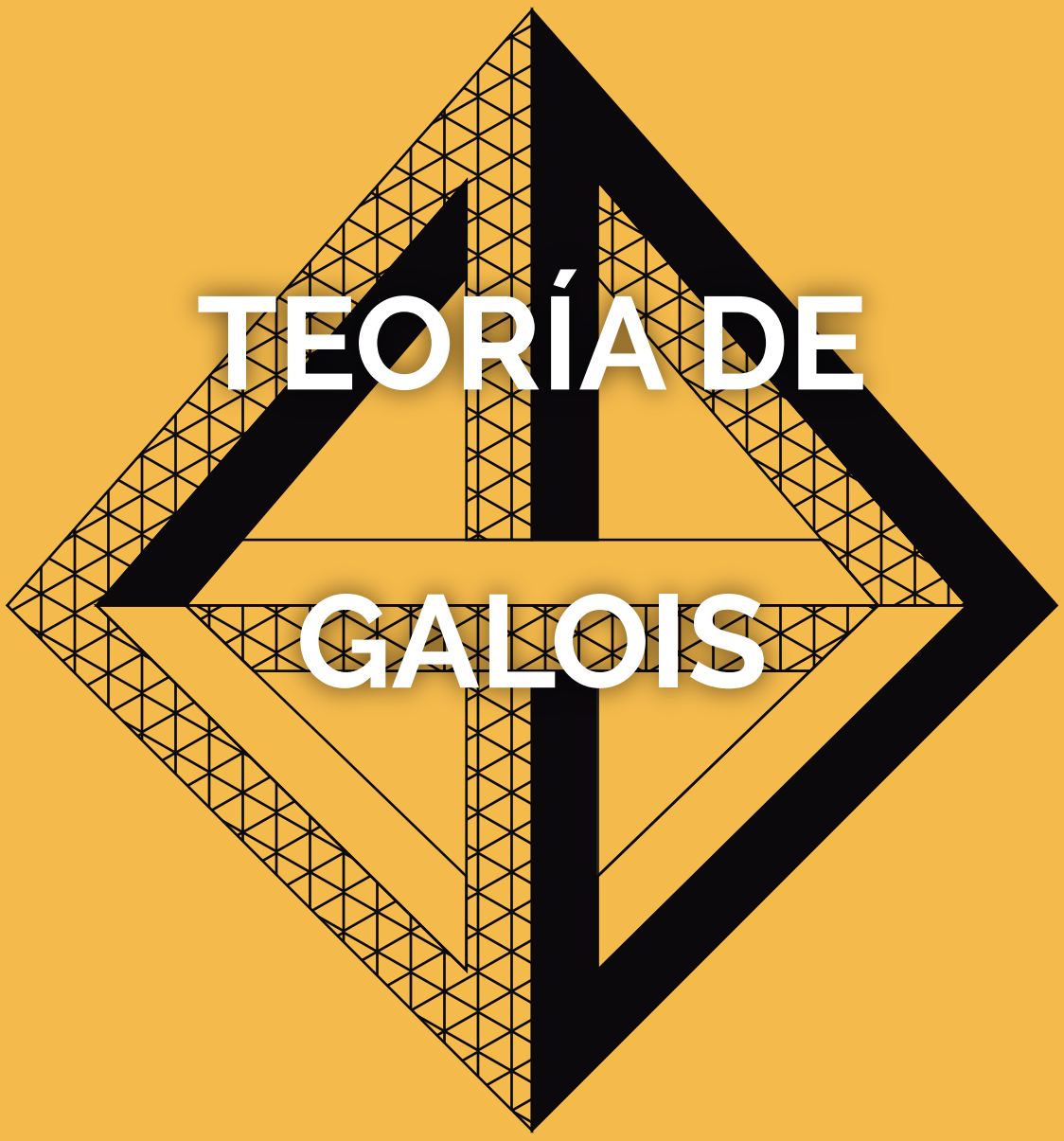

TEORÍA DE GALOIS

APUNTES DEL CURSO 2019-2020 IMPARTIDO POR CAROLINA VALLEJO

Rafael Sánchez

Revisión del 12 de noviembre de 2019 a las 13:25.

Índice general

Parte I

Primer parcial

Capítulo 1

Anillos, polinomios y cuerpos

1.1. Anillos

A lo largo de este curso se supondrán conocidos los contenidos de la asignatura *Estructuras Algebraicas*, se pueden encontrar unos apuntes de los mismos en: `https://github.com/knifecake/apuntes/raw/master/ea/apuntes-ea.pdf`.

Definición 1 (Anillo)**.** Un **anillo** es una terna $(A, +, \cdot)$ donde $+ : A \times A \to A$ es una operación a la que llamamos suma, $\cdot : A \times A \to A$ es otra operación a la que llamamos producto y se verifican las siguientes propiedades

1. El par $(A, +)$ es un grupo abeliano
2. El producto $\cdot$ es asociativo
3. Se cumplen las propiedades distributivas:

$$\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c \tag{1.1}$$
$$\forall a, b, c \in A,\ (a + b) \cdot c = a \cdot c + b \cdot c \tag{1.2}$$

Con la operación $+$ tenemos las siguientes propiedades

1. Asociatividad: $(a + b) + c = a + (b + c)$
2. Elemento neutro aditivo: $\exists! \mathbf{0} \in A \mid \mathbf{0} + a = a$
3. Elemento inverso aditivo: $\forall a \in A, \exists - a \in A \mid a + (-a) = \mathbf{0}$
4. Conmutatividad aditiva: $\forall a, b \in A,\ a + b = b + a$

Con la operación $\cdot$ tenemos las siguientes propiedades

1. Asociatividad: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. No siempre existe el neutro multiplicativo: $\mathbf{1} \in A \mid a \cdot 1 = 1 \cdot a = a$
3. No siempre el producto es conmutativo.
4. No siempre existe inverso multiplicativo: $a^{-1} \mid a \cdot a^{-1} = \mathbf{1}$
5. No siembre se da la conmutatividad multiplicativa: $a \cdot b = b \cdot a$

Proposición 1 (Producto con 0 en anillos)**.** $\forall a \in A,\ a \cdot \mathbf{0} = \mathbf{0}$

Demostración. $a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0} \implies \mathbf{0} = a \cdot \mathbf{0}$ ♢

Además, a lo largo de este curso vamos a referirnos únicamente a los anillos conmutativos con unidad (o unitario), que cumplen las siguientes definiciones.

Definición 2 (Anillo con unidad o anillo unitario)**.** Sea $(A, +, \cdot)$ un anillo. Decimos que es un anillo con unidad o un **anillo unitario** si tiene elemento neutro multiplicativo, es decir, si $\exists \mathbf{1} \in A \mid \forall a \in A, \mathbf{1}a = a\mathbf{1} = a$.

Definición 3 (Anillo conmutativo)**.** Sea $(A, +, \cdot)$ un anillo. Decimos que es un **anillo conmutativo** si se cumple que:

$$r \cdot s = s \cdot r, \ \forall r, s \in A$$

Ejemplo 1 (*Ejemplos de anillos*)

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma y producto usual verifican todas las definiciones de anillo, anillo conmutativo y anillo unitario.

Vamos a considerar además el concepto de anillo de polinomios:

Definición 4 (Anillo de polinomios)**.** Sea R un anillo, definimos el **anillo de polinomios** $R[x]$ como:

$$R[x] = \left\{ \sum_{i>0}^{n} a_i \cdot x^i \mid a_i \in R, \ n \in \mathbb{N} \right\}$$

Es fácil ver que $R[x]$ es un anillo pues la suma y el producto son transitivas y asociativas.

Observación. Vamos a considerar algunas definiciones y convenciones menores.

1. Sea $p \in R[x]$, p es un polinomio y escribimos:

   $$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

   Donde llamamos *coeficientes* del polinomio a los a_i.

2. Sea $p \in R[x] = \sum_{i>0} a_i x^i$, denominamos grado de p a:

   $$\delta(p) = \text{máx}\,\{i \mid a_i \neq 0\}$$

3. Sea $p \in R[x] = a_0 + a_1 x + \ldots + a_n x^n$, llamamos *coeficiente director* al coeficiente del término de mayor grado (a_n).

4. Sea $p \in R[x] = a_0 + a_1 x + \ldots + a_n x^n$, llamamos *termino independiente* al coeficiente libre (a_0).

5. Sea $p \in R[x]$ con todos los coeficientes nulos, entonces p es el *polinomio cero*.

   $$0 = \sum_{i>0} 0 \cdot x^n$$

   Por convención, $\delta(0) = -\infty$.

Definición 5 (Polinomio mónico)**.** Sea $R[x]$ un anillo de polinomios, decimos que $p \in R[x]$ es **mónico** si y sólo si su *término director* es 1.

Definición 6 (Divisor de cero)**.** Sea R un anillo, decimos que $r \in R$ es un **divisor de cero** si satisface:

$$\exists s \in R, \ s \neq 0 \ : \ r \cdot s = \mathbf{0}$$

Definición 7 (Unidad de un anillo)**.** Sea R un anillo, decimos que $r \in R$ es una **unidad** si satisface:

$$\exists s \in R \ : \ r \cdot s = \mathbf{1}$$

Decimos entonces que $r \in \mathcal{U}(R)$, con $\mathcal{U}(R) = \{a \mid a \text{ es una unidad}\}$

Definición 8 (Dominio de integridad)**.** Sea R un anillo, R es un **dominio de integridad** si no tiene divisores de $\mathbf{0}$.

Definición 9 (Cuerpo)**.** Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Diremos que A es un cuerpo si $A^\times = A \backslash \{\mathbf{0}\}$ es cerrado por la segunda operación (el *producto*).

Observación.

- R es un cuerpo si $\mathcal{U}(R) = R$.
- $\mathbf{1} \in \mathcal{U}(R)$, para todo R anillo unitario.

Proposición 2 (Cuerpo y dominio de integridad)**.** Sea R un cuerpo, entonces R es un dominio de integridad.

Demostración. Vamos a ver que R no tiene divisores de $\mathbf{0}$. Sea $r \in R^\times = R \backslash \{\mathbf{0}\}$, supongamos $\exists s \in R^\times$ tal que:

$$r \cdot s = 0$$

Como $r \in \mathcal{U}(R) = R^\times$ pues R es un cuerpo, entonces, $\exists t \in R$ tal que $t \cdot r = r \cdot t = \mathbf{1}$. Por tanto:

$$\mathbf{0} = t \cdot (r \cdot s) = (t \cdot r) \cdot s = \mathbf{1} \cdot s = s$$

Y $s = \mathbf{0}$ contradice la hipótesis. Concluimos con que $\nexists r, s \in R$ tal que $r \cdot s = \mathbf{0}$ ♢

Proposición 3 (Dominio de integridad en anillos de polinomios)**.** Sea R un anillo. Si R es un dominio de integridad, entonces $R[x]$ es un dominio de integridad.

Demostración. Sean $f, g \in R[x]^\times$, y a_m, b_k sus términos directores respectivamente. Como R es un dominio de integridad, $a_m \cdot b_k \neq \mathbf{0}$, que coincide con el término director de $f \cdot g$ y no es nulo. Por tanto, $R[x]$ es un dominio de integridad. ♢

Proposición 4 (Propiedad de cuerpo en anillos de polinomios)**.** $R[x]$ nunca es un cuerpo.

Demostración. Solo hay que comprobar que aunque $f(x) = x \in R[x]$, $f(x) \notin \mathcal{U}(R[x])$. Y por tanto $\mathcal{U}(R[x]) \neq R[x]$, lo que nos dice que $R[x]$ no es un cuerpo. ♢

Proposición 5 (Unidades en anillos de polinomios)**.** Sea R un anillo, si R es un dominio de integridad, entonces $\mathcal{U}(R) = \mathcal{U}(R[x])$.

Observación. Podemos definir anillos como *extensión* de otros, al igual que hicimos con los anillos de polinomios:

- $\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$, con $d \neq e^2, \ \forall e \in \mathbb{Z}$ es un anillo y un dominio de integridad, pero no es un cuerpo.
- $\mathbb{Q}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$, con $d \neq e^2, \ \forall e \in \mathbb{Z}$ es un cuerpo. Decimos que $\left\{1, \sqrt{d}\right\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}[\sqrt{d}]$, pues todos los elementos de $\mathbb{Q}[\sqrt{d}]$ se pueden expresar como combinación lineal de los elementos de la $\mathbb{Q}$-base.

Definición 10 (Subanillo)**.** Sea R un anillo, $S \subseteq R$, $\mathbf{1} \in S$. Decimos que S es un **subanillo** si:
- S es cerrado por suma y producto.
- Todo elemento tiene opuesto, es decir, $\forall a \in S, \exists b \in S \ : \ a + b = \mathbf{0}$.

Definición 11 (Subcuerpo)**.** Sean R un cuerpo, $S \subseteq R$. Decimos que S es un **subcuerpo** si:
- S es un subanillo de R
- Todo elemento no nulo tiene inverso, es decir, $\forall a \in S^\times, \exists b \in S^\times \ : \ a \cdot b = \mathbf{1}$

Ejemplo 2 (*Ejemplos de subanillos y subcuerpos*)

- $\mathbb{Z}$ *es subanillo de* $\mathbb{Q}$
- $\mathbb{Q}$ *es subcuerpo de* $\mathbb{R}$ *y* $\mathbb{C}$
- $\mathbb{Z}[\sqrt{d}]$ *es subanillo de* $\mathbb{Q}[\sqrt{d}]$

1.2. Ideales

Definición 12 (Ideal)**.** Sea R un anillo, e $I \subseteq S$. I es un **ideal** si:
1. $\forall a, b \in I, \ a - b \in I$
2. $\forall r \in R, \ \forall a \in I$ se satisface: $r \cdot a \in I$

Los ideales triviales son $\{\mathbf{0}\}$ y R.

Observación. Sea R un anillo, denotamos al ideal generado por $a \in R$ como $\langle a \rangle$

Proposición 6 (Ideal propio)**.** Sea R un anillo, I un ideal:

$$I \subsetneq R \iff \mathbf{1} \in I \iff I \cap \mathcal{U}(R) \neq \varnothing$$

Observación. Sea R un anillo, $I \leqslant R$ un ideal:

$$I \leqslant R \iff I \cap \mathcal{U}(R) = \varnothing$$

$$I = R \iff I \cap \mathcal{U}(R) \neq \varnothing$$

Proposición 7 (Ideales y cuerpos)**.** Sea R un cuerpo, y sea I un ideal de R (escribimos $I \leqslant R$), entonces $I = \{\mathbf{0}\}$ o $I = R$, (I es impropio).
El recíproco también es cierto.

Demostración.

- ($\Longrightarrow$)
$$R \text{ cuerpo} \implies \mathcal{U}(R) = R^\times \implies I = \mathcal{U}(R) \cup \{\mathbf{0}\} \text{ o trivialmente } I = \{\mathbf{0}\}$$
- ($\Longleftarrow$)
Sea $a \in R^\times$, $a \in \langle a \rangle \leqslant R$

  $\{\mathbf{0}\} \neq I = \langle a \rangle$, entonces $I = R \implies \exists u \in I \cap \mathcal{U}(R) \neq \varnothing \implies u \in \langle a \rangle \implies u = a \cdot r$, con $r \in R$

  y por tanto:
$$1 = u \cdot u^{-1} = a \cdot r \cdot u^{-1} \implies a \in \mathcal{U}(R) \implies R \text{ es un cuerpo}$$

♢

Ejemplo 3 (*Ejemplos de ideales*)

1. $n\mathbb{Z} \leqslant \mathbb{Z}$

2. $I = \{f \in \mathbb{Z}[x] \mid$ *el termino independiente de f es par*$\}$

Definición 13 (Ideal principal)**.** Sea R un anillo, $a \in R$ un elemento. El ideal generado por a:

$$\langle a \rangle = \{a \cdot r \mid r \in R\} = aR$$

se denomina **ideal principal** generado por a.

Proposición 8 (Propiedades de ideales)**.** Sea R un anillo e $I \leqslant R$ un ideal.

1. Sean $I, J \leqslant R$ ideales, entonces $I + J = \{a + b \mid a \in I,\ b \in J\} \leqslant R$ es un ideal.
2. Sea $\mathbf{a} \in \mathbb{R}^n$, entonces $I = \langle \mathbf{a} \rangle = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\} \leqslant R$ es un ideal.
3. ${}^{R}\!/_{I} = \{r + I \mid r \in R\}$ es un anillo.
4. (Teorema de correspondencia) Existe una biyección de la forma:

$$\begin{array}{ccc} \{J \leqslant R \mid I \subseteq J \subseteq R\} & \longrightarrow & \{{}^{J}\!/_{I} \leqslant {}^{R}\!/_{I}\} \\ J & \longmapsto & \{r + I \mid r \in J\} \end{array}$$

Observación. En particular, si en R todo ideal es principal e $I \leqslant R$, en ${}^{R}\!/_{I}$ todo ideal es principal.

Ejercicio (H1.5)**.** Sea n un número natural. Prueba que $\mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ es un cuerpo si y sólo si n es primo.

- ($\Longleftarrow$)

  n primo $\implies \forall k:\ 0 < k < n$ se cumple que $\text{mcd}(k, n) = 1$, y por Bezout:

  $$1 = ka + nb, \quad \text{con } a, b \in \mathbb{Z}$$

  Donde el término $nb \equiv 0$ en ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ y por tanto queda $1 = ka$, lo que quiere decir que k es el inverso de a en ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

- ($\Longrightarrow$)

  Partimos de que ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ es cuerpo, por la proposición 2 sabemos que ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ es un dominio de integridad. Supongamos n no primo, entonces $n = a \cdot b$, entonces:

  $$n \equiv \mathbf{0} (\text{mod } n) \implies \mathbf{0} = (a + n\mathbb{Z})(b + n\mathbb{Z})$$

  Pero es imposible, ya que a y b serían divisores de $\mathbf{0}$ pero estamos en un dominio de integridad. Por tanto, n es necesariamente primo.

Ejercicio (H1.12)**.** ¿Cuántos elementos tiene el anillo ${}^{\mathbb{Z}[i]}\!/_{\langle 2i \rangle}$?¿Se trata de un cuerpo?

Comenzamos escribiendo los conjuntos que forman parte del cociente:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

$$\langle 2i \rangle = \langle 2 \rangle = 2\mathbb{Z}[i] = \{2(a + bi) \mid a, b \in \mathbb{Z}\} = (2\mathbb{Z})[i] = \{a + bi \mid a, b \in 2\mathbb{Z}\}$$

El conjunto cociente es por tanto:

$${}^{\mathbb{Z}[i]}\!/_{\langle 2i \rangle} = {}^{\mathbb{Z}[i]}\!/_{2\mathbb{Z}[i]} = \{a + bi + 2\mathbb{Z}[i] \mid a, b \in \mathbb{Z}\}$$

Donde se tiene que:

$a+bi+2\mathbb{Z}[i] = a_1+b_1 i+2\mathbb{Z}[i] \iff a-a_1 \in 2\mathbb{Z}$ y $b-b_1 \in 2\mathbb{Z} \iff \{a + bi + 2\mathbb{Z}[i] \mid a, b \in \{0, 1\}\} = \{0, 1, i, 1 + i\}$

De esta forma vemos que el anillo tiene 4 elementos y además no es un cuerpo ya que i no tiene inverso.

