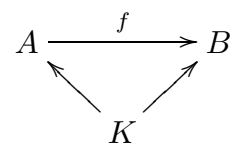
TEORÍA DE CUERPOS (VERSIÓN PRELIMINAR)

Jorge A Guccione y Juan J. Guccione

1. Algebras y extensiones

Sea K un anillo conmutativo. Una K-álgebra es un anillo A junto con una estructura de K-módulo a izquierda de A que satisface $\lambda(ab) = (\lambda a)b = a(\lambda b)$ para todo $\lambda \in K$ y $a, b \in A$. Un morfismo $f\colon A \to B$ de K-álgebras es una función que es simultaneamente un morfismo de anillos y de K-módulos. Claramente la composición (en el sentido conjuntista) de dos morfismos de K-álgebras es un morfismo de K-álgebras. Dos elementos x e y de una K-algebra A se llaman conjugados si existe un automorfismo de K-álgebras $f\colon A \to A$ tal que $f(x) = y$. Una K-álgebra es conmutativa si lo es como anillo. Sea A una K-álgebra. Un subconjunto B de A es una subálgebra de A si es a la vez un subanillo y un submódulo de A. Es claro que B es en si mismo una K-álgebra y que la inclusión canónica de B en A es un morfismo de K-álgebras. El centro $\mathrm{Z}(A)$ de A es el conjunto de todos los elementos $a \in A$ que satisfacen $ab = ba$ para todo $b \in A$. Es claro que $\mathrm{Z}(A)$ es una subálgebra conmutativa de A.

Observación 1.1. Dada una K-álgebra A se obtiene un morfismo $\varphi\colon K \to \mathrm{Z}(A)$ definiendo $\varphi(\lambda) = \lambda 1$. Recíprocamente, dado un morfismo de anillos $\varphi\colon K \to \mathrm{Z}(A)$, se le puede dar a A una estructura de K-álgebra, poniendo $\lambda a = \varphi(\lambda)a$. Como claramente estas construcciones son recíprocas, tener una K-álgebra A equivale a tener un morfismo de anillos de K en $\mathrm{Z}(A)$. Con esta interpretación un morfismo de K-álgebras $f\colon A \to B$ es un morfismo de anillos tal que el triángulo,



conmuta.

Observación 1.2. Sea E una K-álgebra. La intersección de una familia de subálgebras de E es una subálgebra de E. En particular, dado un subconjunto S de E existe una mínima subálgebra $K[S]$ de E que contiene a S.

Notación 1.3. Sean F y G dos subálgebras de una K-álgebra E. Denotamos con $F\square G$ a la mínima subálgebra de E que contiene a F y a G. Es claro que $F\square G = G\square F$ y que si los elementos de F conmutan con los de G, entonces $F\square G = \{\sum x_i y_i : x_i \in F \text{ y } y_i \in G\}$. Si además F es conmutativo, entonces $F\square G = F[G]$.

Definición 1.4. Sea K un cuerpo. Se llama extensión de K a toda K-álgebra E que es un cuerpo. Un morfismo de extensiones es un morfismo de K-álgebras. Si una subálgebra F de una extensión E de K es un cuerpo, decimos que F es una subextensión de E.

Notaciones 1.5. Denotamos con E/K a una extensión E de K y denotamos con $\mathrm{Hom}(E/K, F/K)$ al conjunto de morfismos de una extensión E/K en otra F/K. Cuando $E/K = F/K$ a este conjunto lo denotamos con $\mathrm{End}(E/K)$. Finalmente, denotamos con $\mathrm{G}(E/K)$ o $\mathrm{Aut}(E/K)$ al subconjunto de $\mathrm{End}(E/K)$ formado por los automorfismos de E/K.

Observación 1.6. $\mathrm{Aut}(E/K)$ y $\mathrm{End}(E/K)$, provistos de las operaciones definidas por $g * f = g \circ f$ son respectivamente un grupo y un monoide. Es claro que $\mathrm{Aut}(E/K)$ es el grupo de unidades de $\mathrm{End}(E/K)$. A $\mathrm{Aut}(E/K)$ se lo denomina el grupo de Galois de la extensión E/K.

Observación 1.7. La intersección de una familia de subcuerpos de un cuerpo dado K es un cuerpo. En particular todo cuerpo K contiene a un cuerpo mínimo, que se llama el cuerpo primo de K. Si la característica de K es $p > 0$, el cuerpo primo de K es $\mathbb{Z}/p\mathbb{Z}$ y si K es de característica 0, el cuerpo primo de K es $\mathbb{Q}$. De ahora en más escribiremos $\mathbb{F}_p$ en lugar de $\mathbb{Z}/p\mathbb{Z}$.

Notación 1.8. Sea E/K una extensión y S un subconjunto de E. Denotamos con $K(S)$ al mínimo subcuerpo de E que contiene a S.

Definición 1.9. Sea E/K una extensión y F y G dos subextensiones de E. Llamamos compuesto de F y G y lo denotamos $F.G$ a la mínima subextensión de E que contiene a F y a G. Es claro que $F.G = F(G) = G(F) = K(F \bigcup G) = \left\{ \left(\sum x_i y_i\right) \left(\sum x_j y_j\right)^{-1} : x_i, x_j \in F,\ y_i, y_j \in G \text{ y } \sum x_j y_j \neq 0 \right\}$.

Observación 1.10. Sea K un cuerpo de característica positiva p. La aplicación $\sigma\colon K \to K$, definida por $\sigma(x) = x^p$, es un endomorfismo de K, que se llama morfismo de Frobenius de K. Si x pertenece al cuerpo primo de K, entonces $\sigma(x) = x$.

Observación 1.11. Todo morfismo de un cuerpo en un anillo es inyectivo.

2. Extensiones finitas

Definición 2.1. Una K-álgebra E es finita si es finitamente generada como K-módulo.

Notación 2.2. Sea K un cuerpo. Dada una K-álgebra E denotamos con $(E : K)$ a la dimensión de E como K-espacio vectorial. Cuando E es un cuerpo a $(E : K)$ se lo denomina el grado de la extensión E/K.

Sean K un anillo conmutativo, E una K-álgebra y a un elemento de A. Decimos que a es divisor de cero a izquierda si existe $b \in E \setminus \{0\}$ tal que $ab = 0$, que es divisor de cero a derecha si existe $b \in E \setminus \{0\}$ tal que $ba = 0$, que es inversible a izquierda si existe $b \in A \setminus \{0\}$ tal que $ba = 1$ y que es inversible a derecha si existe $b \in A \setminus \{0\}$ tal que $ab = 1$. Es claro que si a es inversible a izquierda, entonces no es divisor de cero a izquierda y que si a es inversible a derecha, entonces no es divisor de cero a derecha.

Proposición 2.3. *Sea K un cuerpo, E una K-álgebra finita y a un elemento de E. Son equivalentes:*

1) a no es divisor de cero a izquierda.

2) a no es divisor de cero a derecha.

3) a es inversible a izquierda.

4) a es inversible a derecha.

En consecuencia son equivalentes:

1) E no tiene divisores de cero a izquierda no nulos.

2) E no tiene divisores de cero a derecha no nulos.

3) E es un anillo de división.

Demostración. Ya sabemos que 3) $\Rightarrow$ 1) y 4) $\Rightarrow$ 2). Veamos que 1) $\Rightarrow$ 4) Por hipótesis la aplicación K-lineal $f_a\colon L \to L$, definida por $f_a(x) = ax$, es inyectiva y, por lo tanto, sobreyectiva. Así, existe $a' \in L$ tal que $aa' = 1$. Similarmente 2) $\Rightarrow$ 3). $\square$

Proposición 2.4. *Se satisfacen:*

1) Sea F una K-álgebra conmutativa y E una F-álgebra. Si $(e_i)_{i\in I}$ es un conjunto de generadores de F como K-módulo y $(f_j)_{j\in J}$ es un conjunto de generadores de E como F-módulo, entonces $(e_i f_j)_{i\in I, j\in J}$ es un conjunto de generadores de E como K-módulo. En particular si F es una K-álgebra finita y E es una F-álgebra finita, entonces E es una K-álgebra finita.

2) Sean F y G dos subálgebras de una K-álgebra E, tales que los elementos de F conmutan con los de G. Todo conjunto de generadores de F como K-módulo, es un conjunto de generadores de $F\square G$ como G-módulo. En particular, si G es conmutativo y F es una K-álgebra finita tal que todos sus elementos conmutan con los de G, entonces $F\square G$ es una G-álgebra finita y si además, K y G son cuerpos, entonces $(F\square G : G) < (F : K)$.

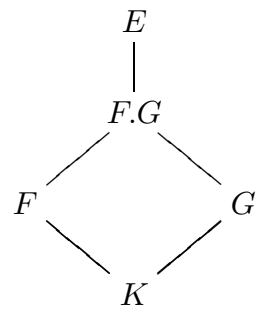
Demostración. 1) Sea $x \in E$. Existe una familia $(b_j)_{j\in J}$ con soporte finito, de elementos de F, tal que $x = \sum_j b_j f_j$. Ahora, para cada $j \in J$ existe una familia $(a_{ij})_{i\in I_j}$ con soporte finito, de elementos de K, tal que $b_{ij} = \sum_i a_{ij} e_i$. Así, $x = \sum_j b_j f_j = \sum_j \sum_i a_{ij} e_i f_j$.

