

# Álgebra

Ignacio Cordon Castillo



## Álgebra conmutativa

### Tema 1: Anillos e ideales

### Tema 3: Bases de Groebner y algoritmos básicos

**Definición.** Sea  $R$  anillo. Un  $R$  módulo (izquierda) es un grupo abeliano  $M$ , junto a una operación externa

$$\begin{array}{ccc} R \times M & \longrightarrow & M \\ (r, x) & \mapsto & rx \end{array}$$

verificando,  $\forall x, y \in M, \forall r, s \in R$

- $r(x + y) = rx + ry$
- $(r + s)x = rx + sx$
- $r(sx) = (rs)x$
- $1x = x$

**Definición.** Una  $R$  álgebra es un anillo  $S$  que tiene estructura de  $R$  módulo tal que  $(rx)y = r(xy) = x(ry) \quad \forall r \in R, \quad \forall x, y \in S$

También puede caracterizarse una  $R$  álgebra como un anillo  $S$  junto a un homomorfismo de anillos  $\lambda : R \longrightarrow S$ . El homomorfismo  $\lambda$  se llama homomorfismo de estructura de la  $R$  álgebra  $S$ .

Si  $R = K$  cuerpo,  $\lambda$  es inyectiva,  $S$  es  $K$  álgebra que contiene a  $K$  como subanillo.

Como caso particular, todo anillo es una  $\mathbb{Z}$  álgebra.

**Definición.** Dadas  $S_1, S_2$   $R$  álgebras. Un homomorfismo de  $R$ -álgebras de  $S_1$  en  $S_2$  es un homomorfismo de anillos  $f : S_1 \rightarrow S_2$  que es también homomorfismo de  $R$  módulos.

**Proposición 1. Propiedad universal de  $R[X_1, \dots, X_n]$**

Sea  $S$  anillo,  $f : R \rightarrow S$  homomorfismo de anillos. Sean  $s_1, \dots, s_n \in S$  elementos arbitrarios. Entonces  $\exists f_{s_1, \dots, s_n} : R[X_1, \dots, X_n] \rightarrow S$  homomorfismo de  $R$  álgebras verificando  $f_{s_1, \dots, s_n}(X_i) = s_i$  y  $f_{s_1, \dots, s_n} \circ \lambda = f$  que además es único.

**Definición.** Una  $R$  álgebra  $S$  se llama finitamente generada si existe un homomorfismo de  $R$  álgebras sobreyectivo  $f : R[X_1, \dots, X_n] \rightarrow S$

Dado  $F \in K[X_1, \dots, X_n]$ , 
$$F = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$

$\{X^\alpha : \alpha \in \mathbb{N}^n\}$  es  $K$  base de  $K[X_1, \dots, X_n]$

Cualquier orden en  $\mathbb{N}^n$  induce un orden en  $\{X^\alpha : \alpha \in \mathbb{N}^n\}$

**Definición.** Un orden  $\leq$  en  $\mathbb{N}^n$  diremos que es **compatible** si siempre que  $\alpha \geq \beta$  entonces  $\alpha + \gamma \geq \beta + \gamma \quad \forall \gamma \in \mathbb{N}^n$ .

Diremos que es **monótono** si  $0$  es mínimo en  $\mathbb{N}^n$

Diremos que un orden es **monomial** si es compatible, total y monótono.

**Proposición 2.** Si  $\leq$  es orden monomial en  $\mathbb{N}^n$  entonces se verifica que dados  $\alpha, \beta \in \mathbb{N}^n$ :

$$\alpha \leq_{pr} \beta \implies \alpha \leq \beta$$

## Ejercicios

### Ejercicio 1.12

Demuestra que si un anillo verifica que cada elemento  $x$  verifica  $x^n = x$  para

algún  $n \geq 2$  (dependiente de  $x$ ) entonces todo ideal primo es maximal.

---

### Ejercicio 1.16

---

Un anillo  $R$  se dice anillo de Boole si  $x^2 = x$  para todo  $x \in R$ . Probar que en un anillo de Boole se tiene:

1.  $2x = 0$  para todo  $x \in R$
  2. Cada ideal primo  $\Pi$  es maximal y  $R/\Pi$  es un cuerpo con dos elementos.
  3. Cada ideal finitamente generado es principal.
- 

1-

Se tiene:

$$2x^2 = 2x = (2x)^2 = 4x^2$$

Luego  $2x^2 = 0$ .

2-

Sea  $\Pi$  ideal primo. Entonces  $R/\Pi$  es dominio de integridad. Pero dado  $x + \Pi \in R/\Pi$ ,  $x$  no unidad, se tiene  $(x + \Pi) + (x + \Pi) = (2x + \Pi) = \Pi$  que por ser dominio de integridad  $x \in \Pi$ . Luego  $R/\Pi$  es cuerpo con dos elementos y  $\Pi$  maximal.

3-

Solución propuesta por M42

Por inducción,  $(a, b) = (a + b + ab)$  ya que  $a(a + b + ab) = a^2 = a$  y análogo  $b$ .

Y el paso de inducción es trivial.

### Ejercicio 1.17

---

En un anillo  $R$  sea  $\Sigma$  el conjunto de todos los ideales en los que cada elemento es un divisor de cero. Probar que el conjunto  $\Sigma$  tiene elementos maximales y que cada elemento maximal de  $\Sigma$  es un ideal primo. Por tanto el conjunto de los divisores de cero en  $R$  es una unión de ideales primos.

---

### Ejercicio 1.18

---

Sea  $K$  un cuerpo, demuestra que el ideal  $(X^3 - Y^2) \subseteq K[X, Y]$  es un ideal primo del anillo  $K[X, Y]$ .

---

Se puede probar, con una discusión de casos, escribiendo  $X^3 - Y^2$  como producto de dos polinomios en  $K[X, Y]$  que no puede ocurrir esta circunstancia, luego  $X^3 - Y^2$  es irreducible en  $K[X, Y]$  y por tanto, al ser  $K$  cuerpo,  $(X^3 - Y^2)$  es primo.

### Ejercicio 1.25

---

Sean  $\alpha$  y  $\beta$  ideales de un anillo  $R$

1. Demuestra que  $\alpha + \beta = R$  si y sólo si  $\alpha^n + \beta^n = R$  para cada natural  $n$
  2. Demuestra que si  $\alpha, \beta$  son ideales comaximales propios entonces  $\alpha, \beta \subsetneq J(R)$
  3. Demuestra que si  $\alpha_1, \dots, \alpha_t$  son ideales comaximales dos a dos, entonces  $\alpha_1 + (\alpha_2, \dots, \alpha_t)^n = R$  para cada  $n \in \mathbb{N}$ .
- 

1-

La implicación hacia la izquierda es trivial tomando  $n = 1$ .