Definición 14 (Ideal primo)**.** Sea R un anillo e $I \leqslant R$ un ideal, diremos que I es un **ideal primo** si:

$$a \cdot b \in I \implies a \in I \text{ ó } b \in I$$

Definición 15 (Ideal maximal)**.** Sea R un anillo e $I \leqslant R$ un ideal, diremos que I es un **ideal maximal** si:

$$I \subseteq J \leqslant R \implies J = I \text{ ó } J = R$$

Teorema 9 (Cociente de ideales primos y maximales)**.** Sea R un anillo, $I \leqslant R$ un ideal:

1. I es primo $\iff {}^{R}/_{I}$ es un dominio de integridad.
2. I es maximal $\iff {}^{R}/_{I}$ es un cuerpo.
3. I ideal maximal $\implies I$ ideal primo.

Demostración.

1. Se deja como ejercicio. Es directa usando definiciones.
2. I es maximal $\iff {}^{R}/_{I}$ no tiene ideales propios (por el teorema de correspondencia 4). Y ya sabemos que ${}^{R}/_{I}$ no tiene ideales propios $\iff {}^{R}/_{I}$ es un cuerpo.
3. Se sique de los apartados anteriores junto a la proposición 2 que nos dice que un cuerpo es un dominio de integridad.

♢

1.3. Homomorfismos

Definición 16 (Homomorfismo de anillos)**.** Sean R, S anillos, $\varphi : R \to S$ es un **homomorfismo de anillos** si:

1. φ es homomorfismo de grupos, es decir, $\varphi(0) = 0$ y $\varphi(a - b) = \varphi(a) - \varphi(b)$.
2. $\varphi(1) = 1$.
3. $\varphi(ab) = \varphi(a)\varphi(b)$.

Observación.

- $\ker \varphi = \{a \in R \mid \varphi(a) = 0\} \leqslant R$.
- $\varphi(R) \subseteq S$ es un subanillo. (No es ideal en general).
- φ sobreyectiva, es decir, φ es un epimorfismo $\iff \varphi(R) = S$.

Observación. Si R y S son cuerpos y $\varphi : R \to S$ es un homomorfismo de anillos, llamaremos a φ homomorfismo de cuerpos. Además φ es inyectivo pues:

$$1 \notin \ker \varphi \leqslant R \text{ cuerpo} \implies \ker \varphi = 0$$

Ejemplo 4 (*Proyección canónica*)

Sea R un anillo, $I \leqslant R$ un ideal, es fácil ver que $\pi : R \to {}^{R}/_{I}$; $r \mapsto r + I$ es un epimorfismo de anillos con $\ker \pi = I$.

Observación.

$${}^{R}/_{\ker \varphi} = {}^{R}/_{I}$$

Teorema 10 (Primer teorema de isomorfía)**.** Sea $\varphi : R \to S$ un homomorfismo de anillos, se tiene que:

$$\begin{aligned} \overline{\varphi} : {}^{R}\!/_{\ker \varphi} &\longrightarrow \varphi(S) \\ r + \ker\varphi &\longmapsto \overline{\varphi}(r + \ker\varphi) = \varphi(r) \end{aligned}$$

es un isomorfismo de anillos.

Demostración. Se deja como ejercicio. ♢

Observación. Sea π la proyección canónica, $\overline{\pi} = id_{R/I}$

Ejercicio (H1.14)**.** Demuestra que si $\varphi : R \to S$ es un homomorfismo de anillos y $a \in \mathcal{U}(R)$, entonces $\varphi(a) \in \mathcal{U}(S)$. ¿Es cierto el recíproco?.

Si $a \in \mathcal{U}(R)$, tntonces $\exists b \in R$ tal que $\mathbf{1} = a \cdot b$. Por tanto:

$$\mathbf{1} = \varphi(\mathbf{1}) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \implies \varphi(a) \in \mathcal{U}(S)$$

El recíproco solo es cierto si φ es un isomorfismo, pero en general no. Como contraejemplo consideramos el homomorfismo identidad $\iota : \mathbb{Z} \to \mathbb{Q};\ a \mapsto a$. Es fácil ver que es un homomorfismo de anillos, sin embargo: $\iota(2) = (2)$ pero $\iota(2) \in \mathcal{U}(\mathbb{Q})$ y $2 \notin \mathcal{U}(\mathbb{Z})$.

Ejercicio (H1.16)**.** Demuestra que:

1. No existe ningún homomorfismo de anillos $\varphi : \mathbb{Q} \to \mathbb{Z}_p$ para $p \in \mathbb{Z}$ primo.
2. No existe ningún homomorfismo de anillos $\varphi : \mathbb{R} \to \mathbb{Q}$.

Solución:

1. Sea $\varphi : \mathbb{Q} \to \mathbb{Z}_p;\ \mathbf{1} \mapsto \mathbf{1} + p\mathbb{Z}$.

   $$\varphi(p) = \varphi\left(\sum_1^p 1\right) = \sum_1^p (\mathbf{1} + p\mathbb{Z}) = p + p\mathbb{Z} = 0.$$

   y como $p \in \mathcal{U}(\mathbb{Q})$, es imposible que la imagen de una unidad no sea otra por medio de un homomorfismo, por tanto, dicho homomorfismo no existe.

2. Sea $\varphi : \mathbb{R} \to \mathbb{Q};\ \sqrt{2} \mapsto a$

   $$2 = \varphi(1+1) = \varphi(2) = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2 = a^2,\ a \in \mathbb{Q}$$

   que es una contradicción pues no existe dicho a, con lo que no existe el homomorfismo.

Ejercicio (H1.21)**.** Fijado un entero $n \in \mathbb{Z}$ con $n \geqslant 2$, demuestra que el anillo cociente ${}^{\mathbb{Z}[x]}\!/_{n\mathbb{Z}[x]}$ es isomorfo a $\mathbb{Z}_n[x]$. Conclute que el ideal $n\mathbb{Z}[x]$ es primo si y sólo si n es un número primo.

Vamos a dar una guía de como proceder con el ejercicio:

$$\text{Sea } \varphi : \mathbb{Z}[x] \to \mathbb{Z}_n[x];\ (a_0 + \ldots + a_n x^n) \mapsto (\overline{a_0} + \ldots + \overline{a_n} x^n)$$

donde $\overline{a_i} = a_i + n\mathbb{Z} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

- Comprobar que φ es un homomorfismo de anillos.
- Comprobar que φ es sobreyectiva.
- Ver que $\ker\varphi = n\mathbb{Z}[x]$.
- Aplicar el teorema de isomorfía.

Ejemplo 5 (*Homomorfismo de evaluación*)

Sea R un anillo, $a \in R$.

$$\begin{aligned} \mathcal{E}_a : R[x] &\longleftarrow R \\ f(x) &\longmapsto f(a) \end{aligned}$$

es un homomorfismo de anillos sobreyectivo.

Observación. Si $R = K$ es un cuerpo:

$$K[x] \Big/ \ker \mathcal{E}_a \simeq K \implies \ker \mathcal{E}_a \text{ es maximal.}$$

1.4. Anillos de polinomios

Proposición 11 (Algoritmo de la división)**.** Sea R un anillo, $f, g \in R[x]^\times$ polinomios con coeficientes en R. Si el coeficiente director de g es una unidad de R, entonces $\exists d, r \in R[x]$ únicos tales que:

$$f = g \cdot d + r \text{ con } \delta(r) < \delta(g)$$

Diremos que $g \mid f$ si $r = \mathbf{0}$.

Definición 17 (Raíz de un polinomio)**.** Sea R un anillo, $f \in R[x]^\times$ un polinomio, decimos que $a \in R$ es una **raíz** de f si $\mathcal{E}_a(f) = f(a) = \mathbf{0}$

Corolario 1 (Ruffini)**.** Sea R un anillo, $f \in R[x]^\times$ un polinomio:

$$a \text{ es raíz de } f \iff f(x) = (x - a) \cdot g(x)$$

Demostración.

- ($\Longleftarrow$)

$$\mathcal{E}_a(f) = \mathcal{E}_a(x - a) \cdot \mathcal{E}_a(g) = \mathbf{0}$$

- ($\Longrightarrow$)

$$f(x) = (x - a) \cdot d(x) + r(x);\ \delta(r) \leqslant \delta(x - a) \implies r \in R;\ f(a) = r = 0 \implies g(x) = d(x)$$

♢

Ejemplo 6 (*Uso de Ruffini*)

Sea $f(x) = x^2 + x + 1$, $f(x) \in \mathbb{Z}_3[x]$.
Es fácil ver que $f(1) = 0$, según Ruffini (corolario 1) $(x-1) \mid f$. Y es cierto, de hecho: $f(x) = (x-1)(x-1)$.

Teorema 12 (Raíces y dominio de integridad)**.** Sea R un dominio de integridad, $f \in R[x]^\times$ un polinomio y $\alpha_1, \ldots, \alpha_n$ raíces distintas de f, entonces $n \leqslant \delta(f)$.

Demostración. Vamos a probarlo por inducción sobre $\delta(f)$

- Caso base: $\delta(f) = 1$. Entonces $f(x) = ax + b$. Sea α_1 raíz de $f(x)$, entonces $a\alpha_1 = -b$. Si α_2 es raíz de f, entonces $a\alpha_2 = -b \implies a\alpha_1 = a\alpha_2 \implies a(\alpha_1 - \alpha_2) = 0$ y como $a \neq 0$ y R es dominio de integridad $\alpha_1 - \alpha_2 = 0 \implies \alpha_1 = \alpha_2$
- $\delta(f) = m > 1$. Sea α_1 raíz de f, por Ruffini $f(x) = (x - \alpha_1)d(x)$. Por hipótesis, $\alpha_2 \ldots \alpha_n$ son raíces de f distintas de α_1, por lo que necesariamente $d(\alpha_i) = 0\ \forall i \in [2, n]$. Por la hipótesis de inducción $n - 1 \leqslant \delta(d) = \delta(f) - 1 \implies n \leqslant \delta(f)$

♢

Observación. La hipótesis de que R sea un dominio integridad es necesaria. Se puede comprobar que en $\mathbb{Z}_8[x]$, el polinomio $f(x) = x^2 - 1$ con $\delta(f) = 2$, tiene 4 raíces: $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Sin embargo, no supondrá un problema a lo largo del curso ya que trabajaremos con cuerpos.

Ejercicio (H1.27)**.** Demuestra que si K es un cuerpo finito y $f, g \in K[x]$ tales que $f(a) = g(a)$ para todo $a \in K$, entonces $f = g$. ¿Qué ocurre si K es finito?.

Supongamos $h = f - g \in K[x]$. Entonces $h(a) = 0\ \forall a \in K$ con $K[x]$ un cuerpo infinito implica necesariamente que $h = 0$ y por tanto $f = g$.
Si K es finito, por ejemplo $K = \mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ con p un primo, consideramos el polinomio $f(x) = x^p - x$. En este caso $f(x) \neq 0$ pero se anula en todo elemento de $\mathbb{Z}_p$ ya que $a^p \equiv a \mod p$ por el pequeño teorema de Fermat.

Teorema 13 (Pequeño teorema de Fermat)**.** Si p es un número primo, entonces, para cada número natural a, con $a > 0$, $a^p \equiv a \mod p$.

Teorema 14 (Ideales principales)**.** Sea K un cuerpo, $I \leqslant K[x]$ un ideal tal que $I \neq \{0\}$, entonces existe un $p \in K[x]$ tal que $I = \langle p \rangle$.

Demostración. Sea $p \in I$ con el menor grado finito posible, es decir, sea $0 \neq g \in I \implies \delta(g) \geqslant \delta(p)\ \forall g \in I$. Entonces por el algoritmo de la division, para $f \in I$, $f = pd + r$, con $d, r \in K[x]$ y $\delta(r) \leqslant \delta(p) \implies r \in I$. Por la elección de p, la única opción es que $r = 0$ entonces $f = pd \implies f \in \langle p \rangle$. ♢

Ejercicio (H1.25)**.** Hallar un generador de $I = \langle x^3 + 1, x^2 + 1 \rangle$ en $\mathbb{Z}_2[x]$.

Basta observar que en $\mathbb{Z}_2[x]$, $(x^2+1) = (x+1)^2$ y $(x^3+1) = (x+1)\cdot(x^2+x+1)$, por tanto, $I = \langle x+1 \rangle$.

Definición 18 (Dominio de ideales principales)**.** Un anillo R en el que todo ideal es principal y es un dominio de integridad se llama **dominio de ideales principales** (o DIP para abreviar).

Definición 19 (Elemento irreducible)**.** Sea R un anillo y $a \neq 0 \in \mathcal{U}(R)$, decimos que a es **irreducible** si $a = b \cdot c \implies$ tiene que ocurrir que $b \in \mathcal{U}(R)$ o que $c \in \mathcal{U}(R)$

Teorema 15 (Irreducibilidad en DIP)**.** Sea R un dominio de ideales principales, entonces:

$$a \in R \text{ irreducible} \iff \langle a \rangle \text{ es maximal.}$$

Demostración.

$\implies$ Sea $\langle a \rangle \subseteq J \leqslant R$, con $J = \langle b \rangle$. Si $J \neq R$ entonces $b \notin \mathcal{U}(R)$. Falta ver que $\langle a \rangle = \langle b \rangle$. Como $\langle a \rangle \subseteq \langle b \rangle$, $a = b \cdot c$ con $c \in R$. Además como $b \notin \mathcal{U}(R)$ y a es irreducible, entonces $c \in \mathcal{U}(R)$ y con ello $\langle a \rangle = \langle bc \rangle = \langle b \rangle$.

$\impliedby$ Sabemos que $\langle a \rangle \leqslant R$ es maximal. Sea $a = bc$ con $b, c \in R$, entonces:

$$\langle a \rangle \subseteq \langle b \rangle \leqslant R \implies \text{ o bien } (\langle a \rangle = \langle b \rangle \implies c \in \mathcal{U}(R)) \text{ o bien } (\langle b \rangle = R \implies b \in \mathcal{U}(R))$$

y por tanto a es irreducible.

♢

Corolario 2. Sea $0 \neq f \in K[x]$, con K un cuerpo.

$$f \text{ es irreducible } \iff K[x]\Big/\langle f\rangle \text{ es un cuerpo.}$$

Demostración. La prueba es directa sabiendo que $K[x]$ es un DIP, el teorema anterior y el teorema 9. ♢

Observación. $f \in K[x]$ es irreducible si $\delta(f) > 1$ y $f \neq gh$ con $g, h \in K[x]$, $\delta(g) < \delta(f)$ y $\delta(h) < \delta(f)$.

Observación. En $K[x]$ los polinomios de grado 1 son irreducibles por definición. Los de grado 2 y grado 3 son irreducibles $\iff$ no tienen raíces en K (por Ruffini).

Corolario 3 (Euclides)**.** Sea $0 \neq f \in K[x]$ irreducible, si $f \mid gh$ entonces $f \mid g$ o $f \mid h$.

Demostración.

$$f \text{ irreducible} \implies \langle f\rangle \text{ es maximal} \implies \langle f\rangle \text{ es primo.}$$

Por definición de ideal primo:

$$f \mid gh \iff gh \in \langle f\rangle \iff g \in \langle f\rangle \vee h \in \langle f\rangle$$

♢

Ejemplo 7

Este corolario nos permite construir cuerpos finitos distintos a los $\mathbb{F}_p$.
$E = \mathbb{F}_2[x]\Big/\langle x^2 + x + 1\rangle$ es un cuerpo. Veamos su caracterización.

- *Primero comprobamos que $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ es irreducible. Como es un polinomio de grado 2, es irreducible si no tiene raíces en $\mathbb{F}_2$, y es cierto ya que $f(0) = f(1) = 1$.*
- *Los elementos de E son de la forma: $g + \langle f\rangle$, y además $g + \langle f\rangle \neq 0$ en $E \iff g \notin \langle f\rangle$.*
  $g = fq + r$, $\delta(r) < \delta(f) = 2$ y como g no es múltiplo, $0 \leqslant \delta(r) \leqslant 2$.
  $g + \langle f\rangle = r + fq + \langle f\rangle = r + \langle f\rangle$. Por tanto, todo elemento en E tiene un representante con grado menor a 2.

Y por tanto:

$$E = \{a + bx + \langle f\rangle \mid a, b \in \mathbb{F}_2\} \implies E = \{0, 1, x, x + 1\}$$

Teorema 16 (Máximo común divisor)**.** Sean K cuerpo, $0 \neq f, g \in K[x]$ polinomios, existe un único polinomio mónico $d \in K[x]$ tal que:

$$\langle f\rangle + \langle g\rangle = \langle d\rangle \text{ es decir, } \exists a, b \in K[x] : \ d = af + bg$$

Además, $d \mid f$ y $d \mid g$ y si $\exists$: $e \mid f$ y $e \mid g \implies e \mid d$ en $K[x]$. Denotamos al polinomio d por $mcd_K(f, g)$.

Demostración. Se deja como ejercicio. ♢

Proposición 17 (Máximo común divisor en subcuerpos)**.** Sean $E, K \subseteq E$ cuerpos, y $0 \neq f, g \in K[x]$ polinomios.

$$mcd_K(f, g) = mcd_E(f, g)$$

Demostración. Sea $d = mcd_K(f, g)$, $e = mcd_E(f, g)$. Entonces, $d = af + bg$ en $K[x] \subseteq E[x] \implies e \mid d$ en $E[x]$. Como $d \mid f$ y $d \mid g$ en $K[x]$ (y en particular también en $E[x]$), entonces $d \mid e$ en $E[x]$. Por tanto:

$$(d \mid e) \wedge (e \mid d) \wedge \text{ e, d mónicos} \implies e = d \in K[x]$$

♢

Corolario 4. Sea $0 \neq f, g \in K[x]$ con f irreducible.

1. $mcd(f,g) = 1$ o $f \mid g$.
2. Si tenemos $K \subseteq E$, y f, g tienen una raíz común en E, entonces $f \mid g$ en $K[x]$.

Demostración.

1. Si $d = mcd(f,g) \neq 1 \implies \delta(d) > 1 \implies f = ad \implies d = a \cdot f,\ a \in K^\times$. Sea $b \in K[x]$, $g = b \cdot d = baf \implies f \mid g$.
2. Sea $a \in E$ la raíz común, por Ruffini $(x-a) \mid f, g$ en $E[x] \implies mcd_E(f,g) = mcd_K(f,g) > \implies f \mid g$.

♢

Corolario 5 (Descripción de $\mathcal{U}(K[x]/\langle f \rangle)$)**.** Sea $0 \neq f \in K[x]$, $R = K[x]/\langle f \rangle$. Entonces:

$$\bar{g} = g + \langle f \rangle \in \mathcal{U}(R) \iff mcd(f,g) = 1$$

Es decir, $\exists a, b \in K[x]$ tal que $1 = af + bg$ y por tanto $(g + \langle f \rangle)^{-1} = b + \langle g \rangle$.

Ejercicio (H1.24)**.** Sea $p \in \mathbb{Q}[x]$ dado por $p(x) = (x^2+1)(x^4+2x+2)$. Escribimos $R = \mathbb{Q}[x]/\langle p \rangle$ y $\bar{f} = f + \langle p \rangle$.

1. Describe los ideales en R. ¿Es R un cuerpo?.
2. Decide justificadamente si $\bar{x}$ y $\overline{x+1}$ son divisores de cero en R.
3. Decide si $\bar{x}$ y $\overline{x+1}$ son elementos invertibles en R y, en caso afirmativo, encuentra sus inversos.

El primer apartado se resuelve por el teorema de correspondencia.
En el segundo apartado tenemos que ver que $mcd(x,p) = 1 = mcd(x+1,p)$. Con ello vemos que $\bar{x}$ y $\overline{x+1} \in \mathcal{U}(R)$ y por tanto no pueden ser divisores de cero.
En el tercer apartado faltaría calcular los inversos con la identidad de Bezout.

