subset E_2 \subset N$ con lo que $G_2 = Gal(N/E_2)$, ya que $N : E_2$ es de Galois (4.60). Además, como G_2 es normal en G_1 la extensión $E_2 : \mathbb{C}$ es también de Galois con grupo isomorfo a G_1/G_2, y, por lo tanto, de orden 2. Se llega así a que la extensión $E_2 : \mathbb{C}$ es de grado 2, lo que contradice la tesis del Lema 5.15. Por lo tanto, necesariamente $\#G_1 = 1 = [N:\mathbb{C}]$, es decir, $N = \mathbb{C}$. □

5.3. Cuerpos finitos. Raíces de la unidad

Esta sección se inicia con algunas precisiones sobre la estructura de los cuerpos finitos que se deducen, de forma casi inmediata, del resultado ya probado que establece que todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico (4.53). Más concretamente, se obtiene que los cuerpos finitos son los cuerpos de escisión de polinomios de la forma $X^{q-1} - 1$, donde q es potencia de la característica, y se analiza el retículo de subcuerpos. El resto de la sección se dedica al estudio de las ecuaciones de la forma $X^n - a = 0$ con coeficientes en un cuerpo que, a menudo, será considerado de característica cero. Los cuerpos de escisión de dichos polinomios jugarán un papel esencial en el estudio de la resolubilidad por radicales.

Si F es un cuerpo finito con q elementos, F es necesariamente de característica un número primo p (si $Caract(F) = 0$, entonces F contiene un subcuerpo, el subcuerpo primo, que es isomorfo al cuerpo $\mathbb{Q}$ de los números racionales). Como ya es bien conocido, el subcuerpo primoF_p de F es isomorfo al de las clases de restos de enteros módulo p, $F_p \simeq \mathbb{Z}/p\mathbb{Z}$. Desde ahora designaremos con una igualdad este isomorfismo, al no haber ninguna razón algebraica para establecer distinciones.

Sea $r = [F : F_p] = \dim_{F_p} F$. Entonces F es isomorfo como F_p-espacio vectorial a F_p^r y $\#F = q = p^r$. En virtud del Lema 4.53 el grupo multiplicativo $F^* = F \setminus \{0\}$ tiene orden $q-1$, y, por lo tanto, $\alpha^{q-1} = 1$, para cada $\alpha \in F^*$. Esto significa que los elementos no nulos de F son los ceros (en $\overline{F}$) del polinomio $X^{q-1} - 1 \in F_p[X]$, o, lo que es equivalente, F es el conjunto de ceros del polinomio $X^q - X$ y es cuerpo de escisión sobre F_p del polinomio $X^{q-1} - 1 \in F_p[X]$.

Para cada entero $r > 0$ existe un cuerpo de p^r elementos que está constituido por los ceros (en $\overline{F_p}$) del polinomio $X^{p^r} - X \in F_p[X]$. En efecto, sea F dicho conjunto de ceros y $\alpha, \beta \in F$, entonces, ya que $Caract(\overline{F_p}) = p$ (4.31),

$$(\alpha - \beta)^{p^r} = \sum_0^{p^r} \binom{p^r}{i} \alpha^i \beta^{p^r - i} = \alpha^{p^r} - \beta^{p^r} = \alpha - \beta.$$

Además

$$\left(\alpha\beta^{-1}\right)^{p^r} = \alpha^{p^r} \left(\beta^{-1}\right)^{p^r} = \alpha^{p^r} \left(\beta^{p^r}\right)^{-1} = \alpha\beta^{-1} \text{ si } \beta \neq 0,$$

y así F es un subcuerpo de $\overline{F_p}$ (y, por ello, de característica p). Además F tiene p^r elementos, pues el polinomio $X^{p^r} - X \in F_p[X]$ es separable (4.26) al no tener ceros en común con su derivada $p^r X^{p^r - 1} - 1 = -1$ que al ser una constante no nula no tiene ceros. Obsérvese, de paso, que la extensión $F : F_p$ es separable ya que para cada $\alpha \in F$ el $Irr(\alpha, F_p)$ es divisor de $X^{p^r} - X$.

Proposición 5.17. *El número de elementos de un cuerpo finito es una potencia de su característica. Para cada número primo p y cada entero $r > 0$ existe un cuerpo, F_{p^r}, con p^r elementos que es extensión de Galois de su cuerpo primo F_p. Si $q = p^r$, cada cuerpo con q elementos es cuerpo de escisión del polinomio $X^{q-1} - 1$ sobre F_p. Se verifica que $[F_{p^r} : F_p] = r$ y, además, para enteros $r, s > 0$, $F_{p^r} \subset F_{p^s}$ si, y solo si, r es divisor de s.*

Demostración. Solo será necesario probar la última afirmación.

Para $s = rt$, si $\alpha \in F_{p^r}$, lo que equivale a $\alpha^{p^r} = \alpha$, se tiene

$$\alpha^{p^s} = \alpha^{p^{rt}} = \left(\left(\left((\alpha)^{p^r}\right)^{p^r}\right)^{p^r} \overset{t)}{\ldots}\right)^{p^r} = \left(\left((\alpha)^{p^r}\right)^{p^r} \overset{t-1)}{\ldots}\right)^{p^r} = \cdots = \alpha,$$

y, por lo tanto, $\alpha \in F_{p^s}$. Recíprocamente, si $\mathbb{Z}/p\mathbb{Z} = F_p \subset F_{p^r} \subset F_{p^s}$, de las consideraciones previas se obtiene $s = [F_{p^s} : F_p] = [F_{p^s} : F_{p^r}]\,[F_{p^r} : F_p] = [F_{p^s} : F_{p^r}]\,r$, en virtud del Teorema del grado. □

Proposición 5.18. *Todo cuerpo finito es perfecto y el grupo de sus automorfismos es cíclico generado por el endomorfismo de Frobenius.*

Demostración. Si $F = \mathbb{Z}_p$ el endomorfismo de Frobenius en F es la identidad como consecuencia del pequeño Teorema de Fermat (4.54). Si $F = F_{p^n}$ es el cuerpo de p^n elementos y $\varphi\colon F \to F$ es el endomorfismo de Frobenius de F, se tiene $\varphi^n(x) = x^{p^n} = x, \forall x \in F$, como consecuencia de la Proposición 5.17, y así $\varphi^n = id_F$. Por lo tanto, el período de φ es un divisor de n. Si $|\varphi| = s$ con $s \leqslant n$ tiene $\varphi^s(x) = x^{p^s} = x$, para cada $x \in F$, de lo que se deduce $F_{p^n} \subset F_{p^s}$. La Proposición antes citada permite afirmar $n \leqslant s$, de donde resulta la igualdad $s = n$. Además cada automorfismo de F deja fijos los elementos del cuerpo primo F_p y, por lo tanto, el grupo de todos los automorfismos de F es el grupo de Galois de la extensión $F : F_p$ cuyo grado es igual al orden de dicho grupo (5.9). Se tiene así que $n = [F : F_p] = \#Gal(F/F_p) = \#Aut(F)$ y que $Aut(F) = \langle\varphi\rangle$. □

El resto de la sección se dedicará al estudio de las raíces de la unidad, es decir, las raíces de polinomios de la forma $X^n - 1$.

Proposición 5.19. *Si K es un cuerpo, entonces el conjunto U_n de las raíces en $\overline{K}$ de la ecuación $X^n - 1 = 0$ es un grupo cíclico respecto de la multiplicación. Si además K es de característica nula o un primo no divisor de n, dicho grupo es de orden n.*

Demostración. En cualquier caso si $\alpha, \beta \in U_n$ se tiene que $(\alpha\beta)^n = \alpha^n\beta^n = 1$. También $\left(\alpha^{-1}\right)^n = (\alpha^n)^{-1} = 1$ y, como $1 \in U_n$, el Lema 4.53 proporciona directamente el resultado.

Bajo ambas hipótesis acerca de la característica de K, el polinomio $X^n - 1$ es separable ya que su derivada nX^{n-1} no es nula y solamente admite al 0 como raíz. Por lo tanto, el grupo U_n es de orden n. □

Definición 5.20. Cada generador del grupo cíclico U_n se llamará *raíz primitiva n-ésima de 1.*

Observación 5.21. Nótese que, en virtud de la Proposición 5.19, si la característica de K es nula o un número primo no divisor de n, entonces el orden de U_n es n. En cualquiera de ambos casos el número de posibles generadores de U_n es el *indicador de Euler*

$$\varphi(n) = \#\{r \in \mathbb{N} \mid 1 \leqslant r < n, (r, n) = 1\},$$

ya que dado un generador ξ de U_n resulta que ξ^r es también generador si, y solamente si, r y n son primos entre sí.

Proposición 5.22. *Sean K un cuerpo y $\xi \in \overline{K}$ una raíz primitiva n-ésima de 1.*

1) *$K(\xi) : K$ es una extensión normal y, si K es de característica nula o un primo no divisor de n, dicha extensión es de Galois.*

2) *En cualquier caso $Gal(K(\xi)/K)$ es abeliano y resoluble.*

Demostración. 1) $K(\xi)$ es cuerpo de escisión sobre K del polinomio $X^n - 1$. En efecto, tal cuerpo de escisión debe estar generado sobre K por los ceros de dicho polinomio, es decir, por los elementos de U_n. Ahora, cada elemento de U_n pertenece a $K(\xi)$ ya que $\langle \xi \rangle = U_n$, y así $U_n \subset K(\xi)$. Es decir, $K(\xi) = K\left(1, \xi, \ldots, \xi^{n-1}\right)$ y $K(\xi) : K$ es, por tanto, una extensión normal. La separabilidad de ξ sobre K es consecuencia de que el polinomio $Irr(\xi, K)$ es divisor (en $K[X]$) del polinomio $X^n - 1$ que es separable en virtud de la hipótesis sobre la característica, ya que la derivada $(X^n - 1)' = nX^{n-1}$ solo admite al cero como raíz en ese caso. De (4.42) resulta la separabilidad de $K(\xi) : K$.

2) Para probar que $Gal(K(\xi)/K)$ es abeliano bastará con demostrar que dados $\sigma, \tau \in Gal(K(\xi)/K)$ entonces $(\sigma \circ \tau)(\xi) = (\tau \circ \sigma)(\xi)$, pues en ese caso se tendría $(\sigma \circ \tau)(x) = (\tau \circ \sigma)(x)$, $\forall x \in K(\xi)$. Ahora, si $\gamma \in Gal(K(\xi)/K)$, se tiene $\gamma(\xi) = \xi^r$ para algún $r < n$, pues $\xi^n = 1 \Leftrightarrow \gamma(\xi^n) = [\gamma(\xi)]^n = \gamma(1) = 1$ y, por tanto, $|\gamma(\xi)| = |\xi|$. Es decir, $\gamma(\xi)$ es también raíz primitiva n-ésima de 1. Entonces si $\sigma(\xi) = \xi^r$ y $\tau(\xi) = \xi^t$, resulta que $(\sigma \circ \tau)(\xi) = \sigma(\tau(\xi)) = \sigma\left(\xi^t\right) = (\sigma(\xi))^t = (\xi^r)^t = \xi^{rt}$ y $(\tau \circ \sigma)(\xi) = \tau(\sigma(\xi)) = \tau(\xi^r) = (\tau(\xi))^r = \left((\xi)^t\right)^r = \xi^{tr}$, de lo que se deduce $\sigma \circ \tau = \tau \circ \sigma$. □

Proposición 5.23. *Sea $\xi \in \overline{\mathbb{Q}}$ una raíz primitiva n-ésima de 1. Entonces*

1)

$$\Phi_n := Irr(\xi, \mathbb{Q}) = \prod_{m<n,(m,n)=1} (X - \xi^m)$$

es la factorización de $Irr(\xi, \mathbb{Q})$ en $\overline{\mathbb{Q}}[X]$. A Φ_n se le denomina n-ésimo polinomio ciclotómico y a la extensión $\mathbb{Q}(\xi) : \mathbb{Q}$ extensión ciclotómica.

2) $[\mathbb{Q}(\xi) : \mathbb{Q}] = \partial(Irr(\xi, \mathbb{Q})) = \varphi(n)$.

Demostración. 1) Para la prueba de este resultado demostraremos en primer lugar que cada raíz primitiva n-ésima de 1 es una raíz de $f = Irr(\xi, \mathbb{Q})$. Para ello será suficiente con demostrar que ξ^p es un cero de f cada vez que $p < n$ sea un primo no divisor de n. En efecto, cada raíz primitiva n-ésima es de la forma ξ^r con $1 \leqslant r < n$ y $(r, n) = 1$. Ahora, cada primo p divisor de r no es divisor de n y entonces $\xi^r = (\xi^p)^t$, con $r = pt$, en donde, de nuevo $1 \leqslant t < n$, $(t, n) = 1$; por lo tanto, si ξ^p es raíz de f, se tiene que $f = Irr(\xi^p, \mathbb{Q})$, y de nuevo se tendrá que $(\xi^p)^q = \xi^{pq}$ es raíz de f para cada divisor primo q de t. Por este método se agotarán todos los factores primos (no necesariamente distintos) de r y, por recurrencia, resultará que ξ^r es un cero de f cada vez que $1 \leqslant r < n$ y $(r, n) = 1$.

Sea $g \in \mathbb{Q}[X]$ tal que $X^n - 1 = fg$. Tal polinomio g existe ya que ξ es un cero de $X^n - 1 \in \mathbb{Q}[X]$ y $f = Irr(\xi, \mathbb{Q})$. Además, como consecuencia del Lema 2.54, se puede suponer que $g, f \in \mathbb{Z}[X]$.

Consideremos $g = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in \mathbb{Z}[X]$, y sea ahora p un número primo no divisor de n. Como $\xi^p \in U_n$ es también un cero de $X^n - 1$ entonces ξ^p es necesariamente un cero de f o de g. En el primer caso la prueba terminaría aquí, por lo que se puede suponer que $g(\xi^p) = 0$, o, lo que es lo mismo, que ξ es un cero del polinomio $g(X^p) \in \mathbb{Z}[X]$. Pero $g(X^p) \equiv [g]^p\,(mód\ p)$, ya que cada coeficiente $a_i \in \mathbb{Z}$ del polinomio g satisface $a_i \equiv a_i^p (mód\ p)$ en virtud del pequeño Teorema de Fermat (4.54), y entonces el homomorfismo de anillos $\overline{(-)} : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$, definido por $\left(\overline{b_sX^s + b_{s-1}X^{s-1} + \cdots + b_0}\right) = \overline{b_s}X^s + \overline{b_{s-1}}X^{s-1} + \cdots + \overline{b_0}$, proporciona que

$$\begin{aligned}
\overline{g(X^p)} &= \left(\overline{X^{pr} + a_{r-1}X^{p(r-1)} + \cdots + a_0}\right) = X^{pr} + \overline{a_{r-1}}X^{p(r-1)} + \cdots + \overline{a_0} \\
&= X^{pr} + \overline{a_{r-1}^p}X^{p(r-1)} + \cdots + \overline{a_0^p} = X^{pr} + \overline{a_{r-1}}^pX^{p(r-1)} + \cdots + \overline{a_0}^p \\
&= \left(X^r + \overline{a_{r-1}}X^{r-1} + \cdots + \overline{a_0}\right)^p = (\overline{g})^p = \overline{(g)^p}
\end{aligned}$$

(4.31) al ser p la característica de $\mathbb{Z}_p[X]$. Resulta así :

a) $g(X^p) = fh$, para un cierto $h \in \mathbb{Z}[X]$ al ser ξ un cero de $g(X^p)$ y de $f = Irr(\xi, \mathbb{Q})$ (nótese que se puede suponer h con coeficientes enteros como consecuencia del algoritmo de Euclides en $\mathbb{Z}[X]$, pues f y $g(X^p)$ son elementos de $\mathbb{Z}[X]$ y el coeficiente principal

de f es 1).

b) Entonces $(\overline{g})^p = \overline{g(X^p)} = \overline{fh}$, lo que significa que $\overline{f}$ y $\overline{g}$ tienen algún factor común en $\mathbb{Z}_p[X]$ al ser este último anillo un dominio de factorización única. Ello significa que ambos polinomios tienen algún cero común en $\overline{\mathbb{Z}_p}$, lo cual está en contradicción con el hecho de que el polinomio $X^n - \overline{1} = \overline{X^n - 1} = \overline{f}\overline{g}$ no tiene ceros múltiples pues su derivada $\left(n\overline{1}\right) X^{n-1} \neq 0$ solamente admite a 0 como raíz.

En consecuencia ξ^p es necesariamente un cero de f, y por lo tanto, como ya fue indicado, todas las raíces primitivas n-ésimas de 1 son ceros de f.

Veamos ahora que tales raíces primitivas son los únicos ceros de f, con lo que quedará probado 2). Tenemos que f es divisor en $\mathbb{Q}[X]$ del polinomio $X^n - 1$, y así todo cero de f es una raíz n-ésima de 1. Sea $\alpha \in U_n$ un cero de f y supongamos que $\alpha^r = 1$, con $r \mid n$ y $r < n$, es decir, que α es una raíz n-ésima de 1, pero no primitiva. Entonces $f = Irr(\alpha, \mathbb{Q})$ al ser$f$ mónico e irreducible en $\mathbb{Q}[X]$ y, como α es un cero de $X^r - 1$, resultará que f divide a $X^r - 1$ en $\mathbb{Q}[X]$. Ahora todo cero de f lo será también de $X^r - 1$ y, en particular, se tendrá que $\xi^r = 1$, siendo ξ cualquier raíz primitiva n-ésima, pues todas ellas son ceros de f, como ya ha sido probado. Ello no es posible ya que tales ξ son de período $n > r$.

2) Es consecuencia inmediata de 1). Como $\partial(f)$ es el número de raíces primitivas n-ésimas de 1, se tiene $[\mathbb{Q}(\xi) : \mathbb{Q}] = \partial(Irr(\xi, \mathbb{Q})) = \varphi(n)$. □

Corolario 5.24. *Sea $n > 1$ un número natural. Entonces*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Demostración. En primer lugar obsérvese que U_d es subgrupo de U_n, para cada $d \mid n$. En la factorización

$$X^n - 1 = \prod_{\alpha \in U_n} (X - \alpha)$$

reagrúpense los factores correspondientes a aquellas $\alpha \in U_n$ que tienen el mismo período. Para un período d, necesariamente divisor de n, $\Phi_d = \prod_{|\xi|=d}(X - \xi)$ (por el apartado 2 de la Proposición anterior), y el resultado se sigue de forma inmediata. □

Proposición 5.25. *Si K es un cuerpo de característica nula o un primo p no divisor de n. Si $\xi \in \overline{K}$ es una raíz primitiva n-ésima de 1, y $\alpha \in \overline{K}$ es tal que $a = \alpha^n \in K$, entonces $K(\xi, \alpha)$ es cuerpo de escisión del polinomio $X^n - a$ sobre K y $K(\xi, \alpha) : K$ es una extensión de Galois. Además si $\xi \in K$, dicha extensión es abeliana, es decir, el grupo $Gal(K(\alpha)/K)$ es abeliano.*

Demostración. $\left(\alpha\xi^i\right)^n = \alpha^n\left(\xi^n\right)^i = a$, para cualquier i, y los elementos $\alpha, \alpha\xi, \ldots, \alpha\xi^{n-1}$ de $\overline{K}$ son ceros del polinomio $X^n - a$; $\alpha, \alpha\xi, \ldots, \alpha\xi^{n-1}$ son diferentes ya que de $\alpha\xi^i = \alpha\xi^j$ (con $1 \leqslant i < j < n$) resultaría $\xi^{j-i} = 1$ con $j - i < n$, lo cual es absurdo pues por ser $Caract(K)$ no divisor de n el grupo U_n es de orden n (5.19). Es inmediato entonces que

$$K(\xi, \alpha) = K\left(\alpha, \alpha\xi, \ldots, \alpha\xi^{n-1}\right)$$

es cuerpo de escisión de $X^n - a$ sobre K. Los polinomios $Irr(\alpha\xi^i, K)$ $(i = 0, 1, \ldots, n-1)$ son todos separables por ser divisores del $X^n - a$ que tiene n ceros diferentes. Entonces $K(\xi, \alpha) : K$ es separable por (4.42).

Para probar la segunda afirmación obsérvese que si $\xi \in K$ se verifica que $K(\xi, \alpha) = K(\alpha)$, y cada $\sigma \in Gal(K(\alpha)/K)$ está determinado por su valor $\sigma(\alpha)$, como ya se ha dicho en diversas ocasiones. Además $\sigma(\alpha)$ es necesariamente un cero de $X^n - a$ (5.4). Sean entonces $\sigma, \tau \in Gal(K(\alpha)/K)$ y $\sigma(\alpha) = \alpha\xi^r$, $\tau(\alpha) = \alpha\xi^s$. Se tiene $(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha\xi^s) = \sigma(\alpha)\sigma(\xi)^s = \alpha\xi^r\xi^s = \alpha\xi^{r+s}$ ya que $\sigma(\xi) = \xi \in K$; de modo análogo se obtiene $(\tau\sigma)(\alpha) = \alpha\xi^{s+r}$, con lo cual resulta $\sigma\tau = \tau\sigma$. □

Observaciones 5.26.

1) $\Phi_1 = X - 1$.

2) $\Phi_2 = X + 1$, pues $X^2 - 1 = \Phi_1\Phi_2$.

3) Si p es un número primo, $X^p - 1 = \prod_{d|p} \Phi_d = \Phi_1\Phi_p$ y

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

4)

$$X^4 - 1 = \Phi_1\Phi_2\Phi_4 \Rightarrow \Phi_4 = X^2 + 1.$$

5)

$$X^6-1=\Phi_1\Phi_2\Phi_3\Phi_6 \Rightarrow$$
$$\Phi_6=\frac{X^6-1}{\Phi_1\Phi_2\Phi_3}=\frac{X^6-1}{(X-1)(X+1)(X^2+X+1)}=X^2-X+1.$$

De modo alternativo: los ceros de Φ_6 son las dos raíces primitivas sextas de 1 (a saber: $\xi=cos\frac{2\pi}{6}+isen\frac{2\pi}{6}$ y $\xi^5=\cos\frac{10\pi}{6}+isen\frac{10\pi}{6}=\overline{\xi}=\xi^{-1}$), y entonces

$$\Phi_6=(X-\xi)\left(X-\overline{\xi}\right)=X^2-(\xi+\overline{\xi})X+\xi\overline{\xi}=X^2-2\cos\frac{2\pi}{6}X+1=X^2-X+1.$$

6)

$$X^{12}-1=\Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12}=\left(X^6-1\right)\Phi_4\Phi_{12} \Rightarrow$$
$$\Phi_{12}=\frac{X^{12}-1}{\left(X^6-1\right)\left(X^2+1\right)}=\frac{X^6+1}{X^2+1}=X^4-X^2+1.$$

Observación 5.27. Si ξ es una raíz primitiva n-ésima de 1, entonces $\sigma(\xi)$ es también raíz primitiva n-ésima de 1, para cada $\sigma\in Gal(\mathbb{Q}(\xi)/\mathbb{Q})$. De hecho $\xi^r=1\Leftrightarrow\sigma(\xi)^r=1$. Además, según lo establecido en el Teorema de extensión de encajes a extensiones simples 4.4, y a la luz de las proposiciones 5.23 y 5.4 se tiene:

$$\begin{aligned}\alpha \text{ es raíz primitiva } n\text{-ésima de } 1 &\Leftrightarrow Irr(\xi,\mathbb{Q})=Irr(\alpha,\mathbb{Q})=\Phi^n\\ &\Leftrightarrow \exists\sigma\in Gal(\mathbb{Q}(\xi):\mathbb{Q}) \text{ tal que } \sigma(\xi)=\alpha.\end{aligned}$$

Ejercicio 5.28. Sea ξ una raíz primitiva duodécima de $1\in\mathbb{Q}$. Como $\varphi(12)=4$ el número de raíces primitivas duodécimas de 1 es 4, y tales raíces son ξ,ξ^5,ξ^7,ξ^{11}. Por la Proposición 5.23, la extensión $\mathbb{Q}(\xi):\mathbb{Q}$ es de Galois y por tanto $[\mathbb{Q}(\xi):\mathbb{Q}]=\#Gal(\mathbb{Q}(\xi)/\mathbb{Q})=4$.

El ejercicio consiste en determinar la estructura del grupo $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$, su retículo de subgrupos y los cuerpos intermedios de la extensión $\mathbb{Q}(\xi):\mathbb{Q}$.

Solución: Sea $\left\{\sigma_0=id_{\mathbb{Q}(\xi)},\sigma_1,\sigma_2,\sigma_3\right\}=Gal(\mathbb{Q}(\xi)/\mathbb{Q})=G$, con $\sigma_1(\xi)=\xi^5$, $\sigma_2(\xi)=\xi^7$, $\sigma_3(\xi)=\xi^{11}$ (recuérdese que la imagen de ξ mediante cualquier automorfismo de $\mathbb{Q}(\xi)$ sobre $\mathbb{Q}$ debe ser una raíz primitiva duodécima de 1 (5.27)).

