Teoría de Galois

por
José Antonio Belinchón

Última actualización Julio 2008

Índice general

Prólogo

La idea fundamental de esta notas confecionadas a modo de resumen (personal) es la de tener a mano un recordatorio de por donde iban los tiros. Sólo se demuestran los teoremas fundamentales y se acompoña el texto con una serie de ejercios más o menos trabajados. En modo alguno pretenden sustituir (porque es implosible) los manuales clásicos o las notas de clase de un profesor. Es decir, estas notas estan confeccionadas a modo de refrito entre las notas de clase y de distintos libros clásicos como los siguientes:

1. Ian Stewart. Galois Theory. Chapman & Hall. 2004.
2. J. M. Howie. Fields and Galois Theory. Springer. 2006.
3. T.S. Blyth and E.F. Robertson. Algebra through the practice. Cambridge University Press 2001.
4. J. B. Fraleigh. Álgebra Abstracta. Addison-Wesley. 1987.
5. S. Xambó et al. Introducción al Álgebra, I, II, III. UCM (1993) U. Valladolid (2001).

todo ello aderezado (como he indicado antes) con una serie de ejemplos (ejercicios donde se aplica de forma inmediata los conceptos teóricos expuestos) desarrollados (eso espero) al final de cada capitulillo (todos ellos muy sencillos).

ADVERTENCIA: No están concluidas y es muy posible que hayan sobrevivido numerosas erratas. Toda observación en este sentido es bien recibida.

Capítulo 1

Anillos y cuerpos

1.1. Anillos

Definición **1.1.1** *Un **anillo** es un conjunto R junto con dos operaciones $+$ y $\cdot$, $(R, +, \cdot)$, que verifican las siguientes condiciones:*

1. *$(R, +)$ es un grupo abeliano;*
2. *$\cdot$ es una operación asociativa;*
3. *la operación $\cdot$ es distributiva con respecto a $+$, es decir, $\forall x, y, z \in R$, se cumplen*

$$(x + y)z = xz + yz, \qquad z(x + y) = zx + zy.$$

Si la operación $\cdot$ es conmutativa, el anillo se llama conmutativo. Se dice que un **anillo es unitario** si la operación $\cdot$ posee un elemento neutro. Normalmente usamos 1 o 1_R para el elemento neutro. El elemento neutro con respecto a la suma se denota 0_R o 0 si está claro de que anillo se trata.

Ejemplo 1.1.1 *1. Los siguientes sistemas algebraicos son anillos: $(\mathbb{Z}, +, \cdot)$, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.*

2. *$\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con las operaciones estándar.*
3. *Si R es un anillo entonces las matrices $M_n(R)$ sobre este anillo también lo es.*
4. *$(\mathbb{N}, +, \cdot)$, $(\mathbb{R}_{\geq 0}, +, \cdot)$ **no** son anillos.*

Lema **1.1.1** *Sea R un anillo, entonces*

1. *para cualquier $r \in R$ tenemos $r \cdot 0 = 0 \cdot r = 0$;*
2. *para todo r y $s \in R$ se cumple $(-r) \cdot s = -(r \cdot s)$.*

Subanillos

El mayor objetivo de la teoría de anillos es la clasificación de todos los anillos. Es claro que en general este problema es muy difícil o probablemente imposible. Pero es posible clasificar algunas familias de anillos bajo unas restricciones. Es razonable pensar que primero podemos clasificar los anillos más pequeños y a partir de ellos los más grandes. Esto nos motiva a dar la siguiente definición

Definición 1.1.2 *Sea R un anillo. Se dice que un subconjunto S de R es un* ***subanillo*** *si S es un subgrupo de $(R,+)$ y para todo s_1 y $s_2 \in S$ tenemos que $s_1 s_2 \in S$.*

Ejemplo 1.1.2 *1. $\mathbb{Z}$ y $\mathbb{Q}$ son subanillos de $\mathbb{R}$, $\mathbb{R}$ y $\mathbb{Z}[i]$ son subanillos de $\mathbb{C}$.*

2. $\mathbb{N}$ y $\mathbb{R}^* = \{r \in R \mid r \neq 0\}$ no son subanillos de $\mathbb{R}$.

Ideales

Los subanillos en un anillo juegan el papel de subgrupos en un grupo. En la teoría de grupos se introduce también el concepto de un subgrupo normal. Este concepto está relacionado con grupos cocientes y homomorfismos de grupos. En la teoría de anillos una noción análoga a un subgrupo normal es un ideal.

Definición 1.1.3 *Sea R un anillo. Se dice que un subconjunto I de R, $I \lhd R$, es un* ***ideal*** *si I es un subgrupo de $(R,+)$ y para todo $r \in R$ y $m \in I$ tenemos que $rm, mr \in I$.*

Ejemplo 1.1.3 *1. Sean $R = \mathbb{Z}$ e $I = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Entonces I es un ideal de R.*

2. De la definición de ideal vemos que un ideal es también un subanillo. No es cierta la implicación inversa. Por ejemplo, $\mathbb{Z}$ no es un ideal de $\mathbb{Q}$.

3. Sea R un anillo cualquiera. Entonces en R siempre hay dos ideales: uno es $\{0\}$ que consta únicamente del elemento 0 y el otro es R que contiene a todos los elementos de R.

4. $I = \{$números pares$\}$ es un ideal de $\mathbb{Z}$.

5. $I = \langle d \rangle = \{$múltiplos de $d\}$ es un ideal de $\mathbb{Z}$.

Ahora tratemos de justificar la aparición del concepto de ideal. Como en la teoría de grupos, los subgrupos normales ayudan a construir nuevos grupos, de la misma forma a partir de los ideales construimos nuevos anillos.

Supongamos que I es un ideal de un anillo R. Como $(R,+)$ es un grupo abeliano, I es un subgrupo normal del grupo aditivo $(R,+)$. Esto nos permite considerar el grupo cociente R/I. Recordemos este concepto. Si A y B son dos subconjuntos de R, entonces el conjunto $A+B$ es el conjunto $\{a+b \mid a \in A, b \in B\}$. Si A consiste solamente de un elemento, a. escribimos simplemente $a+B$. Si I es un ideal de R y $r_1, r_2 \in R$, entonces se comprueba que los conjuntos r_1+I y r_2+I tienen una intersección no vacía si y sólo si son iguales. Esto nos da una partición de $R = \cup_{r \in R}(r+I)$. Definamos **anillo cociente** R/I como el conjunto de subconjuntos de R : $R/I = \{r+I \mid r \in R\}$.

La suma en R/I está definida como suma de conjuntos. Resulta que $(r+I)+(s+I)$ es también un elemento de R/I y es igual a $(r+s)+I$. El elemento neutro respecto a esta operación es $0+I=I$ y el inverso de $r+I$ es $-r+I$. Ahora definamos la estructura de un anillo sobre R/I. Para este propósito tenemos que definir la multiplicación. La definimos de la siguiente forma:

$$(r+I)\cdot(s+I)=(rs)+I, \text{ con } r+I \text{ y } s+I \in R/I.$$

Teorema 1.1.1 *La definición de la multiplicación no depende de la elección de los representantes r, s, es decir si $r+I=r'+I$ y $s+I=s'+I$, entonces $(rs)+I=(r's')+I$.*

Con las operaciones anteriormente definidas $(R/I,+,\cdot)$ es un anillo.

Observación 1.1.1 *Si A y B son dos subconjuntos de R definamos por AB el conjunto $\{ab \mid a\in A, b\in B\}$. Entonces el primer apartado del teorema anterior es también una consecuencia de que el producto de conjuntos*

$$(r+I)(s+I)$$

está contenido en $(rs)+I$ por ser I ideal.

Ejemplo 1.1.4 *Sea $R=\mathbb{Z}$ e $I=6\mathbb{Z}$. Entonces el anillo $R/I=\mathbb{Z}/6\mathbb{Z}$ tiene 6 elementos*

$$\{\bar{0}=6\mathbb{Z}, \bar{1}=1+6\mathbb{Z}, \bar{2}=2+6\mathbb{Z}, \bar{3}=3+6\mathbb{Z}, \bar{4}=4+6\mathbb{Z}, \bar{5}=5+6\mathbb{Z}\}.$$

Si multiplicamos $\bar{4}$ por $\bar{5}$, obtenemos la clase $20+6\mathbb{Z}$ que es igual a $\bar{2}$. La multiplicación de $\bar{3}$ por $\bar{4}$ nos da $\bar{0}$.

Definición 1.1.4 *Sean R y S dos anillos. Un* ***homomorfismo de anillos*** *es una aplicación $f: R\to S$ tal que*

$$f(x+y)=f(x)+f(y), \qquad f(xy)=f(x)f(y),$$

para todo $x, y\in R$.

Si la operación f es biyectiva, entonces f se llama **isomorfismo** y diremos que los anillos R y S son isomorfos. Lo vamos a denotar como $R\cong S$. Si, además R coincide con S, entonces esta aplicación se llama **automorfismo**.

El conjunto de elementos r de R, tales que $f(r)=0$ se llama **núcleo de** f y se denota por $\ker f$. El conjunto de elementos de S, $\{s\in S \mid \exists r\in R, s=f(r)\}$ se llama la **imagen de** f y se denota por $\operatorname{Im} f$.

Ejemplo 1.1.5

1. *Sea $R=\mathbb{Z}[x]$ y $S=\mathbb{Z}$. Definamos $f: R\to S$ de la siguiente forma: $f(p(x))=p(7)$, donde $p(7)$ significa la sustitución de x por 7 en el polinomio $p(x)$. Entonces f es un homomorfismo. El núcleo de f es igual a los polinomios de $\mathbb{Z}[x]$ que tienen 7 como una raíz y la imagen de f es todo $\mathbb{Z}$.*
2. *Sea R un anillo e I un ideal de R. Pongamos $S=R/I$, entonces la aplicación $f: R\to S$ definida como $f(r)=r+I$ es un homomorfismo de anillos.*

Lema 1.1.2 *Sean R y S anillos y $f: R\to S$ un isomorfismo de anillos, entonces $f(1_R)$ es un elemento neutro de S. En particular, como hay solamente un elemento neutro, $1_S=f(1_R)$.*

A la hora de clasificar los anillos no distinguimos entre anillos isomorfos. Si queremos demostrar que dos anillos no son isomorfos, tenemos que encontrar una propiedad que se conserva bajo isomorfismo y ver que un anillo la posee y el otro no.

Ejemplo 1.1.6 *Demostrar que $\mathbb{R}$ y $\mathbb{C}$ no son isomorfos como anillos. Para eso vemos que la propiedad de un anillo de tener un elemento a tal que $a^2 = -1$ se conserva bajo isomorfismo. En efecto, sean R y S anillos y $f : R \to S$ un isomorfismo de anillos. Supongamos que $a \in R$ y $a2 = 1_R$. Pongamos $b = f(a)$. Entonces*

$$b^2 = f(a)^2 = f(a^2) = f(-1_R) = -f(1_R) = -1_S.$$

Como $\mathbb{C}$ posee un elemento que elevado al cuadrado es -1 y $\mathbb{R}$ no lo posee, y esta propiedad se conserva bajo isomorfismo, estos dos anillos no pueden ser isomorfos.

Teorema 1.1.2 ***(El primer teorema de isomorfía para anillos)***. *Sea $f : R \to S$ un homomorfismo de anillos. Entonces, $Ker f = \{x \in R \mid f(x) = 0\}$ es un ideal de R, $Im f$ es un subanillo de S y $R/Ker f \cong Im f$.*

Ejemplo 1.1.7 *Sea $R = \mathbb{Z}[x]$ e $I = \{p(x) \in R \mid p(2) = 0\}$. Entonces I es un ideal de R y $R/I \cong Z$ por el primer teorema de isomorfía. El isomorfismo explícito entre R/I y $\mathbb{Z}$ está dado mediante la aplicación*

$$g(p(x) + I) = p(2).$$

Para entender bien la estructura y propiedades de un anillo es muy importante conocer sus ideales. En el siguiente resultado damos la descripción de los ideales de R/I a partir de los ideales de R.

Teorema 1.1.3 *Sea R un anillo e I un ideal de R.*

1. *Si J es un ideal de R con $I \subseteq J$ definamos $J/I = \{x + I \mid x \in J\}$. Entonces, J/I es un ideal de R/I. Además, si K es otro ideal de R con $I \subseteq K$, tenemos que $K = J$ si y sólo si $K/I = J/I$.*
2. *Sea L un ideal de R/I y sea $J = \{x \in R \mid x + I \in L\}$. Entonces, J es un ideal de R que contiene a I y $J/I = L$.*

Ejemplo 1.1.8 *Sea $R = \mathbb{Z}/6\mathbb{Z}$. Entonces $I = 2\mathbb{Z}$ es un ideal de $\mathbb{Z}$ que contiene a $6\mathbb{Z}$. Entonces $2\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{2}, \bar{4}\}$ es un ideal de $\mathbb{Z}/6\mathbb{Z}$.*

Definición 1.1.5 *Sea R un anillo y $x \in R$. El **ideal** (x) generado solamente por un elemento x se llama **principal**.*

*Si todos los ideales de R son principales, entonces decimos que R es un **anillo de ideales principales.***

Teorema **1.1.4** *El anillo $\mathbb{Z}$ es un anillo de ideales principales.*

Definición **1.1.6** *Sean a y b dos números enteros no nulos. Digamos que un número positivo c es el* ***máxino común divisor*** *de a y b si*

1. *c divide a a y b;*
2. *c es el máximo entre los números positivos que cumplen esta propiedad.*

Escribiremos (a, b) para denotar el máxino común divisor de a y b.

Ahora podemos reformular la **identidad de Bezout**.

Teorema **1.1.5** *Sean a y b dos números enteros no nulos y $c = (a, b)$. Entonces c genera el ideal generado por a y b; en particular, existen m y $n \in \mathbb{Z}$ tales que $c = na + mb$.*

Ejemplo 1.1.9 *Generadores de ideales.*

En $\mathbb{Z}$, $(2, 5) = (1)$, identidad de Bezout.

Los ideales de $\mathbb{Z}_4$ son

$$I_1 = \{0\}, \qquad I_2 = \{0, 2\}, \qquad I_2 = \mathbb{Z}_4$$

Definición **1.1.7** *Se dice que un* ***ideal*** *I de un anillo R es* ***maximal*** *si $I \neq R$ y no existe ningún ideal J distinto de I y R tal que $I \subset J$.*

Ejemplo 1.1.10 *El ideal $I = (6, 10) = (2) \subset \mathbb{Z}$ es principal.*

$I = (2)$ es maximal porque si intentamos "añadir" un número impar, $2n + 1$, a I entonces también debería estar $(2n + 1) + (-n) \cdot 2 = 1$ y por tanto todo $\mathbb{Z}$.

$I = (9)$ es principal pero no es maximal ya que $I \subsetneq J = (3) \subsetneq \mathbb{Z}$.

Observación 1.1.2 *El anillo $\mathbb{Z}/n\mathbb{Z}$ lo vamos a denotar por $\mathbb{Z}_n$. Cuando n es un número primo usaremos también $\mathbb{F}_p$ para denotar $\mathbb{Z}/p\mathbb{Z}$, en particular se trata de un campo.*

En $\mathbb{Z}$ todos los ideales $I = (p)$ son pincipales y si p es primo entonces es maximal.

Ejemplo 1.1.11 *El ideal* $I = \left(2, 1+\sqrt{-5}\right)$ *es maximal en* $\mathbb{Z}\left[\sqrt{-5}\right]$ *pero no principal ya que si*

$$\alpha = a + b\sqrt{-5} \notin I$$

entonces $(a-b)$ *es impar, ya que de otra forma*

$$\alpha = \frac{2(a-b)}{2+b\left(1+\sqrt{-5}\right)} \in I,$$

pero si $(a-b)$ *es impar entonces*

$$1 = \frac{2(a-b+1)}{2+b\left(1+\sqrt{-5}\right)} + (-1)\,\alpha$$

entonces

$$\left(2, 1+\sqrt{-5}, \alpha\right) = (1) = A$$

es maximal.

Veamos ahora que no es principal en $\mathbb{Z}\left[\sqrt{-5}\right]$. *Si* $I = \langle\alpha\rangle$ *con* $\alpha = a + b\sqrt{-5}$, *entonces* $2 = \alpha\beta$ *y* $1+\sqrt{-5} = \alpha\gamma$ *para ciertos* $\beta, \gamma \in A$. *Multiplicando estas igualdades por sus conjugadas se tiene que* $a^2 + 5b^2$ *debe dividir a* 4 *y a* 6. *Esto sólo deja las posibilidades* $a = \pm 2; b = 0$ *y* $a = \pm 1; b = 0$.

El primer caso es imposible porque $1+\sqrt{-5}$ *no es un múltiplo de* 2. *El segundo caso sólo se daría si* $I = A$, *y esto no es cierto porque no es difícil ver que si* $x + y\sqrt{-5} \in A$ *es múltiplo de* 2 *o de* $1+\sqrt{-5}$ *entonces* x *e* y *tienen la misma paridad.*

1.2. Cuerpos

Definición **1.2.1** *Sea* R *un anillo unitario. Digamos que* r *es una* ***unidad*** *si existe un elemento* $s \in R$ *tal que* $rs = sr = 1$.

El conjunto de unidades de R *lo denotamos por* $U(R)$.

Lema **1.2.1** *Sea* R *un anillo unitario. El conjunto* $U(R)$ *es un grupo con respecto a la multiplicación.*

Observación 1.2.1 *Si* R *es un anillo unitario y* $1 = 0$, *entonces* R *consta sólo de un elemento.*

Un ***anillo*** *así se llama* ***trivial***. *En adelante siempre suponemos que los anillos considerados no son triviales. En este caso* $0 \notin U(R)$.

Ejemplo 1.2.1 *Las unidades de* $\mathbb{Z}$ *son* 1 *y* -1. *Entonces* $U(\mathbb{Z})$ *es isomorfo a* C_2 *el grupo cíclico de orden* 2.

Las unidades de $\mathbb{Z}[i]$ *son* $1, -1, i, -i$. *Entonces* $U(\mathbb{Z}[i])$ *es isomorfo a* C_4.

Lema **1.2.2** *Sea* R *un anillo unitario conmutativo. Entonces* $a \in U(R)$ *si y sólo si* $(a) = R$.

Cuerpo

Definición 1.2.2 *Un **cuerpo** es un anillo conmutativo y unitario (no trivial) K tal que $U(K) = K\backslash\{0\} = K^*$.*

En el siguiente resultado damos una caracterización de cuerpos a través de la descripción de sus ideales.

Teorema 1.2.1 *Un anillo conmutativo unitario no trivial R es un cuerpo si y sólo si los únicos ideales de R son $\{0\}$ y R.*

Corolario 1.2.1 *Sea R un anillo conmutativo y unitario y sea I un ideal de R. Entonces I es un ideal maximal si y sólo si el anillo cociente R/I es un cuerpo.*

Ejemplo 1.2.2 *Hemos visto que los ideales maximales de $\mathbb{Z}$ son de la forma $(p) = p\mathbb{Z}$, con p primo. Del último resultado se obtiene que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ es un cuerpo*

Definición 1.2.3 *Sea R un anillo. Se dice que un elemento $r \in R$ no nulo es un **divisor de cero** si existe $0 \neq y \in R$ tal que $xy = 0$.*

*Un **dominio de integridad** (DI) es un anillo conmutativo y unitario sin divisores de cero.*

*Un **ideal I es primo** si R/I no tiene divisores de cero.*

Ejemplo 1.2.3

1. *En $\mathbb{Z}_6$*
$$2 \cdot 3 = 6 = 0$$
pero $2 \neq 0$, y $3 \neq 0$. En este caso el 2 y el 3 son divisores de 0. Por lo tanto $\mathbb{Z}_6$, es un anillo conmutativo pero no es un dominio de integridad.
2. *Si R es un anillo no trivial, una unidad nunca es un divisor de cero y, por lo tanto, cualquier cuerpo es un dominio de integridad.*
3. *$\mathbb{Z}$ es un anillo conmutativo con unidad, de hecho un dominio de integridad.*
4. *$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ es un dominio de integridad.*
5. *Los enteros pares (divisibles por dos, negativos incluidos) conforman un anillo conmutativo pero no un anillo con unidad.*

Definición 1.2.4 *Sea F un cuerpo. Un **subcuerpo** de F es un subconjunto $K \subseteq F$ que, con las operaciones de F, tiene estructura de cuerpo no trivial.*

Tiene especial interés el caso $S = \{\emptyset\}$, es decir, el cuerpo que es igual a la intersección de todos los subcuerpos de K. Claramente este subcuerpo no es vacío porque por la definición de subcuerpo contiene $\{0, 1\}$.

Definición **1.2.5** *Sea K un cuerpo. Se llama* ***subcuerpo primo*** *de K a la intersección de todos los subcuerpos de K.*

Consideremos ahora el cuerpo $\mathbb{F}_p$. Es un cuerpo con un número finito de elementos. Vemos que en $\mathbb{F}_p$ se cumple que $1+...p\text{-veces....}+1 = 0$. Esta propiedad es tan importante a la hora de clasificar los cuerpos que requiere una definición especial.

Definición **1.2.6** *Diremos que un cuerpo tiene* ***característica*** *n si n es el menor número natural tal que $1+\cdots n\ veces\cdots+1 = 0$. Si esta suma fuera siempre distinta de cero se dice que el cuerpo tiene* ***característica cero****.*

Así por ejemplo $\mathbb{R}$ y $\mathbb{Q}$ tienen característica cero y $\mathbb{F}_p$ tiene característica p. En adelante vamos a usar la siguiente notación: si R es un anillo, $a \in R$ y $n \in \mathbb{N}$, vamos a escribir na para denotar $a+\cdots n-veces\cdots+a$. Es claro que se cumplen las siguientes propiedades:

$$(nm)a = n(ma), \qquad n(a+b) = na+nb, \qquad (n+m)a = na+mb,$$

con $a, b \in R$,y $n, m \in \mathbb{N}$.

Definición **1.2.7** *Un* ***homomorfismo de cuerpos*** *es un homomorfismo de anillos entre dos cuerpos con una imagen no trivial. Un isomorfismo de cuerpos es un homomorfismo de cuerpos biyectivo.*

Hemos visto que la imagen de un homomorfismo de anillos es siempre un subanillo. En el caso de homomorfismos de cuerpos, la imagen es un subcuerpo.

Teorema **1.2.2** *Sea K un cuerpo. Entonces la característica de K es cero o un número primo p. En el primer caso el subcuerpo primo de K es isomorfo a $\mathbb{Q}$ y en el segundo, isomorfo a $\mathbb{F}_p$.*

Supongamos que K es un cuerpo y $R \subseteq K$ es un subanillo de K con $1 \in R$ (por ejemplo, $\mathbb{R} = \mathbb{Z}$ y $\mathbb{K} = \mathbb{R}$). Evidentemente, $\mathbb{R}$ es un dominio de integridad. Naturalmente, si $0 \neq x \in R$, el inverso de x, $x-1$ (que sabemos existe y está en K), no tiene por qué ser un elemento de R, por lo que tiene sentido plantearse cuál es el menor subcuerpo de K que contiene a R.

Teorema **1.2.3** *El menor subcuerpo de K que contiene un subanillo R de K es el conjunto*

$$\{xy^{-1} \mid x, y \in R, y \neq 0\}.$$

Ejemplo 1.2.4

1. *$\mathbb{Z} \subset \mathbb{R}$., el menor subcuerpo en R que contiene a $\mathbb{Z}$ es $\mathbb{Q}$.*
2. *$\mathbb{Z}[i] \subset \mathbb{C}$, el menor subcuerpo en $\mathbb{C}$ que contiene a $\mathbb{Z}[i]$ es $\mathbb{Q}[i]$.*

Teorema **1.2.4** *Sea R un dominio de integridad y K el cuerpo de cocientes de R construido antes. Si F es otro cuerpo arbitrario con $R \subseteq F$, entonces el menor subcuerpo de F que contiene a R es isomorfo a K.*

Definición **1.2.8** *Sea F/K una* ***extensión*** *y $S \subseteq F$. Llamaremos* ***adjunción*** *de S a K el menor subcuerpo de F que contiene a K y a S. Lo denotaremos $K(S)$. Si $S = \{u_1, \cdots, u_n\}$ es un subconjunto finito de F, escribiremos simplemente, $K(u_1, \cdots, u_n)$. También vamos a decir que el subcuerpo $K(S)$ está generado por S sobre K.*

Observación 1.2.2 *1. Evidentemente $K(S)$ es la intersección de todos los subcuerpos de F que contienen a K y a S.*

2. Si $S \subseteq F$, el subcuerpo de F generado por S coincide con $P(S)$, donde P es el subcuerpo primo de F.

3. $K(S \cup T) = K(S)(T) = K(T)(S)$.

1.3. Dominios de factorización única

Definición 1.3.1 *Se dice que R (DI) es un **dominio de factorización única** (DFU) si todo elemento de $R - \{0\} = R^*$, que no sea una unidad se puede expresar como un producto de factores irreducibles de forma única salvo el orden de los factores y el empleo de irreducibles asociados.*

Ejemplo 1.3.1 *1. $\mathbb{Z}$ es un DFU.*

2. $\mathbb{Z}\left[\sqrt{-5}\right]$ no es un dominio de factorización única, ya que por ejemplo

$$2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right).$$

Comprobar que los factores de esta doble factorización son realmente irreducibles conlleva algunos cálculos. Si fuera

$$2 = (x + y\sqrt{-5})(u + v\sqrt{-5}),$$

multiplicando por el conjugado se tendría

$$4 = (x^2 + 5y^2)(u^2 + 5v^2),$$

y evidentemente esto sólo es posible si $y = v = 0$, y se tiene $x + y\sqrt{-5} = \pm 1$ o $u + v\sqrt{-5} = \pm 1$.
La misma demostración sirve para 3. Análogamente

$$1 \pm \sqrt{-5} = (x + y\sqrt{-5})(u + v\sqrt{-5}),$$

implica

$$6 = (x^2 + 5y^2)(u^2 + 5v^2),$$

y la única posibilidad, salvo intercambiar x e y por u y v, es $x = \pm 1$, $y = \pm 1$, $u = \pm 1$, $v = 0$.

3. $\mathbb{Z}\left[\sqrt{-3}\right]$ tampoco es un dominio de factorización única ya que por ejemplo

$$2 \cdot 2 = \left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right).$$

4. El anillo $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ es DFU, de hecho es DE.
Observar que

$$\left(\frac{1 + \sqrt{-3}}{2}\right)^2 = \frac{1}{2}\left(-1 + \sqrt{-3}\right),$$

y por lo tanto podemos deducir que

$$\mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right] = \left\{a + \frac{b}{2}\left(1 + \sqrt{-3}\right) : a, b \in \mathbb{Z}\right\}.$$

Definición **1.3.2** *Sea R un dominio de integridad y supongamos que existe una aplicación $g : R^* \to \mathbb{N}$ con las siguientes propiedades:*

1. *Para todo $a \neq 0$ y $b \neq 0$ de R se cumple $g(ab) \geq g(a)$,*
2. *(La propiedad de división) Para todo $a \neq 0$ y b de R existen q y $r \in R$ tal que $b = qa + r$, con $r = 0$ ó $g(r) < g(a)$.*

Entonces R es un ***dominio euclídeo*** *(DE).*

En $\mathbb{Z}$ la función g está definida como $g(z) = |z|$. Análogamente como en el caso de los números enteros obtenemos

Teorema **1.3.1** *Un dominio euclídeo es un dominio de ideales principales (es decir, cualquier ideal es principal).*

$$DE \Longrightarrow DIP \Longrightarrow DFU.$$

Teorema **1.3.2** *El anillo de enteros de Gauss $\mathbb{Z}[i]$ es un dominio euclídeo.*

Dos elementos a y b de un anillo de ideales principales R generan un ideal (a, b). Este ideal que también es principal está generado, por ejemplo, por d (notemos que la elección de d no es única). Como a y b están en (d), vemos que existen g y h tales que $a = gd$ y $b = hd$ y, por lo tanto, d es un divisor común de a y b. Es fácil comprobar que para cualquier otro divisor común e de a y b, existe f tal que $d = fe$. Por eso, decimos que d es el máximo común divisor de a y b.

Vamos a describir ahora como se puede usar la propiedad de división para buscar el máximo común divisor de dos elementos. Supongamos que tenemos dos elementos a_0 y a_1, y sea $g(a_1) \leq g(a_0)$. Usando la propiedad de división obtenemos

$$a_0 = q_1 a_1 + a_2,$$

donde $a_2 = 0$ ó $g(a_2) < g(a_1)$. Si $a_2 \neq 0$ seguimos dividiendo:

$$a_1 = q_2 a_2 + a_3.$$

De esta forma obtenemos a_i y q_i hasta que $a_{s-1} = q_s a_s$.. El proceso anterior se puede invertir y calcular e y f tales que $a_s = ea_0 + fa_1$. Este proceso se llama el **algoritmo de Euclides**.

Si p es un número primo en el anillo de los números enteros, entonces tenemos las siguientes descomposiciones de p:

$$p = p \cdot 1 = (-p) \cdot (-1).$$

Sin embargo, en esta situación uno de los factores es una unidad de $\mathbb{Z}$. Si consideramos una situación más general, donde R es un dominio de integridad y u es una unidad de R y a es un elemento arbitrario, entonces podemos descomponer a de la siguiente forma:

$$a = a \cdot u \cdot u^{-1}.$$

Este tipo de descomposiciones, donde uno de los factores es una unidad se llama trivial.

Definición **1.3.3** *Un elemento p que solamente tiene descomposiciones triviales se llama simple o* ***irreducible****.*

A los elementos a y $b = a \cdot u$ que sólo difieren en multiplicación por una unidad u les llamaremos asociados. Antes hemos definido la noción de un ideal maximal. En los dominios de ideales principales este término está relacionado con elementos irreducibles.

Lema 1.3.1 *Sea R un dominio de ideales principales y $a \in R$. Entonces (a) es un ideal maximal si y sólo si a es un elemento primo.*

Corolario 1.3.1 *Sea R un dominio de ideales principales y $a \in R$. Supongamos que $a = bc$ y un elemento irreducible p divide a a. Entonces p divide a b o p divide a c.*

Definición 1.3.4 *Si c es un divisor de a, es decir existe $d \in R$ tal que $a = cd$, pero a y c no son asociados (d no es una unidad), entonces vamos a decir que c es un **divisor propio** de a.*

Lema 1.3.2 *Sea R un dominio euclídeo con la función g. Si c es un divisor propio de a, entonces $g(c) < g(a)$.*

Teorema 1.3.3 *Sea R un anillo euclídeo y $0 \neq a \in R$. Entonces, existe una única descomposicción de a como un producto de elementos primos: $a = p_1 \cdots p_r$. (Única en el siguiente sentido: si existen dos descomposiciones $p_1 \cdots p_n = q_1 \cdots q_m$, entonces $m = n$ y existe una permutación de $\{1, \cdots, n\}$ tal que p_i y $q_{\sigma(i)}$ son asociados para todo i).*

1.4. Anillo de polinomios

Definición 1.4.1 *Sea R un anillo y $P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ con $a \neq 0$. Diremos que P tiene **grado** n y escribiremos* $\operatorname{grad} P = n$. *Si $P = 0$ escribiremos formalmente* $\operatorname{grad} P = 0$.

Lema 1.4.1 *Si R es un dominio de integridad, $R[x]$ también lo es. Además si $P, Q \in R[x]$*

1. $\operatorname{grad}(P + Q) \leq \operatorname{máx}(\operatorname{grad} P, \operatorname{grad} Q)$,
2. $\operatorname{grad}(PQ) = \operatorname{grad} P + \operatorname{grad} Q$.

Lema 1.4.2 *Si K es un cuerpo, $K[x]$ es un dominio euclídeo. Más concretamente, si P y $Q \in K[x]$ con $Q \neq 0$, entonces existen dos polinomios C y R tales que $P = QC + R$ con* $\operatorname{grad} R < \operatorname{grad} Q$.

Corolario 1.4.1 *Si K es un cuerpo, $K[x]$ es un dominio de ideales principales. Todo polinomio de $K[x]$ se puede descomponer como producto de polinomios irreducibles, además esta descomposición es única salvo el orden de los factores y multiplicación por elementos de $K \setminus \{0\}$.*

Lema 1.4.3 *Sea K un cuerpo y a y $b \in K$. Entonces los polinomios $x - a$ y $x - b$ están asociados en $K[x]$ si y sólo si $a = b$.*

Teorema 1.4.1 *Sea K un cuerpo y $P \in K[x]$ un polinomio de grado n. Entonces P tiene como máximo n raíces.*

Ahora fijémonos en los polinomios sobre $\mathbb{Z}$ y $\mathbb{Q}$. El primer resultado es un lema de Gauss que, en realidad, puede ser generalizado fácilmente sobre dominios de factorización única.

Lema 1.4.4 ***(de Gauss)*** *Sea P un polinomio sobre $\mathbb{Z}$ de grado positivo. Si P es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$.*

Ahora vamos a ver algunos criterios de irreducibilidad.

Teorema 1.4.2 ***(Criterio de Eisenstein)*** *Sea $P \in \mathbb{Z}[x]$, $P = a_n x^n + \cdots + a_0$, con $a_n \neq 0$. Supongamos que existe un número primo p tal que $p \mid a_j$ para todo $0 \leq j \leq n-1$, $p \not| a_n$ y $p^2 \not| a_0$. Entonces, P es irreducible en $\mathbb{Q}[x]$.*

Ejemplo 1.4.1 *$P = x^5 - 2x + 6$ es irreducible en $\mathbb{Q}[x]$, basta tomar $p = 2$.*

$Q = x^7 - 12$ es irreducible en $\mathbb{Q}[x]$, basta tomar $p = 3$.

Teorema 1.4.3 *Sea $P \in \mathbb{Z}[x]$ un polinomio mónico y $\bar{P} \in \mathbb{F}_p[x]$ el polinomio que resulta al reducir los coeficientes módulo p. Si $\bar{P}$ es irreducible en $\mathbb{F}_p[x]$, entonces P es irreducible en $\mathbb{Q}[x]$.*

Ejemplo 1.4.2 *$P = x^3 - 17x^2 + 10x + 105$ es irreducible en $\mathbb{Q}[x]$, ya que al tomar $\bmod 2$ obtenemos $x^3 + x^2 + 1$ y si este polinomio se pudiera descomponer en $\mathbb{Z}_2[x]$ se podría escribir como $(x^2 + ax + b)(x - c)$, lo cual es imposible porque ni x ni $x - 1$ dividen a $x^3 + x^2 + 1$.*

1.5. Ejercicios

Estructuras algebraicas.

Ejercicio 1.5.1 *Demostrar que:*

Solución.

1. $\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$ es un anillo
   Tenemos que comprobar toda la ristra de propiedades i.e.:
   $\left(\mathbb{Z}\left[\sqrt{3}\right], +\right)$ es grupo abeliano, i.e. definimos

   $$x = a_1 + b_1\sqrt{3}, \qquad y = a_2 + b_2\sqrt{3},$$

   tal que

   $$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{3},$$

   y comprobamos que verifica las propiedades
   Asociativa,

Elemento neutro, i.e. $\exists e$ tal que $\left(a+b\sqrt{3}\right)+e=a+b\sqrt{3}$, por lo que $e=0\in\left(\mathbb{Z}\left[\sqrt{3}\right],+\right)$

Elemento inverso, i.e. $\exists x$ tal que $\left(a+b\sqrt{3}\right)+x=e=0$, por lo que $x=-\left(a+b\sqrt{3}\right)\in\left(\mathbb{Z}\left[\sqrt{3}\right],+\right)$

Conmutativa, i.e. $x+y=y+x$.