2) Es inmediato. $\square$

Proposición 2.5. *Se satisfacen:*

1) Si F/K una extensión y E es una F-álgebra, entonces $(E : K) = (E : F)(F : K)$.

2) Sea,



un diagrama de extensiones. Se satisfacen:

i) Si $(F\square G : G) < \infty$, entonces $F.G$ es igual a $F\square G$.

ii) Si $(F : K) < \infty$, entonces $(F.G : G) < (F : K)$ y $F.G = F\square G$.

Demostración. 1) Por el punto 1) de la Proposición 2.4 es suficiente ver que si $(e_i)_{i\in I}$ es una familia linealmente independiente sobre K de elementos de F y

$(f_j)_{j\in I}$ es es una familia linealmente independiente sobre F de elementos de E, entonces $(e_if_j)_{i\in I,j\in J}$ es una es una familia linealmente independiente sobre K de elementos de E. Sea $0=\sum_{ij}a_{ij}e_if_j$ donde $(a_{ij})_{i\in I,j\in J}$ es una es una familia con soporte finito de elementos de K. Como $(f_j)_{j\in I}$ es linealmente independiente sobre F, tenemos que $0=\sum_i a_{ij}e_i$, para cada $j\in J$. Así, como $(e_i)_{i\in I}$ es linealmente independiente sobre K, cada a_{ij} es igual a cero.

2i) Es consecuencia inmediata de la Proposición 2.3.

2ii) Por el punto 2) de la Proposición 2.4, $(F\square G:G)<(F:K)<\infty$. Así, por i) $F.G$ es igual a $F\square G$. $\square$

3. Extensiones algebraicas

Definición 3.1. Sea K un cuerpo y E una K-álgebra. Un elemento $x\in E$ es entero o algebraico sobre K si es solución de algún polinomio no nulo con coeficientes en K. A los elementos que no son algebraicos los llamamos trascendentes.

Notación 3.2. Sea K un cuerpo, E una K-álgebra y x un elemento de E algebraico sobre K. Denotamos con $\mathrm{irr}(x,K)$ al único polinomio mónico que genera el ideal de $K[X]$ consistente de los polinomios que anulan a x. Observese que el grado de $\mathrm{irr}(x,K)$ es 1 si y sólo si $x\in K$ y que si $x\in E$ es algebraico y E no tiene divisores de cero no nulos, entonces $\mathrm{irr}(x,K)$ es irreducible. Cuando x es trascendente ponemos $\mathrm{irr}(x,K)=0$.

Observación 3.3. Sea F/K una extensión y E una F-álgebra. Todo elemento x de E entero sobre K es entero sobre F. Además $\mathrm{irr}(x,F)\mid\mathrm{irr}(x,K)$.

Proposición 3.4. *Sea K un cuerpo, E una K-álgebra y $x\in E$ un elemento entero sobre K. Son equivalentes:*

1) $\mathrm{gr}(\mathrm{irr}(x,K))=n$.

2) $\{1,x,x^2,\ldots,x^{n-1}\}$ *es una base de* $K[x]$ *como* K*-espacio vectorial.*

En particular x es entero sobre K si y sólo si $K[x]$ es finita sobre K. En este caso también tenemos que $(K[x]:K)=\mathrm{gr}(\mathrm{irr}(x,K))$.

Demostración. Es inmediato. $\square$

Definición 3.5. Sea K un cuerpo y E una K-álgebra. Si todos los elementos de E son enteros sobre K decimos que E es entera. Si E es un cuerpo decimos también que E es algebraica.

Proposición 3.6. *Sea K un cuerpo, E una K-álgebra entera y a un elemento de E. Son equivalentes:*

1) a no es divisor de cero a izquierda.

2) a no es divisor de cero a derecha.

3) a es inversible a izquierda.

4) a es inversible a derecha.

En consecuencia son equivalentes:

1) E no tiene divisores de cero a izquierda no nulos.

2) E no tiene divisores de cero a derecha no nulos.

3) E es un anillo de división.

Demostración. Ya sabemos que 3) $\Rightarrow$ 1) y 4) $\Rightarrow$ 2). Veamos que 1) $\Rightarrow$ 4) Por la equivalencia entre los puntos 1) y 4) de la Proposición 2.3, existe $a' \in K[a]$ tal que $aa' = 1$. Similarmente 2) $\Rightarrow$ 3). $\square$

Proposición 3.7. *Sea K un cuerpo y E una K-álgebra conmutativa. Son equivalentes:*

1) E es finita.

2) E es entera y existe un conjunto finito S de elementos de E tal que $E = K[S]$.

3) Existe un conjunto finito de elementos enteros S de E tal que $E = K[S]$.

Demostración. 1) $\Rightarrow$ 2) Tomemos como S a cualquier conjunto finito de generadores de E como K-módulo. Para cada $x \in E$, la K-álgebra $K[x]$ es finita. Así, por la Proposición 3.4, E es entera.

2) $\Rightarrow$ 3) Es trivial.

3) $\Rightarrow$ 1) Tomemos $x \in S$. Podemos suponer por inducción que $K[S \setminus \{x\}]$ es finita sobre K. Ahora, por el item 2) de la Proposición 2.4 y por la Proposición 3.4, $K[S]$ es finita sobre $K[S \setminus \{x\}]$. Así, por el item 1) de la Proposición 2.4, E es finita sobre K. $\square$

Observese que en la demostración de 3) $\Rightarrow$ 1) es en el único lugar en el que se usa que E es conmutativa.

Proposición 3.8. *Sea K un cuerpo y E una K-álgebra conmutativa. Si $S \subseteq E$ es un conjunto de elementos enteros de E, entonces $K[S]$ es una K-álgebra entera. Si además E es un dominio, entonces $K[S]$ es un cuerpo.*

Demostración. Dado $x \in K[S]$ existe $S' \subseteq S$ finito tal que $x \in K[S']$. Por la Proposición 3.7, x es algebraico. Como esto vale para cada $x \in K[S]$, la K-álgebra $K[S]$ es entera. Por último, si E es un dominio, también lo es $K[S]$, de donde, por la Proposición 3.6, $K[S]$ es un cuerpo. $\square$

Proposición 3.9. *Sea F/K una extensión algebraica y E una F-álgebra. Todo elemento de E entero sobre F es entero sobre K.*

Demostración. Sea $x \in E$ un elemento entero sobre F. Si $a_n X^n + \cdots + a_0 \in F[X]$ es un polinomio con $a_n \neq 0$, en el que x se anula, entonces x es entero sobre $K[a_0, \ldots, a_n]$, que por la Proposición 3.8, es un cuerpo. Como, por la Proposición 3.4, $K[a_0, \ldots, a_n][x]$ es una $K[a_0, \ldots, a_n]$-álgebra finita y, por la Proposición 3.7, $K[a_0, \ldots, a_n]$ es una K-álgebra finita, tenemos que $K[a_0, \ldots, a_n][x]$ es una K-álgebra finita. Así, $K[x]$ es finita y, por la Proposición 3.4, x es entero sobre K. $\square$

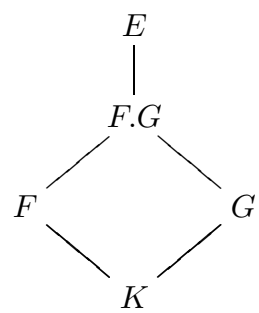
Corolario 3.10. *Sea E una K-álgebra conmutativa. Los elementos de E que son enteros sobre K forman una subálgebra F de E. Si además E es un dominio, entonces F es un cuerpo y todo elemento de E que es entero sobre F pertenece a F.*

Definición 3.11. Sea K un cuerpo y E una K-álgebra. La clausura entera F de K en E es el conjunto de los elementos de E que son enteros sobre K. Cuando F es igual a K decimos que K es algebraicamente cerrado en E.

Proposición 3.12. *Se satisfacen:*

1) Sea F/K una extensión y E una F-álgebra. Entonces E es entero sobre K si y sólo si E es entero sobre F y F/K es algebraica.

2) Sea



un diagrama de extensiones. Se satisfacen:

i) Si $F\square G/G$ es entera, entonces $F.G$ es igual a $F\square G$.

ii) Si F/K es algebraica, entonces $F.G/G$ también lo es y, además, $F.G = F\square G$.

3) Si $(E_i/K)_{i\in I}$ es una familia de subextensiones algebraicas de E/K, entonces $K(\bigcup_{i\in I} E_i)/K$ también es algebraica.

Demostración. 1) Es claro que si E es entero sobre K, entonces E es entero sobre F y F/K es algebraica. Por la Proposición 3.9 si E es entero sobre F y F/K es algebraica, entonces E es entero sobre K.