Para cada $i = 0, 1, 2, 3$, sea $H_i = \langle \sigma_i \rangle$. Es fácil comprobar que $H_0 = \left\{ id_{\mathbb{Q}(\xi)} \right\}$, y que H_1, H_2 y H_3 son subgrupos diferentes de G de orden 2 (por ejemplo, $\sigma_1^2(\xi) = \sigma_1(\sigma_1(\xi)) = \sigma_1\left(\xi^5\right) = (\sigma_1(\xi))^5 = \left(\xi^5\right)^5 = \xi^{251} = \left(\left(\xi^{12}\right)\right)^2 \xi = \xi$, y entonces $\sigma_1^2 = \sigma_0 = id_{\mathbb{Q}(\xi)}$), por lo cual se puede afirmar que G no es un grupo cíclico (si G fuese cíclico solamente admitiría un único subgrupo de orden 2). Por lo tanto, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, y los H_i, $i = 0, \ldots, 3$, son los únicos subgrupos propios de G.

Por el Teorema Fundamental de Teoría de Galois, para la determinación de los cuerpos intermedios bastará con obtener los cuerpos fijos de dichos subgrupos. Para ello considérese la $\mathbb{Q}$-base $\left\{1, \xi, \xi^2, \xi^3\right\}$ de $\mathbb{Q}(\xi)$, respecto de la cual cada elemento $x \in \mathbb{Q}(\xi)$ admite una única expresión $x = a + b\xi + c\xi^2 + d\xi^3$ con a, b, c, d números racionales. Considérese también que $\xi^{12} = 1$ y que $Irr(\xi, \mathbb{Q}) = \Phi_{12} = X^4 - X^2 + 1$.

Obtención de $\mathbb{Q}(\xi)^{H_1}$:

Si $x = a+b\xi+c\xi^2+d\xi^3 \in \mathbb{Q}(\xi)$, $\sigma_1(x) = a+b\sigma_1(\xi)+c\sigma_1\left(\xi^2\right)+d\sigma_1\left(\xi^3\right) = a+b\xi^5+c\xi^{10}+d\xi^{15}$, y como, por el algoritmo de Euclides en $\mathbb{Q}[X]$, $dX^{15}+cX^{10}+bX^5+a = (X^4-X^2+1)(dX^{11}+aX^9+cX^6-dX^5+cX^4-d^3+X-c)+(b+d)X^3-cX^2-bX+c+a$, resulta $\sigma_1(x) = (a+c) - b\xi - c\xi^2 + (b+d)\xi^3$.

Entonces,

$$\begin{aligned} x \in \mathbb{Q}(\xi)^{H_1} &\Leftrightarrow x = \sigma_1(x) \\ &\Leftrightarrow a + b\xi + c\xi^2 + d\xi^3 = (a+c) - b\xi - c\xi^2 + (b+d)\xi^3 \\ &\Leftrightarrow a + c = a,\ b = -b,\ -c = c,\ b + d = d \\ &\Leftrightarrow b = c = 0 \Leftrightarrow x = a + d\xi^3. \end{aligned}$$

Por lo tanto, $\sigma_1(x) = x \Rightarrow x \in \mathbb{Q}\left(\xi^3\right)$, es decir, $\mathbb{Q}(\xi)^{H_1} \subset \mathbb{Q}\left(\xi^3\right)$. Como, por otra parte $\sigma_1(\xi^3) = \xi^{15} = \xi^3$, se tiene $\mathbb{Q}\left(\xi^3\right) \subset \mathbb{Q}(\xi)^{H_1}$, y así $\mathbb{Q}(\xi)^{H_1} = \mathbb{Q}\left(\xi^3\right)$.

(La expresión de $\sigma_1(x)$ se puede obtener de forma alternativa a partir de la igualdad $\sigma_1(x) = a+b\xi^5+c\xi^{10}+d\xi^{15}$ haciendo uso de que $\xi^{15} = \xi^3$, y $\xi^4 = \xi^2 - 1$, pues entonces $\xi^5 = \xi^3 - \xi$ y $\xi^{10} = \left(\xi^5\right)^2 = \left(\xi^3 - \xi\right)^2 = \xi^6 - 2\xi^4 + \xi^2 = \xi^4 - \xi^2 - 2\left(\xi^2 - 1\right) + \xi^2 = -\xi^2 + 1$).

De forma similar se prueba que $\mathbb{Q}(\xi)^{H_2} = \mathbb{Q}\left(\xi^2\right)$ y que $\mathbb{Q}(\xi)^{H_3} = \mathbb{Q}\left(-2\xi + \xi^3\right)$, que, junto con $\mathbb{Q}(\xi)^{H_1} = \mathbb{Q}\left(\xi^3\right)$, constituyen los únicos cuerpos estrictamente interme-

dios de la extensión $\mathbb{Q}(\xi) : \mathbb{Q}$.

5.4. Resolubilidad por radicales

Definición 5.29. Sea K un cuerpo de característica 0. Una extensión $F : K$ es *radical* si existe una torre de cuerpos (en lo sucesivo *torre radical*)

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r = F$$

donde, para cada $i = 1, 2, \ldots, r$, $K_i = K_{i-1}(\alpha_i)$, con $\alpha_i \in K_i$ tal que $a_i = \alpha_i^{n_i} \in K_{i-1}$ para ciertos enteros positivos n_i.

Observaciones 5.30.

1) Si $F : K$ es una extensión radical entonces $F = K(\alpha_1, \ldots, \alpha_r)$ y, por tanto, $F : K$ es finita ya que cada α_i es algebraico sobre $K(\alpha_1, \ldots, \alpha_{i-1}) = K_{i-1}$.

2) Si K es de característica 0 y $F : K$ es radical, como $\left\{1, \alpha_1, \ldots, \alpha_1^{n_1-1}\right\}$ es un sistema de generadores de $K(\alpha_1)$ como K-espacio, resulta

$$\alpha_2 = \sqrt[n_2]{a_2} = \sqrt[n_2]{c_0 + c_1 \sqrt[n_1]{a_1} + \cdots + c_{n_1-1} \sqrt[n_1]{a_1^{n_1-1}}} \quad (*)$$

con $a_1 = \alpha_1^{n_1}, c_j \in K$ para $j = 0, 1, \ldots, n_1 - 1$. De forma recurrente el elemento $\alpha_3 = \sqrt[n_3]{a_3}$ con $a_3 \in K(\alpha_1)(\alpha_2)$ y, por tanto, α_3 será una expresión del tipo (*) con a_2 en lugar de a_1, con n_2 en lugar de n_1, con n_3 en lugar de n_2, y con los $c_j \in K(\alpha_1)$ que serán a su vez expresiones del tipo $c_j = g_j(\alpha_1)$ con $g_j \in K[X]$. Iterativamente, cualquier elemento de $K(\alpha_1, \ldots, \alpha_n)$ será una expresión algebraica de expresiones radicales de expresiones algebraicas de elementos de K y de los generadores de la extensión.

En el caso de característica positiva, en la extensión finita $F : K$ pueden aparecer elementos puramente inseparables y es por esto que, para ampliar la validez del gran Teorema de Galois, la definición de extensión radical deberá ser modificada, admitiendo extensiones intermedias con grado divisible por la característica.

Definición 5.31. Si K es de característica $p \neq 0$, una extensión $F : K$ se dice que es radical si existe una torre (en lo sucesivo *torre radical*)

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r = F$$

tal que cada paso $K_{i-1} \subset K_i$ es de uno de los siguientes tipos:

1) $K_i = K_{i-1}(\xi_i)$ con ξ_i una raíz n_i-ésima primitiva de 1, para algún entero positivo n_i.

2) $K_i = K_{i-1}(\alpha_i)$ con $a_i = \alpha_i^{n_i} \in K_{i-1}$ para algún entero positivo n_i no divisible por p.

3) $K_i = K_{i-1}(\alpha_i)$ donde α_i es un cero de algún polinomio $X^p - X - a_i$ con $a_i \in K_{i-1}$.

4) $K_i = K_{i-1}(\beta_i)$ donde β_i es un cero de algún polinomio $X^{p^{\mu_i}} - b_i$ con $b_i \in K_{i-1}$ y μ_i un entero positivo.

Observación 5.32. Es preciso hacer notar que si K es de característica $p \neq 0$ el polinomio $X^p - X - a \in K[X]$ es separable pues su derivada $(X^p - X - a)' = -1$. Para ver esto de otro modo obsérvese que si α es un cero de $f = X^p - X - a$, los p elementos diferentes $\alpha, \alpha + 1, \ldots, \alpha + p - 1$ son todos los ceros de f.

Observación 5.33. Sea K de característica p y $F = K(\alpha)$ con $\alpha^n \in K$ para un entero $n > 0$. Si $F : K$ es separable el entero n que satisface la anterior propiedad se puede seleccionar primo con p. En efecto, si $n = p^r m$ con $p \nmid m$ entonces $\alpha^n = (\alpha^m)^{p^r} \in K$ y, por tanto, α^m es puramente inseparable sobre K, con lo cual se tiene $\alpha^m \in K$ en virtud de la separabilidad supuesta (4.52).

Por lo tanto si K es de característica p, una extensión separable es radical si, y solo si, existe una torre como en (5.31) tal que cada paso $K_{i-1} \subset K_i$ es de uno de los siguientes tipos:

1) $K_i = K_{i-1}(\alpha_i)$ con $\alpha_i^{n_i} \in K_{i-1}$ para algún entero positivo n_i.

2) $K_i = K_{i-1}(\alpha_i)$ donde α_i es un cero de algún polinomio $X^p - X - a_i$ con $a_i \in K_{i-1}$.

Por lo dicho, la condición $p \nmid n_i$ puede ser suprimida con lo cual las condiciones 1) y 2) de 5.31) quedan englobadas en una, y la 4) es obviamente superflua. Si además el cuerpo K es extensión algebraica de $\mathbb{Z}_p$, la anterior condición 2) queda asumida en la 1), pues si $K_i = K_{i-1}(\alpha_i)$ donde α_i es un cero de algún polinomio $X^p - X - a_i$ con $a_i \in K_{i-1}$ -ahora extensión algebraica de $\mathbb{Z}_p$- resulta que α_i es también algebraico sobre $\mathbb{Z}_p$ y por tanto $\mathbb{Z}_p(\alpha_i) : \mathbb{Z}_p$ es finita, con lo que $\mathbb{Z}_p(\alpha_i) = F_{p^{m_i}}$ para algún entero m_i. De este modo se obtiene que α_i es un cero del polinomio $X^{p^{m_i}-1} - 1 \in \mathbb{Z}_p[X]$ (5.17) y

la extensión $K_i : K_{i-1}$ es de las de tipo 1).

La condición de que $K : \mathbb{Z}_p$ sea extensión algebraica es crucial en la anterior argumentación. De hecho la afirmación no es válida si $K = \mathbb{Z}_p(t)$, siendo t trascendente sobre $\mathbb{Z}_p$. Por ejemplo, si α es un cero del polinomio separable $X^p - X - t \in \mathbb{Z}_p(t)[X]$, entonces $\alpha^m \notin K$, cualquiera que sea el entero $m > 0$. En caso contrario se podrá seleccionar, como antes, el menor m tal que $\alpha^m \in K$, y en ese caso p no divide a m, pues si fuese $m = p^r s$, con $p \nmid s$, se tendría $\alpha^m = (\alpha^s)^{p^r} \in \mathbb{Z}_p(t)$ con lo que $\alpha^s \in \mathbb{Z}_p(t)$ (pues α^s sería entonces un elemento separable y puramente inseparable sobre $\mathbb{Z}_p(t)$) lo que está en contradicción con la selección de m. Poniendo $\alpha^m = \dfrac{f(t)}{g(t)}$ con $f, g \in \mathbb{Z}_p[t]$ coprimos, resulta

$$g(\alpha^p - \alpha)\alpha^m - f(\alpha^p - \alpha) = 0.$$

Ello implica que α es cero del polinomio

$$F(Y) = g(Y^p - Y)Y^m - f(Y^p - Y),$$

de lo que se deduce necesariamente $F(Y) = 0$, ya que α es trascendente sobre $\mathbb{Z}_p$ (en otro caso $t = \alpha^p - \alpha$ sería algebraico sobre $\mathbb{Z}_p$). Los polinomios $f(Y^p - Y)$ y $g(Y^p - Y)$ son coprimos en $\mathbb{Z}_p[Y]$ y, por lo tanto, se tiene necesariamente $Y^m = f(Y^p - Y)$ (además de $g(Y^p - Y) = cte.$) por la factorización única en $\mathbb{Z}_p[Y]$. Ahora, si $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[t]$ se tiene

$$Y^m - a_n (Y^p - Y)^n - a_{n-1} (Y^p - Y)^{n-1} - \cdots - a_0 = Y^m - a_n Y^{pn} + H(Y) = 0$$

y entonces es nulo el polinomio $Y^m - a_n Y^{pn}$ ya que, de no serlo, sería de grado estrictamente mayor que el de $H(Y)$. Resulta entonces $m = pn$, lo que contradice la selección de m.

Además tampoco es posible, en general, encontrar un $\beta \in K(\alpha)$ que satisfaga la condición $\beta^m \in K = \mathbb{Z}_p(t)$, para algún entero $m > 0$, con $K(\alpha) = K(\beta)$, siendo α un cero de $X^p - X - t \in K[X]$. Para ver esto consideraremos el caso más sencillo, $p = 2$. Si existe, tal $\beta \in K(\alpha)$ se expresa como $\beta = \lambda\alpha + \mu$ con $0 \neq \lambda, \mu \in K = \mathbb{Z}_p(t)$ y también es de K el elemento β'^m, con $\beta' = \beta\lambda^{-1} = \alpha + \mu\lambda^{-1} = \alpha + \gamma$ que cumple

también $K(\alpha) = K(\beta') = K(\beta)$, lo que nos permite suponer $\beta = \alpha + \gamma$, $\gamma \in K$. Como $0 = \alpha^2 - \alpha - t = (\beta - \gamma)^2 - (\beta - \gamma) - t = \beta^2 - \beta - \left(\gamma^2 - \gamma + t\right)$, resulta de modo inmediato $Irr(\beta, \mathbb{Z}_p(t)) = X^2 - X - t'$, donde $t' = \gamma^2 - \gamma + t \in K = \mathbb{Z}_p(t)$. Como consecuencia, β es algebraico de grado 2 tanto sobre $\mathbb{Z}_p(t)$ como sobre $\mathbb{Z}_p(t')$ y, por lo tanto, se tiene $\mathbb{Z}_p(t) = \mathbb{Z}_p(t') = K$, con lo que β se encuentra ahora en las mismas condiciones que el α elegido inicialmente, para el cual no existía ningún entero $m > 0$ tal que $\alpha^m \in K$.

Proposición 5.34. *i) Sea $K \subset F \subset E$ una torre de cuerpos. Entonces, si $F : K$ y $E : F$ son extensiones radicales, $E : K$ es también radical.*

ii) Sean F y L subcuerpos de un mismo cuerpo E tales que $F : K$ y $L : K$ son extensiones radicales. Entonces $LF : K$ es también una extensión radical.

iii) Si $F : K$ es radical y $\tau\colon F \to F'$ es un isomorfismo, entonces, poniendo $\tau(K) = K'$, la extensión $F' : K'$ es radical también. En particular, si $\tau\,|_K = id_K$, entonces $F' : K$ es radical.

iv) Si $F : K$ es radical finita, la clausura normal de F sobre K es también una extensión radical de K.

Demostración. La prueba de i) es obvia. La concatenación de las dos torres radicales, existentes por hipótesis, proporciona una torre radical para la extensión $E : K$.

Para demostrar ii) obsérvese que la torre radical

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r = F$$

proporciona una torre del mismo tipo

$$L = LK \subset LK_1 \subset \cdots \subset LK_{i-1} \subset LK_i \subset \cdots \subset LK_r = LF,$$

ya que $LK_i = LK_{i-1}(\alpha_i)$ y al ser $K_i = K_{i-1}(\alpha_i)$ (el elemento α_i cumple, respecto de LK_{i-1} una condición idéntica a la que cumple respecto de K_{i-1}). Por tanto, $LF : L$ es radical y, por aplicación de i), resulta que $LF : K$ es radical al serlo también $L : K$.

iii) Si $K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r = F$ es una torre radical, y si $K_i = K_{i-1}(\alpha_i)$, con $a_i \in K_i$ tales que $\alpha_i^{n_i} \in K_{i-1}$ para ciertos enteros positivos

n_i, poniendo $\tau(K_i) = K'_i$ resulta que $K' \subset K'_1 \subset \cdots \subset K'_r = F'$ es también una torre radical, pues $K'_i = K'_{i-1}(\tau\alpha_i)$ y $[\tau(\alpha_i)]^{n_i} = \tau({\alpha_i}^{n_i}) \in K'_{i-1}$, o bien $\tau\alpha_i$ es un cero del polinomio $X^p - X - \tau a \in F'[X]$, según proceda.

iv) Es consecuencia inmediata de la Proposición 4.64 y de las afirmaciones *ii*) y *iii*) ya demostradas. □

Definición 5.35. Si P es el cuerpo primo de K, y si $f = a_n X^n + \cdots + a_0 \in K[X]$, llamaremos aquí *cuerpo de coeficientes de* f al menor subcuerpo de K que contiene dichos coeficientes, es decir al cuerpo $K_f = P(a_0, \ldots, a_n)$. El cuerpo de coeficientes de f es, $K_f = \mathbb{Q}(a_0, \ldots, a_n)$ en caso de característica 0, o $K_f = F_p(a_0, \ldots, a_n)$ en caso de característica $p \neq 0$.

Definición 5.36. Un polinomio $f \in K[X]$ se dice que es *resoluble por radicales sobre* K (o que la ecuación algebraica $f = 0$ es resoluble por radicales sobre K) si un cuerpo de escisión de f sobre K está contenido en una extensión radical de K. La expresión "f es resoluble por radicales" será sinónima de "f es resoluble por radicales sobre su cuerpo de coeficientes".

Ejemplo 5.37. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}$ es una extensión radical. La torre

$$\mathbb{Q}_0 = \mathbb{Q} \subset \mathbb{Q}_1 = \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}_2 = \mathbb{Q}_1(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$$

es una torre radical.

Nótese que si el cuerpo de escisión sobre $\mathbb{Q}$ del polinomio $f \in \mathbb{Q}[X]$ está contenido en $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ entonces los ceros de f son combinación lineal, con coeficientes en $\mathbb{Q}$, de los elementos 1, $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt{2}\sqrt[3]{2}$, $\sqrt{2}(\sqrt[3]{2})^2$ y $(\sqrt[3]{2})^2$. Es decir, los ceros de f serán una expresión algebraica de ciertos radicales.

Supóngase ahora $f = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$ y que un cuerpo de escisión de f sobre K_f es $E = K_f(\sqrt[3]{2}, \sqrt{2})$. En ese caso los ceros de f aparecerán como combinación lineal con coeficientes en K_f de los mismos $1, \sqrt{2}, \sqrt[3]{2}, \sqrt{2}\sqrt[3]{2}, \sqrt{2}(\sqrt[3]{2})^2$ y $(\sqrt[3]{2})^2$. Ahora, los coeficientes de dicha expresión lineal son, a su vez, expresiones algebraicas en las que intervienen solamente los coeficientes de f y números racionales. Este es el genuino

significado de la expresión: *la ecuación algebraica* $f = 0$ *es resoluble por radicales.* En lo sucesivo no se hará uso explícito del *cuerpo de coeficientes de un polinomio,* pero será muy ilustrativo su uso en la interpretación de los resultados sobre resolubilidad.

En general, si $f \in K[X]$ es tal que su cuerpo de escisión sobre K está contenido en una extensión radical F de K, entonces los ceros de f son una expresión algebraica del tipo de las obtenidas en 5.30.

Nótese que, como consecuencia de que la condición de extensión radical es invariante para isomorfismos, apartado *iii*) de la Proposición 5.34), de que cuerpos de escisión del mismo polinomio $f \in K[X]$ sobre K son K-isomorfos (4.14), y de (5.39) resulta que la condición de resolubilidad sobre K para un polinomio $f \in K[X]$ no depende del cuerpo de escisión de f sobre K que se considere. Nótese también que, en ese caso, los ceros de f pueden ser obtenidos mediante expresiones como las establecidas en 5.30.

Definición 5.38. Si E es un cuerpo de escisión sobre K del polinomio $f \in K[X]$, al grupo $Gal(E/K)$ se le denomina *grupo de Galois de* f *sobre* K y se denotará por $Gal_K(f)$. En la línea de lo establecido en (5.36) con $Gal(f)$ se indicará el grupo de Galois de f sobre su cuerpo de coeficientes y se denominará grupo de Galois de f.

Observación 5.39. Este grupo está determinado salvo isomorfismos. Es decir, si E y F son cuerpos de escisión del mismo polinomio $f \in K[X]$ sobre K, es sabido que existe un isomorfismo $\psi\colon E \to F$ sobre K (4.14) y la aplicación

$$\begin{aligned} Gal(E/K) &\to Gal(F/K) \\ \sigma &\mapsto \psi \circ \sigma \circ \psi^{-1} \end{aligned}$$

es un isomorfismo de grupos.

Para la prueba del Teorema 5.42, que constituye el resultado principal de esta sección -y de estas notas-, necesitaremos los dos Lemas siguientes.

Lema 5.40. *Sea* $F : K$ *una extensión finita de Galois con grupo de Galois cíclico de orden primo* $Caract(K) \neq p$, *tal que* K *contiene una raíz primitiva* p*-ésima de* 1. *Entonces existe un* $\alpha \in F$, *tal que* $F = K(\alpha)$ *y* $\alpha^p \in K$.

Demostración. Sea $\xi \in K$ raíz primitiva p-ésima de 1. Las potencias ξ^i, con $i = 1, 2, \ldots, p-1$, son precisamente todas las raíces primitivas p-ésimas de 1, ya que $Caract(K) \neq p$ y así U_p es de orden p (5.19) (nótese que si fuese $Caract(K) = p$ resultaría $X^p - 1 = (X-1)^p$, y que, como $F : K$ es de Galois, se tendría $\#Gal(F/K) = [F : K] = 1$ (5.9, apartado *ii*)). Sean $Gal(F/K) = \langle \sigma \rangle$ y $\beta \in F \setminus K$, si para cada $i = 0, 1, \ldots, p-1$ consideramos la resolvente de Lagrange definida por

$$\alpha_i := \beta + \xi^i \sigma(\beta) + \xi^{2i} \sigma^2(\beta) + \cdots + \xi^{(p-1)i} \sigma^{p-1}(\beta),$$

entonces

$$\sum_0^{p-1} \alpha_i = p\beta + \sum_{j=1}^{p-1} (1 + \xi^j + \xi^{2j} + \cdots + \xi^{(p-1)j}) \sigma^j(\beta) = p\beta,$$

ya que las ξ^j son todas ceros del polinomio $X^{p-1} + \cdots + X + 1 \in K[X]$ (son ceros de $X^p - 1$ y no lo son de $X - 1$). Por lo tanto, $\sum_0^{p-1} \alpha_i = p\beta \notin K$ pues, en caso contrario, se tendría $\beta \in K$ al ser $p\beta = (p1)\beta$, y $p1 \in K^*$ ($Caract(K) \neq p$), en contra de la hipótesis $\beta \notin K$. En particular, algún $\alpha_i \notin K$.

Ahora, para un tal α_i se tiene

$$\begin{aligned} \sigma(\alpha_i) &= \sigma(\beta + \xi^i \sigma(\beta) + \xi^{2i} \sigma^2(\beta) + \cdots + \xi^{(p-1)i} \sigma^{p-1}(\beta)) \\ &= \sigma(\beta) + \xi^i \sigma^2(\beta) + \xi^{2i} \sigma^3(\beta) + \cdots + \xi^{(p-1)i} \beta = (\xi^i)^{-1} \alpha_i, \end{aligned}$$

y, por lo tanto, $\sigma(\alpha_i^p) = ((\xi^i)^{-1} \alpha_i)^p = ((\xi^i)^p)^{-1} \alpha_i^p = \alpha_i^p$. Entonces $\alpha_i^p \in K$ ya que dicho elemento es fijo para cualquier automorfismo de F sobre K y $K = \alpha_i^p \in F^{Gal(F/K)}$, al ser la extensión $F : K$ de Galois. Por otra parte, como $\alpha_i \in F \setminus K$, se tiene $[K(\alpha_i) : K] \neq 1$ y, como consecuencia del Teorema del grado, $F = K(\alpha_i)$ ya que $[F : K] = p$ primo. □

Lema 5.41. *Sea K un cuerpo de característica 0 o un primo p no divisor del número natural m, y sea $F : K$ una extensión finita de Galois de grado n que es múltiplo de m. Entonces, si $\xi \in \overline{F}$ es una raíz primitiva m-ésima de 1 la extensión $F(\xi) : K(\xi)$ es de Galois finita y $[F(\xi) : K(\xi)]$ es divisor de n. Además, $Gal(F(\xi)/K(\xi))$ es isomorfo a un subgrupo de $Gal(F/K)$.*

Demostración. Si $f \in K[X]$ es tal que F es cuerpo de escisión de f sobre K, entonces $F(\xi)$ es cuerpo de escisión de $f(X^m - 1) \in K[X]$ sobre K, y también sobre $K(\xi)$. Además $F = K(\alpha_1, \ldots, \alpha_s)$, donde $\alpha_1, \ldots \alpha_s$ son los diferentes ceros de f, con lo que $F(\xi) = K(\alpha_1, \ldots, \alpha_s, \xi)$, y así resulta que $F(\xi) : K$ es separable pues los elementos $\alpha_1, \ldots, \alpha_s, \xi$ son todos separables sobre K (4.42) (el elemento ξ es separable sobre K por la hipótesis sobre la característica). Por lo tanto, $F(\xi) : K(\xi)$ es también de Galois finita. La aplicación $\psi\colon Gal(F(\xi)/K) \to Gal(F/K)$, con $\psi(\sigma) := \sigma\,|_F$, está bien definida ya que $\sigma|_F(F) = F$ al ser $F : K$ de Galois (4.61). Además ψ es un homomorfismo de grupos: $(\sigma \circ \tau)|_F = \sigma|_F \circ \tau|_F$.