Hacia la derecha,  $n = 1$  obvio

Por inducción, supuesto que se cumple hasta  $n \in \mathbb{N}$

Existen  $u + v = 1$ ,  $u \in \alpha^n, v \in \beta^n$ . Desarrollando  $(u + v)^{n+1} = 1$  es fácil comprobar que pertenece a  $\alpha^n + \beta^n$

2-

Supuesto sin pérdida de generalidad que  $\alpha \subset J(R)$ .

Como existen  $x \in \alpha$ ,  $y \in \beta$  verificando  $x + y = 1$  por ser comaximales,  $y = 1 - x \in U(R)$  por caracterización de radical de Jacobson, luego  $\beta = R$ , contradicción.

3-

Si son primos dos a dos  $\exists x_{i1} \in \alpha_1, y_i \in \alpha_i$  verificando  $1 = x_i + y_i$  para todo  $i \geq 2$ . Luego:

$$\prod_{i=1}^t (1 - x_{i1}) = 1 + z = y_1 \cdots y_n \in \alpha_1, \cdots \alpha_t$$

con  $z \in \alpha_1$ . Luego  $1 \in \alpha_1 + (\alpha_1, \cdots \alpha_t)$ . Y la caracterización del apartado 1 acaba teniendo en cuenta que:

$$\alpha_1^n + (\alpha_1, \cdots \alpha_t)^n \subset \alpha_1 + (\alpha_1, \cdots \alpha_t)^n$$

### Ejercicio 1.24

---

Sea  $R$  un anillo y  $\mathcal{N}$  su nilradical. Demostrar que son equivalentes:

1.  $R$  tiene exactamente un ideal primo.
2. Cada elemento de  $R$  es o una unidad o nilpotente.
3.  $R/\mathcal{N}$  es un cuerpo.

---

$1 \implies 2$ . Entonces  $\mathcal{N}$  es maximal en  $R$ , por existir los ideales maximales en un anillo, ser todo ideal maximal primo y ser  $Nil(R) = \{x \in R : \exists n, x^n = 0\} = \bigcap_{\Pi \in Spec(R)} \Pi$  y en particular  $R$  es anillo local con maximal  $\mathcal{N} \iff R - \mathcal{N} \subseteq U(R)$  lo que nos da el resultado.

$2 \implies 3$ . Trivialmente, ya que todo elemento no nulo es invertible.

$3 \implies 1$ . Los ideales primos de  $R/\mathcal{N}$  son de la forma  $\alpha + \mathcal{N}$  con  $\alpha$  ideal primo de  $R$ . Pero como  $R/\mathcal{N}$  es cuerpo, se tiene que sus únicos ideales son el total y  $\mathcal{N} \equiv 0$ . Es decir  $\alpha \subseteq \mathcal{N} \subseteq \alpha$  donde el último contenido viene dado por ser  $\mathcal{N}_\infty = \bigcap_{\Pi \in Spec(R)} \Pi$ .

Luego  $\alpha = \mathcal{N}$  único ideal primo de  $R$ .

## Álgebra III

### Resumen

#### Elementos algebraicos

**Proposición 3.** *El elemento  $\alpha$  es algebraico sobre  $F$  si y solo si la extensión  $F(\alpha)/F$  es finita.*

**Proposición 4.** *Si la extensión  $K/F$  es finita, entonces es algebraica*

**Definición.** *La extensión  $K/F$  es finita si y solo si  $K$  está generado por un número finito de elementos algebraicos sobre  $F$ . De hecho, una extensión generada por elementos de grado  $n_1, \dots, n_k$  tiene grado menor o igual  $n_1 n_2 \dots n_k$*

**Teorema 1.**  *$K$  algebraico sobre  $F$  y  $L$  algebraico sobre  $K$  entonces  $L$  es algebraico sobre  $F$*

## Cuerpos de descomposición

- Cuerpo de descomposición

**Proposición 5.** Sea  $\alpha : K_1 \rightarrow K_2$  un isomorfismo de cuerpos. Existe una única extensión a un isomorfismo  $\sigma : K_1[X] \rightarrow K_2[X]$  definido por  $\sigma(x) = x$

La demostración se basa en la propiedad universal del anillo de polinomios.

**Proposición 6.** En las condiciones de la proposición anterior si  $F_i/K_i$  son extensiones algebraicas,  $\tau : F_1 \rightarrow F_2$  un homomorfismo sobre  $\sigma$  y  $u \in F_1$  una raíz de  $f_1$ . Entonces  $\tau(u)$  es una raíz de  $f_2 = \sigma(f_1)$

$$\text{Sea } f_1 = \sum_{i=1}^n a_i X^i$$

Entonces:

$$\begin{aligned} f_2(\tau(u)) &= \sum_{i=1}^n \sigma(a_i) \tau(u)^i = \sum_{i=1}^n \tau(a_i) \tau(u)^i \\ &= \tau\left(\sum_{i=1}^n a_i u^i\right) = \tau(0) = 0 \end{aligned}$$

**Proposición 7.** En las condiciones de la proposición anterior sea  $u_i$  raíz de  $f_i$  en alguna extensión  $F_i/K_i$ . Entonces existe un único isomorfismo  $\tau : K_1(u_1) \rightarrow K_2(u_2)$  sobre  $\sigma$  tal que  $\tau(u_1) = u_2$

Existen isomorfismos  $\rho_i : K_i[X]/(f_i) \cong K_i(u_i)$  y vienen dados por  $X + (f_i) \mapsto u_i$ .  $\bar{\sigma}$  viene dado por la proposición anterior llevándonos  $(f_1)$  en  $(f_2)$ . La aplicación buscada será  $\tau = \rho_2 \bar{\sigma} \rho_1^{-1}$

**Definición.** Sea  $K$  cuerpo,  $E/K$  extensión.  $f(X) \in K[X]$  descompone en  $E$  si en  $E[X]$  se factoriza como:

$$f(X) = a(X - a_1) \cdots (X - a_n), \quad a \in K, \quad a_1, \dots, a_n \in E$$

Cada  $(X - a_i)$  es un factor lineal.

Si no existe  $F$  verificando  $K \subseteq F \subseteq E$  y que  $f(X)$  descomponen en  $F[X]$ ,  $E[X]$  se llama cuerpo de descomposición.

Se deduce que  $E = K(\alpha_1, \dots, \alpha_n)$  donde  $\alpha_i$  son raíces de  $f(X)$  en  $E[X]$ . Por tanto todo polinomio  $f(X) \in K[X]$  tiene un cuerpo de descomposición sobre  $K$

**Proposición 8.** Un cuerpo de descomposición de un polinomio de grado  $n$  sobre  $F$  es de grado como mucho  $n!$  sobre  $F$ . Si el grado es  $n!$  entonces el polinomio es irreducible. El recíproco no se verifica.