2i) Se lo deduce inmediatamente de la Proposición 3.6.

2ii) Por la Proposición 3.8, $F\square G = G[F]$ es una G-álgebra entera. Así, por i) $F.G$ es igual a $F\square G$.

3) Esto se deduce inmediatamente de la Proposición 3.8. $\square$

4. Existencia de morfismos

Sean F/K y C/K dos extensiones y f un morfismo de F/K en C/K. Dado un polinomio $P = a_0 + \cdots + a_nX^n \in F[X]$, denotamos con P^f al polinomio $P^f = f(a_0) + \cdots + f(a_n)X^n \in f(F)[X]$.

Proposición 4.1. *Sean F/K, E/F y C/K tres extensiones, f un morfismo de F/K en C/K, $x \in E$ e $y \in C$. Son equivalentes:*

1) Existe $\widehat{f} \in \mathrm{Hom}(F(x)/K, C/K)$ tal que $\widehat{f}_{|F} = f$ y $\widehat{f}(x) = y$.

2) $\mathrm{irr}(x, F)^f = \mathrm{irr}(y, f(F))$.

Demostración. 1) $\Rightarrow$ 2) Es claro que si x es trascendente sobre F, entonces y lo es sobre $f(F)$. Supongamos ahora que x es algebraico sobre F. Entonces $\mathrm{irr}(x, F)^f(y) = \widehat{f}(\mathrm{irr}(x, F)(x)) = 0$ y así, como $\mathrm{irr}(x, F)^f$ es irreducible, resulta que $\mathrm{irr}(y, f(F)) = \mathrm{irr}(x, F)^f$.

2) $\Rightarrow$ 1) Es claro que si x es trascendente sobre F, entonces y lo es sobre $f(F)$ y existe $\widehat{f} \in \mathrm{Hom}(F(x)/K, C/K)$, tal que $\widehat{f}_{|F} = f$ y $f(x) = y$. Supongamos que x es algebraico. Por las Proposiciones 2.3 y 3.4, $F(x) = F[x] = F[X]/\langle \mathrm{irr}(x, F)\rangle$. Sea $g\colon F[X] \to C$ el morfismo de K-álgebras definido por $g_{|F} = f$ y $g(X) = y$. Como $g(\mathrm{irr}(x, F)) = 0$, g se factoriza a través de un morfismo $\widehat{f}$ de $F[X]/\langle \mathrm{irr}(x, F)\rangle$ en C. $\square$

Proposición 4.2. *Sean F/K y C/K dos extensiones arbitrarias, E/F una extensión algebraica, $S \subseteq E$ tal que $E = F(S)$ y $f \in \mathrm{Hom}(F/K, C/K)$. Si, para cada $x \in S$, el polinomio $\mathrm{irr}(x,F)^f$ se factoriza en $C[X]$ como un producto de polinomios lineales, entonces existe una extensión $\widehat{f}\colon E \to C$ de f.*

Demostración. Por el lema de Zorn existe un morfismo $\widehat{f}$ de E'/K en C/K que extiende a f y que es maximal con respecto a esta propiedad. Hay que ver que $E' = E$. Como $\mathrm{irr}(x,E')$ divide a $\mathrm{irr}(x,F)$, el polinomio $\mathrm{irr}(x,E')^{\widehat{f}}$ se factoriza en $C[X]$ como un producto de polinomios lineales. Sea y una de las raíces de $\mathrm{irr}(x,E')^{\widehat{f}}$. Como $\mathrm{irr}(x,E')^{\widehat{f}}$ es un polinomio irreducible de $\widehat{f}(E')[X]$, tenemos que $\mathrm{irr}(y,\widehat{f}(E')) = \mathrm{irr}(x,E')^{\widehat{f}}$. Así, por la Proposición 4.1, $x \in E'$. □

Proposición 4.3. *Sean E/K y C/K dos extensiones algebraicas, f un elemento de $\mathrm{Hom}(E/K, C/K)$ y $S \subseteq C$ tal que $C = f(E)(S)$. Si, para cada $y \in S$, $\mathrm{irr}(y,K)$ tiene la misma cantidad de raíces en C que en E, entonces f es un isomorfismo.*

Demostración. Basta ver que S está en la imagen de f. Dado $y \in S$ sean $x_1, \ldots, x_n$ las raíces de $\mathrm{irr}(y,K)$ en E. Como $f(x_1), \ldots, f(x_n)$ son raíces distintas de $\mathrm{irr}(y,K)$ en C y, por hipótesis, $\mathrm{irr}(y,K)$ tiene n raíces en C, existe $1 \leq i \leq n$ tal que $f(x_i) = y$. □

Corolario 4.4. *Si E/K es algebraica, entonces $\mathrm{Aut}(E/K) = \mathrm{End}(E/K)$.*

5. Existencia de clausura algebraica

Definición 5.1. Un cuerpo es algebraicamente cerrado si no tiene extensiones algebraicas propias.

Proposición 5.2. *Sean K un cuerpo y $P_1, \ldots, P_n$ polinomios no constantes de $K[X]$. Existe una extensión finita E/K en la que cada P_i tiene una raíz.*

Demostración. La prueba se hace por inducción en la cantidad n de polinomios. Cuando $n = 0$ no hay nada que probar. Supongamos ahora que $n > 0$ y que el resultado vale para una cantidad menor que n de polinomios. Sea Q un factor irreducible de P_1 y $F = K[X]/\langle Q\rangle$. Es claro que F/K es una extensión finita y que la clase de X en F es una raíz de Q y, por lo tanto, de P_1. Para terminar la demostración basta observar que, por hipótesis inductiva, existe una extensión finita E/F en la que cada P_i con $2 \leq i \leq n$ tiene una raíz. □

Proposición 5.3. *Sea K un cuerpo. Son equivalentes:*

1) *K es algebraicamente cerrado.*
2) *Todo polinomio no constante de $K[X]$ tiene una raíz en K.*
3) *Todo polinomio no constante de $K[X]$ se factoriza como un producto de polinomios lineales.*
4) *Todo polinomio irreducible de $K[X]$ tiene grado 1.*

Demostración. 1) ⇒ 2) Sea P un polinomio no constante de $K[X]$. Por la Proposición 5.2 hay una extensión finita E/K en la que P tiene una raíz. Como por hipótesis $E = K$, el polinomio P tiene una raíz en K.

2) ⇒ 3) Es trivial.

3) ⇒ 4) Es trivial.

4) $\Rightarrow$ 1) Sea E/K una extensión algebraica y sea $x \in E$. Por hipótesis $\mathrm{irr}(x,K)$ es igual a $X-c$ con $c \in K$. Como x se anula en $\mathrm{irr}(x,K) = X-c$, tenemos que $x = c \in K$ y así $E = K$. $\square$

Definición 5.4. Sea E/K una extensión algebraica. Si E es algebraicamente cerrado decimos que E es una clausura algebraica de K.

Proposición 5.5. *Sea E/K una extensión algebraica. Son equivalentes:*

1) *E es una clausura algebraica de K.*
2) *Todo polinomio con coeficientes en K se factoriza en $E[X]$ como un producto de polinomios lineales.*
3) *Todo polinomio irreducible de $K[X]$ se factoriza en $E[X]$ como un producto de polinomios lineales.*

Demostración. 1) $\Rightarrow$ 2) y 2) $\Rightarrow$ 3) son triviales. Veamos que 3) $\Rightarrow$ 1). Sea E'/E una extensión algebraica y sea $x \in E'$. Por hipótesis $\mathrm{irr}(x,K)$ tiene todas sus raíces en E. Así, como x es una raíz de $\mathrm{irr}(x,K)$, tenemos que $x \in E$. $\square$

Teorema 5.6. *Se satisfacen:*

1) *Todo cuerpo K tiene una clausura algebraica.*
2) *Si E/K y E'/K son dos clausuras algebraicas de K, entonces existe un isomorfismo de extensiones $f\colon E/K \to E'/K$.*

Demostración. 1) Primera demostración (Artín): Sea $(P_i)_{i\in I}$ la familia de todos los polinomios de grado positivo de $K[X]$ y sea $A = K[X_i\ (i \in I)]$ la K-álgebra de polinomios en las variables $(X_i)_{i\in I}$. Afirmamos que el ideal J de A generado por $(P_i(X_i))_{i\in I}$ es propio. En efecto, supongamos que se tiene una igualdad $(*)$ de la forma $1 = \sum_{j=1}^{n} Q_{i_j} P_{i_j}(X_{i_j})$ con los i_j en I y los $Q_{i_j} \in A$. Por la Proposición 5.2 existe una extensión F/K en la que cada P_{i_j} tiene una raíz a_{i_j}. Por la propiedad universal de A existe un morfismo de K-álgebras $\mu\colon A \to F$ tal que $\mu(X_h) = 0$ si $h \neq i_1,\dots,i_n$ y tal que $\mu(X_{i_j}) = a_{i_j}$. Aplicando μ a $(*)$ obtenemos que $1 = \sum_{j=1}^{n} \mu(Q_{i_j}) P_{i_j}(a_{i_j}) = 0$, lo que es absurdo. Sea $\mathfrak{m}$ un ideal maximal de A que contiene a J y sea $E_1 = A/\mathfrak{m}$. Es claro que E_1 es un cuerpo que contiene a K y que E_1 está generado por la familia $(\overline{X_i})_{i\in I}$, donde $\overline{X_i}$ es la clase de X_i en E_1. Como $P_i(\overline{X_i}) = 0$, tenemos tanto que E_1 algebraico sobre K como que cada polinomio de grado positivo de $K[X]$ tiene una raíz en E_1. Procediendo recursivamente obtenemos una sucesión $(E_j/K)_{j\geq 1}$ de extensiones algebraicas de K con $E_j \subseteq E_{j+1}$ para todo $j \geq 1$ y tal que cada polinomio de grado positivo de $E_j[X]$ tiene una raíz en E_{j+1} $(j \geq 1)$. Sea $E = \bigcup_{j\geq 1} E_j$. Es claro que E/K es una extensión de algebraica de K y que E es algebraicamente cerrado (ya que cada polinomio de $E[X]$ está en algún $E_j[X]$).