Proposición 18 (Cociente de cuerpo e ideal de polinomio irreducible)**.** Sea K un cuerpo, $f \in K[x]$ irreducible, $K[x]/\langle f \rangle$ es un cuerpo.

Demostración. Ver el corolario 2. ♢

Teorema 19 (Factorización única)**.** Sea $K[x]$ un dominio de factorización única (DFU), sea $0 \neq f \in K[x]$, de la forma:

$$f(x) = a p_1(x) \cdot \cdots \cdot p_r(x),\ a \in K^\times,\ p_i \text{ irreducibles mónicos no necesariamente distintos}$$

entonces la expresión es única (salvo el orden de los factores).

Demostración. Se deja como ejercicio. ♢

1.5. Criterios de irreducibilidad

Lema 20 (de Gauss)**.** Sea $f(x) \in \mathbb{Z}[x]$ un polinomio con $\delta(f) \geqslant 2$, entonces:

$$f(x) \text{ irreducible en } \mathbb{Z}[x] \implies f(x) \text{ irreducible en } \mathbb{Q}(x)$$

Demostración. Se deja como ejercicio. ♢

Lema 21 (Reducción módulo p)**.** Sea f un polinomio entero mónico, y $\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$; $\sum a_j x^d \mapsto \sum \overline{a_j} x^d$. Si existe algún primo p de forma que $\varphi_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible en $\mathbb{Z}[x]$.

Demostración. Se deja como ejercicio. ♢

Ejercicio (H1.34 (c))**.** Demuestra que $f(x) = x^3 + x + 1$ es irreducible en $\mathbb{Q}[x]$.

Usamos reducción módulo p con $p = 2$.

$$f(0) = 1,\ f(1) = 1$$

Como es un polinomio de grado 3 sin raíces, es irreducible en $\mathbb{Z}_2[x]$ y por tanto es reducible en $\mathbb{Q}[x]$.

Teorema 22 (Criterio de Einsestein)**.** Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$. Si existe un primo p tal que:
1. $p \nmid a_n$.
2. $p^2 \nmid a_0$.
3. $p \mid a_i,\ \forall i \in \{0, \ldots, n-1\}$.

Entonces f es irreducible en $\mathbb{Q}[x]$.

Demostración. Se deja como ejercicio. ♢

Proposición 23 (Raíces racionales de un polinomio)**.** Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$. Si $\frac{r}{s} \in \mathbb{Q}$ con $mcd(r, s) = 1$ es una raíz de f, entonces: $s \mid a_n$ y $r \mid a_0$. En particular, si $f \in \mathbb{Z}[x]$ es mónico, las raíces racionales están contenidas en los enteros.

Demostración.

$$\begin{aligned} 0 = f(\frac{r}{s}) &= a_0 + a_1\frac{r}{s} + \ldots + a_n\frac{r^n}{s^n} \\ 0 &= a_0 s^n + a_1 r s^{n-1} + \ldots + a_n r^n \\ -a_0 s^n &= a_1 r s^{n-1} + \ldots + a_n r^n = r(s^{n-1}a_1 + \ldots + a_n r^{n-1}) \implies r \mid a_0 s^n \implies r \mid a_0 \\ -a_n r^n &= s(a_0 s^{n-1} + \ldots + a_{n-1} r^{n-1}) \implies s \mid a_n r^n \implies s \mid a_n \end{aligned}$$

♢

Ejemplo 8 (*Irreducibilidad cuando fallan otros criterios*)

¿Es $x^3 + x + 6$ irreducible en $\mathbb{Q}[x]$?.

Si intentamos comprobarlo con el criterio de Einsestein o por reducción módulo p no llegamos a nada. Podemos utilizar la proposición 23 para hallar que las únicas raíces racionales del polinomio son los divisores de 6, es decir, $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ y si evaluamos el polinomio en los posibles valores ninguno resulta 0. Por tanto, es un polinomio de grado 3 sin raíces y entonces es irreducible en $\mathbb{Q}[x]$.

Lema 24 (Irreducibilidad evaluando en $x + a$)**.** Sea $f \in K[x]$ (K cuerpo), $a \in K$.

$$f(x) \text{ irreducible} \iff f(x + a) \text{ irreducible}$$

Demostración. La demostración se sigue de demostrar que $\varphi_a : K[x] \to K[x]$; $f(x) \mapsto f(x + a)$ es un isomorfismo de anillos (cuerpos). ♢

Teorema 25 (Irreducibilidad de polinomios ciclotómicos)**.** Sea p primo, $\Phi_p(x) = x^{p-1} + \ldots + x + 1$ es irreducible en $\mathbb{Q}[x]$.

Demostración. Partimos de $(x-1)\Phi_p(x) = x^p - 1$. Aplicamos el lema 24 con $a = 1$. Tenemos por tanto: $x\Phi(x+1) = (x+1)^p - 1$. Desarrollando con el binomio de newton llegamos a la expresión:

$$\Phi(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-1}$$

Ahora aplicamos Einsestein para el primo p, donde vemos que $p \mid \binom{p}{i}$ y $p^2 \nmid \binom{p}{p-1} = p$, por lo que $\Phi_p(x+1)$ es irreducible y también lo es $\Phi_p(x)$. ♢

1.5.1. Raices múltiples e irreducibilidad

Definición 20 (Raíz múltiple)**.** Sea $0 \neq f(x) \in K[x]$ un polinomio, $a \in K$ un raíz de f, existe un $m \in \mathbb{N} > 0$ tal que $f(x) = (x-a)^m g(x)$ con $g(a) \neq 0$ aplicando Ruffini y siendo $K[x]$ un DFU.
Decimos que a es **raíz múltiple** s i $m > 1$.

Definición 21 (Derivada formal)**.** Sea $f(x) = a_0 + a_1x + \ldots a_nx^n \in K[x]\backslash K$. Se define $f'(x) = a_1 + 2a_2x + \ldots na_nx^{n-1} \in K[x]$ como **derivada formal**. Si $f \in K$, $f'(x) = 0$.

Proposición 26 (Propiedades de derivada formal)**.** Sean $f, g \in K[x]$

1. $(f+g)' = f' + g'$; $(af)' = a \cdot f'$, $\forall a \in K$.
2. $(fg)' = f' \cdot g + f \cdot g'$.
3. Si $f(x) = (x-a)^m$, $m \geqslant 1$ entonces $f'(x) = m(x-a)^{m-1}$.

Proposición 27 (Raíz de derivadas)**.** Sean $K \subseteq E$ un subcuerpo, $f(x), f'(x) \in K[x]$ polinomios, $a \in E$ una raíz múltiple (con multiplicidad m) de f, entonces:

$$f(a) = f'(a) = 0 \iff m > 1$$

Demostración. En ambos supuestos: $f(x) = (x-a)^m g(x)$, con $m \geqslant 1$, $g(a) = 0$ y $f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m \cdot g'(x)$.

$\implies$ $m > 1 \implies m - 1 \geqslant 1$ y $(f(a) = f'(a) = 0)$.

$\impliedby$ $0 = f'(a) = m \cdot 0^{m-1} \cdot g(a) \implies m > 1$. $(g(a) \neq 0)$. Si tuvieramos $m = 1$ entonces $f'(x) = g(x) + (x-a)g'(x)$, con lo que llegaríamos a $0 = f'(a) = g(a) \neq 0$ lo que es imposible y la desigualdad es necesariamente estricta.

♢

Teorema 28 (Irreducibilidad y raíces múltiples)**.** Sea $K \subseteq E$ un subcuerpo, $f(x) \in K[x]$ un polinomio con $f'(x) \neq 0$.
1. $mcd(f, f') = 1 \implies f$ no tiene raíces múltiples en E.
2. Si f es irreducible, entonces f no tiene raíces múltiples en E.

Demostración.

1. $mcd(f, f') = 1 \implies \exists g, h \in K[x] : \ 1 = fg + hf'$. Por reducción al absurdo, si supones que un cierto $a \in E$ es raíz múltiple de f, entonces $f(a) = f'(a) = 0$ y llegaríamos a $1 = 0$.
2. Como $f, f' \neq 0$ y f es irreducible, por el lema de Euclides o bien son coprimos o bien $f \mid f'$. Si $f \mid f'$, entonces $\delta(f) < \delta(f')$ pero $\delta(f') = \delta(f) - 1$ y llegamos a una contradicción, por tanto $mcd(f, f') = 1$ ya que son coprimos.

♢

Ejercicio (H1.30 (parte))**.** Enumera los polinomios irreducibles en $\mathbb{F}_2$ de grado 1, 2, y 3.

$\delta(f) = 1$ $f(x) = x$, $f(x) = x + 1$.

$\delta(f) = 2$ $f(x) = x^2 + x + 1$.

$\delta(f) = 3$ $f(x) = x^3 + x^2 + 1$, $f(x) = x^3 + x + 1$.

Ejercicio (H1.35)**.** Discute la irreducibilidad de $f(x) = x^5 + 11x^2 + 15$ en $\mathbb{Q}[x]$.

Vamos a ver que es irreducible por medio de reducción módulo p con $p = 2$. $\varphi_2(f) = f_2(x) = x^5 + x^2 + 1$.

1. Vemos que no tiene raíces: $f_2(0) = 1$, $f_2(1) = 1$. Por tanto, no existe una forma de factorizarlo en un producto de dos polinomios de grado 1 y grado 4.
2. Faltaría ver que no se puede factorizar en un producto de polinomios de grado 2 y grado 3. Si fuera posible: $f_2(x) = g(x) \cdot h(x)$. Además, g y h han de ser irreducibles ya que no existe un polinomio de grado 1 en sus factores. Con el ejercicio anterior, basta ver que $f_2(x)$ no es el resultado de multiplicar los posibles polinomios irreducibles de grados 2 y 3.

$$(x^2 + x + 1)(x^3 + x^2 + 1) \neq f_2(x) \neq (x^2 + x + 1)(x^3 + x + 1)$$

Ejercicio (H1.39)**.** Factoriza $x^4 - 1$ como producto de irreducibles mónicos en: $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{F}_2[x]$ y $\mathbb{F}_3[x]$.

- $\mathbb{R}[x]$ y $\mathbb{Q}[x]$: $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$.
- $\mathbb{C}[x]$: $x^4 - 1 = (x - 1)(x + 1)(x - i)(x + i)$.
- $\mathbb{F}_2[x]$: Como $f'(x) = 0$, 1 es una raíz con multiplicidad 4, y por tanto $x^4 - 1 = (x - 1)^4$.
- $\mathbb{F}_3[x]$: $f'(x) = 4x = x \in \mathbb{F}_3[x] \implies$ las raíces son simples. Se pueden comprobar a mano y obtenemos $x^4 - 1 = (x - 1)(x - 2)(x^2 + 1)$.

1.6. Cuerpos

Definición 22 (Cuerpo primo)**.** Sea K un cuerpo, $\mathcal{A} = \{L \subseteq K \text{ subcuerpos}\}$. Sea $F = \bigcap_{L \in \mathcal{A}} L$, es un subcuerpo de K (se puede comprobar). Llamamos a F el **cuerpo primo** de K, y tiene la característica de ser el menor subcuerpo contenido en K, es decir, si $E \subseteq K$ y $E \subseteq F$, entonces $E = F$.

Teorema 29 (Isomorfías del cuerpo primo)**.** Sea K un cuerpo y F su cuerpo primo, entonces F es isomorfo a:

- $\mathbb{Q} \iff \sum_1^n \mathbf{1} \neq 0 \forall n \in \mathbb{Z}^\times$
- $\mathbb{F}_p \iff \sum_1^n \mathbf{1} = \mathbf{0} \iff p \mid n$ para algún primo p.

Observación. Vamos a abreviar $\sum_1^n \mathbf{1}$ por $n\mathbf{1}$, donde $\mathbf{1} \in F$ y $n \in \mathbb{Z}^\times$.

Demostración. Consideramos el homomorfismo $\alpha : \mathbb{Z} \to F$; $n \mapsto n\mathbf{1}$. Si $I = \ker(\alpha) = \{0\} \iff n\mathbf{1} \neq \mathbf{0}$ $\forall n \in \mathbb{Z}^\times$, α se puede extender a $\tilde{\alpha} : \mathbb{Q} \to F$; $\frac{n}{m} \mapsto (n\mathbf{1}) \cdot (m\mathbf{1})^{-1}$.

Tenemos que comprobar que $\tilde{\alpha}$ está bien definida. Partimos de $\frac{n}{m} = \frac{a}{b} \in \mathbb{Q}$:

$$nb = ma \implies \alpha(nb) = \alpha(ma) \implies (n\mathbf{1})(b\mathbf{1}) = (m\mathbf{1})(a\mathbf{1}) \implies (*)$$
$$(*) \implies (n\mathbf{1})(m\mathbf{1})^{-1} = (a\mathbf{1})(b\mathbf{1})^{-1} \implies \tilde{\alpha}\left(\frac{n}{m}\right) = \tilde{\alpha}\left(\frac{a}{b}\right)$$

Concluimos con que $\tilde{\alpha}$ está bien definida y es un homomorfismo de grupos inyectivo. Por el primer teorema de isomorfía (teorema 10):

$$\tilde{\alpha}(\mathbb{Q}) \subseteq F \subseteq K \text{ donde además } \tilde{\alpha}(\mathbb{Q}) \simeq \mathbb{Q}$$

y por la definición de cuerpo primo: $\mathbb{Q} \simeq \tilde{\alpha}(\mathbb{Q}) = F$.

Consideremos ahora el caso en que $I = \ker(\alpha) \neq \{0\} \iff (\alpha(n) = 0 \iff p \mid n)$. Entonces, existe p primo tal que $I = \langle p \rangle$.
Como $\mathbb{Z}$ es un dominio de ideales principales, e $I \leqslant \mathbb{Z}$, existe $0 \neq m \in \mathbb{Z}$ que cumple $I = \langle m \rangle = m\mathbb{Z}$. Supongamos $m = a \cdot b$, entonces $0 = \alpha(m) = \alpha(a)\alpha(b) \implies \alpha(a) = 0$ ó $\alpha(b) = 0 \implies a$ ó $b \in \langle m \rangle \implies m \mid a$ ó $m \mid b \implies m = p$ primo.

Entonces, de nuevo por el primer teorema de isomorfía:

$$\mathbb{Z}\Big/_{\ker(\alpha)} = \mathbb{Z}\Big/_{p\mathbb{Z}} = \mathbb{F}_p \simeq \alpha(\mathbb{Z}) \subseteq F \subseteq K$$

y por la definición de cuerpo primo: $\mathbb{F}_p \simeq \alpha(\mathbb{Z}) = F$ ♢

Definición 23 (Característica de un cuerpo)**.** Sea K un cuerpo y F su cuerpo primo, decimos que su **característica** $\text{car}(K)$, es $\text{car}(K) = 0$ si $F \simeq \mathbb{Q}$ y $\text{car}(K) = p$ si $F \simeq \mathbb{F}_p$.

Ejercicio (H1.40)**.** Sean K y E dos cuerpos de distinta característica, demuestra que no existe $\varphi : K \to E$ tal que φ sea un homomorfismo de cuerpos.

Supongamos $\text{car}(E) = 0$ y $\text{car}(K) = p > 0$. Entonces:

$$\mathbf{0} = \varphi(p\mathbf{1}) = p\varphi(\mathbf{1}) = p\mathbf{1} \neq 0(\text{en E})$$

Faltaría ver el caso en que $\text{car}(E) = p \neq q = \text{car}(K)$ con p, q primos:

$$\mathbf{0} = \varphi(q\mathbf{1}) = q\varphi(\mathbf{1}) = q\mathbf{1} \neq 0(\text{en E})$$

Con lo que llegamos a una contradicción en ambos casos, y no existe dicho homomorfismo.

Observación. En un cuerpo de característica p, $(a \pm b)^p = a^p \pm b^p$.

Definición 24 (Cuerpo perfecto)**.** Sea K un cuerpo de característica p, y el monomorfismo $Frob : K \to K$; $a \mapsto a^p$. Decimos que K es **perfecto** si $Frob$ es sobreyectivo, es decir, $Frob$ es un isomorfismo de cuerpos.

Proposición 30 (Endomorfismo y cuerpo primo)**.** Sea K un cuerpo, F su cuerpo primo y $\sigma : K \to K$ un endomorfismo de cuerpos, entonces;

$$\sigma(a) = a, \ \forall a \in F$$

Demostración. Se deja como ejercicio. ♢

Ejercicio (H1.42 (parte))**.** Si $n > 0$ no es un cuadrado, demuestra que:

1. $\mathbb{F}_3[\xi] = \left\{a + b\xi \mid a, b \in \mathbb{F}_3,\ \xi^2 = -1\right\}$ es un cuerpo.
2. No existe un homomorfismo de anillos $\varphi : \mathbb{Q}[i] \to \mathbb{Q}[\sqrt{2}]$.

1. Sea el polinomio $f(x) = x^2 + 1$, de forma que $f(\xi) = 0$. Otra forma de describir $\mathbb{F}_3[\xi]$ es:

$$\mathbb{F}_3[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_3,\ f(\xi) = 0\} \simeq \mathbb{F}_3[x] \Big/ \langle f(x) \rangle$$

   por lo que es un cuerpo ya que $x^2 + 1$ es irreducible en $\mathbb{F}_3[x]$ al no tener raíces.
2. El problema surge de la imagen de i. $\varphi(i)$ será de la forma: $a + b\sqrt{2}$, y entonces:

$$-1 = \varphi(-1) = \varphi(i^2) = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

   de donde podría deducirse que $\sqrt{2} \in \mathbb{Q}$ y es imposible. Por tanto no existe dicho homomorfismo.

Capítulo 2

Extensiones de cuerpos

2.1. Grados de cuerpos

Definición 25 (Extensión)**.** Sean K, E cuerpos, decimos que E es una **extensión** de K (denotado por E/K) si K es un subcuerpo de E.

Ejemplo 9 (*Extensiones*)

- $\mathbb{C}/\mathbb{Q}$
- $\mathbb{R}/\mathbb{Q}$
- $\mathbb{C}/\mathbb{R}$
- $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ *con* $n \neq$ *de un cuadrado perfecto.*

Proposición 31 (Extensión como espacio vectorial)**.** Si E es una extensión de K, entonces E es un espacio vectorial sobre K.

Demostración. Basta interpretar el producto por escalares $\cdot : K \times E \to E$ como la restricción del producto sobre $E \times E$ a K. La suma está bien definida por ser E un grupo abeliano con la suma. ♢

Definición 26 (Grado de una extensión)**.** Sea E/K una extensión, el grado de la extensión es $|E : K| = \dim_K E$, que coincide con la dimensión del espacio vectorial que define E sobre K.

Definición 27 (Extensión finita)**.** Sea E/K una extensión, es **finita** si y sólo si $\exists \{a_1, \ldots, a_n\} \subseteq E$ tales que forman una K-base. Es equivalente a decir que $\dim_K E = n < \infty$.

Lema 32 (Extensión de grado 1)**.** Sea E/K una extensión:

$$|E : K| = 1 \iff E = K$$

Demostración.

$\implies$ Si $|E : K| = \mathbf{1}$, entonces $\exists e \in E$ tal que $\{e\}$ es una K-base. Por tanto: $\mathbf{1} = k \cdot e$ con $k \in K \implies e = k^{-1} \implies e \in K \implies E = K$.

$\impliedby$ $\{\mathbf{1}\}$ es K-base de K. $\dim_K K = 1 = |K : K|$.

