Álgebra

Ignacio Cordón 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* $\$\begin{matrix} RM\& \longrightarrow \&M \\ (r,x)\& \mapsto \&rx \end{matrix}\$$

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 λ se llama homomorfismo de estructura de la R álgebra S.

Si $R = K$ cuerpo, λ 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 $f : S_1 \longrightarrow S_2$ que es también homomorfismo de R módulos.*

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

Sea S anillo, $f : R \longrightarrow S$ homomorfismo de anillos. Sean $s_1, \dots s_n \in S$ elementos arbitrarios. Entonces $\exists f_{s_1,\dots s_n} : R[X_1, \dots X_n] \longrightarrow S$ 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 $f : R[X_1, \dots X_n] \longrightarrow S$*

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

$\{X^\alpha : \alpha \in \mathbb{N}^n\}$ 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 $\alpha + \gamma \geq \beta + \gamma \qquad \forall \gamma \in \mathbb{N}^n$.*

*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 $\alpha, \beta \in \mathbb{N}^n$:*

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

Ejercicios

Ejercicio 1.12

Demuestra que si un anillo verifica que cada elmento 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 Π es maximal y R/Π 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 Π ideal primo. Entonces R/Π 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/Π es cuerpo con dos elementos y Π 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 Σ el conjunto de todos los ideales en los que cada elemento es un divisor de cero. Probar que el conjunto Σ tiene elementos maximales y que cada elemento maximal de Σ 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 α y β 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 α, β son ideales comaximales propios entonces $\alpha, \beta \subsetneq J(R)$
3. Demuestra que si $\alpha_1, \ldots \alpha_t$ son ideales comaximales dos a dos, entonces $\alpha_1 + (\alpha_2, \cdots \alpha_t)^n = R$ 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 $u + v = 1, \quad u \in \alpha^n, v \in \beta^n$. 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.

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

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

$3 \Longrightarrow 1$. Los ideales primos de $R/\mathcal{N}$ son de la forma $\alpha + \mathcal{N}$ con α 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.

Ejercicio 2.2

1. Tomamos:

$$F = X^2Y + XY^2 = XY(X + Y)$$

$$G = XY^4$$

$mcd(F, G) = XY$, pero sin embargo $XY \neq (F, G)$, luego no se verifica la identidad de Bezout. En general, dados dos polinomios cualesquiera, dicha identidad no se verifica

1. Queda como ejercicio.

TODO Ejercicio 2.15

Ejercicio 2.16

Sea $\leq$ un orden en $\mathbb{N}^n$ que es total y compatible. Haciendo usod e la teoría de ideales monoiales, probad que $\leq$ es un buen orden sii es monótono.

Hacia la izquierda, como $\leq$ es monomial, entonces es buen orden.

Hacia la derecha, si 0 no fuese mínimo, $\exists x \in \mathbb{N}^n$ verificando $x < 0$. Como el orden es compatible tendríamos que $x + x < x$, lo que es contradicción.

Ejercicio 2.17

Sean $I, J \subset K[X_1, \ldots X_n]$ ideales monomiales generados por $\{A_1, \ldots A_s\}$ y $\{B_1 \ldots B_t\}$, A_i, B_j monomios:

1. Demuestra que $I \cap J$ es un ideal monomial.

2. Prueba que $\{M_{ij} : i = 1 \ldots s, j = 1 \ldots t\}$ donde $M_{ij} = mcm(A_i, B_j)$ es un sistema de generadores de $I \cap J$

---

1. Se tiene $F \in I$ sii todos los monomios de $F∈ I4.

Además $I \cap J = (F_1, \ldots F_r)$, con $F_i = \sum_{j=1}^{n_i} a_{ij} R_i j$ monomios.

Si $F_i \in I \cap J$, entonces $F_i \in I$ y $F_i \in J$. Lueg $R_{ij} \in I$, $R_{ij} \in J$ y por tanto $R_{ij} \in I \cap J$

Por tanto $I \cap J = (R_{ij} : i = 1 \ldots r, 1 \leq j \leq n_i)$, luego $I \cap J$ es monomial.

1. Es claro que $(M_{ij}) \subset I \cap J$

Para el otro contenido, si $X^\alpha \in I \cap J$ entonces $X\alpha \in I \implies X^\alpha = FA_i$ y análogo para $X^\alpha \in J$, luego $M_{ij} | X^\alpha$.

1. $I = (X = A_1, Y^2Z = A_2, YZ^2 = A_3)$, y por otor lado $J = (X^3YZ = B_1, X^2Y = B_2, Y^2Z^3 = B_3)$

Calculando $M_{11} = mcm(A_1, B_1)$, $M_{12} = X^2Y$.

Al final $I \cap J = (X^2Y, Y^2Z^3)$

Ejercicio 2.18

Sean I_1, I_2 ideales monomiales con sistema de generadores G_1, G_2 resp. Demuestra que:
1.$I_1 + I_2$ está generado por $G_1 \cup G_2$ 2.$I_1 I_2$ está generado por $\{HL : H \in G_1, L \in G_2\}$

Hay que comprobar que si $I_1 = (G_1, \ldots G_k)$, $I_2 = (H_1, \ldots H_s)$ entonces:

$$I_1 + I_2 = (G_1, \ldots G_k, H_1, \ldots H_s)$$
$$I_1 I_2 = (G_i H_j : i = 1 \ldots k, j = 1 \ldots s)$$

Ejercicio 2.21

Demostrar que si I, J son dos ideales monomiales entonces $(I : J)$ es un ideal monomial.