1) Segunda demostración: Veamos primero que si E/K es una extensión algebraica, entonces $\#(E) \leq \max(\#(\mathbb{N}), \#(K))$. Para cada $n \geq 1$ denotemos con $\mathcal{P}_n$ al conjunto de los polinomios mónicos e irreducibles de grado n de $K[X]$ y con J_n a $\{1,\dots,n\}$. Como cada $x \in E$ determina $\mathrm{irr}(x,K)$ y cada polinomio de grado n tiene a lo sumo n raíces, se puede definir una función inyectiva de E en $\bigcup_{n\geq 1} \mathcal{P}_n \times J_n$. Así, $\#(E) \leq \max(\#(\mathbb{N}), \#(K))$. Sea ahora C un conjunto de cardinal mayor que $\max(\#(\mathbb{N}), \#(K))$ que contiene a K y sea $\mathcal{S} = \{(E,+,.) : E \subseteq C$ y $(E,+,.)/K$ es una extensión algebraica$\}$. Consideremos a $\mathcal{S}$ ordenado por la relación "ser subcuerpo de". Por el lema de Zorn $\mathcal{S}$ tiene un elemento maximal E.

Afirmamos que E es algebraicamente cerrado. Hay que probar que si E'/E es una extensión algebraica de E, entonces $E' = E$. Por la elección de C existe una inyección $i\colon E' \to C$ que se reduce a la identidad en E. Dándole a $i(E')$ la estructura de cuerpo que convierte a $i\colon E' \to i(E')$ en un isomorfismo obtenemos un elemento de $\mathcal{S}$ que contiene a E. Por la maximalidad de E resulta que $i(E') = E$, de donde $E' = E$.

2) Por la Proposición 4.2 existe un morfismo f de E/K en E'/K. Por la Proposición 4.3, para ver que f es sobreyectivo es suficiente probar que, para cada $x \in E'$, el polinomio $\operatorname{irr}(x, K)$ tiene la misma cantidad de raíces en E que en E'. Sean $x_1, \ldots, x_n$ las raíces de $\operatorname{irr}(x, K)$ en E e $\operatorname{irr}(x, K) = (X - x_1)^{\alpha_1} \ldots (X - x_n)^{\alpha_n}$. Entonces $\operatorname{irr}(x, K) = (X - f(x_1))^{\alpha_1} \ldots (X - f(x_n))^{\alpha_n}$, de donde $f(x_1), \ldots, f(x_n)$ son las raíces de $\operatorname{irr}(x, K)$ en E'. □

Corolario 5.7. *Sean E/K y E'/K dos extensiones y sea P un polinomio con coeficientes en K. Si P se factoriza, tanto en $E[X]$ como en $E'[X]$, como un producto de polinomios de grado* 1*, entonces la cantidad de raíces de P en E y en E' coinciden.*

Demostración. Sea F y F' las clausuras algebraicas de K en E y E' respectivamente y sean C y C' las clausuras algebraicas de F y F'. Como, por el Teorema 5.6, C y C' son isomorfos, P tiene la misma cantidad de raíces en C que en C'. La demostración se termina observando que las raíces de P en E están en F y, por lo tanto, coinciden con las de P en C y las raíces de P en E' están en F' y, por lo tanto, coinciden con las de P en C'. □

6. Grado de separabilidad

Definición 6.1. Sea E/K una extensión algebraica y sea C una clausura algebraica de K. El grado de separabilidad $\gamma(E/K)$ de E/K es el cardinal de $\operatorname{Hom}(E/K, C/K)$

Proposición 6.2. *Sea E/K una extensión algebraica. Si $E = K(x)$, entonces $\gamma(E/K)$ es igual al número de raíces distintas de* $\operatorname{irr}(x, K)$ *en una clausura algebraica de K.*

Demostración. Es consecuencia inmediata de la Proposición 4.1 aplicada al caso $F = K$ y $f = \mathrm{id}_K$. □

Proposición 6.3. *Sean F/K y E/F dos extensiones algebraicas y sea C una clausura algebraica de K. Cada morfismo de F/K en C/K tiene $\gamma(E/F)$ extensiones a E. En consecuencia $\gamma(E/K) = \gamma(E/F)\gamma(F/K)$.*

Demostración. Sea $f\colon F/K \to C/K$ un morfismo. Tomemos una clausura algebraica C' de F y un isomorfismo $\widehat{f}\colon C'/K \to C/K$ que extiende a f (Proposiciones 4.2 y 4.3). Consideremos la función

$$\theta\colon \operatorname{Hom}(E/F, C'/F) \to \{g\colon E/K \to C/K : g_{|F} = f\},$$

definida por $\theta(\gamma) = \widehat{f} \circ \gamma$. Es claro que θ es inyectiva. Puesto que si $g\colon E/K \to C/K$ satisface $g_{|F} = f$, entonces $\gamma = \widehat{f}^{-1} \circ g$ pertenece a $\operatorname{Hom}(E/F, C'/F)$ y $\theta(\gamma) = g$, tenemos también que θ es sobreyectiva. Así, $\#\left(\{g\colon E/K \to C/K : g_{|F} = f\}\right) = \gamma(E/F)$. □

Proposición 6.4. *Sea E/K una extensión algebraica. Se satisfacen:*

1) $|\,\mathrm{G}(E/K)| \leq \gamma(E/K)$.

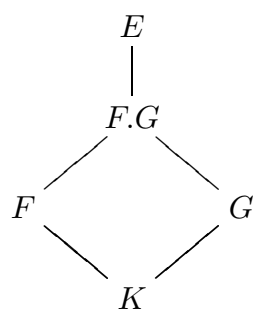
2) $\gamma(E/K) \leq (E : K)$.

Demostración. 1) Es trivial.

2) Es claro que podemos suponer que $(E : K)$ es finito. Hacemos la demostración por inducción en $(E : K)$. Si $(E : K) = 1$, entonces $E = K$ y, por lo tanto, $\gamma(E/K) = 1$. Supongamos que $(E : K) > 1$ y que el resultado es verdadero para extensiones de grado menor que $(E : K)$. Tomemos $x \in E \setminus K$. De las Proposiciones 3.4 y 6.2 se sigue inmediatamente que $\gamma(K(x)/K) \leq (K(x) : K)$ y así, por las Proposiciones 2.5 y 6.3 y la hipótesis inductiva,

$$\gamma(E/K) = \gamma(E/K(x))\gamma(K(x)/K) \leq (E : K(x))(K(x) : K) = (E : K). \quad \square$$

Proposición 6.5. *Sea*



un diagrama de extensiones. Si F/K es algebraico, entonces $\gamma(F.G/G) \leq \gamma(F/K)$.

Demostración. Sea C una clausura algebraica de $F.G$ y sea C' la clausura algebraica de F en C. Como F/K es algebraica, la inclusión canónica de $\mathrm{Hom}(F/K, C'/K)$ en $\mathrm{Hom}(F/K, C/K)$ es un isomorfismo y así, $\gamma(F/K) = \#(\mathrm{Hom}(F/K, C/K))$. Como el morfismo

$$\mathrm{Hom}(F.G/G, C/G) \to \mathrm{Hom}(F/K, C/K),$$

definido por restricción, es claramente inyectivo, tenemos entonces que $\gamma(F.G/G) \leq \#(\mathrm{Hom}(F/K, C/K)) = \gamma(F/K)$. $\square$

7. Extensiones normales

Definición 7.1. Una extensión algebraica E/K es normal si para cada morfismo de extensiones $f\colon E/K \to C/K$, con C una clausura algebraica de E, se satisface que $f(E) \subseteq E$ (lo que por el Corolario 4.4 implica que $f(E) = E$).