♢

Teorema 33 (Transitividad de grados)**.** Sea una extensión E/K y un subcuerpo L intermedio $K \subseteq L \subseteq E$, entonces la extensión E/K es finita si y sólo si $|E:L| < \infty, \ \wedge |L:K| < \infty$, y en tal caso: $|E:K| = |E:L| \cdot |L:K|$.

Demostración. Supongamos $\dim_K E = r < \infty$, y $\{e_1, \ldots, e_r\}$ una K-base de E, entonces $\{e_1, \ldots, e_r\}$ es un L-sistema generador de $E \implies E/L$ es finita.
Como $K \subseteq L \subseteq E$, L es un K-subespacio vectorial de E, en particular $\dim_K L \leqslant dim_K E < \infty$. Si E/L y L/K son finitas, cogemos $\{b_1, \ldots, b_m\}$ una L-base de E y $\{a_1, \ldots, a_n\}$ una K-base de E.
Queremos ver que $\{a_i b_j \mid 1 \leqslant i \leqslant n, \ 1 \leqslant j \leqslant m\}$ es una K-base de E (en particular con esto habremos probado que $|E:K| = |E:L| \cdot |L:K|$). Sabemos que:

$$x \in E, x = \sum_{j=1}^{m} l_j b_j, \ l_j \in L$$

pero además

$$l_j = \sum_{i=1}^{n} k_{ij} a_i, \ k_{ij} \in K \implies x = \sum_{1 \leqslant i \leqslant n, \ 1 \leqslant j \leqslant m} k_{ij} a_i b_j, \ k_{ij} \in K$$

Faltaría ver que $\{a_i b_j\}$ es K-libre.

$$\sum_{1 \leqslant n, \ 1 \leqslant i \leqslant j \leqslant m} k_{ij} a_i b_j = 0 \implies \sum_j l_j b_j = 0 \implies l_j = 0 \implies \sum_i k_{ij} a_i = 0 \implies k_{ij} = 0 \forall i \forall j$$

♢

Definición 28 (Menor subanillo y subcuerpo)**.** Sea E/K una extensión y sea $a \in E$.

- Denotaremos por $K[a]$ al **menor subanillo** de E que contiene a K y a $a \in E$. Se puede probar que $K[a] = \{f(a) \forall f \in K[x]\}$.
- Denotaremos por $K(a)$ al **menor subcuerpo** de E que contiene a K y a $a \in E$. Se puede probar que $K(a) = \left\{ \frac{f(a)}{g(a)} \forall f, g \in K[x] \mid g(a) \neq 0 \right\}$.

Ejemplo 10

- $\mathbb{Q}[\sqrt{n}] = \{a + \sqrt{n} \mid a, b \in \mathbb{Q}\}$. *En este caso* $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}(n)$.
- $X \subseteq E$, $K(X)$ *es el menor subcuerpo de* E *que contiene a* K *y a* X. $K(X)$ *se obtiene al adjuntar* X *a* K.

Observación. En general $K[a] \subseteq K(a)$, pero hay en casos en los que la igualdad no se cumple.

Definición 29 (Extensión simple)**.** Sea E/K una extensión, es **simple** si $\exists a \in E$ tal que $E = K(a)$.

Ejemplo 11 (*Extensión simple*)

- $\mathbb{C}/\mathbb{R}$, *ya que* $\mathbb{C} = \mathbb{R}(i)$.
- *Con* $p \neq q$ *primos,* $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ *es simple, ya que se puede demostrar que* $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

Proposición 34 (Dimensión de un cuerpo finito)**.** Sea K un cuerpo finito, entonces $|K| = p^n$ con p primo.

Demostración. Sea K un cuerpo y F su cuerpo primo, sabemos que F es isomorfo a algún $\mathbb{F}_p$ con p un primo. Además, K/F es una extensión. Y como K es subespacio vectorial $|K:F| = \dim_F K = n$. Entonces $K \simeq F^n \implies |K| = |F|^n = p^n$. ♢

2.2. Extensiones algebraicas y trascendentes

Definición 30 (Extensión algebraica. Extensión trascendente)**.** Sea E/K una extensión.
- Sea $a \in E$, a es *algebraico* si $\exists f(x) \neq 0 \in K[x] : \ f(a) = 0$. E/K es una **extensión algebraica** si todo $a \in E$ es algebraico sobre E.
- Sea $a \in E$, a es *trascendente* si no es algebraico. E/K es una **extensión trascendente** si existe $a \in E$ trascendente sobre E.

Ejemplo 12 (*Extensiones algebraicas y trascendentes*)

- *K/K es algebraica. Todo elemento de K es raíz de $x - k \in K[x]$.*
- *$\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ es algebraica.*
- *$\mathbb{R}/\mathbb{Q}$ es trascendente. e y π son trascendentes.*
- *Sea $K[t]$ un dominio de integridad- Podemos construir su cuerpo de fracciones:*

$$K(t) = \left\{ \frac{f(t)}{g(t)} \mid f, g \in K[t],\ g(t) \neq 0 \right\}$$

Entonces $K(t)/K$ es trascendente. (t siempre es trascendente).

Proposición 35 (Extensiones y cuerpos intermedios)**.** Sea E/K una extensión y $K \subseteq L \subseteq E$ un cuerpo intermedio:

1. E/K es algebraica $\iff$ L/K y E/L son algebraicas.
2. Si E/L es trascendente, entonces E/K es trascendente.

Demostración. Se deja como ejercicio. ♢

Teorema 36 (Extensiones finitas y algebraicas)**.** Toda extensión finita es algebraica.

Demostración. Sea E/K una extensión, $a \in E$, queremos ver que es raíz de $0 \neq f(x) \in K[x]$. Suponemos $|E : K| = n$ con un K-sistema: $\{1, a_1, \ldots, a^{n-1}\} \subseteq E$ con n elementos. Entonces, el sistema puede ser:

K-ligado Existen $k_i \in K$ no todos nulos tales que $k_0 + k_1 a + \ldots + k_{n-1}a^{n-1} = 0$, entonces a es raíz de $f(x) = k_0 + \ldots + k_{n-1}x^{n-1}$.

K-libre Como $\dim_K E = n$, $\{1, a_1, \ldots, a^{n-1}, a^n\}$ es K-ligado, y de nuevo, a es raíz de $f(x) = k_0 + \ldots + k_{n-1}x^{n-1} + k_n x^n$.

♢

2.3. Teorema del elemento algebraico

Teorema 37 (Teorema del elemento algebraico)**.** Sea E/K una extensión, $a \in E$ un elemento algebraico sobre K.
1. Existe un único polinomio irreducible mónico $p \in K[x]$ tal que $p(a) = 0$.
2. Si $q \in K[x]$ y $q(a) = 0$, entonces $p \mid q$.
3. $K(a) = \{f(a) \mid f \in K[x]\} = K[a]$.
4. Si $\delta(p) = n$, entonces $\{1, a, \ldots, a^{n-1}\}$ es una K-base de $K(a)$. En particular, $|K(a) : K| = \delta(p)$ y $K(a) = \{k_0 + k_1 a + \ldots + k_{n-1}a^{n-1} \mid k_i \in K\}$.

Demostración. $(\cdots)$ (Es muy tarde ahora mismo para pasar esto a limpio, que alguien me mate por favor.) ♢

Definición 31 (Polinomio mínimo)**.** Sea E/K una extensión y $a \in E$ algebraico sobre K, al único polinomio mónico e irreducible $p \in K[x]$ dado por el teorema 37 se le llama **polinomio mínimo** o **polinomio irreducible** de a sobre K y escribimos $p = Irr(K, a)$.

Observación. Sea $b = k_0 + \ldots + k_{n-1}a^{n-1} \in K(a)$, ¿cómo se expresa b^{-1} en la misma base?
Consideramos $f(x) = k_0 + \ldots + k_{n-1}x^{n-1} \in K[x]$, con $f(a) = b \neq 0$ y $\delta(f) \leqslant \delta(p)$, siendo p el polinomio irreducible. Entonces $mcd(f, g) = 1$. Por la identidad de Bezout:

$$\exists h, g \in K[x] : \ 1 = fh+gp \implies \text{(evaluando en } a) 1 = f(a)h(a)+g(a)p(a) \implies 1 = f(a)h(a) = bh(a) \implies b^{-1} = h(a)$$

Ejemplo 13 (*Ejercicio tipo*)
$(\cdots)$ (Es aún más tarde. `https://www.youtube.com/watch?v=I_6Gej1m4SU`*)*

Teorema 38 (Extensión por varios elementos algebraicos)**.** Sea E/K una extensión, y sea $\mathbf{a} = (a_1, \ldots, a_n)$ con $a_i \in E$ algebraicos sobre K, entonces $K(\mathbf{a})/K$ es finita. En particular, $K(\mathbf{a})/K$ es algebraica.

Demostración. Por inducción sobre n. Si $n = 1$ por el teorema del elemento algebraico (teorema 37) sabemos que $|K(a_1)/K| = \delta(Irr(K, a_1)) < \infty$.
Veamos el caso $n > 1$. Sea $L = K(a_1, \ldots, a_{n-1})$, entonces $K(\mathbf{a}) = L(a_n)$. Por la hipótesis de inducción L/K es finita, por el teorema 37 $L(a_n)/L$ es finita y por tanto, por el teorema de transitividad de grados (teorema 33) $L(a_n)/K$ es finita, donde $L(a_n)$ era $K(\mathbf{a})$. La segunda parte se sigue directamente aplicando el teorema 36. ♢

Ejercicio (H2.7)**.** Dada E/K una extensión, prueba que $L = \{e \in E \mid e \text{ es algebraico sobre } K\} \supseteq K$ es un cuerpo. Sea $\mathbb{A} \subset \mathbb{C}$ los elementos algebraicos sobre $\mathbb{Q}$, prueba que $\mathbb{A}/\mathbb{Q}$ es una extensión de grado infinito
Sean $a, b \in L$ cualesquiera, entonces $a, b \in K(a, b)^\times$ y por el teorema 38 $K(a, b)/K$ es algebraica. Como $a \pm b$ y $ab^{\pm 1} \in K(a, b)$, entonces son algebraicos sobre $K \implies (a \pm b), (ab^{\pm 1}) \in L$, con lo que es cerrado por ambas operaciones y L es un cuerpo.
Por la primera parte del ejercicio, sabemos que $\mathbb{Q} \subseteq \mathbb{A} \subseteq \mathbb{C}$ es un subcuerpo intermedio, de $\mathbb{C}/\mathbb{Q}$, y por definición $\mathbb{A}/\mathbb{Q}$ es algebraica.
Por el criterio de Einsestein (teorema 22), para cada $n \in \mathbb{N}^\times$, $x^n - 2$ es irreducible en $\mathbb{Q}[x]$. $\sqrt[n]{2}$ es solución por tanto es algebraico y por el teorema 37 $|\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}| = n$.
Como podemos hacerlo $\forall n \in \mathbb{N}^\times$, hemos comprobado que $\mathbb{A}/\mathbb{Q}$ es no finita.

Ejercicio (H2.6)**.** $(\cdots)$ (Yep. `https://www.youtube.com/watch?v=pwSsT8IU0WE`)

2.4. Isomorfismos de cuerpos

Ya definimos qué es un homomorfismo de cuerpos en la sección 1.3. En esta sección vamos a ampliar los conocimientos cuando aplicamos los homomorfismos específicamente a cuerpos.

Observación. Si $\text{car}(E) \neq \text{car}(K)$ entonces: $Hom(E, K) = \varnothing = Hom(K, E)$, con $Hom(X, Y) = \{\varphi : X \to Y \mid \varphi \text{ es un homomorfismo de cuerpos}\}$. Además, si K es finito, $End(K) = Aut(K)$ (conjunto de endomorfismos y automorfismos respectivamente), pero en general: $End(K) \subsetneq Aut(K)$.

Observación. Sea $\varphi \in End(K)$ y F es el cuerpo primo de K, entonces $\varphi(a) = a, \ \forall a \in F$. De forma más general, si $\varphi \in Hom(E, K)$ y E, K tienen el mismo cuerpo primo, $\varphi(a) = a$, por ejemplo: $Aut(\mathbb{F}_p) = \{id\}$, $Aut(\mathbb{Q}) = \{id\}$.

En ocasiones querremos saber como extender un isomorfismo de cuerpos a una extensión de dichos cuerpos. Vamos a ver un lema y un teorema.

Lema 39 (Restricción de un isomorfismo de cuerpos)**.** Sea E_1/K_1 una extensión, $\theta : E_1 \to E_2$ un isomorfismo de cuerpos, y sea $K_2 = \theta(K_1)$, entonces:

1. E_2/K_2 es una extensión y $|E_1 : K_1| = |E_2 : K_2|$.
2. Sean $a_1, \ldots, a_n \in E_1$. $\theta(K_1(a_1, \ldots, a_n)) = K_2(\theta(a_1), \ldots, \theta(a_n))$.
3. θ se extiende a un isomorfismo de anillos $\theta : K_1[x] \to K_2[x]$, aplicando θ individualmente a cada coeficiente del polinomio.

Demostración. Como ejercicio. ♢

Teorema 40 (Extensión de un isomorfismo de cuerpos)**.** Sean E_1/K_1, E_2/K_2 extensiones, $\sigma : K_1 \to K_2$ un isomorfismo de cuerpos, p_1 irreducible en K_1, p_2 irreducible en K_2, y a_1 y a_2 raíces de los polinomios respectivamente, entonces:

$$\sigma \text{ se extiende a } \theta \iff \theta|_{K_1} = \sigma$$

Donde $\theta : K_1(a_1) \to K_2(a_2)$ tal que $\theta(a_1) = a_2$.

Demostración. A completar. ♢

Corolario 6. Sea E/K una extensión, $p \in K[x]$ irreducible, entonces:

$$a, b \in E \text{ son raíces de } p \iff \exists \text{ un isomorfismo } \theta : K(a) \to K(b) \text{ tal que } \theta(a) = b \text{ y } \theta(k) = k \ \forall k \in K$$

Ejercicio (H2.4 (parte))**.** Halla el grado y base de las siguientes extensiones de cuerpos:

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q}$.
   Consideramos $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ cuerpo intermedio, y además, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = L(i)$. i es raíz del polinomio $x^2 + 1$ qque no tiene raíces en L y por tanto, $x^2 + 1 = Irr(L, i)$. Por el teorema 37, $|\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}| = 2 = \delta(Irr(L, i))$.

   Además, $|L : \mathbb{Q}| = 4$ por el ejercicio 1 de la hoja 2. Por el teorema 33, $|\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}| = |L(i) : L| \cdot |L : \mathbb{Q}| = 8$. Una vez sabemos el grado, podemos encontrar una $\mathbb{Q}$-base:

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

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

2. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.
   $\alpha = \sqrt[4]{2}$ es raíz de $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$, y es irreducible porque no tiene raíces en $Q(\sqrt{2})$, (se prueba por reducción al absurdo).
   Por tanto: $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})| = 2$ y una base:

   $$\left\{1, \sqrt[4]{2}\right\}$$

3. $\mathbb{Q}(\sqrt{1 + \sqrt{3}})/\mathbb{Q}$.
   Consideramos el cuerpo intermedio $L = \mathbb{Q}(\sqrt{3})$. Es fácil ver que $|L/\mathbb{Q}| = 2$. Falta encontrar el grado de $|\mathbb{Q}(\sqrt{1 + \sqrt{3}})/L|$. Sea $\alpha = \sqrt{1 + \sqrt{3}}$, α es raíz de $x^2 - (1 + \sqrt{3})$, que se puede demostrar que es irreducible en L. Por tanto, por el teorema 33, $|\mathbb{Q}(\sqrt{1 + \sqrt{3}}) : \mathbb{Q}| = 4$, y la base:

   $$\left\{1, \sqrt{3}, \sqrt{1 + \sqrt{3}}, \sqrt{3}\sqrt{1 + \sqrt{3}}\right\}$$

Ejercicio (H2.5)**.** Halla grado y base de $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$. Halla la expresión de t^{-1} y $(t+1)^{-1}$ en la base que has hallado.

Consideramos en polinomio $x^2 - t^2 \in F(t^2)[x]$, donde t es una raíz y $\pm t \notin \mathbb{F}_7(t^2)$. Se puede demostrar por reducción al absurdo que el polinomio $x^2 - t^2$ es irreducible. Por tanto, por el teorema 37, $|\mathbb{F}_7(t)/\mathbb{F}_7(t^2)| = 2$.
Una $\mathbb{F}_7(t^2)$-base de $\mathbb{F}_7(t)$ es: $\{1, t\}$.

Vamos a expresar ahora los elementos que se nos piden. Consideramos $t = f(t)$, $f(x) = x$.

$$x^2 - t^2 = 0,\ x \cdot x = t^2 \implies x \cdot \frac{1}{t^2} \cdot x = 1, \text{ que evaluando en } t\text{: } t \cdot \left(\frac{1}{t^2} \cdot t\right) = 1$$

Con ello, hemos hallado el inverso de t. Para hallar el inverso de $t+1$ procedemos de forma parecida. Consideramos $f(x) = x + 1$. Vemos que $mcd(f(x), x^2 - t^2) = 1$. Procediendo con el algoritmo de división de polinomios, podemos expresar:

$$x^2 - t^2 = f(x)(x-1) + (1 - t^2) \implies (x^2 - t^2) + f(x)(1 - x) = 1 - t^2 \in \mathbb{F}_7(t^2)$$

Entonces:

$$\frac{1}{1-t^2}(x^2 - t^2) + f(x)\frac{1-x}{1-t^2} = 1$$

Evaluando en t:

$$f(t)\frac{1-t}{1-t^2} = 1 \implies (t+1)^{-1} = \frac{1}{1-t^2} \cdot 1 + \frac{1}{t^2-1}t$$

Ejercicio (H2.10)**.** Sea E/K una extensión, $\alpha \in E$ algebraico sobre K y L un subcuerpo intermedio. Prueba que $q(x) = Irr(L, \alpha) \mid Irr(K, \alpha) = p(x)$.

$p(x) \in K[x] \subseteq L[x]$, entonces $p(x)$ tambien es un polinomio de $L[x]$. Como $p(\alpha) = 0$, por el teorema del elemento algebraico, (teorema 37) $q(x) \mid p(x)$. Y entonces:

$$|L(\alpha) : L| = \delta(q(x)) \leqslant \delta(p(x)) = |K(\alpha) : K|$$

Ejercicio (H2.11)**.** Sea E/K una extensión. Demuestra:

1. Si $|E/K| = p$ con p primo, demuestra que no hay subcuerpos intermedios.

   Por el teorema de transitividad de grados (teorema 33), sabemos que $|E : K| = |E : L| \cdot |L : K| = p \implies |E : L| = 1 \vee |L : K| = 1$, y por tanto $E = L \vee L = K$.

2. Sea $|E : K| = p$ con p primo, entonces E/K es simple.

   Consideramos $L = K(\alpha)$ con $\alpha \in E, \alpha \ \ inK$, además $K(\alpha) \neq K$ y por tanto (por el primer apartado) $L = E = K(\alpha)$ y es simple ya que $K(\alpha)$ lo es.

3. Supongamos $\alpha \in E$ tal que $Irr(K, \alpha) = x^3 + x - 1$. Queremos calcular $Irr(K, \alpha^2)$. Como sabemos que $K(\alpha)/K$ tiene grado 3, y por el apartado siguiente, $K(\alpha) = K(\alpha^2)$, entonces por el teorema 37, $\delta(Irr(K, \alpha^2)) = 2$.