**Teorema 2.** Sea una torre de cuerpos  $K \subset F \subset E$  con  $E/K$  algebraica y sea  $\bar{K}$  clausura algebraica de  $K$ . Entonces todo homomorfismo  $\sigma : F \rightarrow \bar{K}$  sobre  $K$  tiene una extensión  $\tau : E \rightarrow \bar{K}$  (¡jojo! extensión del homomorfismo)

Tomamos:

$$S = \{(E_i, \sigma_i) : F \subset E_i \subset E, \sigma_i : E_i \rightarrow \bar{K} \quad \sigma_i|_F = \sigma\}$$

$S$  es no vacío y es inductivamente ordenado por inclusión, considerando como orden la inclusión y la igualdad en la restricción de aplicaciones.

Por lema de Zorn existe por tanto un elemento maximal  $(E_1, \sigma_1)$ . Supongamos  $E_1 \subsetneq E$  existe un  $u \in E, u \notin E_1$  del que podemos tomar  $f = \text{Irr}(u, K)$  (porque  $E/K$  es algebraica) y por la proposición 7, como todos los  $\alpha_i$  mantienen  $K$ , llamando  $f_1 = f_2 = f$  en dicha proposición, tengo que existen un  $\sigma_2 : E_1(u) \rightarrow (\sigma_1(E_1))(u)$  que extiende  $\sigma_1 : E_1 \rightarrow \sigma(E_1)$  y el par  $(E_1(u), \sigma_2)$  sería entonces maximal, contradicción, luego  $E_1 = E$  y  $\tau = \sigma_1$ .

## Extensiones normales

**Proposición 9.** Sean  $u, v \in \bar{K}$ . Los siguientes enunciados equivalen:

1.  $\text{Irr}(u, K) = \text{Irr}(v, K)$
2. Existe isomorfismo  $\tau : K(u)/K \rightarrow K(v)/K$  tal que  $\tau(u) = v$
3. Existe homomorfismo  $\alpha_1 : K(u)/K \rightarrow \bar{K}/K$  tal que  $\sigma(u) = v$



4. Existe un automorfismo  $\alpha : \bar{K}/K \rightarrow \bar{K}/K$  tal que  $\sigma(u) = v$

1  $\Rightarrow$  2 Por 1 se tiene que:

$$K(u) \cong K/(Irr(u, K)) = K/(Irr(v, K)) \cong K(v)$$

Donde llevamos  $u \mapsto p(x)$  y  $v \mapsto p(x)$  en los isomorfismos correspondientes.

2  $\Rightarrow$  3 Componemos  $i \circ \tau$

3  $\Rightarrow$  4 implica que si tenemos  $p(x)$  irreducible tal que  $p(u) = 0$ . Entonces  $\sigma(p(x)) = p(x)$  y  $p(v) = \sigma(p(v)) = 0$

4  $\Rightarrow$  1 por el teorema 2

## Teoría de Galois

**Proposición 1.** *Dados  $n$  homomorfismos  $\sigma_1 \dots \sigma_n$  de  $G$  grupo al grupo multiplicativo de un cuerpo  $F$ , entonces son linealmente independientes.*

Supongamos una combinación de longitud mínima  $s$  de homomorfismos independientes de entre esos  $n$ . Podemos suponer s.p.g. que son los  $s$  primeros.

$$\sum_{i=1}^s a_i \sigma_i = 0$$

Entonces, podemos despejar  $\sigma_s = -\sum_{i=1}^{s-1} a_i/a_s \sigma_i$ .

Sea  $y \in G$  fijo tal que  $\sigma_1(y) \neq \sigma_s(y)$  (existe por ser homomorfismos distintos).

Entonces:

$$\sigma_s(xy) = \sigma_s(x)\sigma_s(y) = -\sum_{i=1}^{s-1} a_i/a_s \sigma_i(x)\sigma_i(y)$$

Y multiplicando por  $\sigma_s(y)$ :

$$\sigma_s(x)\sigma_s(y) = \sum_{i=1}^{s-1} a_i/a_s \sigma_i(x)\sigma_s(y)$$

Restando ambas igualdades llegamos a una combinación lineal finita nula y con el primer coeficiente no cero de longitud  $s - 1$ , contradicción.

A partir del lema anterior deducimos:

**Proposición 2. Lema de Dedekind** *Dados  $n$  homomorfismos distintos de  $F_1$  a  $F_2$ , con  $F_i$  cuerpos, entonces son linealmente independientes sobre  $F_2$*

**Corolario 1.** *Si  $[F_1 : K] = n$  existen a lo sumo  $n$  homomorfismos distintos de  $F_1$  a  $F_2$  que fijan  $K$ . Es decir  $|\text{Hom}(F_1/K, F_2/K)| \leq n$*

Sea una base de  $F_1$  sobre  $K$   $\{u_1, \dots, u_n\}$ . Supongamos que existen  $(n + 1)$  homomorfismos distintos  $\alpha_i : F_i \rightarrow F_2$  sobre  $K$ . El sistema de ecuaciones:

$$\sum_{i=1}^{n+1} x_i \sigma_i(u_j) = 0 \quad j = 1 \dots n$$

tiene una solución no trivial (ninguna columna contiene el elemento 0 por tener homomorfismos de cuerpos y podemos triangular por Gauss, luego hay una solución  $c_1 \dots c_{n+1} \in F_2$  al sistema.

Y por tanto al conseguir la misma combinación lineal que anula a todos los elementos por separado de la base, tenemos que  $\forall u \in F_1$ :

$$\sum_i^{n+1} c_i \sigma_i(u) = 0$$

Lo que entra en contradicción con el corolario anteriormente probado.

**Definición.** *Para toda extensión finita  $F/K$  llamamos **grupo de la extensión** al grupo:*

$$\backslash G(F/K) = \backslash \sigma \in \text{Aut}(F) \mid \forall u \in F \sigma(u) = u \backslash \backslash$$

**Corolario 2.** Para toda extensión finita  $F/K$  se verifica  $|G(F/K)| \leq [F : K]$

Trivial a partir del corolario anterior.

**Definición.** Sea  $E$  cuerpo arbitrario y  $G < \text{Aut}(E)$  subgrupo del grupo de automorfismos de  $E$ . Llamamos subcuerpo de  $E$  fijo por  $G$ .  $E^G = \{u \in E \mid \forall \sigma \in G \sigma(u) = u\}$

**Teorema 3. Teorema de Artin** Sea  $G$  subgrupo finito de  $\text{Aut}(E)$ . Entonces  $[E : E^G] = |G|$

Llamamos  $K = E^G$ . Por el corolario anterior sabemos que  $|\text{Aut}(E/K)| \leq [E : K]$  y  $G \subseteq |\text{Aut}(E/K)|$ , luego  $n = |G| \leq [E : E^G]$ .

