TEORÍA DE GALOIS

APUNTES DEL CURSO 2019-2020 IMPARTIDO POR CAROLINA VALLEJO

Rafael Sánchez

Revisión del 16 de octubre de 2019 a las 15:46.

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:

   $$p(x) = a_0 + a_1x + \ldots + a_nx^n$$

   Donde llamamos *coeficientes* del polinomio a los a_i.

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

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

3. Sea $p \in R[x] = a_0 + a_1x + \ldots + a_nx^n$, llamamos *coeficiente director* al coeficiente del término de mayor grado (a_n).

4. Sea $p \in R[x] = a_0 + a_1x + \ldots + a_nx^n$, 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.

- $(\implies)$
$$R \text{ cuerpo} \implies \mathcal{U}(R) = R^\times \implies I = \mathcal{U}(R) \cup \{\mathbf{0}\} \text{ o trivialmente } I = \{\mathbf{0}\}$$

- $(\impliedby)$
Sea $a \in R^\times$, $a \in \langle a \rangle \leqslant R$
$$\{\mathbf{0}\} \neq I = \langle a \rangle, \text{ entonces } I = R \implies \exists u \in I \cap \mathcal{U}(R) \neq \varnothing \implies u \in \langle a \rangle \implies u = a \cdot r, \text{ con } r \in R$$
y por tanto:
$$1 = u \cdot u^{-1} = a \cdot r \cdot u^{-1} \implies a \in \mathcal{U}(R) \implies R \text{ es un cuerpo}$$

$\diamondsuit$

Ejemplo 3 (*Ejemplos de ideales*)

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

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

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 $\mathrm{mcd}(k, n) = 1$, 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 $\mathbb{Z}/n\mathbb{Z}$.
- $(\implies)$

  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:

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

  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 $\mathbb{Z}[i]\big/\langle 2i \rangle$?¿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:

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

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.

$\diamondsuit$

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 $n - 1 \leqslant \delta(d) = \delta(f) - 1 \implies n \leqslant \delta(f)$

$\diamondsuit$

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 $f = pd \implies f \in \langle p \rangle$. $\diamondsuit$

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 $E[x] \implies mcd_E(f, g) = mcd_K(f, g) > \implies f \mid g$.

$\diamondsuit$

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. $\diamondsuit$

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

$$f(x) = ap_1(x) \cdot \dots \cdot p_r(x),\ a \in K^{\times},\ p_i \text{ irreducibles mónicos no necesariamente distintos}$$

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

Demostración. Se deja como ejercicio. $\diamondsuit$

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. $\diamondsuit$

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, $\{\pm1, \pm2, \pm3, \pm6\}$ 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 $f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m \cdot g'(x)$.

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

$\Longleftarrow$ $0 = f'(a) = m \cdot 0^{m-1} \cdot g(a) \Longrightarrow m > 1$. $(g(a) \neq 0)$. 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. $mcd(f, f') = 1 \Longrightarrow f$ no tiene raíces múltiples en E.
2. Si f es irreducible, entonces f no tiene raíces múltiples en E.

Demostración.

1. $mcd(f, f') = 1 \Longrightarrow \exists g, h \in K[x] : \ 1 = fg + hf'$. 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:

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

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. $\diamondsuit$

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.

$\Longrightarrow$ 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 $k \in K \implies e = k^{-1} \implies e \in K \implies E = K$.

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

$\diamondsuit$

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.

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

$\diamondsuit$

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 $K \simeq F^n \implies |K| = |F|^n = p^n$. $\diamondsuit$

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. $\diamondsuit$

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

$\diamondsuit$

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 $\left\{1, a, \ldots, a^{n-1}\right\}$ es una K-base de $K(a)$. En particular, $|K(a) : K| = \delta(p)$ y $K(a) = \left\{k_0 + k_1 a + \ldots + k_{n-1} a^{n-1} \mid k_i \in K\right\}$.

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

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:

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

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

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 ${}_1 \cap L_2 = K$.

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

Apéndices

Capítulo 3

Índices

Lista de definiciones

Lista de teoremas

Lista de ejemplos

Lista de ejercicios