Definición. *Llamo soporte de* $F \in K[X_1, \ldots X_n]$ *a* $Sop(F) = \{X^\alpha : \alpha \in N(F)\}$

Dado $F \in (I : J) \implies FJ \subset I$. En particular $FX^\beta \forall X^\beta \in J$

Esto implica que $X\alpha X\beta \in I \forall \alpha \in N(F) X^\alpha \in J$. Entonces $X\alpha J \subset I \implies X^\alpha \in (I : J) \forall \alpha \in N(F)$. Luego $(I : J)$ es monomial.

Ejercicio 2.22

1. Veamos la implicación hacia la izquierda:

$I = (X_{i1}, \ldots X_{is})$ para $\{X_{1i}, \ldots X_{is}\} \subset \{X_1, \ldots X_n\}$ Entonces $K[X_1 \ldots X_n]/I \cong K[X_j : j \notin \{i_1, \ldots i_s\}]$ es un DI. Luego I es primo.

Veamos la implicación hacia la derecha.

Sea I monomial y primo. $I = (X^\alpha(1), \ldots X^\alpha(s))$.

$X^\alpha(j) \in I$ luego $\exists i_j$ tal que $X_{ij} \in I$.

Todo esto nos da $(X_{i1}, \ldots X_{is}) = I$

1. Queda como ejercicio.

2. $\mathcal{M} = (X_1 \dots X_n)$ es el único maximal que es monomial.

$$K[X_1 \dots X_n]/\mathcal{M} \cong K$$

Luego $\mathcal{M}$ es maximal.

Es el único porque si tenemos $I = (A)$, $I' = (A')$ entonces $A \subset A' \Leftrightarrow I \subset I'$

Álgebra III

Resumen

TODO

- **TODO** 7 de dónde sale?
- **TODO** ¿Qué es exactamente F?
- **TODO** 6 Demostrar el teorema de existencia de cuerpos de descomposición.
- **TODO** Ejemplo X$^{\mathrm{p}}$-t, pág 52 apuntes de Miranda, ¿criterio de Eisenstein?

Extensiones de cuerpos

Definición. *Una extensión de cuerpos F/K es un par de cuerpos F, K tales que K es un sucuerpo de F. K se llama cuerpo base y F cuerpo extensión .*

Definición. *Llamamos grado de la extensión F/K y lo representamos por $[F : K]$ a la dimensión de F como K espacio vectorial. La extensión es finita si su grado es finito.*

Definición. *Una torre de cuerpos es una sucesión de subcuerpos: $F_n \supset F_{n-1} \supset \dots \supset F_0$*

Proposición 3. *Sea $E \supset F \supset K$ torre de inclusiones. Entonces:*

Sean $\{u_i \in E : i \in I\}$ un sistema de generadores (linealmente independientes, base, resp.) de E como espacio vectorial sobre F y $\{v_j \in F : j \in J\}$ un sistema de generadores (linealmente independientes, base, resp.) de F como espacio vectorial sobre K. Entonces $\{u_i v_j : i, j \in I \times J\}$ es sistema de generadores (linealmente indep., base) de E como espacio vectorial sobre K.

Teorema 1. ***Teorema del grado:*** *Sea $E \supset F \supset K$ torre de cuerpos. Entonces:*

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

La demostración se puede deducir de la proposición anterior.

Corolario 1. *Se cumple:*

1. *$E \supset F \supset K$ torre de cuerpos. La extensión E/K es finita sii las extensiones E/F y F/K son ambas finitas.*
2. *Sea F/K extensión tal que $[F : K] = p$ es primo. Entonces no existe ningún cuerpo intermedio distinto de F o K.*

Elementos algebraicos

Proposición 1. *Para todo anillo A existe un único homomorfismo $\upsilon : \mathbb{Z} \to A$ llamado homomorfismo unital.*

Este homomorfismo se define por inducción como $1_{\mathbb{Z}} \mapsto 1_A$ y $n_{\mathbb{Z}} \mapsto 1 + \ldots 1_{n)}$

Definición. *Si el kernel del homomorfismo unital es $n\mathbb{Z}$, la característica del anillo A, se define como $car(A) = n$. Además n queda **caracterizado** por ser el menor número que verifica $na = 0 \quad \forall a \in A$*

La demostración se hace basándonos en el primer teorema de isomorfía. Si su característica fuese $n \neq 0$, tendríamos que $\mathbb{Z}/\mathbb{Z}_n \cong Img(\upsilon)$ y si n no es primo, tenemos un subanillo de A, $Img(\upsilon)$ isomorfo a algo que no es dominio de integridad.

Proposición 4. *La intersección de subanillos es subanillo. La intersección se subcuerpos es subcuerpo.*

Proposición 2. ***Estructura del subanillo imagen del homomorfismo unital*** *El menor subanillo de un anillo A es la intersección de todos sus subanillos. Se llama* anillo primo. *Se cumple:*

1. *Este subanillo es isomorfo a $\mathbb{Z}$ si $car(A) = 0$ y a $\mathbb{Z}_n$ si $car(A) = n \neq 0$.*
2. *Si A es dominio de integridad, entonces o bien $car(A) = 0$ o bien $car(A) = p$ primo.*

Proposición 3. *Al menor subcuerpo de de un cuerpo K lo llamamos* subcuerpo primo*, que es la intersección de todos los subcuerpos de K.*

El subcuerpo primo de un cuerpo K es isomorfo a $\mathbb{Q}$ cuando $car(K) = 0$ y a $\mathbb{Z}/p\mathbb{Z}$ cuando $car(K) = p \neq 0$

Se deduce del lema anterior sin más que pensar que un cuerpo es un anillo en el que hay una operación inversa. Y como $\mathbb{Q}$ es dominio de integridad, la característica debe ser un primo.