Llamamos  $G = \{\alpha_1, \dots, \alpha_n\}$

Supongamos la desigualdad estricta. Tomamos  $n + 1$  elementos linealmente independientes sobre  $E^G$ . Formamos el sistema:

$$\sum_{i=1}^{n+1} x_i \sigma_j(u_i) = 0 \quad j = 1, \dots, n$$

Sea  $a_1, \dots, a_{n+1} \in E$  solución con el mínimo número de elementos no nulos. Sea Un automorfismo  $\sigma \in \text{Aut}(K)$  decimos que fija un elemento  $\alpha \in K$  si  $\sigma\alpha = \alpha$ . Fija  $K$  si fija todos sus elementos.

**Definición.** Una extensión  $E/K$  se llama extensión de Galois si existe un grupo  $G < \text{Aut}(E)$  tal que  $E^G = K$ . En este caso, el grupo se representa por  $\text{Gal}(E/K)$  y se llama grupo de Galois de la extensión  $E/K$

**Proposición 10.** Una extensión finita  $E/K$  es de Galois si y sólo si es normal y separable.

Por ser de Galois,  $K = E^G$  para algún grupo  $G$ . Cada automorfismo  $\sigma \in G$  se extiende a un homomorfismo  $\sigma : E \rightarrow \bar{K}$ , luego  $[E : K]_S \geq |G| = [E : K] \geq [E : K]_S$

Por tanto  $[E : K]_S = [E : K] = |G|$  (Por Artin)

Como para cada homomorfismo  $\tau : E \rightarrow K$  puedo tomarme  $i \circ \tau$  extensión a  $\bar{K}$

Hacia el lado opuesto. Sea  $E/K$  extensión normal y separable. Existen  $n = [E : K]_S = [E : K]$  homomorfismos  $\tau : E \rightarrow \bar{K}$  sobre  $K$  y para todos ellos  $\tau(E) = E$ . Por ello  $G = G(E/K)$  tiene orden  $n$ . Por el teorema de Artin  $[E : E^G] = [E : K]$ .

Además tenemos la torre de cuerpos  $K \subset E^G \subset E$ , lo que sumado a lo anterior da  $[E^G : K] = 1$  y por tanto  $E^G = K$  y la extensión  $E/K$  es de Galois.

???

Denotamos  $\text{Aut}(K/F)$  los automorfismos de  $K$  que fijan  $F$ . Si  $F = (1)$  entonces  $\text{Aut}(K/F) = \text{Aut}(K)$ .

**Proposición 11.**  *$\text{Aut}(K)$  es grupo bajo la composición y  $\text{Aut}(K/F)$  es un subgrupo.*

**Proposición 12.** *Dado un polinomio con coeficientes en  $K$ ,  $\sigma \in K$ , si  $\alpha$  es raíz del polinomio, entonces  $\sigma\alpha$  es raíz del polinomio.*

**Proposición 13.** *Si  $H$  es un subgrupo del grupo de automorfismos de  $K$ , los elementos de  $K$  fijos por  $H$  son subcuerpo de  $K$ , con  $K$  cuerpo.*

**Proposición 14.** 1.  $F_1 \subseteq F_2 \subseteq K$  son dos subcuerpos de  $K$  entonces  $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$

2.  $H_1 \leq H_2 \leq \text{Aut}(K)$  son dos subgrupos de automorfismos con cuerpos fijos asociados  $F_1$  y  $F_2$ , resp. entonces  $F_2 \subseteq F_1$

Esto último establecerá una relación entre los subgrupos del grupo de Galois y los subcuerpos de una extensión.

**Proposición 15.** *Sea  $E$  el cuerpo de descomposición sobre  $F$  del polinomio  $f(x) \in F[x]$ . Entonces:*

$$|\text{Aut}(E/F)| \leq [E : F]$$

con igualdad si  $f(x)$  es separable sobre  $F$

Nótese que este número da la cantidad de diagramas de la forma que se detalla a continuación que pueden construirse.

Conviene tener presente siempre el diagrama:

$$\begin{array}{ccccc} \sigma : & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \tau : & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & | & & | \\ \phi : & F & \xrightarrow{\sim} & F' \end{array}$$

donde la anterior proposición es un caso particular con  $F = F'$ , y  $E = E'$

**Definición.**  $K/F$  extensión finita. Entonces  $K$  se llama de Galois sobre  $F$  y  $K/F$  es una extensión de Galois si  $|Aut(K/F)| = [K : F]$ . Si  $K/F$  es de Galois el grupo de automorfismos  $Aut(K/F)$  es llamada grupo de Galois de  $K/F$ , denominada  $Gal(K/F)$ .

**Corolario 3.** Si  $K$  es el cuerpo de descomposición sobre  $F$  de un polinomio separable  $f(x)$  entonces  $K/F$  es de Galois.

Esto motiva la siguiente definición:

**Definición.** Si  $f(x)$  es un polinomio separable sobre  $F$ , entonces se llama grupo de Galois de  $f(x)$  sobre  $F$  a  $E/F$  con  $E$  cuerpo de descomposición de  $f$  sobre  $F$

Como ejemplo,

1.  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  es extensión de Galois con grupo de Galois  $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}_2$
2.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  no es de Galois ya que dado un  $\sigma \in Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ , debe conservar raíces del polinomio  $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ , pero dos de ellas son complejas, luego no pertenecientes a  $\mathbb{Q}(\sqrt[3]{2})$  por tanto, y no podemos construir más que un elemento de  $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ , la identidad. Nótese que aunque todas las raíces de  $x^3 - 2$  estuviesen en  $\mathbb{Q}(\sqrt[3]{2})$ , ello no nos garantiza que podamos construir siempre "suficientes" automorfismos (por ejemplo si el polinomio no tiene factores lineales de grado 1 sobre la extensión).

3. **El cuerpo de descomposición de cualquier polinomio sobre  $\mathbb{Q}$  es de Galois** según el corolario anterior. Por ejemplo ,  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  donde como sabemos que el grupo de Galois tiene dimensión 4 (la de  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , cuerpo de descomposición del polinomio  $(x^2 - 2)(x^2 - 3)$ ), y los únicos automorfismos posibles se obtienen de asignar  $\sqrt{2} \mapsto \pm\sqrt{2}$  y  $\sqrt{3} \mapsto \pm\sqrt{3}$
4. El cuerpo de descomposición de  $x^3 - 2$  sobre  $\mathbb{Q}$  es Galois de grado 6. Las raíces de esta ecuación son  $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ , y esto da 9 combinaciones distintas de raíces para formar automorfismos, pero como el grupo de Galois tiene orden 6, no todos ellos serán realmente automorfismos.
- 5.