Definición 7.2. Sea K un cuerpo y $(P_i)_{i\in I}$ una familia de polinomios con coeficientes en K. Se llama cuerpo de descomposición de $(P_i)_{i\in I}$ a toda extensión E/K que satisface:

1) Cada P_i se factoriza en $E[X]$ como un producto de polinomios lineales.

2) E está generado sobre K por las raíces de los P_i's.

Teorema 7.3. *Sea K un cuerpo y $(P_i)_{i\in I}$ una familia de polinomios con coeficientes en K. Se satisfacen:*

1) Existe un cuerpo de descomposición de $(P_i)_{i\in I}$.

2) Si E/K y E'/K son dos cuerpos de descomposición de $(P_i)_{i\in I}$, entonces existe un isomorfismo de extensiones $f\colon E/K \to E'/K$.

Demostración. 1) Sea C una clausura algebraica de K y sea S el conjunto de las raíces de los polinomios P_i $(i \in I)$. Es claro que $K(S)/K$ es un cuerpo de descomposición de $(P_i)_{i\in I}$.

2) Por la Proposición 4.2 aplicada al caso $F = K$ y al conjunto S formado por la unión de la raíces de los P_i's, existe un morfismo f de E/K en E'/K. Para ver que f es sobreyectivo es suficiente observar que, por el Corolario 5.7, para cada $x \in S$, el polinomio $\mathrm{irr}(x, K)$ tiene la misma cantidad de raíces en E que en E' y aplicar la Proposición 4.3. □

Teorema 7.4. *Sea E/K una extensión algebraica. Son equivalentes:*

1) E/K es normal.

2) Si $f \in \mathrm{Aut}(C/K)$, con C una clausura algebraica de E, entonces $f(E) \subseteq E$.

3) Para todo $x \in E$, el polinomio $\mathrm{irr}(x, K)$ se factoriza en $E[X]$ como un producto de polinomios lineales.

4) Existe $S \subseteq E$ tal que $E = K(S)$ y tal que $\mathrm{irr}(x, K)$ se factoriza en $E[X]$ como un producto de polinomios lineales, para todo $x \in S$.

5) Si $f \in K[X]$ es irreducible y tiene una raíz en E, entonces f se factoriza en $E[X]$ como un producto de polinomios lineales.

6) Existe una familia $(x_i)_{i\in I}$ de elementos de E, tal que E es el cuerpo de descomposición de $(\mathrm{irr}(x_i, K))_{i\in I}$.

7) E es el cuerpo de descomposición de una familia de polinomios con coeficientes en K.

Demostración. 1) $\Rightarrow$ 2), 3) $\Rightarrow$ 4), 4) $\Rightarrow$ 6), 6) $\Rightarrow$ 7) y 3) $\Leftrightarrow$ 5) son triviales.

2) $\Rightarrow$ 3) Sea $x \in E$ e y una raíz de $\mathrm{irr}(x, K)$. Por las Proposiciones 4.1 y 4.2 y el Corolario 4.4 existe un isomorfismo $f\colon C/K \to C/K$ que envía x en y y así, por hipótesis, $y \in f(E) \subseteq E$.

7) $\Rightarrow$ 1) Sea $(P_i)_{i\in I}$ una familia de polinomios de la que E es el cuerpo de descomposición y sea S el conjunto de las raíces de los P_i $(i \in I)$. Como $E = K(S)$ basta observar que $f(S) \subseteq S$, para todo morfismo $f\colon E/K \to C/K$, con C una clausura algebraica de E. □

Teorema 7.5. *Sea E/K una extensión finita. Son equivalentes:*

1) E/K es normal.

2) $|\,\mathrm{G}(E/K)| = \gamma(E/K)$.

3) E es el cuerpo de descomposición de un polinomio P de $K[X]$. Además si $P = P_1^{n_1} \dots P_r^{n_r}$ donde los P_i's son polinomios irreducibles distintos de $K[X]$, entonces $(E : K) < \mathrm{gr}(P_1)! \dots \mathrm{gr}(P_r)!$.

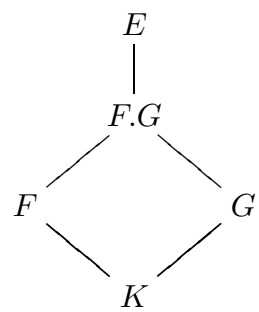
Demostración. 1) $\Leftrightarrow$ 2) Por el punto 2) de la Proposición 6.4, $\gamma(E/K) < \infty$. Es inmediato ahora que 1) y 2) son equivalentes.

1) $\Rightarrow$ 3) Sea $\{x_1, \dots, x_n\}$ una base de E como K-módulo. Por la equivalencia entre los items 1) y 6) del Teorema 7.4, E es el cuerpo de descomposición de $\prod_{i=1}^{n} \operatorname{irr}(x_i, K)$.
3) $\Rightarrow$ 1) Sea S el conjunto de las raíces de P. Por las Proposiciones 3.7 y 3.8, $E = K(S) = K[S]$ y $(E, K) < \infty$. Que E/K es normal es una consecuencia inmediata de la equivalencia entre los puntos 1) y 7) del Teorema 7.4.

Resta probar que si E es el cuerpo de descomposición de P y $P = P_1^{n_1} \dots P_r^{n_r}$ con los P_i's irreducibles distintos de $K[X]$, entonces $(E : K) < \operatorname{gr}(P_1)! \dots \operatorname{gr}(P_r)!$. Para cada $1 \leq i \leq r$, denotemos con $E_i \subseteq E$ al cuerpo de descomposición de P_i. Es inmediato que E es igual al compuesto $E_1 \dots E_r$. Dado que, por la Proposición 2.5, $(E : K) \leq (E_1 : K) \dots (E_r : K)$, es suficiente ver que si E es el cuerpo de descomposición de un polinomio Q, entonces $(E : K) \leq \operatorname{gr}(Q)!$. Demostremos esto por inducción en $n = \operatorname{gr}(Q)$. Si $n = 1$, entonces $E = K$ y no hay nada que probar. Supongamos ahora que $n > 1$ y que el resutado vale para polinomios de grado menor que n. Sea $F = K[X]/\langle T \rangle$, donde T es un factor irreducible de Q. Como la clase de X en F, es una raíz de Q, podemos escribir a Q en la forma $Q = Q_1 Q_2$ con Q_1 y Q_2 pertenecientes a $F[X]$ y Q_1 lineal. Sea E un cuerpo de descomposición de Q_2 sobre F. Es claro que E es un cuerpo de descomposición de Q sobre K. Como $\operatorname{gr}(Q_2) = n - 1$, por las Proposiciones 2.5 y 3.4 y la hipótesis inductiva, $(E : K) = (E : F)(F : K) \leq (n-1)! \operatorname{gr}(T) \leq n!$. $\square$

Proposición 7.6. *Se satisfacen:*

1) *Sean F/K y E/F dos extensiones. Si E/K es normal, entonces E/F también lo es.*
2) *Sea*



un diagrama de extensiones. Si F/K es normal, entonces también lo es $F.G/G$.
3) *Si $(E_i/K)_{i \in I}$ es una familia de subextensiones normales de E/K, entonces $K(\bigcup_{i \in I} E_i)/K$ y $(\bigcap_{i \in I} E_i)/K$ también son normales.*

Demostración. 1) Es inmediato.

2) Por la equivalencia entre los puntos 1) y 4) del Teorema 7.4 basta ver que para cada $x \in F$, el polinomio $\operatorname{irr}(x, G)$ se factoriza en $F.G[X]$ como un producto de polinomios de grado 1, lo que se deduce inmediatamente de que $\operatorname{irr}(x, G)$ divide a $\operatorname{irr}(x, K)$ y de que $\operatorname{irr}(x, K)$ se factoriza en $F[X] \subseteq F.G[X]$ como un producto de polinomios de grado 1.

3) Sea C una clausura algebraica de E y f un morfismo de $K(\bigcup_i E_i)/K$ en C/K. Como, por hipótesis, $f(E_i) \subseteq E_i$ para todo $i \in I$, tenemos que $f(K(\bigcup_i E_i)) = K(f(\bigcup_i E_i))) = K(\bigcup_i f(E_i)) \subseteq K(\bigcup_i E_i)$. Esto prueba que $K(\bigcup_{i \in I} E_i)/K$ es normal. Veamos que $(\bigcap_{i \in I} E_i)/K$ es normal. Sea C una clausura algebraica de $K(\bigcup_{i \in I} E_i)$ y sea $\sigma \colon C/K \to C/K$ un automorfismo. Como C es una clausura

algebraica de cada E_i, tenemos que $\sigma(E_i) = E_i$ para todo $i \in I$. Es claro ahora que $\sigma(\bigcap_{i\in I} E_i) = \bigcap_{i\in I} \sigma(E_i) \subseteq \bigcap_{i\in I} E_i$. Por la equivalencia entre los items 1) y 2) del Teorema 7.4 $(\bigcap_{i\in I} E_i)/K$ es normal. □

Observación 7.7. Sea C/K un clausura algebraica de K. La intersección de una familia de subextensiones normales de C/K, es normal. En particular dada una extensión E/K con $E \subseteq C$ existe una mínima subextensión normal E'/K de C/K que contiene a E. Esta extensión se llama la clausura normal de E en C. Es fácil ver que $E' = K(\bigcup \sigma(E))$, donde σ recorre el conjunto $\mathrm{Hom}(E/K, C/K)$. En particular, por las Proposiciones 2.5 y 6.4, si E/K es finita, entonces E'/K también lo es.