   Entonces:

   $$\alpha^3 + \alpha^2 = 1 \iff \alpha^6 + 2\alpha^4 + \alpha^2 - 1 = 0$$

   Sea $\beta = \alpha^2$, entonces se satisface que:

   $$\beta^3 + 2\beta^2 + \beta - 1 = 0$$

   y con ello hemos hallado el polinomio irreducible que buscábamos.

4. Si $\alpha \in E$, con $|K(\alpha) : K| = n$ impar, calcula $|K(\alpha^2) : K|$.

   Como n es impar sabemos que $\alpha^2 \in K(\alpha)$ y por tanto $K(\alpha^2) = K(\alpha)$.

5. Sea $K \subseteq L_1, L_2 \subseteq E$ dos cuerpos intermedios de grado coprimos sobre K demuestra que $L_1 \cap L_2 = K$.

   Se considera el cuerpo $L_1 \cap L_2$. Sea $d = |L_1 \cap L_2/K$, $n = |L_1/K|$ y $m = |L_2/K$. Entonces por el teorema 33, $d \mid n$ y $d \mid m$ con n, m coprimos, por tanto $d = 1$ y $L_1 \cap L_2 = K$.

Ejercicio (H2.12)**.** Sea E/K una extensión, y sean $a, b \in E$ algebraicos con $|K(a) : K| = n$, $|K(b) : K| = m$. Prueba que:

1. $|K(a, b) : K(b) \leqslant n$.

   Mirar el ejercicio H2.10

2. Sean n y m son coprimos, entonces $K(a) \cup K(b) = K$ y $|K(a, b) : K| = nm$. Deduce que $Irr(K, a) = Irr(K(b), a)$.

   Mirar ejercicio H2.11

3. Calcula $Irr(\mathbb{Q}, \alpha)$ con $\alpha = \sqrt{3} + \sqrt[3]{2}$

Parte II

Segundo parcial

Capítulo 3

Extensiones de Galois

3.1. Cuerpos de escisión

Definición 32 (Escisión de un polinomio)**.** Sea $f \in K[x]$, K cuerpo, decimos que f se **escinde** si $\exists a, a_i \in K$ si:

$$f(x) = a(x - a_1) \dots (x - a_n)$$

Observación. Si $f(x) \in K[x]$, $\delta f = 1$, entonces f se escinde en K.

$$f(x) = ax + b = a\left(x - \left(-\frac{b}{a}\right)\right), \quad a, -\frac{b}{a} \in K$$

Observación. Si $f \in K[x]$, se escinde en E, sea E/K una extensión:

$$f(x) = a(x - a_i) \dots (x - a_n) \in E[x]$$

Entonces las raíces de f en cualquier extensión de E son $a_1, \dots, a_n$

Definición 33 (Cuerpo de escisión)**.** Sea $f \in K[x]$, entonces E es un cuerpo de escisión de f sobre K si:

- E/K es una extensión.
- f se escinde en E.
- Si f se escinde en L, con L un cuerpo intermedio $K \subseteq L \subseteq E$, entonces $L = E$, es decir, $E = K(f)$. (Es el menor subcuerpo con la propiedad de que f se escinda en él).

Ejemplo 14

$x^2 + 1$ *se escinde en* $\mathbb{C}$ *pero su cuerpo de escisión es* $\mathbb{Q}(i)$.

Observación. Si $f \in K[x]$ se escinde en E, entonces E tiene todas las raíces de f. Para construir su cuerpo de escisión basta adjuntar todas las raíces al cuerpo sobre el que está definido:

$$f(x) = a(x - a_1) \dots (x - a_n) \in E[x], \text{ entonces su cuerpo de escisión es } K(f) = K(a_1, \dots, a_n)$$

Lema 41 (Escisión de polinomios no constantes)**.** Sea K un cuerpo:

(*i*) Si $f \in K[x]$ no constante se escinde en K si y sólo si todos los polinomios en la descomposición en términos de factores irreducibles tienen grado 1.

(*ii*) Si $f \in K[x]$ no constante que se escinde en K y sea $p \in K[x]$ tal que $p \mid f$, entonces p se escinde en K.

Demostración. La demostración se deja como ejercicio. ♢

Lema 42 (Cuerpos de escisión y cuerpos intermedios)**.** Sean E/L y L/K extensiones, y $f \in K[x]$ un polinomio no constante. Si E es el cuerpo de escisión de f sobre K, entonces E es el cuerpo de escisión de f sobre L.

Demostración. Como $E = K(f)$, tenemos que $f(x) = a(x-a_1)\dots(x-a_n) \in E[x]$ y $E = K(a_1,\dots,a_n)$. Además, $f \in K[x] \subseteq L[x]$. Si el cuerpo de escisión de f sobre L es E', fácilmente llegamos a que $E' = L(f) \subseteq E$ y por tanto: $E = E'$ ya que E era el menor cuerpo de escisión de f sobre K. ♢

Si f es un polinomio sobre $\mathbb{Q}[x]$ de grado n, *sabemos* que $\exists \alpha_i \in \mathbb{C}$ con $i \in \{1,\dots n\}$ tal que $f(x) = a(x-\alpha_1)\dots(x-\alpha_n)$, y hemos visto para calcular su cuerpo de escisión basta con adjuntar las raíces de f, es decir, $\mathbb{Q}(f) = \mathbb{Q}(\alpha_1,\dots,\alpha_n)$.

Vamos a ver resultados para generalizar este proceso.

Lema 43 (Teorema de Kronecker)**.** Sea $p \in K[x]$ un polinomio irreducible, entonces existe E/K tal que p tiene una raíz en E.

Demostración. Sea $L = {}^{K[x]}\big/_{\langle p\rangle}$, ya vimos que L es un cuerpo por ser p irreducible. Además se puede comprobar que:

$$\bar{x} = x + \langle p\rangle \in L \text{ es raíz de } \bar{p} \in \bar{K}[y]$$

Donde $\bar{p} = \overline{a_0} + \dots + \overline{a_n}x^n$ y $K \simeq \bar{K} = \{\bar{K} \mid k \in K\}$.

Hay que comprobar que $\bar{K} \subseteq L$. Tras ello, habría que ver que $L = \bar{K}(\bar{x})$. ♢

Teorema 44 (Existencia de cuerpos de escisión)**.** Sea K un cuerpo, $f \in K[x]$ un polinomio no constante. Entonces existe un cuerpo de escisión E de f sobre K.

Demostración. Basta construir una extensión en la que f se escinda. La demostración sigue por inducción sobre $\delta(f)$.

$\delta(f) = 1$ Entonces por el lema 41, K es un cuerpo de escisión de f sobre K.

$\delta(f) > 1$ Sea $p \mid f$ un factor irreducible de f en $K[x]$, por el lema 43, sabemos que existe E/K en la que p tiene una raíz $\alpha \in E$, en particular $f(\alpha) = 0$ y por Ruffini:

$$f(x) = (x-\alpha)g(x), \text{ con } g(x) \in K(\alpha)[x]$$

Como $1 \leqslant \delta(g) \leqslant \delta(f) - 1 \leqslant \delta(f)$, por inducción sabemos que existe un cuerpo de escisión L de g sobre $K(\alpha)$. Si $\alpha_1,\dots\alpha_n \in L$ son las raíces de g, entonces:

$$L = K(\alpha)(\alpha_1,\dots\alpha_n) = K(\alpha,\alpha_1,\dots,\alpha_n)$$

y por tanto $f(x) = (x-\alpha)g(x) = (x-\alpha)p(x-\alpha_1)\dots(x-\alpha_n) \in L[x]$, así que f se escinde sobre L, y de hecho L es un cuerpo de escisión de f sobre K.

♢

Ejercicio (Cálculo del cuerpo de escisión)**.** Describir el cuerpo de escisión de $f(x) = x^4 - 4x^2 + 2$ sobre $\mathbb{Q}$.

Comenzamos hallando las raíces, que resulta fácil pues $f(x) = 0$ es una ecuación bicuadrática. Tenemos entonces las raíces:

$$\alpha = \sqrt{2+\sqrt{2}},\ \beta = \sqrt{2-\sqrt{2}},\ -\alpha,\ -\beta$$

De donde vemos que f se escinde en R ya que todas las raíces son reales. Para ver su cuerpo de escisión vamos a adjuntar las raíces a $\mathbb{Q}$.

$$E = \mathbb{Q}(\alpha,\beta,-\alpha,-\beta) = \mathbb{Q}(\alpha,\beta)$$

Sin embargo, podemos reducirlo aún más si vemos que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$.

$$\alpha\beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2},\ \alpha^{-1} = \left(\frac{\beta}{\sqrt{2}}\right) \in \mathbb{Q}(\alpha) \implies \beta = \frac{\beta}{\sqrt{2}} \cdot \sqrt{2} \in \mathbb{Q}(\alpha)$$

Con lo que el cuerpo de escisión es: $\mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Observación. Si $E = K(f)$, entonces E/K es finita por el teorema 38. Anteriormente, vimos que si $f \in K[x]$, entonces existe un cuerpo de escisión de f sobre K.
Sea p un polinomio irreducible tal que $p \mid f$ y $\delta p > 1$, entonces consideramos $K[x]\Big/_{\langle p \rangle}$ y en ese cuerpo hay una raíz de p (que también es raíz de f), y después aplicamos inducción.

Teorema 45. Sea K_1, K_2 cuerpos, y $\sigma : K_1 \to K_2$ un isomorfismo de cuerpos. Sea $f_1 \in K_1[x]$ no constante y $\delta(f_1) = f_2$.
Supongamos que E_i son cuerpos de escisión de f_1 sobre K_i con $i \in \{1, 2\}$. Entonces existe un isomorfismo $\tau : E_1 \to E_2$ que extiende a σ, es decir, $\tau|_{K_1} = \sigma$.

Demostración. Por inducción sobre $|E_1 : K_1| < \infty$.

$|E_1 : K_1| = 1$ En este caso, $|E_1 : K_1| \iff f_1$ se escinde en $K_1[x] \implies \sigma(f_1) = f_2$ se escinde en $K_2[x] \implies E_2 = K_2$ y podemos tomar $\tau = \sigma$.

$|E_1 : K_1| > 1$ En este caso f_1 no se escinde en $K_1[x]$, y podemos escoger p un factor de f_1 irreducible con $\delta(p) > 1$. Además, sea $q = \sigma(p)$ tal que $q \mid f_2$ y es irreducible con $\delta(q) > 1$. Escogemos las raíces de p en $E_1(a)$ y las de q en $E_2(b)$ (por el lema 41 sabemos que p y q se escinden en E_1 y E_2 respectivamente).

$$\begin{array}{ccc}
\tau : E_1 = K_1(f_1) & & E_2 = K_2(f_2) \\
\Big| & & \Big| \\
\tau|_{K_1(a)} = \theta : K_1(a) & \xrightarrow{\simeq} & K_2(b) \\
\Big| & & \Big| \\
\theta|_{K_1} = \sigma : K_1 & \xrightarrow{\simeq} & K_2 \\
\Big| & & \Big| \\
p & \longmapsto & q
\end{array}$$

Por el teorema 40 existe un isomorfismo $\theta : K_1(a) \to K_2(b)$ que extiende a σ.

Por el teorema 37 $|K_1(a) : K_1| = o(p) > 1$, luego por el teorema 33 $|E_1 : K_1(a)| < |E_1 : K_1|$ y además $E_1 = K_1(a)(f_1)$ (por el lema 42). Del mismo modo E_2 es un cuerpo de escisión de f_2 sobre $K_2(b)$. Por inducción, existe un isomorfismo $\tau : E_1 \to E_2$ tal que $\tau|_{K_1(a)} = \theta$. En particular, $\tau|_{K_1} = \left(\tau|_{K_1(a)}\right)\Big|_{K_1} = \theta|_{K_1} = \sigma$.

♢

Corolario 7 (Unicidad de los cuerpos de escisión)**.** Sea K un cuerpo y $f \in K[x]$ no constante. Si E_1 y E_2 son cuerpos de escisión de f sobre K entonces $\exists\tau$ un isomorfismo $\tau : E_1 \to E_2$ tal que $\tau(a) = a$ $\forall a \in K$.

Demostración. Basta tomar $\sigma = id_K$ en el teorema 45. ♢

Observación. Un cuerpo K en el que todo polinomio $f \in K[x]$ se escinde se dice que es *algebraico cerrado*. Por ejemplo $\mathbb{C}$ es un cuerpo algebraico cerrado.

3.2. Extensiones normales

Definición 34 (Extensión normal)**.** Sea K un cuerpo y E/K una extensión, diremos que E/K es una **extensión normal** si E es el cuerpo de escisión de algún polinomio $f \in K[x]$.

Observación. Como consecuencia del teorema 36 y del teorema 38, si E/K es normal $\implies$ E/K es finita $\implies$ E/K es algebraica.

Ejercicio (H3.1)**.** Construye los cuerpos de escisión $\mathbb{Q}(x^3-1)$, $\mathbb{Q}(x^4+5x^2+5)$, $\mathbb{Q}(x^6-8)$ y calcula los grados de las extensiones que resultan.

Solucion

$f(x) = x^3 - 1$ Las raíces son las raíces cúbicas de la unidad: $1, \omega, \bar{\omega} = \omega^2$, por lo que $\mathbb{Q}(f) = \mathbb{Q}(1, \omega, \omega^2) = \mathbb{Q}(\omega)$.

$f(x) = x^4 + 5x^2 + 5$ Muy parecido a un ejemplo ya resuelto.

$f(x) = x^6 - 8$ Las raíces son las complejas de 8.

$$\sqrt[6]{8} = (8^{\frac{1}{3}})^{\frac{1}{2}} = \sqrt{2}$$

Sea $\xi = e^{\frac{2\pi i}{6}} = e^{\pi i}3$, las raíces de f son:

$$\left\{ \sqrt{2},\ \sqrt{2}\xi,\ \sqrt{2}\xi^2,\ \sqrt{2}\xi^3,\ \sqrt{2}\xi^4,\ \sqrt{2}\xi^5 \right\}$$

Por tanto $\mathbb{Q}(f) = \mathbb{Q}(\sqrt{2},\ \sqrt{2}\xi,\ \sqrt{2}\xi^2,\ \sqrt{2}\xi^3,\ \sqrt{2}\xi^4,\ \sqrt{2}\xi^5)$.Faltaría comprobar que esta extensión es la misma que $\mathbb{Q}(\sqrt{2}\xi)$. Procediendo de forma similar a ejercicios anteriores, para hallar el grado de la extensión calculamos el polinomio $Irr(\mathbb{Q}, \sqrt{2}\xi)$ y vemos que es $x^4 + 2x^2 + 4$ con lo que el grado de la extensión es 4.

Ejercicio (H3.5)**.** Decide si las extensiones $\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ son normales.

Solución

$\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}$ Es fácil comprobar que $\mathbb{Q}(\sqrt{5}i) = \mathbb{Q}(x^2+5)$ y por tanto son normales.

$\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ Es fácil comprobar que $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(x^2-5)$ y por tanto son normales.

$\mathbb{Q}(5^{\frac{1}{4}})/\mathbb{Q}$ $x^4 - 5$ tiene una raíz en $\mathbb{Q}(\sqrt[4]{5})$ pero no se escinde, por tanto no es normal.

Lema 46 (Normalidad de extensiones en cuerpos intermedios)**.** $K \subseteq L \subseteq E$ extensiones, entonces:

$$E/K \text{ normal} \implies E/L \text{ normal.}$$

Demostración. Es consecuencia directa del lema 42 y de la definición. ♢

Corolario 8 (al teorema 45)**.** Sea E/K una extensión normal, $K \subseteq M_1, M_2 \subseteq E$ con M_1, M_2 cuerpos intermedios.

Si existe un isomorfismo $\sigma : M_1 \to M_2$ que fija a K, es decir, $\sigma(a) = a,\ \forall a \in K$, entonces σ se extiende a un isomorfismo $\tau : E \to E$ ($\tau|_{M_1} = \sigma$).

Demostración. Sea $E = K(f)$ con $f \in K[x]$ no constante. En particular por el lema 42, $E = M_1(f) = M_2(f)$. Como $\sigma(f) = f$, el resultado se sigue del teorema 45. ♢

Observación. La hipótesis $\sigma(a) = a,\ \forall a \in K$ es necesaria. La idea es que sin esta hipótesis:

$$E = M_1(f) = M_2(f)$$

pero no sabríamos si $E = M_2(\sigma(f))$.

Teorema 47 (Condición necesaria y suficiente para la normalidad de una extensión)**.** Sea E/K una extensión finita, E/K es normal si y sólo si todo polinomio $p \in K[x]$ irreducible con una raíz en E se escinde en E.

Demostración.

$\Longleftarrow$ Sabemos que E/K es finita, digamos $|E : K| = n$, podemos tomar una K-base $\{a_1, \ldots, a_n\}$. En particular $E = K(a_1, \ldots, a_n)$.
Como E/K es finita, por el teorema 36, los a_i en son algebraicos sobre K. Sea $p_i = Irr(k, a_i) \in K[x]$, por hipótesis cada p_i se escinde en E.

Tomamos $f = \prod_{i=1}^{n} p_i \in K[x]$ se escinde en E. De hecho, $E = K(f)$. De esta forma hemos probado que:

$$K(f) \subseteq E = K(a_1, \ldots, a_n) \subseteq K(f)$$

$\Longrightarrow$ Ahora partimos de que E/K es finita y normal. Entonces $\exists f \in K[x]$ tal que $E = K(f)$.
De hecho, si $f(x) = c(x - b_1) \ldots (x - b_n) \in E[x]$, $E = K(b_1, \ldots, b_n)$.
Sea $p \in K[x]$ irreducible con una raíz $a \in E$, por Ruffini (corolario 1) $p(x) = (x - a)g(x) \in E[x]$.
Además, por el teorema 44, existe M/E un cuerpo de escisión de p sobre E, por tanto:

$$p(x) = d(x - d_1) \cdot \ldots \cdot (x - d_r),\ \text{podemos suponer que } a = d_1$$

Dado d_i con $i > 1$, queremos ver que $d_i \in E$. Llamemos $b = d_i$ para algún i. Como a y b son raíces de $p \in K[x]$ irreducible, por el teorema 40 $\exists \sigma : K(a) \to K(b)$ tal que $\sigma(k) = k,\ \forall k \in K$.

$$\begin{array}{ccc} \sigma : K(a) & \longrightarrow & K(b) \\ \updownarrow & & \updownarrow \\ id : K & \longrightarrow & K \end{array}$$

Como $K(a) \subseteq E$, en particular $E = K(a)(f)$. Por otro lado $K(b)(f) = E(b)$. Las raíces de f en $E(b)$ son $b_1, \ldots, b_m$, así que:

$$K(b)(f) = K(b)(b_1, \ldots, b_m) = K(b_1, \ldots, b_m) = E(b)$$

Por el teorema 45 existe un isomorfismo $\tau : E \to E(b)$ que extiende a σ.

$$\begin{array}{ccc} \tau : E = K(a)(f) & \longrightarrow & E(b) = K(b)(f) \\ | & & | \\ \sigma : K(a) & \longrightarrow & K(b) \\ \updownarrow & & \updownarrow \\ id : K & \longrightarrow & K \end{array}$$

Por el ejercicio $H2$,15, $|E : K| = |E(b) : K|$ y $|K(a) : K| = |K(b) : K|$. Además $|E : K(a)| = |E(b) : K(b)|$. Por tanto:

$|E : K| = |E : K(a)||K(a) : K| = |E(b) : K(b)||K(b) : K| = |E(b) : K| = |E(b) : E||E : K|$ usando el teorema 33.