Ahora, si $\sigma \in Gal(F(\xi)/K(\xi)) \subset Gal(F(\xi)/K)$ y $\psi(\sigma) = \sigma|_F = id_F$, se sigue que $\sigma = id_{F(\xi)}$, ya que $\sigma(\xi) = \xi$.

Por tanto, el homomorfismo $\psi|_{Gal(F(\xi)/K(\xi))}\colon Gal(F(\xi)/K(\xi)) \to Gal(F/K)$ es inyectivo y $\psi(Gal(F(\xi)/K(\xi))$ es un subgrupo de $Gal(F/K)$ isomorfo a $Gal(F(\xi)/K(\xi))$ cuyo orden divide a $\#Gal(F/K)$, por el Teorema de Lagrange. Siendo de Galois las extensiones $F : K$ y $F(\xi) : K(\xi)$ sus grados coinciden con los órdenes de sus grupos respectivos, y de ahí se sigue el resultado. □

Teorema 5.42. *(Gran Teorema de Galois en característica 0)*

Sea K un cuerpo de característica 0 y sea $f \in K[X]$ tal que $\partial(f) > 0$. La ecuación algebraica $f = 0$ es resoluble por radicales sobre K si, y solo si, el grupo $Gal_K(f)$ es resoluble.

Demostración. Sea f resoluble por radicales sobre K. Por hipótesis, existe una extensión radical $F : K$ tal que un cuerpo E_f, de escisión de f sobre K, está contenido en F. Pondremos $K \subset E_f \subset F \subset \overline{K} = \overline{F} = \overline{E_f}$. Además, se puede suponer que $F : K$ es una extensión normal (es decir, de Galois al ser K de característica 0), pues en otro caso, la clausura normal N de F sobre K (tomada dentro de $\overline{K}$) estaría en la misma situación, es decir, $K \subset E_f \subset N \subset \overline{K} = \overline{F} = \overline{E_f}$ y, por la Proposición 4.63, $N : K$ sería radical, finita y de Galois.

Sea entonces $F : K$ radical de Galois finita, y sea la torre de cuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = F$$

donde, para cada $i = 1, \ldots, r$, $K_i = K_{i-1}(a_i)$ con los $a_i \in K_i$ tales que $a_i^{n_i} \in K_{i-1}$ para ciertos enteros positivos n_i. Sea $n = \prod_i n_i$ y sea $\xi \in \overline{K}$ una raíz primitiva n-ésima de 1. Entonces, poniendo $F_i = K_i(\xi)$, se obtiene una torre radical

$$K = K_0 \subset F_0 \subset F_1 \subset \cdots \subset F_r = K_r(\xi) = F(\xi),$$

ya que $F_i = K_i(\xi) = K_{i-1}(\alpha_i, \xi) = F_{i-1}(\alpha_i)$, $\alpha_i^{n_i} \in K_{i-1} \subset F_{i-1} = K_{i-1}(\xi)$, para todo $i = 1, 2, \ldots, r$, y $F_0 = K(\xi)$ con $\xi^n = 1 \in K$. Nótese que $\xi^{n/n_i} \in F_0$ es una raíz primitiva n_i-ésima de 1, para cada $i = 1, \ldots, r$. Por lo tanto, cada extensión $F_i : F_{i-1}$ es una extensión finita de Galois de grupo abeliano (pues $Gal(F_i/F_{i-1})$ es abeliano por la Proposición 5.25), y también lo es la extensión $F_0 = K(\xi) : K_0 = K$ (proposición 5.22, apartado 2). Además, $F(\xi) : K$ es finita de Galois ya que F es cuerpo de escisión sobre K de algún polinomio $g \in K[X]$ al ser $F : K$ normal, y por lo tanto $F(\xi)$ es cuerpo de escisión sobre K del polinomio $g(X^n - 1) \in K[X]$. Si $G = Gal(F(\xi)/K)$, entonces, como consecuencia del Teorema fundamental de teoría de Galois, cada $H_i = Gal(F(\xi)/F_i)$ es un subgrupo normal de $H_{i-1} = Gal(F(\xi)/F_{i-1})$, y además $Gal(F_i/F_{i-1}) \simeq H_{i-1}/H_i$ es un grupo abeliano. El grupo $G = Gal(F(\xi)/K)$ es así resoluble y también lo es el grupo $Gal_K(f) = Gal(E_f/K)$ ya que, como $E_f : K$ es de Galois, $Gal(F(\xi)/E_f)$ es subgrupo normal de G y $G/Gal(F(\xi)/E_f) \simeq Gal_K(f)$ es resoluble al ser isomorfo a un cociente de un grupo resoluble (1.65).

Recíprocamente, supongamos que $Gal_K(f) = Gal(E/K)$ es grupo resoluble donde E es un cuerpo de escisión de f sobre K. El Teorema quedará probado si se encuentra una extensión radical de K que contiene a E. Sea $n = [E : K] = \#Gal(E/K)$ (la última igualdad se sigue de que $E : K$ es de Galois finita), y sea ξ una raíz primitiva n-ésima de 1. Por el Lema 5.41 sabemos que $[E(\xi) : K(\xi)]$ es divisor de n y que el grupo $\widetilde{G} := Gal(E(\xi)/K(\xi))$ es resoluble al ser isomorfo a un subgrupo de $G := Gal(E/K)$, que es resoluble por hipótesis. Existe entonces una torre normal

$$\left\{id_{E(\xi)}\right\} = H_m \subset H_{m-1} \subset \cdots \subset H_1 \subset H_0 = \widetilde{G}$$

en la que cada grupo cociente H_i/H_{i+1} es de orden primo p_i (1.64), divisor de $\#\widetilde{G} = [E(\xi) : K(\xi)]$ que es, a su vez, divisor de n, y así cada p_i divide a n. Sea $F_i = E(\xi)^{H_i}$, para cada $i = 0, 1, \ldots, m-1$. Por el Teorema fundamental de teoría de Galois resulta entonces una torre de cuerpos

$$K(\xi) = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_m = E(\xi),$$

y como $E(\xi) : E(\xi)^{H_{i+1}}$ y $E(\xi) : E(\xi)^{H_i}$ son extensiones de Galois, siendo H_{i+1} subgrupo normal de H_i, resulta que $F_{i+1} : F_i$ es una extensión de Galois con grupo isomorfo a H_i/H_{i+1}. Nótese que, para cada $i = 0, 1, \ldots, m-1$, $p_i = \#(H_i/H_{i+1})$ es divisor de n y, como ξ es raíz primitiva n-ésima de 1, $F_i = E(\xi)^{H_i}$ contiene a ξ^{n/p_i}, que es una raíz primitiva p_i-ésima de 1. Como $\left[E(\xi)^{H_{i+1}} : E(\xi)^{H_i}\right] = p_i$ es primo y $E(\xi)^{H_i}$ contiene una raíz primitiva p_i-ésima de 1, la aplicación del Lema 5.40 proporciona la existencia de un $\alpha_i \in F_{i+1}$ tal que $F_{i+1} = F_i(\alpha_i)$ y tal que $\alpha_i^{p_i} \in F_i$. Entonces la torre

$$K \subset K(\xi) = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_m = E(\xi)$$

es una torre radical con $E \subset E(\xi)$. Por tanto, f es resoluble por radicales sobre K. □

La resolubilidad por radicales (según lo establecido en (5.44)) de la ecuación $f = 0$ ($f \in \mathbb{R}[X]$) es bien conocida para polinomios f de grados 2, 3 y 4. La de grado 2 era esencialmente conocida ya por la civilización babilónica (1700 a. C.), y para los grados 3 y 4 las soluciones fueron dadas por Cardano (1545) y Tartaglia (1539). Durante mucho tiempo han sido infructuosos los intentos de encontrar procedimientos algebraicos análogos para la ecuación algebraica de grado 5. El primero en resolver el problema ha sido el matemático noruego N. Abel quien prueba, en 1829,) que la ecuación algebraica general de grado $n \geqslant 5$ no es resoluble por radicales.

El objetivo del resto de la sección es la prueba de este Teorema. Necesitaremos algunos resultados previos.

Proposición 5.43. *Si $f \in K[X]$ es un polinomio con m ceros diferentes, el grupo $Gal_K(f)$ es isomorfo a un subgrupo del grupo S_m de las permutaciones de m elementos.*

Demostración. Sea $E = K(\alpha_1, \ldots, \alpha_m) \subset \overline{K}$ cuerpo de escisión de f sobre K y sea $f = c(X - \alpha_1)^{r_1} \cdots (X - \alpha_m)^{r_m}$ su factorización en $E[X]$.

Para $\sigma \in Gal_K(f)$, se tiene $f = f^\sigma = c(X - \sigma\alpha_1)^{r_1} \cdots (X - \sigma\alpha_m)^{r_m}$ y, por la unicidad de la factorización en irreducibles en $E[X]$, se verifica que $\{\alpha_1, \ldots, \alpha_m\}$

$= \{\sigma\alpha_1, \ldots, \sigma\alpha_m\}$, es decir, σ establece una permutación del conjunto $\{\alpha_1, \ldots, \alpha_m\}$. Además si $\sigma, \tau \in Gal(E/K)$ establecen la misma permutación necesariamente se tiene $\sigma = \tau$, pues el valor de cada isomorfismo en un $x \in E$ está determinado por su valor en los generadores de la extensión. Sea $\widetilde{\sigma} \in S_m$ definida por $\widetilde{\sigma}(i) = j \Leftrightarrow \sigma(\alpha_i) = \alpha_j$. Entonces la aplicación $Gal_K(f) \to S_m$, definida por $\sigma \mapsto \widetilde{\sigma}$, es un homomorfismo inyectivo de grupos que establece un isomorfismo entre $Gal_K(f)$ y el grupo imagen, que es un subgrupo de S_m. □

Esta Proposición tiene un corolario inmediato.

Corolario 5.44. *Si K es de característica 0 y $f \in K[X]$ es de grado menor o igual que 4, f es resoluble por radicales sobre K.*

Demostración. Si $r \leqslant 4$ es el número de raíces diferentes de f entonces, en virtud de la Proposición anterior, $Gal_K(f)$ es isomorfo a un subgrupo del grupo S_r que es resoluble (1.69). Del gran Teorema de Galois se sigue que el polinomio f es resoluble por radicales sobre K. □

Obsérvese que sin haber hecho mención explícita del procedimiento de obtención de las raíces de un polinomio de grado $\leqslant 4$ con coeficientes racionales mediante expresiones algebraicas con radicales, como se indicaba en 5.30, el corolario 5.44 afirma que tal procedimiento existe.

Lema 5.45. *Si $f \in \mathbb{Q}[X]$ es un polinomio irreducible en $\mathbb{Q}[X]$ de grado primo p y con exactamente dos raíces complejas no reales, entonces $Gal_{\mathbb{Q}}(f) \simeq S_p$.*

Demostración. El polinomio irreducible f es separable ya que $Caract(\mathbb{Q}) = 0$ y, por tanto, $f = c\prod_1^p (X - \alpha_i)$, con $\alpha_1, \ldots, \alpha_p$ elementos de $\mathbb{C}$ diferentes. Sean $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$, $\alpha_3, \ldots \alpha_p \in \mathbb{R}$ y sea $E_f = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p)$ el cuerpo de escisión, en $\mathbb{C}$, de f sobre $\mathbb{Q}$. Por la Proposición 5.43 se sabe que $Gal_{\mathbb{Q}}(f)$ es isomorfo a un subgrupo H del grupo S_p. Además, la torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset E_f$ proporciona $[E_f : \mathbb{Q}] = [E_f : \mathbb{Q}(\alpha_1)]\,[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [E_f : \mathbb{Q}(\alpha_1)]\,p$, ya que $f = cIrr(\alpha_1, \mathbb{Q})$ (c es el coeficiente principal de f), y entonces p es divisor del orden de H, pues $[E_f : \mathbb{Q}] = \#Gal_{\mathbb{Q}}(f) = \#H$ al ser de Galois la extensión $E_f : \mathbb{Q}$. Por el Teorema de Cauchy (1.45) sabemos que existe un elemento $\widetilde{\sigma} \in H$ de período p que es un p-ciclo (1.59) de S_p. Además, necesariamente

se tiene $\alpha_1 = \overline{\alpha_2}$ ya que los coeficientes de f son números reales, y así la conjugación $(-) : \mathbb{C} \to \mathbb{C}$ se restringe a un $\mathbb{Q}$-automorfismo

$$\tau \colon \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p) \to \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p),$$

ya que $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p) : \mathbb{Q}$ es normal y $\tau(\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_p)) \subset \overline{\mathbb{Q}} \subset \mathbb{C}$. El automorfismo $\tau \in Gal_{\mathbb{Q}}(f)$ está definido por las condiciones $\tau(\alpha_1) = \overline{\alpha_1} = \alpha_2$, $\tau(\alpha_2) = \overline{\alpha_2} = \alpha_1$ y $\tau(\alpha_i) = \alpha_i$, para $i = 3, \ldots, p$. En consecuencia, utilizando las notaciones de la prueba de (5.43), resulta que la trasposición $\widetilde{\tau}$ y el p-ciclo $\widetilde{\sigma}$ son elementos de H. El subgrupo H de S_p satisface entonces las hipótesis de la Proposición 1.60 y se sigue que $Gal_{\mathbb{Q}}(f) \simeq H = S_p$. □

Teorema 5.46. *(Teorema de Abel)*

Para cada $n \geqslant 5$ existe una ecuación algebraica $f = 0$ con coeficientes racionales y de grado n que no es resoluble por radicales sobre $\mathbb{Q}$.

Demostración. Bastará con encontrar un $f \in \mathbb{Q}[X]$ de grado 5 que no sea resoluble por radicales sobre $\mathbb{Q}$, ya que para $n > 5$, el polinomio $g = X^{n-5}f$ es de grado n y tiene el mismo cuerpo de escisión que f sobre $\mathbb{Q}$ y, por lo tanto, el mismo grupo de Galois cuya no resolubilidad establecerá el resultado.

Sea $f = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$. Por el criterio de Eisenstein (para el primo 5) f es irreducible sobre $\mathbb{Q}$ (por lo tanto, separable sobre $\mathbb{Q}$) y tiene exactamente dos raíces complejas no reales. En efecto, la función continua $f \colon \mathbb{R} \to \mathbb{R}$ es creciente en el intervalo $(-\infty, -1)$, tiene un máximo en $x = -1$, es decreciente en el intervalo $(-1, 1)$, tiene un mínimo en $x = 1$, y es creciente en el intervalo $(1, \infty)$. Además $f(-2) < 0 < f(-1)$, $f(1) < 0 < f(2)$. Así, como consecuencia del Teorema de Bolzano, $f = 0$ tiene tres raíces reales $\alpha_1 \in [-2, -1]$, $\alpha_2 \in [-1, 1]$ y $\alpha_3 \in [1, 2]$. En virtud del Teorema de Rolle se puede afirmar que éstas son las únicas raíces reales de f. Las otras dos α, β son elementos de la clausura algébrica de $\mathbb{Q}$ que está contenida en $\mathbb{C}$. Entonces el polinomio f satisface las hipótesis del Lema 5.43 y por ello $Gal_{\mathbb{Q}}(f) \simeq S_5$, que es un grupo no resoluble, como ya ha sido probado en teoría de grupos (1.70). El gran Teorema de Galois proporciona el resultado. □

Para el estudio de la resolubilidad por radicales en característica p necesitaremos estudiar por separado las extensiones con grupo cíclico, tanto de orden p como de orden primo con p. Las versiones aditiva y multiplicativa del Teorema 90 de Hilbert - que a su vez necesitan de ciertas consideraciones acerca de la norma y la traza de una extensión finita - abrirán el camino a la Proposición 5.51 y al Teorema de Artin-Schreier (5.52) que caracterizan dichas extensiones.

Si S es un conjunto y K un cuerpo, el conjunto $\mathfrak{M}(S,K)$ de aplicaciones $\varphi\colon S \to K$ es un K-espacio vectorial con las operaciones $(\varphi+\psi)(x) = \varphi(x)+\psi(x)$ y $(a\varphi)(x) = a\varphi(x)$, para todos $x \in S$ y $a \in K$. Si ahora G es un grupo, nos fijaremos en aquellos $\varphi \in \mathfrak{M}(G,K)$ tales que establecen homomorfismos de G en K^*. Tales aplicaciones se denominarán caracteres de G en K.

Lema 5.47. *(Lema de Dedekind)*

Sea G un grupo. Si $\sigma_1,\ldots,\sigma_n\colon G \to K^*$ son n caracteres diferentes de G en K, entonces son elementos linealmente independientes del K-espacio vectorial $\mathfrak{M}(G,K)$.

Demostración. Es lícito suponer que $n \geqslant 1$, pues un carácter es obviamente independiente al ser un elemento no nulo de $\mathfrak{M}(G,K)$. De entre las hipotéticas relaciones de dependencia lineal $\sum_1^n a_i\sigma_i = 0$ seleccionamos una de menor número de sumandos con constante a_i no nula. Podemos suponer que tras una renumeración tal relación de dependencia minimal es

$$a_1\sigma_1 + \cdots + a_r\sigma_r = 0, \quad (*)$$

con todos los $a_i \neq 0$ (y $r \geqslant 2$). Siendo diferentes los caracteres, existe un $g \in G$ tal que $\sigma_1(g) \neq \sigma_2(g)$, y dado cualquier $h \in G$ se tiene $\sum_1^r a_i\sigma_i(gh) = \sum_1^r a_i\sigma_i(g)\sigma_i(h) = \Big(\sum_1^r a_i\sigma_i(g)\sigma_i\Big)(h) = 0$, es decir, $\sum_1^r a_i\sigma_i(g)\sigma_i = 0$. Como $\sigma_1(g) \neq 0$ se tiene la relación

$$a_1\sigma_1 + a_2\sigma_2(g)\sigma_1(g)^{-1}\sigma_2 + \cdots + a_r\sigma_r(g)\sigma_1(g)^{-1}\sigma_r = 0$$

que restándole $(*)$ proporciona

$$\left[a_2\sigma_2(g)\sigma_1(g)^{-1} - a_2\right]\sigma_2 + \cdots + \left[a_r\sigma_r(g)\sigma_1(g)^{-1} - a_r\right]\sigma_r = 0$$

que es una relación de dependencia lineal con menor número de sumandos no triviales que la $(*)$, lo que contradice la minimalidad de dicha relación. □

Si ahora E es un cuerpo, diferentes encajes $\sigma_1,\ldots,\sigma_n\colon E \to K$ pueden ser considerados como caracteres de E^* en K^*.

Definición 5.48. Sea $E:K$ una extensión finita y sea $[E:K]_s = r$ (que coincide con $[E:K]$ si K es de característica 0) y $[E:K]_i = p^\mu$ (como se sabe esta última igualdad solo tiene sentido si $Caract(K) = p$). Sean $\sigma_1, \ldots, \sigma_r$ los diferentes encajes, sobre K, de E en la clausura algébrica $\overline{K}$ de K. Para un elemento $\alpha \in E$ se define su *norma* respecto de la extensión $E:K$ mediante la expresión

$$N_K^E(\alpha) = \prod_1^r \sigma_i \alpha^{p^\mu} = \Big(\prod_1^r \sigma_i \alpha\Big)^{[E:K]_i}.$$

Se define también la *traza* de α respecto de la extensión $E:K$ como

$$Tr_K^E(\alpha) = [E:K]_i \sum_i^r \sigma_i \alpha,$$

que es obviamente nula en el caso de que la extensión $E:K$ no sea separable. Si $E:K$ es separable se tiene $N_K^E(\alpha) = \prod_1^r \sigma_i\alpha$ y $Tr_K^E(\alpha) = \sum_i^r \sigma_i\alpha$.

Para un elemento $\alpha \in E$ algebraico sobre K el conjunto de raíces distintas en $\overline{K}$ del polinomio $Irr(\alpha, K)$ es, precisamente, el conjunto $\{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$, en donde $\sigma_1, \ldots, \sigma_r$ son todos los encajes de $K(\alpha)$ en $\overline{K}$ sobre K. Por tanto, se tiene

$$Irr(\alpha, K) = X^n - Tr_K^{K(\alpha)}(\alpha)X^{n-1} + \cdots + (-1)^n N_K^{K(\alpha)}(\alpha),$$

en donde $n = r$ si α es separable sobre K, y $Tr_K^{K(\alpha)}(\alpha) = 0$ en otro caso. Obsérvese que $N_K^{K(\alpha)}(\alpha)$ y $Tr_K^{K(\alpha)}(\alpha)$ son, por lo tanto, elementos de K.

En nuestro estudio, la utilidad de la norma y la traza estará restringida a la obtención del Teorema 90 de Hilbert en sus formas aditiva y multiplicativa, y que será utilizado para la caracterización de extensiones cíclicas. Recuérdese que una extensión cíclica es una extensión de Galois con grupo de Galois cíclico.

Teorema 5.49. *(Teorema 90 de Hilbert. Forma multiplicativa)*

Sean $E:K$ una extensión cíclica de grado n, $G = \langle\sigma\rangle$ su grupo de Galois y $\beta \in E$. Entonces $N_K^E(\beta) = 1$ si, y solo si, existe un $\alpha \in E^*$ tal que $\beta = \dfrac{\alpha}{\sigma(\alpha)}$.

Demostración. Cada $\tau \in G$ será considerado como un encaje de E en $\overline{K} = \overline{E}$ sobre K y, por lo tanto, como un elemento del $\overline{K}$- espacio (y, por ello, E-espacio) $\mathfrak{M}(G, \overline{K})$.

Para $\tau, \tau' \in G$ denotaremos con $\tau * \tau' \in \mathfrak{M}(G, \overline{K})$ la aplicación definida por $(\tau * \tau')(x) = \tau(x)\tau'(x)$, y usaremos la notación exponencial $x^\tau = \tau(x)$, por lo que $x^{\tau * \tau'} = x^\tau x^{\tau'}$. Como consecuencia del Lema de Dedekind (5.47) la aplicación

$$id_E + \beta\sigma + \beta^{id_E * \sigma}\sigma^2 + \cdots + \beta^{id_E * \sigma * \sigma^2 * \cdots * \sigma^{n-2}}\sigma^{n-1} : E \to \overline{K}$$

no es idénticamente nula (los caracteres $id_E, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ son diferentes), es decir, existe un elemento $\gamma \in E$ tal que no es nulo el siguiente elemento:

$$\begin{aligned}\alpha &= \big(id_E + \beta\sigma + \beta^{id_E*\sigma}\sigma^2 + \cdots + \beta^{id_E*\sigma*\sigma^2*\cdots*\sigma^{n-2}}\sigma^{n-1}\big)(\gamma)\\ &= \gamma + \beta\gamma^{\sigma} + \beta^{id_E*\sigma}\gamma^{\sigma^2} + \cdots + \beta^{id_E*\sigma*\sigma^2*\cdots*\sigma^{n-2}}\gamma^{\sigma^{n-1}}.\end{aligned}$$

Ahora, si $1 = N_K^E(\beta) = \beta^{id_E*\sigma*\sigma^2*\cdots*\sigma^{n-2}*\sigma^{n-1}}$ se tiene

$$\beta\sigma(\alpha) = \beta\gamma^{\sigma} + \beta^{id_E*\sigma}\gamma^{\sigma^2} + \cdots + \beta^{id_E*\sigma*\sigma^2*\cdots*\sigma^{n-2}\gamma^{\sigma^{n-1}}} + \beta^{id_E*\sigma*\sigma^2*\cdots*\sigma^{n-1}}\gamma = \alpha.$$

Recíprocamente, si existe $\alpha \in E$ tal que $\beta = \dfrac{\alpha}{\sigma\alpha}$ resulta

$$N_K^E(\beta) = N_K^E\big(\frac{\alpha}{\sigma(\alpha)}\big) = \frac{N_K^E(\alpha)}{N_K^E(\sigma(\alpha))} = 1,$$

ya que N_K^E es evidentemente multiplicativa y además $N_K^E(\sigma(\alpha)) = N_K^E(\alpha)$, pues las expresiones para ambos miembros dadas por 5.48 solo se diferencian en una permutación del orden de sus factores. □

Teorema 5.50. *(Teorema 90 de Hilbert. Forma aditiva)*

Sean $E : K$ una extensión cíclica de grado n con grupo $G = \langle\sigma\rangle$. Entonces $\beta \in E$ es tal que $Tr_K^E(\beta) = 0$ si, y solo si, existe un $\alpha \in E$ tal que $\beta = \alpha - \sigma(\alpha)$.