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

muestra que no toda extensión de Galois de una extensión de Galois lo es (ya que tenemos **una extensión de grado 2, es de Galois por tanto**), pero las raíces de  $x^4 - 2 = \text{Irr}(\sqrt[4]{2}, \mathbb{Q})$  son  $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$  y de esas 4 raíces hay 2 que no están en  $\mathbb{Q}\sqrt[4]{2}$

6. Automorfismo de Frobenius

**NOTA:** Conveniente para efectuar demostraciones de estructura de subgrupos de Galois:

$$\begin{aligned} \langle \sigma, \tau : \sigma^2 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma \rangle &= K_4 \\ \langle \sigma, \tau : \sigma\tau = \tau\sigma^2, \tau^2 = 1, \sigma^3 = 1 \rangle &= S_3 \end{aligned}$$

## Ejercicios

### Ejercicio 1.24

---

Dado un término  $X_1^{e_1} \cdots X_n^{e_n}$  con  $e_1 \geq \dots \geq e_n$ , el polinomio simétrico mínimo que contiene a  $X_1^{e_1} \cdots X_n^{e_n}$  lo representamos por  $(X_1^{e_1} \cdots X_n^{e_n})$ , y podemos escribirlo fácilmente como

$$(X_1^{e_1} \cdots X_n^{e_n}) = \frac{1}{k} \sum_{\sigma \in S_n} X_{\sigma(1)}^{e_1} \cdots X_{\sigma(n)}^{e_n}$$

donde  $k$  es el número de términos  $X_{\sigma(1)}^{e_1} \cdots X_{\sigma(n)}^{e_n}$  que son iguales a  $X_1^{e_1} \cdots X_n^{e_n}$ .  
Calcula el valor de  $k$ , y el número de monomios de  $(X_1^{e_1} \cdots X_n^{e_n})$ .

---

Notamos  $d_1, \dots, d_m$ ,  $d_1 > \dots > d_m$ , donde  $d_1, \dots, d_m \in \{e_1, \dots, e_n\}$

y  $k_i = \text{card}(\{e_j : e_j = d_i\})$

Por combinatoria, sabemos por tanto que  $k = \prod k_i!$  y que tendremos un número  $\frac{k}{n}$  de monomios de tipo  $(X_1^{e_1} \cdots X_n^{e_n})$ .

### Ejercicio 1.25

---

Se considera el polinomio  $p(x) = x^3 - 5x - 5$  con raíces  $\alpha, \beta, \gamma$ . Calcula el valor de  $\left(\frac{1}{\alpha+1}\right)^3 + \left(\frac{1}{\beta+1}\right)^3 + \left(\frac{1}{\gamma+1}\right)^3$

---

$\frac{1}{\alpha+1}, \frac{1}{\beta+1}, \frac{1}{\gamma+1}$  anulan a  $p(\frac{1}{x} - 1)$  donde:

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

Luego  $a = \frac{1}{\alpha+1}, b = \frac{1}{\beta+1}, c = \frac{1}{\gamma+1}$  son raíces de:

$$q(x) = x^3 + 2x^2 + 3x - 1 = (x - a)(x - b)(x - c)$$

Definimos:

$$e_1 = a + b + c$$

$$e_2 = ab + ac + bc$$

$$e_3 = abc$$

Por un teorema visto en clase, podemos expresar de forma única  $a^3 + b^3 + c^3$  (que es lo pedido por el enunciado, y un polinomio simétrico en las variables  $a, b, c$ ) como un polinomio de grado 3 en función de  $e_1, e_2, e_3$

Se comprueba fácilmente que  $a^3 + b^3 + c^3 = e_1^3 - 3e_1e_2 + 3e_3$  Por otro lado, igualando los coeficientes de  $q$  factorizado y sin factorizar:

$$e_1 = -2$$

$$e_2 = 3$$

$$e_3 = 1$$

$$\text{Así } a^3 + b^3 + c^3 = 13$$

### Ejercicio 2.14

---

Sea  $A$  un anillo y  $\phi : A[X] \rightarrow A[X]$  un homomorfismo tal que  $\phi(a) = a$  para cada  $a \in A$ . Supongamos que  $\phi(X) = f(X) \in A[X]$ .

1. Si  $A$  es un dominio de integridad (DI), ¿qué condición tiene que verificar  $f(X)$  para que  $\phi$  sea un isomorfismo?\*
2. ¿Qué ocurre cuando  $A$  no es un DI?

---

1-

Se tiene  $\phi\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n a_i f(X)^i$ , si  $f(X) = ux + a$  con  $u$  unidad en  $A$ .



Para  $g(x) = u^{-1}(x - a)$  se tiene  $f \circ g = id = g \circ f$  y por tanto definiendo  $\gamma(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n a_i g(X)^i$  se cumple que  $\gamma \circ \phi = id = \phi \circ \gamma$

Claramente,  $f(X)$  no puede ser constante, ya que entonces tendríamos  $Img(\phi) \subseteq A$ .

Si  $gr(f(X)) = m \geq 2$ , puesto que al ser dominio de integridad, no se anula el coeficiente del término de mayor grado, tendríamos que:

$$gr(\phi(p(x))) = gr(p(X)) \cdot m$$

Y por tanto la función  $\phi$  no podría ser sobreyectiva, ya que en  $Img(\phi)$  sólo estarían contenidos los polinomios de grado un múltiplo de  $m$ . También se verifica que en  $f(X) = ux + a$ ,  $u$  no puede ser no unidad, puesto que en dicho caso tendríamos que el término líder de un polinomio  $\phi(p(x))$  debería estar en el ideal generado por  $u$ , que sería todo  $A$  si y solo si  $u$  es unidad.

2-

Podría ocurrir que si el coeficiente líder de  $f(X)$  es nilpotente,  $\phi$  fuera isomorfismo, como por ejemplo con  $f(X) = 2X^2 + X$  en  $\mathbb{Z}_4$ . Con dicho  $f$ , tendríamos  $\phi(X^2 + 2X) = X$ , lo que asegura sobreyectividad, y como  $gr(\phi(x)) \geq gr(p(x))$ , el kernel de  $\phi$  debería ser  $\{0\}$ , lo que asegura inyectividad.

### Ejercicio 2.15

---

Consideramos  $\mathbb{Z} \subset \mathbb{Q}$

1. Si  $f(X) \in \mathbb{Z}[X]$  es irreducible, prueba que  $f(X)$  es irreducible sobre  $\mathbb{Q}$
2. Si  $f(X) \in \mathbb{Z}[X]$  es irreducible, entonces  $F = \frac{\mathbb{Q}[X]}{(f(X))}$  es un cuerpo y tenemos inclusiones  $\mathbb{Z} \subset \mathbb{Q} \subset F$ .
3. Si llamamos  $x = X + (f(X)) \in F$ , prueba que  $x$  es una raíz de  $f(X) \in F[X]$

---

Supongamos que  $f(X)$  es reducible sobre  $\mathbb{Q}$ . Entonces:

$$f(X) = p_1(X) \cdot p_2(X), \quad \text{gr}(p_1) \geq 1, \text{gr}(p_2) \geq 1$$

Tomamos el menor  $n \in \mathbb{N}$  verificando  $nP = (b_l + b_{l-1}x^{l-1} + \dots + b_0) \cdot (c_mx^m + c_{m-1}x^{m-1} + \dots + c_0)$  donde todos los  $b_i$  y todos los  $c_j$  son enteros.