Definición. *Sea F/K extensión, S un subconjunto de F. LLamamos subanillo (resp. subcuerpo) generado por S sobre K y lo representamos por $K[S]$ (resp. $K(S)$) a la intersección de todos los subanillos (resp. cuerpos) de F que contengan a K y a S.*

Para los casos $S = \{u_1, \dots u_n\}$ notamos $K[u_1, \dots u_n]$ en lugar de $K[\{u_1, \dots u_n\}]$. Análogo para $K(S)$

Proposición 4. *Se verifica:*

1. $K[S \cap T] = K[S][T] = K[T][S]$
2. $K(S \cap T) = K(S)(T) = K(T)(S)$

Definición. ***Subcuerpo compuesto****. pDados los cuerpos $L \supset E \supset K$, $L \supset F \supset K$, llamamos* compuesto de E y F *al cuerpo $EF = E(F) = F(E)$. Es decir, el menor subcuerpo de L que contiene a E y F.*

Definición. ***Conjunto de generadores****. Sea F/K extensión, S subconjunto de F. Diremos que S es conjunto de generadores para F sobre K si $F = K(S)$.*

F/K extensión se dice ***finitamente generada*** *si existe un conjunto finito de generadores de F sobre K, es decir $S = \{u_1 \dots u_n\}$ con $F = K(S)$*

F/K exntesión se dice ***simple*** *si existe un único elemento $u \in F$ tal que $F = K(u)$. u se llama elemento primitivo para la extensión u.*

Sea F/K extensión y $u \in F$. La **propiedad universal del anillo de polinomios** nos da un homomorfismo de anillos $\lambda : K[X] \to K[u]$ tal que conserva K y $\lambda(X) = u$. Por el primer teorema de isomorfía para anillos $K[u] \cong K[X]/ker(\lambda)$

1. Si $Ker(\lambda) = 0$, existe un isomorfismo $K[X] \cong K[u]$. Entonces u se dirá **trascendente** sobre K. $K(u)$ se llama cuerpo de fracciones de $K[u]$ y es isomorfo a $K(X)$ (cuerpo de fracciones de $K[X]$).

2. Si $Ker(\lambda) \neq 0$ se dice que u es **algebraico** sobre K y al ser $K[X]$ dominio de ideales principales, se tendrá $Ker(\lambda) = (p(X))$ para algún polinomio que además podemos considerar mónico. Además $p(X) = Irr(u, K)$ y por tanto $K[X]/Ker(\lambda)$ es dominio de integridad (tanto por ser $p(X)$ irreducible y por tanto $(p(X))$ ideal primo, como por tenerse que $K[u]$ es un subanillo de F, cuerpo).

Proposición 5. *Sea F/K extensión de cuerpos y sea $u \in F$ elemento algebraico sobre K con polinomio mínimo $p(X) = Irr(u, K)$. Entonces:*

1. *$K(u) = K[u] \cong K[X]/(p(X))$*

2. *$[K(u) : K] = gr(p(X)) \equiv$ grado de u sobre K y una base de $K[u]$ como K espacio vectorial es \${1,u,u^2,... u^{n-1}}.*

3. *Para $f \in K[X]$ se verifica $f(u) = 0$ si y solo si $p|f$*

Proposición 5. ***Elementos algebraicos en torres de cuerpos***

Sea $F \supset E \supset K$ y sea $u \in F$ algebraico sobre K. Entonces u es algebraico sobre E y $Irr(u, E)$ divide a $Irr(u, K)$

Proposición 6. ***Caracterización de elementos algebraicos***

Sea F/K extensión. El elemento $\alpha \in F$ es algebraico sobre K si y solo si la extension $K(\alpha)/K$ es finita.

Se deduce a partir de 3 y 4 desde 5

Extensiones algebraicas

Definición. *Una extensión F/K se llama* algebraica *si todos los elementos de F son algebraicos sobre K Una extensión F/K se llama* trascendente *si existe algún elemento $u \in F$ que es trascendente sobre K.*

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 $n_1, \ldots, n_k$ tiene grado menor o igual $n_1 n_2 \ldots n_k$*

Teorema 2. *K algebraico sobre F y L algebraico sobre K entonces L es algebraico sobre F*

Proposición 6. *Sea F/K extensión arbitraria y sea S un subconjunto de F.*

1. *Para todo $u \in K[S]$ existe un subconjunto finito $\{u_1, \ldots, u_n\} \subset S$ tal que $u \in K[u_1, \ldots, u_n]$*
2. *Para todo $u \in K(S)$ existe un subconjunto finito $\{u_1, \ldots, u_n\} \subset S$ tal que $u \in K(u_1 \ldots u_n)$.*

Proposición 7. *Sean $L \supset E, F \supset K$. Entonces:*

1. *Si $F = K(S)$ entonces $EF = E(S)$*
2. *$[EF : K] \leq [E : K][F : K]$*
3. *Si $[E : K]$ y $[F : K]$ son primos relativos, se da la igualdad.*

La primera parte se deduce de que $EF = E(F) = E(K(S)) = E(S)$

Para deducir la segunda parte: $[EF : K] = [EF : F][F : K]$ por el teorema del grado. Además si tenemos B base de E como K espacio vectorial, y B' base de F como K espacio vectorial, tendremos que $B \cap B'$ es sistema de generadores de $EF = F(E)$ y por tanto $[EF : F] < |B| = [E : K]$. Además, del argumento hecho se deduce 3.