Con lo que concluimos:

$$|E(b) : E| = 1 \implies E(b) = E \implies b \in E$$

$\diamondsuit$

Ejercicio (H3.5)**.** Decide si son normales las siguientes extensiones:

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

   Es normal ya que $\mathbb{Q}(\sqrt{5}i) = \mathbb{Q}(x^2+5)$ es el cuerpo de escisión de x^2+5.

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

   Es normal ya que $\mathbb{Q}(\sqrt{5})/\mathbb{Q} = \mathbb{Q}(x^2-5)$ es el cuerpo de escisión de x^2-5.

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

   No es normal. Sabemos que $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ es finita, y como $p(x) = x^4 - 5$ es irreducible en $\mathbb{Q}[x]$, tiene una raíz en $\mathbb{Q}(\sqrt[4]{5})$ pero no escinde, por la caracterización de normalidad (teorema 47), concluimos con que $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ no es normal.

Ejercicio (H3.6)**.** Demuestra que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal. Encuentra una extensión normal que contenga $\mathbb{Q}(\sqrt[3]{2})$ como subcuerpo.

Sabemos que no es normal porque sea $p(x) = x^3 - 2 \in \mathbb{Q}[x]$, se puede comprobar que $p(x)$ es irreducible y tiene una raíz en $\mathbb{Q}(\sqrt[3]{2})$ pero no se escinde. Por tanto, por el teorema 47, el cuerpo no es normal.
Una extensión normal que contiene a $\mathbb{Q}(\sqrt[3]{2})$ puede ser $\mathbb{Q}(\sqrt[3]{2}, \omega)$ con $\omega \in \mathbb{C},\ o(\omega) = 3$.

Observación. Si E/K es normal y $f \in K[x]$ no necesariamente irreducible que tiene una raíz en E, f no tiene por que escindirse.

3.3. El grupo de Galois de una extensión

3.3.1. Acción de un grupo

Vamos a ver un repaso de algunos conceptos de la acción de un grupo sobre un conjunto.

Definición 35 (Acción de un grupo)**.** Una **acción** de un grupo $(G, \star)$ sobre un conjunto X es una aplicación: $\phi : G \times X \to X$ que cumple:
1. $\forall x \in X,\ \phi(e, x) = x$ donde e es el elemento neutro del grupo.
2. $\forall x \in X,\ g, h \in G,\ \phi(g \star h, x) = \phi(g, \phi(h \star x))$

Observación.

- El cumplimiento de las dos condiciones hace que la aplicación $\phi(g, \cdot) : X \to X$ sea biyectiva para cada $g \in G$. Con esto se puede dar una definición alternativa de la acción de un grupo:

$$\phi : G \to \{\text{funciones biyectivas } X \to X\}$$

- Una notación alternativa usada para las acciones es:

$$(g, x) \mapsto x \cdot g$$

  Con lo que las dos condiciones se reescriben como:

  1. $x \cdot e = x$, con e el neutro del grupo.
  2. $(x \cdot g) \cdot h = x \cdot (g \cdot h),\ \forall g, h \in G,\ x \in X$

Proposición 48 (Una acción es un homomorfismo)**.** Sea $(G, \cdot)$ un grupo, $\Omega \neq \varnothing$ un conjunto. Si G actúa sobre Ω (lo denotamos por $\Omega^{\curvearrowleft G}$), la aplicación:

$$\rho : G \to S_\Omega;\ g \mapsto f \circ g : \Omega \to \Omega;\ \omega \mapsto \omega \cdot g$$

es un homomorfismo de grupos, en particular $\ker(\rho) \lhd G$. Y tenemos que:

$$G/_{\ker \rho} \simeq \rho(G) \leqslant S_\Omega$$

Recíprocamente, todo homomorfismo $\rho : G \to S_\Omega$ define una acción de G en S_Ω.

Además, sea $(G, \cdot)$ un grupo, $\Omega \neq \varnothing$ un conjunto. Si G actúa sobre Ω ($\Omega^{\curvearrowleft G}$), entonces define una relación binaria de equivalencia (r.b.e) de la forma:

$$\omega \sim \omega' \iff \exists g \in G :\ \omega \cdot g = \omega'$$

Las clases de equivalencia definidas por esta relación se denominan G-órbitas.

Definición 36 (G-órbita de un elemento de un conjunto)**.** Sea G un grupo, la **órbita** de un elemento ω de un conjunto Ω es la clase de equivalencia:

$$\omega^G = \theta_\omega = \{\omega \cdot g \mid \forall g \in G\} \subseteq \Omega$$

Definición 37 (Estabilizador de un elemento de un conjunto)**.** Sea G un grupo, el **estabilizador** de un elemento ω de un conjunto Ω es:

$$G_\omega = \mathrm{St}(\omega) = \{g \in G \mid \omega \cdot g = \omega\} \leqslant G$$

que es un subgrupo de G.

Teorema 49 (Teorema de la Órbita-Estabilizador)**.** Sea G un grupo que actúa sobre Ω y $\omega \in \Omega$ un elemento, entonces la longitud de la G-órbita de ω ($|\theta_\omega| = |G_\omega|$) es:

$$|G_\omega| = |\theta_\omega| = |G : G_\omega|$$

Definición 38 (Puntos fijos por la acción de un grupo)**.** Sea G un grupo y Ω un conjunto.

- Los puntos fijos por la acción de G son los pertenecientes al conjunto:

$$\Omega^G = \{\omega \in \Omega \mid \omega \cdot g = \omega,\ \forall g \in G\}$$

- Los puntos fijos por la acción de $g \in G$ son los pertenecientes al conjunto:

$$\Omega^g = \{\omega \in \Omega \mid \omega \cdot g = \omega\}$$

3.3.2. Grupo de Galois

En esta subsección, vamos a considerar E como una extensión. Además, sea $\mathrm{Aut}(E)$ el conjunto de automorfismos de E, podemos comprobar que $(\mathrm{Aut}(E), \circ)$ es un grupo (no abeliano en general).

El grupo $(\mathrm{Aut}(E), \circ)$, actúa sobre E. $(e \cdot \sigma = \sigma(e) = e)$.

Definición 39 (Grupo de Galois)**.** Sea $\sigma \in \mathrm{Aut}(E)$, $E^\sigma = \{e \in E \mid e\sigma = e\}$ el conjunto de puntos fijos de E por la acción de σ (es subcuerpo de E). Sea E/K una extensión, llamamos **grupo de Galois** de E/K a:

$$\mathrm{Gal}(E/K) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(k) = k \forall k \in K\} = \{\sigma \in \mathrm{Aut}(E) \mid K \subseteq E^\sigma\}$$

Donde además, el *grupo de Galois* es un cuerpo intermedio de E/K.

Proposición 50. Sea L un cuerpo intermedio de E/K, entonces: $\mathrm{Gal}(E/L) \leqslant \mathrm{Gal}(E/K)$. En general $\sigma|_L \notin \mathrm{Gal}(L/K)$.

Observación (Notación)**.** Sea $\sigma \in \mathrm{Gal}(E/K)$, decimos que es un K-automorfismo de E si fija todo K elemento a elemento.

Definición 40 (K-isomorfismo)**.** Sea E/K una extensión, L_1, L_2 cuerpos intermedios, $\sigma : L_1 \to L_2$ es un **K-isomorfismo** si $\sigma : L_1 \to L_2$ es un isomorfismo y $\sigma(k) = k,\ \forall k \in K$.

Con esta notación vamos a reescribir el teorema **??**.

Teorema 51. Sea E/K extensión normal,L_1, L_2 cuerpos intermedios. Si $\sigma : L_1 \to L_2$ es un K-isomorfismo, entonces: $\exists \tau \in \mathrm{Gal}(E/K)$ tal que $\tau|_{L_1} = \sigma$.

Corolario 9 (al teorema 51)**.** Sea E/K una extensión normal, $p \in K[x]$ un polinomio irreducible. Si a y b son raíces de p en E, entonces $\exists \tau \in \mathrm{Gal}(E/K) :\ \tau(a) = b$.

Demostración. Por el corolario 6, existe un K-isomorfismo $\sigma : K(a) \to K(b)$. Por el teorema 51, σ se extiende a $\tau \in \mathrm{Gal}(E/K)$. ♢

Observación. $\mathrm{Gal}(E/K)$ actúa sobre las raíces de $f \in K[x]$ en E.

Teorema 52 (Grupo de Galois y raíces de un polinomio)**.** Sea E/K una extensión, $0 \neq f \in K[x]$, $\Omega = \{a_1, \ldots, a_n\}$ el conjunto de todas las raíces distintas de f en E (no quiere decir que E contenga todas las raíces de f), con $n \leqslant 1$ y sea $L = K(\mathbf{a}) \subseteq E$ un subcuerpo intermedio, entonces:

(a) Si $a \in \Omega$ y $\sigma = \mathrm{Gal}(E/K)$, entonces $\sigma(a) \in \Omega$. En particular, $\sigma|_\Omega \in S_\Omega$ y $\sigma(L) = L$.

(b) La aplicación $\psi : \mathrm{Gal}(E/K) \to \mathrm{Gal}(L/K);\ \sigma \mapsto \sigma|_L$ es un homomorfismo de grupos con $\ker(\psi) = \mathrm{Gal}(E/L) \triangleleft \mathrm{Gal}(E/K)$.

(c) Si E/K es normal, entonces ψ es sobreyectivo. En particular, $\mathrm{Gal}(E/K)\Big/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/K)$.

(d) La aplicación $\rho : \mathrm{Gal}(E/K) \to S_\Omega;\ \sigma \mapsto \sigma|_\Omega$ es un homomorfismo de grupos con $\ker(\rho) = \mathrm{Gal}(E/L)$.

(e) Si E/K es normal y ρ es irreducible, dados $a, b \in \Omega$ existe $\sigma \in \mathrm{Gal}(E/K)$ tal que $\sigma(a) = b$. Por tanto:
$$n = |\mathrm{Gal}(E/K) : \mathrm{Gal}(E/K(a))|$$

Observación (al teorema 52)**.**
$$(\mathrm{Gal}(L/L) = \{id\})$$

En el teorema, (d) aplicado a L/K implica que:
$$\mathrm{Gal}(L/K) \simeq \rho(\mathrm{Gal}(L/K)) \leqslant S_\Omega$$

Demostración.

(a)
$$0 = \sigma(0) = \sigma(f(a)) = \sigma(f)(\sigma(a)) = f(\sigma(a)) \implies \sigma(a) \in \Omega$$
Como:
$$\sigma|_\Omega : \Omega \to \Omega \text{ es inyectiva,}$$
entonces:
$$\Omega \text{ es finita} \implies \sigma|_\Omega \in S_\Omega \text{ es biyectiva,}$$
por tanto:
$$\sigma(L) = \sigma(K(a_1, \ldots, a_n)) = \sigma(K)(\sigma(a_1), \ldots, \sigma(a_n)) = K(a_1, \ldots, a_n) = L$$

(b) Se deja como ejercicio.

(c) Sea $\theta \in \mathrm{Gal}(L/K)$, por el teorema 51, $\exists \sigma \in \mathrm{Gal}(E/K)$ tal que $\sigma|_L = \theta$. En particular, ψ es sobreyectiva. (La segunda conclusión se sigue del teorema de isomorfía).

(d) Se deja como ejercicio partiendo de $\sigma|_\Omega \in S_\Omega$.

(e) Por el corolario 9 si $a, b \in \Omega$ cualesquiera, $\exists \sigma \in \mathrm{Gal}(E/K)$ con $a\sigma = \sigma(a) = b$ y $\theta_a = \Sigma$ por el teorema 49.

♢

Corolario 10 (Caracterización de normalidad a través de isomorfismos)**.** Sea E/K una extensión, L un cuerpo intermedio:

(a) Si L/K es normal entonces $\tau \in \mathrm{Gal}(E/K)$:

$$\tau(L) = L\,(\tau|_L) \in \mathrm{Gal}(L/K)$$

(b) Si E/K es normal:

$$L/K\text{es normal} \iff \forall \tau \in \mathrm{Gal}(E/K),\ \tau(L) = L$$

En particular $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/K)$ y $\mathrm{Gal}(E/K)\Big/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/K)$.

Demostración.

(a) $L = K(f) = K(a_1, \ldots, a_n)$. $f \in K[x] = K(a_1, \ldots, a_n)$. Con $\Omega = \{a_i\}$ todas las raíces distintas entre sí de f en L. Por el teorema 52(a), si $\sigma \in \mathrm{Gal}(E/K)$ $\sigma(L) = L$.

(b) Supongamos E/K normal.

($\Longrightarrow$) Directo de firma análoga al apartado (a).

($\Longleftarrow$) Suponemos que $\tau \in \mathrm{Gal}(E/K)$, $\tau(L) = L$ y queremos probar que L/K es normal. Para ello, usamos el teorema 47.

Sea $p \in K[x]$ irreducible con una raíz $a \in L$m queremos ver que p se escinde en L. Por el teorema 47, p se escinde en E (pues E/K) es normal. Sea $b \in E$ una raíz de p, por el corolario 9, $\exists \tau \in \mathrm{Gal}(E/K)$ tal que $\tau(a) = b$ y además $a \in L \implies b = \tau(a) \in L$.

Como L tiene todas las raíces de p, entonces p se escinde en L. La última parte se demuestra de forma directa aplicando el teorema 52(c).

♢

Observación. Puede parecer que el corolario 10(b) no nos da una caracterización por que requiere estar dentro de una extensión normal, pero si L/K es finita, existe una extensión E/K, $L \subseteq E$, tal que E/K es normal (y es la menor con estas propiedades). E es la *clausura normal* de L/K.

Por ejemplo, sea $L = K(a_1, \ldots, a_n)$ (por ejemplo adjuntando una K-base). Sea $a_i \in L$ es algebraico sobre K. Para constuir E la clausura normal:

$$p_i = Irr(K, a_i),\ f = \prod_{i=1}^{n} p_i,\ \text{entonces } E = K(f)$$

Proposición 53 (Finitud de las extensiones de Galois)**.** Sea L/K una extensión, si L/K es finita entonces $\mathrm{Gal}(L/K)$ es finita.

Demostración. Si L/K es normal, entonces sea $L = K(a_1, \ldots, a_n)$ y $\Omega = \{a_i\}$ todas las raíces distintas entre sí de $f \in K[x]$. Por 52(d), $\mathrm{Gal}(L/K) \leqslant S_\Omega \simeq S_n$, donde S_n es el enésimo grupo simétrico.
Sabemos que $|S_n| = n! \implies (porLagrange)\,|\mathrm{Gal}(L/K)| \mid |S_n| = n!$.

♢

Ejemplo 15 (*Ejemplos de ejercicios de extensiones de Galois*)

1. *Sea* $E = \mathbb{F}_2[x]\Big/\langle x^2+x+1\rangle = \{\bar{0},\bar{1},\bar{x},\bar{x}+\bar{1}\}$, *además* $E/\bar{\mathbb{F}}_2$, *de hecho,* $E = \bar{\mathbb{F}}_2(\bar{x})$. *Comprueba que* $E = \bar{\mathbb{F}}_2(y^2+y+1)$ *y calcula* $\mathrm{Gal}(E/\bar{\mathbb{F}}_2)$.

   Por el lema 43 $\bar{x}$ *es una raíz, y* $y^2+y+1 \in \bar{\mathbb{F}}_2[y]$. *Sabemos además que* y^2+y+1 *tiene como máximo dos raíces distintas en su cuerpo de escisión.*
   $\mathrm{Gal}(E/\bar{\mathbb{F}}_2)$ *manda* $\bar{x}$ *en otra raíz de* y^2+y+1. *Es decir, sea* $\sigma \in \mathrm{Gal}(E/K), f \in K[x], a \in E$ *una raíz de* f, *entonces:*

   $$0 = \sigma(0) = \sigma(f(a)) = \sigma(f)(\sigma(a)) = f(\sigma(a))$$

   Sabemos además que $Frob \in \mathrm{Gal}(E/\bar{\mathbb{F}}_2)$ *donde* $Frob$ *es el automorfismo de Frobenius, ya que fija el cuerpo primo de* E *que es* $\bar{\mathbb{F}}_2$. *Por tanto:*

   $$Frob(\bar{x}) = \bar{x}^2 = \bar{x}+\bar{1} \in E \text{ es otra raíz de } y^2+y+1$$

   Por tanto, $E = \bar{\mathbb{F}}_2(\bar{x}, \bar{x}+\bar{1})$, *es el cuerpo de escisión de* y^2+y+1.

   Para calcular $\mathrm{Gal}(E/\bar{\mathbb{F}}_2)$, *por 52(d):* $\{id, Frob\} = \mathrm{Gal}(E/\bar{\mathbb{F}}_2) \leqslant S_2$ *Donde* $|S_2| = 2 \implies \mathrm{Gal}(E/\bar{\mathbb{F}}_2) = \{id, Frob\} = \langle Frob\rangle$.
2. *Sea* $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.
   (a) $E = \mathbb{Q}(f)$.
   (b) $|E:\mathbb{Q}|$
   (c) *Calcula* $\mathrm{Gal}(E/\mathbb{Q})$.

   Vamos a ver la solución:
   (a) *Las raíces de* f *en* $\mathbb{C}$ *son* $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ *donde:*

   $$\omega = exp\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

   y por tanto:

   $$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$$

   (b) *Sabemos por el teorema 37 que* $\left|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right| = 3$ *y* $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$. *Por tanto:*

   $$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})(\omega) \implies \left|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}\right| = 6$$

   (c) *Sea* $L = \mathbb{Q}(\omega)$, *sabemos que* $\mathbb{Q} \subseteq L \subseteq E$. *Por el teorema 52(d):*

   $$\mathrm{Gal}(E/\mathbb{Q}) \leqslant S_3 \implies |\mathrm{Gal}(E/\mathbb{Q})| \mid 6$$

   Por el teorema 33, sabemos que una $\mathbb{Q}$*-base de* E *es* $\{1, \sqrt[3]{2}, \sqrt[3]{4}\,\sqrt[3]{2}\omega, \sqrt[3]{4}\omega, \omega\}$. *Luego* $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ *queda determinado por* $\tau(\sqrt[3]{2})$ *y* $\tau(\omega)$.
   Las distintas posibilidades de τ *son:*

   $$\tau(\omega) \in \{\omega, \bar{\omega}\} \text{ y } \tau(\sqrt[3]{2}) \in \left\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\bar{\omega}\right\}$$

   Donde con un rápido cálculo combinatorio vemos que hay como mucho 6 posibles τ.

Ejemplo 16 (*Hallar grupo de Galois dado un polinomio y una extensión*)

Sea $f \in \mathbb{Q}[x]$, $f(x) = x^4-2$. *Y sea* $E = \mathbb{Q}(\sqrt[4]{2})$, *entonces el conjunto* Ω *del teorema 52 es* $\Omega = \{\sqrt[4]{2}, -\sqrt[4]{2}\}$. *Sea* $L = \mathbb{Q}(\Omega) = E$, *por el teorema 52(d),* $\mathrm{Gal}(E/\mathbb{Q}) \leqslant S_\Omega \simeq S_2 \implies |\mathrm{Gal}(E/\mathbb{Q})| = 1$ *o* 2 *por el teorema de Lagrange de grupos. Además:*

$$\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Aut}(E) = \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}))$$

Por 6, $\exists K$*-isomorfismo* σ *tal que:*

$$\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(-\sqrt[4]{2}) = E; \quad \sqrt[4]{2} \mapsto -\sqrt[4]{4} \implies \sigma \in \mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma\}$$

Considerando las extensiones:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}) = E & \longrightarrow & E \\ | & & | \\ \mathbb{Q}(\sqrt{2}) = L & \longrightarrow & L \\ | & & | \\ \mathbb{Q} & \longrightarrow & \mathbb{Q} \end{array}$$

Donde la extensión $L/\mathbb{Q}$ es normal pero $E/\mathbb{Q}$ no. Además, sea $\theta : L \to L$; $\sqrt{2} \mapsto \sqrt{2}$ no se extiende a E.