8. Extensiones separables

Definición 8.1. Sea K un cuerpo. Un polinomio $P \in K[X]$ es separable si no tiene raíces múltiples en ninguna clausura algebraica de K.

Proposición 8.2. *Sea K un cuerpo, P un polinomio de $K[X]$ y $x \in K$. Son equivalentes:*

1) $(X - x)^2$ divide a P.

2) $X - x$ divide a P y a P'.

En particular, P es separable si y sólo si es coprimo con P'.

Demostración. 1) ⇒ 2) Escribamos $P = (X - x)^2 Q$. Derivando obtenemos que $P' = (X - x)^2 Q' + 2(X - x)Q = (X - x)((X - x)Q' + 2Q)$, de donde $X - x$ divide a P'.

2) ⇒ 1) Escribamos $P = (X - x)Q$. Derivando obtenemos $P' = Q + (X - x)Q'$. Como $X - x$ divide a P' y a $(X - x)Q'$, divide también a Q. Así, $(X - x)^2$ divide a P. □

Proposición 8.3. *Sea K un cuerpo y P un polinomio irreducible de $K[X]$. Son equivalentes:*

1) P es separable.

2) Alguna raíz de P es simple.

3) $P' \neq 0$.

Demostración. 1) ⇒ 2) Es trivial.

2) ⇒ 3) Sea C una clausura algebraica de K y $x \in C$ una raíz de P. Si P' fuera cero, entonces $X - x$ dividiría a P' y, por la Proposición 8.2, $(X - x)^2$ a P.

3) ⇒ 1) Como $\mathrm{gr}(P') < \mathrm{gr}(P)$ y P es irreducible, $\langle P, P' \rangle = K[X]$. Así, P y P' no pueden tener ninguna raíz en común en ninguna extensión de K, lo que por la Proposición 8.2, muestra que P es separable. □

Proposición 8.4. *Sea K un cuerpo y P un polinomio irreducible de $K[X]$. Se satisfacen:*

1) Si la característica de K es cero, entonces P es separable.

2) Si la característica de K es $p > 0$, entonces existe un polinomio irreducible y separable $Q \in K[X]$ y un entero no negativo h tal que $P = Q(X^{p^h})$.

Demostración. 1) es trivial. Veamos que vale 2). Sea h máximo tal que existe $Q \in K[X]$ con $P = Q(X^{p^h})$. Como P es irreducible también lo es Q. Así, por

la Proposición 8.3, si Q no fuera separable, Q' sería igual a cero. En consecuencia Q tendría la forma $Q = T(X^p)$ y P sería igual a $T(X^{p^{h+1}})$, contradiciendo la maximalidad de h. $\square$

Definición 8.5. Sea E/K una extensión algebraica y sea $x \in E$. Decimos que x es separable sobre K si $\mathrm{irr}(x, K)$ lo es.

Observación 8.6. Sea E/K una extensión algebraica y sea $x \in E$. Por las Proposiciones 3.4 y 6.2, x es separable si y sólo si $\gamma(K(x)/K) = (K(x) : K)$. Además si $x \in E$ es separable, también lo son todos sus conjugados.

Observación 8.7. Sea K un cuerpo de característica 0, E/K una extensión algebraica y $x \in E$. Por la Observación 8.6 y el item 1) de la Proposición 8.4, $(K(x) : K) = \gamma(K(x)/K)$.

Observación 8.8. Sea K un cuerpo de característica $p > 0$, E/K una extensión algebraica y $x \in E$. Por el item 2) de la Proposición 8.4 existe un polinomio irreducible y separable $P \in K[X]$ y un entero no negativo h tal que $\mathrm{irr}(x, K) = P(X^{p^h})$. Sea C una clausura algebraica de E y sean $y_1, \ldots, y_n$ las raíces de P en C. Como C es algebraicamente cerrado existen $x_1, \ldots, x_n \in C$ tales que $y_i = x_i^{p^h}$ para todo $1 \leq i \leq n$. Así,

$$\mathrm{irr}(x, K) = P(X^{p^h}) = \prod_{i=1}^{n}(X^{p^h} - y_i) = \prod_{i=1}^{n}(X^{p^h} - x_i^{p^h}) = \left(\prod_{i=1}^{n}(X - x_i)\right)^{p^h}.$$

En consecuencia, por las Proposiciones 3.4 y 6.2, $(K(x) : K) = \gamma(K(x)/K)p^h$.

Proposición 8.9. *Sea E/K una extensión finita. Si la característica de K es 0, entonces $\gamma(E/K) = (E : K)$ y si la característica de K es $p > 0$, entonces $\gamma(E/K)$ divide a $(E : K)$ y su cociente es una potencia de p.*

Demostración. Hacemos la demostración por inducción en $(E : K)$. Si $(E : K) = 1$ no hay nada que probar. Supongamos ahora que $(E : K) > 1$ y que el resultado vale para extensiones de grado menor que $(E : K)$. Tomemos $x \in E \setminus K$. Por la hipótesis inductiva, si la característica de K es cero, $(E : K(x)) = \gamma(E/K(x))$ y, si la característica de K es $p > 0$, existe un número natural h tal que $(E : K(x)) = \gamma(E/K(x))p^h$. La demostración se termina usando las Observaciones 8.7 y 8.8 y la Proposición 6.3. $\square$

Definición 8.10. Una extensión algebraica E/K es separable si lo son todos sus elementos.

Proposición 8.11. *Sea E/K una extensión finita y $S \subseteq E$ tal que $E = K(S)$. Son equivalentes:*

1) E/K es separable.

2) Todo $x \in S$ es separable.

3) $\gamma(E/K) = (E : K)$

Demostración. Que 1) implica 2) es inmediato. Como $(E : K) < \infty$ existe un subconjunto finito S' de S tal que $E = K(S')$. Vamos probar que 2) $\Rightarrow$ 3) por inducción en la cantidad de elementos de S'. Por la Observación 8.6, $(K(x) : K) =$

$\gamma(K(x)/K)$. Así, por las Proposiciones 2.5 y 6.3 y la hipótesis inductiva aplicada a la extensión $E/K(x)$,

$$(E : K) = (E : K(x))(K(x) : K) = \gamma(E/K(x))\gamma(K(x)/K) = \gamma(E/K).$$

Veamos ahora que 3) implica 1). Tomemos $x \in E$. Por las Proposiciones 2.5 y 6.3 y la hipótesis,

$$(E : K(x))(K(x) : K) = (E : K) = \gamma(E/K) = \gamma(E/K(x))\gamma(K(x)/K).$$

Como, por el punto 2) de la Proposición 6.4,

$$\gamma(E/K(x)) \leq (E : K(x)) \quad \text{y} \quad \gamma(K(x)/K) \leq (K(x) : K),$$

de la igualdad anterior se sigue que $\gamma(K(x)/K) = (K(x) : K)$. Así, por la Observación 8.6, x es separable. □

Proposición 8.12. *Sea E/K una extensión algebraica y $S \subseteq E$ tal que $K(S) = E$. Si S es un conjunto de elementos separables de E, entonces E/K es separable y además $\gamma(E/K) = (E : K)$.*

Demostración. Por la Proposición 8.11 podemos suponer que E/K es infinita. Dado $x \in K(S)$ existe $S' \subseteq S$ finito tal que $x \in K(S')$ y $(K(S') : K) \geq n$. Por las Proposiciones 3.7 y 3.8, la extensión $K(S')/K$ es finita. Así podemos aplicar la Proposición 8.11, lo que muestra que x es separable. Como esto vale para cada $x \in K(S)$, la extensión E/K es separable. La última afirmación se sigue de que dado $n \in \mathbb{N}$ existe una subextensión finita E'/K de E/K tal que $(E' : K) \geq n$ y de que, por las Proposiciones 6.3 y 8.11, $\gamma(E/K) \geq \gamma(E'/K) = (E' : K)$. □

Proposición 8.13. *Sean F/K y E/F dos extensiones algebraicas. Si F/K es separable, entonces todo elemento de E que es separable sobre F, es también separable sobre K.*

Demostración. Sea $x \in E$ un elemento separable sobre F. Consideremos la subextensión F'/K de F/K generada por los coeficientes de $\mathrm{irr}(x, F)$. De las Proposiciones 3.7, 3.8 y 8.11 se sigue que F'/K y $F'(x)/F'$ son finitas y separables. Así, por las Proposiciones 2.5, 6.3 y 8.11,

$$\gamma(F'(x)/K) = \gamma(F'(x)/F')\gamma(F'/K) = (F'(x) : F')(F' : K) = (F'(x) : K),$$

lo que, por la Proposición 8.11, muestra que x es separable sobre K. □

Corolario 8.14. *Sea E/K una extensión algebraica. El conjunto F de los elementos de E que son separables sobre K es una subextensión separable F/K de E/K. Además se satisfacen:*

1) Todo elemento de E separable sobre F pertenece a F.