Proposición 7. *Sea $F = K(u_1, \dots u_n)$ una extensión finitamente generada por elementos u_i algebraicos. Entonces la extensión F/K es finita.*

La demostración se deduce de 2 de 7 sin más que tener en cuenta que $K(u1, \dots u_n)$ estará contenido en $\prod_{i=1}^{n} K(u_i)$ y esa extensión es finita.

Corolario 2. *Sea $F = K(S)$ con $S \subset F$ arbitrario. Entonces F/K es algebraica si y sólo si todo elemento $u \in S$ es algebraico sobre K*

La implicación hacia la derecha es trivial. Para la implicación hacia la izquierda basta usar que dado $s \in K(S)$, existirán finitos $\{u_{1,s}, \dots u_{n,s}\} \subset S$ algebraicos verificando $s \in K(\{u_{1,s}, \dots u_{n,s}\}$ y la proposición anterior acaba, al tener una extensión finitamente generada por elementos algebraicos, lo que implica que la extensión es finita, y que s es algebraico sobre K.

Corolario 3. ***Relación de extensiones finitas y algebraicas***

Se tiene:

1. *Si la extensión F/K es finita, entonces es algebraica (y finitamente generada por ser finita)*
2. *Una extensión F/K es algebraica y finitamente generada, entonces es finita.*

Se deduce trivialmente de las proposiciones y corolarios anteriores.

Corolario 4. *Un elemento $u \in F$ es algebraico sobre K si y solo si existe un cuerpo intermedio E verificando que E/K es extensión finita y $u \in E$.*

La implicación hacia la izquierda es trivial sin más que considerar $K(u)$. La implicación hacia la derecha se deduce de ser E extensión finita, luego algebraica sobre K.

Corolario 5. *Dada una torre de cuerpos $E \supset F \supset K$ la extensión E/K es algebraica si y solo las extensiones E/F y F/K son algebraicas.*

Cuerpos de descomposición

Teorema 3. ***Teorema de Kronecker***

Sea f un polinomio de grado positivo sobre un cuerpo K. Entonces existe una extensión F/K y un $u \in F$ verificando $f(u) = 0$. Esta extensión viene dada por $K[X]/(f_1)$ con f_1 un factor irreducible del polinomio sobre K.

Definición. ***Extensión de homomorfismos***

Sean F_i/K_i dos extensiones de cuerpos y sean $\tau : F_1 \to F_2$ y $\sigma : K_1 \to K_2$ homomorfismos verificando $\tau(a) = \sigma(a)$. A τ lo llamamos ***extensión de*** *σ. Si $\sigma = id$, lo llamamos* ***homomorfismo sobre*** *K*

Proposición 8. *Sea $\alpha : K_1 \to K_2$ un isomorfismo de cuerpos. Existe una única extensión a un isomorfismo $\sigma : K_1[X] \to K_2[X]$ definido por $\sigma(x) = x$*

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

Proposición 9. *En las condiciones de la proposición anterior si F_i/K_i son extensiones algebraicas, $\tau : F_1 \to F_2$ un homomorfismo sobre $\sigma : K_1 \to K_2$ y $u \in F_1$ una raíz de f_1. Entonces $\tau(u)$ es una raíz de $f_2 = \sigma(f_1)$*

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

Entonces:

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

Corolario 6. *Sea F/K extensión algebraica y $\sigma : F \to F$ un homomorfismo sobre K. Entonces σ es un automorfismo.*

Para demostrar esto, veamos que la aplicación es sobreyectiva (es inyectiva por ser homomorfismo de cuerpos). Consideramos $u \in F$. Tomo

$f = Irr(u, K)$, que puedo hacerlo por tratarse de una extensión algebraica, y se tiene que $\sigma(f) = f$. Tomo todas las raíces $\{u_1, \dots u_k\}$ de f que hay en F. Tomo $F_1 = K(u_1 \dots u_k)$ el subcuerpo de F generado por todas ellas. La extensión F_1/K es finita y para cualquier homomorfismo $\sigma : F \to F$ verifica que $\sigma(u_i)$ es raíz de f. Así, $\sigma|F_1$ e una aplicación lineal inyectiva, luego sobreyectiva y eso nos lleva a decir que $\exists v \in F_1$ verificando $\sigma(v) = u$.