De igual forma deberemos probar que $\left(\mathbb{Z}\left[\sqrt{3}\right],\cdot\right)$ es asociativa y por último

La operación $\cdot$ es distributiva con respecto a $+$, es decir, $\forall x,y,z\in\mathbb{Z}\left[\sqrt{3}\right]$, se cumplen

$$(x+y)z=xz+yz,\qquad z(x+y)=zx+zy.$$

por lo tanto es anillo.

2. $\mathbb{Q}\left[\sqrt{3}\right]=\left\{a+b\sqrt{3}:a,b\in\mathbb{Q}\right\}$ es un anillo tal que todos sus elementos no nulos son unidades.
Vemos que
$$\frac{1}{a+b\sqrt{3}}=\frac{a-b\sqrt{3}}{a^2-3b^2}=\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\in\mathbb{Q}\left[\sqrt{3}\right],$$
para todo a,b no nulos simultáneamente
$$a^2-3b^2=0\qquad\Longrightarrow\qquad\frac{a}{b}=\sqrt{3}\notin\mathbb{Q}.$$

3. $R=\left\{a+b\sqrt[4]{3}:a,b\in\mathbb{Q}\right\}$ no es anillo
Definimos
$$x=a_1+b_1\sqrt[4]{3},\qquad y=a_2+b_2\sqrt[4]{3},$$
tal que
$$x+y=(a_1+a_2)+(b_1+b_2)\sqrt[4]{3}\in R,$$
sin embargo
$$\begin{aligned}x\cdot y&=\left(a_1+b_1\sqrt[4]{3}\right)\left(a_2+b_2\sqrt[4]{3}\right)=\\&=a_1a_2+b_1b_2\sqrt{3}+(a_1b_2+a_2b_1)\sqrt[4]{3}\notin R,\end{aligned}$$
ya que $b_1b_2\sqrt{3}\notin\mathbb{Q}$.

4. $R=\left\{a+b\sqrt[3]{3}+c\sqrt[3]{9}:a,b,c\in\mathbb{Q}\right\}$ es un anillo tal que todos sus elementos no nulos son unidades.
Vemos que
$$\frac{1}{a+b\sqrt[3]{3}+c\sqrt[3]{9}}=\frac{1}{a+\left(b+c\sqrt[3]{3}\right)\sqrt[3]{3}}=\frac{a-\left(b+c\sqrt[3]{3}\right)\sqrt[3]{3}}{\left(a+\left(b+c\sqrt[3]{3}\right)\sqrt[3]{3}\right)\left(a-\left(b+c\sqrt[3]{3}\right)\sqrt[3]{3}\right)}\in R,$$
para todo a,b no nulos simultáneamente etc....

Tal y como queríamos hacer ver. ■

Ejercicio 1.5.2 *Sea* $R=\left\{r=\left(a+b\sqrt{-5}\right):a,b\in\mathbb{Z}\right\}$, *demostrar*

1. *R es anillo,*

2. *R es DI*
3. *Definimos la aplicación*

$$\begin{aligned} N &: R \to Z \\ &: r \to a^2 + 5b^2, \end{aligned}$$

demostrar que es no negativa y satisface $N(xy) = N(x)N(y)$.

4. *Determinar las unidades de R.*

Solución. Se trata de probar con un poco de paciencia toda la ristra de propiedades i.e. definidas las operaciones $(+, \cdot)$

$$\begin{aligned} \left(a + b\sqrt{-5}\right) + \left(a' + b'\sqrt{-5}\right) &= \left(\left(a + a'\right) + \left(b + b'\right)\sqrt{-5}\right) \in R \\ \left(a + b\sqrt{-5}\right) \cdot \left(a' + b'\sqrt{-5}\right) &= \left(\left(aa' - 5bb'\right) + \left(ab' + ab'\right)\sqrt{-5}\right) \in R \end{aligned}$$

entonces $(R, +)$ es grupo abeliano, el producto es asociativo y distributivo, por lo tanto R es anillo.

Para ver que es un DI (un anillo conmutativo con unidad y sin divisores de cero ($\nexists \quad ab = 0$)). Por lo tanto sólo tenemos que ver la unidad es

$$1_R = 1 + 0\sqrt{-5} \in R.$$

Con respecto a la tercera pregunta, vemos que

$$N\left(a + b\sqrt{-5}\right) = a^2 + 5b^2$$

es no negativo y satisface $N(xy) = N(x)N(y)$.

Vemos que $\forall r \in R$,

$$N(r) = a^2 + 5b^2 \geq 0,$$

sean

$$x = a + b\sqrt{-5}, \qquad y = a' + b'\sqrt{-5},$$

observando que

$$N\left(a + b\sqrt{-5}\right) = a^2 + 5b^2 = \left|a + b\sqrt{5i}\right|^2,$$

por lo tanto

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|, \qquad |z|^2 = z \cdot \bar{z},$$

así que

$$N(xy) = |x \cdot y|^2 = |x|^2 \cdot |y|^2 = N(x)N(y).$$

Con relación al úlimo apartado vemos que dado $x \in R$, decimos que $x \in U(R) \iff N(x) = 1$, por lo tanto $x \in U(R) \iff \exists y \in R : xy = 1_R$, entonces

$$N(xy) = N(1_R) = 1,$$

donde $1_R = 1 + 0\sqrt{-5}$. Como $x = a + b\sqrt{-5} \in U(R) \iff N(x) = 1$, entonces

$$N(x) = a^2 + 5b^2 = 1 \qquad \iff \qquad a = \pm 1, b = 0,$$

por lo tanto $U(R) = \pm 1$.

Observación. Si $R = \{a + bi : a, b \in \mathbb{Z}\}$, entonces $U(R) = \{\pm 1, \pm i\}$. ya que $a^2 + b^2 = 1$. ■

Ejercicio 1.5.3 *Sea* $R = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$, *demostrar*

1. $I = \left\{a + b\sqrt{-5} : a = b \bmod 2\right\}$ *es un ideal maximal,*
2. $I = \left(2, 1 + \sqrt{-5}\right)$ *no es principal.*

Solución. Veamos que $I = \left\{a + b\sqrt{-5} : a = b \bmod 2\right\}$ es un ideal maximal. Para ello supongamos que J es otro ideal de R tal que $I \subsetneq J$, ntonces existe $a + b\sqrt{-5} \in J$ tal que $a = b \bmod 2$ i.e. $a - b = 2m + 1$, por lo que

$$(a-1) + b\sqrt{-5} \in I \qquad \Longrightarrow \qquad (a-1) + b\sqrt{-5} \in J,$$

$$1 = \left(a + b\sqrt{-5}\right) - \left((a-1) + b\sqrt{-5}\right) \in J,$$

por lo que concluimos que $J = R$ y por lo tanto I es maximal.

$I = \left(2, 1 + \sqrt{-5}\right)$ no es principal. Es evidente que $2, 1 + \sqrt{-5} \in I$ luego $\left(2, 1 + \sqrt{-5}\right) \subset I$. Para ver el otro contenido pensemos de la siguiente manera. Sea $a + b\sqrt{-5} \in I$

$$a + b\sqrt{-5} = 2m + \left(1 + \sqrt{-5}\right) b \in \left(2, 1 + \sqrt{-5}\right)$$

viendo así que I no es principal. Por reducción al absurdo. Supongamos que I es principal, entonces

$$I = \left(a + b\sqrt{-5}\right), \qquad a, b \neq 0,$$

como $2 \in I$, entonces existirán dos elementos $u, v \in \mathbb{Z}$ tales que

$$2 = \left(u + v\sqrt{-5}\right)\left(a + b\sqrt{-5}\right)$$

por lo que

$$\begin{aligned} au - 5bv &= 2, \\ av + bu &= 0, \end{aligned}$$

despejando encontramos que

$$v\left(a^2 + 5b^2\right) = -2,$$

dado que $a - b$ es par, entonces $a^2 - b^2$ es par, por lo que $a^2 + 5b^2 = a^2 - b^2 + 6b^2$ que es par y por otra parte tenemos que $a^2 + 5b^2 = 2m$ con $m > 1$, pero hemos obtenido que $vm = -1$, llegando así a una contradicción y por lo tanto concluimos que I no es principal. ■

Ejercicio 1.5.4 *Sea* $R = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$, *demostrar que no es DFU.*

Solución. Se tiene que

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right).$$

Se trata de ver que 2 y 3 son irreducibles en dicho anillo, lo mismo que $\left(1 + \sqrt{-5}\right)$ y $\left(1 - \sqrt{-5}\right)$. Estos elementos no son tampoco asociados. ■

Ejercicio 1.5.5 *Sea* $R = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$, *demostrar que no es DIP. Indicación, estudiar el ideal* $\left(3, 2 + \sqrt{-5}\right)$.

Solución. Tomando la norma

$$N\left(a+b\sqrt{-5}\right)=a^2+5b^2$$

hallar las unidades y los irreducibles de $\mathbb{Z}\left[\sqrt{-5}\right]$.

Sean $x,y\in\mathbb{Z}\left[\sqrt{-5}\right]$.

$$\begin{array}{rcll} N(x) & = & 0, & \iff \quad x=0, \\ N(xy) & = & N(x)\,N(y), & \\ N(1) & = & 1, & \iff \quad x=\pm 1, \end{array}$$

veamos que $N(1)=1\iff x=\pm 1$. Sea $x=a+b\sqrt{-5}\in U(R)\iff N(x)=1$

$$N\left(a+b\sqrt{-5}\right)=a^2+5b^2=1 \qquad \iff \qquad a=\pm 1, b=0$$

por lo tanto $x=\pm 1$, i.e. $U(R)=\pm 1$.

Supongamos ahora que el ideal $\left(3,2+\sqrt{-5}\right)$ está generado por x, i.e.

$$x=\left(3,2+\sqrt{-5}\right),$$

por lo tanto

$$3=xy, \qquad x\in R,$$

así que

$$N(3)=9=N(x)\,N(y),$$

encontrando las siguientes posibilidades:

1. $N(x)=1, N(y)=9,$
$$\left(3,2+\sqrt{-5}\right)=\mathbb{Z}\left[\sqrt{-5}\right], \text{¡!}, \qquad 1\notin\left(3,2+\sqrt{-5}\right),$$
2. $N(x)=3, N(y)=3,$
$$x=a^2+5b^2=3, \qquad \text{¡!},$$
3. $N(x)=9, N(y)=1,$ ¡! $(a=\pm 3, b=0)$ ó $(a=\pm 2, b=\pm 1)$ ya que por ejemplo
$$3=\left(3,2+\sqrt{-5}\right) \qquad \iff \qquad 2+\sqrt{-5}=3m$$
todos los casos son absurdos.

Por lo tanto concluimos el ideal no es principal. ■

Ejercicio 1.5.6 *Sea* $R=\left\{a+b\sqrt{-7}:a,b\in\mathbb{Z}\right\}$, *demostrar que no es DFU.*

Solución. Indicación. Tomando la norma

$$N\left(a+b\sqrt{-7}\right)=a^2+7b^2$$

hallar las unidades y los irreducibles de $\mathbb{Z}\left[\sqrt{-7}\right]$.

Sean $x, y \in \mathbb{Z}\left[\sqrt{-7}\right]$.

$$\begin{aligned} N(x) &= 0, \quad \Longleftrightarrow \quad x = 0, \\ N(xy) &= N(x)\,N(y), \\ N(1) &= 1, \quad \Longleftrightarrow \quad x = \pm 1, \end{aligned}$$

veamos que $N(1) = 1 \Longleftrightarrow x = \pm 1$. Sea $x = a + b\sqrt{-7} \in U(R) \Longleftrightarrow N(x) = 1$

$$N\left(a + b\sqrt{-7}\right) = a^2 + 7b^2 = 1 \quad \Longleftrightarrow \quad a = \pm 1, b = 0$$

por lo tanto $x = \pm 1$, i.e. $U(R) = \pm 1$.

Por otro lado podemos observar que

$$8 = 2 \cdot 2 \cdot 2 = \left(1 + \sqrt{-7}\right)\left(1 - \sqrt{-7}\right)$$

viendo que $\left(2, 1 + \sqrt{-7}, 1 - \sqrt{-7}\right)$ son irreducibles.

Sea $2 = xy$, entonces $N(2) = 4 = N(x)\,N(y)$,

$$N(x)\,N(y) = 4, \quad \Longrightarrow \quad N(x) = 2 = N(y),$$

pero esto es imposible ya que

$$N(x) = a^2 + 7b^2 = 2, \quad a, b \in \mathbb{Z},$$

entonces $N(x) = 4$, y $N(y) = 1$!¡, por lo tanto concluimos que 2 es irreducible.

De igual forma concluimos que $\left(1 + \sqrt{-7}\right)$ es irreducible, ya que si lo fuera entonces $\left(1 + \sqrt{-7}\right) = xy$,

$$N\left(1 + \sqrt{-7}\right) = 8 = N(x)\,N(y)$$

$$\begin{aligned} N(x) &= 2, N(y) = 4, \quad N(y) = a^2 + 7b^2 = 4, \quad a, b \in \mathbb{Z}, \quad \text{¡!}, \\ N(x) &= 1, N(y) = 8, \quad N(y) = a^2 + 7b^2 = 8, \quad a, b \in \mathbb{Z}, \quad \text{¡!}, \end{aligned}$$

por lo que es irreducible. Por lo tanto tenemos dos descomposiciones de 8, en irreducibles, por lo tanto R no es DFU. ■

Ejercicio 1.5.7 *Escribir la tabla de* $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$

Solución. Vemos que $\mathbb{Z}_3 = \{0, 1, 2\}$ por lo tanto

$\times$	0	$1+i$	$2+2i$	i	$2i$	1	$1+2i$	2	$2+i$
0	0	0	0	0	0	0	0	0	0
$1+i$	0	$2i$	i	$2+i$	$1+2i$	$1+i$	2	$2+2i$	1
$2+2i$	0	i	$2i$	$1+2i$	$2+i$	$2+2i$	1	$1+i$	2
i	0	$2+i$	$1+2i$	2	1	i	$1+i$	$2i$	$2+2i$
$2i$	0	$1+2i$	$2+i$	1	2	$2i$	$2+2i$	i	$1+i$
1	0	$1+i$	$2+2i$	i	$2i$	1	$1+2i$	2	$2+i$
$1+2i$	0	2	1	$1+i$	$2+2i$	$1+2i$	i	$2+i$	$2i$
2	0	$2+2i$	$1+i$	$2i$	i	2	$2+i$	1	$1+2i$
$2+i$	0	1	2	$2+2i$	$1+i$	$2+i$	$2i$	$1+2i$	i

por ejemplo vemos que

$$i(1+i) = i + i^2 = -1 + i \overset{\mathbb{Z}_3}{=} 2 + i, \quad \text{etc....}$$

tal y como queríamos hacer ver ■

Ejercicio 1.5.8 *El conjunto* $\{0,2,4,6,8\}$. *En un anillo conmutativo con unidad con la suma y el producto* $\mathrm{mod}(10)$ *¿Cuál es la unidad multipliativa? ¿y los elementos invertibles?*

Solución. Vemos que

$$\begin{aligned} 2\cdot 2 &\neq 2, \\ 2\cdot 4 &\neq 2, \\ 2\cdot 6 &= 12 = 2\,\mathrm{mod}(10) \end{aligned}$$

y comprobamos que deja el resto invariante i.e.

$$\begin{aligned} 4\cdot 6 &= 24 = 4, \\ 6\cdot 6 &= 36 = 6, \\ 8\cdot 6 &= 48 = 8, \end{aligned}$$

por lo tanto el $6 = e$ es la unidad multiplicativa.

Los inversos son

$$\begin{aligned} 2\cdot 8 &= 6 = e, \\ 4\cdot 4 &= 6 = e, \end{aligned}$$

de esta forma vemos que las unidades son $(2,4,6,8)$. ■

Ejercicio 1.5.9 *Cuantas unidades hay en* $\mathbb{Z}_{10^6}$.

Solución. u es una unidad sii $(u, 10^6) = 1$. Aplicando el pequeño teorema de Fermat vemos que

$$U(\mathbb{Z}_n) = \varphi(n)$$

por lo tanto

$$\varphi(10^6) = \varphi\left(p^k\right) = p^{k-1}(p-1)$$

sabemos que $10^6 = 2^6 5^6$, entonces

$$\varphi(10^6) = \varphi(2^6 5^6) = \varphi(2^6)\varphi(5^6) = 2^5 5^5 4$$

tal y como queríamos hacer ver. ■

Ejercicio 1.5.10 *Hallar las unidades en* $M_{2\times 2}(\mathbb{Z})$

Solución. Las unidades de $M_{2\times 2}(\mathbb{Z})$ son

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

tal que

$$M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

sii $ad - bc = 1$. Si $\det M \neq \pm 1$ entonces $\det A^{-1} \notin \mathbb{Z}$ y por lo tanto $A \notin M_{2\times 2}(\mathbb{Z})$. De esta forma concluimos que ls unidades de $M_{2\times 2}(\mathbb{Z})$ son las matrices de determinante igual a ± 1. ■

Ejercicio 1.5.11 *Probar que* $2x+1$ *tiene inverso multiplicativo en* $\mathbb{Z}_4[x]$

Solución. Tenemos que calcular

$$(2x+1)\,p(x)=1,$$

donde el polinomio $p(x)$ es de la forma $p(x)=ax+b$ (recordando que estamos trabajando en $\mathbb{Z}_4[x]$)

$$(2x+1)(ax+b)=1,$$

por lo tanto

$$\begin{array}{rcll} 2ax^2+ax+2bx+b & = & 1, & \\ 2ax^2+(a+2b)\,x+b & = & 1, & \Longleftrightarrow \quad b=1, \\ 2ax^2+(a+2)\,x & = & 0\bmod(4) & \Longleftrightarrow \quad a=2, \end{array}$$

por lo tanto $p(x)=2x+1$. ■

Ejercicio 1.5.12 *Si* R *no es un DI, buscar un anillo* R *en el que la ecuación* $ax=b$ *tenga más de una solución.*

Solución. Sea $R=\mathbb{Z}_6$, entonces $2x=4$, por lo tanto $x=2,5$. ■

Ejercicio 1.5.13 *Probar que*

$$\mathbb{Z}\left[\sqrt{7}\right]\simeq R=\left\{\begin{pmatrix} c & 7d \\ d & c \end{pmatrix};c,d\in\mathbb{Z}\right\}$$

Solución. Existe

$$\begin{array}{rcl} \phi & : & \mathbb{Z}\left[\sqrt{7}\right]\longrightarrow R \\ & : & a+b\sqrt{7}\longrightarrow \begin{pmatrix} a & 7b \\ b & a \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}+\begin{pmatrix} 0 & 7b \\ b & 0 \end{pmatrix} \end{array}$$

un isomorfismo pasa unidades en unidades

$$\phi:a\longrightarrow\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\qquad \phi:b\sqrt{7}\longrightarrow\begin{pmatrix} 0 & 7b \\ b & 0 \end{pmatrix}$$

comprobamos que

$$\phi(\alpha+\beta)=\phi(\alpha)+\phi(\beta),\qquad \phi(\alpha\beta)=\phi(\alpha)\,\phi(\beta)$$

por lo tanto

$$\begin{array}{rcl} \mathrm{Im}(\phi) & = & R,\ \text{inyectiva}, \\ \ker(\phi) & = & \{0\},\ \text{sobre}, \end{array}$$

por lo tanto la aplicación así construida es biyectiva ■

Ejercicio 1.5.14 *Demostrar que* $f:\mathbb{Z}_n\to\mathbb{Z}_n$ *tal que* $f(x)=x^n$ *es homeomorfismo de anillos sii* n *es primo.*

Solución. Se observa que

$$\begin{aligned} \phi(\alpha+\beta) &= \phi(\alpha)+\phi(\beta), \\ (x+y)^p &= x^p+y^p \equiv (x+y)(p), \end{aligned}$$

donde hemos tenido en cuenta el teorema de Fermat $a^p \equiv a(p)$,

Ahora vemos que

$$\begin{aligned} \phi(\alpha\beta) &= \phi(\alpha)\phi(\beta), \\ (x\cdot y)^p &= x^p \cdot y^p, \end{aligned}$$

y por último comprobamos que

$$\phi(1)=1, \qquad \Longrightarrow \qquad 1^p=1,$$

por lo que se trata de un homeomorfismo.

Si n es no primo entonces por ejemplo $f:\mathbb{Z}_6 \to \mathbb{Z}_6$ si verifica el producto pero no la suma ya que $(1+1)^6 = 1^6+1^6$, luego no es homeomorfismo si n es no primo. ■

Ejercicio 1.5.15 *Hallar el generador mónico del ideal*

$$I=\left(x^3+1, x^2+1\right)$$

en $\mathbb{Z}_2[x]$.

Solución. $I=(p)$ ¿p? si se cumple $I=(p)$, entonces $p \mid \left(x^3+1\right)$ y $p \mid \left(x^2+1\right)$ pero esto es imposible ya que no existe ningún polinomio que divida a la vez a estos dos polinomios.

Se observa que en $\mathbb{Z}_2[x]$

$$x^2+1=(x+1)^2,$$

como debe ser mónico entonces tenemos las siguientes posibilades:

$$p=1, \qquad p=x+1, \qquad p=(x+1)^2,$$

y comprobamos que

$$x+1 \mid \left(x^3+1\right), \qquad (x+1)^2 \not| \left(x^3+1\right),$$

por lo tanto

$$I=x+1.$$

Vemos que $I \subset (x+1)$, es obvio que $x+1 \mid \left(x^3+1\right)$, y $x+1 \mid \left(x^2+1\right)$. Falta probar que $x+1 \in I$ de ahí que $(x+1) \subset I$

$$(x+1)=A\left(x^3+1\right)+B\left(x^2+1\right)=\left(x^3+1\right)+(-x)\left(x^2+1\right),$$

llegando así al resultado deseado. ■

Ejercicio 1.5.16 *El ideal generado por* x^2-1, *¿es primo?,¿es máximal?. Que pasa si el ideal es* x^2+1.

Solución. $\left(x^2-1\right)=(x+1)(x-1)$ al ser reducible entonces no es maximal, tampoco es primo.

x^2+1 es primo y maximal al no tener raíces en $\mathbb{R}$. ■

Ejercicio 1.5.17 *Hallar un subanillo de* $A = \mathbb{Z}\left[\sqrt{2}\right]$ *que no sea ideal.*

Solución. $A = \mathbb{Z}\left[\sqrt{2}\right]$, consideramos $B = \mathbb{Z}$ un subanillo. No es ideal porque si tomo un elemento de $\mathbb{Z}$ y lo multiplico por un elemento entonces deja de pertenecer a $\mathbb{Z}$, por ejemplo

$$\left(1+\sqrt{2}\right)3 \notin \mathbb{Z}$$

tal y como queríamos hacer ver. ■

Ejercicio 1.5.18 *Probar que* $\mathbb{Z}\left[\sqrt{-2}\right]$ *y* $\mathbb{Z}\left[\sqrt{2}\right]$ *son DFU. Factorizar* 20.

Solución. Lo que sabemos probar es que es un DE lo que implica que es un DFU. Utilizando la norma usual

$$N\left(a+b\sqrt{-2}\right) = a^2+2b^2,$$

vemos que

$$\begin{array}{rcl} |z_1-z_2|^2 & = & |z_1|^2\,|z_2|^2, \qquad \Longrightarrow \qquad N(z_1z_2) \geq N(z_1), \\ z_1 & = & z_2w+r, \qquad / \qquad N(r) \geq N(z_2), \qquad r \neq 0 \end{array}$$

y ahora comprobamos que $N(r) < N(z_2)$

De igual forma podemos probar que $\mathbb{Z}\left[\sqrt{2}\right]$ es un DFU.

Para factorizar 20 en $\mathbb{Z}\left[\sqrt{2}\right]$ observamos que $20 = 2^2 \cdot 5$ por lo que tendremos que ver que el 2 y el 5 son irreducibles en $\mathbb{Z}\left[\sqrt{2}\right]$

$$\begin{array}{rcl} 2 & = & \sqrt{2}\cdot\sqrt{2}, \\ 5 & = & a\cdot b, \\ 20 & = & \left(\sqrt{2}\right)^4 5 \end{array}$$

tal y como queríamos calcular. ■

Ejercicio 1.5.19 *Explicar como construir campos con exactamente:*

Solución. Para ello tendremos en cuenta que si un campo finito, L, tieme m elementos y f es un polinomio irreducible de grado n sobre L entonces

$$E = m^n$$

donde

$$E = L/fL$$

es el campo de descomposición de f sobre L.

1. 125 elementos necesitamos encontrar por lo tanto un polinomio cúbico irreducible en $\mathbb{Z}_5$.
2. 49 elementos necesitamos encontrar por lo tanto un polinomio cuadrático irreducible en $\mathbb{Z}_7$.

3. 81 elementos necesitamos encontrar por lo tanto un polinomio cuadrático irreducible en $\mathbb{Z}_9$, o uno cuértico sobre $\mathbb{Z}_3$.

4. 243 elementos necesitamos encontrar por lo tanto un polinomio quíntico irreducible en $\mathbb{Z}_3$. Observar que $(243) = 3^5$.

5. $729 = 3^6 = \left(3^3\right)^2$ encontranto un polinomio de sexto grado en $\mathbb{Z}_3$.

■

Ejercicio 1.5.20 *Demostrar que* $\mathbb{F}_2/\left\langle x^2+x+1\right\rangle$ *es campo.*

Solución. $\mathbb{F}_2/\left\langle x^2+x+1\right\rangle$ es un cuerpo si y sólo si el ideal (x^2+x+1) es maximal.

Como $\mathbb{F}_2[x]$ es un dominio de ideales principales, el ideal (x^2+x+1) es maximal si y sólo si x^2+x+1 es irreducible sobre $\mathbb{F}_2$.

Como el grado del polinomio x^2+x+1 es 2, x^2+x+1 es irreducible sobre $\mathbb{F}_2$ si y sólo si no tiene raíces en $\mathbb{F}_2$. Sustituyendo $0;1 \in \mathbb{F}_2$ en x^2+x+1 obtenemos $1;1$ respectivamente. Por lo tanto, $\mathbb{F}_2/\left\langle x^2+x+1\right\rangle$ **es un cuerpo**. ■

Ejercicio 1.5.21 *Considera el conjunto* $A = \{0,2,4,6,8,10\}$ *sobre el que definimos la suma y el producto módulo* 12.

1. *Escribe las tablas de la suma y la multiplicación en* A.
2. *Demuestra que* A *es un anillo con la suma y el producto módulo* 12.
3. *¿Cuáles son las soluciones de la ecuación* $x^2 = x$ *en* A*?*
4. *¿Es cierto que* A *es isomorfo a* $\mathbb{Z}/6\mathbb{Z}$*?*

Solución. Con respecto al primer apartado vemos que

$+$	0	2	4	6	8	10
0	0	2	4	6	8	10
2	2	4	6	8	10	0
4	4	6	8	10	0	2
6	6	8	10	0	2	4
8	8	10	0	2	4	6
10	10	0	2	4	6	8

$\times$	0	2	4	6	8	10
0	0	0	0	0	0	0
2	0	4	8	0	4	8
4	0	8	4	0	8	4
6	0	0	0	0	0	0
8	0	4	8	0	4	8
10	0	8	4	0	8	4

Con respecto al segundo apartado vemos que si consideramos A como subconjunto de $\mathbb{Z}_{12}= \mathbb{Z}/12\mathbb{Z}$, A es igual a $2\mathbb{Z}/12\mathbb{Z}$. Como $2\mathbb{Z}$ es un subanillo de $\mathbb{Z}$, A es un subanillo de $\mathbb{Z}12$ y, en particular es anillo.

De la tabla de multiplicación se observa que hay dos soluciones: 0 y 4.

Por último. Si dos anillos son isomorfos y uno de ellos es unitario, entonces el otro también lo es. Como $\mathbb{Z}6$ es unitario y A no lo es, concluimos que **no** son isomorfos. ■

Ejercicio 1.5.22 *Sea $I \subset \mathbb{Z}[\sqrt{7}]$ el ideal generado por $\sqrt{7}-2$.*

1. *Demuestra que $3 \in I$.*
2. *Sea ahora$R = \mathbb{Z}[\sqrt{7}]/I$. Escribe la lista de los elementos de R.*
3. *Encuentra un anillo conocido que sea isomorfo a R. Presenta un isomorfismo.*

Solución. Se observa que

$$3 = (\sqrt{7}-2)(\sqrt{7}+2) \in I.$$

Como $3 \equiv \bmod I$ y $\sqrt{7} \equiv \bmod I$, se tiene que $\bar{0}, \bar{1}, \bar{2} \bmod I$ son suficientes para representar los elementos de R. Veamos que este conjunto de representantes no es redundante. Si lo fuera, entonces 1 ó 2 tendrían que estar en I. Pero el sistema de ecuaciones

$$n = (\sqrt{7}-2)(a+b\sqrt{7})$$

con $a, b \in \mathbb{Z}$ no tiene solución para $n = 1, 2$. Luego $R = \{\bar{0}, \bar{1}, \bar{2}\}$.

Por último vemos que un candidato natural es $\mathbb{Z}_3$. Para construir el isomorfismo observamos los siguientes pasos:

1. La inclusión $i : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]$ es obviamente un homomorfismo de anillos.

2. El paso al cociente $\pi : \mathbb{Z}[\sqrt{7}] \to \mathbb{Z}[\sqrt{7}]/I = R$ es un homomorfismo de anillos.

3. Como consecuencia, la composición $f = \pi \cdot i : \mathbb{Z} \to R$ es un homomorfismo de anillos.

4. El Primer Teorema de Isomorfía nos dice que $\mathbb{Z}/\ker f \simeq \operatorname{Im} f$.

5. Como $Im f R$, se tiene que $|\mathbb{Z}/\ker f| = |\operatorname{Im} f| \leq 3$.

6. Como $3 \in I, \langle 3 \rangle \subset \ker f$. De hecho $\langle 3 \rangle = \ker f$, pues de lo contrario $\ker f = \langle 1 \rangle$ y entonces f sería el homomorfismo 0.

7. Por 4, 5 y 6, comparando cardinales se tiene que $\mathbb{Z}/\langle 3 \rangle \simeq R$. ■

Ejercicio 1.5.23 *En $\mathbb{Z}[x]$ consideramos el conjunto*

$$B := \{p(x) \in \mathbb{Z}[x] : p(0) \text{ es par}\}.$$

1. *Demuestra que B es un ideal de $\mathbb{Z}[x]$.*
2. *Encuentra generadores para B.*
3. *¿A qué anillo conocido es isomorfo $\mathbb{Z}[x]/B$? Encuentra un isomorfismo.*

Solución. Con respecto al primer apartado basta observar que:

1.- Si $p(x), q(x) \in B$, entonces $p(x) - q(x) \in B$. Esto es claro dado que si $p(0)$ y $q(0)$ son pares, entonces $p(0) - q(0)$ también lo es.

2.- Si $p(x) \in B$ y $q(x) \in \mathbb{Z}[x]$ entonces $p(x)q(x) \in B$. Esto también es claro porque si $p(0)$ es par, entonces $p(0)q(0)$ también lo es.

Con respecto al segundo apartado vemos que obviamente todos los números pares están en B, así como todos los polinomios con término independiente nulo. Por lo tanto $2, x \in B$ y como consecuencia $\langle 2, x \rangle \in B$. El hecho es que estos dos ideales son iguales, y para probarlo hay que verificar la otra inclusión.

Si

$$p(x) = a_0 + a_1x + ... + a_nx^n \in B$$

entonces $p(0) = a_0 = 2m$ para algún $m \in \mathbb{Z}$. Por lo tanto,

$$p(x) = 2m + a_1x + ... + a_nx^n = 2m + x(a_1 + ... + a_nx^{n-1}) \in \langle 2, x\rangle .$$

Luego $B = \langle 2, x\rangle$.

Por último con respecto al tercer apartado vemos que en el anillo $\mathbb{Z}[x]/B$ sólo hay dos elementos, la clase correspondiente a polinomios que tienen término independiente par, y la de aquellos que tienen término independiente impar. Por lo tanto podríamos esperar que $\mathbb{Z}[x]/B$ sea isomorfo a $\mathbb{Z}_2$.

Construyamos explícitamente el isomorfismo.

1. Consideramos la aplicación

$$\begin{array}{rccl} g & : & \mathbb{Z}[x] & \longrightarrow \mathbb{Z}_2 \\ & & p(x) & \longrightarrow p(0) \bmod 2 \end{array}$$

que es trivialmente un homomorfismo de anillos sobreyectivo.

2. El Primer Teorema de Isomorfía para anillos nos dice que $\mathbb{Z}[x]/\ker g \simeq \mathbb{Z}_2$.

3. Para concluir observamos que $\ker g = B$. ■

Ejercicio 1.5.24 *Sea A el anillo $\mathbb{Z}[\sqrt{-2}]$*

1. *Decide razonadamente si $\langle 1 + 3\sqrt{-2}\rangle$ es un ideal maximal en A.*
2. *Escribe 3 como producto de irreducibles en A.*
3. *Encuentra un generador para el ideal $\langle 3, -1 + 2\sqrt{-2}\rangle$.*

Solución.

1. Como A es un dominio de ideales principales, ya que es dominio euclídeo con la norma

$$N(a + b\sqrt{-2}) = a^2 + 2b^2,$$

para probar que un ideal es maximal es suficiente con demostrar que está generado por un elemento irreducible.
Como $N(1 + 3\sqrt{-2}) = 19$ es primo, necesariamente $1 + 3\sqrt{-2}$ es irreducible, y por tanto $\langle 1 + 3\sqrt{-2}\rangle$ es maximal.

Observación 1.5.1 *Hay elementos irreducibles cuya norma no es un número primo, de modo que esta propiedad no caracteriza a los elementos irreducibles (por ejemplo, $N(5) = 25$ pero 5 es irreducible en A). Lo que sí es cierto es que si la norma de un elemento es un número primo entonces el elemento es irreducible, y esto es así incluso si el dominio del que se trate no es un dominio euclídeo (por ejemplo explorar $Z[\sqrt{-3}]$).*
Para demostrar que $\langle 1 + 3\sqrt{-2}\rangle$ es maximal no basta con demostrar que $1 + 3\sqrt{-2}$ es irreducible. Hay que observar además que A es un dominio de ideales principales (dado que es un dominio euclídeo con la norma arriba indicada), y que en un DIP los ideales maximales están generados por irreducibles. Este punto es fundamental, porque sobre un anillo que no sea DIP puede haber elementos irreducibles que no generen ideales maximales (por ejemplo x es irreducible en $\mathbb{Z}[x]$ pero no genera un ideal maximal).

En un dominio eucídeo no todo ideal primo es maximal. Por ejemplo en $\mathbb{Z}$ el ideal (0) es primo pero no maximal. Lo que sí es cierto es que un elemento es irreducible si y sólo si es primo y que todo irreducible (y por tanto todo elemento primo) genera un ideal maximal (observad que el elemento 0 no es primo ni irreducible por definición, pero genera un ideal primo).