Demostración. Si existe tal elemento α se tiene $Tr_K^E(\beta) = Tr_K^E(\alpha - \sigma(\alpha)) = 0$ ya que Tr_K^E es evidentemente aditiva y $Tr_K^E(\alpha) = Tr_K^E(\sigma(\alpha))$ pues ambos miembros solo se diferencian en el orden de los sumandos.

Recíprocamente, si $Tr_K^E(\beta) = 0$, utilizando la misma notación exponencial que antes, podemos afirmar que existe un $\gamma \in E$ tal que $Tr_K^E(\gamma) \neq 0$, como consecuencia del Lema de Dedekind 5.47. Entonces, poniendo

$$\alpha = \frac{1}{Tr_K^E(\gamma)}\Big[\beta\gamma + (\beta + \beta^{\sigma})\gamma^{\sigma} + \cdots + (\beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-2}})\gamma^{\sigma^{n-2}}\Big]$$

resulta

$$\alpha - \sigma(\alpha) = \frac{1}{Tr_K^E(\gamma)}[\beta\gamma + (\beta + \beta^{\sigma})\gamma^{\sigma} + \cdots + (\beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-2}})\gamma^{\sigma^{n-2}} -$$

$$-[\beta^{\sigma}\gamma^{\sigma}+(\beta^{\sigma}+\beta^{\sigma^2})\gamma^{\sigma^2}+\cdots+(\beta^{\sigma}+\beta^{\sigma^2}+\cdots+\beta^{\sigma^{n-1}})\gamma^{\sigma^{n-1}}]]=$$

$$=\frac{1}{Tr_K^E(\gamma)}\left[\beta\gamma+\beta\gamma^{\sigma}+\cdots+\beta\gamma^{\sigma^{n-1}}\right]=\beta.$$

Para los anteriores cálculos se ha tenido en cuenta que $Tr_K^E(\gamma)\in K$ (pues es evidente que $\sigma\left(Tr_K^E(\gamma)\right)=Tr_K^E(\gamma)$) y la hipótesis $Tr_K^E(\beta)=0$. □

Las dos versiones del Teorema 90 permitirán caracterizar las extensiones cíclicas de grado p y las de grado primo con p, siendo p la característica de K.

Proposición 5.51. *Sea p un primo no divisor de $n>0$ y sea K un cuerpo de característica p que contiene una raíz primitiva n-ésima de 1. Entonces, si $E:K$ es una extensión cíclica de grado n, existe un $\alpha\in E$ tal que $E=K(\alpha)$ y tal que $a=\alpha^n\in K$, es decir, α es un cero del polinomio $X^n-a\in K[X]$. Recíprocamente, si $\alpha\in\overline{K}$ es un cero de $X^n-a\in K[X]$, entonces la extensión $K(\alpha):K$ es cíclica, de grado d, que es divisor de n, y además $\alpha^d\in K$.*

Demostración. Sea $\xi\in K$ raíz primitiva n-ésima de 1 y sea $G=Gal(E/K)=\langle\sigma\rangle$. Siendo separable la extensión $E:K$, y como $\sigma\left(\xi^{-1}\right)=\xi^{-1}$, resulta $N_K^E(\xi^{-1})=\prod_1^n\sigma^i(\xi^{-1})=\left(\xi^{-1}\right)^n=1$, con lo cual, por el Teorema 90 de Hilbert en su forma multiplicativa (5.49), podemos afirmar que existe un $\alpha\in E$ tal que $\sigma(\alpha)=\xi\alpha$. Como $\xi\in K$ resulta $\sigma^2(\alpha)=\sigma(\xi\alpha)=\xi^2\alpha$ y también $\sigma^i(\alpha)=\xi^i\alpha$, para $i=1,\ldots,n$. Por ello, el polinomio irreducible de α sobre K tiene al menos n ceros diferentes (los $\sigma^i(\alpha)=\xi^i\alpha$) y así $n=[E:K]\geqslant[K(\alpha):K]=\partial Irr(\alpha,K)\geqslant n$. Resultando así $E=K(\alpha)$, y además $\sigma(\alpha^n)=(\sigma(\alpha))^n=(\xi\alpha)^n=\xi^n\alpha^n=\alpha^n$, con lo que se tiene $\alpha^n\in E^G=K$.

Si $\alpha\in\overline{K}$ es un cero de $f=X^n-a\in K[X]$, todos los ceros de f son los n elementos diferentes $\xi^i\alpha\in K(\alpha)$, para $i=1,\ldots,n$, y así $K(\alpha)$ es cuerpo de escisión de f sobre K. La extensión $K(\alpha):K$ es separable al serlo el polinomio f y, por tanto, también el $Irr(\alpha,K)$ divisor de f. Así $K(\alpha):K$ es de Galois finita. Si $G=Gal(K(\alpha)/K)$ y $\sigma\in G$, entonces $\sigma(\alpha)$ es también un cero de X^n-a y, por lo tanto, $\sigma(\alpha)=\gamma_\sigma\alpha$, siendo γ_σ una raíz de la unidad (es decir una potencia de ξ). Se establece así un homomorfismo $G\to U_n$, $\sigma\mapsto\gamma_\sigma$, obviamente inyectivo, de G en el grupo de las raíces n-ésimas de $1\in K$ que es de orden n, al ser n primo con p (5.21). Entonces G es cíclico y su orden

d es divisor de n. Si se pone $G = \langle\sigma\rangle$, resulta $\sigma\left(\alpha^d\right) = (\sigma(\alpha))^d = (\gamma_\sigma\alpha)^d = \gamma_\sigma^d\alpha^d = \alpha^d$ pues γ_σ es una raíz d-ésima (primitiva) de 1. En consecuencia, $\alpha^d \in K(\alpha)^G = K$. □

Proposición 5.52. *(Artin-Schreier)*

Sea K un cuerpo de característica p. Si $E : K$ es cíclica de grado p, entonces $E = K(\alpha)$ donde $\alpha \in E$ es un cero de algún polinomio $X^p - X - a \in K[X]$. Recíprocamente, si un polinomio $f = X^p - X - a \in K[X]$ no escinde en K es irreducible en $K[X]$ y, en este caso, la extensión $K(\alpha) : K$ es cíclica de grado p, siendo α cualquier cero de f.

Demostración. Sea $G = \langle\sigma\rangle = Gal(E/K)$ de orden p. La extensión $E : K$ es separable y $Tr_K^E(x) = \sum_1^p \sigma^i(x)$ para $x \in E$. Ahora, $Tr_K^E(-1) = \sum_1^p \sigma^i(-1) = p(-1) = 0$ y, por el Teorema 90 de Hilbert en su forma aditiva (5.50) se puede asegurar la existencia de un $\alpha \in E$ tal que $1 = \sigma(\alpha) - \alpha$. Por lo tanto, $\sigma^i(\alpha) = \alpha + i$, $i = 1, \ldots, p$, son ceros del $Irr(\alpha, K)$, y al ser diferentes proporcionan $p = [E : K] \geqslant [K(\alpha) : K] = \partial Irr(\alpha, K) \geqslant p$. Por ello, $E = K(\alpha)$ y $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, con lo cual se tiene que $a = \alpha^p - \alpha \in E^G = K$; es decir, α es cero del polinomio $X^p - X - a \in K[X]$ que es mónico de grado p, y por esto $X^p - X - a = Irr(\alpha, K)$.

Recíprocamente, si $\alpha \in \overline{K}$ es cualquier cero de $f = X^p - X - a \in K[X]$, el conjunto de las raíces de f es $\{\alpha, \alpha + 1, \ldots, \alpha + p - 1\}$. Por lo tanto, f es separable y $[K(\alpha) : K]$ es de Galois finita (la extensión trivial si f escinde en K). Supongamos que f no escinde en K y probemos que entonces f es irreducible en $K[X]$, con lo cual la extensión será cíclica de grado p. Para ello sea $f = gh$ una factorización de f en $K[X]$; entonces, si g no es constante será un producto de algunos de los factores $(X - \alpha - i)$, $i \in \{1, 2, \ldots, p\}$, puesto que la factorización de f en $\overline{K}[X]$ es

$$f = \prod_{i=1}^{p}(X - \alpha - i);$$

si el grado de g es d, el coeficiente del término de grado $d - 1$ será una suma de d sumandos de la forma $-(\alpha + i)$ y, por ello, igual $-d\alpha + j$ para un cierto entero j. Así, si $d < p$ se tiene $\alpha \in K$ ya que $d\alpha = (d1_K)\alpha$ y $d1_K \neq 0$, en ese caso. Ello contradice la hipótesis de que f no escinde en K, y se concluye que f es irreducible en $K[X]$. La extensión $[K(\alpha) : K]$ es de Galois de grado p y, en consecuencia, cíclica. □

Observación 5.53.

Es necesario destacar que si K es de característica p y si $F : K$ es un extensión finita, entonces $Gal(F/F_s(K)) = \{id_F\}$, siendo $F_s(K)$ la subextensión maximal separable de K en F definida en (4.52). En efecto, si $\beta \in F$, el elemento β es el único cero del polinomio $Irr(\beta, F_s(K)) = X^{p^\mu} - b = (X - \beta)^{p^\mu}$ (4.48) y, por lo tanto, para cada encaje $\sigma\colon F \to \overline{K} = \overline{F} = \overline{F_s(K)}$ sobre K (y en particular para cada $\sigma \in Gal(F/F_s(K))$) se tiene necesariamente $\sigma(\beta) = \beta$. Además, si $\alpha \in F_s(K)$ y $\sigma \in Gal(F/K)$ entonces $\sigma(\alpha)$ es un cero del polinomio separable $Irr(\alpha, K)$ y así $Irr(\alpha, K) = Irr(\sigma(\alpha), K)$, de lo que resulta que $\sigma(\alpha)$ es un elemento de F también separable sobre K. Es decir, para cada $\sigma \in Gal(F/K)$, su restricción a $F_s(K)$ establece un encaje $F_s(K) \to F_s(K)$ que es un automorfismo de $F_s(K)$ al ser una extensión finita de K. Ahora el homomorfismo de grupos $Gal(F/K) \to Gal(F_s(K)/K)$, definido por $\sigma \mapsto \sigma\,|_{F_s(K)}$, tiene por núcleo el grupo $Gal(F/F_s(K)) = \{id_F\}$ y entonces la restricción establece un isomorfismo de $Gal(F/K)$ con un subgrupo de $Gal(F_s(K)/K)$. Si además $F : K$ es normal, el anterior homomorfismo restricción es un isomorfismo. En efecto, cada $\sigma \in Gal(F_s(K)/K)$ se extiende a un encaje $\tau\colon F \to \overline{K} = \overline{F} = \overline{F_s(K)}$ sobre K que ahora es necesariamente un automorfismo de F.

Obsérvese también que si $F : K$ es una extensión normal, entonces $F_s(K)\colon K$ es una extensión de Galois. En efecto, si f es un polinomio irreducible en $K[X]$ que tiene un cero α en $F_s(K)$, los restantes ceros de f (como elementos de $\overline{F} = \overline{K}$), que están en F, al ser $F : K$ normal, son también separables sobre K pues todos tienen el mismo polinomio irreducible sobre K, y así f escinde en $F_s(K)$.

Se puede enunciar ahora:

Proposición 5.54. *Si $Caract(K) = p \neq 0$ y $F : K$ es una extensión normal finita, entonces la subextensión maximal separable $F_s(K)$ de K en F es una extensión finita de Galois de K y los grupos $Gal(F/K)$ y $Gal(F_s(K)/K)$ son isomorfos.*

Observación 5.55. Conviene destacar que, como consecuencia de lo anterior, en una extensión normal $F : K$ el orden del grupo de Galois es divisor del grado de la extensión,

pues

$$\#Gal(F/K) = \#Gal(F_s(K)/K) = [F_s(K) : K] \mid [F : K].$$

Observación 5.56. Si una extensión $F : E$ es puramente inseparable finita, $F = E(\beta_1, \ldots, \beta_t)$ para ciertos $\beta_1, \ldots, \beta_t$ puramente inseparables sobre E y existen enteros μ_i $(i = 1, \ldots, t)$ tales que $\beta_i^{\mu_i} \in E$. Es entonces evidente que la extensión $F : E$ es radical; la torre $E \subset E(\beta_1) \subset \cdots \subset E(\beta_1, \ldots, \beta_t)$ es una torre radical (5.31).

El siguiente Teorema establece la resolubilidad por radicales en característica positiva.

Teorema 5.57. *Sea K un cuerpo de característica $p \neq 0$ y $f \in K[X]$ un polinomio no constante. Entonces son equivalentes las afirmaciones*

i) El polinomio f es resoluble por radicales sobre K.

ii) $Gal_K(f)$ es un grupo resoluble.

Demostración. ii) $\Rightarrow$ i)

Sea F cuerpo de escisión de f sobre K y sea E la subextensión maximal separable de F sobre K. Por (5.54) la extensión $E : K$ es de Galois y los grupos $Gal_K(f) = Gal(F/K)$ y $Gal(E/K)$ son isomorfos. Por tanto, $Gal(E/K)$ es un grupo resoluble en virtud de la hipótesis. Sea $n = [E : K] = \#Gal(E/K) = p^r m$, con p no divisor de m, y sea $\xi \in \overline{K} = \overline{E} = \overline{F}$ una raíz primitiva m-ésima de $1 \in K$. Si $F = E(\beta_1, \ldots, \beta_t)$ con $\beta_i^{\mu_i} \in E$, para cada $i = 1, \ldots, t$, la extensión $F(\xi) : E(\xi)$ es radical pues $F(\xi) = E(\xi)(\beta_1, \ldots, \beta_t)$ y se aplica (5.56). Por otra parte, la extensión $E(\xi) : K(\xi)$ es de Galois con grupo de $\widetilde{G} = Gal(E(\xi)/K(\xi)$ isomorfo a un subgrupo del grupo $Gal(E/K)$ y por ello resoluble de orden un divisor de $n = [E : K] = \#Gal(E/K)$ (5.41). Resulta de este modo una torre

$$K \subset K(\xi) \subset E(\xi) \subset F(\xi)$$

de la que el primero y tercer pasos son extensiones radicales ((5.34) y (5.56)) con lo que $i)$ quedará probado si se demuestra que $E(\xi) : K(\xi)$ es radical pues así el cuerpo F resultará contenido en la extensión radical $F(\xi)$ de K. Por la resolubilidad del grupo $Gal(E(\xi)/K(\xi))$ existe una torre normal

$$\left\{id_{E(\xi)}\right\} = H_r \subset H_{r-1} \subset \cdots \subset H_1 \subset H_0 = \widetilde{G}$$

en la que cada grupo cociente H_i/H_{i+1} es de orden primo q_i (1.64), divisor de $\#\widetilde{G} = [E(\xi) : K(\xi)]$ que es, a su vez, divisor de n, y así cada q_i divide a n. Sea $F_i = E(\xi)^{H_i}$, para cada $i = 0, 1, \ldots, r-1$, por el Teorema fundamental de teoría de Galois se obtiene una torre de cuerpos

$$K(\xi) = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_r = E(\xi),$$

y como $E(\xi) : E(\xi)^{H_{i+1}}$ y $E(\xi) : E(\xi)^{H_i}$ son extensiones de Galois, siendo H_{i+1} subgrupo normal de H_i, resulta que $F_{i+1} : F_i$ es una extensión de Galois con grupo isomorfo a H_i/H_{i+1}. Nótese que, cada $q_i = \#(H_i/H_{i+1}) \neq p$ es divisor de m al ser divisor de n y primo con p, por la selección que se ha hecho del entero m. Como $\left[E(\xi)^{H_{i+1}} : E(\xi)^{H_i}\right] = q_i \neq p$ es primo y, como ξ es raíz primitiva m-ésima de 1, resulta que $F_i = E(\xi)^{H_i}$ contiene a ξ^{m/q_i} que es una raíz primitiva q_i-ésima de 1. La aplicación de la Proposición 5.51 (o , alternativamente, el Lema 5.40) proporciona la existencia de un $\alpha_i \in F_{i+1}$ tal que $F_{i+1} = F_i(\alpha_i)$ y tal que $\alpha_i^{q_i} \in F_i$. En el caso de un $q_j = \#(H_j/H_{j+1}) = p$ la extensión $F_{j+1} : F_j$ es cíclica de grado p y se aplica el Lema de Artin-Schreier (5.52), con lo cual $F_{j+1} = F_j(\alpha)$ siendo α un cero de un polinomio del tipo $X^p - X - a \in F_j[X]$. Entonces la torre

$$K \subset K(\xi) = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_r = E(\xi)$$

es una torre radical.

$i) \Rightarrow ii)$

Sea $F \subset \overline{K}$ cuerpo de escisión del polinomio f sobre K y sea L una extensión radical de K que contiene a F. Supondremos además que la extensión $L : K$ es normal finita pues en otro caso puede ser sustituida por otra de este tipo tomando la clausura normal de L (contenida en $\overline{K}$) sobre K (5.34). Sean E y M las subextensiones maximales separables de K en F y en L, respectivamente, que son extensiones finitas de Galois de K y además $Gal(F/K) \simeq Gal(E/K)$ y $Gal(L/K) \simeq Gal(M/K)$ (5.54). Obviamente se tiene $E \subset M$. Sea $n = [L : K] = p^r m$ con $p \nmid m$ y $r \geqslant 0$, y sea $\xi \in \overline{K}$ una raíz primitiva m-ésima de $1 \in K$. Si

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$$

es una torre radical con pasos de los tipos especificados en (5.31), la torre obtenida de ésta por ξ-levantamiento

$$K_0(\xi) \subset K_1(\xi) \subset \cdots \subset K_r(\xi)$$

tiene los correspondientes pasos de los mismos tipos que la anterior, pero ahora cada cuerpo contiene raíces primitivas de la unidad suficientes como para poder afirmar, a la luz de (5.51), que todas aquellas extensiones $K_{i+1}(\xi) : K_i(\xi)$, tales que $[K_{i+1} : K_i]$ es primo con p, tienen grupo de Galois cíclico de orden primo con p (isomorfo por (5.41)a un subgrupo del grupo de Galois de la extensión de Galois $K_{i+1} : K_i$ cuyo grado es divisor de n y primo con p). Las extensiones de grado una potencia de p tienen grupos de Galois de orden también potencias de p (5.55) y, por tanto, grupos resolubles (1.48). Resulta así que el grupo $Gal(L(\xi)/K(\xi)) \simeq Gal(M(\xi)/K(\xi))$ es resoluble y entonces lo es también el grupo $Gal(M(\xi)/K)$ pues

$$Gal(K(\xi)/K) \simeq Gal(M(\xi)/K)/Gal(M(\xi)/K(\xi)),$$

ya que $K(\xi) : K$ es normal de grupo de Galois resoluble, en virtud de la selección del entero m (5.22), y se aplica (1.65). Ahora

$$Gal(F/K) \simeq Gal(E/K) \simeq Gal(M(\xi)/K)/Gal(M(\xi)/E),$$

por la misma Proposición (1.65), y por lo tanto $F : E$ es resoluble. □

Conviene hacer un comentario acerca de la forma en que el gran Teorema de Galois en característica p aparece en la literatura. No existe uniformidad en el modo de abordar la noción de extensión radical, aunque en la mayor parte de los manuales se restringe al caso de extensiones separables (por ejemplo [LAN]), e incluso de extensiones algebraicas del cuerpo primo $\mathbb{Z}_p$ (confróntese la noción de extensión radical dada en [DFX] con la de este manual, a la luz de los comentarios de 5.33). La prueba del Teorema estará mediatizada entonces por estas convenciones. Hemos presentado aquí una noción de extensión radical no necesariamente separable - siguiendo una sugerencia de Lang [LAN]- y ello ha permitido acceder a la demostración del gran Teorema de Galois sin grandes complicaciones.

5.5. La ecuación general de grado n

Esta sección ilustra la teoría desarrollada hasta ahora obteniendo, para cada n, una ecuación algebraica de grado n cuyo grupo de Galois (5.38) es el grupo simétrico S_n.

A partir de ahora K es un cuerpo y $\{t_1, \ldots, t_n\}$ es un conjunto trascendente sobre K cuyos elementos supondremos en una extensión F de K. Ello significa, esencialmente, que $K[t_1, \ldots, t_n]$ es el anillo de polinomios en n variables sobre K y que la subextensión $K(t_1, \ldots, t_n)$ de F es el cuerpo de funciones racionales en n variables sobre K (véase ejercicio 26 del capítulo 3).

Cada $\sigma \in S_n$ define una biyección $\sigma\colon \{t_1, \ldots, t_n\} \to \{t_1, \ldots, t_n\}$ y también, por la propiedad universal del anillo de polinomios, un isomorfismo de K-álgebras

$$\begin{aligned} \widetilde{\sigma}\colon K[t_1, \ldots, t_n] &\to K[t_1, \ldots, t_n] \\ f(t_1, \ldots, t_n) &\mapsto f\left(t_{\sigma(1)}, \ldots, t_{\sigma(n)}\right), \end{aligned}$$

cuyo inverso es $\widetilde{\sigma^{-1}}$, definido de similar modo a partir de $\sigma^{-1} \in S_n$. Nótese que la existencia de $\widetilde{\sigma}$ solamente está garantizada si $\{t_1, \ldots, t_n\}$ es un conjunto trascendente sobre K, es decir, si $K[t_1, \ldots, t_n]$ es un anillo de polinomios. El isomorfismo $\widetilde{\sigma}$ se extiende a un automorfismo de $K(t_1, \ldots, t_n)$ sobre K que seguiremos denotando con $\widetilde{\sigma}$.

Definición 5.58. Un elemento $s \in K[t_1, \ldots, t_n]$ se dirá que es un polinomio simétrico (en las variables $t_1, \ldots, t_n$) si para cada permutación $\sigma \in S_n$ se tiene

$$s(t_1, \ldots, t_n) = s(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).$$

Los polinomios homogéneos (2.34)

$$s_1 = t_1 + \cdots + t_n, \ \ldots \ , s_r = \sum_{1 \le i_1 < \cdots < i_r \le n} t_{i_1} \cdots t_{i_r}, \ \ldots \ , s_n = t_1 \cdots t_n$$

reciben el nombre de polinomios simétricos elementales.

Definición 5.59. El polinomio

$$\begin{aligned} F_n &= (X - t_1)(X - t_2) \cdots (X - t_n) \\ &= X^n - s_1 X^{n-1} + \cdots + (-1)^r s_r X^{n-r} + \cdots + (-1)^n s_n \in K(t_1, \ldots, t_n)[X] \end{aligned}$$

tiene sus coeficientes en el subcuerpo $K(s_1, \ldots, s_n)$, y la ecuación

$$F_n(X) = 0$$

recibe el nombre de ecuación algebraica general de grado n (sobre K).

Obsérvese que si se sustituye $t_n = 0$ en la expresión para F_n dada en (5.59) resulta

$$\begin{aligned} (F_n)_0 &= (X - t_1)(X - t_2) \cdots (X - t_{n-1})X \\ &= X^n - (s_1)_0 X^{n-1} + \cdots + (-1)^r (s_r)_0 X^{n-r} + \cdots + (-1)^{n-1} (s_{n-1})_0 X, \end{aligned}$$

(aquí, con $(s_i)_0$ se indica el resultado de sustituir $t_n = 0$ en la expresión de s_i). Los $(s_i)_0$ son precisamente los polinomios simétricos elementales en las variables $t_1, \ldots, t_{n-1}$, y además $(F_n)_0 = XF_{n-1}$.

Observación 5.60. Nótese también que si $\alpha_1, \ldots, \alpha_n \in \overline{K}$, el homomorfismo evaluación $\varphi\colon K[t_1, t_2, \ldots, t_n] \to \overline{K}$, definido por $\varphi(t_i) = \alpha_i$ $(i = 1, \ldots, n)$, induce el homomorfismo de K-álgebras $\varphi[X] : K[t_1, \ldots, t_n][X] \to \overline{K}[X]$ definido por

$$\varphi[X][a_r(t_1, \ldots, t_n)X^r + \cdots + a_0(t_1, \ldots, t_n)] = a_r(\alpha_1, \ldots, \alpha_n)X^r + \cdots + a_0(\alpha_1, \ldots, \alpha_n).$$

En particular, si $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X] \subset \overline{K}[X]$ y $\alpha_1, \ldots, \alpha_n \in \overline{K}$ son los ceros de f, entonces

$$\varphi[X](F_n) = f.$$

Cualquier polinomio mónico f de grado n es una especialización del polinomio general F_n.

Si $\sigma \in S_n$ y $\widetilde{\sigma}$ es el automorfismo de $K(t_1, \ldots, t_n)$ sobre K definido antes, sabemos que $\widetilde{\sigma}$ induce un isomorfismo

$$\overline{\widetilde{\sigma}}\colon K(t_1, \ldots, t_n)[X] \to K(t_1, \ldots, t_n)[X]$$

mediante

$$\overline{\widetilde{\sigma}}(\sum_i r_i X^i) = \sum_i \widetilde{\sigma}(r_i)X^i,$$

en donde las r_i denotan funciones racionales en las trascendentes $t_1, \ldots, t_n$.