Proposición 10. *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 $\tau : K_1(u_1) \to K_2(u_2)$ sobre σ 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 $X + (f_i) \mapsto u_i$. $\bar{\sigma}$ lo obtenemos por la proposición anterior llevándonos (f_1) en (f_2). La aplicación buscada será $\tau = \rho_2 \bar{\sigma} \rho_1^{-1}$

Definición. ***Cuerpo de descomposición*** *Un cuerpo extensión $F \supset K$ se llama /cuerpo de descomposición de f sobre K sii existen $u_1 \dots u_n \in F$ tales que $f(X) = (X - u_1) \cdots (X - u_n)$, y $F = K(u_1, \dots u_n)$. Es decir, esta última condición nos dice que es el menor cuerpo en que descompone el polinomio.*

Proposición 11. ***Cuerpo de descomposición sobre cuerpos intermedios*** *Sea $E \supset F \supset K$ torre de cuerpos tal que $$ es cuerpo de descomposición de un polinomio f sobre K. Entonces E es también cuerpo de descomposición de f sobre F.*

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

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

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

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

Se deduce que $E = K(\alpha_1, \dots, \alpha_n)$ donde α_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

Teorema 4. ***Grado del cuerpo de descomposición*** *Un cuerpo de descomposición F de un polinomio de grado n sobre K es de grado como mucho $n!$ sobre K. Si el grado es $n!$ entonces el polinomio es irreducible. El recíproco no se verifica.*

El recíproco no se verifica en el caso de $(X^2-2)(X^2-3) \in \mathbb{Q}(X)$ que es irreducible, pero su cuerpo de descomposición es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ que tiene grado 4.

Teorema 5. ***Extensión a cuerpos de descomposición*** *Sea $\sigma : K_1 \to K_2$ isomorfismo de cuerpos, $f_1 \in K_1[X]$ y sea $f_2 = \sigma(f_1)$. Sea F_i cuerpo de descomposición de f_i sobre K_i. Entonces existe un isomorfismo $\tau : F_1 \to F_2$ que es una extensión de σ. De aquí se deuce que dos cuerpos de descomposición de un $f \in K[X]$ son isomorfos.*

Definición. ***Cuerpo de descomposición*** *Sea $\mathcal{F} \subset K[X]$ cualquier conjunto de polinomios no constantes. Una extensión E/K se llama cuerpo de descomposición de $\mathcal{F}$ si es cuerpo de descomposición de cada uno de sus polinomios. Además $E = K(\{u \in F : \exists f \in \mathcal{F}, f(u) = 0\})$*

Teorema 6. ***Existencia de cuerpo de descomposición*** *Para todo conjunto de polinomios no constantes $\mathcal{F} \subset K[X]$ existe un cuerpo de descomposición sobre K*

Teorema 7. *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 $\sigma : F \to \bar{K}$ sobre K tiene una extensión $\tau : E \to \bar{K}$ (¡ojo! extensión del homomorfismo*

Tomamos:

$$S = \{(E_i, \sigma_i) : F \subset E_i \subset E, \sigma_i : E_i \to \bar{K} \qquad \sigma_{i|F} = \sigma\}$$

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, σ_1). Supongamos $E_1 \subsetneq E$ existe un $u \in E, u \neq E_1$ del que podemos tomar $f = Irr(u, K)$ (porque E/K es algebraica) y por la proposición 10, como todos los α_i mantienen K, llamando $f_1 = f_2 = f$ en dicha proposición, tengo que existen un a $\sigma_2 : E_1(u) \to (\sigma_1(E_1))(u)$ que extiende $\sigma_1' : E_1 \mapsto \sigma(E_1)$ y el par $(E_1(u), \sigma_2)$ sería entonces maximal, contradicción, luego $E_1 = E$ y $\tau = \sigma_1$.

Extensiones normales

Proposición 12. *Sean $u, v \in \bar{K}$.Los siguientes enunciados equivalen:*

1. *$Irr(u,K) = Irr(v,K)$*
2. *Existe isomorfismo $\tau : K(u)/K \to K(v)/K$ tal que $\tau(u) = v$*
3. *Existe homomorfismo $\alpha_1 : K(u)/K \to \bar{K}/K$ tal que $\sigma(u) = v$*
4. *Existe un automorfismo $\alpha : \bar{K}/K \to \bar{K}/K$ 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 7

Teoría de Galois

Proposición 8. *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 9. ***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 7. *Si $[F_1 : K] = n$ existen a lo sumo n homomorfismos distintos de F_1 a F_2 que fijan K. Es decir $|Hom(F_1/K, F_2/K)| \leq n$*

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

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

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 $c_1 \ldots c_{n+1} \in F_2$ 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:*

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

Corolario 8. *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 $G < Aut(E)$ subgrupo del grupo de automorfismos de E. Llamamos subcuerpo de E fijo por G.* $\backslash[E^G = \{u\in E/\forall \ \sigma \in \ G \ \sigma(u) = u\}\backslash$

Teorema 8. ***Teorema de Artin*** *Sea G subgrupo finito de $Aut(E)$. Entonces $[E : E^G] = |G|$*

Llamo $K = E^G$. Por el corolario anterior sabemos que $|Aut(E/K)| \leq [E : K]$ y $G \subseteq |Aut(E/K)|$, 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:

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

Sea $a_1, \dots a_{n+1} \in E$ solución con el mínimo número de elementos no nulos. Sea Un automorfismo $\sigma \in Aut(K)$ 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 $G < Aut(E)$ tal que $E^G = K$. En este caso, el grupo se representa por $Gal(E/K)$ y se llama grupo de Galois de la extensión E/K*

Proposición 13. *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 $\sigma : E \to \bar{K}$, 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 $\tau : E \to K$ 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 $\tau : E \to \bar{K}$ 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.