2. Como $N(3) = 9$ si queremos escribirlo como producto de irreducibles necesitamos buscar elementos que en A tengan norma 3. Esto nos conduce a elementos de la forma $\pm 1 \pm \sqrt{-2}$, de donde deducimos que

$$3 = \left(1 + \sqrt{-2}\right)\left(1 - \sqrt{-2}\right)$$

Cada uno de estos factores es irreducible porque tiene norma 3 que es primo. Además esta factorización es única salvo el orden de los factores y producto por invertibles porque A es DFU (al ser DIP).

3. El ideal $\langle 3, -1 + 2\sqrt{-2}\rangle$ está generado por el máximo común divisor de sus generadores. Para calcularlo podemos proceder de dos modos:

a) Aplicando el Algoritmo de Euclides:

$$\begin{aligned} 3 &= (\sqrt{-2}(1 - 2\sqrt{-2}) + \left(-1 - \sqrt{-2}\right), \\ 1 - 2\sqrt{-2} &= -\left(1 + \sqrt{-2}\right)\left(1 + \sqrt{-2}\right) + 0, \end{aligned}$$

por lo tanto $m.c.d.(3, -1 + 2\sqrt{-2}) = 1 + \sqrt{-2}$, y como consecuencia,

$$\left\langle 3, -1 + 2\sqrt{-2}\right\rangle = \left\langle 1 + \sqrt{-2}\right\rangle.$$

b) Factorizando como producto de irreducibles:

$$\begin{aligned} 3 &= (1 + \sqrt{-2})(1 - \sqrt{-2}), \\ 1 - 2\sqrt{-2} &= \left(1 + \sqrt{-2}\right)^2, \end{aligned}$$

por lo tanto $m.c.d.(3, -1 + 2\sqrt{-2}) = 1 + \sqrt{-2}$, y como consecuencia,

$$\left\langle 3, -1 + 2\sqrt{-2}\right\rangle = \left\langle 1 + \sqrt{-2}\right\rangle.$$

Tal y como queríamos hacer ver. ■

Ejercicio 1.5.25 *Decide razonadamente si las siguientes afirmaciones son verdaderas o falsas.*

Solución.

1. En $\mathbb{Z}[x]$ todo elemento irreducible genera un ideal maximal.

Falso: Un elemento irreducible en un dominio de integridad es un elemento p, tal que si p se factoriza como producto $p = ab$, a o b es inversible. Los elementos inversibles de $\mathbb{Z}[x]$ son polinomios ± 1. Por lo tanto 2 no es inversible y como en cualquier factorización de 2 está 1 o -1, 2 es un elemento irreducible en $\mathbb{Z}[x]$. Por otro lado, el ideal generado por 2 no es maximal (por ejemplo, está contenido propiamente en el ideal generado por 2 y x).

Observar que $\mathbb{Z}[x]$ no es un dominio euclídeo. En la teoría hemos visto que los anillos de polinomios sobre cuerpos son dominios euclídeos. Pero $\mathbb{Z}$ no es un cuerpo.

2. Sea K un cuerpo y sea $f : \mathbb{Z} \to K$ un homomorfismo sobreyectivo. Entonces $K \simeq \mathbb{F}_p$ para algún primo $p \in \mathbb{Z}$.

   Verdadero. Por el primer teorema de Isomorfía

   $$K = \operatorname{Im} f \simeq \mathbb{Z}/\ker f :$$

   Por lo tanto, $\ker f$ es un ideal maximal de $\mathbb{Z}$ y por eso existe un primo p tal que $\ker f = (p)$. Entonces,

   $$K \simeq \mathbb{Z}/\ker f = \mathbb{Z}/(p) = \mathbb{F}_p.$$

3. Sea K un cuerpo y sea $f : \mathbb{Z}[i] \to K$ un homomorfismo sobreyectivo. Entonces $K \simeq \mathbb{F}_p$ para algún primo $p \in \mathbb{Z}$.

   Falso: Basta encontrar un ideal maximal I de $\mathbb{Z}[i]$ tal que el número de elementos del cuerpo $\mathbb{Z}[i]/I$ no es un número primo. Los ideales maximales en $\mathbb{Z}[i]$ están generados por elementos irreducibles. Si cogemos $i+1$, entonces $\mathbb{Z}[i]/(i+1)$ tiene dos elementos y es isomorfo a $\mathbb{F}_2$ y por lo tanto no nos proporciona un contraejemplo.

   Sin embargo si cogemos el elemento 3, es irreducible en $\mathbb{Z}[i]$ y el cuerpo $\mathbb{Z}[i]/(3)$ tiene 9 elementos y por lo tanto no es isomorfo a ningún $\mathbb{F}_p$ con p primo.

■

Ejercicio 1.5.26 *Sea*

$$R = \mathbb{F}_5[x]/\left\langle x^2 + x + 1 \right\rangle$$

1. *Decide razonadamente si R es un cuerpo*
2. *Resuelve la ecuación $(x+1)\cdot Y = 4$ sobre R.*
3. *Demuestra que el polinomio $p(Y) = Y^2 + Y + 1$ tiene dos soluciones en R.*
4. *Sea $g : R \to R$ un automorfismo. Decide razonadamente cuáles son los posibles valores de $g(x)$.*

Solución.

1. R es un cuerpo si y sólo si el ideal (x^2+x+1) es maximal. Como $\mathbb{F}_5[x]$ es un dominio de ideales principales, el ideal (x^2+x+1) es maximal si y sólo si x^2+x+1 es irreducible sobre $\mathbb{F}_5$. Como el grado del polinomio x^2+x+1 es 2, x^2+x+1 es irreducible sobre $\mathbb{F}_5$ si y sólo si no tiene raíces en $\mathbb{F}_5$. Sustituyendo $0;1;2;3;4 \in \mathbb{F}_5$ en x^2+x+1 obtenemos $1;3;2;3;1$ respectivamente. Por lo tanto, R **es un cuerpo**.
2. Como R es un cuerpo y $x+1 \neq 0$, existe $(x+1)^{-1}$. Por lo tanto

   $$Y = (x+1)^{-1}4,$$

   para encontrar $(x+1)^{-1}$ usaremos la identidad de Bezout para $x+1$ y x^2+x+1. Tenemos que

   $$1 = -x\,(x+1) + \left(x^2+x+1\right),$$

   por lo tanto

   $$(x+1)^{-1} = -x$$

   y por eso deducimos que

   $$Y = -x4 = x.$$

3. La primera solución se ve enseguida es $Y = \bar{x}$, ya que

$$p(x) = \bar{x}^2 + \bar{x} + 1 = \overline{x^2 + x + 1} = \bar{0}.$$

Para encontrar la otra solución hay que recordar que si tenemos un polinomio mónico $y^2 + ay + b$ que tiene dos raíces r_1 y r_2, entonces

$$y^2 + ay + b = (y - r_1)(y - r_2)$$

y por lo tanto

$$a = -(r_1 + r_2) \qquad b = r_1 r_2.$$

Usando estas formulas obtenemos que la segunda raíz es $\overline{-1 - x}$.

4. Como g es un automorfismo de R, g manda el 1 de R al 1 y el 0 al 0. Por lo tanto, $g(x)$ es una raíz del polinomio $Y^2 + Y + 1$:

$$g(\bar{x})^2 + g(\bar{x}) + 1 = g(\bar{x}^2 + \bar{x} + 1) = g(\bar{0}) = \bar{0}.$$

Por eso, $g(x)$ es igual a $\bar{x}$ o $\overline{-1 - x}$.

El automorfissmo identidad de R lleva $\bar{x}$ a $\bar{x}$.

La aplicación $g : R \to R$ definida mediante $g(\overline{p(x)}) = p(\overline{-1 - x})$ está bien definida y es un automorfismo de R. Además, g lleva $\bar{x}$ a $\overline{-1 - x}$.

■

Ejercicio 1.5.27 *Decide razonadamente si las siguientes afirmaciones son verdaderas o falsas.*

1. *El* $J := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a + b \equiv 0 \bmod 4\}$ *es un ideal de* $\mathbb{Z} \times \mathbb{Z}$.
2. *El elemento* $\sqrt{-5} + 6 \in \mathbb{Z}[\sqrt{-5}]$ *es irreducible.*

Solución.

1. **FALSO** Basta observar que $(2, 2) \in J, (1, 0) \in \mathbb{Z} \times \mathbb{Z}$ pero $(1, 0)(2, 2) \notin J$.
2. **VERDADERO** En primer lugar observamos que la función norma $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$ con

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

es multiplicativa y además cumple que $x \in \mathbb{Z}[\sqrt{-5}]$ es invertible si y sólo si $N(x) = 1$. De aquí deducimos que si la norma de un elmento es un número primo, entonces el elemento en cuestión es irreducible. Como

$$N(\sqrt{-5} + 6) = 41,$$

$\sqrt{-5} + 6$ es irreducible.

Observación: Para usar la norma no hace falta que el anillo sea un dominio euclídeo. Más aún, $\mathbb{Z}[\sqrt{-5}]$ no es un dominio euclídeo (no es muy difícil comprobar que no es un dominio de factorización única).

■

Ejercicio 1.5.28 *Considera el anillo*

$$R = \left\{ A = \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

con la suma y producto de matrices habituales, y también la aplicación:

$$\begin{array}{rcl} \eta & : & R \longrightarrow \mathbb{Z} \\ & : & A \longrightarrow a - b \end{array}$$

Responde razonadamente a las siguientes preguntas:

1. *Demuestra que η es un homomorfismo de anillos.*
2. *Describe el núcleo de η.*
3. *Demuestra que $R/\ker\eta \simeq \mathbb{Z}$.*
4. *Demuestra que $\ker\eta$ es primo pero no maximal.*
5. *Encuentra un ideal maximal de R que contenga a $\ker\eta$.*
   Sugerencia*: Observa primero que el subconjunto de R formado por las matrices diagonales es un conjunto de representantes de $R/\ker\eta \simeq \mathbb{Z}$.*

Solución.

1. Para ello debemos demostrar que η conserva la suma y el producto. Sean

$$A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \qquad A' = \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}$$

vemos que η conserva la suma, ya que

$$\begin{array}{rcl} \eta(A) + \eta(A') & = & \eta\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) + \eta\left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}\right) = a - b + a' - b' = \\ & = & (a + a') - (b - b') = \eta\left(\begin{pmatrix} a + a' & b + b' \\ b + b' & a + a' \end{pmatrix}\right) = \eta(A + A'). \end{array}$$

Para probrar que η conserva el producto vemos que

$$\begin{array}{rcl} \eta(A) \cdot \eta(A') & = & \eta\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) \cdot \eta\left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}\right) = (a - b) \cdot (a' - b') \\ & = & (aa' + bb') - (ab' - a'b) = \eta\left(\begin{pmatrix} aa' + bb' & ab' - a'b \\ ab' - a'b & aa' + bb' \end{pmatrix}\right) = \eta(A \cdot A'). \end{array}$$

2.

$$\begin{array}{rcl} \ker\eta & = & \{A \in R : \eta(A) = 0\} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} : a - b = 0 \right\} \\ & = & \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{Z} \right\}. \end{array}$$

3. Probamos en primer lugar que η es sobreyectiva: dado un entero cualquiera $n \in \mathbb{Z}$, se tiene que

$$\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \in R, \qquad \eta\left(\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}\right) = n,$$

por lo tanto

$$\operatorname{Im}\eta = \mathbb{Z}$$

i.e. η es sobreyectiva. Por el Primer Teorema de Isomorfía para anillos, $R/\ker\eta \simeq \mathbb{Z}$.

4. Por el apartado anterior, $R/\ker\eta \simeq \mathbb{Z}$. Como $\mathbb{Z}$ es un dominio de integridad, $\ker\eta$ es necesariamente un ideal primo. Como $\mathbb{Z}$ no es un cuerpo, $\ker\eta$ no puede ser maximal.

5. Como $R/\ker\eta \simeq \operatorname{Im}\eta = \mathbb{Z}$, la preimagen de cualquier ideal maximal de $\mathbb{Z}$ es un ideal maximal de $R/\ker\eta \simeq \mathbb{Z}$. Por otro lado, dado que hay una correspondencia biyectiva entre ideales $R/\ker\eta \simeq \mathbb{Z}$ e ideales de R que contienen a $\ker\eta$, un ideal maximal de $R/\ker\eta$ se corresponde con un ideal maximal de R que contiene a $\ker\eta$. Usando estas ideas, encontraremos un ideal maximal de R que contenga a $\ker\eta$.

   Consideramos por ejemplo el ideal maximal $\langle 3\rangle \in \mathbb{Z}$. Entonces, usando la sugerencia del enunciado,

$$\eta^{-1}(\langle 3\rangle) = \left\{ \overline{\begin{pmatrix} 3k & 0 \\ 0 & 3k \end{pmatrix}} : k \in \mathbb{Z} \right\}$$

   es un ideal maximal de $R/\ker\eta$, y como consecuencia

$$\begin{aligned} \left\{ \begin{pmatrix} 3k & 0 \\ 0 & 3k \end{pmatrix} : k \in \mathbb{Z} \right\} + \ker\eta &= \left\{ \begin{pmatrix} 3k & 0 \\ 0 & 3k \end{pmatrix} : k \in \mathbb{Z} \right\} + \left\{ \begin{pmatrix} n & n \\ n & n \end{pmatrix} : n \in \mathbb{Z} \right\} = \\ &= \left\{ \begin{pmatrix} 3k+n & n \\ n & 3k+a \end{pmatrix} : k, n \in \mathbb{Z} \right\} = \\ &= \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a - b \in \langle 3\rangle \subset \mathbb{Z} \right\} \end{aligned}$$

   es un ideal maximal de R que contiene a $\ker\eta$.

■

Sobre polinomios.

Ejercicio 1.5.29 *Mostrar que $f = x^2 + 1 \in \mathbb{Z}_7[x]$ es irreducible en $\mathbb{Z}_7[x]$.*

Solución. Al ser f cuadrático bastará con probar que no tiene raíces en $\mathbb{Z}_7[x]$. Calculando, vemos que

$$f(i) \neq 0, \qquad \forall i = 0, ..., 6,$$

por ejemplo

$$\begin{aligned} f(2) &= 4 + 1 = 5, \\ f(5) &= 26 \underset{\text{mod } 7}{=} 5 \neq 0 \end{aligned}$$

por lo tanto es irreducible. ■

Ejercicio 1.5.30 *Mostrar que $f = 2x^3 + 2x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$. De igual forma mostrar que*

$$g = x^6 + 2x^5 + x^4 + x^3 + x^2 + 1$$

es irreducible en $\mathbb{Z}_3[x]$ pero no tiene raíces en $\mathbb{Z}_3[x]$.

Solución. Al ser $f(i) \neq 0, \quad \forall i = 0,1,2$, entonces es irreducible.

De igual forma vemos que $f^2 = g$, es irreducible en $\mathbb{Z}_3[x]$ pero no tiene raíces en $\mathbb{Z}_3[x]$

$$\begin{aligned}\left(2x^3+2x^2+1\right)^2 &= 4x^6+8x^5+4x^4+4x^3+4x^2+1 \\ &\underset{\text{mod }3}{=} x^6+2x^5+x^4+x^3+x^2+1.\end{aligned}$$

Vemos que si $g(a) = 0$ entonces $(x-a)$ es un factor irreduciblede g ya que $g = f^2$ y la fatorización es única, por lo que $(x-a)$ debe ser un factor de f pero esto es una contradicción ya que f no tiene raíces. ■

Ejercicio 1.5.31 *Factorizar $f(x) = 3x^4+3x^3+x+1$ en $\mathbb{Z}_5[x]$.*

Solución. $f(x) = 3x^4+3x^3+x+1 \in \mathbb{Z}_5[x]$ por lo tanto las raíces serán de la forma $(0,1,2,3,4)$ viendo que

$$f(2) = f(4) = 0,$$

por lo tanto

$$f = (x+3)(x+1)\left(ax^2+bx+c\right)$$

i.e.

$$\begin{aligned}3x^4+3x^3+x+1 &= (x+3)(x+1)\left(ax^2+bx+c\right) \\ &= \left(x^2+4x+3\right)\left(ax^2+bx+c\right) \\ &= ax^4+(4a+b)x^3+(3a+4b+c)x^2+(3b+4c)x+3c\end{aligned}$$

por lo que

$$\begin{aligned} a &= 3, & & & & \\ 4a+b &= 3, & \Longrightarrow \quad & 12+b=3 & \Longrightarrow \quad & b=1 \\ 3a+4b+c &= 0, & \Longrightarrow \quad & 1+c=0 & \Longrightarrow \quad & c=2 \\ 3c &= 1, & \Longrightarrow \quad & c=2 & & \end{aligned}$$

de esta forma encontramos que

$$f = (x+3)(x+1)\left(3x^2+x+2\right)$$

tal y como queríamos hacer ver. ■

Ejercicio 1.5.32 *Sea $I = \left(x^2+1\right)\mathbb{R}[x]$ un ideal principal de $\mathbb{R}[x]$ generado por $\left(x^2+1\right)$. Explicar porqué $\mathbb{R}[x]/I$ es un campo y encontrar polinomios f, g tales que*

$$\begin{aligned}\left(x^4+3x+1\right)+I &= f(x)+I, \\ \left(2x^5+7x^2+x+3\right)+I &= g(x)+I.\end{aligned}$$

Solución. Vemos que $f(x) = x^2+1$ es un polinomio que no tiene raíces en $\mathbb{R}$ por lo tanto es irreducible en $\mathbb{R}$, al ser cuadrático. Como $I = \left(x^2+1\right)\mathbb{R}[x]$ es maximal entonces $\mathbb{R}[x]/I$ es un campo.

Ahora vemos que

$$\begin{aligned}\left(x^4+3x+1\right) &= \left(x^2-1\right)\left(x^2+1\right)+(3x+2),\\ \left(2x^5+7x^2+x+3\right) &= \left(2x^3-2x+7\right)\left(x^2+1\right)+(3x-4),\end{aligned}$$

de esta forma

$$\left(x^4+3x+1\right)-(3x+2)=\left(x^2-1\right)\left(x^2+1\right)\in I,$$

y por lo tanto

$$\left(x^4+3x+1\right)+I=(3x+2)+I,$$

De forma similar llegamos a que

$$\left(2x^5+7x^2+x+3\right)+I=(3x-4)+I,$$

tal y como queríamos hacer ver. ■

Ejercicio 1.5.33 *Mostrar que* $f(x)=x^2+2x+2$ *es irreducuble en* $\mathbb{Z}_3[x]$.

Solución. Vemos que

$$f(i)\neq 0, \qquad \forall i=0,1,2.$$

Sea $I=f(x)\mathbb{Z}_3[x]$, I es maximal entonces $\mathbb{Z}_3[x]/I$ es un campo. Sabemos que para todo $u,v\in\mathbb{Z}_3[x]$

$$u+I=v+I, \qquad \Longleftrightarrow \qquad u=v,$$

y para algun $w\in\mathbb{Z}_3[x]$

$$w+I=r+I,$$

tal que

$$w=fq+r,$$

así que tenemos 9 elementos

$$(0,1,2,x,2x,1+x,1+2x,2+x,2+2x),$$

así

$$x^2+2x+2 \qquad \Longrightarrow \qquad x^2=-2x-2=x+1$$

y por lo tanto tenemos la siguiente tabla

	0	1	2	x	$2x$	$1+x$	$1+2x$	$2+x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$2x$	$1+x$	$1+2x$	$2+x$	$2+2x$
2	0	2	1	$2x$	x	$2+2x$	$2+x$	$1+2x$	$1+x$
x	0	x	$2x$	$1+x$	$2+2x$	$1+2x$	2	1	$2+x$
$2x$	0	$2x$	x	$2+2x$	$1+x$	$2+x$	1	2	$1+2x$
$1+x$	0	$1+x$	$2+2x$	$1+2x$	$2+x$	2	$2x$	x	1
$1+2x$	0	$1+2x$	$2+x$	2	1	$2x$	$2+2x$	$1+x$	x
$2+x$	0	$2+x$	$1+2x$	1	2	x	$1+x$	$2+2x$	$2x$
$2+2x$	0	$2+2x$	$1+x$	$2+x$	$1+2x$	1	x	$2x$	2

con G el grupo multiplicativo decimos que $G=\langle x\rangle$ que es equivalente a x teniendo orden 8.

De igual forma se demuestra que el polinomio $p(x)=x^3-x+1$ es irreducible en $\mathbb{Z}_3[x]$. ■

Ejercicio 1.5.34 *Comprobar si los siguientes polinomios son irreducibles en* $\mathbb{Q}[x]$.

Solución.

1. $f(x) = 3x^2 - 7x - 5$, aplicando el criterio de Eisestein con $p = 7$, ademas se puede comprobar con facilidad que las raices peretenecen a $\mathbb{R}$.

2. $f(x) = 6x^3 - 3x - 18$, simplificamos la expresión viendo que $f(x) = 2x^3 - x - 6$ e intentamos descomponerlo de la siguiente forma, sea $\alpha = a/b$, entonces

$$\begin{aligned} 2\left(\frac{a}{b}\right)^3 - \left(\frac{a}{b}\right) - 6 &= 0, \\ \frac{1}{b^3}\left(-2a^3 + ab^2 + 6b^3\right) &= 0 \end{aligned}$$

de donde

$$2a^3 - b^2(a - 6b) = 0$$

con $b \mid 2$, y $a \mid 6$. i.e. $\frac{a}{b} = \pm 6, \pm 3, \pm 2, \pm 1, \pm\frac{3}{2}, \pm\frac{1}{2}$ ninguno de ellos es raíz, entonces f es irreducible en $\mathbb{Q}[x]$.

3. $f(x) = x^3 - 7x + 1$, vemos que este polinomio es irreducible en $\mathbb{Z}_2[x]$, $f(x) = x^3 + x + 1$, ya que las únicas posibles raices son $(0, 1)$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

4. $f(x) = x^5 - 3x + 3$, aplicando el criterio de Eisestein con $p = 3$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

5. $f(x) = x^6 - 6x + 2$, aplicando el criterio de Eisestein con $p = 2$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

6. $f(x) = x^2 + 1$, las raices son complejas y por lo tanto es irreducible en $\mathbb{Q}[x]$.

7. $f(x) = x^4 + 1$, las raices son complejas y por lo tanto es irreducible en $\mathbb{Q}[x]$.

8. $f(x) = x^6 + x^3 + 1$, vemos que este polinomio es irreducible en $\mathbb{Z}_2[x]$, ya que las únicas posibles raices son $(0, 1)$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

9. $f(x) = x^4 + 3x + 6$, aplicando el criterio de Eisestein con $p = 3$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

10. $f(x) = x^3 + 11^{11}x + 13^{13}$, vemos que este polinomio es irreducible en $\mathbb{Z}_2[x]$, ya que las únicas posibles raices son $(0, 1)$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

11. $f(x) = \frac{1}{3}x^5 + \frac{5}{2}x^4 + \frac{3}{2}x^3 + \frac{1}{2}$, vemos que podemos reescribir el polinomio de la siguiente manera: $2x^5 + 15x^4 + 9x^3 + 3$, aplicando el criterio de Eisestein con $p = 3$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

12. $f(x) = x^5 - 9x^2 + 1$, vemos que este polinomio es irreducible en $\mathbb{Z}_2[x]$, $f(x) = x^5 + x^2 + 1$, ya que las únicas posibles raices son $(0, 1)$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

13. $f(x) = x^4 - x^3 - x - 1$, vemos que este polinomio es irreducible en $\mathbb{Z}_2[x]$, $f(x) = x^4 + x^3 + x + 1$, ya que las únicas posibles raices son $(0, 1)$ y por lo tanto es irreducible en $\mathbb{Q}[x]$

14. $f(x) = x^7 + 3x^3 + 6x - 3$, aplicando el criterio de Eisestein con $p = 3$ y por lo tanto es irreducible en $\mathbb{Q}[x]$.

15. $f(x) = x^4 + 2x + 1$, no podemos aplicar el criterio E, pero observamos que

$$f(x-1) = (x-1)^4 + 2(x-1) + 1 = x^4 - 4x^3 + 6x^2 - 2x,$$

por lo que

$$f(x-1) = xg(x)$$

para algun polinomio $g(x) \in \mathbb{Q}[x]$ de grado 3. Por lo tanto, $f(x-1)$ y f son irreducible.

16. $f(x) = x^4 + 2x + 3$, siguiendo el ejemplo anterior vemos

$$f(x+1) = (x+1)^4 + 2(x+1) + 3 = x^4 + 4x^3 + 6x^2 + 6x + 6,$$

irreducible aplicando el criterio E y por lo tanto f es irreducible.

■

Ejercicio 1.5.35 *Comprobar si los siguientes polinomios son irreducibles en* $\mathbb{Z}_i[x]$.

Solución.

1. $f(x) = x^5 \pm x^2 + 1$ en $\mathbb{Z}_2[x]$, ya que las únicas posibles raices son $(0, 1)$
2. $f(x) = x^2 + bx + c$ en $\mathbb{Z}_7[x]$ sii $b^2 - 4c = 3, 5, 6$.
   Se observa que
   $$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$
   entonces si tenemos en cuenta que en $\mathbb{Z}_7$,
   $$2^{-1} = 4$$
   entonces
   $$\left(-b \pm \sqrt{b^2 - 4c}\right) 4 \in \mathbb{Z}_7$$
   sii
   $$b^2 - 4c$$
   es el cuadrado de un número en $\mathbb{Z}_7$, por lo que el polinomio será irreducible cuando $b^2 - 4c = 3, 5, 6$.
3. $f(x) = x^2 + 1$ en $\mathbb{Z}_5[x]$. vemos que $f(2) = 0$ y por lo tanto el polinomio es reducible.

■

Capítulo 2

Extensiones de cuerpos

2.1. Extensiones finitas

La idea principal en el estudio de las raíces de polinomios consiste en la siguiente observación: sea p un polinomio irreducible sobre un cuerpo K, las propiedades de las raíces de este polinomio están reflejadas en las propiedades del cuerpo $K[x]/(p)$, i.e. sea $p(x) \in K[x]$ donde p es irreducible en K, sin embargo existe un cuerpo que ahora llamaremos $K[x]/(p)$ donde $p(x)$ se descompone i.e. existe $\alpha \in K[x]/(p)$ tal que $p(\alpha) = 0$. Esta idea nos conduce al estudio más profundo de los cuerpos. Veamos un ejemplo motivador.

Ejemplo 2.1.1 *Sea $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Este polinomio es irreducible en $\mathbb{R}$. $\langle x^2+1\rangle$ es un ideal maximal en $\mathbb{R}[x]$ y por lo tanto $\mathbb{R}[x] / \langle x^2+1\rangle$ es un campo (cuerpo). Podemos considerar por lo tanto*

$$\mathbb{R} \subset \mathbb{R}[x] / \left\langle x^2+1 \right\rangle.$$

Sea $\alpha = x + \langle x^2+1\rangle$ entonces

$$\begin{aligned} \alpha^2 + 1 &= \left(x + \left\langle x^2+1 \right\rangle\right)^2 + \left(x + \left\langle x^2+1 \right\rangle\right) \\ &= \left(x^2+1\right) + \left(x^2+1\right) = 0, \end{aligned}$$

α es un cero de x^2+1. Se observa que

$$\mathbb{R}[x] / \left\langle x^2+1 \right\rangle \approx \mathbb{C}.$$

Definición 2.1.1 *Sean K y F dos cuerpos. Se dice que F es una **extensión** de K si existe un homomorfismo de cuerpos $\phi : K \to F$. En este caso escribimos F/K.*

Observación 2.1.1 *Como un homomorfismo de cuerpos es siempre inyectivo, podemos identificar los elementos de K con sus imágenes en F. Esto nos permite ver K como un subcuerpo de F y por eso también vamos a escribir $K \subseteq F$.*

Ejemplo 2.1.2 *1.* $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$; $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$; $\mathbb{R} \subseteq \mathbb{C}$;

2. $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2}, a, b \in \mathbb{Q}\right\} \subseteq \mathbb{R}$.

3. *Sea K un cuerpo, $p \in K[x]$ un polinomio irreducible y $E = K[x]/(p)$. Entonces, E/K es una extensión.*

4. *Sea $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Este polinomio es irreducible en $\mathbb{Q}$. Observemos ahora que $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ y que*

$$x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right),$$

por lo tanto es reducible en $\mathbb{Q}(\sqrt{2})$. Esta es la idea que se persigue.

5. *Sea, el "archiconocido" polinomio $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Este polinomio es irreducible en $\mathbb{Q}$. Vemos que*

$$f(x) = \left(x^2 - 2\right)\left(x^2 - 3\right)$$

y que por lo tanto una extensión puede ser:

$$E = \mathbb{Q}[x] / \left(x^2 - 2\right),$$
$$E = \mathbb{Q}[x] / \left(x^2 - 3\right), \qquad \acute{o}$$
$$E = \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right] / \mathbb{Q}.$$

Observación 2.1.2 *Como cualquier cuerpo K contiene un subcuerpo primo P, K es una extensión de P. Por tanto, se puede considerar que todo cuerpo es una extensión de $\mathbb{Q}$ ó $\mathbb{F}_p$.*

Definición 2.1.2 *Sea F/K una **extensión** de cuerpos. Se dice que F/K es finitamente generada si existe un subconjunto $S \subseteq F$ finito tal que $F = K(S)$. Se dice que es **simple** si existe $u \in F$ tal que $F = K(u)$.*

Ejemplo 2.1.3 1. *$\mathbb{C}/\mathbb{R}$ es una extensión simple puesto que $\mathbb{C} = \mathbb{R}(i)$.*

2. *Sea K un cuerpo y $F = K(x)$ el cuerpo de cocientes del anillo de polinomios $K[x]$. Entonces F/K es una extensión simple.*

3. *$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2}, a, b \in \mathbb{Q}\right\}$ puede verse como $\mathbb{Q} \cup (\sqrt{2})$, donde $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, $\mathbb{Q}(\sqrt{2})$ es el subcampo más pequeño donde el polinomio $x^2 - 2$ se descompone en factores lineales.*

4. *La idea del anterior ejemplo es la siguiente. Sean $L, S, T \subset K$ i.e. subcampos de K entonces*

$$L(S \cup T) = L(S)(T)$$

por ejemplo

$$\mathbb{Q}(\sqrt{2})\left(\sqrt{3}\right) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Sea F/K una extensión de cuerpos. Entonces, F tiene una estructura natural de $K-$espacio vectorial. Esta observación nos permite utilizar los conceptos y resultados del álgebra lineal en el estudio de los extensiones de cuerpos.

Definición 2.1.3 *Se dice que una extensión F/K es finita si F como K-espacio vectorial es de dimensión finita. A la dimensión de este espacio vectorial se le llama* ***grado de la extensión*** *y se denota* $[F:K]$.

Ejemplo 2.1.4 1. $[\mathbb{C}:\mathbb{R}]=2$,

2. $\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right]=2$. $\mathbb{Q}(\sqrt{2})=\left\{a+b\sqrt{2}, a,b\in\mathbb{Q}\right\}$, $B=\left\{1,\sqrt{2}\right\}$ *generan* $\mathbb{Q}(\sqrt{2})$

3. $[\mathbb{Q}(x):\mathbb{Q}]=\infty$.

4. *En general* $\left[\mathbb{Q}(\sqrt{d}):\mathbb{Q}\right]=2$, *donde* $\mathbb{Q}(\sqrt{d})=\left\{a+b\sqrt{d}, a,b\in\mathbb{Q}\right\}$, $B=\left\{1,\sqrt{d}\right\}$.

5. $\left[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}\right]=4$, $\mathbb{Q}(\sqrt[4]{3})=\left\{a+b\sqrt[4]{3}+c\sqrt[4]{9}+d\sqrt[4]{27}, a,b,c,d\in\mathbb{Q}\right\}$

Lema 2.1.1 *Sea K un cuerpo y P un polinomio irreducible sobre K de grado n. Pongamos $F=K[x]/(P)$. Entonces, $1+(P), x+(P), \cdots, x^{n-1}+(P)$ es una $K-$base de F y $[F:K]=n=grP$.*

Sea F/K una extensión finita y $\{u_1,...,u_n\}$ una $K-$base de F. Entonces, claramente, $F=K(u_1,...,u_n)$. En particular, F/K finita implica que F/K es finitamente generada. Pero no es cierto recíprocamente.

Teorema 2.1.1 *(**Transitividad de índices o the tower law**) Sean F/E y E/K extensiones de cuerpos. Entonces, F/K es una extensión finita si y sólo si F/E y E/K son extensiones finitas y*

$$[F:K]=[F:E][E:K].$$

De hecho si F/E y E/K son finitas y $\{x_i\}_{i=1}^{r}$ y $\{y_j\}_{j=1}^{s}$ son sus respectivas bases entonces $\{x_iy_j\}_{i,j=1}$ es una base de F/K.

Ejemplo 2.1.5 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

$(\sqrt{2},\sqrt{3})\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ *por lo tanto* $(\sqrt{2}+\sqrt{3})\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, *además* $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ *por lo que* $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Ahora vemos que

$$\left(\sqrt{2}+\sqrt{3}\right)^{-1}=\frac{1}{\sqrt{2}+\sqrt{3}}=\sqrt{3}-\sqrt{2}$$

por lo que $\left(\sqrt{2}+\sqrt{3}\right), \left(\sqrt{3}-\sqrt{2}\right)\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *así como* $2\sqrt{2}, 2\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *de esta forma llegamos a que* $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *y por lo tanto*

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$$

así que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Ejemplo 2.1.6 $\mathbb{Q}(\sqrt{3},\sqrt{15}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$.

En prier lugar observamos que

$$\sqrt{5} = \frac{1}{3}\sqrt{3}\sqrt{15}$$

y por lo tanto

$$\mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{15}).$$

Ahora vemos que

$$\sqrt{15} = \sqrt{3}\sqrt{5} \in \mathbb{Q}(\sqrt{3},\sqrt{5}),$$

y por lo tanto

$$\mathbb{Q}(\sqrt{3},\sqrt{15}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{5})$$

así que $\mathbb{Q}(\sqrt{3},\sqrt{15}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$. *Si seguimos el argumento del ejemplo anterior entonces probamos que*

$$\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5}).$$

2.2. Extensiones algebraicas y transcendentes

Definición **2.2.1** *Sea F/K una extensión de cuerpos. Se dice que un elemento $u \in F$ es **algebraico** sobre K si existe un polinomio no nulo $P \in K[x]$ tal que $P(u) = 0$. Si u no es algebraico sobre K se dice que u es **transcendente** sobre K.*

Ejemplo 2.2.1

1. *Consideremos la extensión $\mathbb{R}/\mathbb{Q}$. Evidentemente, $\sqrt{2}$, de $\left(x^2-2\right)$ y $\sqrt[3]{2}$ de $\left(x^3-2\right)$, son algebraicos sobre $\mathbb{Q}$ y se puede demostrar que e y π son números transcendentes sobre $\mathbb{Q}$.*
2. *De igual forma se prueba que i, $\left(x^2+1\right)$, es algebraico sobre $\mathbb{Q}$.*
3. *Así como $\sqrt{1+\sqrt{3}}$ cuyo polinomio es $\left(x^4-2x^2-2\right)$ es algebraico sobre $\mathbb{Q}$. Sea $\alpha = \sqrt{1+\sqrt{3}}$ entonces $\alpha^2 = 1+\sqrt{3}$, entonces $\alpha^2-1 = \sqrt{3}$, $\left(\alpha^2-1\right)^2 = 3$ y por lo tanto α será un cero de x^4-2x^2-2*

Teorema **2.2.1** *Sea F/K una extensión de cuerpos y $u \in F$ un elemento algebraico sobre K. Entonces, existe un único polinomio mónico irreducible $P \in K[x]$ tal que $P(u) = 0$. Además, si $Q \in K[x]$ y $Q(u) = 0$, entonces P divide a Q.*

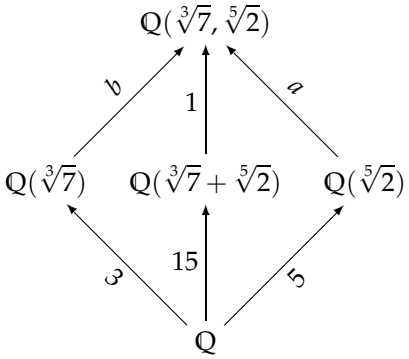
El **polinomio** del teorema anterior lo denotaremos por $\mathrm{Irr}(u,K)$ o **mínimo**.