El polinomio $F_n = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$ es tal que $\overline{\widetilde{\sigma}}(F_n) = F_n$, ya que $F_n = (X - t_1)\cdots(X - t_n)$ y la aplicación $\overline{\widetilde{\sigma}}$ consiste solamente en la alteración del orden de los factores. Por tanto, los coeficientes de F_n no se modifican con la aplicación de $\overline{\widetilde{\sigma}}$, cualquiera que sea $\sigma \in S_n$, es decir, son simétricos.

Como $K(t_1, \ldots, t_n) = K(s_1, \ldots, s_n)(t_1, \ldots, t_n)$, resulta que $K(t_1, \ldots, t_n)$ es el cuerpo de escisión de $F_n(X)$ sobre $K(s_1, \ldots, s_n)$, es decir, que es normal la extensión $K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)$. Tenemos así

$$Gal_{K(s_1,\ldots,s_n)}(F_n) = Gal(K(t_1, \ldots, t_n)/K(s_1, \ldots, s_n)).$$

Además, se tiene un homomorfismo de grupos

$$S_n \to Gal(K\,(t_1,\ldots,t_n)\,/K(s_1,\ldots,s_n))$$
$$\sigma \mapsto \widetilde{\sigma}$$

que la siguiente Proposición permitirá probar que es un isomorfismo.

Para la demostración de dicha Proposición utilizaremos la noción de *peso* de un polinomio.

Definición 5.61. Se define el peso del monomio

$$M(X_1, X_2, \ldots, X_n) = X_1^{\nu_1} X_2^{\nu_2} \cdots X_n^{\nu_n}$$

como el entero

$$w(M) := \nu_1 + 2\nu_2 + \cdots + n\nu_n.$$

Para un polinomio $f = \sum_{(\upsilon)} a_{(\upsilon)} M_{(\upsilon)}(X_1, X_2, \ldots, X_n) \in K\,[X_1, \ldots, X_n]$ el peso $w(f)$ queda definido como el máximo de los pesos de sus monomios, es decir,

$$w(f) = \max_{a_{(\upsilon)} \neq 0} w(M_{(\upsilon)}).$$

Proposición 5.62. *Si A es un anillo conmutativo y $f\,(t_1,\ldots,t_n) \in A\,[t_1,\ldots,t_n]$ es simétrico de grado d, entonces existe un polinomio $g\,(X_1,\ldots,X_n) \in A\,[X_1,\ldots,X_n]$ de peso $\leqslant d$ tal que $f\,(t_1,\ldots,t_n) = g(s_1,\ldots,s_n)$.*

En particular, si $f\,(t_1,\ldots,t_n) \in A\,[t_1,\ldots,t_n]$ es un polinomio simétrico, entonces $f\,(t_1,\ldots,t_n) \in A\,[s_1,\ldots,s_n]$, es decir, $A\,[s_1,\ldots,s_n]$ es el anillo de los polinomios simétricos con coeficientes en A.

Demostración. La prueba será por inducción en n. La tesis es obvia en el caso $n = 1$. Supondremos el resultado cierto para polinomios en $n-1$ variables y para polinomios en n variables procederemos a razonar por inducción en el grado d.

Es evidente que el enunciado es válido (en cualquier número de variables) si $d = 0$. Sea $d > 0$ y supongamos entonces que el resultado es cierto para polinomios en n variables de grado menor que d. Tomemos $f\,(t_1,\ldots,t_n)$ simétrico de grado $d > 0$, para el cual se tiene necesariamente que $\partial f\,(t_1,\ldots,t_{n-1},0) < \partial f\,(t_1,\ldots,t_n) = d$, en virtud

de la simetría de f, y entonces, por hipótesis de inducción en n, existe un polinomio $g_1(X_1,\ldots,X_{n-1})$ con peso $w(g_1(X_1,\ldots,X_{n-1}))\leqslant \partial f(t_1,t_2,\ldots,t_{n-1},0)<d$ tal que

$$f(t_1,\ldots,t_{n-1},0)=g_1((s_1)_0,\ldots,(s_{n-1})_0).$$

Como $w(g_1(X_1,\ldots,X_{n-1}))=\partial g_1((s_1)_0,\ldots,(s_{n-1})_0)<d$, el polinomio simétrico

$$f_1(t_1,\ldots,t_n):=f(t_1,\ldots,t_n)-g_1((s_1)_0,\ldots,(s_{n-1})_0)$$

tiene grado d (en las $t_1,\ldots,t_n$). Además

$$f_1(t_1,\ldots,t_{n-1},0)=f(t_1,\ldots,t_{n-1},0)-g_1((s_1)_0,\ldots,(s_{n-1})_0)=0,$$

es decir, t_n es divisor de $f_1(t_1,\ldots,t_n)$ en $A[t_1,\ldots,t_n]$, y por la simetría de f_1, deberá ser cada s_i divisor de f_1 (en la expresión $f=\sum_{(\nu)}a_{(\nu)}t_1^{\nu_1}\cdots t_n^{\nu_n}$ se tiene $\nu_i>1$, para todo i, en cada monomio). Resulta entonces que

$$f_1(t_1,\ldots,t_n)=s_nf_2(t_1,\ldots,t_n),$$

para un cierto $f_2(t_1,\ldots,t_n)\in A[t_1,\ldots,t_n]$, necesariamente simétrico, cuyo grado es $d-n<d$. Por lo tanto, $f_2(t_1,\ldots,t_n)=g_2(s_1,\ldots,s_n)$ para un cierto $g_2(X_1,\ldots,X_n)$ de peso $\leqslant \partial f_2<d$, en virtud de la hipótesis de inducción en d. Se tienen así las igualdades

$$\begin{aligned}f(t_1,\ldots,t_n)&=f_1(t_1,\ldots,t_n)+g_1(s_1,\ldots,s_{n-1})\\&=g_1(s_1,\ldots,s_{n-1})+s_nf_2(t_1,\ldots,t_n)\\&=g_1(s_1,\ldots,s_{n-1})+s_ng_2(s_1,\ldots,s_n),\end{aligned}$$

la última de las cuales culmina la demostración pues el polinomio

$$g(X_1,\ldots,X_n):=g_1(X_1,\ldots,X_{n-1})+X_ng_2(X_1,\ldots,X_n)$$

tiene peso $\leqslant d$.

Nótese que el polinomio g tiene ahora peso d ya que dicho peso es el grado de f en el conjunto de trascendentes $\{t_1,\ldots,t_n\}$. □

Observación 5.63. Nótese que un polinomio simétrico en n variables $f(t_1,\ldots,t_n) \in A[s_1,\ldots,s_n]$ se puede interpretar como un polinomio simétrico en r variables si $r \geqslant n$, teniendo en cuenta que $A[s_1,\ldots,s_n] \subset A[s_1,\ldots,s_r]$ (el j-ésimo polinomio simétrico elemental en n variables $s_j(t_1,\ldots,t_n)$ se puede considerar como un polinomio simétrico en r variables en el cual no intervienen $t_{n+1},\ldots,t_r$). Además, el homomorfismo canónico

$$\varphi\colon A[t_1,\ldots,t_r] \to A[t_1,\ldots,t_n]$$

definido por

$$\varphi|_A = id_A,\ \varphi(t_i) = t_i \text{ si } i = 1,\ldots,n,\ \text{y } \varphi(t_k) = 0,\ \text{si } k = n+1,\ldots,r,$$

es tal que $\varphi(A[s_1,\ldots,s_r]) = A[s_1,\ldots,s_n]$ y además $\varphi|_{A[s_1,\ldots,s_n]} = id_{A[s_1,\ldots,s_n]}$.

El j-ésimo polinomio simétrico elemental $s_j(t_1,\ldots,t_n)$ en las n variables $t_1,\ldots,t_n$ se puede obtener a partir del j-ésimo polinomio simétrico elemental $s_j(t_1,\ldots,t_r)$ mediante la sustitución $s_j(t_1,\ldots,t_n) = s_j(t_1,\ldots,t_n,0,\ldots,0) = \varphi[s_j(t_1,\ldots,t_r)]$.

Corolario 5.64. *Con las mismas notaciones que hasta ahora se tiene*

$$Gal(K(t_1,\ldots,t_n)/K(s_1,\ldots,s_n)) \simeq S_n.$$

Demostración. Si τ es un automorfismo de $K(t_1,\ldots,t_n)$ que deja fijos los elementos de $K(s_1,\ldots,s_n)$, τ deja fijos los polinomios simétricos elementales y entonces

$$\begin{aligned} F_n^\tau :=& X^n - \tau(s_1)X^{n-1} + \cdots + (-1)^n\tau(s_n) \\ =& (X-\tau(t_1))\cdots(X-\tau(t_n)) \\ =& X^n - s_1X^{n-1} + \cdots + (-1)^n s_n \\ =& (X-t_1)(X-t_2)\cdots(X-t_n) = F_n. \end{aligned}$$

De la factorización única en $K(t_1,\ldots,t_n)[X]$ se obtiene que τ determina, necesariamente, una permutación del conjunto $\{t_1,\ldots,t_n\}$. Es muy fácil probar que la aplicación resultante

$$\begin{aligned} Gal(K(t_1,\ldots,t_n)/K(s_1,\ldots,s_n)) &\to S_n \\ \tau &\mapsto \widehat{\tau} \end{aligned}$$

definida por $\widehat{\tau}(i) = j :\Leftrightarrow \tau(t_i) = t_j$, es inversa del homomorfismo

$$\begin{aligned} S_n &\to Gal(K\left(t_1, \ldots, t_n\right)/K(s_1, \ldots, s_n)) \\ \sigma &\mapsto \widetilde{\sigma} \end{aligned}$$

definido más arriba. □

Como consecuencia de todo lo anterior resulta,

Teorema 5.65. *La ecuación general de grado n sobre un cuerpo K es resoluble por radicales si, y solo si,* $n \leqslant 4$.

Demostración. Sea P el cuerpo primo de K.

El polinomio $F_n = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$ tiene coeficientes en $P(s_1, \ldots, s_n)$. La resolubilidad por radicales aquí debe ser entendida sobre $P(s_1, \ldots, s_n)$ según lo establecido en 5.36. El Teorema 5.57 y el Corolario anterior proporcionan el resultado. □

Definición 5.66. Siendo $t_1, \ldots, t_n$ como antes, se pone

$$\delta_n = \prod_{1 \leqslant i < j \leqslant n} (t_i - t_j)$$

y se define el discriminante de F_n como

$$D_n = (\delta_n)^2 .$$

El discriminante de un polinomio $f \in K[X]$ de grado n se obtiene como

$$D(f) = \varphi[X](D_n),$$

con $\varphi[X]$ definido en (5.60).

De la propia definición y de (1.57) es muy fácil obtener que si

$$\widetilde{\sigma} \in Gal(K\left(t_1, t_2, \ldots, t_n\right)/K(s_1, s_2, \ldots, s_n)) \simeq S_n,$$

entonces $\widetilde{\sigma}(\delta_n) = \varepsilon(\sigma)\,\delta_n$, siendo $\sigma \in S_n$ la permutación de subíndices correspondiente a $\widetilde{\sigma}$ en la prueba del isomorfismo que se establece en (5.64). Por lo tanto, es evidente

que $\widetilde{\sigma}(D_n) = D_n$ para todo $\widetilde{\sigma} \in Gal(K(t_1,\ldots,t_n)/K(s_1,\ldots,s_n))$, con lo que resulta que $D_n \in K(s_1,\ldots,s_n)$ y es un polinomio simétrico en $t_1,\ldots,t_n$.

Por ejemplo, para $n = 2$,

$D_2 = (t_1 - t_2)^2 = t_1^2 + t_2^2 - 2t_1t_2 = (t_1 + t_2)^2 - 4t_1t_2 = s_1^2 - 4s_2$, y para el polinomio $f = X^2 + bX + c$, se tiene $D(f) = b^2 - 4c$.

Para $n = 3$, $D_3 = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$, y para el polinomio $f = X^3 - a_1X^2 + a_2X - a_3$ se tiene $D(f) = -4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2$.

Mediante el cambio (Tschirnhausen) de variable $X \mapsto X + \dfrac{a_1}{3}$ (se supone que la característica de K es diferente de 3) el anterior polinomio cúbico se transforma en $f = X^3 + pX + q$, con lo que el discriminante adopta la forma $D(f) = -4p^3 - 27q^2$.

Para $n = 4$, suponiendo que K no es de característica 2, el polinomio, de grado 4, $f = X^4 - a_1X^3 + a_2X^2 - a_3X + a_4$ se transforma en $f = X^4 + pX^2 + qX + r$ mediante el cambio (Tschirnhausen) $X \mapsto X + \dfrac{a_1}{4}$, y se puede probar que $D(f) = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$.

LAS ECUACIONES DE GRADOS 3 Y 4

Utilizando la teoría de Galois daremos ahora las indicaciones necesarias para la obtención de los métodos clásicos de resolución de la cúbica y la cuártica sobre un cuerpo K que supondremos de característica diferente de 2 y de 3. La resolución de las correspondientes ecuaciones generales de grados 3 y 4 proporcionará las de cualquier cúbica o cuártica por conveniente especialización (5.60).

LA CÚBICA

Supondremos que K contiene las raíces cúbicas de la unidad. Esta última suposición no constituye ninguna restricción pues en otro caso se procederá sustituyendo K por $K(\xi)$, siendo ξ una raíz primitiva cúbica de 1.

La ecuación general de grado 3 es $F_3 = X^3 - s_1X^2 + s_2X - s_3$. Para abreviar pondremos $F = K(s_1, s_2, s_3)$ y $L = K(t_1, t_2, t_3)$. La extensión $L : F$ es de Galois y su grupo será identificado con S_3 (5.64). Sabemos que $D = D_3 = (\delta_3)^2 \in F$, y que $\delta = \delta_3 \notin F$ (el polinomio $\delta_3(t_1, t_2, t_3)$ no es simétrico), con lo cual se tiene $[F(\delta) : F] = 2$, y así $L : F(\delta)$ es una extensión de Galois cíclica de grado 3. Por el Teorema fundamental de teoría de Galois (5.12) la torre de cuerpos

$$F \subset F(\delta) \subset L$$

proporciona la de grupos

$$G = Gal(L/K) = S_3 \supset A_3 \supset \{1\},$$

ya que $\delta \in L^{A_3}$ y $Gal(L/F(\delta)) = A_3$ es el único subgrupo de orden 3 de S_3. Obsérvese que $t_1, t_2, t_3 \notin F(\delta) = L^{A_3}$, y que -en virtud de la hipótesis sobre la característica-. se puede aplicar ahora el Lema 5.40 a la extensión $L : F(\delta)$. En la prueba de dicho

Lema se supone dado un generador β de la extensión, y ahora se puede tomar $\beta = t_i$ para cualquier $i = 1, 2, 3$, ya que, por el Teorema del grado se tiene $[L : F(\delta)(t_i)] = 1$. Entonces, poniendo $\beta = t_1$ las transformadas de Lagrange adoptan la forma

$$\alpha_i = t_1 + \xi^i \sigma(t_1) + \xi^{2i} \sigma^2(t_1),$$

con $i = 0, 1, 2$ (5.40), donde $\langle \sigma \rangle = A_3$. Poniendo ahora $\sigma = (123)$ resulta definitivamente

$$\begin{array}{l} \alpha_0 = t_1 + t_2 + t_3 = s_1 \\ \alpha_1 = t_1 + \xi t_2 + \xi^2 t_3 \quad (*) \\ \alpha_2 = t_1 + \xi^2 t_2 + \xi t_3. \end{array}$$

La trascendencia de $\{t_1, t_2, t_3\}$ sobre K proporciona que $\alpha_0, \alpha_1, \alpha_2 \notin F(\delta) = L^{A_3}$ (por ejemplo, de $\sigma(\alpha_1) = \alpha_1$ se obtendría $(1 + \xi)t_1 + t_2 + \xi t_3 = 0$). Resulta entonces $L = F(\delta)(\alpha_1)$ y $(\alpha_1)^3 \in F(\delta)$. Así

$$(\alpha_1)^3 = R + Q\delta$$

para ciertos $R, Q \in F = K(s_1, s_2, s_3)$ -cuyo cálculo es tedioso y no se realizará aquí- de lo que resulta

$$\alpha_1 = \sqrt[3]{R + Q\delta}.$$

Poniendo $\tau = (23) \in S_3$ se tiene $\alpha_2 = \tau(\alpha_1)$, por lo que

$$(\alpha_2)^3 = R - Q\delta,$$

y así,

$$\alpha_2 = \sqrt[3]{R - Q\delta},$$

ya que R , $Q \in F = L^{S_3}$, $\tau(\delta) = -\delta$.

Para la obtención de las expresiones radicales de las t_1, t_2, t_3 comenzaremos sumando miembro a miembro las ecuaciones $(*)$, con lo que resulta

$$3t_1 + (1 + \xi + \xi^2)t_2 + (1 + \xi + \xi^2)t_3 = 3t_1 = \alpha_0 + \alpha_1 + \alpha_2,$$

ya que $\xi \neq 1$ y es un cero de $X^3 - 1 = (X - 1)(X^2 + X + 1)$. De forma análoga, a partir de

$$\begin{array}{r} \alpha_0 = t_1 + t_2 + t_3 \\ \xi\alpha_1 = \xi t_1 + \xi^2 t_2 + t_3 \\ \xi^2\alpha_2 = \xi^2 t_1 + t_3 + \xi t_2 \end{array}$$

se obtiene $3t_3 = \alpha_0 + \xi\alpha_1 + \xi^2\alpha_2$, y a partir de

$$\begin{array}{r} \alpha_0 = t_1 + t_2 + t_3 \\ \xi^2\alpha_1 = \xi^2 t_1 + t_2 + \xi t_3 \\ \xi\alpha_2 = \xi t_1 + \xi^2 t_3 + t_2 \end{array}$$

resulta $3t_2 = \alpha_0 + \xi^2\alpha_1 + \xi\alpha_2$. Por lo tanto,

$$\begin{aligned} t_1 &= \frac{1}{3}(\alpha_0 + \alpha_1 + \alpha_2) \\ t_2 &= \frac{1}{3}\left(\alpha_0 + \xi^2\alpha_1 + \xi\alpha_2\right) \\ t_3 &= \frac{1}{3}\left(\alpha_0 + \xi\alpha_1 + \xi^2\alpha_2\right) \end{aligned}$$

son las expresiones buscadas para las raíces de F_3 que culminan la resolución por radicales de la ecuación cúbica general pues los elementos $\alpha_0, \alpha_1, \alpha_2$ son expresiones radicales de los coeficientes del polinomio F_3.

LA CUÁRTICA

Dada la cuártica general $F_4 = \prod_1^4 (X - t_i) = X_4 - s_1X^3 + s_2X^2 - s_3X + s_4 = 0$ con coeficientes en K, se trata de obtener t_1, t_2, t_3 y t_4 como expresiones radicales de los coeficientes s_1, s_2, s_3 y s_4. Como antes, denotaremos con $L = K(t_1, t_2, t_3, t_4)$ el cuerpo de escisión de F_4 sobre $F = K(s_1, s_2, s_3, s_4)$. Por (5.64), el grupo de Galois de F_4 sobre F es $G = Gal_F(F_4) = Gal(L/F) = S_4$. Recuérdese que la resolubilidad de G se obtiene en la prueba de (1.69) mediante la construcción de la torre

$$\{1\} \subset W \subset V \subset A_4 \subset G = S_4,$$

en la cual $V = \{id_F, (12)(34), (13)(24), (14)(23)\}$ es el grupo de Klein (véase el ejercicio. 6 del capítulo 1) considerado como subgrupo normal de A_4, y $W = \langle(12)(34)\rangle$ es subgrupo normal de V pero no de A_4. Por el Teorema fundamental de teoría de Galois (5.12) se obtiene la cadena de extensiones

$$L \supset L^W \supset L^V \supset L^{A_4} = F(\delta) \supset F$$

cuyos grados se determinan a continuación.

$$\begin{aligned} \left[L : L^W\right] &= \#W = |(13)(24)| = 2, \\ \left[L^W : L^V\right] &= (V : W) = 2, \\ \left[L^V : L^{A_4}\right] &= (A_4 : V) = 3 \text{ (véase prueba de (1.69))}, \\ \left[L^{A_4} : F\right] &= (S_4 : A_4) = 2. \end{aligned}$$

La extensión $L^V : L^{A_4}$ es cíclica de grado 3, y admite como elemento primitivo cualquier $\alpha \in L^V \backslash L^{A_4}$. El elemento $\alpha = (t_1+t_2)(t_3+t_4)$ es tal que $(123)(\alpha) = (t_2+t_3)(t_1+t_4) \neq \alpha$, y α queda fijo por cualquier elemento de V, aAsí se tiene $L^V = L^{A_4}(\alpha) = F(\delta, \alpha)$. Ahora, como $\left[L^V : L^{A_4}\right] = 3$ el polinomio $Irr(\alpha, L^{A_4}) = X^3 - a_1X^3 + a_2X^2 - a_3X + a_4 \in L^{A_4}[X]$ tiene por ceros todos los conjugados de α por la acción del grupo $Gal(L^V/L^{A_4}) = A_4/V$ que es cíclico de orden 3 generado por $\overline{\sigma} = \sigma V$, la clase módulo V de cualquier permutación par $\sigma \in S_4$ que no sea elemento de V. El elemento $\sigma = (123)$ satisface las condiciones y de ello resultan las igualdades

$$\begin{aligned} Irr(\alpha, L^{A_4}) &= X^3 - a_1X^3 + a_2X^2 - a_3X + a_4 = (X - \alpha)(X - \sigma(\alpha))(X - \sigma^2(\alpha)) \\ &= (X - ((t_1 + t_2)(t_3 + t_4))\,(X - ((t_2 + t_3)(t_1 + t_4))\,(X - ((t_3 + t_1)(t_2 + t_4)) \end{aligned}$$

que, tras un cálculo laborioso y las correspondientes identificaciones, nos permiten obtener las a_i como el valor en $\alpha, \beta = \sigma(\alpha)$ y $\gamma = \sigma^2(\alpha) = (t_3 + t_1)(t_2 + t_4)$ de los polinomios simétricos elementales de tres variables. Por lo tanto, α, β y γ se obtienen como expresiones radicales de las $a_1, a_2, a_3, a_4 \in F(\delta)$ resolviendo la cúbica $X^3 - a_1X^3 + a_2X^2 - a_3X + a_4 = 0$.

El elemento $\zeta = t_1 + t_2$ es un generador de la extensión cuadrática $L^W : L^V$ ya que $\zeta \in L^W$ pero $((13)(24))(\zeta) \neq \zeta$. Ahora, de

$$\begin{aligned} t_1 + t_2 + t_3 + t_4 &= s_1 \\ (t_1 + t_2)(t_3 + t_4) &= \alpha \end{aligned}$$

resulta $t_1 + t_2 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\alpha}}{2}$, y entonces $t_3 + t_4 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\alpha}}{2}$, donde la elección de un signo en la raíz para el valor de $t_1 + t_2$ condiciona la selección del signo contrario para la raíz que expresa el valor de $t_3 + t_4$.

De forma análoga, de

$$\begin{aligned} t_1 + t_2 + t_3 + t_4 &= s_1 \\ (t_2 + t_3)(t_1 + t_4) &= \beta \end{aligned}$$

proporciona $t_1 + t_4 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\beta}}{2}$, y entonces $t_2 + t_3 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\beta}}{2}$, con las mismas consideraciones acerca del signo de las raíces.

Y también, de

$$\begin{aligned} t_1 + t_2 + t_3 + t_4 &= s_1 \\ (t_1 + t_3)(t_2 + t_4) &= \gamma \end{aligned}$$

se obtiene $t_1 + t_3 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\gamma}}{2}$, y entonces $t_2 + t_4 = \dfrac{s_1 \pm \sqrt{s_1^2 - 4\gamma}}{2}$, con consideraciones análogas respecto de los signos de los radicales.

En cualquier caso, una vez seleccionados los valores de dos de los elementos $t_1 + t_2$, $t_1 + t_4$ y $t_1 + t_3$ la selección del tercero está condicionada por el hecho de que $\alpha\beta\gamma = a_4$ y las expresiones radicales de las t_1, t_2, t_3 y t_4 se obtienen ahora de lo anterior. Así, por ejemplo, seleccionando signo $+$ para el radical de las expresiones correspondientes a $t_1 + t_2$ y $t_1 + t_3$ se obtiene

$$t_1 = \frac{1}{4}\Big(s_1 + \sqrt{s_1^2 - 4\alpha} + \sqrt{s_1^2 - 4\gamma} \pm \sqrt{s_1^2 - 4\beta}\Big),$$

en donde, la correspondiente imprecisión de signo en el último radical está sujeta a las restricciones antes mencionadas.

5.6. Ejercicios

1.- Sea $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Calcular el grupo de Galois de la extensión $E : \mathbb{Q}$ y todos los cuerpos intermedios entre $\mathbb{Q}$ y E.

2.- Descríbase el grupo de Galois sobre $\mathbb{Q}$ de cada uno de los siguientes polinomios:
a) $X^4 + 4$.
b) $X^4 - 3X^2 - 28$.
c) $X^3 - 2$.