Si tuviéramos  $n = 1$ , ya habríamos acabado. Suponemos  $n > 1$ . Sea  $p$  divisor primo de  $n$ . Entonces no todos los  $b_i$  ni todos los  $c_j$  son divisibles por  $p$ , puesto que  $n$  es mínimo.

Sean  $k, t$  los índices de los primeros  $b_i, c_j$  verificando que  $p \nmid b_i, p \nmid c_j$

$$\text{Así, } n_{k+t} = b_{k+t}c_0 + b_{k+t-1}c_1 + \dots + b_kc_t + \dots + b_0c_{k+t}$$

Pero como  $p \mid b_{k+t}c_0, p \mid b_{k+t-1}c_1, \dots, b_{k+1}c_{t-1}, b_{k-1}c_{t+1}, \dots, b_0c_{k+t}$  necesariamente debe tenerse, por  $p \mid n$  que  $p \mid b_kc_t$ , lo cual es contradicción.

Por tanto  $n = 1$ .

2-

Sabemos que  $A/I$  con  $A$  anillo,  $I$  ideal, es cuerpo si y solo si  $I$  es maximal.

$I = (f(X))$  es maximal en  $\mathbb{Q}[\mathbb{X}]$ , ya que dado otro ideal  $(f(X)) \subsetneq M$ , como  $\mathbb{Q}[\mathbb{X}]$  es DIP,  $M = (g(X))$ , con  $g(X) \in \mathbb{Q}[\mathbb{X}]$ , pero eso quiere decir que  $f(X) = a(x) \cdot g(X)$  con  $a(X)$  no constante, ya que en caso opuesto, los dos ideales serían iguales, pero esto entra en contradicción con el hecho de que  $f(X)$  es irreducible.

Luego  $(f(X))$  es maximal y  $F$  cuerpo.

Además, a cada elemento  $q \in \mathbb{Q}$  podemos asignarle un elemento  $q + (f(X))$ . Dados  $q, q' \in \mathbb{Q}$ , se tiene que  $q + \mathbb{Q} \neq q' + \mathbb{Q}$ , ya que caso opuesto tendríamos  $q - q' \in (f(X))$ , lo que es imposible, puesto que  $q - q' \neq 0$  y es una constante.

3-

Sea  $f(X) = \sum a_i X^i$  en  $\mathbb{Q}[\mathbb{X}]$ . Entonces tenemos que en  $F[X]$ :

$$\begin{aligned} f(x) &= \sum (a_i + (f(X)) \cdot (X^i + (f(X)))) = \sum (a_i \cdot X^i + (f(X))) = \\ &= (\sum a_i X^i + (f(X))) = (f(X) + (f(X))) = (f(X)) \end{aligned}$$

Luego es una raíz del polinomio.

### Ejercicio 2.16

---

Describe los elementos del cuerpo  $\frac{\mathbb{F}_2[X]}{(X^3 + X + 1)}$ , completando las tablas de la suma y el producto.

---

Los elementos del cuerpo citado son de la forma  $p(X) + (X^3 + X + 1)$  con  $p(X)$  un polinomio producto de irreducibles en  $\mathbb{F}_2[X]$ . Así, los elementos de este cuerpo son:

$$\begin{aligned} 0 &= 0 + (X^3 + X + 1) \\ 1 &= 1 + (X^3 + X + 1) \\ a &= X + (X^3 + X + 1) \\ b &= X + 1 + (X^3 + X + 1) \\ c &= X^2 + X + 1 + (X^3 + X + 1) \\ d &= X^2 + X + (X^3 + X + 1) \\ e &= X^2 + (X^3 + X + 1) \\ f &= X^2 + 1 + (X^3 + X + 1) \end{aligned}$$

- Tabla del producto

$\cdot$	0	1	$a$	$b$	$c$	$d$	$e$	$f$
0	0	0	0	0	0	0	0	0
1	0	1	$a$	$b$	$c$	$d$	$e$	$f$
$a$	0	$a$	$e$	$d$	$f$	$c$	$b$	1
$b$	0	$b$	$d$	$f$	$a$	1	$c$	$e$
$c$	0	$c$	$f$	$a$	$b$	$e$	1	$d$
$d$	0	$d$	$c$	1	$e$	$a$	$f$	$b$
$e$	0	$e$	$b$	$c$	1	$f$	$d$	$a$
$f$	0	$f$	1	$e$	$d$	$b$	$a$	$c$

- Tabla de la suma

$+$	0	1	$a$	$b$	$c$	$d$	$e$	$f$
0	0	1	$a$	$b$	$c$	$d$	$e$	$f$
1	1	0	$b$	$a$	$d$	$c$	$f$	$e$
$a$	$a$	$b$	0	1	$f$	$e$	$d$	$c$
$b$	$b$	$a$	1	0	$e$	$f$	$c$	$d$
$c$	$c$	$d$	$f$	$e$	0	1	$b$	$a$
$d$	$d$	$c$	$e$	$f$	1	0	$a$	$b$
$e$	$e$	$f$	$d$	$c$	$b$	$a$	0	1
$f$	$f$	$e$	$c$	$d$	$a$	$b$	1	0

### Ejercicio 2.17

Se considera  $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5} \in F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

1. Prueba que  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$
2. Prueba que  $F = \mathbb{Q}(\alpha)$
3. Calcula  $\text{Irr}(\alpha, \mathbb{Q})$
4. Encuentra elementos  $\beta \in F$ , de grado cuatro sobre  $\mathbb{Q}$

1-

Tenemos la torre de cuerpos:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5})$$

Y por tanto se cumple:

$$\begin{aligned} [\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) : \mathbb{Q}] &= \\ &= [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2})(\sqrt{3})] \end{aligned}$$

Se verifica:

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

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

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

ya que es conocido que  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , y además se tienen las otras dos igualdades, al no poder expresar  $\sqrt{2} = a + b\sqrt{3}$ ,  $a, b \in \mathbb{Q}$  ni  $\sqrt{2} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ ,  $a, b, c, d \in \mathbb{Q}$

2-

Claramente  $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  Se tiene que:

$$(\sqrt{2} + \sqrt{3} + \sqrt{5})^2 = 2\sqrt{15} + 2\sqrt{10} + 2\sqrt{6} + 10$$

Por tanto  $\beta = \sqrt{15} + \sqrt{10} + \sqrt{6} \in F$

Además  $\beta^2 = 4\sqrt{15} + 6\sqrt{10} + 10\sqrt{6} + 31$

Y por tanto  $\gamma = 4\sqrt{15} + 6\sqrt{10} + 10\sqrt{6} \in F$

Además:

$$\delta = \frac{1}{2}(\gamma - 4\beta) = \sqrt{10} + 3\sqrt{6}$$

$$\theta = \frac{1}{2}(6\beta - \gamma) = \sqrt{15} - 2\sqrt{6}$$

$$\delta^2 = 10 + 9 \cdot 6 + 4\sqrt{15}$$

$$\theta^2 = 15 + 4 \cdot 6 - 12\sqrt{10}$$

Juntando toda esta información con que  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$  es base de  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  deducimos que  $1, \sqrt{15}, \sqrt{10}, \sqrt{6}, \sqrt{2} + \sqrt{3} + \sqrt{5} \in F$ , 5 elementos linealmente independientes, y  $F$  sólo puede tener grado 8, 4 o 2 luego debe ser 8.