- Correspondencia de Galois

  Sea E/K extensión finita de Galois, $G = Gal(E/K)$. Definimos una correspondencia entre el conjunto $\mathcal{S}(G)$ de subgrupos de G y el conjunto $\mathcal{F}(E/K)$ de cuerpos intermedios de E/K. Para $H < G$ definimos $E^H = H^*$. A cada cuerpo intermedio F entre E y K le hacemos corresponder el grupo de Galois de la extensión E/F y llamamos $G^F = F^*$

  A $F \mapsto F^*, H \mapsto H^*$ las denominamos correspondencia de Galois para la extensión E/K

  Proposición 14. *Sean F, F_1, F_2 cuerpos intermedios de E/K y H, H_1, H_2 subgrupos de $G = Gal(E/K)$. Entonces:*

  1. $F_1 \subset F_2 \implies F_2^* \subset F_1^*$; $H_1 \subset H_2 \implies H_2^* \subset H_1^*$
  2. $F \subset F^{**}$; $H < H^{**}$
  3. $F^* = F^{***}$; $H^* = H^{***}$

  Teorema 9. ***Teorema fundamental*** *Sea E/K una extensión de Galois finita con grupo $G = Gal(E/K)$*

  1. *La correspondencia de Galois establece una biyección $\mathcal{F}(E/K) \cong \mathcal{S}(G)$ dada por $F = H^* \leftrightarrow H = F^*$. Además $F_1 \subset F_2$ si y solo si $H_1 \subset H_2$*

2. Dicha biyección es antiisomorfismo de retículos: $(F_1 \cdot F_2)^* = F_1^* \cap F_2^*$ *y* $(F_1 \cap F_2)^* = F_1 * \vee F_2^*$

3. $F_1/K, F_2/K$ *son conjugadas si y sólo si los subgrupos* F_1^* *y* F_2^* *son conjugados en* G.

4. F/K *es normal sii* F^* *es un subgrupo normal de* G. *En este caso* $Gal(F/K) \cong G/F^*$

5. Para todo subgrupo $H < G$ *se tiene* $|H| = [E : H^*]$ *y* $[G : H] = [H^* : K]$. *Para todo* $F \in \mathcal{F}(E/K)$ *se verifica* $[E : F] = |F^*|$ *y* $[F : K] = [G : F^*]$

Demostración de 5.

$|G| = [E : E^G] = [E : K]$ y $|H| = [E : E^H] = [E : H^*]$ por tereoma de Artin.

Por Lagrange $|G| = [G : H]|H|$. Simplificando factores $[F : K] = [G : F^*]$

Por el grado de las extensiones: $[E : K] = [E : H^*][H^* : K]$

Demostración de 1.

Tenemos la torre $G > H^{**} > H$ y:

$$[G : H^{**}] = [H^{***} : K] = [H^* : K] = [G : H]$$

Tenemos la torre $E \supset F^{**} \supset F$ y:

$$[E : F] = |F^*| = |F^{***}| = [E : F^{**}]$$

La segunda parte sale de la proposición anterior y de haber probado que la conexión de Galois nos da una biyección.

Demostración de 2.

Por ser antiisomorfismos de conjuntos ordenados (son biyecciones de conjuntos que invierten el orden).

Demostración de 3.

Sea $f : E/K \to E/K$ isomorfismo que conjuga F_2 y F_1 (esto es $f(F_1) = F_2$. Sea $u = f(v) \in F_2; v \in F_1$. Así, dado $\tau \in F_1^*$ automorfismo, se tiene $f\tau f^{-1}(u) = f\tau(v) = f(v)$, luego $fF_1^*f^{-1} \subset F_2^*$

El otro contenido es igual.

Demostración de 4.

Desde 3.

Para demostrar la isomorfía: $\Phi : G = Gal(E/K) \to Gal(F/K)$ dado por restricción. Aplicando primer teorema de isomorfía:

$$Img(\Phi) = Gal(F/K) \cong Gal(E/K)/Ker(\Phi)$$

Y $Ker(\Phi) = F^*$. Estamos usando 12 y que E es normal por ser de Galois.

- Propiedades de extesniones de Galois

  Proposición 15. *Sea $K \subset F \subset E$ una torre de cuerpos tal que E/K es una extensión de Galois finita. Entonces la extensión E/F es de Galois finita y el grupo $Gal(E/F)$ es un subgrupo de $Gal(E/K)$*

  Definición. *Una extensión finita E/K **de Galois** se dice:*

  1. ***Abeliana** si el gupo $G = Gal(E/K)$ es abeliano.*
  2. ***Cíclica** si $G = Gal(E/K)$ es cíclica.*

  *3 **Soluble** si G es soluble*

???

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

Proposición 16. *$Aut(K)$ es grupo bajo la composición y $Aut(K/F)$ es un subgrupo.*

Proposición 17. *Dado un polinomio con coeficientes en K, $\sigma \in K$, si α es raíz del polinomio, entonces $\sigma\alpha$ es raíz del polinomio.*

Proposición 18. *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 19. *1. $F_1 \subseteq F_2 \subseteq K$ son dos subcuerpos de K entonces $Aut(K/F_2) \leq Aut(K/F_1)$*

2. $H_1 \leq H_2 \leq Aut(K)$ *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 20. *Sea* E *el cuerpo de descomposición sobre* F *del polinomio* $f(x) \in F[x]$*. Entonces:*

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

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:

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

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 9. *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 $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \equiv \mathbb{Z}_2$