3.- Si E es cuerpo de escisión sobre $\mathbb{Q}$ del polinomio $X^4 + 1$ demuéstrese que $Gal(E/\mathbb{Q})$ tiene orden 4. Justifíquese, utilizando la correspondencia de Galois, que $Gal(E/\mathbb{Q})$ no es un grupo cíclico.

4.- Sea E un cuerpo de escisión de $f = X^5 - 1$ sobre $\mathbb{Q}$.
a) Demuéstrese que $Gal(E/\mathbb{Q})$ es un grupo cíclico de orden 4.
b) Calcúlense los cuerpos intermedios entre $\mathbb{Q}$ y E.
c) Si $\xi = e^{\frac{2\pi i}{5}}$, calcular $Irr(\xi^2 + \xi^3, \mathbb{Q})$ e $Irr(\xi, \mathbb{Q}(\xi^2 + \xi^3))$.

5.- Sea E cuerpo de escisión de $X^4 - 2$ sobre $\mathbb{Q}$.
a) Pruébese que $G = Gal(E/Q)$ es isomorfo a $D_{2,4}$.
b) Calcúlense los subgrupos de G de orden 4 y sus cuerpos fijos.

6.- Sea ξ una raíz primitiva séptima de la unidad. Pruébese que:
a) El grado de $\mathbb{Q}(\xi) : \mathbb{Q}$ es 6.
b) $Gal(\mathbb{Q}(\xi)/\mathbb{Q}) = \langle\sigma\rangle$, siendo σ el $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\xi)$ dado por $\sigma(\xi) = \xi^3$.
c) $Irr(1 + 2(\xi + \xi^2 + \xi^4), \mathbb{Q}) = X^2 + 7$.

7.- Justifíquese la veracidad o la falsedad de la siguiente afirmación:
Si E es el cuerpo de escisión de $X^4 - 2$ sobre $\mathbb{Q}$ en $\mathbb{C}$, para demostrar que el grado del polinomio irreducible de $i + \sqrt[4]{2}$ sobre $\mathbb{Q}$ es igual al grado de E sobre $\mathbb{Q}$ basta con probar que existen al menos 5 elementos distintos en la órbita de $i + \sqrt[4]{2}$ mediante la acción del grupo $Gal(E : \mathbb{Q})$.

8.- a) Sea $f = X^4 + X^2 - 6 \in \mathbb{Q}[X]$. ¿Es f irreducible sobre $\mathbb{Q}$? Determínese su cuerpo de escisión E_f sobre $\mathbb{Q}$ calculando, si es posible, un elemento primitivo de $E_f : \mathbb{Q}$. Hallar $Gal(E_f/\mathbb{Q})$ y sus subgrupos. ¿Existe algún cuerpo intermedio F tal que $F : \mathbb{Q}$ sea una extensión normal?
b) Pruébese que si g es un polinomio irreducible sobre un cuerpo K y tiene un cero en una extensión radical de K, entonces g es resoluble por radicales.

9.- Sean $f = X^5 - 2 \in \mathbb{Q}[X]$ y $G = Gal_{\mathbb{Q}}(f)$.
a) Calcúlese el orden de G.
b) Demuéstrese que G tiene un subgrupo normal de orden 5.
c) Pruébese que G es resoluble.
d) Demuéstrese que G no es abeliano.
e) Pruébese que G es isomorfo a un subgrupo de S_5 que no contiene trasposiciones.

10.- Sea $E = \mathbb{Q}(\sqrt{2}, \sqrt[7]{5}, i)$.
a) Calcúlese $[E : \mathbb{Q}]$ y pruébese que $E : \mathbb{Q}$ no es normal.
b) Demuéstrese que $E : \mathbb{Q}(\sqrt[7]{5})$ es normal y determínese una $\mathbb{Q}\left(\sqrt[7]{5}\right)$-base de E.
c) Pruébese que $Gal(E/\mathbb{Q}(\sqrt[7]{5})) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
d) ¿Es $-\sqrt{2} + 5i$ un cero de $Irr(\sqrt{2} + 5i), \mathbb{Q}(\sqrt[7]{5}))$?

11.- Justifíquese la veracidad o la falsedad de las siguientes afirmaciones:
a) $X^4 + 1 \in \mathbb{Q}[X]$ es un polinomio ciclotómico.
b) $X^3 + aX^2 + bX + 2 \in \mathbb{Q}[X]$ no tiene ceros en $\mathbb{R}$.
c) El grupo de Galois de la extensión $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i) : \mathbb{Q}$ es un grupo cíclico.

12.- Sea ξ una raíz primitiva novena de la unidad.
a) Justifíquense las relaciones de inclusión existentes entre los siguientes cuerpos: $\mathbb{Q}(\xi)$, $\mathbb{Q}(\xi^3)$ y $\mathbb{Q}(\xi^6)$.
b) Calcúlese $Irr(\xi^2, \mathbb{Q}\left(\xi^6\right))$.

13.- Sea p un número primo. Demuéstrese que si r es un número natural entonces $\Phi_{p^r} = \Phi_p(X^{Pr-1})$.

14.- Sea K un cuerpo, $n \geqslant 1$ un entero impar y $\xi \in K$ una raíz primitiva n-ésima de 1. Demuéstrese que K contiene también una raíz primitiva $2n$-ésima de 1.

15.- Para $r \in \mathbb{N}$ denotamos con U_r el grupo de las raíces n-ésimas de $1 \in \mathbb{Q}$. Demuéstrese que si n y m son enteros positivos primos entre si, entonces se tiene que $U_n \cap U_m = \{1\}$ y que $U_{nm} = U_n U_m \equiv U_n \times U_m$.

16.- Para $r \in \mathbb{N}$ denotamos con ξ_r una raíz primitiva r-ésima de $1 \in \mathbb{Q}$. Demuéstrese que si n y m son enteros positivos primos entre si, entonces se tiene que $\mathbb{Q}\left(\xi_n\right)\mathbb{Q}\left(\xi_m\right) = \mathbb{Q}\left(\xi_{nm}\right)$ y que $\mathbb{Q}\left(\xi_n\right) \cap \mathbb{Q}\left(\xi_m\right) = \mathbb{Q}$.

Capítulo 6

Complementos

6.1. Constructibilidad de polígonos regulares. Teorema de Gauss-Wantzel

La finalidad de este apéndice es dar noticia de una interesante aplicación de la teoría de Galois a la Geometría Euclídea plana, completando algún aspecto del contenido de la sección 3.3 que se ha dedicado al estudio de los problemas geométricos clásicos. En concreto se trata ahora de caracterizar aquellos polígonos regulares que son constructibles con regla y compás.

Definición 6.1. Si m es un número natural y $p = 2^m + 1$ es un número primo se dirá que p es un *primo de Fermat*.

Proposición 6.2. *Los primos de Fermat son todos de la forma* $p = 2^{2^n} + 1$.

Demostración. Bastará con demostrar que si $p = 2^m + 1$ $(m > 1)$ es un número primo entonces m solamente admite a 2 como divisor primo. Supóngase que m admite algún divisor impar q. Entonces, de $m = qr$ resulta:

a) X^q+1 admite a -1 como raíz al ser q impar, lo cual implica que $X^q+1 = (X+1)g$, donde $g \in \mathbb{Z}[X]$.

b) Como consecuencia de *a*) se tiene que $p = 2^m + 1 = (2^r)^q + 1 = (2^r + 1)g(2^r)$ y, por ser p número primo, resulta $2^r + 1 = 2^{rq} + 1$. Entonces debe ser $rq = r$, es decir, $q = 1$.

Resumiendo, 1 es el único divisor impar de m y $m = 2^n$ para algún entero n. □

Los primos de Fermat han sido bautizados así por Mersenn. Fermat había conjeturado que todos los números de la forma $2^{2^n} + 1$ eran primos, pero Euler probó que $2^{2^5} + 1 = 4294967297$ no lo es. Son primos de Fermat los números $3 = 2^{2^0} + 1$, $5 = 2^{2^1} + 1$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$ y $65357 = 2^{2^4} + 1$, y no se conoce ninguno más. Actualmente se sabe que $2^{2^n} + 1$ no es primo si $5 \leqslant n \leqslant 16$.

Observación 6.3.

1) El polígono regular de n lados (o n-ágono regular) es constructible si, y solamente si, $\cos \dfrac{2\pi}{n}$ es un número real constructible.

2) Si $\xi = \cos \dfrac{2\pi}{n} + isen\dfrac{2\pi}{n} = e^{\frac{2\pi i}{n}}$, entonces $\cos \dfrac{2\pi}{n} = \dfrac{1}{2}\left(\xi + \overline{\xi}\right) \in \mathbb{Q}(\xi)$, ya que $\overline{\xi} = \xi^{-1}$ (al ser $|\xi| = 1$). Se tiene así a torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}\Big(\cos \dfrac{2\pi}{n}\Big) \subset \mathbb{Q}(\xi)$.

3) Recuérdese que, según establece el Teorema fundamental sobre constructibilidad 3.28, un número real α es constructible si, y solo si, existe una torre

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_r \subset \mathbb{R}$$

tal que $[F_i : F_{i-1}] \leqslant 2$, para $i = 1, \ldots, r$, y tal que $\alpha \in F_r$.

Proposición 6.4. *Sea $\alpha \in \mathbb{R}$ algebraico sobre $\mathbb{Q}$ y sea $E \subset \mathbb{C}$ cuerpo de escisión sobre $\mathbb{Q}$ del polinomio $Irr(\alpha, \mathbb{Q})$. Si $E \subset \mathbb{R}$ y si $[E : \mathbb{Q}]$ es una potencia de 2, entonces α es constructible.*

Demostración. $E : \mathbb{Q}$ es extensión finita de Galois y, por tanto, se tiene $\#G = [E : \mathbb{Q}] = 2^r$, en donde se ha puesto $G = Gal(E/\mathbb{Q})$. Así G es un 2-grupo que admitirá una filtración de subgrupos

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = G,$$

en la cual cada H_i es subgrupo normal y de índice 2 en H_{i+1} (1.48).

Si $F_i := E^{H_i}$, para $i = 0, 1, \ldots, r$, son los correspondientes cuerpos fijos, se tiene una torre de cuerpos

$$\mathbb{R} \supset E = E^{H_0} \supset F_1 = E^{H_1} \supset \cdots \supset F_i = E^{H_i} \supset F_{i+1} = E^{H_{i+1}} \supset \cdots \supset F_r = E^G = \mathbb{Q}$$

en la cual cada $F_i : F_{i+1}$ es una extensión de Galois cuyo grupo $Gal(F_i/F_{i+1})$ es isomorfo al grupo cociente H_{i+1}/H_i (por el Teorema fundamental de teoría de Galois) y que, por lo tanto es de grado 2. Entonces, como $\alpha \in E \subset \mathbb{R}$, el elemento α es constructible. □

La última afirmación del Teorema fundamental sobre constructibilidad (3.28) establece que si α es un número real constructible, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2.

Lema 6.5. *Sean* $\theta = \dfrac{2\pi}{n}$ *y* $\xi = \cos\theta + i sen\theta$ *una raíz primitiva* n*-ésima de* 1. *Entonces*

1) $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ *es una potencia de* $2 \Leftrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}]$ *es una potencia de* 2.

2) $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ *es una potencia de* $2 \Leftrightarrow \cos\theta$ *es un número real constructible.*

Demostración. Por la observación anterior, se tiene: $\mathbb{Q} \subset \mathbb{Q}(\cos\theta) \subset \mathbb{Q}(\xi)$. Así la "⇐" de 1) es obvia. Para la completa demostración de 1) obsérvese que el polinomio $(X - \xi)\left(X - \overline{\xi}\right) = X^2 - 2\cos\theta X + 1 \in \mathbb{Q}(\cos\theta)[X]$ es irreducible en $\mathbb{Q}(\cos\theta)[X]$ ya que tiene a ξ y $\overline{\xi}$ como ceros, y ninguno de ellos es elemento de $\mathbb{Q}(\cos\theta)$, que es subcuerpo de $\mathbb{R}$. Por lo tanto, la extensión $\mathbb{Q}(\cos\theta)(\xi) = \mathbb{Q}(\xi) : \mathbb{Q}(\cos\theta)$ es de grado 2, y entonces $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ es una potencia de 2.

2) " ⇒ "

$\mathbb{Q}(\xi)$ es cuerpo de escisión de $Irr(\xi, \mathbb{Q})$ sobre $\mathbb{Q}$, con lo que $\mathbb{Q}(\xi) : \mathbb{Q}$ es de Galois con grupo abeliano (5.23), y así resulta que $\mathbb{Q}(\cos\theta) : \mathbb{Q}$ es de Galois también y su grupo $Gal(\mathbb{Q}(\cos\theta)/\mathbb{Q})$ es isomorfo a un grupo cociente de $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ y, por eso, es también abeliano. Entonces $\mathbb{Q}(\cos\theta)$ es cuerpo de escisión sobre $\mathbb{Q}$ de $Irr(\cos\theta, \mathbb{Q})$ (ya que, al ser $\mathbb{Q}(\cos\theta) : \mathbb{Q}$ normal, el cuerpo $\mathbb{Q}(\cos\theta)$ debe contener a todos los ceros de dicho polinomio, y así $\mathbb{Q}(\cos\theta)$ está generado sobre $\mathbb{Q}$ por dichos ceros). Como, por hipótesis, $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ es una potencia de 2, la aplicación de la Proposición 6.4 al elemento $\alpha = \cos\theta$ proporciona que $\cos\theta$ es un número real constructible.

2) " ⇐ "

Si $\cos\theta$ es constructible $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ es una potencia de 2 (comentario previo al enunciado de este Lema). □

Lo obtenido permite demostrar el resultado definitivo sobre la constructibilidad de polígonos regulares:

Teorema 6.6. *(Teorema de Gauss-Wantzel)*

Sea $n > 2$ un número entero. Entonces son equivalentes las afirmaciones:

i) El n-ágono regular es constructible.

ii) El indicador de Euler $\varphi(n)$ es una potencia de 2.

iii) $n = 2^m p_1 \cdots p_t$, con m y t números naturales, y $p_1, \ldots, p_t$ primos de Fermat diferentes.

Demostración. i) $\Leftrightarrow$ ii)

En efecto, el n-ágono regular es constructible $\Leftrightarrow \cos\theta$ es constructible ($\theta = \dfrac{2\pi}{n}$) $\Leftrightarrow [\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ es una potencia de 2, (en virtud del Lema 6.5 en su apartado 2) $\Leftrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}] = 2^s$, siendo ξ una raíz primitiva n-ésima de 1 (en virtud del mismo Lema, apartado 1) $\Leftrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}] = \partial(Irr(\xi, \mathbb{Q})) = \partial(\Phi_n) = \varphi(n) = 2^s$.

Ahora, si $n = p_1^{r_1} \cdots p_t^{r_t}$ es la factorización de n en números primos, es conocido que $\varphi(n) = (p_1 - 1)\, p_1^{r_1 - 1} \cdots (p_t - 1)\, p_t^{r_t - 1}$, y entonces, $\varphi(n)$ es una potencia de dos $\Leftrightarrow$ para cada $p_j \neq 2$, $r_j = 1$ y $p_j - 1$ es una potencia de 2. Ello es equivalente a decir que para cada $p_j \neq 2$ en la anterior factorización de n, $r_j = 1$ y p_j es un primo de Fermat (Proposición 6.2) Esto establece la equivalencia *ii)* $\Leftrightarrow$ *iii)* y el Teorema queda probado. □

Así, por ejemplo, no son constructibles ni el heptágono, ni el undecágono regulares, ni los polígonos regulares de trece o dieciocho lados. Los polígonos regulares con un número de lados primo p son constructibles si, y solo si, p es un primo de Fermat. Son constructibles, entre otros, los polígonos regulares de $15 = 2^0\big(2^{2^0}+1\big)\big(2^{2^1}+1\big)$, $16 = 2^{2^2}$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$ y $65537 = 2^{2^4} + 1$ lados.

6.2. La trascendencia de π

Recuérdese que la prueba completa de la imposibilidad de obtener la cuadratura del círculo utilizando solamente la regla y el compás está supeditada a la demostración de la trascendencia de π. Como ya se he dicho el resultado se debe a F. von Lindemann (*Über die Zahl* π. Mathematische Annalen Vol. 20 (1882) 213-225). A continuación transcribimos la prueba que de este crucial resultado aparece en las páginas 170-177 de [$HAWR$] y que, según sus autores, es esencialmente la misma que puede ser consultada en *Vorlesungen über Zahlentheorie* (Hirzel, Leipzig (1927) de E. Landau, o en *Irrationalzahlen* (de Gruyter, Berlin (1910)) de O. Perron (discípulo de Lindemann al igual

que Hilbert). Se completa así el contenido de estas notas en lo relativo a construcciones geométricas.

Recordemos la definición de exponencial compleja e^α poniendo, para $\alpha = a + bi$

$$e^\alpha = e^a e^{bi} = e^a(\cos b + isenb).$$

Comenzamos con la introducción del símbolo h^r, en donde r es un número natural, poniendo

$$h^0 := 1 \text{ y } h^r := r!, \text{ si } r \geqslant 1.$$

Con esta convención, si $f = \sum_{r=0}^m c_r X^r \in \mathbb{C}[X]$ es cualquier polinomio de grado m se tiene

$$f(h) := \sum_{r=0}^m c_r h^r = \sum_{r=0}^m c_r r!,$$

y, poniendo $F(Y) = f(X + Y)$, resulta $f(X + h) = F(h)$. Además, es fácil comprobar (recurriendo por ejemplo a la fórmula de Taylor) que

$$f(X + Y) = \sum_{r=0}^m \frac{f^{(r)}(X)}{r!} Y^r,$$

y, por lo tanto,

$$f(X + h) = F(h) = \sum_{r=0}^m \frac{f^{(r)}(X)}{r!} h^r = \sum_{r=0}^m f^{(r)}(X).$$

Para $x \in \mathbb{C}$ y $r \geqslant 0$, se define también, $u_r(x)$ y $\epsilon_r(x)$ mediante

$$u_r(x) = \frac{x}{r+1} + \frac{x^2}{(r+1)(r+2)} + \cdots = \sum_{n>0} \frac{r! x^n}{(n+r)!} = e^{|x|}\epsilon_r(x).$$

Por comparación con el desarrollo de Taylor de la función e^x resulta $|u_r(x)| < e^{|x|}$, puesto que $\sum_{n\geqslant 0} \frac{x^n}{n!} > \sum_{n\geqslant 0} \frac{r! x^n}{(n+r)!}$ al ser $\frac{r!}{(r+n)!} < \frac{1}{n!}$, para todo $r > 0$. En consecuencia, $|\epsilon_r(x)| < 1$, para cualquier $x \in \mathbb{C}$.

Lema 6.7. *Si para un polinomio $\phi = \sum_{r=0}^s c_r X^r \in \mathbb{C}[X]$ se considera la expresión $\psi(x) = \sum_{r=0}^s c_r \epsilon_r(x) x^r$, definida para cualquier $x \in \mathbb{C}$, se tiene entonces la igualdad*

$$e^x \phi(h) = \phi(x + h) + \psi(x) e^{|x|},$$

para cualquier $x \in \mathbb{C}$.

Demostración.

$$\begin{aligned}(X+h)^r &= \sum_{j=0}^{r}\binom{r}{j}X^j h^{r-j} = h^r + rXh^{r-1} + \frac{r\,(r-1)}{2}X^2h^{r-2} + \cdots + X^r \\ &= r! + r\,(r-1)!X + \frac{r\,(r-1)}{2}\,(r-2)!X^2 + \cdots + X^r \\ &= r!\left(1 + X + \frac{X^2}{2!} + \cdots + \frac{X^r}{r!}\right).\end{aligned}$$

Ahora para cualquier $x \in \mathbb{C}$

$$r!\left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^r}{r!}\right) = r!e^x - u_r(x)x^r = e^x h^r - u_r(x)x^r.$$

Entonces

$$e^x h^r = (x+h)^r + u_r(x)x^r = (x+h)^r + e^{|x|}\epsilon_r(x)x^r.$$

Multiplicando la última igualdad por c_r y sumando se obtiene el resultado. □

Lema 6.8. *Si $m \geqslant 2$, $f \in \mathbb{Z}\,[X]$ y se pone*

$$F_1 = \frac{X^{m-1}}{(m-1)!}f \quad y \quad F_2 = \frac{X^m}{(m-1)!}f,$$

entonces $F_1(h)$ y $F_2(h)$ son números enteros y además $F_1(h) - f(0)$ y $F_2(h)$ son múltiplos de m.

Demostración. Sea $f = \sum_{l=0}^{L} a_l X^l \in \mathbb{Z}\,[X]$. Se tiene

$$F_1 = \sum_{l=0}^{L} a_l \frac{X^{l+m-1}}{(m-1)!},$$

y, por tanto,

$$F_1(h) = \sum_{l=0}^{L} a_l \frac{(l+m-1)!}{(m-1)!}.$$

Como $\dfrac{(l+m-1)!}{(m-1)!} = (l+m-1)\,(l+m-2)\cdots m$ es múltiplo de m si $l \geqslant 1$, resulta que $F_1 - a_0$ es múltiplo de m. De modo análogo

$$F_2 = \sum_{l=0}^{L} a_l \frac{X^{l+m}}{(m-1)!}$$

y entonces

$$F_2(h) = \sum_{l=0}^{L} a_l \frac{(l+m)!}{(m-1)!}$$

es múltiplo de m, pues para $l = 0, \ldots, L$ el entero $\dfrac{(l+m)!}{(m-1)!}$ es múltiplo de m. □

Lema 6.9. *Sea $dX^m + d_1X^{m-1} + \cdots + d_m \in \mathbb{Z}[X]$ y $\beta_1, \ldots, \beta_m \in \mathbb{C}$ sus raíces. Entonces si $f(t_1, \ldots, t_m) \in \mathbb{Z}[t_1, \ldots, t_m]$ es un polinomio simétrico, el valor numérico $f(d\beta_1, \ldots, d\beta_m)$ es un número entero. De hecho, para cada tal f existe un polinomio $g(t_1, \ldots, t_m) \in \mathbb{Z}[t_1, \ldots, t_m]$ tal que*

$$f(d\beta_1, \ldots, d\beta_m) = g(d_1, \ldots, d_m).$$

Demostración. Es conocido que $\mathbb{Z}[s_1, \ldots, s_m]$ es el anillo de los polinomios simétricos en m variables (5.62), siendo $s_1(t_1, \ldots, t_m), \ldots, s_m(t_1, \ldots, t_m)$ los polinomios simétricos elementales (cada s_i es homogéneo de grado i). Sea entonces $f(t_1, \ldots, t_m) = k(s_1, \ldots, s_m)$ con $k \in \mathbb{Z}[X_1, \ldots, X_m]$, es decir, un polinomio en m variables con coeficientes enteros. Además, como es bien conocido

$$\begin{aligned}
\frac{d_1}{d} &= -s_1(\beta_1, \ldots, \beta_m), \\
&\cdots \\
\frac{d_i}{d} &= (-1)^i s_i(\beta_1, \ldots, \beta_m), \\
&\cdots \\
\frac{d_m}{d} &= (-1)^m s_m(\beta_1, \ldots, \beta_m),
\end{aligned}$$

y entonces

$$\begin{aligned}
f(d\beta_1, d\beta_2, \ldots, d\beta_m) &= k(s_1(d\beta_1, \ldots, d\beta_m), \ldots, s_m(d\beta_1, \ldots, d\beta_m)) \\
&= k(-\frac{d_1 d}{d}, \frac{d_2 d^2}{d}, \ldots, (-1)^m \frac{d_m d^m}{d}),
\end{aligned}$$

en virtud de la homogeneidad de los s_i. Se tiene ahora

$$f(d\beta_1, d\beta_2, \ldots, d\beta_m) = k(-d_1, dd_2, \ldots, (-1)^m d^{m-1} d) = g(d_1, d_2, \ldots, d_m),$$

en donde se ha puesto $g(X_1, X_2, \ldots, X_n) := k(-X_1, dX_2, \ldots, (-1)^m d^{m-1} X_m)$. □