Ejemplo 2.2.2

1. $\mathrm{Irr}(\sqrt{2},\mathbb{Q}) = x^2-2$,
2. $\mathrm{Irr}(\sqrt[4]{2},\mathbb{Q}) = x^4-2$, $\mathrm{Irr}(\sqrt[4]{d},\mathbb{Q}) = x^4-d$,
3. $\mathrm{Irr}(\sqrt[4]{2},\mathbb{Q}[\sqrt{2}]) = x^2-\sqrt{2}$, $\mathrm{Irr}(\sqrt[4]{d},\mathbb{Q}[\sqrt{d}]) = x^2-\sqrt{d}$,
4. $\mathrm{Irr}(\sqrt{1+\sqrt{3}},\mathbb{Q}) = x^4-2x^2-2$.

5. $\mathrm{Irr}(\sqrt[3]{7}, \mathbb{Q}\left(\sqrt[5]{2}\right))$. *Queremos calcular el grado del polinomio mínimo.*

   Para ello observemos el siguiente gráfico,



   y lo único que hacemos ahora es aplicar el teorema de la tower law i.e.

$$\left[\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt[5]{2})\right] = \left[\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt[3]{7})\right] \left[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}(\sqrt[5]{2})\right]$$

   y designamos por $n = \left[\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}\right]$. *De esta forma vemos que*

$$n = 5a, \qquad n = 3b,$$

   luego $5a = 3b$, *además se observa que* $(5/b)$ *y* $(3/a)$.

   Considermaos ahora el polinomio $P = x^3 - 7 \in \mathbb{Q}(\sqrt[5]{2})[x]$ *donde* $\sqrt[3]{7}$ *es uno de sus ceros, por lo tanto el grado del polinomio mínimo es* ≤ 3 *y así* $a \leq 3$, *pero como* $(3/a)$ *entonces* $a = 3$ *y por lo tanto* $b = 5$, *llegando así a que* $n = 15$.

   Por curiosidad, el polinomio mínimo en este caso resulta ser:

$$x^{15} - 35x^{12} - 6x^{10} + 490x^9 - 1260x^7 - 3430x^6 + 12x^5 - 13230x^4 + 12005x^3 - 840x^2 - 10290x - 16815.$$

Teorema **2.2.2** *Sea* F/K *una extensión de cuerpos y* $u \in F$ *un elemento algebraico sobre* K. *Entonces* $K(u)$ *es* ***isomorfo*** *a* $K[x]/(\mathrm{Irr}(u, K))$ *i.e.*

$$K(u) \approx K[x]/(\mathrm{Irr}(u, K)).$$

Además, existe un isomorfismo de cuerpos

$$\phi : K[x]/(\mathrm{Irr}(u, K)) \to K(u),$$

tal que

$$\phi(x + (\mathrm{Irr}(u, K)) = u.$$

Corolario **2.2.1** *Sea* F/K *una extensión de cuerpos y* $u \in F$. *Entonces,* u *es algebraico sobre* K *si y sólo si* $K(u)/K$ *es una extensión finita. Además, si* n *es igual al grado de* $\mathrm{Irr}(u, K)$, *entonces* $\left(1, u, \cdots, u^{n-1}\right)$ *es una* $K-$*base de* $K(u)$ *y* $[K(u) : K] = n$.

La base está generada por:

$$B = \sum_{i=1}^{n} b_i u^{i-1}.$$

Ejemplo 2.2.3 *1.* $\mathbb{Q}(\sqrt[4]{3}) \approx \mathbb{Q}[x]/(x^4-3)$.

$$\left[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}[x]\right] = 4,$$

donde

$$\mathbb{Q}(\sqrt[4]{3}) = \left\{a, b\sqrt[4]{3}, c\sqrt[4]{3^2}, d\sqrt[4]{3^3} : a,b,c,d \in \mathbb{Q}\right\},$$

i.e.

$$B_\alpha = \left\{1, \alpha, \alpha^2, \alpha^3\right\}$$

con $\alpha = \sqrt[4]{3}$.

2. $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ *Sabemos que existe* $\alpha \in F/\mathbb{Z}_2[x]$ *tal que* $p(\alpha) = 0$. *Por el anterior colorario sabemos que existe una base generada por*

$$B = \{0\alpha, 1+0\alpha, 1\alpha, 1+1\alpha\},$$

observar que las posibles raíces de p *en* $\mathbb{Z}_2[x]$ *son* $(0,1)$.

3. *Sea* $p(x) = x^3 - 2, \nexists \alpha \in \mathbb{Q}(\sqrt{2})$ *tal que* $p(\alpha) = 0$ *ya que*

$$\begin{aligned}\operatorname{grad}(\sqrt{2}, \mathbb{Q}) &= 2,\\ \operatorname{grad}(x^3 - 2, \mathbb{Q}) &= 3\end{aligned}$$

y como sabemos 3 *no es divisible por* 2.

4. $a = 2^{1/3}$ *es algebraico sobre* $\mathbb{Q}$ *ya que* $p(a) = 0$, *siendo* $p(x) = x^3 - 2$ *que es irreducible por el criterio de Eisenstein. Luego*

$$\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}[x]\right] = 3,$$

donde

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\right\},$$

será una base para $\mathbb{Q}(\sqrt[3]{2})$ *sobre* $\mathbb{Q}$.

5. *Consideramos* $\mathbb{Q}(\sqrt{2})$ *entonces una base es:*

$$B = \left\{1, \sqrt{2}\right\}$$

el polinomio mínimo es $x^2 - 2$.

El polinomio mínimo de $\mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$ *es* $x^4 - 10x^2 + 1$ *ya que una base está dada por*

$$B_{(\sqrt{2},\sqrt{3})} = \left\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\right\},$$

donde

$$B_\alpha = \{1, \alpha\} \qquad B_\beta = \{1, \beta\},$$

con $\alpha = \sqrt{2}, \beta = \sqrt{3}$, *por lo tanto*

$$B_{(\alpha,\beta)} = \{1, \alpha, \beta, \alpha\beta\}.$$

Teorema 2.2.3 *Sea* F/K *una extensión de cuerpos y* $u \in F$ *un elemento transcendente sobre* K. *Entonces,*

$$K(u) \simeq K(x).$$

Teorema **2.2.4** *Sea F/K una extensión de cuerpos y u, $v \neq 0$ elementos algebraicos. Entonces $u+v$, uv, v^{-1} son también elementos algebraicos.*

Corolario **2.2.2** *Sea F/K una extensión de cuerpos. Entonces el conjunto*

$$E = \{u \in F | u \text{ es algebraico sobre } K\}$$

*es un subcuerpo de F que contiene a K. (E se llama la **clausura algebraica** de K en F).*

Definición **2.2.2** *Sea F/K una extensión de cuerpos. Se dice que F/K es una **extensión algebraica** si todo elemento de F es algebraico sobre K.*

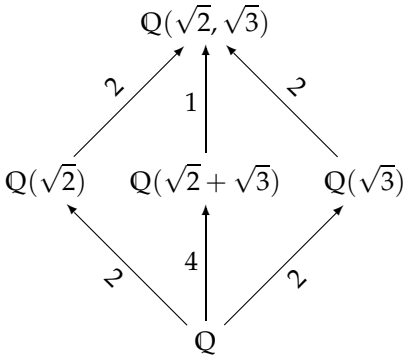
*En el caso contrario se dice que la **extensión es transcendente**.*

Teorema **2.2.5** *Una extensión algebraica finitamente generada es finita.*

Ejemplo 2.2.4 *Comparar los cuerpos:*

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{2}+\sqrt{3}), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{3}), \quad y \quad \mathbb{Q}.$$

La relación es la siguiente:



para ello vemos que los polinomios mínimos de $\sqrt{2}, \sqrt{3}$ sobre $\mathbb{Q}$ son:

$$\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2, \qquad \left(x^2-2\right), \qquad \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2, \qquad \left(x^2-3\right).$$

Por lo tanto

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$$

ahora por la tower law sabemos que

$$\begin{aligned}\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\right] &= \left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right]\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] \\ &= ? \cdot 2\end{aligned}$$

luego nos falta por saber $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] = ?$. Pero $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] = 2$, siendo una base $B = \left\{1, \sqrt{3}\right\}$, de esta forma por la tower law llegamos a que

$$\left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\right] = 4$$

donde

$$B = \left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$$

mientras que el polinomio mínimo es:

$$x^4 - 10x^2 + 1.$$

Vemos también que $\left(x^2 - 2\right)$ *es polinomio mínimo de* $\sqrt{2}$ *sobre* $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$*, ya que si factorizásemos en* $\mathbb{Q}(\sqrt{3})$ *obtendríamos*

$$\sqrt{2} = r + s\sqrt{3}, \qquad r, s \in \mathbb{Q},$$

por lo que $d = f = e = 2$*. También sabemos que* $ab = cd = ef = 4$*, entonces* $c = 2$ *sii* $b = 4/a$*, de esta forma vemos que* $a = 1, 2, 4$*. Vemos que si* $a = 4$ *entonces llegaríamos a una contradicción ya que* $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$*. Para ver que* $a = 1$*,* y $b = 4$ *consideramos los polinomios*

$$p = \left(\left(x - \left(\sqrt{2} + \sqrt{3}\right)\right)^2 - 3\right) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})\,[x]\,,$$
$$q = \left(x^2 - 2\right) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})\,[x]\,,$$

distintos y $x = \sqrt{2}$ *es raíz, entonces*

$$m.c.d\,(p, q) = x - \sqrt{2},$$

viendo que

$$\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$
$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

entonces:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Veamos ahora con un poco más de detalle el cálculo del polinomio mínimo de $\sqrt{2} + \sqrt{3}$*, sobre* $\mathbb{Q}$*. Sabemos que* $\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right] = 4$*, por lo tanto el grado de dicho polinomio será* 4*, digamos*

$$x^4 + ax^3 + bx^2 + cx + d$$

por lo tanto

$$\left(\sqrt{2} + \sqrt{3}\right)^4 + a\left(\sqrt{2} + \sqrt{3}\right)^3 + b\left(\sqrt{2} + \sqrt{3}\right)^2 + c\left(\sqrt{2} + \sqrt{3}\right) + d = 0,$$

si desarrollamos esta ecuación entonces obtenemos:

$$5b + d + 11\sqrt{2}a + 9\sqrt{3}a + \sqrt{2}c + \sqrt{3}c + 20\sqrt{2}\sqrt{3} + 2\sqrt{2}\sqrt{3}b + 49 = 0$$

operando llegamos a que

$$A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6} = 0,$$

y por lo tanto el sistema a resolver es:

$$A = 49 + 5b + d = 0,$$
$$B = 11a + c = 0,$$
$$C = 9a + c = 0,$$
$$D = 20 + 2b = 0$$

de esta forma obtenemos $a = c = 0, b = -10$ *y* $d = 1$*, por lo tanto*

$$P = x^4 - 10x^2 + 1.$$

Otra forma *de atacar este problema, el de encontrar el* ***polinomio mínimo****, es la siguiente. Consideramos el polinomio* $P = \left(x - \sqrt{2}\right)^2 - 3 = x^2 - 2\sqrt{2}x - 1$*, tal que* $\sqrt{2} + \sqrt{3}$ *sea una raíz de p. Vemos que* $x^2 - 2\sqrt{2}x - 1 \notin \mathbb{Q}[x]$*, entonces para eliminar los radicales podemos multiplicar por el conjungado así que*

$$\left(x^2 - 2\sqrt{2}x - 1\right)\left(x^2 + 2\sqrt{2}x - 1\right) = x^4 - 10x^2 + 1$$

tal y como queríamos hacer ver.

2.3. Ejercicios.

Veremos unos cuantos ejercicios resueltos. En realidad se trata de generalizaciones de los ejemplos ya expuestos.

Ejercicio 2.3.1 *Establer las relaciones de inclusión entre los siguientes campos*

$$\mathbb{Q}\left(i, \sqrt{3}\right), \qquad \mathbb{Q}\left(\sqrt{-3}\right), \qquad \mathbb{Q}\left(i + \sqrt{3}\right).$$

Solución. Vemos que $\left(i + \sqrt{3}\right) \in \mathbb{Q}\left(i, \sqrt{3}\right)$, entonces

$$\mathbb{Q}\left(i + \sqrt{3}\right) \subseteq \mathbb{Q}\left(i, \sqrt{3}\right).$$

De igual forma se observa que $\sqrt{-3} = i\sqrt{3} \in \mathbb{Q}\left(i, \sqrt{3}\right)$, entonces

$$\mathbb{Q}\left(\sqrt{-3}\right) \subset \mathbb{Q}\left(i, \sqrt{3}\right).$$

Por último vemos que $\sqrt{-3} \in \mathbb{Q}\left(i + \sqrt{3}\right)$, ya que

$$\left(i + \sqrt{3}\right)^2 = -1 + 3 + \sqrt{-3} = 2 + i\sqrt{3},$$

ahora bien

$$i\sqrt{3} = \left(i + \sqrt{3}\right)^2 - 2 \in \mathbb{Q}\left(i + \sqrt{3}\right),$$

y por lo tanto

$$\mathbb{Q}\left(\sqrt{-3}\right) \subset \mathbb{Q}\left(i + \sqrt{3}\right),$$

de hecho se tiene que

$$\mathbb{Q}\left(i + \sqrt{3}\right) = \mathbb{Q}\left(i, \sqrt{3}\right),$$

tal y como queríamos hacer ver. ■

Ejercicio 2.3.2 *Hallar el grado de las siguientes extensiones.*

Solución.

1.
$$\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right),$$

Vemos que $\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right)=\mathbb{Q}\left(\sqrt[4]{2}\right)$, ya que $\sqrt{2}=\left(\sqrt[4]{2}\right)^2$. El grado de la extensión es:

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]=n$$

será igual al grado del polinomio mínimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}\left(\sqrt{2}\right)$ y dicho polinomio es: $P=x^2-\sqrt{2}$, por lo que $n=2$.

$$\begin{array}{c}\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right)\\ |\,2\\ \mathbb{Q}\left(\sqrt{2}\right)\\ |\,2\\ \mathbb{Q}\end{array}$$

2. Sea $\xi=e^{2\pi i/5}$ una raíz quinta de la unidad, $x^5-1=(x-1)\left(x^4+x^3+x^2+x+1\right)$, entonces
$$[\mathbb{Q}(\xi):\mathbb{Q}]=n-1$$
donde $n=5$, en este caso.
En general tenemos que si $\xi=e^{2\pi i/n}$,es una raíz $n-$ésima de la unidad, i.e. es raíz del polinomio
$$x^n-1=(x-1)\left(x^{n-1}+x^{n-2}+.....+x^2+x+1\right)$$
y por lo tanto
$$[\mathbb{Q}(\xi):\mathbb{Q}]=n-1$$
siempre y cuando n sea primo.

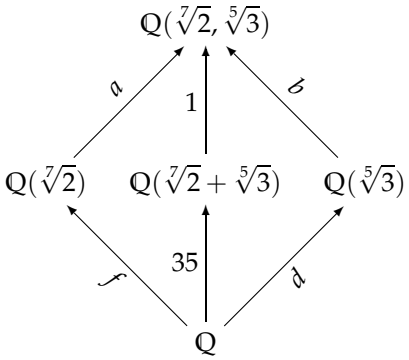
3. En este caso queremos calcular el grado de
$$\left[\mathbb{Q}\left(\sqrt[6]{5}\right):\mathbb{Q}\right]=6$$
ya que por el criterio de Eisentein $x^6-5=0$ es un polinomio irreducible.
Observar que las raíces del polinomio son:
$$\pm\sqrt[6]{5}\left(-\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\pm\sqrt[6]{5}\left(\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\pm\sqrt[6]{5}$$

4. Una pequeña generalización del anterior ejercicio es la siguiente:
$$\left[\mathbb{Q}\left(\sqrt[3]{5},\sqrt[6]{5}\right):\mathbb{Q}\left(\sqrt{5}\right)\right]=3$$
vemos que $\sqrt[3]{5}=\left(\sqrt[6]{5}\right)^2$, entonces $\mathbb{Q}\left(\sqrt[3]{5},\sqrt[6]{5}\right)=\mathbb{Q}\left(\sqrt[6]{5}\right)$, y aplicando el teorema de tower law vemos que
$$\left[\mathbb{Q}\left(\sqrt[6]{5}\right):\mathbb{Q}\right]=6=\left[\mathbb{Q}\left(\sqrt[6]{5}\right):\mathbb{Q}\left(\sqrt{5}\right)\right]\left[\mathbb{Q}:\mathbb{Q}\left(\sqrt{5}\right)\right]=3\cdot 2$$

5. Queremos calcular

$$\left[\mathbb{Q}\left(\sqrt[7]{2},\sqrt[5]{3}\right):\mathbb{Q}\right]=n=35,$$

vemos en el siguiente gráfico la situación



Sabemos que $f=7$, x^7-2, y que $d=5$, x^5-3, por lo que $n=a7=b5$. Aplicando el teorema llegamos a la conclusión de que $a=5$ y $b=7$.

■

Ejercicio 2.3.3 *Calcular el polinomio mínimo de* $\sqrt{3}+\sqrt{5}$ *en* $\mathbb{Q}\left(\sqrt{15}\right)$.

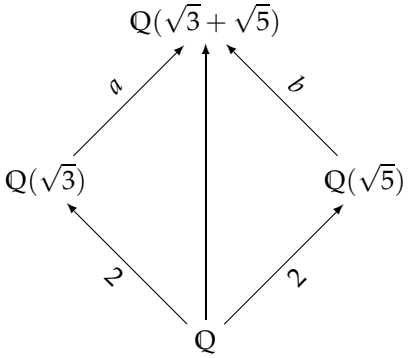
Solución. Sea $\alpha=\sqrt{3}+\sqrt{5}\in\mathbb{Q}\left(\sqrt{15}\right)$, tomamos $\alpha^2=3+2\sqrt{3}\sqrt{5}+5=8+2\sqrt{15}$, entonces

$$x^2-\left(8+2\sqrt{15}\right)\in\mathbb{Q}\left(\sqrt{15}\right)[x]$$

es el polinomio buscado. ■

Ejercicio 2.3.4 *Calcular el grado de* $\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]$.

Solución. Sea



Vemos del gráfico que

$$\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right]=2, \qquad x^2-3=m^{\mathbb{Q}}_{\sqrt{3}},$$
$$\left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right]=2, \qquad x^2-5=m^{\mathbb{Q}}_{\sqrt{5}},$$

queremos calcular $\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]$. Del teorema tower law sabemos que

$$\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right],$$

vemos que el polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$ es x^2-5 por lo que

$$\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]=2,$$

y por lo tanto

$$\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\right]=2\cdot 2=4,$$

tal y como querímos hacer ver.

De igual forma vemos que

$$B_{\sqrt{3}}=\left\{1,\sqrt{3}\right\}=\{1,\alpha\}, \qquad B_{\sqrt{5}}=\left\{1,\sqrt{5}\right\}=\{1,\beta\},$$

son respectivas bases de $\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ sobre $\mathbb{Q}\left(\sqrt{3}\right)$ y $\mathbb{Q}\left(\sqrt{5}\right)$ y por lo tanto

$$B_{\sqrt{3}+\sqrt{5}}=\left\{1,\sqrt{3},\sqrt{5},\sqrt{15}\right\}, \qquad B_{\sqrt{3}+\sqrt{5}}=\{1,\alpha,\beta,\alpha\beta\},$$

es una base de $\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$. Calculamos el polinomio mínimo

$$\left(\sqrt{3}+\sqrt{5}\right)^2=8+2\sqrt{15}, \qquad \left(\sqrt{3}+\sqrt{5}\right)^4=124+32\sqrt{15},$$

de esta forma llegamos a que

$$m^{\mathbb{Q}}_{\sqrt{3}+\sqrt{5}}=x^4-16x^2+4,$$

También podemos proceder como sigue:

$$\left(x-\sqrt{3}\right)^2-5=x^2-2\sqrt{3}x-2,$$

entonces

$$\left(x^2-2\sqrt{3}x-2\right)\left(x^2+2\sqrt{3}x-2\right)=x^4-16x^2+4,$$

tal y como queríamos hacer ver. ■

Ejercicio 2.3.5 *Hallar el grado de la extensión*

$$\left[\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right):\mathbb{Q}\right].$$

Solución. Para ello calculamos el polinomio mínimo. Sea $\alpha = \sqrt{1+\sqrt{3}}$, entonces

$$\alpha^2 = \left(\sqrt{1+\sqrt{3}}\right)^2 = 1+\sqrt{3}, \qquad \alpha^2 - 1 = \sqrt{3},$$

y por lo tanto

$$\alpha^4 - 2\alpha^2 + 1 = 3,$$

de esta forma llegamos a que el polinomio mínimo será:

$$P(x) = x^4 - 2x^2 - 2,$$

que es irreducible por el criterio de Einstein y por lo tanto el grado de la extensión es 4. ■

Ejercicio 2.3.6 *Encontrar un número complejo α tal que*

$$\mathbb{Q}\left(\sqrt{2}, i\right) = \mathbb{Q}\left(\alpha\right).$$

Solución. Podemos sospechar que $\alpha = \sqrt{2}+i$, por lo que llevamos visto, el problema es demostrarlo. Sea $L = \mathbb{Q}\left(\sqrt{2}, i\right)$ sabemos por los ejemplos expuestos que

$$\mathbb{Q}\left(\sqrt{2}, i\right) = \mathbb{Q}\left(\sqrt{2}+i\right),$$

y por lo tanto el número buscado será $\alpha = \sqrt{2}+i$. Claramente $\mathbb{Q}\left(\sqrt{2}+i\right) \subset L$, por lo que sólo tendremos que demostrar la otra inclusión.y para ello es suficiente con demostrar que $\sqrt{2}, i$ están en $\mathbb{Q}\left(\sqrt{2}+i\right)$, (recordar que una vez tengamos que estos dos elementos están en $\mathbb{Q}\left(\sqrt{2}+i\right)$ inmediatamente sabemos que el campo L está contenido en $\mathbb{Q}\left(\sqrt{2}+i\right)$ ya que L es por definición el campo más pequeño que contiene a $\mathbb{Q}$, $\sqrt{2}$ y a i).

Calcualndo potencias de α vemos lo que se genera:

$$\alpha^2 = \left(\sqrt{2}+i\right)^2 = 1+2i\sqrt{2},$$
$$\alpha^3 = \left(\sqrt{2}+i\right)^3 = 5i-\sqrt{2},$$

entonces como estos dos elementos están en $\mathbb{Q}\left(\sqrt{2}+i\right)$ vemos que

$$\alpha+\alpha^3 = \left(\sqrt{2}+i\right) + \left(5i-\sqrt{2}\right) = 6i \in \mathbb{Q}\left(\sqrt{2}+i\right)$$

donde $i \in \mathbb{Q}\left(\sqrt{2}+i\right)$, $\alpha - i \in \mathbb{Q}\left(\sqrt{2}+i\right)$, entonces $\alpha = i+\sqrt{2}$, es el número buscado. ■

Ejercicio 2.3.7 *Demostrar que*

$$\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right).$$

Solución. Vemos que

$$\mathbb{Q}\left(\sqrt{2}, \sqrt[4]{2}\right) = \mathbb{Q}\left(\sqrt[4]{2}\right),$$
$$\mathbb{Q}\cup\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right),$$

dando

$$\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right).$$

Por otro lado sabemos que

$$\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2,$$

ya que su polinomio mínimo es $x^4 - 2 = m^{\mathbb{Q}}_{\sqrt[4]{2}}$, mónico e irreducible y po lo tanto

$$\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 4,$$

entonces

$$\mathbb{Q}\left(\sqrt{2}\right) \neq \mathbb{Q}\left(\sqrt[4]{2}\right),$$

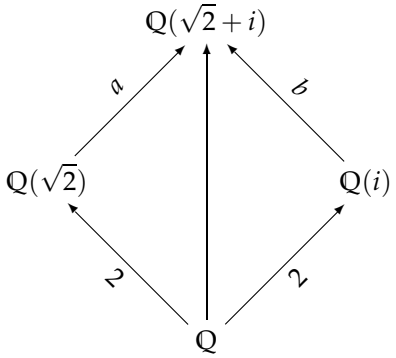
tal y como queríamos hacer ver. ■

Ejercicio 2.3.8 *Encontrar el polinomio mínimo de los siguientes números sobre* $\mathbb{Q}$.

Solución.

1. $(1+i)$. Sea $(1+i) \notin \mathbb{Q}$, sabemos que
$$[\mathbb{Q}(1+i) : \mathbb{Q}] \geq 2,$$
si tenemos en cuenta que
$$(1+i)^2 = 2i = 2(i+1) - 2$$
entonces
$$f(1+i) = 0$$
donde $(x - i - 1)^2 = x^2 - 2(1+i)x + 2i = 0$, entonces
$$f = x^2 - 2x + 2$$
$(2i - 2(i+1) + 2)$, será el polinomio mínimo por el criterio de Eisenstein.

2. $\left(\sqrt{2} + i\right)$, el panorama es el siguiente



por lo tanto uno debe esperar que el polinomio mínimo tenga al menos 4 orden.
Podemos operar de la siguiente forma

$$(x - i)^2 - 2 = x^2 - 2ix - 3$$

así que

$$\left(x^2-2ix-3\right)\left(x^2+2ix-3\right)=x^4-2x^2+9$$

y ahora podemos arguentar que es irreducible sobre $\mathbb{Q}$.

Sabemos que

$$\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right]=2,$$

y que es muy fácil ver que

$$\left[\mathbb{Q}\left(\sqrt{2}+i\right):\mathbb{Q}(\sqrt{2})\right]=2,$$

basta on considerar que $x^2+1\in\mathbb{Q}(\sqrt{2})[x]$. Tenemos en cuenta ahora el teorema tower law

$$\left[\mathbb{Q}\left(\sqrt{2}+i\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{2}+i\right):\mathbb{Q}(\sqrt{2})\right]=2\cdot 2=4,$$

por lo tanto el grado del polinomio mínimo debe ser 4.

■

Ejercicio 2.3.9 *Calcular para cada par de campos L, F*

$$[L:F]$$

y dar una base para L sobre F.

Solución.

1. $L=\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right), F=\mathbb{Q}$. Lo primero que debemos hacer es comprobar que

$$\sqrt[3]{2}\notin\mathbb{Q}\left(\sqrt{2}\right)=\left\{a+b\sqrt{2},a,b\in\mathbb{Q}\right\},$$

viéndose que x^3-2 es irreducible sobre $\mathbb{Q}\left(\sqrt{2}\right)$, y por lo tanto

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=3\cdot 2=6,$$

más aun,

$$B=\left\{1,\sqrt[3]{2},\sqrt[3]{4}\right\}=\left\{1,\beta,\beta^2\right\},$$

es una base de $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)$ sobre $\mathbb{Q}\left(\sqrt{2}\right)$, y

$$B=\left\{1,\sqrt{2}\right\}=\{1,\alpha\},$$

es otra base de $\mathbb{Q}\left(\sqrt{2}\right)$ sobre $\mathbb{Q}$. Por lo tanto por la tower law tenemos que

$$B=\left\{1,\sqrt[3]{2},\sqrt[3]{4},\sqrt{2},\sqrt{2}\sqrt[3]{2},\sqrt{2}\sqrt[3]{4}\right\}=\left\{1,\alpha,\beta,\beta^2,\alpha\beta,\alpha\beta^2\right\},$$

es una base de $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)$ sobre $\mathbb{Q}$.

2. $L = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$, $F = \mathbb{Q}$. Vemos que

$$m_{\sqrt[4]{2}}^{\mathbb{Q}} = x^4 - 2, \qquad B = \left\{1, \sqrt[4]{2}, \left(\sqrt[4]{2}\right)^2, \left(\sqrt[4]{2}\right)^3\right\} = \left\{1, \beta, \beta^2, \beta^3\right\}$$

por otro lado tenemos que

$$m_i^{\mathbb{Q}} = x^2 + 1, \qquad B = \{1, i\} = \{1, \alpha\},$$

y por lo tanto

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8,$$

obteniendo así la siguiente base:

$$\begin{aligned} B &= \left\{1, \sqrt[4]{2}, \left(\sqrt[4]{2}\right)^2, \left(\sqrt[4]{2}\right)^3, i, i\sqrt[4]{2}, i\left(\sqrt[4]{2}\right)^2, i\left(\sqrt[4]{2}\right)^3\right\} \\ &= \left\{1, \alpha, \beta, \beta^2, \beta^3, \alpha\beta, \alpha\beta^2, \alpha\beta^3\right\}, \end{aligned}$$

tal y como queríamos hacer ver.
Si $F = \mathbb{Q}(i)$ entonces deberemos de proceder como sigue:

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}(i)\right][\mathbb{Q}(i) : \mathbb{Q}] = ? \cdot 2 = 8,$$

entonces

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}(i)\right] = 4,$$

tenemos que $x^4 - 2$ es un polinomio sobre $\mathbb{Q}$ y por lo tanto sobre $\mathbb{Q}(i)$, que tiene por raíz $\sqrt[4]{2}$. Por lo tanto

$$m_{\sqrt[4]{2}}^{\mathbb{Q}(i)} = x^4 - 2,$$

y la base de $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$ sobre $\mathbb{Q}(i)$ es en este caso:

$$B = \left\{1, \sqrt[4]{2}, \left(\sqrt[4]{2}\right)^2, \left(\sqrt[4]{2}\right)^3\right\}.$$

3. $L = \mathbb{Q}\left(i, \sqrt{3}, \xi\right)$, $F = \mathbb{Q}$, donde ξ es una raíz cúbica de la unidad $(x^3 - 1)$.
Vemos que

$$\xi = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2} \in \mathbb{Q}\left(i, \sqrt{3}\right)$$

por lo que

$$\mathbb{Q}\left(i, \sqrt{3}, \xi\right) = \mathbb{Q}\left(i, \sqrt{3}\right)$$

y por lo tanto siguiendo los mismos pasos de antes encontramos que

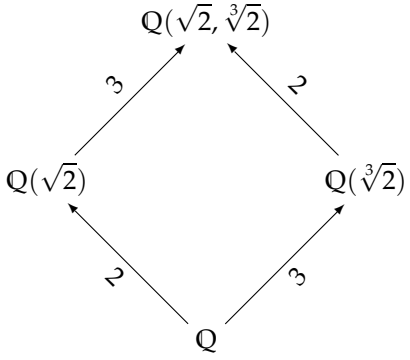
$$B = \left\{1, \sqrt{3}, i, i\sqrt{3}\right\}$$

por lo tanto el grado de la extensión será 4.

Tal y como queríamos hacer ver. ■

Ejercicio 2.3.10 *Determinar una base para* $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$ *sobre* $\mathbb{Q}$. *Deducir que* $\left(\sqrt[6]{2}\right) \in K$ *y que* K *es una extensión simple de* $\mathbb{Q}$.

Solución. Vemos que



donde, (apelando al teorema tower law) vemos que

$$B_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = \left\{1, \sqrt{2}\right\} = \{1, \alpha\},$$
$$B_{\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)/\mathbb{Q}(\sqrt{2})} = \left\{1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right\} = \left\{1, \beta, \beta^2\right\},$$

por lo tanto, la base buscada será:

$$B_{\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)/\mathbb{Q}} = \left\{1, \sqrt{2}, \sqrt[3]{2}, (2)^{5/6}, 2^{2/3}, 2^{7/6}\right\} = \left\{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\right\},$$

ya que

$$2^{1/3} \cdot 2^{1/2} = 2^{5/6}, \qquad y \qquad 2^{2/3} \cdot 2^{1/2} = 2^{7/6},$$

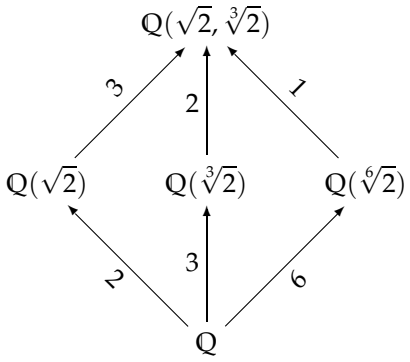
de esta forma vemos que

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[6]{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$$

donde $\left(\sqrt[6]{2}\right)$ es un cero de $p = x^6 - 2$, que e s irreducible sobre $\mathbb{Q}$, entonces p es el polinomio mínimo de $\left(\sqrt[6]{2}\right)$ sobre $\mathbb{Q}$, verificándose

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}\left(\sqrt[6]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[6]{2}\right) : \mathbb{Q}\right] = 1 \cdot 6 = 6,$$

obteniéndose el siguiente diagrama



y por lo tanto

$$\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[6]{2}\right)$$

es una extensión simple. ■

Ejercicio 2.3.11 *Sea $K = \mathbb{Q}/(f,g)$, donde f,g son dos polis. Queremos calcular $[K:\mathbb{Q}]$.*

Solución. Empezamos calculando

$$mcd(f,g) = d$$

observando que $\mathbb{Q}[x]$ es un DIP (Euclides). El polinomio d es irreducible. Por lo tanto

$$K = \mathbb{Q}/d$$

tenemos que calcular las raíces de d para ver los subcuerpos. Por lo tanto

$$[K:\mathbb{Q}] = \partial d$$

i.e. al grado del polinomio d. ■

Ejercicio 2.3.12 *Sean $(p_i)_{i=1}^3$, tres números primos, definimos $K = \mathbb{Q}\left[\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}\right]$, queremos calcular $[K:\mathbb{Q}]$.*

Solución. Vemos que

$$\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{p_1}\right] \subset \mathbb{Q}\left[\sqrt{p_1}, \sqrt{p_2}\right] \subset K = \mathbb{Q}\left[\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}\right]$$

donde denotamos

$$F_2 = \mathbb{Q}\left[\sqrt{p_1}\right], \qquad F_1 = \mathbb{Q}\left[\sqrt{p_1}, \sqrt{p_2}\right],$$

así que por el teorema TL vemos que

$$[K:\mathbb{Q}] = [K:F_1]\,[F_1:F_2]\,[F_2:\mathbb{Q}] = 2\cdot 2\cdot 2 = 8$$

donde

$$[F_2:\mathbb{Q}] = 2, \qquad x^2 - p_1 = 0, \qquad B_{F_2} = \left\{1, \sqrt{p_1}\right\},$$

por otro lado vemos que

$$[F_1:\mathbb{Q}] = 4, \qquad \left(x^2 - p_1\right)\left(x^2 - p_2\right) = 0, \qquad B_{F_2} = \left\{1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1 p_2}\right\},$$

por lo tanto

$$[K:\mathbb{Q}] = 2\cdot 4 = 8$$

tal y como queríamos hacer ver. ■

Ejercicio 2.3.13 *Encontrar E y su grado en los siguientes casos:*

Solución.