Este ejemplo muestra que la hipótesis E/K normal es necesaria en el teorema 51.

3.4. Extensiones separables

El siguiente teorema y proposición se vieron en el capítulo 1 pero vamos a reescribirlos con el lenguaje actual, es por ello que no se aporta demostración de los mismos.

Teorema 54 (Derivada formal y raíces multiples)**.**
(a) Si $f \in K[x]$ tal que $mcd(f, f') = 1$ y $f' \neq 0$ donde f' es la derivada formal, entonces todas las raíces de f en su cuerpo de escisión son distintas.
(b) Si $f \in K[x]$ irreducible y f' su derivada formal tal que $f' \neq 0$, entonces f es separable.

Observación. Si $\text{car}(K) = 0$ y $f \in K[x]$ con $\delta f > 1$, entonces $f' \neq 0$.

Ejemplo 17 (*Aplicación del contrarrecíproco del teorema 54*)

Sea $f(x) = x^p - 1$, $\text{car}(K) = p$, vemos que $f' = 0$. Entonces no todas las raíces de f en su cuerpo de escisión son distintas, de hecho $f = (x-1)^p$.

Proposición 55 (Multiplicidad de raíces y derivada formal)**.** Sea E/K una extensión, $f \in K[x]$ un polinomio y $a \in E$ tal que $f(a) = 0$, y sea m la multiplicidad de la raíz a, entonces:

$$m > 1 \iff f(a) = 0 = f'(a)$$

Definición 41 (Separabilidad. Polinomios, elementos y extensiones)**.**
(*i*) Sea $f \in K[x]$ un polinomio, decimos que es un **polinomio separable** si todas sus raíces en un cuerpo de escisión son distintas, es decir, $f' \neq 0$ (por el teorema 54).
(*ii*) Sea E/K una extensión, $a \in E$ un elemento algebraico, decimos que a es un **elemento separable** si $p = Irr(K, a)$ es separable.
(*iii*) Sea E/K una extensión algebraica, decimos que es una **extensión separable** si todo $a \in E$ es separable.

Proposición 56 (Divisores irreducibles de un polinomio separable)**.** Sea $f \in K[x]$ un polinomio separable, entonces para todo p irreducible tal que $p \mid f$, p es separable.

Demostración. Si p divide a f quiere decir que todas sus raíces están contenidas en las de f, por tanto, si f es separable, p también lo es. ♢

Proposición 57 (Separabilidad de extensiones intermedios)**.** Sea E/K una extensión separable, y L un cuerpo intermedio, entonces, E/L y L/K son separables.

Demostración. Es fácil ver que L/K es separable. Vamos a ver que E/L es separable.
Sean $a \in E$, $p = Irr(L, a)$. Y sea $q = Irr(K, a)$ que es separable por hipótesis. Como $p \mid q$ (en $L[x]$), sea M un cuerpo de escisión de q sobre L (que sabemos que existe por el teorema 44), entonces q se escinde en $M \implies p$ se escinde en M por $41(ii)$.

Si α, β son raíces de p en M, enotnces α, β son raíces de q en $M \implies \alpha \neq \beta$. ♢

Lema 58 (Separabilidad en cuerpos de característica 0)**.** Todo polinomio $f \in K[x]$ con $\text{car}(K) = 0$ es separable y toda extensión E/K algebraica es separable.

Demostración. Se deja como ejercicio. ♢

Corolario 11 (Separabilidad en cuerpos de característica p)**.** Sea $f \in K[x]$ irreducible con $\text{car}(K) = p$:

$$f(x) \text{ es separable} \iff f \notin K[x^p]$$

Sin embargo el corolario no nos resuelve una pregunta. *¿Podemos encontrar polinomios irreducibles que no sean separables?*, es decir, *¿podemos encontrar un polinomio irreducible en $K[x^p]$?.*

Recordemos que un cuerpo K es perfecto si el monomorfismo de Frobenius es un isomorfismo, es decir, $\varphi = Frob \in \text{Aut}(K)$, donde $\varphi(a) = a^p$.
En particular $\forall b \in K, \exists a \in K$ tal que $a^p = b$

Teorema 59 (Irreducibilidad sobre cuerpos perfectos)**.** Sea K un cuerpo perfecto, todo polinomio irreducible sobre K es separable. En particular, todo polinomio es separable.

Demostración. Sea K perfecto, entonces:

$$\forall b \in K,\ \exists a \in K :\ a^p = b.$$

Sea $f \in K[x]$ irreducible. Sabemos por el corolario 11 que si $f \notin K[x^p]$, entonces f es separable. Supongamos que $f \in K[x^p]$ de la forma:

$$\begin{aligned} f &= b_0 + b_1 x^{pn_1} + \cdots + b_k x^{pn_k} \\ &= a_0^p + \cdots + a_k^p (x^{n_k})^p \\ &= a_0^p + \cdots + (a_k x^{n_k})^p \\ &= (a_0 + \cdots a_k x^{n_k})^p \text{ que no es irreducible} \end{aligned}$$

♢

Ejercicio (H3.16)**.** ¿Cuántas raíces distintas tiene $x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$ en su cuerpo de escisión?

$$\begin{aligned} x^{12} + 2x^6 + 1 &= (x^4)^4 + (-1)^3 (x^2)^3 + 1^3 \\ &= (x^4 - x^2 + 1)^3 \\ &= ((x^2 + 1)^2)^3 = (x^2 + 1)^6 \end{aligned}$$

Sabemos que $x^2 + 1$ es separable por ser $\mathbb{F}_3$ perfecto. Además como es separable es irreducible y por tanto, tiene dos raíces distintas en su cuerpo de escisión.

Ejemplo 18 (*Polinomio irreducible que no es separable*)

Vamos a buscar un polinomio f irreducible que no sea separable. Además por el lema 58 y el teorema 59, tenemos que buscar $f \in K[x]$ tal que $\text{car}(K) = p$ con K no perfecto.
Por ejemplo, si consideramos $K = \mathbb{F}_p$, podemos ver que K no es perfecto ya que $\varphi = Frob \in \text{End}(\mathbb{F}_p(t))$. Por otra parte, $\varphi(\mathbb{F}_p(t)) = \mathbb{F}_(t^p) \subsetneq \mathbb{F}_p(t)$. Vamos a considerar entonces la extensión $\mathbb{F}_p(t)/F_p(t^2)$, donde podemos ver que $\left|\mathbb{F}_p(t) : \mathbb{F}_p(t^2)\right| = p$ pues tenemos que t es raíz de $x^p - t^p \in \mathbb{F}_p(t^p)[x]$.

Tenemos que ver ahora que $x^p - t^p = (x - t)^p$ es irreducible. En otro caso, $x^p - t^p = g(x) \cdot h(x)$, con

$\delta g,\ \delta h \leqslant p$. Por tanto:

$$g(x) = (x-t)^n \text{ con } 0 < n < p$$

Lo que es imposible por que el término independiente de g es t^n que no pertenece a $\mathbb{F}_p(t^p)$. Luego $Irr(\mathbb{F}_p(t^p), t) = x^p - t^p$.

Proposición 60 (Raíces comunes y polinomios irreducibles mónicos)**.** Sean $p \neq q \in K[x]$ irreducibles mónicos, entonces p y q no pueden tener una raíz en común.

Demostración. Sea E/K una extensión y $\alpha \in E$ la raíz común de p y q, entonces $p = Irr(K, \alpha) = q$ por la unicidad del polinomio mónico.

Otra forma de verlo es recordar que sean $f, g \in K[x]$ entonces $mcd_K(f,g) = mcd_E(f,g)$. Si α es una raíz común entonces $p \mid q$ y además $(x-\alpha) \mid mcd(p,q) > 1 \implies q \mid p$ y por tanto $p = q$. ♢

Ejercicio (H3.??)**.** Calcular las raíces distintas de $f \in K[x]$ separables en su cuerpo de escisión.

Vamos a dar un esquema de la resolución del ejercicio:

1. Descomponer f es factores irreducibles:

   $$f = a p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \text{ donde los } p_i \text{ son irreducibles y distintos entre sí.}$$

2. Por definición (por ser separable) cada p_i es separable y además el número de raíces de p_i coincide con δp_i.
   Con esto vemos que el número de raíces distintas de f es igual a $\sum \delta p_i$.

Definición 42 (Elemento primitivo)**.** Sea E/K una extensión simple, a un elemento de $\gamma \in E$ se le denomina **elemento primitivo** si $E = K(\gamma)$.

Teorema 61 (del Elemento Primitivo)**.** Toda extensión finita y separable es simple.

Demostración. Se proporciona un esquema de la demostración. Sea E/K finita y separable, entonces $E = K(\alpha_1, \dots, \alpha_n)$ con α_i algebraicos y separables.

- Por inducción sobre n, basta probar el resultado cuando $n = 2$, con $n = 1$ habríamos terminado pues $E = K(\alpha_1)$ y por tanto sería simple. Vamos a considerar el caso $n > 1$, es decir $L = K(\alpha_1, \dots, \alpha_{n-1})$. Por inducción $L = K(\alpha)$ y entonces $E = K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \alpha_{n-1})(\alpha) = K(\alpha)(\alpha_n) = K(\alpha, \beta)$
- Queremos probar que $K(\alpha, \beta)/K$ es simple. Esta parte es constructiva. Habría que conectar separabilidad y normalidad.

♢

Proposición 62 (Irreducibilidad y acción del grupo de Galois)**.** Sea $f \in K[x]$ un polinomio, $E = K(f)$ y $G = \mathrm{Gal}(E/K)$. Entonces:

1. Si f es irreducible, G actúa transitivamente (la acción define una sola G-órbita) sobre el conjunto Ω de raíces de f.
2. Si f no tiene raíces múltiples en E y G actúa transitivamente sobre Ω, entonces f es irreducible.

Demostración.

1. Se sigue inmediatamente del corolario 9.
2. Sea $f = a p_i \dots p_r$ con p_i primos irreducibles. Supongamos que $r > 1$, sea $\alpha \in E$ raíz de p_1, $\beta \in E$ raíz de p_2. Por hipótesis $\exists \sigma \in G$ tal que $\alpha \cdot \sigma = \sigma(\alpha) = \beta$. Entonces:

   $$0 = \sigma(p_1(\alpha)) = \sigma(p_1)(\sigma(\alpha)) = p_1\beta \implies Irr(K,\alpha) = p_1 = Irr(K,\beta) = p_2$$

♢

Teorema 63 (Numero de extensiones de un isomorfismo)**.** Sea $\sigma : K_1 \to K_2$ un isomorfismo, $f_1 \in K_1[x]$, $f_2 = \sigma(f_1) \in K_2[x]$ polinomios y $E_i = K(f_i)$ extensiones. Entonces:
(a) σ se extiende a un isomorfismo $\tau : E_1 \to E_2$. (Teorema 59).
(b) Si f_1 es separable entonces hay exactamente $|E_1 : K_1|$ extensiones como en (a).

Demostración.

(a) Teorema 59.

(b) Por inducción sobre $|E_1 : K_1|$.

- $|E_1 : K_1| = 1 \iff g_1$ se escinde en $E_1 \iff f_2$ se escinde en $E_2 \iff |E_2 : K_2| = 1 \implies \tau = \sigma$
- Podemos suponer que $|E_1 : K_1| > 1$, entonces:

$$f_1 = p_1 g_1 \in K_1[x], \text{ donde } p_1 \text{ es irreducible y } \delta p_1 = d \geqslant 2.$$

por tanto:

$$f_2 = p_2 g_2, \text{ donde } p_2 = \sigma^\star(p_1) \text{ es irreducible y } \delta p_2 = \delta p_1 = d \geqslant 2.$$

Como f_1 es separable, entonces p_1 es separable (por la proposición 56). Como $E_1 = K_1(f_1)$, entonces p_1 se escinde en E_1 (por el lema 41(ii)). Ahora, desarrollando:

$$\begin{aligned} p_1(x) &= (x-\alpha_1)\cdots(x-\alpha_d) \in E_1[x] \\ \text{Por (a)} \exists \tau : E_1 \to E_2 : \ & \tau|_{K_1} = \sigma \\ p_2 = \tau^\star(p_1) &= (x-\tau(\alpha_1))\cdots(x-\tau(\alpha_d)) \\ \beta_j = \tau(\alpha_j) &\text{ donde las } \beta_j \text{ son las raíces distintas de } p_2 \text{ en } E_2. \end{aligned}$$

y por tanto p_2 es spearable.

Sea $\alpha = \alpha_1$, por el teorema 40, para cada $j = 1, \ldots, d$, existe un isomorfismo:

$$\hat{\sigma} : K_1(\alpha) \to K_2(\beta_j)$$

que extiende a σ. Como:

$$|E_1 : K_1(\alpha_1)| = \frac{|E_1 : K_1|}{|K_1(\alpha) : K_1|} = \frac{|E_1 : K_1|}{d} < |E_1 : K_1|\,.$$

Por inducción, para cada $j = 1, \ldots, d$, existen $|E_1 : K_1|$ extensiones exactamente de $\hat{\sigma}_j$.
Es fácil ver que tenemos $\frac{|E_1:K_1|}{d} \cdot d$ extensiones de σ a $E_1 \to E_2$. ¿Por qué son todas?.

Si $\tau : E_1 \to E : 2$ extiende a σ, en particular τ manda σ en una raíz de $\tau^\star(p_1) = \sigma^\star(p_1) = p_2$. Es decir, $\tau(\alpha) = \beta_j$ luego, $\tau|_{K_1(\alpha)} = \hat{\sigma}_j$. Por tanto, σ tiene exactamente $|E_1 : K_1|$ extensiones a $E_1 \to E_2$.

♢

Definición 43 (Extensión de Galois)**.** Sean E, K cuerpos, diremos que la extensión E/K es una **extensión de Galois** si E/K es normal y separable.

Observación. Si la extensión E/K es de Galois, y sea L un cuerpo intermedio, entonces E/L es una extensión de Galois.

Corolario 12. Sea E/K una extensión de Galois, y $K \subseteq L \subseteq E$, L/K es una extensión de Galois. Además, cada $\sigma \in \mathrm{Gal}(L/K)$ tiene exactamente $|E : L|$ extensiones a $\mathrm{Gal}(E/K)$. En particular:

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

Demostración. Consecuencia del teorema 63. Los detalles se dejan como ejercicio. ♢

Ejercicio (Ejercicio)**.** Sea ξ la raíz primitiva quinta de **1**. Demuestra o calcula:

(a) $\mathbb{Q}(\xi)/\mathbb{Q}$ es normal.

(b) $|\mathbb{Q}(\xi) : \mathbb{Q}|$.

(c) $\mathrm{Gal}\mathbb{Q}(\xi)/\mathbb{Q}$.

Solución:

(a) ξ es raíz de $x^5 - 1$ y las raíces de $x^5 - 1$ son $\{1, \xi, \xi^2, \xi^3, \xi^4\}$, que son las raíces del quinto polinomio ciclotómico. Entonces $\mathbb{Q}(\xi) = \mathbb{Q}(x^5 - 1)$. Por tanto, el polinomio irreducible $Irr(\mathbb{Q}, \xi) = \phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

(b) $|\mathbb{Q}(\xi) : \mathbb{Q}| = \delta\phi_5(x) = 4$

(c) Sabemos que $\mathbb{Q}(\xi)/\mathbb{Q}$ es una extensión de Galois, (es normal por (a) y separable por que $\mathrm{car}(\mathbb{Q}) = 0$). Además:

$$|\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})| = 4, \text{ (usando el teorema 52(d) sabemos que } \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \leqslant S_4)$$

Por el corolario 9, para $j = 1, 2, 3, 4$ sabemos que $\exists \sigma_j \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ tal que $\sigma_j(\xi) = \xi^j$, donde $\sigma_1 = id$. Y además, un $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \{id, \sigma_2, \sigma_3, \sigma_4\}$ está determinado por la imagen de ξ. De hecho, $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \langle \sigma_2 \rangle \simeq C_4$.

3.5. Cuerpos finitos

Vamos a empezar con un recordatorio de *Teoría de Grupos*.

Definición 44 (Orden del elemento de un grupo)**.** Sea G un grupo finito, $g \in G$ un elemento, decimos que el **orden** de g es:

$$o(g) = n = \min\{m \mid g^m = 1\} < \infty$$

Teorema 64 (Resultados de orden en un grupo)**.** Sea G un grupo finito, $g \in G$ un elemento del grupo:
(a) $g^m = 1 \iff o(g) \mid m$.
(b) $o(g) \mid |G|$. En particular $g^{|G|} = 1$.
(c) Si $o(g) = n$, entonces $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ y $\langle g \rangle = \langle g^k \rangle \iff mcd(g, k) = 1$.
(d) G es cíclico $\iff \exists g \in G : \ o(g) = |G|$.

Observación. Sea K un cuerpo finito y F su cuerpo primo. Entonces:

$$F \simeq \mathbb{F}_p \text{ y además } |K : F| = n$$

$$K \simeq F^n \simeq \mathbb{F}_p^n \implies |K| = p^n$$

Teorema 65 (Clasificación de cuerpos finitos)**.**
(a) Para cada primo p y natural n, existe un cuerpo $|E| = p^n$.
(b) Dos cuerpos E y L con el mismo número de elementos son isomorfos.

Observación.

$$\mathbb{F}_{p^n} = GF(p^n)$$

Demostración.

(a) Sea $F = \mathbb{F}_p$ y $f(x) = x^{p^n} - x \in F[x]$, entonces $E = F(f)$ (por el teorema 44).
Sea U el conjunto de raíces de f en E, y como $f'(x) = -1$, entonces $mcd(f, f') = 1$. Por el teorema 54(a), obtenemos que $|U| = p^n$.

1. $F \subseteq U$ ya que $\forall a \in F$ tenemos que $a^p = a$ (por el pequeño teorema de Fermat).
2. U es un cuerpo:

$$\alpha, \beta \in U \text{ consideramos } \alpha^{p^n} = \alpha, \beta^{p^n} = \beta$$
$$(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$$
$$\text{Si } \beta \neq 0 \implies \frac{\alpha^{p^n}}{\beta^{p^n}} = \frac{\alpha}{\beta}$$

Y por tanto, $F \subseteq U \subseteq E = F(U) \implies E = F(U) = U$.

(b) Supongamos que L es otro cuerpo con $|L| = p^n$. Sea $D \subseteq L$ su cuerpo primo, $D \simeq \mathbb{F}_p \simeq F$. Ahora $L^\times = \mathcal{U}(L)$ es un grupo de $p^n - 1$ elementos. En particular si $l \in L^\times$, entonces $l^{p^n-1} = 1$. (por 64(b)) $\implies l^{p^n} = l$. Es decir, L es un cuerpo de escisión de $f(x) = x^{p^n} - x$. Entonces tenemos el diagrama (que demuestra el isomorfismo):

$$\begin{array}{ccc} E = F(f) & \longrightarrow & L = D \\ | & & | \\ F & \xrightarrow{\simeq} & D \end{array}$$

con $f(n) = x^{p^n} - x$.