Teorema 6.10. *π es trascendente sobre $\mathbb{Q}$.*

Demostración. Supongamos que π es algebraico sobre $\mathbb{Q}$. En ese caso $\mathbb{Q}(i,\pi)$ es extensión finita de $\mathbb{Q}$ y, por lo tanto, también es algebraico sobre $\mathbb{Q}$ el complejo $i\pi$ que será entonces un cero de algún polinomio no nulo $f = dX^m + d_1X^{m-1} + \cdots + d_m \in \mathbb{Z}[X]$, con $m = \partial(f)$. Sean $\omega_1, \ldots, \omega_m \in \mathbb{C}$ los ceros de f, con $\omega_j = i\pi$ para algún j, y

$$\prod_{k=1}^{m} (1 + e^{\omega_k}) = 0,$$

(recuérdese la identidad euleriana $-1 = e^{i\pi}$). Efectuando el producto indicado en la anterior igualdad resulta una expresión,

$$1 + \sum_{i=1}^{2^m-1} e^{\alpha_i} = 0 \ \ (*)\,,$$

en donde la sucesión de números complejos

$$\alpha_1, \alpha_2, \ldots, \alpha_{2^m-1}$$

es la formada por

$$\omega_1, \omega_2, \ldots, \omega_m, \omega_1+\omega_2, \omega_1+\omega_3, \ldots, \omega_{m-1}+\omega_m, \ldots, \omega_1+\omega_2+\cdots+\omega_m, \quad (**)$$

de los cuales supondremos que son nulos $C-1$ de ellos y que, por tanto, después de una reordenación, se tiene la sucesión

$$\alpha_1, \alpha_2, \ldots, \alpha_n, 0, 0, \ldots, 0$$

con $n = 2^m - 1 - (C-1) \neq 0$, y los $\alpha_1, \alpha_2, \ldots, \alpha_n$ no nulos. Con estas convenciones la expresión $(*)$ adquiere la forma

$$C + \sum_{i=1}^{n} e^{\alpha_i} = 0. \quad (***)\,.$$

Sea ahora p un número primo tal que $p > máx(d, C, |d^n\alpha_1 \cdots \alpha_n|)$ y definamos

$$\begin{aligned}
\phi :&= \frac{d^{np+p-1}X^{p-1}}{(p-1)!}\left[(X-\alpha_1)\cdots(X-\alpha_n)\right]^p \\
&= \frac{X^{p-1}}{(p-1)!}d^{p-1}\left[(dX-d\alpha_1)\cdots(dX-d\alpha_n)\right]^p \\
&= \frac{X^{p-1}}{(p-1)!}d^{p-1}\Big[\sum_{k=0}^{n} s_k\left(d\alpha_1, \ldots, d\alpha_n\right)(dX)^k\Big]^p
\end{aligned}$$

donde $s_0 = 1$ y cada $s_k(t_1, \ldots, t_n)$ es el polinomio simétrico elemental de grado k. Realizando las operaciones indicadas en el segundo miembro de la anterior igualdad y agrupando monomios del mismo grado resulta

$$\phi = \frac{X^{p-1}}{(p-1)!} \sum_{k=0}^{np} d^{p-1} g_l(d\alpha_1, \ldots, d\alpha_n) (dX)^l,$$

en donde ahora, de nuevo los $g_l(d\alpha_1, \ldots, d\alpha_n)$ son expresiones polinómicas simétricas y con coeficientes enteros. Ahora bien, por (5.63), si f es un polinomio simétrico en n variables con coeficientes enteros, f puede ser considerado como polinomio simétrico con coeficientes enteros en $2^m - 1$ variables (no intervienen en f las restantes $2^m - 1 - n$ variables) y así se tiene

$$f(d\alpha_1, \ldots, d\alpha_n) = f(d\alpha_1, \ldots, d\alpha_n, 0, \overset{2^m-1-n)}{\ldots}, 0) = f(d\alpha_1, \ldots, d\alpha_{2^m-1}).$$

Teniendo en cuenta la forma de las α_j obtenida en $(**)$ resulta que $f(d\alpha_1, \ldots, d\alpha_{2^m-1}) = g(d\omega_1, \ldots, d\omega_m)$, siendo de nuevo g un polinomio simétrico con coeficientes enteros. Por aplicación de (6.9) se obtiene que $f(d\alpha_1, \ldots, d\alpha_n)$ es un número entero. En particular, cada $d^{p-1} g_l(d\alpha_1, \ldots, d\alpha_n)$ es un número entero. Sean, ahora,

$$S_0 = C\phi(h), \; S_1 = \sum_{t=1}^{n} \phi(\alpha_t + h) \quad \text{y} \quad S_2 = \sum_{t=1}^{n} \psi(\alpha_t) e^{|\alpha_t|}$$

(6.7), con cuyas convenciones la igualdad $(***)$ adquiere el aspecto

$$S_0 + S_1 + S_2 = 0.$$

Como consecuencia del Lema 6.8 resulta que

$$\phi(h) = \frac{h^{p-1}}{(p-1)!} \sum_{l=0}^{np} d^{p-1} g_l(d\alpha_1, \ldots, d\alpha_n) d^l h^l = \sum_{l=0}^{np} d^{p-1} g_l(d\alpha_1, \ldots, d\alpha_n) d^l l!$$

es un entero congruente módulo p con el entero

$$d^{p-1} [(d0 - d\alpha_1) \cdots (d0 - d\alpha_n)]^p = (-1)^{np} d^{p-1} (d\alpha_1 \cdots d\alpha_n)^p,$$

que no es múltiplo de p por la selección que se ha hecho de este primo. Como consecuencia, S_0 es un entero no divisible por p ya que p no divide a C. Por otro lado, después

de la correspondiente substitución y de reordenar se obtiene

$$\phi(\alpha_j + x) = \frac{x^p}{(p-1)!} \sum_{l=0}^{np-1} f_{l,j} x^l$$

en donde $f_{l,j} = f_l(d\alpha_j; d\alpha_1, \ldots, \widehat{d\alpha_j}, \ldots, d\alpha_n)$ es una expresión polinómica con coeficientes enteros que es simétrica en las $d\alpha_1, \ldots, d\alpha_{j-1}, d\alpha_{j+1} \ldots, d\alpha_n$. Entonces

$$\sum_{j=1}^{n} \phi(\alpha_j + x) = \frac{x^p}{(p-1)!} \sum_{l=0}^{np-1} F_l x^l,$$

siendo $F_l = \sum_j f_{l,j} = \sum_{j=1}^{n} f_l(d\alpha_j; d\alpha_1, \ldots, \widehat{d\alpha_j}, \ldots, d\alpha_n)$ que es ahora una expresión polinómica simétrica con coeficientes enteros en las $d\alpha_1, d\alpha_2, \ldots, d\alpha_n$ y, por tanto, $\sum_{j=1}^{n} \phi(\alpha_j + x)$ es un entero. Además, por el Lema 6.8 resulta que $S_1 = \sum_{j=1}^{n} \phi(\alpha_j + h)$ es múltiplo de p.

Como consecuencia, $S_0 + S_1$ es un entero no nulo que no es múltiplo de p.

Por otra parte, para cualquier x se tiene

$$|\psi(x)| < \frac{|d|^{np+p-1} |x|^{p-1}}{(p-1)!} [(|x| + |\alpha_1|) \cdots (|x| + |\alpha_n|)]^p$$

que define una sucesión de números reales convergente a cero según se incremente el valor de p (para el cual, en todo lo dicho, solo existe restricción sobre su valor mínimo). Por tanto, para valores de p suficientemente grandes se tiene

$$\frac{|d|^{np+p-1} |\alpha_t|^{p-1}}{(p-1)!} [(|\alpha_t| + |\alpha_1|) \cdots (|\alpha_t| + |\alpha_n|)]^p < \frac{1}{2ne^{|\alpha_t|}},$$

para cualquier valor $t = 1, 2, \ldots, n$, y entonces

$$|S_2| = \left| \sum_{t=1}^{n} \psi(\alpha_t) e^{|\alpha_t|} \right| < \frac{1}{2}.$$

Así tenemos $|S_0 + S_1| \geqslant 1$ (ya que $S_0 + S_1$ es un entero no nulo) y $|S_2| < \frac{1}{2}$. Ambas afirmaciones son incompatibles con $S_0 + S_1 + S_2 = 0$.

Por lo tanto π es trascendente sobre $\mathbb{Q}$. □

Indicaciones para los ejercicios

Ejercicios del capítulo 1

2.- La aplicación $\varphi_a\colon G \to G$, $\varphi_a(x) = axa^{-1}$ (conjugación por a es isomorfismo de grupos.

3.- $x = x^{-1}$, $\forall x \in G \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

4.- Con la notación $S^{-1} = \{s^{-1} \mid s \in S\}$ se puede escribir $(HK)^{-1} = H^{-1}K^{-1}$. El resto es fácil.

5.- a) Si $\alpha = (1\ 2)(3\ 4)$, $\beta = (1\ 3)(2\ 4)$ y $\gamma = (1\ 4)(2\ 3)$ un sencillo cálculo proporciona $\alpha\beta = \gamma$, $\alpha\gamma = \beta$, $\beta\gamma = \alpha$ y $\alpha^2 = \beta^2 = \gamma^2 = id$.

b) V es el único 2-subgrupo de Sylow de A_4 (véase prueba de 1.69).

c) $(1\ 2\ 3)(1\ 2)(3\ 4) \neq (1\ 2)(3\ 4)(1\ 2\ 3)$ y es fácil ver que V es abeliano (por ejemplo, usando el ejercicio 3).

7.- $(a,b)^r = (a^r, b^r) = (e_G, e_H) \Leftrightarrow r$ es múltiplo de $|a|$ y de $|b|$.

8.- $ab = ba \Rightarrow (ab)^r = a^r b^r$, $\forall r \in \mathbb{Z}$.

Si $|ab| = s$ se tiene $a^s = b^{-s} \in \langle a\rangle \cap \langle b\rangle = \{e\} \Rightarrow |a|$ y $|b|$ son divisores de s. El resto es fácil.

9.- Un cálculo elemental con matrices proporciona

$$(AB)^n = \begin{pmatrix} (-1)^n & (-1)^{n-1}\, n \\ 0 & (-1)^n \end{pmatrix}.$$

10.- a) Es fácil y b) se deduce de a) observando que $ba = b(ab)b^{-1}$.

11.-a) $\left(a^j\right)^r = a^{rj} = e \Leftrightarrow rj \in n\mathbb{Z} \Leftrightarrow rj = t(mcm(n,j))$, para un cierto entero t $\Leftrightarrow \exists t \in \mathbb{Z} \mid rj = \dfrac{nj}{(n,j)}t \Leftrightarrow r = \dfrac{n}{(n,j)}t$, para un cierto entero t.

b) $n = rs \Rightarrow |a^s| = r \Rightarrow \langle a^s\rangle = H$ es de orden r; si $x = a^l$ es de período r, entonces $x^r = a^{rl}e \Rightarrow rl = nt = rst$ para un cierto entero $t \Rightarrow \exists t \in \mathbb{Z} \mid l = st \Rightarrow x = a^l = (a^s)^t \in H$.

12.- $H = \langle a^4 \rangle$.

13.- $\langle (a,b) \rangle = G \times H \Leftrightarrow |(a,b)| = mcm(|a|, |b|) = mn$ (ejercicio 7) $\Leftrightarrow (|a|, |b|) = 1$.

14.- G es finito, pues en otro caso contendría un subgrupo propio isomorfo a $\mathbb{Z}$. Ahora $G = \langle x \rangle, \forall x \in G \setminus \{e\}$; $r | \#G \Rightarrow \exists H$ subgrupo de G de orden r (1.30).

15.- En primer lugar pruébese que $H' = \{x \in G \mid |x| \text{ es una potencia de } p\}$ es subgrupo de G con lo que necesariamente H es subgrupo de H'. Si la inclusión $H \subset H'$ es estricta se llega a un absurdo, pues $\#H'$ deberá ser, en ese caso, divisible por un primo p' diferente de p, y, aplicando lo establecido en (1.31), deberá existir en H' un elemento de periodo p'.

16.- $a^r = e_G \Rightarrow (f(a))^r = f(a^r) = e_H$, y si f es inyectivo $a^r = e_G \Leftrightarrow (f(a))^r = e_H$.

17.- Si $G = \{e, \alpha, \beta, \gamma\}$ no es un grupo cíclico, se tiene $|\alpha| = |\beta| = |\gamma| = 2$. Además, $\alpha\beta \neq e, \alpha, \beta \Rightarrow \alpha\beta = \gamma$. Análogamente $\alpha\gamma = \beta$ y $\beta\gamma = \alpha$ (véase ejercicio 6).

18.- $\mathbb{Z}_{35}/(5\mathbb{Z}/35\mathbb{Z}) \simeq \mathbb{Z}_5 \Rightarrow \#(5\mathbb{Z}/35\mathbb{Z}) = 7$.

19.- $f(a) = a^m \neq e$, $\forall a \in G$.

20.- Ni $(\mathbb{Q}, +)$ ni $(\mathbb{Q}^*, .)$ son cíclicos. En el primer caso porque de lo contrario existiría $\frac{p}{q} \in \mathbb{Q}$ (siempre se puede suponer que p y q son enteros primos entre sí) tal que cada $x \in \mathbb{Q}$ se pondría como $x = n_x \frac{p}{q}$ con $n_x \in Z$ y en particular sería $1 = n_1 \frac{p}{q}$ y así $q = n_1 p$ lo cual es absurdo salvo que $q = 1$, pero en ese caso n_1 no sería entero. En el caso de $(\mathbb{Q}^*, .)$, si $\frac{p}{q}$ genera $\mathbb{Q}^*$ multiplicativamente, se tiene $1 = \left(\frac{p}{q}\right)^{n_1}$. Entonces $\frac{p}{q} = \pm 1$ y $\langle \frac{p}{q} \rangle$ tiene a lo sumo dos elementos.

21.- G no es cíclico pues no lo es $S_3 \times \{\overline{0}\}$.

El grupo $\{id\} \times \mathbb{Z}_5$ es el único 5-subgrupo de Sylow de G y es cíclico. $s_3 = 1$ ya que $A_3 \times \{\overline{0}\}$ es subgrupo normal de G. De forma alternativa, todo 3-subgrupo de Sylow de G es de orden 3. Si $(a,b) \in G$ es de orden 3 necesariamente se tiene $b = \overline{0}$ y $a \in S_3$ de período 3, es decir, 3-ciclo y así $\langle (a,b) \rangle = A_3 \times \{\overline{0}\}$.

22.- La parte difícil es $c) \Rightarrow a)$, ya que hay que probar que Φ es homomorfismo. Pero para $a \in A$ y $b \in B$ se tiene $aba^{-1}b^{-1} \in A \cap B = \{e\}$ por las hipótesis de $c)$.

23.- Es fácil demostrar que $s_5 = s_{13} = 1$.

24.- Es fácil demostrar que $s_7 = s_5 = 1$.

25.- En el grupo de orden 56, $s_2 = 1$ o $s_7 = 1$. En el grupo de orden 132, se tiene $s_2 = 1$, o bien $s_3 = 1$, o bien $s_{11} = 1$.

27.- $s_2 = 1$, o bien $s_3 = 1$ o bien $s_5 = 1$. Si, G es resoluble. Si G es de orden 60 y H es subgrupo normal propio de G el grupo cociente G/H es resoluble. Esto se obtiene argumentando con los posibles órdenes de H y de G/H.

28.- $s_7 = 8 = \mathfrak{O}_G(P) = (G : N_G(P)) \Rightarrow \#N_G(P) = 21$. Si $\#H = 14$, H contiene un 7-subgrupo de Sylow P que es normal en H y por tanto $H \subset N_G(P)$ lo que es imposible pues $\#N_G(P) = 21$.

29.- a) $(H : H \cap P)(HP : H) = (P : H \cap P)(HP : P)$, y teniendo en cuenta que $(HP : H) = (P : H \cap P)$, al ser $HP/H \simeq P/H \cap P$, resulta que $(H : H \cap P)$ divide a $(G : P)$ y, por tanto, es primo con p. Además $H \cap P$ es p-grupo.

b) Para $\#G = p^m r$, $\#H = p^n l$ se tiene $n \leqslant m$ y $r = ls$ con $s \in \mathbb{Z}$. Por a) $\#(H \cap P) = p^n$ y, por el Teorema de Lagrange, $\#(G/H) = p^{m-n}s$ y $\#(HP/H) = \#(P/H \cap P) = p^{m-n}$.

30.- a) Necesariamente $s_p = 1$.

b) Tiene un subgrupo normal de orden 7 y un subgrupo de orden 3.

31.- Si P es p-subgrupo de Sylow y K es subgrupo de orden 2 entonces P es normal y así $KP/P \simeq K$ pues $K \cap P = \{e\}$, con lo que resulta $\#(KP) = 2p$ y, por lo tanto, $G = KP$. Ahora $K = \langle x \rangle$, con $x^2 = e$, y $P = \langle y \rangle$ con $|y| = p$. Si G no es cíclico $|xy| = 2$ o bien $|xy| = p$. Como P es el único p-subgrupo de Sylow de G necesariamente $(xy)^2 = e \Rightarrow xy = (xy)^{-1} = y^{-1}x$. Como $G = \langle x, y \rangle$, de lo anterior se deduce $G \simeq D_{2p}$.

32.- Estudiando los posibles períodos de los elementos de G se demuestra que $s_3 = 1$ o $s_2 = 1$, y que, por tanto, existe un subgrupo normal de orden 3 o de orden 4. El grupo cociente es de orden 4 o de orden 3 y es resoluble. Ahora se aplica (1.65).

33.- a) G es un p-grupo si $p = q$. Si $p > q$, $s_p = 1$ y el único p-subgrupo de Sylow P es normal en G siendo el cociente G/P de orden primo q.

b) Se puede suponer $p < q$ pues en caso contrario el único p-subgrupo de Sylow sería normal y G sería resoluble. Ahora $s_q = 1 + kq \mid p^2 \Rightarrow s_q = 1$ (en cuyo caso el único q-subgrupo de Sylow de G es normal y G es resoluble por (1.65)) o $s_q = p^2$ (pues $p < q$); en este caso $kq = (p-1)(p+1)$ y entonces $p < q \mid p+1$, por lo que $q = p+1$. Necesariamente se tiene $p = 2$ y $q = 3$, con lo cual $\#G = 12$ y así G es resoluble.

34.- a) $D_{2,4}$ no es abeliano, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ no tiene subgrupo cíclico de orden 4.

b) Ninguno cíclico; todos resolubles.

c) Todos.

35.- a) q primo, $q \neq p$, $q \mid \#G \Rightarrow \exists x \in G$ con $|x| = q$.

b) $\mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \times \mathbb{Z}_p$.

36.- a) $s_5 = 1$.

b) $G = HK \simeq G/H \times G/K$ pues $|H| = |G/K| = 5$ y $|K| = |G/H| = 2$ números primos.

37.- a) Si $p < q$ y H es q-subgrupo de Sylow de G, entonces H es normal en G y G/H es cíclico de orden p. S_3 no es abeliano.

b) $pq \mid \#G$, $p \neq q$ números primos $\Rightarrow \exists H, K$ subgrupos de G con $H \nsubseteq K$ y $K \nsubseteq H$).

38.- $\#\left(Aut(\mathbb{Z}_n)\right) = \#\left\{m \in \mathbb{Z} \mid 0 < m < n, \text{ y } (m,n) = 1\right\}$.

39.- a) 1) Es (1.43); 2) Es (1.31) aplicado a Z_G.

b) 1) $G/(\{id\} \times \mathbb{Z}_4) \simeq S_3$; 2) $S_3 \times \left\{\overline{0}\right\} \simeq S_3$ tiene un único subgrupo de orden 3 que es A_3; 3) $\langle(1\ 2)\rangle \times \mathbb{Z}_4$ no es normal en G.

40.- a) G Tiene un subgrupo normal H de orden 11.

b) G/H es de orden 40 y tiene un subgrupo normal de orden 5 y el Teorema de la correspondencia proporciona un subgrupo normal K de G tal que $H \subset K$ y K/H de orden 5.

41.- $(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$ y $(a\underline{)}(b\ c) = (a\ b\ c)$

42.- Para $n \geqslant 3$ obsérvese que si σ es un 3-ciclo, entonces $\langle\sigma\rangle = \langle\sigma^2\rangle \subset S_n^{(1)}$ ya que σ^2 es un conmutador (σ es par). Como consecuencia del ejercicio 41 se tiene $A_n \subset S_n^{(1)} \subset A_n$, ya que $S_n/A_n \simeq \mathbb{Z}_2$ es grupo abeliano 1.67.

Ejercicios del capítulo 2

1.- a) El homomorfismo de anillos $\varphi[X] : A[X] \to (A/J)[X]$ definido por

$$\varphi[X]\left(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0\right) = \overline{a_n}X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0}$$

es sobreyectivo y de núcleo $J[X]$.

b) J primo de $A \Leftrightarrow A/J$ es dominio de integridad $\Leftrightarrow (A/J)[X] \simeq A[X]/J[X]$ es dominio de integridad $\Leftrightarrow J[X]$ es ideal primo de $A[X]$.

c) No, $(A/J)[X]$ no es cuerpo.

2.- $\alpha \in \mathbb{Z}$ cero de $f \Leftrightarrow f = (X-\alpha)g$ con $g \in \mathbb{Z}[X] \Rightarrow f(0) = (0-\alpha)g(0)$, $f(1) = (1-\alpha)g(1) \Rightarrow f(0)$ es par o lo es $f(1)$.

3.- $X^5 - 10X + 12 = \left(X^2+2\right)\left(X^3-2X\right) - 6X + 12$, por lo tanto, la solución es $n = 2, 3, 6$.

4.- $\mathbb{Z}[X]/(n,X) \simeq (\mathbb{Z}[X]/(n))/((n,X)/(n)) \simeq \mathbb{Z}_n[X]/(X) \simeq \mathbb{Z}_n$.

5.- a) f es irreducible y no lineal en $\mathbb{Z}_2[X] \Rightarrow f(\overline{0}) \neq \overline{0} \neq f(\overline{1}) \Rightarrow f$ tiene precisamente un número impar de coeficientes no nulos.

b) X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1, $X^4+X^3+X^2+X+1$, X^4+X^3+1 y X^4+X+1.

6.- a) $f+J=r+J$ donde $f=g(X^3+\overline{2}X+\overline{1})+r$ y $\partial\,(r)<3$ si es $r\neq 0$. Además, $r+J=r'+J$ con $r\neq r'\Rightarrow r'=h(X^3+\overline{2}X+\overline{1})+r$ para un cierto $h\in\mathbb{Z}_3\,[X]\,,$ $h\neq 0\Rightarrow\partial(r')>3$.

b) $X^3+\overline{2}X+\overline{1}$ es irreducible en $\mathbb{Z}_3\,[X]\Leftrightarrow F=\mathbb{Z}_3\,[X]\,/J$ es cuerpo (2.39).

c) $\dim_{\mathbb{Z}_3}F=3$.

7.- $7X^4-28=7(X^2-2)(X^2+2)$ en $\mathbb{Z}\,[X]$ y en $\mathbb{Q}\,[X]\,;$
$7X^4-28=7(X-\sqrt{2})(X+\sqrt{2})(X^2+2)$ en $\mathbb{R}\,[X]\,;$
$7X^4-28=7(X-\sqrt{2})(X+\sqrt{2})(X-i\sqrt{2})(X+i\sqrt{2})$ en $\mathbb{C}\,[X]\,;$
$7X^4-28=X^4$ en $\mathbb{Z}_2\,[X]\,.$

8.- De una hipotética factorización en polinomios no constantes de f en $\mathbb{Q}\,[X]$ se obtiene que $f=gh$, con $g,h\in\mathbb{Z}\,[X]$ (2.54) y con $\partial\,(g)=r>0$, $\partial\,(h)=s>0$. Si $g=b_rX^r+\cdots+b_0$ y $h=c_sX^s+\cdots+c_0$ se tiene $a_n=b_rc_s$ y $a_0=b_0c_0$. De las hipótesis se sigue que $\overline{\varphi_p}(f)=\overline{a_0}=\overline{b_0}\overline{c_0}=\overline{\varphi_p}(g)\overline{\varphi_p}(h)\Rightarrow\partial(\overline{\varphi_p}(g))=\partial(\overline{\varphi_p}(h))=0$, y entonces $p\mid b_r$ y $p\mid c_s$, con lo cual $p^2\mid a_n=b_rc_s$ lo que es contrario a la hipótesis.

9.- $X^7-2X^5+14X^2-8X+22$ es irreducible (2.60) en $\mathbb{Q}\,[X]$;
$4X^3-X^2+7$ es irreducible en $\mathbb{Q}\,[X]$ $\left(X^3+\overline{2}X^2+\overline{1}\right.$ es irreducible en $\left.\mathbb{Z}_3\,[X]\right)\,;$
$X^4+4=(X^2-2X+2)(X^2+2X+2)$; $\overline{\varphi}_2(X^5-2X^3+X^2-4X+3)=X^5+X^2+1$ es irreducible en $\mathbb{Z}_2\,[X]\,;$
$X^4-3X^2+9=(X^2+3X+3)(X^2-3X+3)$;
$3X^5-6X^3-21X^2-15X+100$ es irreducible en $\mathbb{Q}\,[X]$ (Eisenstein)*;
$(X^2-7)(X^6-1)=(X^2-7)(X-1)(X+1)(X^2+X+1)(X^2-X+1)$;
$X^3-X+(3n+2)$ es irreducible en $\mathbb{Q}\,[X]$ $(X^3+\overline{2}X+\overline{2}$ es irreducible en$\mathbb{Z}_3\,[X])$.

10.- a) $\overline{\varphi_2}(f)=X^5+X^2+X=X(X^4+X+\overline{1})$.

b) f no admite factores de grado 2 ni de grado 3 en $\mathbb{Z}\,[X]$ por no admitirlos $\overline{\varphi_2}(f)$ en $\mathbb{Z}_2\,[X]\,.$

11.- a) $\overline{\varphi_2}(f)=(X^3+X+\overline{1})^2$.

b) $\overline{\varphi_3}(f)=(X^2+\overline{1})^3$.

c) f es irreducible en $\mathbb{Z}\,[X]$ y en $\mathbb{Q}\,[X]$ (como consecuencia de a) y b) no tiene factores de grados 1,2 o 3).