1. $\left(x^9 - 1\right)$. Vemos que

   $$\left(x^9 - 1\right) = \left(x^3 - 1\right)\left(x^6 + x^3 + 1\right) = p\cdot q,$$

   donde

   $$R_p = \left\{\frac{1}{2}\left(-1 \pm \sqrt{3i}\right), 1\right\} = \left\{1, r, \bar{r}\right\}, \qquad R_q = \left\{\zeta_i\right\}_{i=1}^6 = \left\{\bar{r}^{1/3}, \bar{r}^{1/3}r, \bar{r}^{1/3}\bar{r}, r^{1/3}r, r^{1/3}\bar{r}\right\},$$

   viendo que $E = \mathbb{Q}(\zeta)$, y de esta forma

   $$[E:\mathbb{Q}] = 6 = \partial q$$

   ya que q es irreducible.

2. $x^4+5x^2+6=\left(x^2+2\right)\left(x^2+3\right)$, por lo tanto $E=\mathbb{Q}\left(\sqrt{2i},\sqrt{3i}\right)$ de esta fora

$$[E:\mathbb{Q}]=4.$$

3. x^6-8, que es irreducible, y donde sus raíces son

$$R_p=\left\{\pm\sqrt{2},\pm\sqrt{2}r,\pm\sqrt{2}r'\right\},$$

donde

$$r=\frac{1}{2}\left(1+\sqrt{3i}\right),\qquad r'=\frac{1}{2}\left(-1+\sqrt{3i}\right),$$

por lo tanto

$$E=\mathbb{Q}\left(\sqrt{2},r\right),$$

concluimos que

$$[E:\mathbb{Q}]=4.$$

Tal y como queríamos hacer ver. ■

Ejercicio 2.3.14 *Calcular la extensión E de $p(x)=x^6-1$, así como el grado.*

Solución. Vemos que

$$p(x)=x^6-1=(x-1)(x+1)\left(x^2+x+1\right)\left(x^2-x+1\right)=\left(x^3-1\right)(x+1)\left(x^2-x+1\right)$$

y donde sus raíces son

$$R_p=\left\{\frac{1}{2}\left(\pm1\pm i\sqrt{3}\right),\pm1\right\},$$

por lo tanto

$$E=\mathbb{Q}\left(\sqrt{3i}\right),$$

de esta forma vemos que:

$$[E:\mathbb{Q}]=2,\qquad [E:\mathbb{Q}(i)]=2,$$

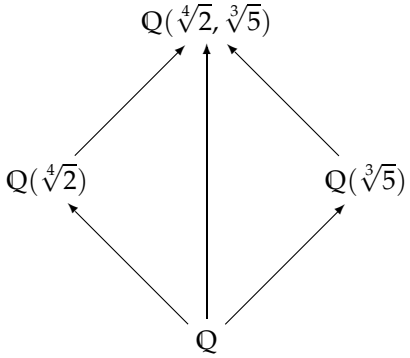
donde en el último caso hemos considerado $E=\mathbb{Q}\left(i,\sqrt{3}\right)$. ■

Ejercicio 2.3.15 *Calcular el grado de cada una de las siguientes extensiones E/K:*

Solución.

1. $\left[\mathbb{Q}\left(\sqrt[4]{2},\sqrt[3]{5}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]$.

Aunque no nos lo piden, comenzamos calculando $\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right]$ ya que esto simplifica considerablemente los cálculos. Consideramos el diagrama:



Como $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 4$, (ya que el polinomio míinimo de $\sqrt[4]{2}$ es $x^4 - 2$ -irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein) se tiene que $4 | \left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right]$. Además, $\left[\mathbb{Q}\left(\sqrt[3]{5}\right) : \mathbb{Q}\right] = 3$ (ya que el polinomio míinimo de $\sqrt[3]{5}$ es $x^3 - 5$ -irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein), por lo que $3 | \left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right]$. Como consecuencia $12 | \left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right]$.

Por otro lado como $x^4 - 2$ es un múltiplo del polinomio míinimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}\left(\sqrt[3]{5}\right)$ se tiene que $\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\left(\sqrt[3]{5}\right)\right] \leq 4$. Por lo tanto:

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\left(\sqrt[3]{5}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{5}\right) : \mathbb{Q}\right] = 4 \cdot 3 = 12.$$

Ahora observamos que como $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ya que el polinomio míinimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $x^2 - 2$ (irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein), necesariamente $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$, como consecuencia:

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = \frac{\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right) : \mathbb{Q}\right]}{\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right]} = 6.$$

El conjunto $\{1, \sqrt[4]{2}\}$ es una base de $\mathbb{Q}\left(\sqrt[4]{2}\right)$ sobre $\mathbb{Q}\left(\sqrt{2}\right)$, mientras que $\{1, \sqrt[3]{5}, \sqrt[3]{5^2}\}$ es una base de $\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[3]{5}\right)$ sobre $\mathbb{Q}\left(\sqrt[4]{2}\right)$, de modo que aplicando el Teorema de la base se tiene que el conjunto

$$\{1, \sqrt[4]{2}, \sqrt[3]{5}, \sqrt[3]{5^2}, \sqrt[4]{2}\sqrt[3]{5}, \sqrt[3]{5}\sqrt[3]{5^2}\} = \left\{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\right\},$$

es una base de E/K.

Observación 2.3.1 *El Criterio de Eisenstein sólo es válido para comprobar la irreducibilidad de un polinomio sobre* $\mathbb{Q}$. ***NO*** *se puede utilizar por ejemplo para demostrar que el polinomio* $x^3 - 5$ *es irreducible sobre* $\mathbb{Q}\left(\sqrt[4]{2}\right)$*, porque sobre este cuerpo el criterio no tiene por qué ser válido.*

Para demostrar que $x^3 - 5$ *no tiene raíces en* $\mathbb{Q}\left(\sqrt[4]{2}\right)$ *hay que probar que no hay ningún elemento en este cuerpo cuyo cubo sea cinco. Para ello* ***no es suficiente*** *suponer que un elemento genérico de* $\mathbb{Q}\left(\sqrt[4]{2}\right)$ *es de la forma* $a + b\sqrt[4]{2}$ *con* $a, b \in \mathbb{Q}$*. Un elemento genérico de* $\mathbb{Q}\left(\sqrt[4]{2}\right)$ *es de la forma* $a + b\sqrt[4]{2} + c\sqrt[4]{2^2} + d\sqrt[4]{2^3}$*, con* $a, b, c, d \in \mathbb{Q}$*.*

2. $E = \mathbb{F}_3(\alpha)$, $K = \mathbb{F}_3$, donde α es una raíz del poli $\left(x^2 + 1\right)\left(x^2 + x + 1\right) \in \mathbb{F}_3[x]$.

Vemos que las raíces del polinomio son

$$R_p = \left\{ \frac{1}{2}\left(-1 \pm \sqrt{3i}\right), \pm i \right\}.$$

Sea $p(x) = x^2 + 1 \in \mathbb{F}_3[x]$ y $q(x) = x^2 + x + 1 \in \mathbb{F}_3[x]$. Entonces $p(\alpha) = 0$ ó $q(\alpha) = 0$

Si $q(\alpha) = 0$ entonces $\alpha = 1$, por lo tanto $E = \mathbb{F}_3$ y por lo tanto $[E : K] = 1$..

Si $p(\alpha) = 0$, entonces $\alpha \notin \mathbb{F}_3$, (ya que p es irreducible sobre $\mathbb{F}_3$, por ser un polinomio de grado dos sin raíces en $\mathbb{F}_3$). Por ser $p(x)$ irreducible sobre $\mathbb{F}_3$ además es el polinomio míinimo de α sobre este cuerpo, por tanto $[E : K] = 2$ y el conjunto $\{1, \alpha\}$ es una base de E/K.

Observación 2.3.2 *Para calcular las raíces de un polinomio de grado 2 sobre un cuerpo K con $charK = p \neq 2$ se puede aplicar la fórmula cuadrática, teniendo presente los siguientes detalles:*

1. La notación no debería ser racional. Por ejemplo, en $\mathbb{F}_3$ no escribimos $1/2$ si no $2^{-1} \equiv 2$.

2. El resultado al aplicar la fórmula, no puede ser un número complejo. Los complejos forman un cuerpo de característica cero cuyo subcuerpo primo es el de los racionales. Por lo tanto nada tienen que ver con una expresión que involucra operaciones entre números que pertenecen a $\mathbb{F}_3$. En particular un polinomio en $\mathbb{F}_p$ no puede tener raíces complejas. Como mucho tendrá raíces en una extensión finita de $\mathbb{F}_p$.

3. $E = \mathbb{R}(x)$, $K = \mathbb{R}(x^2)$ donde x es una variable.
   El polinomio $T^2 - x^2 \in \mathbb{R}(x^2)[T]$ es un múltiplo del polinomio míinimo de x sobre $\mathbb{R}(x^2)$, por lo que $[\mathbb{R}(x) : \mathbb{R}(x^2)] \leq 2$. Si $[\mathbb{R}(x) : \mathbb{R}(x^2)] = 1$ entonces $\mathbb{R}(x) = \mathbb{R}(x^2)$ hecho que no es cierto. Por tanto

$$[\mathbb{R}(x) : \mathbb{R}(x^2))] = 2,$$

   y $\{1, x\}$ es una base de E/K.

■

Ejercicio 2.3.16 *Decide razonadamente si las siguientes afirmaciones son verdaderas o falsas.*

Solución.

1. Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $x^4 - 15x + 9x + 21 \in \mathbb{Q}[x]$. Entonces $\sqrt[3]{5} \in \mathbb{Q}(\alpha)$.
   Falso: Usando el criterio de Eisenstein para el primo 3, obtenemos que el polinomio $x^4 - 15x + 9x + 21$ es irreducible sobre $\mathbb{Q}$ y por lo tanto es el polinomio míinimo de α. Por eso, la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ tiene grado 4. La extensión $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ tiene grado 3, ya que el polinomio míinimo de $\sqrt[3]{5}$ sobre $\mathbb{Q}$ es $x^3 - 5$ y tiene grado 3. Como el grado de subextensión divide al grado de extensión, $\mathbb{Q}(\sqrt[3]{5})$ no puede ser subcuerpo de $\mathbb{Q}(\alpha)$ y por lo tanto $\sqrt[3]{5} \notin \mathbb{Q}(\alpha)$.

2. Sean $K \subset E \subset L$ cuerpos y sea $\beta \in L$. Entonces el grado del polinomio irreducible (míinimo) de sobre E es menor o igual que el grado del polinomio irreducible (míinimo) de sobre K.
   Verdadero: Sea p el polinomio míinimo de sobre K y q el polinomio míinimo de β sobre E. El polinomio p es también un polinomio con coeficientes en E y además anula a β ($p(\beta) = 0$). Por lo tanto q divide a p. Esto implica que el grado de q es menor o igual que el grado de p.

3. El grado del polinomio míinimo de $1 + \sqrt[5]{7} + 2\sqrt[5]{7^2} - 3\sqrt[5]{7^3}$ sobre $\mathbb{Q}$ es 5.
   Verdadero: El polinomio míinimo de $\sqrt[5]{7}$ sobre $\mathbb{Q}$ es $x^5 - 7$. Luego el grado de extensión $\mathbb{Q}(\sqrt[5]{7})/\mathbb{Q}$ es 5. Además,

$$\{1, \sqrt[5]{7}, \sqrt[5]{7^2}, \sqrt[5]{7^3}, \sqrt[5]{7^4}\}$$

es una base de $\mathbb{Q}(\sqrt[5]{7})$ sobre $\mathbb{Q}$. En particular, $1+\sqrt[5]{7}+2\sqrt[5]{7^2}-3\sqrt[5]{7^3} \notin \mathbb{Q}$. Por lo tanto

$$\mathbb{Q}\left(1+\sqrt[5]{7}+2\sqrt[5]{7^2}-3\sqrt[5]{7^3}\right) \neq \mathbb{Q}$$

Como el grado de $\mathbb{Q}(\sqrt[5]{7})/\mathbb{Q}$ es un número primo, $\mathbb{Q}(\sqrt[5]{7})/\mathbb{Q}$ tiene sólo dos subextensiones. Por eso,

$$\mathbb{Q}\left(1+\sqrt[5]{7}+2\sqrt[5]{7^2}-3\sqrt[5]{7^3}\right) = \mathbb{Q}(\sqrt[5]{7}),$$

El grado del polinomio míinimo de $1+\sqrt[5]{7}+2\sqrt[5]{7^2}-3\sqrt[5]{7^3}$ es igual al grado de extensión

$$\mathbb{Q}\left(1+\sqrt[5]{7}+2\sqrt[5]{7^2}-3\sqrt[5]{7^3}\right)/\mathbb{Q}$$

y por lo tanto es igual a 5.

■

Ejercicio 2.3.17 *Sea $\alpha \in \mathbb{C}$ un número algebraico sobre $\mathbb{Q}$.*

1. *Demuestra que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] \leq 3$.*
2. *¿Existe algún $\alpha \in \mathbb{C}$ tal que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] = 1$?*
3. *¿Existe algún $\alpha \in \mathbb{C}$ tal que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] = 2$?*
4. *¿Existe algún $\alpha \in \mathbb{C}$ tal que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] = 3$?*

Solución. Con respecto a la primera cuestión, vemos que como $x^3-\alpha^3 \in \mathbb{Q}(\alpha^3)[x]$ es un múltiplo del polinomio míinimo de a sobre $\mathbb{Q}(\alpha^3)$, se tiene que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] \leq 3$.

Con respecto a la segunda, Para cualquier $\alpha \in \mathbb{Q}$ se tiene que $\mathbb{Q}(\alpha) = \mathbb{Q}$ y por tanto la respuesta es trivialmente afirmativa. La respuesta es también afirmativa para $a = i$ ó $a = \sqrt{2}$ por ejemplo. Hay otras muchas posibles elecciones.

Con respecto a la tercera, vemos que basta tomar a como una raíz cúbica no real de la unidad. Por ejemplo, si $a = e^{2\pi i/3}$ entonces $a^3 = 1$, $\mathbb{Q}(\alpha^3) = \mathbb{Q}$ y el polinómio míinimo de a sobre $\mathbb{Q}$ es el polinomio ciclotómico $p(x) = x^2+x+1$ que es irreducible (usar el Criterio de Eisenstein sobre $p(x+1)$). Por lo tanto en este caso $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] = 2$.

Por último, si tomamos $a = \sqrt[3]{2}$ entonces $a^3 = 2$ y $\mathbb{Q}(\alpha^3) = \mathbb{Q}$. En este caso $\left[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^3)\right] = 3$ ya que el polinomio míinimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es x^3-2 (puesto que es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein). ■

Capítulo 3

Teoría de Galois

3.1. El cuerpo de descomposición

3.1.1. El cuerpo de descomposición de un polinomio

Definición **3.1.1** *Sea F/K una extensión de cuerpos y $P \in K[x]$. Se dice que P se descompone sobre F si P factoriza como producto de polinomios de primer grado con coeficientes en F.*

Evidentemente, si $P \in K[x]$ se descompone sobre F, entonces $P = c(x-u_1)\cdots(x-u_n)$ con $c \in K$ y $u_1,\cdots,u_n$ son raíces de P.

Definición **3.1.2** *Sea F/K una extensión de cuerpos y $P \in K[x]$ un polinomio que se descompone sobre F. Se llama el **cuerpo de descomposición** de P en F sobre K, al menor subcuerpo de F que contiene a K y sobre el cual P se descompone.*

Es claro que si $P \in K[x]$ se descompone sobre F y $u_1,\cdots,u_n$ son sus raíces, entonces el cuerpo de descomposición de P es $K(u_1,\cdots,u_n)$.

Ejemplo 3.1.1

1. $P = x^2 - 2$. *El cuerpo de descomposición de P en $\mathbb{C}$ es $\mathbb{Q}(\sqrt{2})$.*
2. $P = x^2 - 2x - 1$. *El cuerpo de descomposición de P en $\mathbb{C}$ es $\mathbb{Q}(\sqrt{2})$*
3. $P = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. *Observamos que P es irreducible por el criterio de Eisenstein. Las raíces de P en $\mathbb{R}$ son $\alpha = \sqrt{2+\sqrt{2}}$, $\beta = \sqrt{2-\sqrt{2}}$, $-\alpha$ y $-\beta$. Por tanto, el cuerpo de descomposición de P en $\mathbb{C}$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha,\beta)$. Ahora, $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$. Así, tenemos que $\beta \in \mathbb{Q}(\alpha)$ y $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Además, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.*
4. $P = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$, *entonces su CD es $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Observar que*
$$x^4 - 4x^2 + 2 = \left(x^2 - 2\right)\left(x^2 - 3\right)$$
5. $P = x^4 - 2$. *El cuerpo de descomposición de P en $\mathbb{C}$ es $\mathbb{Q}(\sqrt[4]{2}, i) \neq \mathbb{Q}[\sqrt[4]{2}]$.*
6. *El CD de $P = x^n + 1 \in \mathbb{Q}\left(\sqrt{2}\right)[x]$ es $\mathbb{Q}\left(\sqrt{2},\xi\right)$ donde $\xi = e^{2\pi i/n}$.*

Nuestro próximo objetivo es probar que todo polinomio $p \in K[x]$ tiene un cuerpo de descomposición y que éste es único, salvo isomorfismos que fijen los elementos de K (es decir, no depende dentro de qué cuerpo se construye).

Lema 3.1.1 *Supongamos que $p \in K[x]$ es irreducible. Entonces existe una extensión E/K tal que p tiene una raíz en E.*

Teorema 3.1.1 *(Existencia de Cuerpos de Descomposición) Sea K un cuerpo y $f \in K[x]$ no constante. Entonces existe un cuerpo de descomposición de f sobre K.*

Definición 3.1.3 *Sean E/K y F/K dos extensiones de cuerpos y $f : E \to F$ un homomorfismo de cuerpos. Digamos que f es un $K-$homomorfismo si $f(k) = k$ para todo $k \in K$.*

Teorema 3.1.2 *(Unicidad de los Cuerpos de descomposición). Sea K un cuerpo y sea $f \in K[x]$ no constante. Si E_1 y E_2 son cuerpos de descomposición de f sobre K, entonces existe un $K-$isomorfismo $\tau : E_1 \to E_2$.*

3.1.2. Extensiones normales

Definición 3.1.4 *Digamos que F/K es una **extensón normal** si F es el cuerpo de descomposición de un polinomio sobre K.*

Ejemplo 3.1.2 1. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es normal, ya que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de*

$$\left(x^2 - 2\right)\left(x^2 - 3\right)$$

2. *$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ NO es normal, ya que sólo una de las raíces de $\left(x^3 - 2\right) \in \mathbb{Q}(\sqrt[3]{2})$ las otras dos son imaginarias.*
3. *La extensión $\mathbb{Q}(\xi)/\mathbb{Q}$ donde $\xi = e^{2\pi i/n}$ es normal.*

Corolario 3.1.1 *Sea F/K una extensión finita normal. Si E es un subcuerpo intermedio, cualquier $K-$homomorfismo $\phi : E \to F$ se extiende a un $K-$automorfismo $F \to F$.*

Estudiamos ahora una propiedad fundamental de las extensiones normales.

Teorema 3.1.3 *Supongamos que E/K es una extensión finita. Entonces E/K es normal si y sólo si todo $p \in K[x]$ irreducible que tenga una raíz en E se descompone en $E[x]$.*

3.1.3. Extensiones separables

Supongamos que K es un cuerpo. Si $0 \neq f \in K[x]$ y $a \in K$, entonces se puede escribir $f(x) = (x-a)^m g(x)$, donde $g \in K[x]$, $g(a) \neq 0$ y $0 \leq m \leq \text{gr}(f)$. (En cualquier anillo K, utilizamos el convenio de que $r^0 = 1$ para $r \in K$). Si $m > 1$, se dice que a es raíz múltiple de f (con multiplicidad m). Si $m = 1$ digamos que a es raíz simple.

Veamos la relación entre raíces múltiples e irreducibilidad. Para ello es conveniente introducir la derivada de un polinomio f'

Teorema **3.1.4** *Supongamos que E es un cuerpo y que K es un subcuerpo de E. Sea $f \in K[x]$ con $f' \neq 0$.*

1. *Sea $a \in E$. Entonces a es raíz múltiple de f si y sólo si $f(a) = f'(a) = 0$.*
2. *Si $(f, f') = 1$, entonces f no tiene raíces múltiples en E.*
3. *Si f es irreducible en $K[x]$, entonces todas las raíces de f en E son distintas.*

Definición **3.1.5** *Sea K cuerpo y $f \in K[x]$ un **polinomio** irreducible. Se dice que f es **separable** si todas las raíces de f en el cuerpo de descomposición de f sobre K son simples.*

Ejemplo 3.1.3 *Veamos un ejemplo de un polinomio irreducible no separable. Sea $K = \mathbb{F}_2(x)$ y $f = y^2 - x \in K[y]$. Es inmediato que este polinomio es irreducible y si F es una extensión de K donde f tiene una raíz a entonces esta raíz es múltiple: $f = (y - a)^2$.*

Corolario **3.1.2** *Sea K un cuerpo y $f \in K[x]$ un polinomio irreducible. Entonces, f no es separable si y sólo si $f' = 0$. En particular se verifica:*

1. *Si $charK = 0$, todo polinomio irreducible de $K[x]$ es separable.*
2. *Si $charK = p > 0$, un polinomio irreducible no es separable si y sólo si es un polinomio en x^p.*

Definición **3.1.6** *Sea F/K una **extensión** algebraica. Diremos que F/K es **separable** si para cualquier $u \in F$, $\mathrm{Irr}(u, K)$ es un polinomio separable.*

Teorema **3.1.5** *(del elemento primitivo) Sea F/K una extensión finita de característica cero. Entonces, existe $u \in F$ tal que $F = K(u)$.*

3.1.4. El grupo de Galois

Si F es un cuerpo, un automorfismo de F es un homomorfismo biyectivo de cuerpos de F en F. Al conjunto de los automorfismos de F lo denotaremos Aut$F$. Si F/K es una extensión de cuerpos, un $K-$automorfismo de F es un automorfismo $\phi : F \to F$ tal que $\phi(u) = u$ para todo $u \in K$. Al conjunto de todos los $K-$automorfismos de F lo denotaremos $\mathcal{G}al(F/K)$. Evidentemente si $\phi, \psi \in \mathcal{G}al(F/K)$, $\phi \circ \psi \in \mathcal{G}al(F/K)$. Se comprueba de la forma rutinaria que $(\mathcal{G}al(F/K), \circ)$ es un grupo. Este grupo se llama grupo de Galois de la extensión F/K.

La Teoría de Galois estudia las extensiones de cuerpos a través de este grupo. En lo que sigue F/K denotará una extensión de cuerpos finita.

Definición **3.1.7** *Diremos que una **extensión** E/K es **de Galois** si E/K es normal y separable.*

La Teoría de Galois se puede desarrollar para cuerpos de todas las características. Por simplicidad, nosotros estudiamos el caso clásico de cuerpos de característica cero. Por lo tanto una extensión de Galois es una extensión normal. Sin embargo daremos algunos resultados con la máxima generalidad posible.

Teorema **3.1.6** *Supongamos que E/K es separable. Entonces*

$$|\mathcal{G}al(E/K)| \leq [E:K]$$

Además,

$$|\mathcal{G}al(E/K)| = [E:K]$$

si y sólo si E/K es normal (de Galois).

Ejemplo 3.1.4 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. *Si $\phi \in \mathcal{G}al(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, entonces $\phi(\sqrt[3]{2})$ es una raíz del polinomio x^3-2, y $\phi(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$, entonces necesariamente $\phi(\sqrt[3]{2}) = (\sqrt[3]{2})$, entonces $\phi = \mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}$ por lo que*

$$\mathcal{G}al(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}.$$

Teorema **3.1.7** *Sea p un primo. Entonces, salvo isomorfismo, para cualquier $n \in \mathbb{N}$ existe una sólo extensión de $\mathbb{F}_p$ de grado n (que denotamos por $\mathbb{F}_{p^n}$). $\mathbb{F}_{p^n}/\mathbb{F}_p$ es de Galois y su grupo de Galois es cíclico de orden n generado por el automorfismo de Frobenious.*

3.2. El Teorema Fundamental de la Teoria de Galois

3.2.1. Teoremas de Dedekind y Artin

Teorema **3.2.1** ***(Dedekind)*** *Sea K un cuerpo y sean $\tau_1, \ldots, \tau_n$ automorfismos distintos de K. Entonces $\tau_1, \ldots, \tau_n$ son $K-$linealmente independientes.*

Si E es un cuerpo y S es un subgrupo de $\mathrm{Aut}E$, definimos $F(S) = \{e \in E | \sigma(e) = e \text{ para todo } \sigma \in S\}$ es el subcuerpo de E fijado por todos los elementos de S. Notamos que si $S_1 \subseteq S_2 \subseteq \mathrm{Aut}E$, entonces $F(S_2) \subseteq F(S_1)$.

Teorema **3.2.2** ***(Artin)*** *Sea E un cuerpo y sea G un subgrupo finito de $\mathrm{Aut}E$. Si $F = F(G)$, entonces*

$$[E:F] = |G|.$$

Corolario **3.2.1** *Supongamos que E/K es una extensión Galois y sea $G = \mathcal{G}al(E/K)$. Sea $a \in E$. Si $\tau(a) = a$ para todo $\tau \in G$, entonces $a \in K$. En otras palabras, $\mathbb{F}(G) = K$.*

Corolario **3.2.2** *Sea E un cuerpo de característica 0 y $G \leq \mathrm{Aut}E$ un grupo finito. Pongamos $F = \mathbb{F}(G)$. Entonces E/F es una extensión de Galois y $\mathcal{G}al(E/F) = G$.*

3.2.2. Teorema Fundamental de Galois

Teorema **3.2.3** *Sea K un cuerpo de característica 0. Supongamos que E/K es una extensión y sea $K \subseteq L \subseteq E$ un subcuerpo tal que L/K es normal.*

1. *Entonces $\sigma(L) = L$ para todo $\sigma \in \mathcal{G}al(E/K)$.*

2. *Supongamos que E/K es normal. Entonces la aplicación*

$$\rho : \mathcal{G}al(E/K) \to \mathcal{G}al(L/K)$$

que manda ϕ a $\rho(\phi) = \phi_L$ está bien definida, su núcleo es $\mathcal{G}al(E/L)$ y es sobreyectiva. En particular, $\mathcal{G}al(E/L) \trianglelefteq \mathcal{G}al(E/K)$ y

$$\mathcal{G}al(E/K)/\mathcal{G}al(E/L) \simeq \mathcal{G}al(L/K)$$

Teorema **3.2.4** *Sea K un cuerpo de característica 0. Supongamos que E/K es una extensión de Galois y sea $K \subseteq L \subseteq E$ un subcuerpo. Entonces L/K es normal si y sólo si $\sigma(L) = L$ para todo $\sigma \in \mathcal{G}al(E/K)$.*

Teorema **3.2.5** *(Fundamental de la Teoría de Galois). Supongamos que E/K es de Galois y sea $G = \mathcal{G}al(E/K)$. Sea $\mathcal{S}$ el conjunto de subgrupos de G y sea $\mathcal{K}$ el conjunto de subcuerpos intermedios $K \subseteq L \subseteq E$.*

1. *Las aplicaciones $f : \mathcal{S} \to \mathcal{K}$ y $g : \mathcal{K} \to \mathcal{S}$ dadas por $f(H) = \mathbb{F}(H)$ y $g(L) = \mathcal{G}al(E/L)$ son biyecciones, inversa la una de la otra.*
2. *Si $K \subseteq L \subseteq E$, entonces L/K es normal si y sólo si $\mathcal{G}al(E/L) \trianglelefteq \mathcal{G}al(E/K)$. En este caso*

$$\mathcal{G}al(E/K)/\mathcal{G}al(E/L) \simeq \mathcal{G}al(L/K).$$

Una consecuencia no trivial del teorema anterior es que si E/K es de Galois, entonces sólo hay un número finito de cuerpos intermedios entre E y K.

Ejemplo 3.2.1 *Estudiar el polinomio $x^3 - 2$.*

En primer lugar vemos que las raíces de dicho polinomio son

$$R_p = \left\{ \sqrt[3]{2}, \sqrt[3]{2}\frac{1}{2}\left(-1+\sqrt{3i}\right), \sqrt[3]{2}\frac{1}{2}\left(-1-\sqrt{3i}\right) \right\},$$

y que pasamos a reescribir como

$$R_p = \left\{ \alpha, \alpha\omega, \alpha\omega^2 \right\},$$

con

$$\alpha = \sqrt[3]{2}, \qquad \omega = \frac{1}{2}\left(-1+\sqrt{3i}\right) \qquad \Longrightarrow \qquad \bar{\omega} = \frac{1}{2}\left(-1-\sqrt{3i}\right) = \omega^2 = -1-\omega.$$

Las correspondietes bases son

$$\begin{aligned} B_\alpha &= \left\{1, \alpha, \alpha^2\right\}, \qquad p_\alpha = x^3 - 2, \\ B_\omega &= \{1, \omega\}, \qquad p_\omega = x^2 + x + 1, \\ B_{(\alpha,\omega)} &= \left\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\right\}, \end{aligned}$$

de esta forma vemos que el campo de descomposición de dicho polinomio es

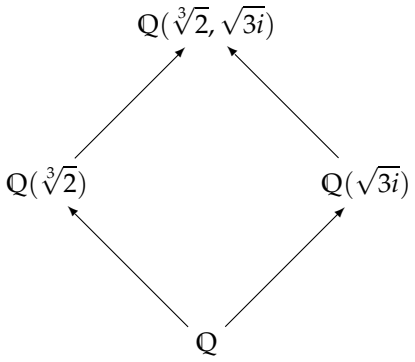
$$E = \mathbb{Q}\left(\alpha, \sqrt{3i}\right),$$

con

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6,$$

como ya sabemos, al ser el grado del polinomio 3, entonces el grado del cuerpo de descomposición será como mucho 3!.

Tenemos por lo tanto la siguiente descomposición:



El correspondiente grupo de Galois tendrá por lo tanto orden 6

$$|\mathcal{G}al\,(E/\mathbb{Q})| = 6,$$

existiendo dos automorfismos $\sigma, \tau \in Aut(\mathcal{G})$ que lleva las respectivas raíces de los polinomios mínimos p_α y p_ω, donde

$$R_{p_\alpha} = \left\{\alpha, \alpha\omega, \alpha\omega^2\right\}, \qquad R_{p_\omega} = \left\{\omega, \omega^2\right\},$$

así que

$$\mathcal{G}al\,(E/\mathbb{Q}) = \left\{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\right\},$$

(comparar con $B_{(\alpha,\omega)} = \left\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\right\}$. Tenemos la siguiente tabla

	α	ω
id	α	ω
σ	$\alpha\omega$	ω
σ^2	$\alpha\omega^2$	ω
τ	α	ω^2
$\sigma\tau$	$\alpha\omega$	ω^2
$\sigma^2\tau$	$\alpha\omega^2$	ω^2

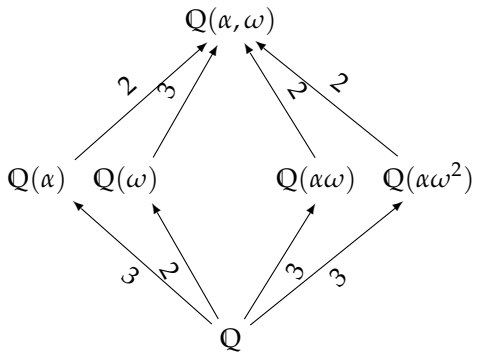
viendo así que el grupo NO es abeliano ya que

$$\sigma\tau\,(\alpha) = \sigma\,(\tau\,(\alpha)) = \sigma\,(\alpha) = \alpha\omega,$$
$$\tau\sigma\,(\alpha) = \tau\,(\sigma\,(\alpha)) = \tau\,(\alpha\omega) = \alpha\omega^2,$$

por lo que sabemos que al tener orden 6 y no ser abeliano, entonces

$$\mathcal{G}al\,(E/\mathbb{Q}) \approx S_3$$

Encontramos la siguiente descomposición:



Los subgrupos correspondientes son:

Subgrupo		*campo*
$G_1 = \{\mathrm{id}, \tau\}$	$\longrightarrow$	$E_1 = \mathbb{Q}(\alpha)$
$G_2 = \{\mathrm{id}, \sigma, \sigma^2\}$	$\longrightarrow$	$E_2 = \mathbb{Q}(\omega)$
$G_3 = \{\mathrm{id}, \sigma\tau\}$	$\longrightarrow$	$E_2 = \mathbb{Q}(\alpha\omega)$
$G_4 = \{\mathrm{id}, \sigma^2\tau\}$	$\longrightarrow$	$E_2 = \mathbb{Q}(\alpha\omega^2)$

En la siguiente tabla se muestra la acción de cada automorfisomo sobre las raíces

	1	α	α^2	ω	$\alpha\omega$	$\alpha^2\omega$
σ	1	$\alpha\omega$	$\alpha^2\omega^2$	ω	$\alpha\omega^2$	α^2
$\sigma\tau$	1	$\alpha\omega$	$\alpha^2\omega^2$	ω^2	α	$\alpha^2\omega$

donde por ejemplo

$$\sigma\left(\alpha^2\omega\right) = \alpha^2\omega^2\omega = \alpha^2, \qquad \omega^3 = 1,$$
$$\sigma\tau(\alpha\omega) = \sigma(\tau(\alpha\omega)) = \sigma\left(\alpha\omega^2\right) = \alpha\omega^3 = \alpha,$$
$$\sigma\tau\left(\alpha^2\omega\right) = \sigma\left(\alpha^2\omega^2\right) = \alpha^2\omega^4 = \alpha^2\omega \qquad etc...$$

Por lo tanto si tomamos un elemento x, que escribimos como

$$x = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\omega + \lambda_4\alpha\omega + \lambda_5\alpha^2\omega,$$

queremos ver la acción

$$\sigma(x) = x,$$

así que

$$\sigma(x) = \lambda_0 + \lambda_1\alpha\omega + \lambda_2\alpha^2\omega^2 + \lambda_3\omega + \lambda_4\alpha\omega^2 + \lambda_5\alpha^2 = x,$$

sii

$$\lambda_1 = \lambda_2 = \lambda_4 = \lambda_5 = 0,$$

por lo que

$$\sigma(x) = \lambda_0 + \lambda_3\omega.$$

Se observa que G_2 es el único subgrupo normal, lo que corresponde al hecho de que E_2 sea normal también.