♢

Observación. Sea K un cuerpo finito, y F su cuerpo primo, como consecuencia del teorema 65, K/F es una extensión de Galois y si $|K : F| = n$ entonces $|\mathrm{Gal}(K/F)| = n$.

Definición 45 (Exponente de un grupo)**.** Sea G un grupo finito, definimos el **exponente** de G como:

$$\exp(G) = \mathrm{mcm}\,\{o(g) \mid g \in G\}$$

que es el menor entero e tal que:

$$g^e = 1, \ \forall g \in G$$

Observación.

$$\exp(G) \mid |G|$$

Ejemplo 19 (*Ejemplos de exponentes de un grupo*)

- $\exp(C_2 \times C_2) = \mathrm{mcm}\,\{1, 2\} = 2$ *Donde* $C_2 \times C_2 = \langle a \rangle \times \langle b \rangle = \{1, a, b, ab\}$ *y tanto* $o(a) = o(b) = o(ab) = 2$.
- $\exp(C_2 \times C_3) = \mathrm{mcm}\,\{1, 2, 3, 6\} = 6$. *Donde* $C_2 \times C_3 = \langle c \rangle \times \langle d \rangle = \{1, c, d, d^2, cd, cd^2\}$ *y* $o(cd^2) = o(cd) = 6$.
- $\exp(S_3) = \mathrm{mcm}\,\{1, 2, 3\} = 6$ *Donde* S_3 *es el grupo simétrico de elementos hasta* $3 -$ *ciclos.*

En los dos primeros casos, existe un elemento cuyo orden es el mismo que el exponente del grupo, sin embargo esto no ocurre en general. Veremos que solo ocurre cuando el grupo es abeliano.

Lema 66 (Orden de elementos que conmutan entre sí)**.**

1. Sea $H = \langle h \rangle$ cíclico y $|H| = n = o(h)$, para cada $d \mid n$ existe un elemento $g \in H$ tal que $d = o(g)$.
2. Sean $g_i, g_j \in G$, si g_i conmuta con g_j ($g_i g_j = g_j g_i$), entonces $o(g_i g_j) \mid o(g_i)o(g_j)$. Si además, $o(g_i) \cdot o(g_j) = 1 \implies o(g_i g_j) = o(g_i)o(g_j)$

Demostración. Se deja como ejercicio. ♢

Lema 67 (Existencia de un elemento de orden el exponente de un grupo)**.** Sea G finito y abeliano, entonces $\exists g \in G$ tal que $o(g) = \exp(G)$.

Demostración. Sea $e = \exp(G) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con p_i primos y distintos entre sí y $\alpha_i \geqslant 1$. Por definición de exponente, para cada j existe $h_j \in G$ tal que $p_j^{\alpha_j} \mid o(h_j)$.
Por el lema 66(1), $\exists g_j \in G$ tal que $o(g_j) = p_j^{\alpha_j}$. Tomamos:

$$g = \prod_{j=1}^{r} g_j \in G, \quad \text{y por el lema 66(2) } o(g) = e$$

♢

Teorema 68 (Subgrupo multiplicativo y subgrupo cíclico)**.** Sea K un cuerpo y $G \leqslant K^\times$ un subgrupo finito, entonces G es cíclico. Enunciado informalmente:

Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico

Demostración. Por el teorema 64(d), queremos encontrar $g \in G$ tal que $o(g) = |G|$.
Como $K^\times$ es abeliano y $G \leqslant K^\times$, entonces G es abeliano (y finito por hipótesis). Sea $e = \exp(G)$, $\forall h \in G,\ h^e = 1$, entonces todo elemento $h \in G$ es raíz del polinomio $x^e - 1 \in K[x]$. Por tanto:

$$|G| \leqslant e \leqslant |G| \text{ pues } e \mid |G| \implies e = |G|$$

Por el lema 67, $\exists g \in G$ tal que $o(g) = e = |G|$. ♢

Observación. Sea K un cuerpo finito, en particular $K^\times$ es cíclico, luego $\exists \xi \in K\ :\ \langle \xi \rangle = K^\times$.

Ejercicio (H3.19)**.** Sea $E = \mathbb{F}_3[x] \Big/ \langle x^2 + 1 \rangle$ (en particular $x^2 = -1 = 2$), halla un generador de $E^\times$.

Solución
Vemos que:

$$E = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\},\ |E| = 9,\ \left|E^\times\right| = 8$$

Buscamos un elemento $g \in E^\times$ tal que $o(g) = 8$. No hay un método general, solo ensayo y error.
Vamos a probar algunos casos:

(x)

$$x^1 = x,\ x^2 = 2,\ x^3 = x \cdot x^2 = 2x,\ x^4 = 2 \cdot 2 = 1 \implies o(x) = 4 \implies x \text{ no es un generador.}$$

$(x+1)$

$$\begin{aligned}
(x+1)^1 &= x + 1 \\
(x+1)^2 &= x^2 + 2x + 1 = 2x \\
(x+1)^3 &= 2x(x+1) = 2x^2 + 2x = 2x + 1 \\
(x+1)^4 &= (2x)^2 = x^2 = 2 \\
(x+1)^5 &= 2x + 2 \\
(x+1)^6 &= 2(2x) = x \\
(x+1)^7 &= x(x+1) = x^2 + x = x + 2 \\
(x+1)^8 &= (x+2)(x+1) = x^2 + 2 = 1
\end{aligned}$$

Ejercicio extra
Halla o calcula:

1. $E/\mathbb{F}_3$ es simple.
2. E es el cuerpo de escisión de y^2+1 sobre $\mathbb{F}_3$.
3. E es el cuerpo de escisión sobre $\mathbb{F}_3$ de cualquier polinomio irreducible de grado 2 en $\mathbb{F}_3[x]$.

Solución

1. Hemos visto que $\exists \xi \in E$ tal que $\langle \xi \rangle = E^\times$. Entonces $\left\{\xi, \xi^2, \ldots, \xi^n\right\} \subset E = \mathbb{F}_3(\xi)$ y por tanto $E/\mathbb{F}_3$ es simple.

Corolario 13 (Teorema del Elemento Primitivo sobre cuerpos finitos)**.** Sea E/K una extensión finita sobre un cuerpo finito K, entonces E/K es simple.

Demostración. Aunque en el teorema del Elemento Primitivo (teorema 61) se pide que la extensión sea separable, en el corolario no hace falta pedirlo.
Como K es finito, entonces K es perfecto y cualquier extensión algebraica sobre un cuerpo finito es automáticamente separable. Además, E/K es algebraica por ser finita (36). Para ver que es finito:

$$|E| = |K|^{|E:K|} < \infty, \implies E \text{ es finito}$$

Además por el teorema 68, $\exists \xi \in E : \langle \xi \rangle = E^\times \implies K(\xi) = E$. ♢

Ejercicio (H3.19)**.** Demuestra que para cada primo p y cada natural $n \in \mathbb{N}$ positivo, existe un polinomio irreducible $f \in \mathbb{F}_p[x]$ de grado n.

Solución
Por el teorema 65(a), $\exists$ un cuerpo E tal que $|E| = p^n$. Sea $F \subseteq E$ su cuerpo primo, $F = \mathbb{F}_p$. Por 13 $\exists \xi \in E$ tal que $E = \mathbb{F}_p(\xi)$.
Por el teorema 37:

$$n = |E : \mathbb{F}_p| = \delta Irr(\mathbb{F}_p, \xi) = \delta f(x)$$

con lo que f es un irreducible de grado n.

Ejercicio (H3.9)**.** Sea $E = \mathbb{Q}(\sqrt[4]{2})$, $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$. Comprueba que E/K no es normal.

Solucion
Sabemos que E/L y L/K son extensiones normales, ya que $E = L(x^2 - \sqrt{2}) = L(\pm\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$ y $L = K(x^2-2) = \mathbb{Q}(\pm\sqrt{2})$. Sin embargo, E/K no es normal porque el polinomio irreducible sobre K (x^4-2) tiene dos raíces en E pero no se escinde en E. (teorema 47)

Ejercicio (Ejercicio de examen)**.** Sea $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Determina:

(a) $E = \mathbb{Q}(f)$.

(b) $|E : Q|$.

(c) $\alpha \in E$ tal que $\mathbb{Q}(\alpha) = E$.

(d) Decide si $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$; $\sqrt{2} \mapsto -\sqrt{2}$ se puede extender a un isomorfismo de $\mathbb{Q}(\sqrt[4]{2})$ o de E.

Solución

(a) Las raíces de f son $\left\{\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i\right\}$ entonces $E = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

(b) Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(i), \mathbb{Q}(\sqrt[4]{2}) \subseteq E$. Vamos a hallar el grado de la extensión $E/\mathbb{Q}(\sqrt[4]{2})$, que resulta ser $2 = \delta Irr(\sqrt[4]{2}, i) = \delta(x^2+1)$.
Por otra parte calculamos $\delta Irr(\mathbb{Q}, \sqrt[4]{2}) = \delta(x^4-2) = 4$. Por tanto:

$$|E : Q| = 2 \cdot 4 = 8$$

(c) Hay dos formas:

1. Usando la demostración del Teorema del Elemento Primitivo (TEP) en el caso infinito: $E = \mathbb{Q}(i = \alpha, \sqrt[4]{2} = \beta)$, entonces

$$\alpha_1 = i, \alpha_2 = -i, \beta_1 = \sqrt[4]{2}, \beta_2 = -\sqrt[4]{2}, \beta_3 = \sqrt[4]{2}i, \beta_4 = -\sqrt[4]{2}i$$

. Tenemos que escoger $c \in \mathbb{Q}$ tal que:

$$c \neq \frac{\beta - \beta_j}{\alpha - \alpha_2} \text{ con } j \in \{1,2,3,4\}, \ \beta = \beta_1, \ \alpha = \alpha_1$$

podemos ver que $c = -1$ funciona. Por la prueba del TEP:

$$E = \mathbb{Q}(c\alpha - \beta) = \mathbb{Q}(-\alpha - \beta) = \mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\sqrt[4]{2} + i)$$

2. Usando todo lo que hemos visto: Sea $L = \mathbb{Q}(i)$, sabemos por el apartado (b) de este ejercicio que $|E : Q| = 8$, y además, $|L : \mathbb{Q}| = 2$ por lo que $|E : L| = 4 \implies x^4 - 2$. Sea $\alpha = \sqrt[4]{2} + i \in E$, por el teorema del elemento algebraico queremos ver que $\delta Irr(\mathbb{Q}, \alpha) = 8$.

   Además, $Irr(L, \sqrt[4]{2}) = x^4 - 2 = f$, y por tanto $p(x) = (x-i)^4 - 2 = f(x-i)$ donde α es una raíz de $p \in L[x]$, $p \notin \mathbb{Q}[x]$. Por el ejercicio H1.32(a), p es irreducible sobre L, es decir, $p(x) = (x-i)^4 - 2 = Irr(L, \alpha)$.

(d) Recordamos que si E/K es normal, y M/K es normal con $K \subseteq M \subseteq K$, entonces todo $\sigma \in \text{Gal}(M/K)$ se puede extender a $\text{Gal}(E/K)$ (Teorema 52 y corolario 10).

Sea $M = \mathbb{Q}(\sqrt[4]{2})$, podemos ver que $E/\mathbb{Q}$ es normal, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ también lo es, pero $M/\mathbb{Q}$ no es normal. Por tanto, σ no se puede extender a un isomorfismo de M. Podemos ver por reducción al absurdo:
Sea $\tau : M \to M$ una extensión de sigma, entonces $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$ o $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$ ya que τ lleva raíces sobre $\mathbb{Q}$ en raíces sobre $\mathbb{Q}$ entonces:

$$-\sqrt{2} = \sigma(\sqrt{2}) = \tau(\sqrt{2}) = \tau((\sqrt[4]{2})^2) = \tau(\sqrt[4]{2})^2 = \pm\sqrt{2}$$

y llegamos a una contradicción.

Para ver que σ se extiende a un isomorfismo ω de E basta aplicar el corolario 10, ya que las dos extensiones $(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ y $E/\mathbb{Q}$ son normales).
Para verlo de otra forma, sea $\omega \in \text{Gal}(E/\mathbb{Q})$ tal que $\omega(\sqrt[4]{2}) = \sqrt[4]{2}i$ (sabemos que existe uno por que tanto $\sqrt[4]{2}$ como $\sqrt[4]{2}i$ son raíces del mimso polinomio irreducible) entonces:

$$\omega(\sqrt{2}) = \omega((\sqrt[4]{2})^2) = \omega(\sqrt[4]{2})^2 = (\sqrt[4]{2}i)^2 = -\sqrt{2} = \sigma(\sqrt{2})$$

Ejercicio (H3.10)**.** Todas las afirmaciones de este ejercicio son ciertas.

(f) Sean E/L y L/K extensiones normales. Si todo $\sigma \in \text{Gal}(L/K)$ se extiende a E ($\text{Gal}(E/K)$) entonces E/K es normal.

Nota
Este resultado se puede usar para ver que $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ con $\sigma(\sqrt{2}) = -\sqrt{2}$ no se puede extender a $M = \mathbb{Q}(\sqrt[4]{2})$, por que si no $M/\mathbb{Q}$ sería normal y ya vimos que no lo es.

Ejercicio (H3.4)**.** Sea $K = \mathbb{F}_2[y]\Big/ y^3 + y + 1$, comprueba que es un cuerpo de escisión de $x^3 + x + 1$ y $x^3 + x^2 + 1$.

Solución
Podemos ver que $K = \{0, 1, y, y+1, y^2, y^2+1, y^2+y, y^2+y+1\}$. Por el lema 43, sabemos que $y \in K$ es raíz de $x^3 + x + 1$. También sabemos que si $\sigma \in \mathrm{Gal}(K/\mathbb{F}_2)$ entonces $\sigma(y)$ es raíz de $x^3 + x + 1$.
Tomamos $\varphi = Frob \in \mathrm{Gal}(K/\mathbb{F}_2)$ y $\varphi^2 \in \mathrm{Gal}(K/\mathbb{F}_2)$. Entonces $\varphi(y) = y^2$ es otra raíz, y $\varphi^2(y) = \varphi(y^2) = y^4 = y \cdot y^3 = y^2 + y$.
Sabemos que $x^3 + x + 1$ y $x^3 + x^2 + 1$ no comparten raíces en K. Comprobamos que $y + 1$ es raíz de $x^3 + x^2 + 1$ y vemos que $\varphi(y+1) = y^2 + 1$ y $\varphi(y^2 + 1) = y^2 + y + 1$ por lo que claramente $\mathbb{F}_2(y) = K$ y $\mathbb{F}_2(y+1)$

Ejercicio (H3.15)**.** ¿Cuántas raíces tiene distintas $f(x) = x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$ en su cuerpo de escisión?

Solución
Empezamos comprobando si tiene raíces en $\mathbb{F}_3$.

$$f(0) = 0 + 0 + 1 \neq 0$$
$$f(1) = 1 + 2 + 1 \neq 0$$
$$f(2) = 1 + 2 + 1 \neq 0$$

Y vemos que no, sin embargo esto no quiere decir que el polinomio sea irreducible. De hecho, como $f(x) \in \mathbb{F}_3[x^3]$ es reducible. Usando un poco la intuición podemos observar que $f(x)$ es el desarrollo del producto notable:

$$f(x) = (x^6 + 1)^2$$

Sin embargo, este polinomio sigue sin ser irreducible, ya que $x^6 + 1 \in \mathbb{F}_3[x^3]$. Además como estamos en un cuerpo de característica p, sabemos que $(x^k + 1)^p = x^{k \cdot p} + 1$ por que los términos intermedios tienen todos un coeficiente que es múltiplo de 3. Por tanto:

$$f(x) = x^{12} + 2x^6 + 1 = (x^6 + 1)^2 = ((x^2 + 1)^3)^2 = (x^2 + 1)^6$$

Ahora consideramos $g(x) = x^2 + 1$, como $g(x)$ es irreducible sobre $\mathbb{F}_3$, sabemos que $\mathbb{F}_3(g)/\mathbb{F}_3$ es una extensión separable y por tanto $g(x)$ tiene dos raíces distintas en su cuerpo de escisión lo que implica que f también.

Por otra parte, si queremos hallar la descomposición de f en el cuerpo de escisión, consideramos $\mathbb{F}_3[t]\Big/\langle t^2 + 1\rangle = \mathbb{F}_3[t]\Big/\langle g(t)\rangle$ que es un cuerpo con $9 = |\mathbb{F}_3| \cdot \delta(t^2 + 1)$ elementos. Ahora tendremos que ver que raíces del polinomio $\mathbb{F}_3[x]$ están presentes en $\mathbb{F}_3[t]\Big/\langle t^2 + 1\rangle$.

$$\mathbb{F}_3[t]\Big/\langle t^2 + 1\rangle = \{0, 1, 2, t, 1 + t, 2 + t, 2t, 1 + 2t, 2 + 2t\}$$

Como estamos cocientando por $t^2 + 1$, sabemos que $t^2 + 1 = 0 \implies t^2 = -1$ y por tanto t es raíz de $x^2 + 1$. Además, $(2t)^2 = 4t^2 = -1$ y por tanto también es raíz de $x^2 + 1$. Entonces podemos descomponer de la forma:

$$x^2 + 1 = (x - t) \cdot (x - 2t)$$

Por tanto, tendríamos:

$$f(x) = (x - t)^6 (x - 2t)^6$$

Ejercicio (H3.18)**.** Sea $f(x) = x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$. Demuestra que:

(a) Cualquier polinomio $g(x)$ irreducible en $\mathbb{F}_p[x]$ de grado n divide a f.

(b) El grado de todos los factores irreducibles de f divide a n.

Solución

(a) Sabemos que por ser $f(x)$ irreducible de grado q entonces:

$$K = \mathbb{F}_p(f) \simeq \mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$$

entonces $f(x) = \prod_{i=1}^{q}(x - \alpha_i)$.
Por el teorema de Kronecker (lema 43), sabemos que $L = \mathbb{F}_p[t]\Big/\langle g \rangle$ es una extensión de $\mathbb{F}_p$ de grado n, que contiene una raíz de $g \in L[x]$. Además, L contiene $p^{\delta(g)} = p^n = q$ elementos y por tanto es isomorfo a K (por el teorema 65).
También sabemos que existe un isomorfismo que fija $\mathbb{F}_p$ y por tanto, como g no cambia por el isomorfismo, también tiene una raíz en K. Es decir, $\exists \alpha K$ con $(x - \alpha) \mid g(x)$.
Sabemos que $(x - \alpha) \mid g(x)$ y $(x - \alpha) \mid f(x)$ lo que quiere decir que $(x - \alpha) \mid mcd_{K[x]}(f, g) = mcd_{\mathbb{F}_p[x]}(f, q)$ y como $g(x)$ es irreducible, entonces $g(x) \mid f(x)$.

(b) Sea $g \in \mathbb{F}_p[x]$ factor irreducible con $\delta(g) = d$. Sea $K = \mathbb{F}_p(f)$. Como f se escinde en K es obvio que g se escinde en K. Sea α una raíz cualquiera de g. Vamos a construir un cuerpo intermedio L de forma $\mathbb{F}_p \subseteq L = \mathbb{F}_p(\alpha) \subseteq K$. Sabemos que $|K : \mathbb{F}_p| = n$, y que por la elección de α, $|L : \mathbb{F}_p| = d$. Entonces por transitividad de grados:

$$\delta(g) = d \mid n$$

Parte III

Apéndices

Capítulo 4

Índices

Lista de definiciones

Lista de teoremas

Lista de ejemplos

Lista de ejercicios