12.- a) $J=\{f\in\mathbb{Z}\,[X]\mid f(0)=0\}=(X)$ por el Teorema del factor y teniendo en cuenta que $\mathbb{Z}\,[X]\,/(X)\simeq\mathbb{Z}$ se sigue que J es primo y no maximal.

b) X^4+6X^2+7 no tiene factores de grado 1 ni de grado 2.

13.- a) $n\in\mathbb{Z}\backslash\{-7,-4,-1,2\}\,.$

b) $\overline{\varphi_2}\left(X^3+mX+n\right)=X^3+X+\overline{1}$ es irreducible en $\mathbb{Z}_2\,[X]\,.$

c) $\{1,-1,p,-p\}\nsubseteq\{ceros\ de\ f\}\,.$

14.- $f=(X^2-2X+2)(X^2+X+1)$ en $\mathbb{R}\,[X]\,;$
$f=(X-(1+i))(X-(1-i))(X-\dfrac{-1+i\sqrt{3}}{2})(X-\dfrac{-1-i\sqrt{3}}{2})$ en $\mathbb{C}\,[X]\,.$

Ejercicios del capítulo 3

1.- Para $\alpha \in F \setminus K$ considérese la torre $K \subset K(\alpha) \subset F$ y aplíquese el Teorema del grado.

2.- X^2-7; X^2-4X+1; e es trascendente sobre $\mathbb{Q}$; X^5-7; $X^2-6X+10$; X^4+2X^2-1 y $X^4+X^3+X^2+X+1$.

3.- a) Ambas igualdades son consecuencia inmediata de las definiciones.
b) Se puede proceder por inducción en n.

4.- a) Pruébese que $\sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$ y aplíquese el Teorema del grado.
b) i) $X^2-2iX-3$; ii) $X^2-2\sqrt{2}X+3$ y iii) $X^2-1-2i\sqrt{2}$.

5.- Si $\alpha = \sqrt{3+4i}) + \sqrt{3-4i}$ se obtiene $\alpha^2 = 16$. Si $\beta = \sqrt{1+\sqrt{3}} + \sqrt{1-\sqrt{3}}$ se obtiene $\beta^2 = 2+2i\sqrt{2}$.

6.- Si $\alpha \notin K(\alpha^2)$ se obtiene que $[F:K]$ es necesariamente par.

7.- a) i) 2 y ii) 3.
b) X^3-6X-6.

8.- De la hipótesis se deduce fácilmente que $[F:\mathbb{Q}]$ es potencia de 2, mientras que $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$.

9.- 8.

10.- En el caso contrario se tendría que $\partial(f) \mid [F:K]$.

11.- Utilizando el problema anterior $\alpha \notin K(\beta)$ y $\beta \notin K(\alpha)$, y se prueba que $\partial(Irr(\alpha, K(\beta))) = \partial(Irr(\alpha, K))$ por el Teorema del grado, lo que proporciona el resultado y que $[K(a) \cap K(\beta) : K] = 1$.

12.- Pruébese, en primer lugar, que, bajo las hipótesis de finitud, se tiene la igualdad $EF = E[F] = F[E]$. Si $\{\beta_1, \ldots, \beta_n\}$ es una K-base de E, entonces $\{\beta_1, \ldots, \beta_n\}$ es un sistema de generadores de EF como F-espacio y así $[EF:F] \leqslant n$. De modo análogo se obtiene $[EF:E] \leqslant m$. La aplicación del Teorema del grado y la condición $(n,m)=1$ proporciona el resultado.

13.- a) i) En otro caso se tendría $\sqrt{2} \in \mathbb{Q}$. ii) Es consecuencia de i). iii) Pruébese que $\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}-\sqrt{3}\right)$.
b) $X^2-2\sqrt{3}X+1$.
c) $X^5-2 = Irr(\alpha,\mathbb{Q}) = Irr(\alpha, \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right))$ ya que 5 y 4 son primos entre si.

14.- a) Utilícese el método constructivo de la prueba del Teorema del grado y obsérvese que $\sqrt[3]{4}\sqrt{2}$ forma parte de una $\mathbb{Q}$-base de la extensión.

b) $\mathbb{Q}\left(\sqrt[6]{2}\right) \subset \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$ y ambas extensiones tienen el mismo grado sobre $\mathbb{Q}$.

c) También es generador de la extensión anterior el elemento $\sqrt{2}+\sqrt[3]{2}$ cuyo polinomio mínimo sobre $\mathbb{Q}$ ha de ser, entonces, de grado 6.

15.- a) $\alpha^{-1} = -\frac{1}{2}\alpha^2 - 1$, $\frac{1}{\alpha^2+\alpha+1} = \frac{2}{7}\alpha^2 - \frac{3}{7}\alpha + \frac{5}{7}$, $u = 6\alpha$.

b) $Irr\,(u, \mathbb{Q}) = X^3 + 72X + 532$, $Irr(\alpha^{-1}, \mathbb{Q}) = X^3 + X^2 + \frac{1}{2}$.

16.- a) Aplicación directa de la teoría.

b) $f = (X - \alpha)\, g$ con $g \in K\,(\alpha)\,[X]$ que tiene a β y γ como ceros.

c) $g = (X - \beta)\,(X - \gamma)$.

17.- a) $Irr(\alpha, \mathbb{Q}) = X^4 - 2X^2 - 2$; $Irr(\alpha, \mathbb{Q}\left(\sqrt{3}\right)) = X^2 - (1 + \sqrt{3})$.

b) $[F : \mathbb{Q}] = 4$.

18.- a) $\alpha^{-1} \in K\,(\alpha)\,, \alpha \in K\left(\alpha^{-1}\right) \Rightarrow K\,(\alpha) = K\left(\alpha^{-1}\right)$.

b) 3 y 8 son primos entre si.

19.- f es irreducible en $\mathbb{Q}\,[X]$ (Eisenstein) $\beta^{-1} = \frac{1}{2}\beta^5$. $Irr(\beta^{-1}, \mathbb{Q}) = X^6 - \frac{1}{2}$.

20.- a) Teniendo en cuenta que $1 - i \in \mathbb{C}$ es también un cero de $f \in \mathbb{R}\,[X]$ se tiene que $f = \left(X^2 - 2X + 2\right)\left(X^2 + X + 1\right)$, ambos factores irreducibles en $\mathbb{Q}\,[X]$; la factorización en $\mathbb{C}\,[X]$ es

$$f = (X - [1+i])\left(X - [1-i]\,\right)\left(X - \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\right)\left(X - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\right).$$

b) De una relación de dependencia lineal $a\sqrt{2} + b\sqrt[3]{2} + c\sqrt[5]{2} = 0$ con $a, b, c \in \mathbb{Q}$, si fuese $a \neq 0$ se tendría $\mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[5]{2}\right)$ y resultaría que 15 es par. De modo análogo se descarta $b \neq 0$ y $c \neq 0$.

21.- a) $f = 2\left(X^3 + 5X + 2\right)$, f es irreducible en $\mathbb{Q}[X]$ y no lo es en $\mathbb{R}\,[X]$ ni en $\mathbb{C}[X]$; f es irreducible en $\mathbb{Q}(\sqrt[5]{2})[X]$ al ser de grado 3 y no tener ningún cero en $\mathbb{Q}(\sqrt[5]{2})$, siendo 3 y 5 primos entre si (ejercicio 10).

b) $Irr(1 + \alpha, \mathbb{Q}) = X^3 - 3X^2 + 8X - 4$; $Irr(a^{-1}, \mathbb{Q}) = X^3 + \frac{5}{2}X^2 + \frac{1}{2}$.

22.- a) $f = \left(X^2 + 2\right)\left(X^2 - 2X + 3\right)$ en todos los casos.

b) 1) No. 2) No.

23.- a) Del ejercicio 5 resulta $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$. Además $\alpha^2 = \frac{\left(\alpha\sqrt{2}\right)^2}{2} \in \mathbb{Q}(\alpha\sqrt{2})$, y si fuese $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha\sqrt{2})$ se tendría $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\,(\alpha)$ lo cual es imposible por el Teorema del grado.

b) Para $\beta = \alpha\sqrt{2}$ se tiene $[\mathbb{Q}(\beta) : \mathbb{Q}] = 6$ y de $\left(\frac{\beta}{\sqrt{2}}\right)^3 + \frac{\beta}{\sqrt{2}} + 1 = 0$ se sigue que $\beta^6 + 4\beta^4 + 4\beta^2 - 8 = 0$.

24.- a) $F = K(\alpha_1, \ldots, \alpha_n)$ con cada α_i algebraico sobre K y $EF = E(\alpha_1, \ldots, \alpha_n)$.

b) Por aplicación directa del Teorema del grado.

c) Para $x \in EF$ existen $\alpha_1, \ldots, \alpha_n \in F$ tales que $x \in E(\alpha_1, \ldots, \alpha_n)$ y entonces se aplica a).

d) La concatenación de extensiones algebraicas es algebraica.

25.- La equivalencia se obtiene fácilmente considerando que $K[X, Y] = K[X][Y]$.

26.- La evaluación $\psi^{\chi}\colon K[X_1, \ldots, X_t] \to F$ para $\chi\{X_1, \ldots, X_t\} \to F$ dada por $\chi(X_i) = u_i$ $(i = 1, \ldots, t)$ es un isomorfismo y, por tanto,

$$K(u_1, \ldots, u_t) \simeq K(X_1, \ldots, X_t).$$

27.- Por recurrencia constrúyase un subconjunto $\{u_1, \ldots, u_t\}$ trascendente sobre K tal que cada u_j es algebraico sobre $K(u_1, \ldots, u_t)$, para $j = t+1, \ldots, n$.

28.- a) Cada polinomio $f \in A[X]$ puede ser identificado con un conjunto finito y ordenado de elementos (posiblemente con repeticiones) de A. Por ello $\#A[X] \leqslant \sum_{I \in \mathfrak{P}_F(A)} (\#I)^{\#I} = \#A$. La desigualdad es consecuencia de encontrar un polinomio representado en diferentes conjuntos finitos de elementos de A. (Por ejemplo: $aX^2 + c = aX^2 + 0X + c$ y, por lo tanto, forma parte de $I = \{a, c\}$ y de $J = \{a, 0, c\}$); $\mathfrak{P}_F(A)$ es el conjunto de las partes finitas de A, cuyo cardinal es el mismo que el de A al ser éste no finito.

b) $A[X] = \oplus_{t \in \mathbb{N}} AX^t \simeq \oplus_{t \in \mathbb{N}} M_t$.

c) Si, para cada t se pone $M_t \simeq A \oplus \overset{r_t)}{\cdots} \oplus A$, entonces $\oplus_{t \in \mathbb{N}} M_t \simeq \oplus_{i \in \mathbb{N}} A_i$, con $A_i = A$ $\forall i \in \mathbb{N}$.

d) $K = (A \times (A \setminus \{0\})) / \sim$, en donde $\sim$ es la relación de equivalencia

$$(a, b) \sim (c, d) :\Leftrightarrow ad = bc.$$

Por tanto, por el Axioma de Elección, existe una aplicación inyectiva $K \to A \times (A \setminus \{0\})$ y así resulta $\#K \leqslant \#(A \times (A \setminus \{0\})) \leqslant \#A$).

29.- La segunda afirmación es consecuencia de la primera y de la Hipótesis del Continuo. Para demostrar la primera obsérvese que $F = \bigcup_{E:K \text{ finita}} E$ donde todos los E son K-espacios de dimensión finita. Como existe un homomorfismo sobreyectivo $\bigoplus_{E:K \text{ finita}} E \to \bigcup_{E:K \text{ finita}} E$ y entonces $\#\Big(\bigcup_{E:K \text{ finita}} E\Big) \leqslant \#\Big(\bigoplus_{E:K \text{ finita}} E\Big) = \#K$. La desigualdad es consecuencia del Axioma de Elección, como antes, y la igualdad por el apartado c) del ejercicio anterior.

Ejercicios del capítulo 4

1.- Aplicación directa de la teoría.

2.- Los cuerpos de escisión y sus grados sobre $\mathbb{Q}$ son, respectivamente:
-$[\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) : \mathbb{Q}] = 4$;
-$[\mathbb{Q}\left(\xi\right) : \mathbb{Q}] = 6$, siendo ξ una raíz primitiva séptima de 1;
-$[\mathbb{Q}\left(i\sqrt{3}\right) : \mathbb{Q}] = 2$;
-$[\mathbb{Q}\left(i, \sqrt[4]{3}\right) : \mathbb{Q}] = 8$;
-$[\mathbb{Q}\left(\sqrt{2}, \xi\right) : \mathbb{Q}] = 4$, con ξ una raíz primitiva sexta de 1;
-$[\mathbb{Q}\left(i, \sqrt{3}\right) : \mathbb{Q}] = 4$;
-$[\mathbb{Q}\left(\sqrt{7}, \sqrt{3}\right) : \mathbb{Q}] = 4$;
-$[\mathbb{Q}\left(\sqrt[5]{2}, \xi\right) : \mathbb{Q}] = 20$, con ξ una raíz primitiva quinta de 1;
-$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{7}\ , \xi) : \mathbb{Q}] = 12$, con ξ una raíz primitiva cúbica de 1.

3.- $f = \prod_{k=0}^{11}\left(X - \xi^k \sqrt[3]{2}\right)\left(X^2 - 3\right)$ con ξ raíz primitiva duodécima de 1, teniendo en cuenta que $i = 2\xi - \sqrt{3}$ si $\xi = e^{\frac{2\pi i}{12}}$ y $[E : \mathbb{Q}] = 12$.

4.- a) $E_f = \mathbb{Q}\left(\left(1 + i\right)\sqrt{2}\right)$;
b) $E_f = \mathbb{Q}\left(i\right)$.

5.- a) f es irreducible en $\mathbb{Q}[X]$ y tiene un cero $\alpha \in \mathbb{R}$ y, así, $f(X) = X^3 - X - 1 = \left[X^2 + \alpha X + (\alpha^2 - 1)\right](X - \alpha)$. Como $\delta = \alpha^2 - 4(\alpha - 1) = -(3\alpha^2 - 4) < 0$, pues en otro caso se tendría $\alpha^3 - \alpha - 1 < 0$, los otros ceros de f no son reales y $Gal_{\mathbb{Q}}(f) \simeq S_3$; b) S_3; $c)$ S_3 y d) $\mathbb{Z}_3$.

6.- Aplicación directa de la teoría.

7.- a) $E_f = \mathbb{Q}\left(\xi, \sqrt[6]{2}\right)$ y $E_g = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$ con $\xi = e^{\frac{2\pi i}{6}}$ y $\omega = e^{\frac{2\pi i}{3}}$; $[E_f : \mathbb{Q}] = 12$.
b) $\left\{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5\right\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\beta)$, y $\beta^6 - 2 = 0 \Rightarrow \beta^{-1} = \dfrac{1}{2}\beta^5$.

8.- El resultado se tiene al conocer los ceros de f y de g en $\mathbb{C}$.

9.- a) Es de grado impar.
b) Criterio de Eisenstein y 3, 5 son primos entre si.
c) $\mathbb{Q}\left(\sqrt[3]{2}, i\right) : \mathbb{Q}$ no es normal pues el polinomio $X^3 - 2$ tiene un cero en el cuerpo $\mathbb{Q}\left(\sqrt[3]{2}, i\right)$ pero no escinde en él.

10.- $[\mathbb{Q}(\alpha, \xi) : \mathbb{Q}] = 20$.

11.- La primera parte es fácil. El ejemplo se puede dar con el polinomio $\left(X^2 - 2\right)(X - 5)$.

12.- Resolviendo la ecuación bicuadrada $f = 0$ resulta
$f = (X - \alpha)\left(X - \alpha^{-1}\right)(X + \alpha)\left(X + \alpha^{-1}\right)$.

13.- 6.

14.- $[L_1 : \mathbb{Q}] = 2 = [L_2 : L_1]$; el polinomio $f = X^4 - 2X^2 - 2$ es el irreducible de $\alpha = \sqrt{\sqrt{3}+1}$ sobre $\mathbb{Q}$, f tiene un cero en L_2 pero $\beta = \sqrt{1-\sqrt{3}}$, que es también cero de f, no pertenece a L_2.

15.- a) $f = (X-2)\left(X^4 + X^3 + X^2 + X + 1\right)$, $E_f = \mathbb{Q}(\xi)$ con $\xi \neq 1$ y $\xi^5 = 1$, $[E_f : \mathbb{Q}] = 4$.

b) $X^3 - 3aX + 3$ es irreducible en $\mathbb{Q}[X]$ y si este último polinomio tuviese un cero en común con f se tendría que 3 es divisor de 4, como consecuencia del Teorema del grado.

16.- $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(i\sqrt{5}\right)\right] = 2$; $Irr(\alpha, \mathbb{Q}) = X^4 + 20$ tiene un cero en $\mathbb{Q}(\alpha)$ pero $\pm\sqrt[4]{5}(1-i) \notin \mathbb{Q}(\alpha)$; la clausura normal es el cuerpo de escisión de $X^4 + 20$ sobre $\mathbb{Q}$, es decir, $\mathbb{Q}\left(\sqrt[4]{5}, i\right)$.

17.- Tienen ambos dimensión 2 como $\mathbb{Q}$-espacios; si $\sigma\colon \mathbb{Q}(i) \to \mathbb{Q}\left(\sqrt{2}\right)$ fuese un isomorfismo se tendría que -1 es un cuadrado en $\mathbb{R}$.

18.- a) No existe ninguno.

b) $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ y la extensión $\mathbb{Q}(\alpha) : \mathbb{Q}$ es cuerpo de escisión del polinomio $X^4 + X^3 + X^2 + X + 1$ sobre $\mathbb{Q}$.

Ejercicios del capítulo 5

1.- $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{6})$.

2.- a) $E_f = \mathbb{Q}(i)$, $G = Gal_{\mathbb{Q}}(f) \simeq \mathbb{Z}_2$.

b) $[E_f : \mathbb{Q}] = 4$, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

c) $E_f = \mathbb{Q}\left(\sqrt[3]{2}, \xi\right)$ con ξ primitiva cúbica de 1, $\#G = 6$ y G no es abeliano.

3.- $X^4 + 1$ es irreducible en $\mathbb{Q}[X]$ y $E = \mathbb{Q}\left(\sqrt{2}, i\right)$ contiene dos subextensiones de grado 2 sobre $\mathbb{Q}$.

4.- a) Si ξ es raíz primitiva quinta de 1, $Irr(\xi, \mathbb{Q}) = X^4 + X^3 + X^2 + X + 1$ y $E = \mathbb{Q}(\xi)$; $\left\{1, \xi, \xi^2, \xi^3\right\}$ es $\mathbb{Q}$-base de E y el automorfismo $\sigma\colon E \to E$ definido por $\sigma(\xi) = \xi^2$ genera el grupo $G = Gal(E/\mathbb{Q})$.

b) σ^2 genera el único subgrupo propio de G cuyo cuerpo fijo $E^{\langle\sigma^2\rangle} = \mathbb{Q}\left(\xi^2 + \xi^3\right)$ es el único cuerpo estrictamente intermedio entre $\mathbb{Q}$ y E.

c) $Irr(\xi^2 + \xi^3, \mathbb{Q}) = X^2 + X - 1$ e $Irr(\xi, \mathbb{Q}(\xi^2 + \xi^3)) = X^2 + \left(1 + \xi^2 + \xi^3\right)X + 1$.

5.- $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Si σ es el automorfismo de E definido por $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ y $\sigma(i) = i$, entonces σ genera un subgrupo de orden 4. Si τ es el automorfismo de E dado por $\tau\left(\sqrt[4]{2}\right) = -\sqrt[4]{2}$ y $\tau(i) = i$, entonces $H := \{1, \sigma^2, \tau, \sigma^2\tau\}$ y $L := \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$

son también subgrupos de G de orden 4. Los cuerpos fijos correspondientes a estos tres subgrupos son $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(i\sqrt{2})$.

6.- a) $Irr(\xi,\mathbb{Q}) = X^6+X^5+\cdots+X+1$.
b) σ tiene período 6.
c) La G-órbita de $1+2(\xi+\xi^2+\xi^4)$ es $\left\{1+2(\xi+\xi^2+\xi^4), -\left[1+2(\xi+\xi^2+\xi^3)\right]\right\}$, y se aplica (5.6).

7.- $E=\mathbb{Q}\left(\sqrt[4]{2},i\right)$ y así $[E:\mathbb{Q}]=8$; $\alpha=i+\sqrt[4]{2}\in E$ y $\#(G-\textit{órbita de }\alpha) = \partial(Irr(\alpha,\mathbb{Q}) = [\mathbb{Q}(\alpha):\mathbb{Q}] \geqslant 5$ (5.6) que no puede ser divisor de 8. El Teorema del grado se aplica ahora.

8.-a) No. $E_f=\mathbb{Q}\left(\sqrt{2},i\sqrt{3}\right)$ y $[E_f:\mathbb{Q}]=4$.
b) Aplicación directa de la teoría.

9.- a) $\#G=20$.
b) Si ξ es raíz primitiva quinta de 1 entonces $\xi\in E_f$, cuerpo de escisión de f sobre $\mathbb{Q}$, $H=Gal(E_f,\mathbb{Q}(\xi))$ es de orden 5.
c) La torre $G\supset H\supset\{e\}$ es abeliana.
d) Si $\alpha=\sqrt[5]{2}$ la extensión $\mathbb{Q}(\alpha):\mathbb{Q}$ no es normal.
e) G es isomorfo a un subgrupo de S_5 que contiene un 5-ciclo.

10.- a) X^7-5 tiene un cero en E y no escinde en E.
b) E es cuerpo de escisión de $\left(X^2-2\right)\left(X^2+1\right)$ sobre $\mathbb{Q}\left(\sqrt[7]{5}\right); \left\{1,\sqrt{2},i,i\sqrt{2}\right\}$.
c) $G=\{id_E,\sigma,\tau,\gamma\}$ donde $\sigma\left(\sqrt{2}\right)=-\sqrt{2}, \sigma(i)=i, \tau\left(\sqrt{2}\right)=\sqrt{2}, \tau(i)=-i$, $\gamma\left(\sqrt{2}\right)=-\sqrt{2}$ y $\gamma(i)=-i$.
d) $-\sqrt{2}+5i$ pertenece a la G-órbita de $\sqrt{2}+5i$.

11.- a) $\Phi_8=X^4+1$. b) Falso. c) Falso.

12.- a) $\mathbb{Q}\subsetneq\mathbb{Q}\left(\xi^6\right)=\mathbb{Q}\left(\xi^3\right)\subsetneq\mathbb{Q}(\xi)$.
b) $Irr(\xi^2,\mathbb{Q}\left(\xi^6\right))=X^3-\xi^6$.

13.- Sea p un número primo. Demuéstrese que si r es un número natural entonces $\Phi_{p^r} = \Phi_p(X^{P^{r-1}})$.

14.- De $n=2k+1$ se obtiene que ξ^{-1} es un cuadrado en K. El resto es fácil.

15.- La primera afirmación es consecuencia directa del Teorema de Lagrange. Además U_n y U_m son subgrupos de U_{nm}, para los que es fácil demostrar que la aplicación $\Psi\colon U_nU_m\to U_n\times U_m$ definida por $\varphi(xy)=(x,y)$ es isomorfismo de grupos.

16.- ξ_{rs}^r es raíz primitiva s-ésima de 1 si r y s son primos entre si y, entonces, $\mathbb{Q}(\xi_n)$,$\mathbb{Q}(\xi_m)\subset\mathbb{Q}(\xi_{nm})$. Por otra parte, $\xi_n\xi_m$ es primitiva nm-ésima y eso proporciona $\mathbb{Q}(\xi_{nm})\subset\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m)$. La segunda afirmación resulta de la igualdad $\varphi(nm)=\varphi(n)\varphi(m)$, donde φ es el indicador de Euler, y de contar los grados de las extensiones implicadas.

Bibliografía

[1] COHN,P. *Algebra* (vol 1 y 2). Wiley (1984, 1989).

[2] CASTELLET, M. & LLERENA, I. Álgebra Lineal y Geometría. Ed. Reverté S.A. UAB. (1991).

[3] COX, D. A. Galois Theory. Wiley (2004).

[4] DELGADO, F.; FUERTES,C.; XAMBÓ, S. Introducción al Álgebra: Anillos, Factorización y Teoría de cuerpos. Secretariado de Publicaciones e Intercambio Científico. Univ. Valladolid (1998).

[5] DUMMIT, D.S. Abstrac Algebra.Wiley (1999).

[6] ESCOFIER, J.P. Galois Theory. GTM 204 Springer (2000).

[7] FENRICK, M.H. Introduction to the Galois Correspondence. Birkhäuser (1992).

[8] GARLING, D.J.H. A Course in Galois Theory. Cambridge Univ. Press (1986).

[9] HARDY, G.M. y WRIGHT, E.M. An intruduction to the theory of numbers. Oxford at the Clarendon Press (1959).

[10] LANG, S. Algebra. Addison-Wesley (1993).

[11] NAVARRO, G. Un curso de Álgebra. Universitat de Valencia (2002).

[12] ROTMAN, J. Galois Theory. Springer-Verlag (1990).

[13] ROWEN, L. Algebra. Groups rings, and fields. AK Peters (1994).

[14] STEWART, I. Galois Theory. Chapman and Hall Mathematics (1980).