2) Si E/K es normal, entonces F/K también lo es.

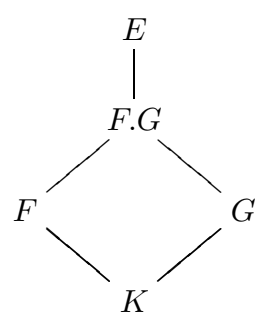
Demostración. La parte principal del Corolario y el item 1) se siguen de la Proposiciones 8.12 y 8.13, respectivamente, mientras que el item 2) es consecuencia inmediata de la Observación 8.6. □

Definición 8.15. Sea E/K una extensión algebraica. La clausura separable F de K en E es el conjunto de los elementos de E que son separables sobre K. Cuando F es igual a K decimos que K es separablemente cerrado en E.

Proposición 8.16. *Se satisfacen:*

1) Sean F/K y E/F dos extensiones. Entonces E/K es separable si y sólo si F/K y E/F lo son.

2) Sea



un diagrama de extensiones. Si F/K es separable, entonces también lo es $F.G/G$.

3) Si $(E_i/K)_{i\in I}$ es una familia de subextensiones separables de E/K, entonces $K(\bigcup_{i\in I} E_i)/K$ también es separable.

Demostración. 1) Que E/K separable implica que E/F y F/K son separables es inmediato. Por la Proposición 8.13 si E/F y F/K son separables, entonces E/K también lo es.

2) Se lo deduce de la Proposición 8.12, de que $F.G = G(F)$ y de que $\mathrm{irr}(x, G)$ divide a $\mathrm{irr}(x, K)$, para cada $x \in F$.

3) Esto se sigue inmediatamente de la Proposición 8.12. □

Proposición 8.17. *La clausura normal E'/K de una extensión separable E/K, es separable.*

Demostración. Sea $I = \mathrm{Hom}(E/K, C/K)$, donde C es una clausura algebraica de E. El resultado se sigue inmediatamente de que $E' = K(\bigcup_{\sigma\in I} \sigma(E))$, de que cada una de las extensiones $\sigma(E)/K$ es separable y de la Proposición 8.12. □

Dado un subconjunto S de una K-álgebra E y un número natural entero n, denotamos con S^n a $\{s^n : s \in S\}$.

Lema 8.18. *Sea K un cuerpo de característica $p > 0$, E/K una extensión algebraica de K y $S \subseteq E$. Son equivalentes:*

1) Existe $k \geq 1$ tal que $K(S^{p^k}) = K(S)$.

2) $K(S^{p^k}) = K(S)$ para todo $k \geq 1$.

Demostración. Que 2) implica 1) es trivial. Veamos que 1) implica 2). Es claro que $K(S^{p^{i+1}}) \subseteq K(S^{p^i})$, para todo $i \geq 0$. En particular, $K(S^{p^k}) \subseteq K(S^p) \subseteq K(S)$, lo que junto con la hipótesis implica que $K(S^p) = K(S)$. Así,

$$K(S^{p^i}) \subseteq K(K(S)^{p^i}) = K(K(S^p)^{p^i}) \subseteq K(K(S^{p^{i+1}})) = K(S^{p^{i+1}}),$$

para todo $i \geq 0$. □

El item 1) se puede demostrar de forma más pedestre. Esta última demostración tiene la ventaja de ser constructiva. Sea $S = (s_j)_{J\in J}$ una familia de elementos de E tal que $K(S) = K(S^p)$. Supongamos que $x \in K(S^{p^i})$ y escribamos $x = P(s_{j'}^{p^i})$ y $s_{j'} = P_{j'}(s_j^p)$, donde $P(X_{j'}\ (j' \in J))$ y los $P_{j'}(X_j\ (j \in J))$'s son polinomios con coeficientes en K. Entonces $x = P((P_{j'}(s_j^p))^{p^i}) \in K(S^{p^{i+1}})$.

Proposición 8.19. *Sea K un cuerpo de característica $p > 0$, E/K una extensión algebraica de K y $S \subseteq K$ tal que $E = K(S)$. Se satisfacen:*

1) Si E/K es separable, entonces $E = K(S^{p^k})$ para todo $k \geq 1$.
2) Si E/K es finito y $E = K(S^{p^k})$ para algún $k \geq 1$, entonces E/K es separable.

Demostración. 1) Sea $x \in S$. Como x es raíz de $(X - x)^p = X^p - x^p \in K(x^p)[X]$, existe $1 \leq i \leq p$ tal que $\mathrm{irr}(x, K(x^p)) = (X - x)^i$. Así, dado que $\mathrm{irr}(x, K(x^p))$ divide a $\mathrm{irr}(x, K)$ y este último polinomio es separable, $i = 1$. En consecuencia, $X - x \in K(x^p)[X]$, lo que implica que $x \in K(x^p)$. Como esto vale para todo $x \in S$, tenemos que $E = K(S^p)$. La demostración se termina inmediatamente usando el Lema 8.18.

2) Como E/K es finito, tenemos que $E = K(T) = K(T^{p^k})$ para un subconjunto finito T de S. Sea $r \geq 1$ tal que todos los elementos de T^{p^r} son separables. Por el Lema 8.18, $E = K(T^{p^r})$ que, por la Proposición 8.12, es separable. □

Notemos que en la demostración del item 1) hemos probado que para cada $x \in E$ vale que $x \in K(x^p)$. Pero esto se deduce también de item 1) aplicado a la extensión $K(x)/K$. En realidad de esta manera vemos que $x \in K(x^{p^k})$ para todo $k \geq 1$. La hipótesis de finitud del item 2) se puede evitar pidiendo que exista una familia $(S_i)_{i\in I}$ de subconjuntos finitos de S tales que cada subextensión finita de E/K sea una subextensión de alguna de las extensiones $K(S_i)/K$'s y para cada $i \in I$ exista $k_i \geq 1$ tal que $K(S_i) = K(S_i^{p^{k_i}})$. Esto da una recíproca de la formulación mas fina del item 1) que acabamos de dar recién.

Corolario 8.20. *Sea K un cuerpo de característica $p > 0$, E/K una extensión separable de K y $S \subseteq K$. Se satisfacen:*

1) *Si el K-espacio vectorial generado por S es igual a E, entonces el K-espacio vectorial generado por S^p es también igual a E.*
2) *Si S es linealmente independiente sobre K, entonces S^p también es linealmente independiente sobre K.*
3) *Si S es una base de E sobre K, entonces S^p también es una base de E sobre K.*

Demostración. 1) Dado un subcuerpo F de E y un subconjunto de T de E, denotemos con $F\langle T\rangle$ al subespacio F-lineal de E generado por T. Como $E = K\langle S\rangle$, tenemos que $E^p = K^p\langle S^p\rangle$ y como $K\langle E^p\rangle$ es un álgebra tenemos que $K\langle E^p\rangle = K[E^p]$. Así, por las Proposiciones 3.8 y 8.19,

$$E = K[E^p] = K\langle E^p\rangle = K\langle K^p\langle S^p\rangle\rangle = K\langle S^p\rangle.$$

2) Es claro que podemos suponer que S es finito. Sea T un subconjunto K-linealmente independiente de $K(S)$ tal que $S \subseteq T$ y $K(S) = K\langle T\rangle$. Por el item 1), $K\langle T\rangle = K\langle T^p\rangle$. Como $\#(T^p) = \#(T) = (K(S) : K) < \infty$, de la independencia lineal de T sobre K se deduce la de T^p.

3) Es consecuencia inmediata de los items 1) y 2). □

Notación y Observación 8.21. Sea E/K una extensión finita. Se llama grado de inseparabilidad de E/K al cociente $(E:K)_i = (E:K)/\gamma(E/K)$. Es claro que si la característica de K es cero, entonces $(E:K)_i = 1$ y que si la característica de K es $p > 0$, entonces $(E:K)_i$ es una potencia de p. Además, por las Proposiciones 2.5 y 6.3, si E/F y F/K son extensiones finitas, entonces $(E:K)_i = (E:F)_i(F:K)_i$. Por último, de la definición y de la Proposición 8.11, se deduce inmediatamente que E/K es separable si y sólo si $(E:K)_i = 1$.

9. Existencia de clausura separable

Definición 9.1. Un cuerpo es separablemente cerrado si no tiene extensiones separables propias.

Proposición 9.2. *Sea K un cuerpo. Son equivalentes:*

1) K es separablemente cerrado.

2) Todo polinomio no constante y separable de $K[X]$ se expresa como producto de polinomios lineales.

3) Todo polinomio no constante y separable de $K[X]$ tiene una raíz en K.

4) Todo polinomio separable e irreducible de $K[X]$ es lineal.