3-

$$\begin{aligned} \beta = \sqrt{5} + \sqrt{2} + \sqrt{3} &\Leftrightarrow (\beta - \sqrt{5})^2 - (\sqrt{2} + \sqrt{3})^2 = 0 \Leftrightarrow \beta^2 - 2\sqrt{5}\beta - 2\sqrt{6} = 0 \Leftrightarrow \\ &\Leftrightarrow (\beta^2 - 2\sqrt{6})^2 = 4 \cdot 5\beta^2 \Leftrightarrow \beta^4 - 4\sqrt{6}\beta^2 - 20\beta^2 + 24 = 0 \Leftrightarrow \\ &\Leftrightarrow (\beta^4 - 20\beta^2 + 24)^2 - 16 \cdot 6 \cdot \beta^4 = 0 \Leftrightarrow \\ &\Leftrightarrow \beta^8 - 40\beta^6 + 352\beta^4 - 960\beta^2 + 576 = 0 \end{aligned}$$

Por tanto  $X^8 - 40X^6 + 352X^4 - 960X^2 + 576$ , al ser polinomio de grado 8, que es el grado de la extensión, debe ser irreducible,  $\text{Irr}(\alpha, \mathbb{Q})$

4-

Nos basta demostrar que  $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$  y por tanto  $\sqrt{2} + \sqrt{3} = \omega$  sería elemento de grado 4.

Claramente  $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , y como  $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$ ,  $\mathbb{Q}(\omega)$  tendrá grado 4 o 2 sobre  $\mathbb{Q}$ . Además:

$$\omega^2 = 2 + 3 + \sqrt{6}$$

,

$$\omega^3 = 9\sqrt{3} + 11\sqrt{2}$$

y podemos obtener a partir de combinaciones de  $\omega, \omega^2, \omega^3$  los elementos  $\sqrt{2}, \sqrt{3}, \sqrt{6}$ , que pertenecen a  $\mathbb{Q}(\omega)$ , y que están en la base  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  de  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Por tanto  $\omega$  es elemento de grado 4.

### Ejercicio 3.11

Sea  $K$  una extensión de  $\mathbb{F}_2$  de grado  $n > 1$ , y  $f(X) \in \mathbb{F}_2[X]$  un polinomio no constante\*

1. Prueba que si  $\alpha \in K$  es una raíz de  $f(X)$ , entonces  $\{\alpha^2, \alpha^4, \alpha^{2n-1}\}$  son raíces de  $f(X)$  en  $K$
2. Prueba que en general  $\{\alpha, \alpha^2, \alpha^4, \alpha^{2n-1}\}$  no son todas las raíces de  $f(X)$
3. Prueba que si  $\beta$  es una raíz primitiva de  $K$ , que es raíz de  $f(X)$ , entonces el grado de  $f(X)$  es mayor o igual que  $n$

1-

Trivialmente, en  $\mathbb{F}_2$  tenemos que:  $\left(\sum_{i=1}^k a_i\right)^2 = \sum_{i=1}^k a_i^2$

Por inducción:  $\left(\sum_{i=1}^k a_i\right)^{2n} = \sum_{i=1}^k a_i^{2n}$

Así:

$$f(\alpha^{2n}) = \sum_{i=1}^m \alpha^{2ni} = \left(\sum_{i=1}^m \alpha^i\right)^{2n} = f(\alpha)^{2n} = 0$$

2-

Tenemos el caso trivial  $x(x+1)$ , en el que las raíces  $0, 1$  están en  $\mathbb{F}_2 \subseteq K$ , pero  $0$  no es potencia de  $1$  (entendiendo como  $0$  y como  $1$  los del cuerpo  $K$  que cojamos como extensión, que puede ser por ejemplo  $\frac{\mathbb{F}_2[X]}{x^2+x+1}$  con  $x^2+x+1$  irreducible en  $\mathbb{F}_2[X]$ )

3-

Si  $\beta$  es raíz primitiva de  $K$ , se tiene que  $\{1, \beta, \dots, \beta^{n-1}\}$  es base de  $K$  sobre  $\mathbb{F}_2$ .

Si el grado de  $f(X)$  fuese menor que  $n$ , tendríamos que  $f(\beta) = 0$  es una combinación lineal de los elementos de la base que vale  $0$ , y esto entra en contradicción con que sea base.

#### Ejercicio 4.17

---

Sea  $K \subseteq E \subseteq F$  una torre de cuerpos y supongamos que  $\alpha_1, \dots, \alpha_r$  son algunas de las raíces de  $f(X) \in K[X]$  y  $E = K(\alpha_1, \dots, \alpha_r)$ . Demuestra que  $F$  es el cuerpo de descomposición de  $f(X)$  sobre  $K$  si, y sólo si,  $F$  es el cuerpo de descomposición de  $f(X)$  sobre  $E$

---

Sean  $\alpha_1, \dots, \alpha_n$  todas las raíces de  $f(X)$  con  $n > r$

Basta con afirmar que el cuerpo de descomposición de  $f(X)$  sobre  $K$  es:

$$G = K(\alpha_1, \dots, \alpha_n)$$

Y el de  $f(X)$  sobre  $E$ :

$$G' = E(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_r)(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n) = G$$



### Ejercicio 4.18

---

Sea  $a \in \mathbb{Q}$  y  $n$  un número entero positivo impar tal que  $\sqrt[n]{a} \in \mathbb{R} \setminus \mathbb{Q}$ . Demuestra que la extensión  $\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$  no es normal

---

La extensión no es normal ya que si lo fuese, como  $x^n - a$  es un polinomio que divide a  $p(X) = \text{Irr}(\alpha, K)$  sobre  $\mathbb{Q}[X]$ , y como  $n$  es impar,  $x^n - a$  sólo puede tener una raíz real, por ser sus raíces de la forma  $\omega^k \sqrt[n]{a}$ , con  $\omega$  raíz  $n$ -ésima de la unidad. Luego todas las raíces de  $p(X)$  deberían estar en la extensión  $E = \mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$ . Además  $E \subseteq \mathbb{R}$ , luego  $\sqrt[n]{a} \in \mathbb{Q}$ , es decir, el polinomio debería ser forzosamente  $x - \sqrt[n]{a}$ , que implica que  $\sqrt[n]{a} \in \mathbb{Q}$ , ¡contradicción!