De igual forma podemos ver que

$$\tau(x) = x$$

sii

$$\tau(x) = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\omega^2 + \lambda_4\alpha\omega^2 + \lambda_5\alpha^2\omega^2$$

por lo que $\lambda_3 = \lambda_4 = \lambda_5 = 0$, así que G_1 genera E_1. Los otros dos casos se deducen fácilmente.

3.3. Ejercicios.

En esta sección veremos unos cuantos ejercicios. La mayor parte de ellos son muy mecánicos (por eso son ejercicios y no problemas), están pensados para hacer mano, de ahí que tengan tanto detalle (supérfluo) en la mayoría de los casos.

3.3.1. Cuerpo de descomposición

Campos de descomposición (SF)

Ejercicio 3.3.1 *Sea K un cuerpo de característica $p > 0$. Sea $a \in K$ y sea $f(x) \in K[x]$ tal que $R_p = (\alpha)$ i.e. una de las raíces de f es α. Encontrar el cuerpo de descomposición de f sobre $K[x]$, $f(x) = x^p - x - a$.*

Solución. Sea $E = K[x]/f$ y sea α una raíz. Entonces

$$a = \alpha^p - \alpha,$$

al ser K cuerpo de característica p, entonces

$$f(x) = (x-\alpha)^p - (x-\alpha).$$

Si $\beta \in E$ es otra raíz de f entonces $b = \beta - \alpha$, sería raíz de $x^p - x$ i.e. $b^p = b$, $b \in \mathbb{Z}_p$, entonces

$$E = K[\alpha],$$

donde $R_p = \{\alpha + b : b \in \mathbb{Z}_p\}$. ■

Ejercicio 3.3.2 *Mostrar que $\mathbb{Q}\left(\sqrt{3}, i\right)$ es un cuerpo de descomposición para*

$$f(x) = \left(x^3+1\right)\left(x^2-3\right) = x^5 - 3x^3 + x^2 - 3.$$

Solución. Como siempre empezamos calculando las raices del polinomio f, siendo éstas

$$R_f = \left\{\pm\sqrt{3}, -1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$$

viendo que efectivamente dichas raices pertenecen al campo $\mathbb{Q}\left(\sqrt{3}, i\right)$. Por otro lado, si f se descompone en $K \subseteq \mathbb{Q}\left(\sqrt{3}, i\right)$ entonces todas las raices de f deben estar en K. Por lo tanto, como $\mathbb{Q} \subseteq K$, por definición de campo de descomposición (**splitting field SF**) y $\frac{1}{2} \pm i\frac{\sqrt{3}}{2} \in K$, entonces tenemos que $i\sqrt{3} \in K$. Ahora, $\sqrt{3} \in K$, también nos da que $i \in K$ y que por lo tanto $\mathbb{Q}\left(\sqrt{3}, i\right) \subseteq K$, concluyendo por lo tanto que $\mathbb{Q}\left(\sqrt{3}, i\right) = K$, y que se trata del SF de f. ■

Ejercicio 3.3.3 *Calcular el SF K de $f = x^4 - 2 \in \mathbb{Q}[x]$. Calcular $[K : \mathbb{Q}]$.*

Solución. Vemos que una raíz de f es $\left(\sqrt[4]{2}\right)$ y que f es irreducible en $\mathbb{Q}$. Sin embargo $\mathbb{Q}\left(\sqrt[4]{2}\right)$ no es un SF para f. Veámoslo.

$$f(x) = x^4 - 2 = \left(x^2 + \sqrt{2}\right)\left(x^2 - \sqrt{2}\right),$$

si f fuese descomponible en

$$\mathbb{Q}\left(\sqrt[4]{2}\right) = \left\{a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{2^3} : a, b, c, d \in \mathbb{Q}\right\} \subseteq \mathbb{R},$$

entonces $\left(x^2 + \sqrt{2}\right)$ debería tener una raíz real, cosa que no sucede.

Sea $K = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$ el SF de f, calculmos $[K : \mathbb{Q}] = 8$. Como en el ejercicio anterior calculamos las raices de f viendo que éstas son:

$$\pm\sqrt[4]{2}, \quad \pm i\sqrt[4]{2},$$

viéndose que todas ellas están en K, y como en el ejercicio anterior podríamos suponer que existe otro campo pero llegaríamos a la conclusión de que ambos campos son iguales (no es más comprobar el resultado del teorema de unicidad del SF).

Con respecto al cálculo de $[K : \mathbb{Q}] = 8$, vemos que

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8,$$

donde

$$\begin{aligned}\left[K : \mathbb{Q}\left(\sqrt[4]{2}\right)\right] &= 2, \qquad x^2 + 1,\\ \left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] &= 4, \qquad x^4 - 2,\end{aligned}$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.4 *Calcular el SF K de $f = x^6 - 8 \in \mathbb{Q}[x]$. Calcular $[K : \mathbb{Q}]$.*

Solución. Es una réplica del anterior. Vemos que las raíces de f son;

$$\pm\sqrt{2}, \qquad \pm\frac{\sqrt{2}}{2}\left(1 \pm i\sqrt{3}\right),$$

donde $\sqrt[6]{8} = \sqrt{2}$, o escrito de otro modo

$$\left(\sqrt{2}, \xi\right), \qquad \xi = e^{2\pi i/6} = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2} + i\frac{\sqrt{3}}{2},$$

por lo tanto

$$K = \mathbb{Q}\left(\sqrt{2}, i\sqrt{3}\right),$$

sólo falta calcular

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 4$$

donde

$$\begin{aligned}\left[K : \mathbb{Q}\left(\sqrt{2}\right)\right] &= 2,\\ \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] &= 2, \qquad x^2 - 2,\end{aligned}$$

tal y como queríamos hacer ver. Observar que un polinomio irreducible es: $\left(x - \sqrt{2}\right)p^5$ donde $p^5 = x^5 + x^4 + x^3 + x^2 + x + 1$. ■

Ejercicio 3.3.5 *Calcular el SF K de $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$. Calcular $[K : \mathbb{Q}]$.*

Solución. Las raíces de f son

$$\pm\sqrt{\frac{-5 \pm \sqrt{5}}{2}} \in \mathbb{C},$$

por lo tanto definimos

$$\alpha = \sqrt{\frac{-5 + \sqrt{5}}{2}}, \qquad \beta = \sqrt{\frac{-5 - \sqrt{5}}{2}}$$

de esta forma

$$K = \mathbb{Q}(\alpha, \beta)$$

pero vemos que en realidad $\beta \in \mathbb{Q}(\alpha)$ por lo que $K = \mathbb{Q}(\alpha)$. Con respecto al grado de la extensión vemos sin problemas que

$$[K : \mathbb{Q}] = 4.$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.6 *Calcular el SF K de*

$$f = x^4 - 2x^3 - x^2 - 2x - 2 \in \mathbb{Q}[x].$$

Calcular $[K : \mathbb{Q}]$.

Lo mismo para el polinomio

$$g = x^5 - 3x^3 + x^2 - 3.$$

Solución. Las raíces de f son

$$\left(\pm i, 1 \pm \sqrt{3}\right) \qquad \Longrightarrow \qquad K = \mathbb{Q}\left(\sqrt{3}, i\right) \qquad \Longrightarrow \qquad [K : \mathbb{Q}] = 4.$$

Para el polinomio g encontramos que

$$\left(-1, \pm\sqrt{3}, \frac{1}{2}\left(1 \pm i\sqrt{3}\right)\right)$$

y por lo tanto su SF es

$$K = \mathbb{Q}\left(\sqrt{3}, i\right) \qquad \Longrightarrow \qquad [K : \mathbb{Q}] = 4$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.7 *Mostrar que los polinomios $f = x^2 - 3$ y $g = x^2 - 2x - 2$ son ambos irreducibles y tienen el mismo SF S.*

Solución. Las raíces de f son

$$R_f = \left(\pm\sqrt{3}\right) \qquad \Longrightarrow \qquad S = \mathbb{Q}\left(\sqrt{3}\right) \qquad \Longrightarrow \qquad [S : \mathbb{Q}] = 2.$$

Para el polinomio g encontramos que

$$R_g = \left(1 \pm \sqrt{3},\right)$$

y por lo tanto su SF es

$$K = \mathbb{Q}\left(1 \pm \sqrt{3}\right) \qquad \Longrightarrow \qquad [K : \mathbb{Q}] = 2$$

pero podemos observar que en realidad

$$K \subset S = \mathbb{Q}\left(\sqrt{3}\right) = \left\{a + b\sqrt{3}; a, b \in \mathbb{Q}\right\}$$

y por lo tanto $K = S$, tal y como queríamos hacer ver. ■

Ejercicio 3.3.8 *Sea K un campo y sean $a, b \in K$. Probar que $x + a + b$ divide a $x^3 - 3abx + a^3 + b^3$ en $K[x]$ y determinar $q(x) \in K[x]$ tal que*

$$x^3 - 3abx + a^3 + b^3 = q(x)(x + a + b).$$

Encontrar el SF de $x^6 - 6x^3 + 8$ sobre $\mathbb{Q}$. Calcular $[S : \mathbb{Q}]$ y mostrar que $\xi = \left(\sqrt[3]{4} + \sqrt[3]{2}\right) \in S$, encontrando el polinomio mínimo de este elemento. ¿Es verdad que $\mathbb{Q}(\xi)$ sea un SF para $p = x^6 - 6x^3 + 8$?.

Solución. Aplicando Rufini directamente, encontramos que

$$x^3 - 3abx + a^3 + b^3 = q(x)(x + a + b),$$

donde

$$q(x) = x^2 + (a + b)x + (a + b)^2 - 3ab.$$

Con respecto al segundo apartado vemos que

$$x^6 - 6x^3 + 8 = \left(x^3 - 2\right)\left(x^3 - 4\right)$$

por lo que podríamos pensar que el SF de dicho polinomio es:

$$\mathbb{Q}\left(\sqrt[3]{4}, \sqrt[3]{2}\right)$$

pero no es así ya que $\left(x^3 - 2\right)$ tiene raíces complejas, por lo que en realidad

$$S = \mathbb{Q}\left(\sqrt[3]{4}, \sqrt[3]{2}, \sqrt{3i}\right)$$

además se observa trivialmente que

$$\sqrt[3]{4} = \sqrt[3]{2^2}$$

por lo que el SF resulta ser:

$$S = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3i}\right)$$

donde

$$[S : \mathbb{Q}] = \left[S : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 2 \cdot 3 = 6.$$

Vemos igualmente que $\xi = \left(\sqrt[3]{4} + \sqrt[3]{2}\right) \in S$, ya que tanto $\sqrt[3]{4}$, como $\sqrt[3]{2}$ pertenecen ambos a S.

Ahora tomamos

$$\alpha = -\sqrt[3]{4}, \qquad \beta = -\sqrt[3]{2}$$

por lo que (por la primera parte del problema)

$$\left(x - \left(\sqrt[3]{4} + \sqrt[3]{2}\right)\right)$$

divide a

$$x^3 - 6x - 6.$$

Al pertenecer $\xi = \left(\sqrt[3]{4} + \sqrt[3]{2}\right) \in S$, que tiene grado 3 sobre $\mathbb{Q}$ y como $\xi \notin \mathbb{Q}$ entonces el poli mínimo debe tener grdo 3 (y por la primera parte del ejercicio) tenemos que es $x^3 - 6x - 6$. Por lo tanto

$$\xi \in S, \qquad \mathbb{Q}(\xi) \subset S$$

pero $\mathbb{Q}(\xi) \subsetneq S$, por los grados. ■

Ejercicio 3.3.9 *Encontrar factores cuadráticos para el poli*

$$f(x) = x^4 + 2x^3 - 8x^2 - 6x - 1$$

y demostrar que $S = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ *es su SF sobre* $\mathbb{Q}$.

Demostrar que $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$, *mostrar que* $[S : \mathbb{Q}] = 4$, *calcular un base. Mostrar igualmente que* $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} - \sqrt{3}\right)$ *y calcular el poli mínimo de* $\mathbb{Q}\left(\sqrt{2} - \sqrt{3}\right)$ *sobre* $\mathbb{Q}\left(\sqrt{3}\right)$.

Solución. Vemos que las raíces de f son

$$x^4 + 2x^3 - 8x^2 - 6x - 1 = \left(x^2 + 4x + 1\right)\left(x^2 - 2x - 1\right)$$

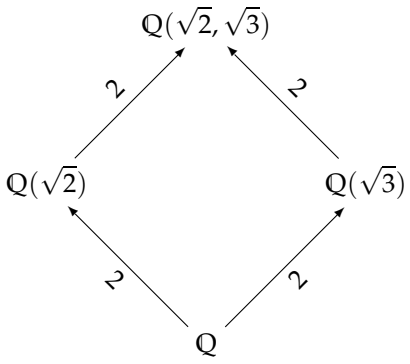
por lo que las raíces son:

$$\left(2 \pm \sqrt{3}\right) \quad \text{y} \quad \left(-1 \pm \sqrt{2}\right)$$

por lo que su campo de descomposición S será:

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$$

Vemos el siguiente diagrama:



donde por la tower law tenemos que

$$[S : \mathbb{Q}] = \left[S : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4.$$

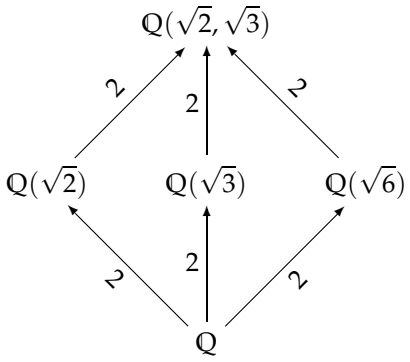
donde una base es:

$$B_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}} = \left\{1, \sqrt{2}, \sqrt{3}, \sqrt{2 \cdot 3} = \sqrt{6}\right\}$$

y

$$B_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = \left\{1, \sqrt{2}\right\}, \qquad x^2 - 2, \qquad B_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}} = \left\{1, \sqrt{3}\right\}, \qquad x^2 - 3.$$

A la vista de estos resultados podemos rehacer el gráfico de la siguiente forma



Igualmente vemos que si $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2}; a, b \in \mathbb{Q}\right\}$, entonces

$$\sqrt{3} = a + b\sqrt{2}$$

y por lo tanto

$$3 = a^2 + 2ab\sqrt{2} + 2b^2$$

y discutimos en función de los distintos valores que puedan tomar $a, b \in \mathbb{Q}$.

1. Si $a, b \neq 0$, entonces $\sqrt{2} \in \mathbb{Q}$, ¡!.
2. Si $a = 0$, entonces $\sqrt{3} = b\sqrt{2}$ y por lo tanto $\sqrt{6} = 2b \in \mathbb{Q}$, ¡!.
3. Si $b = 0$, entonces $\sqrt{3} = a \in \mathbb{Q}$, ¡!.

Concluimos por lo tanto que $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$.

Nos queda por mostrar que $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} - \sqrt{3}\right)$ y calcular el poli mínimo de $\mathbb{Q}\left(\sqrt{2} - \sqrt{3}\right)$ sobre $\mathbb{Q}\left(\sqrt{3}\right)$.

Para ello pensemos de la siguiente forma: sea $\xi = \sqrt{2} - \sqrt{3}$, su poli mínimo debe tener o grado 4 o grado 2. Si fuese de grado 2 entonces para $a, b \in \mathbb{Q}$ tendríamos que

$$\left(\sqrt{2} - \sqrt{3}\right)^2 + a\left(\sqrt{2} - \sqrt{3}\right) + b = 0$$

i.e.

$$b + 5 - 2\sqrt{2}\sqrt{3} + \left(\sqrt{2} - \sqrt{3}\right)a = 0$$

pero ¡! ya que una base es $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ por lo que el poli mínimo debe tener grado 4. y $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} - \sqrt{3}\right)$. El poli mínimo de $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$ es $x^4 - 10x^2 + 1$ (ya calculado en otro ejercicio) mientras que El poli mínimo de $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}\left(\sqrt{3}\right)$ es $x^2 - 2\sqrt{3}x + 1 = \left(x - \sqrt{3}\right)^2 - 2$.

Recordamos el cálculo del otro poli mini.

$$\left(\left(x-\sqrt{3}\right)^2-2\right)\left(\left(x+\sqrt{3}\right)^2-2\right)=x^4-10x^2+1, \qquad ó$$
$$\left(\left(x-\sqrt{2}\right)^2-3\right)\left(\left(x+\sqrt{2}\right)^2-3\right)=x^4-10x^2+1,$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.10 *Encontrar factores irreducubles en* $\mathbb{Q}[x]$ *para*

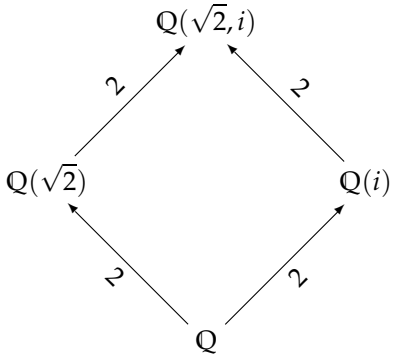
$$f(x)=x^4-x^2-2.$$

Mostrar que $S=\mathbb{Q}\left(\sqrt{2},i\right)$ *es un SF para* f, $[S:\mathbb{Q}]=4$ *y calcular una base. Describir las relaciones entre los campos intermedios, sus bses y polis mínimos.*

Solución. Vemos que las raíces de f son

$$x^4-x^2-2=\left(x^2-2\right)\left(x^2+1\right)$$

por lo tanto $S=\mathbb{Q}\left(\sqrt{2},i\right)$. La imagen es la siguiente:



donde

$$[S:\mathbb{Q}]=\left[S:\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2\cdot 2=4,$$

ya que

$$\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2, \qquad \left(x^2-2\right), \qquad B=\left\{1,\sqrt{2}\right\},$$
$$\left[\mathbb{Q}\left(i\right):\mathbb{Q}\right]=2, \qquad \left(x^2+1\right), \qquad B=\left\{1,i\right\},$$

entonces

$$[S:\mathbb{Q}]=4, \qquad x^4-2x^2+9, \qquad B=\left\{1,\sqrt{2},i,\sqrt{2i}\right\},$$

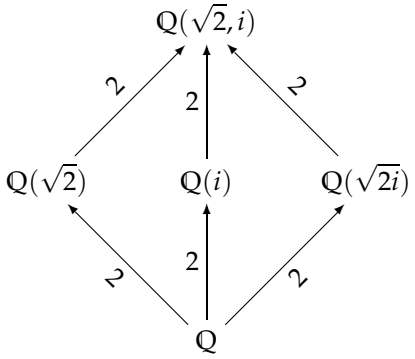
donde el poli mínimo lo hemos calculado de la siguiente manera:

$$x^4+ax^3+bx^2+cx+d=0,$$
$$A+B\sqrt{2}+\mathrm{Ci}+D\sqrt{2i}=0.$$

o, como siempre, de una formamás directa calculando el producto

$$\left((x-i)^2-2\right)\left((x+i)^2-2\right)=x^4-2x^2+9.$$

Así que tenemos este nuevo panorama



Igualmente vemos que

$$\mathbb{Q}\left(\sqrt{2}+i\right)\subseteq\mathbb{Q}\left(\sqrt{2},i\right)$$

por lo que, nos preguntamos sobre el grado de la extensión

$$\left[\mathbb{Q}\left(\sqrt{2}+i\right):\mathbb{Q}\right]=\begin{cases}4\\2\end{cases}\ .??$$

Vemos que

$$\left(i+\sqrt{2}\right)^2=1+2i\sqrt{2},$$

y si el poli mínimo de $\left(i+\sqrt{2}\right)$ fuese de grado 2, entonces existirian $a,b\in\mathbb{Q}$ tales que

$$0=\left(i+\sqrt{2}\right)^2+a\left(i+\sqrt{2}\right)+b=ia+b+\sqrt{2}a+2i\sqrt{2}+1$$

llegando así a una contradicción pues sabemos de antemano que la base está generada por los 4 elementos $\left\{1,\sqrt{2},i,\sqrt{2i}\right\}$. Por lo tanto el poli debe tener grado 4. De esta forma vemos que si $\xi=\left(i+\sqrt{2}\right)$ entonces

$$\left[\mathbb{Q}\left(\xi\right):\mathbb{Q}\right]=4,$$

y que

$$\mathbb{Q}\left(\xi\right)=\mathbb{Q}\left(\sqrt{2},i\right),$$

ya que claramente

$$\left(i+\sqrt{2}\right)^2=1+2i\sqrt{2},\qquad\left(i+\sqrt{2}\right)^4=\left(1+2i\sqrt{2}\right)^2=-7+4i\sqrt{2},$$

y por lo tanto

$$\left(i+\sqrt{2}\right)^4-2\left(i+\sqrt{2}\right)^2+9=0,\qquad x^4-2x^2+9.$$

Por último calculamos los polinomios mínimos de los campos intermedios i.e.

$$m_{\left(i+\sqrt{2}\right)}^{\mathbb{Q}(i)}=x^2-2ix-3$$

ya que $\left(i+\sqrt{2}\right)^2 = 1+2i\sqrt{2} = 1+2i\left(i+\sqrt{2}\right)+2$.

De igual forma vemos que

$$m_{\left(i+\sqrt{2}\right)}^{\mathbb{Q}\left(\sqrt{2}\right)} = x^2 - 2\sqrt{2}x + 3$$

ya que $\left(i+\sqrt{2}\right)^2 = 1+2i\sqrt{2} = 1+2\sqrt{2}\left(i+\sqrt{2}\right)-4$.

Por último vemos que

$$m_{\left(i+\sqrt{2}\right)}^{\mathbb{Q}\left(\sqrt{2i}\right)} = x^2 - 2i\sqrt{2} - 1$$

ya que $\left(i+\sqrt{2}\right)^2 = 1+2i\sqrt{2}$. ■

Ejercicio 3.3.11 *El polinomio $x^5 - 12x + 2$ es irreducible sobre $\mathbb{Q}(\sqrt{7})$.*

Solución. VERDADERO Sea M el cuerpo de descomposición de $x^5 - 12x + 2$ sobre $\mathbb{Q}$ y sea $\alpha \in M$ una de sus raíces. Para demostrar la afirmación es suficiente con probar que el grado del polinomio míinimo de sobre $\mathbb{Q}(\sqrt{7})$ es 5, o en otras palabras, que

$$[\mathbb{Q}(\alpha, \sqrt{7}) : \mathbb{Q}(\sqrt{7})] = 5$$

En primer lugar observamos que como

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$$

ya que $x^5 - 12x + 2$ es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein (con $p = 2$). Como consecuencia,

$$[\mathbb{Q}(\alpha, \sqrt{7}) : \mathbb{Q}(\sqrt{7})] \leq 5$$

Por otro lado,

$$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$$

ya que $x^2 - 7$ es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein (con $p = 7$). Como 2 y 5 son coprimos,

$$[\mathbb{Q}(\alpha, \sqrt{7}) : \mathbb{Q}] = 10$$

y por tanto necesariamente

$$[\mathbb{Q}(\alpha, \sqrt{7}) : \mathbb{Q}(\sqrt{7})] = 5.$$

tal y como queríamos hacer ver. ■

3.3.2. Extensiones Normales

Extensiones normales

Ejercicio 3.3.12 *Estudiar si las siguientes extensiones son normales.*

1. $K_1 = \mathbb{Q}\left(\sqrt[3]{-2}, \sqrt{-2}\right)/\mathbb{Q}$,
2. $K_2 = \mathbb{Q}\left(\sqrt[3]{-3}, \sqrt{-3}\right)/\mathbb{Q}$.

Solución. Sea $p = x^3 + 2$, irreducible por Eisenstein, definimos $\alpha = \sqrt[3]{-2}$, entonces vemos que $\alpha \in \mathbb{Q}\left(\alpha, \sqrt{-2}\right)$, sin embargo vemos que $\sqrt[3]{-2}\omega, \sqrt[3]{-2}\bar{\omega} \notin K_1$, por lo que esta extensión no puede ser normal.

Sea $p = x^3 + 3$, irreducible por Eisenstein, definimos $\alpha = \sqrt[3]{-3}$, entonces vemos que $\alpha \in \mathbb{Q}\left(\alpha, \sqrt{-3}\right)$, además vemos que: $\sqrt[3]{-3}\omega, \sqrt[3]{-3}\bar{\omega} \in K_2$, por lo que esta extensión es normal. Obsérvese que

$$\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{1}{2}\left(-1 + i\sqrt{3}\right).$$

Tal y como queríamos hacer ver. ■

Ejercicio 3.3.13 *Estudiar si dado $f(x) = x^6 + x^3 + 1$, la extensión $K = \mathbb{Q}(\xi)/\mathbb{Q}$, es normal. $\xi = e^{2\pi i/9}$.*

Solución. Vemos que ξ es raíz de f, y que f es el polinomio mínimo de ξ ya que es irreducuble,

$$[K : \mathbb{Q}] = 6$$

al grado del polinomio mínimo. La extensión es normal ya que si tomamos $y = x^3$, entonces $y^2 + y + 1$, viendo de esta forma que y es raíz cúbica de la unidad y por lo tanto x es una ráiz novena de la unidad, entonces todas las raíces de f son de la forma $e^{2\pi ik/9}$. ■

Ejercicio 3.3.14 *Dado $f(x) = x^4 + x^2 - 6$, estudiar su campo de descompsición etc...*

Solución. Las raícesde f, son, vemos que

$$x^4 + x^2 - 6 = y^2 + y - 6$$

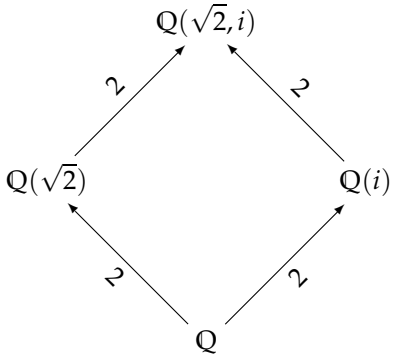
y por lo tanto son

$$\left(\pm\sqrt{2}, \pm\sqrt{3i}\right)$$

por lo que su campo de descomposición es:

$$S = \mathbb{Q}\left(\sqrt{2}, \sqrt{3i}\right)$$

viéndose que



y por lo tanto

$$[S:\mathbb{Q}] = \left[S:\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2\cdot 2 = 4,$$

se trata de una extensión finita, normal y separable (es extensión de un cuerpo de característica cero).

Obsérvese que

$$\mathbb{Q}\left(\sqrt{3i}\right) \notin \mathbb{Q}\left(\sqrt{2}\right)$$

de lo contrario tendríamos la siguiente situación:

$$a+b\sqrt{2} = \sqrt{3i} \qquad \Longrightarrow \qquad -3 = a^2+2b^2+2\sqrt{2}ab \qquad \Longrightarrow \begin{cases} a^2+2b^2 = -3 \\ 2ab = 0 \end{cases} \quad ¡!$$

Para ver que realmente se trata de una extensión normal simplemente observar que se trata de un cuerpo de descomposición y que por lo tanto contiene todas las raíces

Lo único que podemos avanzar por aharo es que

$$\mathcal{G}al\,(S/\mathbb{Q}) \simeq G, \qquad |G| = 4, \qquad G \simeq \mathbb{Z}_2\times\mathbb{Z}_2.$$

tal y queríamos hacer ver. ■

Ejercicio 3.3.15 *Sean*

$$L_1 = \mathbb{Q}\left(\sqrt{3}\right) \qquad y \qquad L_2 = \mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)$$

estudiar si las siguientes extensiones son normales.

Solución. Vemos que $(L_1/\mathbb{Q})$ y (L_2/L_1) son normales ya que

$$[L_1:\mathbb{Q}] = [L_2:L_1] = 2$$

vemos que el polinomio mínimo de $\alpha = \sqrt{1+\sqrt{3}}$ es:

$$f(x) = x^4-2x^2-2 \in \mathbb{Q}[x], \qquad R_f = \{\pm\alpha, \pm\beta\}$$

donde $\beta = \sqrt{1-\sqrt{3}}$, ya que es irreducible por el criterio de E. Puesto que $\beta \in \mathbb{C}$, y $L_2 \subset \mathbb{R}$ entonces $\beta \notin L_2$ por lo tanto $(L_2/\mathbb{Q})$ no puede ser normal

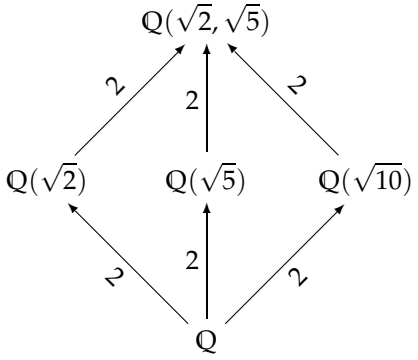
Si $\sigma \in \mathcal{G}al\,(L_2/\mathbb{Q})$, entonces $\sigma(\alpha) \in \{\pm\alpha\}$ por lo tanto $\mathcal{G}al\,(L_2/\mathbb{Q}) \simeq \mathbb{Z}_2$. ■

3.3.3. Grupo de Galois

Grupo de Galois

Ejercicio 3.3.16 *Hallar el grupo de Galois de* $\mathbb{Q}\left(\sqrt{2},\sqrt{5}\right)/\mathbb{Q}$.

Solución. Vemos que



son los cuerpos intermedios y que

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt{5}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2},\sqrt{5}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2\cdot 2=4,$$

los cálculos con las otras extensiones es semejante.

Tenemos que

$$B_{\sqrt{2}}=\{1,\alpha\},\qquad B_{\sqrt{5}}=\{1,\beta\},\qquad B_{SF}=\{1,\alpha,\beta,\alpha\beta\}=\left\{1,\sqrt{2},\sqrt{5},\sqrt{10}\right\}.$$

Tenemos 4 posibilidades: Sea $r\in\mathbb{Q}\left(\sqrt{2},\sqrt{5}\right)$, entonces $r=x+y\sqrt{2};\,x,y\in\mathbb{Q}\left(\sqrt{5}\right)$. Me invento los automorfismos σ_1,σ_2 tales que

$$\sigma_1\left(x+y\sqrt{2}\right)=x-y\sqrt{2},$$

análogamente definimos $r=x+y\sqrt{5};\,x,y\in\mathbb{Q}\left(\sqrt{2}\right)$

$$\sigma_2\left(x+y\sqrt{5}\right)=x-y\sqrt{5}$$

por lo tanto

	$\sqrt{2}$	$\sqrt{5}$
id	$\sqrt{2}$	$\sqrt{5}$
σ_1	$-\sqrt{2}$	$\sqrt{5}$
σ_2	$\sqrt{2}$	$-\sqrt{5}$
$\sigma_1\cdot\sigma_2$	$-\sqrt{2}$	$-\sqrt{5}$

de esta forma vemos que:

$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{5}\right)/\mathbb{Q}\right)\simeq G=\{id,\sigma_1,\sigma_2,\sigma_1\cdot\sigma_2\},$$

con

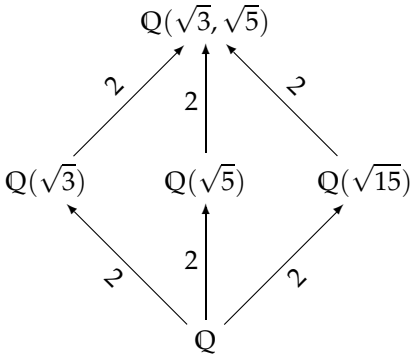
$$|G|=4,\qquad G\simeq\mathbb{Z}_2\times\mathbb{Z}_2,$$

tal y como queríamos hacer ver.

Otro ejemplo absolutamente idéntico es el siguiente. Dado $p(x)=x^4-8x^2+15$,vemos que $R_p=\left\{\pm\sqrt{3},\pm\sqrt{5}\right\}$, entonces

$$p(x)=x^4-8x^2+15=\left(x^2-3\right)\left(x^2-5\right),$$

y por lo tanto estamos en la situación del ejercicio expuesto, con las misma descomposiciones



y grupo de Galois $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Ejercicio 3.3.17 *Hallar* $\mathcal{G}al\left(x^4-9\right)$.

Solución. Las raíces del poli son $\left(\pm\sqrt{3},\pm\sqrt{3i}\right)$, y de forma automática vemos que

$$S = \mathbb{Q}\left(\sqrt{3},\sqrt{3i}\right)$$

por lo que

$$\left[\mathbb{Q}\left(\sqrt{3},\sqrt{3i}\right):\mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{3},\sqrt{3i}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right] = 2\cdot 2 = 4$$

así que

$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{3},\sqrt{3i}\right)/\mathbb{Q}\right) \simeq G, \qquad |G| = 4, \qquad G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.18 *Sea* $p \in K[x]$, *tal que* $K[x] = \mathbb{Q}(\xi)$ *donde* $\xi = e^{2\pi i/5}$, *y* $p(x) = x^5 - 7$. *Estudiar* $\mathcal{G}al\,(S/K)$.

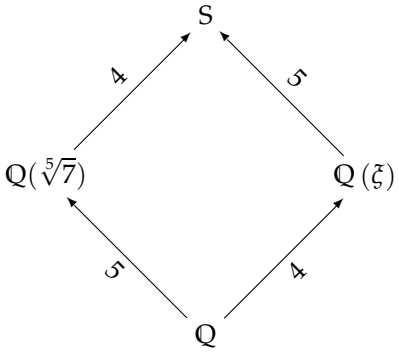
Solución. Como siempre lo primero es calcular las raíces de p, siendo éstas:

$$\left(\sqrt[5]{7},\xi\right)$$

por lo tanto

$$S = \mathbb{Q}\left(\sqrt[5]{7},\xi\right), \qquad K = \mathbb{Q}(\xi)$$

y el diagrama es:



por lo que

$$[S:\mathbb{Q}]=\left[S:\mathbb{Q}\left(\sqrt[5]{7}\right)\right]\left[\mathbb{Q}\left(\sqrt[5]{7}\right):\mathbb{Q}\right]=4\cdot 5=20,$$

observar que

$$\begin{aligned}[\mathbb{Q}(\xi):\mathbb{Q}]&=4, \qquad x^4+x^3+x^2+x+1,\\ \left[\mathbb{Q}\left(\sqrt[5]{7}\right):\mathbb{Q}\right]&=5, \qquad x^5-7,\end{aligned}$$

Al ser

$$[S:K=\mathbb{Q}(\xi)]=5,$$

entonces

$$\mathcal{G}al\left(\mathbb{Q}\left(S/K\right)\right)\simeq G, \qquad |G|=5, \qquad G\simeq\mathbb{Z}_5.$$

existen 5 automorfismos tales que, si $\alpha=\sqrt[5]{7}$

$$\begin{aligned}\sigma_1&:\alpha\longrightarrow\alpha\\ \sigma_2&:\alpha\longrightarrow\alpha\xi\\ \sigma_3&:\alpha\longrightarrow\alpha\xi^2\\ \sigma_4&:\alpha\longrightarrow\alpha\xi^3\\ \sigma_5&:\alpha\longrightarrow\alpha\xi^4\end{aligned}$$

y por lo tanto

$$\mathcal{G}al\left(\mathbb{Q}\left(S/K\right)\right)=\{\mathrm{id}=\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5\}\simeq\mathbb{Z}_5$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.19 *Estudiar el grupo* $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)\right)$.