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 raices 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 $x^4 - 2 = Irr(\sqrt[4]{2}, \mathbb{Q})$ 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:

$$< \sigma, \tau : \sigma^2 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma >= K_4$$
$$< \sigma, \tau : \sigma\tau = \tau\sigma^2, \tau^2 = 1, \sigma^3 = 1 >= S_3$$

Ejercicios

Ejercicio 1.24

Dado un término $X_1^{e_1}\cdots X_n^{e_n}$ con $e_1 \geq \ldots \geq e_n$, 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 $d_1,\ldots d_m$, $d_1 > \ldots > d_m$, donde $d_1,\ldots d_m \in \{e_1,\ldots e_n\}$

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

Por combinatoria, sabemos por tanto que $k = \prod k_i!$ y que tendremos un número $\dfrac{k}{n}$ 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 α, β, γ. Calcula el valor de $\left(\dfrac{1}{\alpha+1}\right)^3 + \left(\dfrac{1}{\beta+1}\right)^3 + \left(\dfrac{1}{\gamma+1}\right)^3$

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

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

Luego $a = \dfrac{1}{\alpha+1}, b = \dfrac{1}{\beta+1}, c = \dfrac{1}{\gamma+1}$ 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:

$$e_1 = -2$$
$$e_2 = 3$$
$$e_3 = 1$$

Así $a^3+b^3+c^3 = 13$

Ejercicio 2.14

Sea A un anillo y $\phi : A[X] \to A[X]$ 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 ϕ sea un isomorfismo?*
2. ¿Qué ocurre cuando A no es un DI?

1-

Se tiene $\phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} a_i f(X)^i$, 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 ϕ 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, ϕ 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 ϕ 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 $F = \dfrac{\mathbb{Q}[X]}{(f(X))}$ 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:

$$f(X) = p_1(X) \cdot p_2(X), \qquad gr(p_1) \geq 1, gr(p_2) \geq 1$$

Tomamos el menor $n \in \mathbb{N}$ verificando $nP = (b_l + b_{l-1}x^{l-1} + \cdots b_0) \cdot (c_m x^m + c_{m-1}x^{m-1} + \cdots c_0)$ 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 $p \nmid b_i$, $p \nmid c_j$

Así, $n_{k+t} = b_{k+t}c_0 + b_{k+t-1}c_1 + \cdots b_k c_t + \cdots + b_0 c_{k+t}$

Pero como $p \mid b_{k+t}c_0, p \mid b_{k+t-1}c_1, \ldots b_{k+1}c_{t-1}, b_{k-1}c_{t+1}, \ldots b_0 c_{k+l}$ necesariamente debe tenerse, por $p \mid n$ que $p \mid b_k c_t$, 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 $F[X]$:

$$f(x) = \sum (a_i + (f(X)) \cdot (X^i + (f(X))) = \sum (a_i \cdot X^i + (f(X))) =$$

$$= (\sum a_i X^i + (f(X))) = (f(X) + (f(X))) = (f(X))$$

Luego es una raíz del polinomio.

Ejercicio 2.16

Describe los elementos del cuerpo $\dfrac{\mathbb{F}_2[X]}{(X^3 + X + 1)}$, 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:

$$0 = 0 + (X^3 + X + 1)$$

$$1 = 1 + (X^3 + X + 1)$$

$$a = X + (X^3 + X + 1)$$

$$b = X + 1 + (X^3 + X + 1)$$

$$c = X^2 + X + 1 + (X^3 + X + 1)$$
$$d = X^2 + X + (X^3 + X + 1)$$
$$e = X^2 + (X^3 + X + 1)$$
$$f = X^2 + 1 + (X^3 + X + 1)$$

- 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 $Irr(\alpha, \mathbb{Q})$

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:

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

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 $\sqrt{2} = a + b\sqrt{3}, \quad a, b \in \mathbb{Q}$ ni $\sqrt{2} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q}$

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, $Irr(\alpha, \mathbb{Q})$

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 ω 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 β 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 $\dfrac{\mathbb{F}_2[X]}{x^2+x+1}$ con x^2+x+1 irreducible en $\mathbb{F}_2[X]$)

3-

Si β 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:

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

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

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

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 $p(X) = Irr(\alpha, K)$ 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 ω raíz $n-$ oésima 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 $\sigma : E/K \longrightarrow E/K$ tal que $f_1^\sigma(X) = f_2(X)$

Sea α raíz de f_1 y β raíz de f_2 en una clausura de K. Como $f = Irr(\alpha, K)$, $f = Irr(\beta, K)$, tenemos que existe un isomorfismo $\sigma : \overline{K}/K \longrightarrow \overline{K}/K$ 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 $\mathbb{F}_{7^7}$
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 $\mathbb{F}_{7^7}$ 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 $X^p - t^p = (X-t)^p = Irr(t, \mathbb{F}_{p^2}(t^p))$, 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 $K = \{e \in e | \phi_i(e) = e, 1 \leq i \leq n\}$. 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 $G = Gal(f/K)$. 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 $Gal(f/K) = Gal(E/K)$. Sabemos que E/K es de Galois $\Longleftrightarrow$ E/K es normal y separable, luego:

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

$2 \implies 1$.

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 contradición, ya que α_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 $\sigma : K(\alpha_1, \ldots \alpha_n) \longrightarrow K(\alpha_1, \alpha_n)$ sobre φ.