### Ejercicio 4.19

---

Sea  $E/K$  una extensión normal y  $f(X) \in K[X]$  un polinomio(mónico) irreducible. Si  $f(X)$  se factoriza en  $E$  como producto de dos polinomios(mónicos) irreducibles  $f_1(X)$  y  $f_2(X)$ . Demuestra que existe un homomorfismo  $\sigma : E/K \rightarrow E/K$  tal que  $f_1^\sigma(X) = f_2(X)$

---

Sea  $\alpha$  raíz de  $f_1$  y  $\beta$  raíz de  $f_2$  en una clausura de  $K$ . Como  $f = \text{Irr}(\alpha, K)$ ,  $f = \text{Irr}(\beta, K)$ , tenemos que existe un isomorfismo  $\sigma : \overline{K}/K \rightarrow \overline{K}/K$  verificando  $\sigma(\alpha) = \beta$ .

Por ser  $E$  extensión normal, luego finita,  $\overline{K}$  es también su clausura algebraica, y por tanto  $E \subseteq \overline{K}$ . Así  $E^\sigma = E$ , luego  $\sigma|_E$  es isomorfismo. Y como  $f_1^\sigma(\beta) = f_1(\alpha) = 0$ , tenemos que  $f_1^\sigma|f_2$ , pero un isomorfismo se lleva polinomios irreducibles en irreducibles, luego  $f_1^\sigma = f_2$

### Ejercicio 5.10

---

Sea  $K$  un cuerpo de característica  $p \neq 0$  y  $t$  una indeterminada sobre  $K$ . Prueba que el polinomio  $X^p - t^p \in K(t^p)[X]$  es irreducible.

---

En una extensión  $K' = K(t)$  de  $K$  tenemos  $X^p - t^p = (X - t)^p$ , ya que los términos intermedios del desarrollo valen 0, al ser  $p$  la característica de  $K$ .

Como  $K(t^p) \subseteq K'$ , tenemos que los únicos factores que pueden dividir a  $X^p - t^p$  son de la forma  $(X - t)^m$ . Supongamos que alguno tuviese coeficientes en  $K(t^p)$ . Entonces tendríamos que sus coeficientes también están en  $K'$ , y por tanto podríamos reescribir  $t^m$  como raíz de un polinomio con coeficientes en  $K$ , pero  $t$  era trascendente.

### Ejercicio 5.11

---

Estudiar si son o no ciertas las siguientes afirmaciones:

1.  $\sqrt[3]{-1}$  es separable sobre  $\mathbb{F}_9$
  2.  $\sqrt[3]{-1}$  es separable sobre  $\mathbb{F}_{49}$
  3.  $\sqrt[7]{5}$  es separable sobre  $\mathbb{F}_{77}$
  4.  $t$  es separable sobre  $\mathbb{F}_{p^2}(t^p)$ , siendo  $p$  un número entero positivo y  $t$  una indeterminada sobre  $\mathbb{F}_{p^2}$
- 

1-

$\mathbb{F}_3$  es cuerpo perfecto por ser finito. Luego por ser  $\mathbb{F}_9$  extensión finita de  $\mathbb{F}_3$  tenemos que es separable, y todo elemento suyo es separable.

2,3-

Se resuelven de manera análoga al primer apartado, ya que  $\mathbb{F}_7$  es cuerpo perfecto por ser finito, y  $\mathbb{F}_{77}$  es extensión finita, luego todo elemento es separable.

4-

El cuerpo  $\mathbb{F}_p$  tiene característica  $p$  y su extensión  $\mathbb{F}_{p^2}$  tiene también por tanto característica  $p$ .

Por el primer ejercicio  $X^p - t^p = (X - t)^p = \text{Irr}(t, \mathbb{F}_{p^2}(t^p))$ , luego  $t$  no es separable.

### Ejercicio 5.12

---

Sea  $E$  un cuerpo y  $\{\phi_1, \dots, \phi_n\}$  un conjunto de  $n$  automorfismos distintos de  $E$ . llamamos  $K = \{e \in E \mid \phi_i(e) = e, 1 \leq i \leq n\}$ . demuestra que  $[E : K] \geq n$

---

El teorema de Artin nos afirma que  $[E : K] = n$

### Ejercicio 7.25

---

Sea  $f \in K[X]$  un polinomio no constante sin raíces múltiples y  $G = \text{Gal}(f/K)$ . Prueba que son equivalentes: list-style-type: lower-roman

1.  $f(X)$  es irreducible
2.  $G$  actúa transitivamente sobre las raíces de  $f$

---

Llamamos  $E$  al cuerpo de descomposición de  $f$  sobre  $K$ . Se tiene  $\text{Gal}(f/K) = \text{Gal}(E/K)$ . Sabemos que  $E/K$  es de Galois  $\iff E/K$  es normal y separable, luego:

$$f(x) = \alpha(x - \alpha_1) \cdots (x - \alpha_n) \quad \alpha, \alpha_i \in E, \quad \alpha_i \neq \alpha_j \quad i \neq j$$

2  $\implies$  1.

Supongamos que  $f$  no es irreducible.

Entonces  $f(x) = p(x) \cdot q(x)$  con  $p(x), q(x) \in K[x]$  no constantes.

Podemos suponer, sin pérdida de generalidad:

$$p(x) = \alpha \prod_{i=1}^m (x - \alpha_i)$$

$$q(x) = \prod_{i=m+1}^n (x - \alpha_i)$$

Dadas  $\alpha_i \neq \alpha_j$  raíces de  $f$ ,  $\exists \varphi_{i,j} \in G : \varphi(\alpha_i) = \alpha_j$

Tomo  $\varphi_{1,n}$ . Se tiene que  $\varphi_{1,n}(p) = p$ ,  $\varphi_{1,n}(q) = q$ , ya que  $\varphi_{1,n}$  conserva  $K$ .

Pero  $\varphi_{1,n}(p(\alpha(n))) = p(\varphi_{1,n}(\alpha(n))) = p(\alpha(1)) = 0$ , lo que es contradicción, ya que  $\alpha_1$  no era raíz de  $p$ . Luego  $f$  es irreducible.

1  $\implies$  2.

Si  $f$  es irreducible, ninguna de sus raíces puede estar en  $K$ , ya que en ese caso  $f(x)/(x - \alpha_i)$  estaría en  $K[x]$  y eso entra en contradicción con que sea irreducible.

En esas condiciones es claro que  $\exists \varphi : K(\alpha_i)/K \longrightarrow K(\alpha_j)/K$  isomorfismo verificando  $\varphi(\alpha_i) = \alpha_j$  y podemos extenderlo a un isomorfismo  $\sigma : K(\alpha_1, \dots, \alpha_n) \longrightarrow K(\alpha_1, \alpha_n)$  sobre  $\varphi$ .

Por tanto  $\sigma$  es automorfismo sobre  $E$  que conserva  $K$  y cumple  $\sigma(\alpha_i) = \varphi(\alpha_i) = \alpha_j$