Solución. El panorama es el siguiente

$$\mathbb{Q}\underset{x^2-2}{\overset{2}{\longrightarrow}}\mathbb{Q}\left(\sqrt{2}\right)\underset{x^2-\sqrt{2}}{\overset{2}{\longrightarrow}}\mathbb{Q}\left(\sqrt[4]{2}\right)$$

se trata de una descomposición normal, y por lo tanto

$$\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=4, \qquad x^4-2$$

tenemos dos automorfismos

$$\begin{aligned}\sigma_1&:\sqrt[4]{2}\longrightarrow\sqrt[4]{2},\\ \sigma_2&:\sqrt[4]{2}\longrightarrow-\sqrt[4]{2},\end{aligned}$$

por lo que

$$\mathcal{G}al\left(\mathbb{Q}\left(S/K\right)\right)=\{\mathrm{id}=\sigma_1,\sigma_2\}\simeq\mathbb{Z}_2$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.20 *Estudiar el grupo* $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\right)$.

Solución. En este caso, como ya sabemos esta descomposición no es normal, ya que $\sqrt[4]{2i} \notin \mathbb{Q}\left(\sqrt[4]{2}\right)$. Consideremos el campo de descomposición $\mathbb{Q}\left(\alpha = \sqrt[4]{2}, i\right)$, donde existe un automorfismo σ tal que

$$\begin{aligned}
&\sigma : \alpha \longrightarrow \alpha \\
&\sigma : \alpha \longrightarrow i\alpha \notin \mathbb{Q}\left(\sqrt[4]{2}\right) \\
&\sigma : \alpha \longrightarrow -\alpha \\
&\sigma : \alpha \longrightarrow -i\alpha \notin \mathbb{Q}\left(\sqrt[4]{2}\right)
\end{aligned}$$

por lo tanto

$$\mathcal{G}al\left(\mathbb{Q}\left(S/K\right)\right) = \{\mathrm{id}, \sigma\} \simeq \mathbb{Z}_2$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.21 *Estudiar el grupo* $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}\right)$.

Solución. En este caso sabemos que $\mathbb{Q}\left(v = \sqrt[4]{2}, i\right)$ es el SF de $x^4 - 2$, sobre $\mathbb{Q}$ y cuyas raíces son

$$R_p = \left\{-i\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, \sqrt[4]{2}\right\} = \{v, -v, iv, -iv\}$$

De esta forma vemos que tenemos la siguiente situación:

$$\begin{aligned}
B_v &= \left\{1, v, v^2, v^3\right\}, \qquad p_v = x^4 - 2, \\
B_i &= \{1, i\}, \qquad p_i = x^2 + 1,
\end{aligned}$$

por lo que una base del SF será

$$B_{(v,i)} = \left\{1, v, v^2, v^3, i, iv, iv^2, iv^3\right\}.$$

Si $\xi \in G$ entonces $\xi\left(i\right) = \pm i$ y

$$\xi\left(v\right) = \{v, iv, -v, -iv\}$$

(observar que son las raíces del poli mini $x^4 - 2$) y que el grupo tiene orden 8, ya que

$$\left[\mathbb{Q}\left(v, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(v, i\right) : \mathbb{Q}\left(v\right)\right]\left[\mathbb{Q}\left(v\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8$$

por lo que $|G| = 8$. Por lo tanto existen dos automorfismos actuando sobre cada una las raíces de tal forma que el grupo de Galois estará formado por:

$$\mathcal{G}\left(\mathbb{Q}\left(v, i\right)/\mathbb{Q}\right) = \left\{id, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\right\} \approx D_4,$$

o escrito de otra forma estos 8 elementos son

	v	i
ι	v	i
$\sigma = \alpha$	iv	i
$\sigma^2 = \beta$	$-v$	i
$\sigma^3 = \gamma$	$-iv$	i
$\tau = \lambda$	v	$-i$
$\tau\sigma = \mu$	iv	$-i$
$\tau\sigma^2 = \nu$	$-v$	$-i$
$\tau\sigma^3 = \rho$	$-iv$	$-i$

y la pertinente tabla multiplicativa del grupo está dada por:

	ι	α	β	γ	λ	μ	ν	ρ
ι	ι	α	β	γ	λ	μ	ν	ρ
α	α	β	γ	ι	μ	ν	ρ	λ
β	β	γ	ι	α	ν	ρ	λ	μ
γ	γ	ι	α	β	ρ	λ	μ	ν
λ	λ	ρ	ν	μ	ι	γ	β	α
μ	μ	λ	ρ	ν	α	ι	γ	β
ν	ν	μ	λ	ρ	β	α	ι	γ
ρ	ρ	ν	μ	λ	γ	β	α	ι

donde algunas cuantecillas son necesarias para explicar los resultados. Por ejemplo vemos que $\alpha(\lambda(v)) = \alpha(v) = iv$, de igual forma se ve que $\alpha(\lambda(i)) = \alpha(-i) = -i$, y por lo tanto deducimos que $\alpha\lambda = \mu$. De forma semejante vemos que $\lambda(\alpha(v)) = \lambda(iv) = \lambda(i)\lambda(v) = -iv$, y por lo tanto $\lambda\alpha = \rho$.

Este grupo tiene tres subgrupos de orden 4, (éstos son normales),

$$H_1 = \{\iota, \alpha, \beta, \gamma\} \approx \mathbb{Z}_4, \qquad H_2 = \{\iota, \beta, \lambda, \nu\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2, \qquad H_3 = \{\iota, \beta, \mu, \rho\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2,$$

y 5 subgrupos de orden 2.

$$H_4 = \{\iota, \beta\} \approx \mathbb{Z}_2, \qquad H_5 = \{\iota, \lambda\} \approx \mathbb{Z}_2, \qquad H_6 = \{\iota, \mu, \} \approx \mathbb{Z}_2, \qquad H_7 = \{\iota, \nu\} \approx \mathbb{Z}_2, \qquad H_8 = \{\iota, \rho\} \approx \mathbb{Z}_2,$$

donde el subgrupo H_4 también es normal.

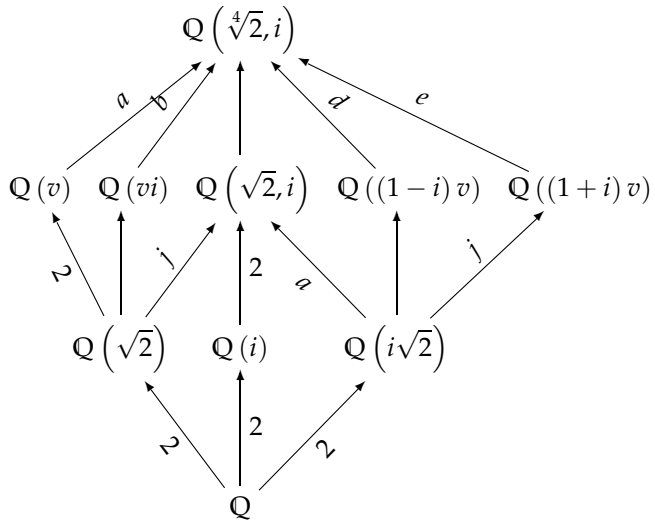
Las correspondencias son los subcampos son: $\phi(H_i) = K_j$

H_i	K_j
$\phi(H_1)$	$\mathbb{Q}(i)$
$\phi(H_2)$	$\mathbb{Q}(v^2) = \mathbb{Q}\left(\sqrt{2}\right)$
$\phi(H_3)$	$\mathbb{Q}\left(i\sqrt{2}\right)$
$\phi(H_4)$	$\mathbb{Q}\left(\sqrt{2}, i\right)$
$\phi(H_5)$	$\mathbb{Q}(v)$
$\phi(H_6)$	$\mathbb{Q}((1+i)v)$
$\phi(H_7)$	$\mathbb{Q}(vi)$
$\phi(H_8)$	$\mathbb{Q}((1-i)v)$

algunas de estas relaciones no son nada obvias. Se observa que los subcampos correspondientes a subgrupos normales son extensiones normales i.e son campos de descomposición,

$$\begin{aligned}
\phi(H_1) &= \mathbb{Q}(i), \qquad x^2 + 1, \\
\phi(H_2) &= \mathbb{Q}\left(\sqrt{2}\right), \qquad x^2 - 2, \\
\phi(H_3) &= \mathbb{Q}\left(i\sqrt{2}\right), \qquad x^2 + 2, \\
\phi(H_4) &= \mathbb{Q}\left(\sqrt{2}, i\right), \qquad \left(x^2 + 1\right)\left(x^2 - 2\right).
\end{aligned}$$

La relación entre los subcampos viene descrita en el siguiente diagrama



Una última obsevación. $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[4]{2},i\right)/\mathbb{Q}\right)$ no es abeliano.

Tomemos un elemento x que escribimos como

$$x=\lambda_0+\lambda_1 v+\lambda_2 v^2+\lambda_3 v^3+\lambda_4 i+\lambda_5 iv+\lambda_6 iv^2+\lambda_7 iv^3,$$

y vemos que x es fijo bajo $\sigma\tau$ sii

$$\begin{aligned}\sigma\tau(x)&=\lambda_0+\lambda_1 iv-\lambda_2 v^2-\lambda_3 iv^3-\lambda_4 i+\lambda_5(-i)iv-\lambda_6 i\,(iv)^2-\lambda_7 i\,(iv)^3,\\&=\lambda_0+\lambda_5 v-\lambda_2 v^2-\lambda_7 v^3-\lambda_4 i+\lambda_1 iv+\lambda_6 iv^2-\lambda_3 iv^3,\end{aligned}$$

y por lo tanto

$$\lambda_0=\lambda_0,\quad \lambda_1=\lambda_5,\quad \lambda_2=-\lambda_2,\quad \lambda_3=-\lambda_7,\quad \lambda_4=-\lambda_4,\quad \lambda_5=\lambda_1,\quad \lambda_6=\lambda_6,\quad \lambda_7=-\lambda_3,$$

de esta forma llegamos a que

$$\lambda_2=\lambda_4=0,\qquad \lambda_1=\lambda_5,\qquad \lambda_7=-\lambda_3,$$

de tal forma que

$$\begin{aligned}x&=\lambda_0+\lambda_1(1+i)v+\lambda_6 iv^2+\lambda_3(1-i)v^3,\\&=\lambda_0+\lambda_1(1+i)v+\frac{\lambda_6}{2}((1+i)v)^2-\frac{\lambda_3}{2}((1+i)v)^3,\end{aligned}$$

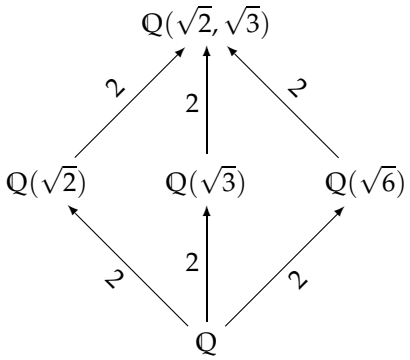
lo que demuestra que

$$\langle\sigma\tau\rangle'=\mathbb{Q}((1+i)v),$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.22 *Sea* $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, *calcular* $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\left(\sqrt{6}\right)\right)$.

Solución. Como ya sabemos el gráfico es el siguente



y por lo tanto

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt{6}\right)\right]\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]=2\cdot 2=4,$$

así que

$$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\left(\sqrt{6}\right)\right)\right|=2,$$
$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\left(\sqrt{6}\right)\right)=\{\mathrm{id},\mu\}=\mathbb{Z}_2,$$

donde $\mu(\alpha)=\pm\alpha$,siendo $\alpha=\sqrt{6}$.

Veamos este mismo ejercicio de forma algo más detallada. Queremos calcular en este caso $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)$. Sabemos que tenemos dos raíces $\sqrt{2},\sqrt{3}$ que que el orden del grupo debe ser 4 por lo expuesto anteriormente i.e.

$$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)\right|=4,$$

con

$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)\approx\mathbb{Z}_2\times\mathbb{Z}_2,$$

ya que

$$B_\alpha=\{1,\alpha\},\qquad p_\alpha=x^2-2,\qquad \alpha=\sqrt{2}$$
$$B_\beta=\{1,\beta\},\qquad p_\beta=x^2-3,\qquad \beta=\sqrt{3},$$

de esta forma una base para el SF $E=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ será

$$B_{(\alpha,\beta)}=\{1,\alpha,\beta,\alpha\beta\}=\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\},\qquad p_{(\alpha,\beta)}=\left(\left(x-\sqrt{2}\right)^2-3\right)\left(\left(x+\sqrt{2}\right)^2-3\right)=x^4-10x^2+1,$$

de esta forma vemos que deben existir dos automorfismos σ,τ que transforman las raíces de los polinomios mínimos, por lo tanto

$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)=\{\mathrm{id},\sigma,\tau,\sigma\tau\},$$

donde

	α	β
σ	$-\alpha$	β
τ	α	$-\beta$
$\sigma\tau$	$-\alpha$	$-\beta$

y por lo tanto encontramos las siguientes correspondencias entre subgrupos y subcampos:

subgrupo		*subcampo*
$G_1=\{id,\sigma\}$		$E_1=\mathbb{Q}\left(\sqrt{3}\right)$
$G_2=\{id,\tau\}$		$E_2=\mathbb{Q}\left(\sqrt{2}\right)$
$G_3=\{id,\sigma\tau\}$		$E_3=\mathbb{Q}\left(\sqrt{6}\right)$

al ser el grupo abeliano, entonces todos los subgrupos son normales y lo tanto las extensiones que generan. Para asegurarnos de esta última afirmación tomamos un elemento x que escribimos como

$$x = \lambda_0 + \lambda_1\alpha + \lambda_2\beta + \lambda_3\alpha\beta,$$

y vemos que

$$\sigma(x) = \lambda_0 - \lambda_1\alpha + \lambda_2\beta - \lambda_3\alpha\beta,$$

por lo que $\sigma(x) = x$ sii $\lambda_1 = \lambda_3 = 0$, de esta forma vemos que $\langle\sigma\rangle' = \mathbb{Q}\left(\sqrt{3}\right)$ ■

Ejercicio 3.3.23 *Sea K es SF de $p(x) = x^2 - x + 1 \in \mathbb{Q}(x)$, y L el SF de $q(x) = x^3 - 2$. Calcular $\mathcal{G}al\,(L/K)$.*

Solución. Como siempre en estos casos empezamos calculando las raíces de ambos polinomios siendo éstas:

$$R_p = \left\{\frac{1}{2}\left(1 \pm \sqrt{3i}\right)\right\}, \qquad \Longrightarrow \qquad K = \mathbb{Q}\left(\sqrt{3i}\right),$$
$$R_q = \left\{\sqrt[3]{2}, -\frac{1}{2}\left(1 \pm \sqrt{3i}\right)\right\}, \qquad \Longrightarrow \qquad K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3i}\right),$$

de esta forma tenemos que

$$\mathbb{Q} \xrightarrow{2} K \xrightarrow{3} L,$$

la extensión L/K es normal

$$|\mathcal{G}al\,(L/K)| = 3 = [L : K]$$

donde

$$L = K\left(\sqrt[3]{2}\right), \qquad m = x^3 - 2, \qquad \alpha = \sqrt[3]{2}.$$

entonces

$$\mathcal{G}al\,(L/K) = \mathbb{Z}_3$$

donde exsiten 3 automorfismos que transforman α en:

$$\sigma_1 : \alpha \to \alpha, \qquad \sigma_2 : \alpha \to \omega\alpha, \qquad \sigma_1 : \alpha \to \bar{\omega}\alpha,$$

donde $\omega = \sqrt{3i}$. ■

Ejercicio 3.3.24 *Sea $\alpha = \sqrt{2} + i$, calcular el poli mínimo, m, todos los subcuerpos así como $\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2}, i\right)/\mathbb{Q}\right)$.*

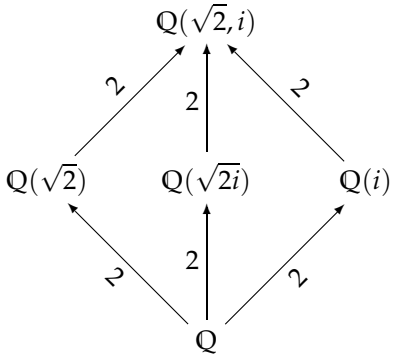
Solución. Definimos

$$\mathbb{Q}\left(\sqrt{2} + i\right) = \mathbb{Q}\left(\sqrt{2}, i\right)$$

el polinomio mínimo es: $\left((x-i)^2 - 2\right)\left((x+i)^2 - 2\right)$ y por lo tanto

$$m = x^4 - 2x^2 + 9$$

y por lo tanto



donde

$$\left[\mathbb{Q}\left(\sqrt{2},i\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2},i\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2\cdot 2=4$$

por lo que

$$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},i\right)/\mathbb{Q}\right)\right|=\left[\mathbb{Q}\left(\sqrt{2},i\right):\mathbb{Q}\right]=4$$

por lo tanto

$$\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2},i\right)/\mathbb{Q}\right)=\{\mathrm{id},\sigma,\tau,\tau\sigma\}=\mathbb{Z}_2\times\mathbb{Z}_2$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.25 *Mostrar que los siguientes grupos de Galois tienen los órdenes dados*

Solución.

1. $\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\right)\right|=2$, simple aplicación del teorema tower law, vemos que

   $$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\right)\right|=\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2,$$

   calculamos el poli minimo de $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$, siendo éste x^2-2.

2. $\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right|=1$. Este es el único caso curioso ya que no es un SF.

   Consideremos un automorfismo ϕ del grupo, $\mathcal{G}$, ϕ debe permutar las raíces del polinomio x^3-2. El problema es que este poli tiene raíces complejas. Sabemos que

   $$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right|=1\neq\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3,$$

   y que

   $$\mathbb{Q}\left(\sqrt[3]{2}\right)=\left\{a+b2^{1/3}+c2^{2/3};a,b,c\in\mathbb{Q}\right\},$$

   y que si $\phi\in\mathcal{G}$, entonces

   $$\phi\left(a+b2^{1/3}+c2^{2/3}\right)=a+b\phi\left(2^{1/3}\right)+c\phi\left(2^{2/3}\right),$$

   por lo que sólo puede tratarse de la idententidad id. Así que

   $$\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right|=1.$$

3. $\left|\mathcal{G}al\left(\mathbb{Q}\left(-\frac{1}{2}\left(1+\sqrt{3i}\right)\right)/\mathbb{Q}\right)\right| = 2$, $m = x^2+x+1$,

$$\left(x+\frac{1}{2}\left(1-\sqrt{3i}\right)\right)\left(x+\frac{1}{2}\left(1+\sqrt{3i}\right)\right).$$

4. $\left|\mathcal{G}al\left(\mathbb{Q}\left(\sqrt[4]{2},i\right)/\mathbb{Q}\right)\right| = 8$.

■

Ejercicio 3.3.26 *Sea* $\xi = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, $S = \mathbb{Q}(\xi)$.

1. *Demostrar que* $S = \mathbb{Q}(\xi)$ *es SF de* $p(x) = x^4+x^3+x^2+x+1$.
2. $|\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q})| = 4$.
3. *Suponer que* $\phi \in \mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q})$, *tal que* $\phi(\xi) = \xi^2$, *entonces mostrar que*

$$\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q}) = \left\{\mathrm{id}, \phi, \phi^2, \phi^3\right\} = \mathbb{Z}_4.$$

4. *Encontrar todos los subcampos y sus subgrupos correspondientes.*

Solución. Consideramos el polinomio $x^4+x^3+x^2+x+1$, cuyas raíces son:

$$R_p = \left\{e^{\frac{2\pi ki}{5}}, k = 1,2,3,4\right\} = \left\{\xi, \xi^2, \xi^3, \xi^4\right\}$$

y el cuerpo $S = \mathbb{Q}(\xi)$ contiene a todas las ráices de p por lo que se trata de un SF. que al ser normal y separable entonces por el teorema fundamental tenemos que

$$|\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q})| = 4 = [\mathbb{Q}(\xi):\mathbb{Q}]$$

donde por supuesto el poli mínimo es $p(x) = x^4+x^3+x^2+x+1$.

Sea la base dada por

$$B = \left\{1, \xi, \xi^2, \xi^3\right\}$$

sabemos que debe haber exactamente 4 automorfismos tales que

$$\phi_1(\xi) = \xi, \qquad \phi_2(\xi) = \xi^2, \qquad \phi_3(\xi) = \xi^3, \qquad \phi_4(\xi) = \xi^4$$

por lo que

$$\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q}) = \left\{\mathrm{id} = \phi_1, \phi_2, \phi_3, \phi_4\right\},$$

pero si por hipótesis $\phi(\xi) = \xi^2$ entonces $\phi^3(\xi) = \xi^3$, y $\phi^2(\xi) = \xi^4$, por lo que

$$\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q}) = <\phi> = \mathbb{Z}_4$$

ya que $\phi_2 = \phi$, $\phi_3 = \phi^2$, $\phi_4 = \phi^3$.

Claramente cualquier subgrupo que contenga a ϕ, contiene todo y como ϕ^3 is el inverso de ϕ lo mismo es verdad de cualquier subgrupo de contenga ϕ^3. Por lo tanto, para un subgrupo propio no debemos incluir ϕ o ϕ^3. De esta

forma llegamos a que dicho subgrupo debe contener $\{\mathrm{id}, \phi^2\}$, siendo éste el único subgrupo. Así que tenemos la siguiente correspondencia

$$\begin{array}{ccc} \mathcal{G}al & \longrightarrow & \mathbb{Q} \\ \uparrow & & \downarrow \\ \{\mathrm{id}, \phi^2\} & \longrightarrow & F_1 \\ \uparrow & & \downarrow \\ \mathrm{id} & \longrightarrow & \mathbb{Q}(\xi) \end{array}$$

Para todo elemento de $\mathbb{Q}(\xi)$ se puede escribir de la forma

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3, \qquad a_i \in \mathbb{Q}$$

el campo intermedio está generado por $\{\mathrm{id}, \phi^2\} = H_1$, de tal forma que

$$\phi^2(x) = x, \qquad \forall x \in \mathbb{Q}(\xi).$$

Calculamos

$$\begin{aligned} \phi^2(x) = \phi^2(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3) = a_0 + a_1\xi^4 + a_2\xi^3 + a_3\xi^2 = \\ = a_0 + a_1\left(-1 - \xi - \xi^2 - \xi^3\right) + a_2\xi^3 + a_3\xi^2 = \\ = (a_0 - a_1) - a_1\xi + (a_3 - a_1)\xi^2 + (a_2 - a_1)\xi^3, \end{aligned}$$

con $\left(\xi^4 = -1 - \xi - \xi^2 - \xi^3\right)$ sii

$$\begin{aligned} a_0 &= a_0 - a_1, \\ a_1 &= -a_1, \\ a_2 &= a_3 - a_1, \\ a_3 &= a_2 - a_1, \end{aligned}$$

por lo tanto

$$a_0 = a_0, \qquad a_1 = 0, \qquad a_2 = a_3,$$

por lo que

$$x = a + b\xi^2 + b\xi^3 = a + b\left(\xi^2 + \xi^3\right) \in \mathbb{Q}(\xi^2 + \xi^3),$$

de esta forma llegamos a que

$$F_1 = \mathbb{Q}(\xi^2 + \xi^3) = \left\{a + b\left(\xi^2 + \xi^3\right)\right\},$$

tal y como querímos hacer ver. Observamos que hemos utilizado el hecho de que

$$\phi^2(a_1\xi) = a_1\phi^2(\xi) = a_1\xi^4, \qquad \phi^2\left(a_2\xi^2\right) = a_2\xi^3, \qquad \phi^2\left(a_3\xi^4\right) = a_3\xi^2.$$

Observación 3.3.1 *En general, si* $\xi = e^{\frac{2\pi k i}{p}}$, $p -$ *primo, entonces*

$$\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q}) = \{\sigma_i\}_{i=1}^{p-1}, \qquad \sigma_i(\xi) = \xi^i,$$

y

$$\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q}) \approx \mathbb{Z}_{p-1},$$

ya que $\mathbb{Q}(\xi)$ *es el CD de* $p = x^p - 1/x - 1$.

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1 = |\mathcal{G}al(\mathbb{Q}(\xi)/\mathbb{Q})|.$$

■

Ejercicio 3.3.27 *Calcular y estudiar el* $\mathcal{G}al\left(x^3-3x+1\right)$.

Solución. Las raíces de

$$x^3-3x+1=0$$

son todas complejas. Sea α una de ellas, entonces las otras dos son α^2-2, y $2-\alpha-\alpha^2$.

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=3$$

y por lo tanto al tratarse de una extensión normal etc... (i.e. podemos aplicar el teoremita)

$$|\mathcal{G}al\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)|=[\mathbb{Q}(\alpha):\mathbb{Q}]=3$$

donde

$$\mathcal{G}al\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)=\mathbb{Z}_3$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.28 *Determinar la clausura normal etc... de* $\mathbb{Q}(\alpha)$, *con* $\alpha=\sqrt[4]{3}$.

Solución. Vemos que el poli mínimo es

$$p_m\left(x\right)=x^4-3,$$

entonces $N=\mathbb{Q}(p_m)$. Las raíces de

$$R_{p_m}=\{\pm\alpha,\pm\alpha i\}=\left\{\alpha i^k\right\}_{k=0}^{3},$$

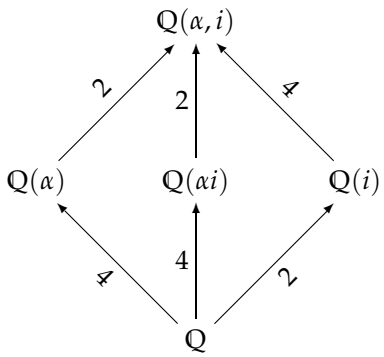
por lo tanto

$$N=\mathbb{Q}(\alpha,i),$$

viendo de esta forma que

$$[N:\mathbb{Q}]=[N:F_1]\,[F_1:\mathbb{Q}]=2\cdot 4=8$$

donde



Ahora bien, al ser todas las extensiones finitas y separables (ya que $\mathrm{char}\mathbb{Q}=0$) para aquellas que sean normales se tiene que

$$|\mathcal{G}al|=[E:\mathbb{Q}],$$

por lo tanto, si $\alpha = \sqrt[4]{3}$ entonces

$$G = \mathcal{G}al\left(\mathbb{Q}\left(\alpha\right)/\mathbb{Q}\right).$$

Como las únicas raíces de p_m en $\mathbb{Q}\left(\alpha\right)$ son $\pm\alpha$, entonces $\sigma\left(\alpha\right) \in \left\{\pm\alpha\right\}$, para cualquier $\sigma \in G$. Dado que existe un automorfismo de $\mathbb{Q}\left(\alpha\right)$ entonces $G = \left\{1, \sigma\right\} \simeq \mathbb{Z}_2$.

Sea ahora

$$G = \mathcal{G}al\left(\mathbb{Q}\left(\alpha, i\right)/\mathbb{Q}\right), \qquad |G| = 8$$

por lo tanto

$$\sigma\left(\alpha\right) \in \left\{\pm\alpha\right\}, \qquad \sigma\left(i\right) \in \left\{\pm i\right\}$$

por lo tanto tenemos 8 posibilidades donde

$$G = \langle \rho, \tau \rangle$$

con ord $(\rho) = 4$, y ord $(\tau) = 2$, por lo tanto $G = \langle \rho, \tau \rangle \simeq D_4$. ■

Ejercicio 3.3.29 *Determinar la clausura normal etc... de* $\mathbb{Q}(\alpha)$*, con* α *raíz sexta de la unidad.*

Solución. Vemos que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es normal.

Las raíces de $p = x^6 - 1 = \left(x-1\right)\left(x+1\right)\left(x^2+x+1\right)\left(x^2-x+1\right)$, son:

$$R_p = \left\{\pm 1, \frac{1}{2}\left(\pm 1 \pm \sqrt{3i}\right)\right\},$$

por lo tanto el poli mín. que genera $\alpha = \frac{1}{2}\left(1 + \sqrt{3i}\right)$, es

$$p_m = x^2 - x + 1,$$

de esta forma llegamos a

$$[E : \mathbb{Q}] = 2$$

Sea

$$G = \mathcal{G}al\left(\mathbb{Q}\left(\alpha\right)/\mathbb{Q}\right).$$

Como las únicas raíces de p_m en $\mathbb{Q}\left(\alpha\right)$ son $\pm\alpha$, entonces $\sigma\left(\alpha\right) \in \left\{\pm\alpha\right\}$, para cualquier $\sigma \in G$. Dado que existe un automorfismo de $\mathbb{Q}\left(\alpha\right)$ entonces $G = \left\{1, \sigma\right\} \simeq \mathbb{Z}_2$. ■

Ejercicio 3.3.30 *Determinar* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *con* α *raíz de* $x^4 - 6x^2 + 6$.

Solución. Vemos que el poli $p = x^4 - 6x^2 + 6$ es irreducible en $\mathbb{Q}\left[x\right]$ (aplicando C.E. con $p = 2$), por lo tanto p es el poli mímino de α sobre $\mathbb{Q}$. De esta forma vemos que

$$E = N = \mathbb{Q}\left(p\right),$$

donde

$$R_p = \left\{\pm\sqrt{3 \pm \sqrt{3}}\right\}$$

por lo tanto

$$N = \mathbb{Q}\left(\alpha, \beta\right),$$

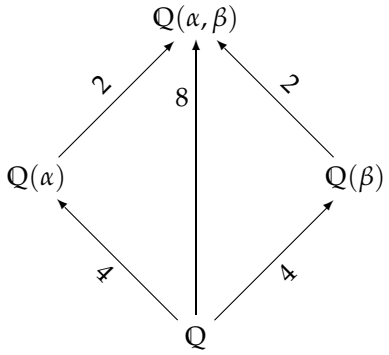
donde

$$\alpha = \sqrt{3 + \sqrt{3}}, \qquad \beta = \sqrt{3 - \sqrt{3}},$$

donde

$$\beta \notin \mathbb{Q}(\alpha).$$

De esta forma vemos que



$$[N:\mathbb{Q}] = 8.$$

De igual forma vemos que si $\alpha \in R_p$, entonces $R_p \in \mathbb{Q}(\alpha) = \{\pm\alpha\}$ y por lo tanto

$$G = \mathcal{G}al\left(\mathbb{Q}\left(\alpha\right)/\mathbb{Q}\right),$$

como las únicas raíces de p_m en $\mathbb{Q}\left(\alpha\right)$ son $\pm\alpha$, entonces $\sigma\left(\alpha\right) \in \{\pm\alpha\}$, para cualquier $\sigma \in G$. Dado que existe un automorfismo de $\mathbb{Q}\left(\alpha\right)$ entonces $G = \{1, \sigma\} \simeq \mathbb{Z}_2$.

Al mismo tiempo vemos que

$$\left|\mathcal{G}al\left(\mathbb{Q}\left(\alpha,\beta\right)/\mathbb{Q}\right)\right| = 8, \qquad G \simeq D_4,$$

por lo tanto tenemos 8 posibilidades donde

$$G = \langle \rho, \tau \rangle$$

con ord $(\rho) = 4$, y ord $(\tau) = 2$, por lo tanto $G = \langle \rho, \tau \rangle \simeq D_4$. ■

Ejercicio 3.3.31 *Determinar* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *con* $\alpha = \sqrt{1+\sqrt{7}}$.

Solución. El polinomio característico de α es:

$$\alpha^2 - 1 = \sqrt{7},$$

por lo tanto

$$x^4 - 2x^2 - 6,$$

viendo que las raices de este polinomio son

$$R_f = \left\{\pm\alpha, \pm\sqrt{1-\sqrt{7}}\right\},$$

por lo que el campo de descomposición es

$$E = \mathbb{Q}\left(\alpha, i\right),$$

y los subcampos:

$$\begin{aligned} \mathbb{Q}\left(\alpha\right), \qquad & B_{\mathbb{Q}(\alpha)} = \left\{1, \alpha, \alpha^2, \alpha^3\right\}, \\ \mathbb{Q}\left(i\right) \qquad & B_{\mathbb{Q}(i)} = \{1, z\} \end{aligned}$$

así que

$$[E:\mathbb{Q}]=4\cdot 2=8,\qquad |\mathcal{G}al\left(\mathbb{Q}\left(\alpha,i\right)/\mathbb{Q}\right)|=8,\qquad G\simeq D_4$$

por lo tanto tenemos 8 posibilidades donde

$$G=\langle\rho,\tau\rangle$$

con ord $(\rho)=4$, y ord $(\tau)=2$, por lo tanto $G=\langle\rho,\tau\rangle\simeq D_4$. ■

Ejercicio 3.3.32 *Determinar* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *con* $\alpha=\sqrt{2+\sqrt{2}}$.

Solución. El polinomio característico de α es:

$$\alpha^2-2=\sqrt{2},$$

por lo tanto

$$x^4-4x^2+2,$$

viendo que las raices de este polinomio son

$$R_f=\left\{\pm\sqrt{2\pm\sqrt{2}}\right\}=\{\pm\alpha,\pm\beta\},\qquad \alpha=\sqrt{2+\sqrt{2}},\qquad \beta=\sqrt{2-\sqrt{2}},$$

por lo que el campo de descomposición es

$$E=\mathbb{Q}\left(\alpha,\beta\right),$$

pero vemos que

$$\beta=\psi\left(\alpha\right)$$

por lo que

$$E=\mathbb{Q}\left(\alpha\right)$$

con:

$$\mathbb{Q}\left(\alpha\right),\qquad B_{\mathbb{Q}(\alpha)}=\left\{1,\alpha,\alpha^2,\alpha^3\right\},$$

así que

$$[E:\mathbb{Q}]=4,\qquad |\mathcal{G}al\left(\mathbb{Q}\left(\alpha,i\right)/\mathbb{Q}\right)|=4,\qquad G\simeq\mathbb{Z}_4$$

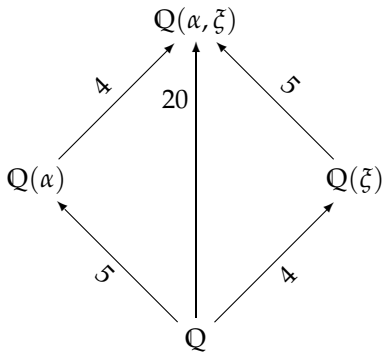
con ord $(\rho)=4$. ■

Ejercicio 3.3.33 *Determinar* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *con* α *raíz de* x^5-2.

Solución. Las raíces de x^5-2 son

$$R_p=\left\{\alpha\xi^k\right\}_{k=0}^{4},\qquad \alpha=\sqrt[5]{2},\qquad \xi=e^{2\pi i/5},$$

por lo tanto la descomposición es la siguiente:



$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha):\mathbb{Q}] = 4\cdot 5 = 20.$$

Vemos que $G = \mathcal{G}al\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right) = \{1\}$, al ser α la única raíz de p en $\mathbb{Q}(\alpha)$. Para determinar el grupo de Galois de $\mathcal{G}al\left(\mathbb{Q}(\alpha,\xi)/\mathbb{Q}\right)$ vemos que

$$\left|\mathcal{G}al\left(\mathbb{Q}(\alpha,\xi)/\mathbb{Q}\right)\right| = 20$$

teniéndose (α,ξ) tales que $\alpha \in R\left(x^5-2\right)$ y $\xi \in R\left(x^4+x^3+x^2+x+1\right)$, por lo tanto existe un automorfismo tal que

$$\sigma_{ij}(\alpha) = \alpha\xi^i, \qquad \sigma_{ij}(\xi) = \xi^j,$$

así que

$$G = \{\sigma_{ij}\} \simeq \mathbb{Z}_5 \times \mathbb{Z}_4,$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.34 *Determinar* $E = \mathbb{Q}(p)/\mathbb{Q}\left(\sqrt{3i}\right)$, *con* $p = \left(x^3-2\right)\left(x^2-5\right)$, *así como* $\mathcal{G}al\left(E/\mathbb{Q}\left(\sqrt{3i}\right)\right)$.