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

Ejercicio 7.27

Prueba que los subgrupos transitivos de S_4 son los subgrupos siguientes:

1. S_4, que es normal.

2. A_4, que es normal.
3. $D_4 =< (1234), (13) >$ y todos sus conjugados.
4. $C_4 =< (1234) >$, y todos son conjugados.
5. $V = \{1, (12)(34), (13)(24), (14)(23)\}$ que es normal.

Como consecuencia, si $f(X) \in \mathbb{Q}[X]$ es un polinomio irreducilbe de grado cuatro, el grupo de Galois de $\mathbb{Q}(f)/\mathbb{Q}$ es isomorfo a uno de estos.

---

1. Es claro que S_4 es transitivo, ya que $E = (12)(34), (13)(24), (14)(24), id \subseteq S_4$ y con alguno de estos elementos, dado $x, y \in \{1, 2, 3, 4\}$ puedo tomar un $\tau \in E$ verificando $\tau(x) = y$.
2. A_4 es transitivo, ya que dado $x, y \in 1, 2, 3, 4$, si $x \neq y$, siempre me puedo tomar $z, u \in \{1, 2, 3, 4\} \setminus \{x, y\}$ con $z \neq u$ y la permutación $\tau = (xy)(zu)$ está en A_4, y cumple $\tau(x) = y$
3. D_4 es transitivo porque contiene a C_4 que lo es, ya que uno de sus generadores es (1234).
4. C_4 es transitivo porque:

$$
\begin{aligned}
\tau_0 &= (1234) \\
\tau_1 &= (1234)^2 = (13)(24) \\
\tau_2 &= (1234)^3 = (1234)(13)(24) = (1432) \\
\tau_3 &= (1234)^4 = id
\end{aligned}
$$

Estos elementos pertenecen a C_4 y se tiene:

$$
\begin{aligned}
&\tau_0(1) = 2, \tau_0(2) = 3, \tau_0(3) = 4, \tau_0(4) = 1 \\
&\tau_1(1) = 3, \tau_1(2) = 4, \tau_1(3) = 1, \tau_1(4) = 2 \\
&\tau_2(1) = 4, \tau_2(2) = 1, \tau_2(3) = 2, \tau_2(4) = 3 \\
&\tau_3(x) = x \qquad \forall x \in \{1, 2, 3, 4\}
\end{aligned}
$$

1. $V = \{\sigma_0 = 1, \sigma_1 = (12)(34), \sigma_2 = (13)(24), \sigma_3 = (14)(23)\}$

$$\begin{aligned}
&\sigma_0(x) = x \qquad \forall x \in \{1,2,3,4\} \\
&\sigma_1(1) = 2, \sigma_1(2) = 1, \sigma_1(3) = 4, \sigma_1(4) = 3 \\
&\sigma_2(1) = 3, \sigma_2(2) = 4, \sigma_2(3) = 1, \sigma_2(4) = 2 \\
&\sigma_3(1) = 4, \sigma_3(2) = 3, \sigma_3(3) = 2, \sigma_3(4) = 1
\end{aligned}$$

Veamos por otro lado que el conjugado de un subgrupo transitivo, es transitivo, ya que si tengo $H < S_4$ subgrupo transitivo, $\sigma \in S_4$, $A = \sigma^{-1}H\sigma$, y dados $x, y \in \{1,2,3,4\}$.

Si $\sigma(y) = z \neq y$, tomo $\tau \in H$ verificando $\tau(\sigma(x)) = z$, que existe por ser H transitivo y se tendrá que $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}(z) = y$

Veamos ahora que son los únicos subgrupos transitivos. El orden de un subgrupo $H < G$ debe dividir a $|G|$. Además, un subgrupo transitivo debe tener necesariamente 4 o más elementos, ya que hay 4 posibles mapeos $x \mapsto y$ con $x, y \in \{1,2,3,4\}$ y 3 elementos sólo pueden darme 12 mapeos diferentes (4 cada uno).

Los posibles subgrupos, salvo conjugación e isomorfismo, de S_4 son:

Subgrupo
A_4
D_4
S_3
C_4
V
$V_4 = \{1, (12), (34), (12)(34)\}$
$\{1, (123), (132)\}$
$\{1, (12)\}$
$\{1, (12), (34)\}$
$\{1\}$

Claramente, S_3 es intransitivo, puesto que $\sigma(4) = 4, \forall \sigma \in S_3$; V_4 también es intransitivo, puesto que $\sigma(1) \neq 3, \forall \sigma \in V_4$. Y el resto de subgrupos tienen menos de 4 elementos.

Ejercicio 7.28

Sea $f(X) \in K[X]$ un polinomio separable y g un factor irreducible de f. ¿Actúa transitivamente $G = Gal(f/K)$ sobre las raíces de g?

Sean u, v raíces de g en E cuerpo de descomposición de f. Entonces como $K[X]/(Irr(u,K)) = K[X]/(g) \cong K(u)$ y $K[X]/(Irr(v,K)) = K[X]/(g) \cong K(v)$ dados por $X+(g) \mapsto u$ y $X+(g) \mapsto v$ respectivamente. Entonces existe un isomorfismo $\tau : K(u) \to K(v)$ verificando $\tau(u) = v$. Este isomorfismo puede extenderse a un automorfismo $\sigma : E \to E$ y por tanto tenemos un automorfismo que fija K y que lleva una raíz en otra. Pero la elección de las raíces la hemos hecho arbitrariamente.