Solución. Las raíces de $p = \left(x^3-2\right)\left(x^2-5\right)$, son

$$R_p = \left\{\pm\sqrt{5}, \sqrt[3]{2}\xi^k\right\}_{k=0}^{2}, \qquad \xi = \frac{1}{2}\left(-1+\sqrt{3i}\right),$$

por lo tanto podemos escribir $R_p = \left\{\pm\beta, \alpha\xi^k\right\}_{k=0}^{2}$. Vemos que $\xi \in \mathbb{Q}\left(\sqrt{3i}\right)$, por lo tanto

$$\mathbb{Q}(p)/\mathbb{Q}\left(\sqrt{3i}\right) = \mathbb{Q}(\beta,\alpha)$$

ya que el cuerpo de descomposición de p es: $\mathbb{Q}(\beta,\alpha,\xi)$, con

$$[\mathbb{Q}(\beta,\alpha,\xi):\mathbb{Q}] = 2\cdot 3\cdot 2 = 12,$$

pero aquí sólo estamos interesados en $\mathbb{Q}(\beta,\alpha)$, viendo que

$$[\mathbb{Q}(\beta,\alpha):\mathbb{Q}] = 2\cdot 3 = 6,$$

de esta forma sabemos que

$$|G| = 6,$$

sea $\sigma \in G$, tal que

$$\sigma(\alpha) = \alpha\xi, \qquad \sigma(\beta) = -\beta, \qquad \sigma(\xi) = \xi,$$

por lo tanto

$$G \simeq S_3,$$

el grupo cíclio de orden 6. ■

Ejercicio 3.3.35 *Determinar el grupo de Galois del poli* $p = \left(x^4-9\right)\left(x^2-5\right)$.

Solución. Las raíces de p son

$$R_p = \left\{\pm\sqrt{3}, \pm\sqrt{5}, \pm\sqrt{3i}\right\}$$

por lo que

$$E = \mathbb{Q}(\alpha,\beta,i),$$

con $\alpha = \sqrt{3}, \beta = \sqrt{5}$, viendo facilmente que

$$[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8, \qquad \Longrightarrow \qquad |G| = 8,$$

sea $\sigma \in G$, tal que

$$\sigma(\alpha) = \{\pm\alpha\}, \qquad \sigma(\beta) = \{\pm\beta\}, \qquad \sigma(\xi) = \pm i,$$

por lo que

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Vemos igualmente que los subcampos son:

$$F_1 = \mathbb{Q}(\alpha), \quad F_2 = \mathbb{Q}(\beta), \quad F_3 = \mathbb{Q}(i), \quad F_4 = \mathbb{Q}(\alpha\beta), \quad F_5 = \mathbb{Q}(\alpha i), \quad F_6 = \mathbb{Q}(\beta i), \quad F_7 = \mathbb{Q}(\alpha\beta i),$$

mientras que los subcuerpos de orden 4 son

$$\mathbb{Q}(\alpha, \beta), \quad \mathbb{Q}(\beta, i), \quad \mathbb{Q}(i, \alpha), \quad \mathbb{Q}(\alpha i, \beta), \quad \mathbb{Q}(\alpha\beta, i), \quad \mathbb{Q}(\alpha, \beta i), \quad \mathbb{Q}(\alpha i, \beta i),$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.36 *Determinar el grupo de Galois de $p = x^3 - x - 1$.*

Solución. Las raíces de p son

$$R_p = \{\alpha, z, \bar{z}\},$$

por lo que su SF será

$$E = \mathbb{Q}(\alpha, z)$$

tal que

$$[\mathbb{Q}(\alpha, z) : \mathbb{Q}] = 3 \cdot 2 = 6, \qquad \Longrightarrow \qquad |G| = 6,$$

ya que $\alpha = \sqrt[3]{x}$. Los subcampos son:

$$\begin{aligned} &\mathbb{Q}(\alpha), && B_{\mathbb{Q}(\alpha)} = \left\{1, \alpha, \alpha^2\right\} \\ &\mathbb{Q}(z), && B_{\mathbb{Q}(z)} = \{1, z\} \end{aligned}$$

Observación 3.3.2 *Lo primero que debemos observar es que p es irreducible y por lo tanto $G \simeq S_3$, i.e. al cíclico cuyo orden coincide con el orden del polinomio. Recordar el teorema correspondiente.*

Sea $\sigma \in G$, tal que

$$\sigma(\alpha) = z, \qquad \sigma(z) = \bar{z}, \qquad \sigma(\bar{z}) = \alpha,$$

por lo que

$$G \simeq S_3,$$

las 6 posibles combinaciones son

$$\left\{1, \alpha, \alpha^2, z, z\alpha, z\alpha^2\right\},$$

por lo tanto

$$G = \left\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\right\},$$

tal y como queríamos hacer ver. ■

Ejercicio 3.3.37 *Decide razonadamente si las siguientes afirmaciones son verdaderas o falsas.*

Solución.

1. Sean $K \subset L \subset E$ cuerpos. Si E/K es una extensión algebraica normal, entonces E/L es normal.
   VERDADERO
   Si se supone que E/K es finita, entonces por ser E/K normal se tiene que E es el cuerpo de descomposición de algún polinomio $p(x) \in K[x]$. En tal caso, E es también el cuerpo de descomposicion sobre L de $p(x) \in L[x]$ y por tanto E/L es normal.
   Si no se supone que E/K es finita, decir que E/K es normal es pedir que todo polinomio irreducible sobre K que tiene una raíz en E descompone en E. Sea $\alpha \in L$, sea $q(x) \in L[x]$ su polinomio míinimo sobre L y sea $p(x) \in K[x]$ su polinomio míinimo sobre K. Para probar que E/L es normal basta probar que $q[x]$ descompone en E, pero esto es claro ya que por ser E/K normal $p(x)$ descompone en E, y como $q(x)$ divide a $p(x)$, $q(x)$ también descompone en E, luego E/L es normal.
2. El polinomio $x^{25} + x^{15} + 1 \in \mathbb{F}_5[x]$ tiene 25 raíces distintas en su cuerpo de descomposición.
   FALSO
   Basta observar que $x^{25} + x^{15} + 1 = (x^5 + x^3 + 1)^5 \in \mathbb{F}_5[x]$, por lo que como mucho tiene 5 raíces distintas.

   Observación 3.3.3 *La derivada del polinomio es cero, por lo tanto el máximo común divisor del polinomio y su derivada es el propio polinomio, y como consecuencia sabemos que $x^{25} + x^{15} + 1$ tiene raíces repetidas.*

3. Sea E/K una extensión finita de cuerpos. Entonces $[E : K] = |\mathcal{G}al(E/K)|$.
   FALSO
   Para que haya igualdad necesitamos que E/K además de ser finita sea normal y separable. Por ejemplo, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es finita pero no normal y
   $$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 1 = |\mathcal{G}al(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|.$$

■

Ejercicio 3.3.38 *Sea $E = \mathbb{F}_7[x]/\langle p(x)\rangle$ donde $p(x) \in \mathbb{F}_7[x]$ es un polinomio irreducible de grado 4.*

1. *Calcula una base de E/K y $|E|$.*
2. *Demuestra que E es el cuerpo de descomposición de $x^{7^4} - x$ sobre $\mathbb{F}_7$.*
3. *Demuestra que E es el cuerpo de descomposición del polinomio $p(x)$ sobre $\mathbb{F}_7$.*
4. *Decide razonadamente si E contiene un subcuerpo isomorfo a $\mathbb{F}_{7^3}$.*

Solución.

1. Como $p(x) \in \mathbb{F}_7[x]$ es un polinomio irreducible de grado 4, se tiene que $[E : F7] = 4$. Una base de E/K podría ser $\{\bar{1}, \bar{x}, \bar{x}^2, \bar{x}^3\}$, y por tanto $|E| = 7^4$.
2. Como el grupo multiplicativo $E^* = E\backslash\{0\}$ tiene $7^4 - 1$ elementos, se tiene que para todo $\alpha \in E$, $\alpha^{7^4-1} = 1$. Como consecuencia, todo elemento $\beta \in E$ verifica la ecuación $x^{7^4} = x$, que, por otro lado, tiene como mucho 7^4 soluciones. Como $|E| = 7^4$ necesariamente E es el cuerpo más pequeno sobre $\mathbb{F}_7$ que contiene a todas las raíces de $x^{7^4} = x$, y por tanto es su cuerpo de descomposición.

3. Sea $L/\mathbb{F}_7$ el cuerpo de descomposición de $p(x)$ sobre $\mathbb{F}_7$, y sea $\beta \in L$ una raíz de $p(x)$. Entonces $E \simeq \mathbb{F}_7(\beta)$, y por lo tanto $E \subset L$. Por otro lado, como E es el cuerpo de descomposición de $x^{7^4} = x$ sobre $\mathbb{F}_7$, la extensión $E/\mathbb{F}_7$ es normal, y como contiene una raíz de $p(x)$, las tiene que contener todas, luego $L \subset E$. En consecuencia $E = L$.

4. Supongamos que $\mathbb{F}_{7^3} \subset E$ y sea $[E : \mathbb{F}_{7^3}] = n$. Entonces

$$4 = [E : \mathbb{F}_7] = [E : \mathbb{F}_{7^3}][\mathbb{F}_{7^3} : \mathbb{F}_7] = n3,$$

lo cual es imposible. Luego E no puede contener un subcuerpo isomorfo a $\mathbb{F}_{7^3}$.

■

Ejercicio 3.3.39 *Sea $p(x) = x^4 + 1 \in \mathbb{Q}[x]$, y sea E el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$.*

Solución.

1. Calcula E y $[E : \mathbb{Q}]$.
   El cuerpo de descomposición de $x^4 + 1$ sobre $\mathbb{Q}$ lo construiremos como subcuerpo de $\mathbb{C}$ añadiendo a $\mathbb{Q}$ las raíces del polinomio $x^4 + 1$. En la forma polar $-1 = 1_\pi$. Por lo tanto la ecuación $x^4 = -1$ tiene 4 soluciones

$$e^{(\pi/4+k\pi/2)i} = \pm\sqrt{2}/2 \pm \left(\sqrt{2}/2\right) i,$$

   $(k = 0, 1, 2, 3)$. Luego,

$$E = \mathbb{Q}(\{\pm\sqrt{2}/2 \pm \left(\sqrt{2}/2\right) i\}) = \mathbb{Q}(\sqrt{2}, i).$$

$$|E : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|.$$

   Como $x^2 - 2$ es irreducible sobre $\mathbb{Q}$, concluimos que $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$. El polinomio $x^2 + 1$ anula a i y también $i \notin \mathbb{Q}(\sqrt{2})$, luego $|\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})| = 2$. Entonces $|E : Q| = 4$.

2. Describe $\mathcal{G}al(E/\mathbb{Q})$.
   El grupo $\mathcal{G}al(E/\mathbb{Q})$ tiene cuatro elementos. Cualquier elemento de $\mathcal{G}al(E/\mathbb{Q})$ está completamente determinado por las imágenes de los generadores $\sqrt{2}$ y i de la extensión $E/\mathbb{Q}$. Notemos que $\phi\left(\sqrt{2}\right) = \pm\sqrt{2}$ (raíces de $x^2 - 2$) y $\phi(i) = \pm i$ (raíces de $x^2 + 1$). Escribimos estos datos en la siguiente tabla.

Automorfismo	i	$\sqrt{2}$
ϕ_1	i	$\sqrt{2}$
ϕ_2	$-i$	$\sqrt{2}$
ϕ_3	i	$-\sqrt{2}$
ϕ_4	$-i$	$-\sqrt{2}$

   Notemos que ϕ_1 es automorfismo identidad y $\phi_k^2 = \phi_1$ para $k = 2, 3, 4$ $(\phi_k(\phi_k(i)) = i, \phi_k(\phi_k(\sqrt{2})) = \sqrt{2})$. Por lo tanto $\mathcal{G}al(E/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Encuentra los valores de $a \in \mathbb{Q}$ para cuales $\sqrt{2}a + i\frac{\sqrt{2}}{3}$ y $\frac{\sqrt{2}}{3} - i\sqrt{2}$ son raíces del mismo polinomio irreducible sobre $\mathbb{Q}$.
   Si dos elementos x y y de E son raíces del mismo polinomio irreducible sobre Q, entonces existe un elemento del grupo $\mathcal{G}al(E/\mathbb{Q})$ que lleva x a y. Notemos que $\phi(\frac{\sqrt{2}}{3} - i\sqrt{2}) = \pm\frac{\sqrt{2}}{3} \pm i\sqrt{2}$ no es igual a $\sqrt{2}a + i\frac{\sqrt{2}}{3}$ para ningún $a \in \mathbb{Q}$ ya que $\sqrt{2}$ y $i\sqrt{2}$ son linealmente independientes sobre $\mathbb{Q}$.

4. Describe $\mathcal{G}al\left(E/\mathbb{Q}\left(\sqrt{2}i\right)\right)$.

   $\mathcal{G}al\left(E/\mathbb{Q}\left(\sqrt{2}i\right)\right)$ consiste de elementos de $\mathcal{G}al(E/\mathbb{Q})$ que fijan a $\mathbb{Q}\left(\sqrt{2}i\right)$. Por lo tanto

$$\mathcal{G}al\left(E/\mathbb{Q}\left(\sqrt{2}i\right)\right) = \{\phi_1, \phi_4\} = \mathbb{Z}_2.$$

■

Ejercicio 3.3.40 *Sea* $\xi = e^{2\pi i/13}$ *y* $E = \mathbb{Q}(\xi)$.

Solución.

1. Demostrar que $E/\mathbb{Q}$ es normal.

   Sea $p(x) = x^{13} - 1 \in \mathbb{Q}[x]$. Las raíces de este polinomio en $\mathbb{C}$ son ξ^k $(k = 0, 1, ..., 12)$. Por lo tanto el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$ es igual a E. Esto implica que $E/\mathbb{Q}$ es normal.

2. ¿Cuantos cuerpos intermedios tiene la extensión $E/\mathbb{Q}$?

   El polinomio míinimo de sobre $\mathbb{Q}$ es el polinomio ciclotómico $x^{12}+\cdots+x+1 = \frac{x^{13}-1}{x-1}$. Por lo tanto

$$[E : \mathbb{Q}] = 12.$$

   Luego el grupo de Galois de $E/\mathbb{Q}$ tiene 12 elementos $\{\phi_i\}_{i=1}^{12}$ donde ϕ_k está determinado por la igualdad

$$\phi_k(\xi) = \xi^k.$$

   La aplicación

$$Gal(E/Q) \longrightarrow \mathbb{F}_{13}^*$$

   que manda k a $k + 13\mathbb{Z}$ es un isomorfismo entre el grupo de Galois de $E/\mathbb{Q}$ y el grupo multiplicativo de $\mathbb{F}_{13}$. Por lo tanto $\mathcal{G}al(E/\mathbb{Q})$ es cíclico.

   También, se puede ver que $\mathcal{G}al(E/\mathbb{Q})$ es cíclico, observando que el orden de ϕ_2 es exactamente 12 y por lo tanto es un generador de $\mathcal{G}al(E/\mathbb{Q})$. Un grupo cíclico de orden 12 tiene un subgrupo total, uno trivial y cuatro subgrupos propios (de ordenes 2, 3, 4 y 6). Por la correspondencia de Galois, $E/\mathbb{Q}$ tiene 4 subextenciones intermedias (distintas de $\mathbb{Q}$ y $\mathbb{E}$).

3. ¿Es cierto que cualquier subextensión de $E/\mathbb{Q}$ es normal?

   Si es cierto, ya que por la correspondencia de Galois una subextensión $F/\mathbb{Q}$ de $E/\mathbb{Q}$ es normal si y sólo si $\mathcal{G}al(E/F)$ es un subgrupo normal de $\mathcal{G}al(E/\mathbb{Q})$. Por el apartado anterior $\mathcal{G}al(E/\mathbb{Q})$ es abeliano y por lo tanto todos sus subgrupos son normales. Por lo tanto todas las subextensiones de $E/\mathbb{Q}$ son normales.

4. Sea el automorfismo de E que manda ξ a ξ^3 y F la subextensión fijada por ϕ. Encontrar $[F : \mathbb{Q}]$ y el grupo de Galois de E/F.

   En la notación del apartado (2) ϕ es ϕ_3. Notemos que $\phi_3^2 = \phi_9$ y $\phi_3^3 = \phi_1$ es identidad. Por lo tanto ϕ_3 tiene orden 3. Por la correspondencia de Galois $\mathcal{G}al(E/F) = \langle\phi_3\rangle$. En particular, $[E : F] = 3$ y por la transitividad de los indices

$$[F : \mathbb{Q}] = \frac{[E : \mathbb{Q}]}{[E : F]} = 4.$$

■

Ejercicio 3.3.41 *Sea E el cuerpo de descomposición de $x^4 - 2$ sobre $\mathbb{Q}$.*

Solución.

1. Describe E y calcula $[E : \mathbb{Q}]$.

   Las raíces de $x^4 - 2$ son $\pm\sqrt[4]{2}$ y $\pm i\sqrt[4]{2}$, por lo que $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Como $x^2 - 2$ es irreducible sobre $\mathbb{Q}$ (Eissenstein con $p = 2$), se tiene que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ y como el polinomio míinimo de i sobre $\mathbb{Q}(\sqrt[4]{2})$ es un divisor de $x^2 + 1$ entonces $[E : \mathbb{Q}(\sqrt[4]{2})] \leq 2$. Como además $Q(\sqrt[4]{2}) \subset R$, necesariamente $[E : \mathbb{Q}(\sqrt[4]{2})] = 2$ y por tanto
   $$[E : \mathbb{Q}] = 8.$$

2. Describe los elementos de $\mathcal{G}(E/\mathbb{Q})$.

   Observamos en primer lugar que $E/\mathbb{Q}$ es una extensión Galois (es separable por ser una extensión de cuerpos de característica cero, y es normal por ser E el cuerpo de descomposición de $x4 - 2$ sobre $\mathbb{Q}$). Por lo tanto
   $$|\mathcal{G}(E/\mathbb{Q})| = 8.$$

   Como $\mathbb{Q}(i) \subset E$ es una extensión normal de $\mathbb{Q}$ de grado 2,
   $$|\mathcal{G}(\mathbb{Q}(i)/\mathbb{Q})| = 2,$$

   De hecho $\mathcal{G}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, \tau\}$, donde τ representa la conjugación compleja.

   Como $E/\mathbb{Q}(i)$ es Galois (en este caso de grado 4), entonces, cada automorfismo de $\mathbb{Q}(i)$ extiende exactamente a cuatro automorfismos de $E/\mathbb{Q}$.

   Observamos además que el polinomio míinimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}(i)$ es $x^4 - 2$, y que por tanto no se modifica por ningún automorfismo de $\mathbb{Q}(i)$. De este modo, cada automorfismo de E extiende a uno de $\mathbb{Q}(i)$ que necesariamente permuta las raíces de $x^4 - 2$.

   Por otro lado, por cada automorfismo de $\mathbb{Q}(i)$, existe un automorfismo de E, digamos ϕ_0, tal que
   $$\phi_0(\sqrt[4]{2}) = \sqrt[4]{2},$$
   otro, ϕ_1 tal que
   $$\phi_1(\sqrt[4]{2}) = -\sqrt[4]{2},$$
   otro
   $$\phi_2(\sqrt[4]{2}) = i\sqrt[4]{2},$$
   y finalmente otro, ϕ_3 tal que
   $$\phi_3(\sqrt[4]{2}) = -i\sqrt[4]{2},$$
   Como sólo hay cuatro automorfismos de E que extiendan a cada uno de los de $\mathbb{Q}(i)$, los descritos anteriormente son las únicas posibles extensiones. Por lo tanto ya podemos confeccionar una tabla con lo ocho automorfismos de E

	i	$\sqrt[4]{2}$	orden
φ_0	i	$\sqrt[4]{2}$	1
φ_1	i	$-\sqrt[4]{2}$	2
φ_2	i	$i\sqrt[4]{2}$	4
φ_3	i	$-i\sqrt[4]{2}$	4
φ_4	$-i$	$\sqrt[4]{2}$	2
φ_5	$-i$	$-\sqrt[4]{2}$	2
φ_6	$-i$	$i\sqrt[4]{2}$	2
φ_7	$-i$	$-i\sqrt[4]{2}$	2

3. ¿A qué grupo conocido es isomorfo $\mathcal{G}(E/\mathbb{Q})$?

   Como $G(E/Q)$ tiene ocho elementos necesariamente es isomorfo a alguno de los siguientes grupos: $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, \mathcal{Q}_8$.

   Como $\mathbb{Q}(\sqrt[4]{2}) \subset E$ no es una extensión normal de $\mathbb{Q}$, $\mathcal{G}(E/\mathbb{Q})$ no puede ser abeliano. Por tanto debe ser isomorfo a D_8 o a $\mathcal{Q}_8$. Por otro lado, $\mathcal{Q}_8$ sólo tiene un elemento de orden 2, mientras que $\mathcal{G}(E/\mathbb{Q})$ tiene 5 (ver la tabla). Por tanto $\mathcal{G}(E/\mathbb{Q}) \simeq D_8$.

4. ¿Cuántos cuerpos intermedios $B \subset E$ tienen grado 4 sobre $\mathbb{Q}$?

   Por el Teorema Fundamental de la Teoría de Galois, estos cuerpos son los cuerpos fijos por los subgrupos de $\mathcal{G}(E/\mathbb{Q})$ que tienen orden 2. Observando la tabla del apartado (b) se tiene que hay exactamente 5 subgrupos distintos de orden 2, y por tanto debe haber exactamente 5 extensiones distintas de grado 4 sobre $\mathbb{Q}$.

5. Describe todos los cuerpos intermedios que tienen grado 2 sobre $\mathbb{Q}$.

   Por el Teorema Fundamental de la Teoría de Galois, estos cuerpos son los cuerpos fijos por los subgrupos de $\mathcal{G}(E/\mathbb{Q})$ que tienen orden 4.

   Como $\mathcal{G}(E/\mathbb{Q}) \simeq D_8$, hay exactamente 3 subgrupos de orden 4:

   $$\langle \varphi_2 \rangle = \langle \varphi_3 \rangle, \qquad \langle \varphi_3, \varphi_5 \rangle, \qquad \langle \varphi_6, \varphi_7 \rangle,$$

   Podemos utilizar esta descripción de los subgrupos de orden 4 de D_8 y una base de $E/\mathbb{Q}$ para describir los cuerpos intermedios, sin embargo en este caso podemos simplificar significativamente los cálculos observando que

   $$Q(\sqrt{2}), Q(i\sqrt{2}), Q(i) \subset E,$$

   son tres extensiones distintas de $\mathbb{Q}$ y por tanto necesariamente coinciden con las que buscamos.

■

Capítulo 4

Aplicaciones

4.1. Ecuaciones y grupos.

La historia se remonta al siglo XV, con las fórmulas de Cardano et al para encontrar algoritmos que permitan resolver ecuaciones cúbicas

$$x^3 + 3ax + b = 0,$$

donde

$$(a, b) \longrightarrow \left[\frac{1}{2}\left(-b \pm \sqrt{b^2 + 4a^3}\right)\right]^{1/3},$$

sólo tomando raíces cuadradas y cúbicas, i.e. por **radicales**. Es, por lo tanto, natural preguntarse si existe algún algoritmo que nos permita resolver ecuaciones de cuarto orden.

En lo que sigue siempre se considerarán cuerpos de característica cero y por lo tanto no nos preocuparemos de su separabilidad etc.... Por lo tanto, sea K un cuerpo y sea L, tal que $K \subset L$, se dice que es una **extensión radical** si existe una familia de subcuerpos tales que

$$K = L_0 \subset L_1 \subset ... \subset L_m = L,$$

tal que

$$L_{j+1} = L\left(\alpha_j\right),$$

donde $\alpha_j \in R_f$, i.e. es una raíz del polinomio $f = x^{n_j} - c_j$. Esta definición viene a formalizar la idea de que los elementos de L se oteinen a partir de K por medio de operaciones racionales.

Ejemplo 4.1.1 $\mathbb{Q}\left(\sqrt{3}, \sqrt{\sqrt[3]{5} + \sqrt[3]{2}}\right)$ *es un extensión radical ya que*

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{5}\right) \subset \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{5}, \sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt{3}, \sqrt{\sqrt[3]{5} + \sqrt[3]{2}}\right).$$

Definición 4.1.1 *Un* ***polinomio*** $f \in K[x]$, *se dice* ***soluble*** *por radicales si existe un campo S que sea cuerpo de descomposión (SF) de f tal que $S \subset L$, donde L es una extensión radical de K.*

Observación 4.1.1 *Toda ecuación (polinomio) de grado ≤ 4, es soluble por radicales.*

Teorema 4.1.1 *Sea L una extensión radical de K y sea M la clausura normal de L, entonces M también es una extensión radical de K.*

Observación 4.1.2 *Sea L una extensión finita de K. Un campo N, tal que $L \subset N$,se dice que es la clausura normal de L sobre K si:*

1. *Es uanextensión normal de K,*
2. *$L \subset E \subset N$, donde E no es una extensión normal de K.*

Por ejemplo. $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, entonces $\mathbb{Q}\left(u, i\sqrt{3}\right)$ es su clausura normal.

4.1.1. Polinomios ciclotómicos

Son de la forma

$$f = x^n - 1,$$

donde $char(K) = 0$, L es su cuerpo de descomposición, normal, separable etc...y $R_f := \{\alpha : f(\alpha) = 0\}$, i.e. el conjunto de sus raíces. Observamos que $\left(R_f, \cdot\right)$ tiene estructura de grupo cíclico.

Sea ξ una raíz $n-$ésima de la unidad i.e. $\xi = e^{2\pi i/n}$, se trata de un generador del grupo cíclico

$$R_f = \left\{1, \xi, \xi^2, ..., \xi^{n-1}\right\},$$

donde ξ^j es otra otra raíz de la unidad sii $(j, n) = 1$, i.e. son primos.

Definimos el polinomio

$$\phi_m = \prod_{\varepsilon \in P_m} (x - \varepsilon).$$

Veamos un ejemplo aclaratorio. Sea $f = x^{12} - 1$, con $K = \mathbb{Q}$, $L \subset \mathbb{C}$ y $\xi = e^{2\pi i/12} = e^{\pi i/6}$. Entonces

$$R_f = \left\{1, \xi, \xi^2 = e^{\pi i/3}, \xi^3 = i, ..., \xi^{11} = e^{11\pi i/6}\right\},$$

y $P_d \subset R_f$, donde d es el conjunto de divisores de $n = 12$, en este caso $d = 1, 2, 3, 4, 6, 12$. De esta forma $\phi_m = \prod_{\varepsilon \in P_m} (x - \varepsilon)$ será de la forma

$$P_{12} = \left\{\xi, \xi^5, \xi^7 = \bar{\xi}^5, \xi^{11} = \bar{\xi}\right\},$$

y por lo tanto

$$\phi_{12} = x^4 - x^2 + 1.$$

Si hacemos lo mismo con P_6, P_4, P_3, P_2 y P_1, entonces vemos que

$$x^{12} - 1 = \prod_{d|12} \phi_d = (x-1)(x+1)\left(x^2 + x + 1\right)\left(x^2 + 1\right)\left(x^2 - x + 1\right)\left(x^4 - x^2 + 1\right),$$

donde se observa que ϕ_d es irreducible en $\mathbb{Q}$.

Llegamos a formular un resultado muy importante en esta sección.

Teorema 4.1.2 *En la condiciones de arriba, $\mathcal{G}(\mathbb{Q}(\xi)/\mathbb{Q})$ es isomorfo a un subgrupo del grupo cíclico $\mathbb{Z}_n$.*

Teorema 4.1.3 *Sea p primo, entonces $\mathcal{G}(L : K)$ es cíclico $\mathbb{Z}_p$. L es el SF de f sobre K.*

4.1.2. Extensiones cíclicas

Teorema 4.1.4 *Sea $f = x^n - 1$, donde L es el SF de f sobre K. $\xi \in L$, $\mathcal{G}(L:K)$ es cíclico y su orden divide a n. Tiene orden n si f es irreducible sobre $K(\xi)$.*

Teorema 4.1.5 *Sea K un cuerpo de característica cero, $f = x^n - 1$, y sea L es el SF de f sobre K donde $[L:K] = n$, entonces existe $a \in K$, tal que $x^n - a$ es irreducible en K y L es el SF de $x^n - a$, i.e. L está generado sobre K por una raíz simple de $x^n - a$.*

Teorema 4.1.6 ***Abel***. *Sea K un cuerpo de característica cero, $f = x^p - a$, con p primo e irreducible sobre K, entonces tiene un factor lineal $(x - c) \in K[x]$.*

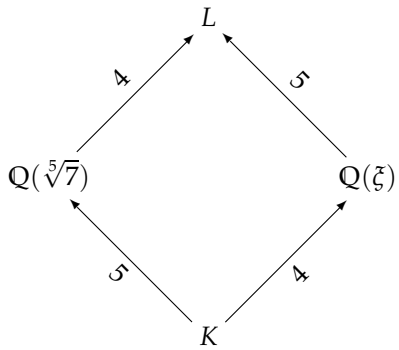
Ejemplo 4.1.2 *Sea $f = x^5 - 7$. Vemos que*

$$R_f = \left\{ \sqrt[5]{7} = v, v\xi, v\xi^2, v\xi^3, v\xi^4 \right\}$$

donde $\xi = e^{2\pi i/5}$. Por los teoremas anteriores vemos que

$$x^5 - 7 = \left(x - \sqrt[5]{7}\right)\left(x^4 + x^3 + x^2 + x + 1\right)$$

el diagrama es:



donde

$$[L:K] = \left[L : \mathbb{Q}\left(\sqrt[5]{7}\right)\right]\left[\mathbb{Q}\left(\sqrt[5]{7}\right) : K\right] = 4 \cdot 5 = 20 = |\mathcal{G}(L:K)|.$$

4.1.3. Grupos

La idea fundamental de toda esta teoría es la de subgrupo normal, i.e. de alguna forma los subgrupos normales son los únicos con los que es posible descomponer un grupo sin perder su estructura, i.e. si en la que G/H sigue teniendo estructura de grupo.

Definición 4.1.2 *Un grupo finito se dice solubel si para algún $n \geq 0$ existe una serie*

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \ldots\ldots \subseteq G_n = G$$

de subgrupos tales que

1. $G_i \lhd G_{i+1}$,
2. G_{i+1}/G_i *es cíclico* $\mathbb{Z}_p$, *donde* p *es primo.*

Teorema 4.1.7 *Todo grupo finito abeliano es soluble.*

Observación 4.1.3 $A_n \subset S_n$.

Teorema 4.1.8 S_n, $n \leq 4$ *es soluble, si* $n \geq 5$, *entonces NO.*

Teorema 4.1.9 A_n, $n \geq 5$ *es simple y por lo tanto NO es soluble.*

Observación 4.1.4 *Se dice que un grupo es simple si NO tiene subgrupos normales propios.*

Teorema 4.1.10 *Sea G un grupo soluble, entonces:*

1. *Todo subgrupo es soluble,*
2. *N es un suggrupo normal, entonces* G/N *es soluble*
3. $N \lhd G$.

Teorema 4.1.11 *Todo grupo de orden impar es soluble.*

4.1.4. Grupos y ecuaciones

Enunciamos el teorema fundamental de esta sección.

Teorema 4.1.12 *Sea* $f \in K[x]$,$char(K) = 0$, f *es soluble por radicales sii* $\mathcal{G}(f)$ *es soluble.*

Otro resultado práctico es el siguiente:

Teorema 4.1.13 *Sea* p *primo y* f *un polinomio de grado* p, *mónico e irreducible sobre* $\mathbb{Q}[x]$. *Si* f *tiene dos raíces complejas i.e. en* $\mathbb{C}\backslash\mathbb{R}$ *entonces* $\mathcal{G}(f) \simeq S_p$ *(i.e. es isomorfo al grupo simétrico* S_p*).*

Veamos un ejemplo.

Ejemplo 4.1.3 *Sea* $f = x^5 - 8x + 2$. *Vemos que sus raíces son*

$$(x + \frac{37068}{21313})(x + \frac{7334}{118931} + \frac{38943}{23078}i)(x + \frac{7334}{118931} - \frac{38943}{23078}i)(x - \frac{365364}{1460741})(x - \frac{27579}{17104})$$

por lo que su grupo es S_5.

Ejemplo 4.1.4 *El polinomio $x^5 - 10x + 5 \in \mathbb{Q}[x]$* ***no*** *es resoluble por radicales.*

VERDADERO *Basta probar que su grupo de Galois es isomorfo a S_5, y para ello es suficiente comprobar que es irreducible sobre $\mathbb{Q}$ y que tiene exactamente 3 raíces reales y dos complejas (conjugadas).*

Sea M el cuerpo de descomposición de $x^5 - 10x + 5$ sobre $\mathbb{Q}$. En primer lugar observamos que $x^5 - 10x + 5$, es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein ($p = 5$). Por lo tanto 5 divide al orden de $\mathcal{G}(M/\mathbb{Q})$, y como consecuencia este grupo contiene un elemento de orden 5. Como además $\mathcal{G}(M/\mathbb{Q}) \subset S_5$, el grupo contiene un $5-$ciclo.

Por otro lado por el Teorema de Bolzano $x^5 - 10x + 5$ tiene ceros en los intervalos $(-2, 0)$, $(0, 1)$ y $(1, 2)$, por lo que tiene al menos tres raíces reales. Como su derivada, $5x^4 - 10$, sólo tiene dos raíces reales, el polinomio no puede tener más de tres ceros reales. Por lo tanto $x^5 - 10x + 5$ tiene exactamente tres raíces reales y dos complejas conjugadas. La conjugación compleja es un automorfismo en $\mathcal{G}(M/\mathbb{Q})$ que intercambia las dos raíces complejas, y por tanto lo podemos identificar con una trasposición de S_5. Por lo tanto $\mathcal{G}(M/\mathbb{Q})$ es isomorfo a un subgrupo de S_5 que contiene un 5-ciclo y una trasposición. Pero S_5 se puede generar con un 5-ciclo y una trasposición, por lo que $\mathcal{G}(M/\mathbb{Q}) \simeq S_5$.

Como S_5 no es soluble (porque contiene un subgrupo que no lo es, A_5) la extensión $M/\mathbb{Q}$ no es radical y en consecuencia $x^5 - 10x + 5$ no es resoluble por radicales.

Teorema **4.1.14** *Sea el polinomio $p(x) = x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n \in K[x]$, donde L es SF, entonces $\mathcal{G}(L : K) \simeq S_n$, donde $L = K(r_1, ..., r_n)$, siendo r_i las raices de p.*