Demostración. 1) $\Rightarrow$ 2) Sea $P \in K[X]$ un polinomio separable, C una clausura algebraica de K y $x_1, \ldots, x_n$ las raíces de P en C. Como, por la Proposición 8.12, $K(x_1, \ldots, x_n)/K$ es separable, $x_1, \ldots, x_n \in K$. Así P se factoriza en $K[X]$ como un producto de polinomios lineales.

2) $\Rightarrow$ 3) Es trivial.

3) $\Rightarrow$ 4) Es trivial.

4) $\Rightarrow$ 1) Sea E/K una extensión separable y $x \in E$. Por hipótesis $\mathrm{irr}(x, K)$ es igual a $X - c$ con $c \in K$. Como x se anula en $\mathrm{irr}(x, K) = X - c$, tenemos que $x = c \in K$ y así $E = K$. □

Definición 9.3. Sea E/K una extensión separable. Si E es separablemente cerrado decimos que E es una clausura separable de K.

Proposición 9.4. *Sea E/K una extensión separable. Son equivalentes:*

1) E es una clausura separable de K.

2) Todo polinomio separable con coeficientes en K se factoriza en $E[X]$ como un producto de polinomios lineales.

3) Todo polinomio separable e irreducible de $K[X]$ se factoriza en $E[X]$ como un producto de polinomios lineales.

Demostración. 1 $\Rightarrow$ 2) y 2) $\Rightarrow$ 3) son triviales. Veamos que 3) $\Rightarrow$ 1). Sea E'/E una extensión separable y sea $x \in E'$. Por hipótesis $\mathrm{irr}(x, K)$ tiene todas sus raíces en E. Así, como x es una raíz de $\mathrm{irr}(x, K)$, tenemos que $x \in E$. □

Teorema 9.5. *Se satisfacen:*

1) Todo cuerpo K tiene una clausura separable.

2) Si E/K y E'/K son dos clausuras separables de K, entonces existe un isomorfismo de extensiones $f\colon E/K \to E'/K$.

Demostración. 1) Sea C una clausura algebraica de K y E la clausura separable de K en C. Es claro que cada polinomio separable de $K[X]$ tiene sus raíces en E. Así, por la Proposición 9.4, E/K es una clausura separable de K.

2) Por la Proposición 4.2 existe un morfismo f de E/K en E'/K. Por la Proposición 9.4, para cada $x \in E'$, el polinomio $\mathrm{irr}(x, K)$ tiene $\mathrm{gr}(\mathrm{irr}(x, K))$ raíces distintas, tanto en E como en E'. Así, por la Proposición 4.3, f es sobreyectivo. □

10. Extensiones puramente inseparables

Definición 10.1. Sea E/K una extensión algebraica, C una clausura algebraica de E y $x \in E$. Decimos que x es puramente inseparable sobre K si $\mathrm{irr}(x, K)$ no tiene ninguna raíz distinta de x en C.

Proposición 10.2. *Sea E/K una extensión algebraica y $x \in E$. Son equivalentes:*

1) x es puramente inseparable.

2) $\gamma(K(x)/K) = 1$.

Demostración. Es consecuencia inmediata de la Proposición 6.2. □

Observación 10.3. Sea K un cuerpo de característica 0 y E/K una extensión algebraica. Por el item 1) de la Proposición 8.4, todo elemento de E, puramente inseparable sobre K, pertenece a K.

Proposición 10.4. *Sea K un cuerpo de característica $p > 0$, E/K una extensión algebraica y $x \in E$. Son equivalentes:*

1) x es puramente inseparable.

2) $\mathrm{irr}(x, K)$ tiene la forma $(X - x)^{p^h} = X^{p^h} - x^{p^h}$.

3) Existe $h > 0$ tal que $x^{p^h} \in K$.

Demostración. 1) ⇒ 2) Es consecuencia inmediata de la Observación 8.8.

2) ⇒ 3) Es trivial.

3) ⇒ 1) Basta observar que $\mathrm{irr}(x, K) \mid (X - x)^{p^h}$, ya que x se anula en $(X - x)^{p^h} = X^{p^h} - x^{p^h}$. □

Definición 10.5. Una extensión algebraica E/K es puramente inseparable si lo son todos sus elementos.

Observación 10.6. Sea K un cuerpo. Por la Observación 10.3, Si K tiene una extensión propia y puramente inseparable, entonces la característica de K es positiva.

Proposición 10.7. *Sea, E/K una extensión algebraica y $S \subseteq E$ tal que $E = K(S)$. Son equivalentes:*

1) E/K es puramente inseparable.

2) Todos los elementos separables de E están en K.

3) Todo $x \in S$ es puramente inseparable.

4) $\gamma(E/K) = 1$.

Demostración. 1) ⇒ 2) Esto es inmediato.

2) $\Rightarrow$ 3) Si la característica de K es cero, entonces por el item 1) de la Proposición 8.4 $E = K$ y el resultado es inmediato. Podemos suponer entonces que la característica de K es $p > 0$. Tomemos $x \in S$. Por la Observación 8.8 existe un polinomio irreducible y separable $P \in K[X]$ y un número natural h tal que $\mathrm{irr}(x, K) = P(X^{p^h})$. Como x^{p^h} es raíz de P es separable. Así, por hipótesis, x^{p^h} pertenece a K y, en consecuencia, por la Proposición 10.4, x es puramente inseparable.

3) $\Rightarrow$ 4) Sea C una clausura algebraica de E y sea f un morfismo de E/K en C/K. Como $f(x) = x$ para todo $x \in S$, tenemos que $f = \mathrm{id}$.

4) $\Rightarrow$ 1) Sea $x \in E$. Por la Proposición 6.3, $1 = \gamma(E/K) = \gamma(E/K(x))\gamma(K(x)/K)$. Así, $\gamma(K(x)/K) = 1$, de donde por la Proposición 10.2, x es puramente inseparable. $\square$

Corolario 10.8. *Si E/K es una extensión finita, entonces E/K es puramente inseparable si y sólo si $(E : K) = (E : K)_i$. En particular, si K tiene característica $p > 0$ y E/K es puramente inseparable, entonces $(E : K)$ es una potencia de p.*

Demostración. Se sigue inmediatamente de la equivalencia entre los puntos 1) y 4) de la Proposición 10.7. $\square$

Proposición 10.9. *Sea E/K una extensión algebraica, F la clausura separable de K en E y C una clausura algebraica de E. Se satisfacen:*

1) *E/F es puramente inseparable, cada morfismo de extensiones de E/K en C/K está univocamente determinado por su restricción a F y $(F : K) = \gamma(E/K)$.*
2) *Si E/F es finita, entonces $E^{(E:F)} \subseteq F$, donde $E^{(E:F)} = \{x^{(E:F)} : x \in E\}$.*
3) *Si E/K es finita, entonces $(E : F) = (E : K)_i$.*

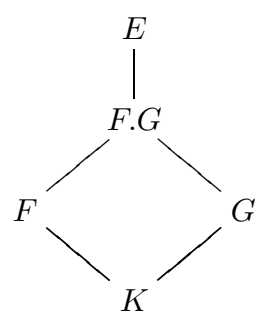
Demostración. 1) Por el Corolario 8.14 y la equivalencia entre los puntos 1) y 2) de la Proposición 10.7, la extensión E/F es puramente inseparable. Además, como $\gamma(E/F) = 1$, cada morfismo de extensiones de E/K en C/K está univocamente determinado por su restricción a F. Por último $(F : K) = \gamma(F/K) = \gamma(F/K)\gamma(E/F) = \gamma(E/K)$.

2) Por la Proposición 10.4, $x^{\mathrm{gr}(\mathrm{irr}(x,F))} \in F$. Así, dado que por la Proposición 3.4 y el item 1) de la Proposición 2.5, $\mathrm{gr}(\mathrm{irr}(x, F))$ divide a $(E : F)$, tenemos que $x^{(E:F)} \in F$.

3) Si E/K es finito, entonces $(E : F) = (E : K)/(F : K) = (E : K)/\gamma(E/K) = (E : K)_i$. $\square$

Proposición 10.10. *Se satisfacen:*

1) *Sean F/K y E/F dos extensiones. Entonces E/K es puramente inseparable, si y sólo si E/F y F/K lo son.*
2) *Sea*



un diagrama de extensiones. Si F/K es puramente inseparable, entonces también $F.G/G$ lo es.

3) Si $(E_i/K)_{i\in I}$ es una familia de subextensiones puramente inseparables de E/K, entonces $K(\bigcup_{i\in I} E_i)/K$ también es puramente inseparable.

Demostración. 1) Se lo deduce inmediatamente de la Proposición 6.3 y de la equivalencia entre los puntos 1) y 4) de la Proposición 10.7.

2) Se lo deduce de que $F.G = G(F)$, de que $\mathrm{irr}(x, G) \mid \mathrm{irr}(x, K)$ para todo $x \in F$ y de la equivalencia entre los puntos 1) y 3) de la Proposición 10.7.

3) Esto se deduce inmediatamente de la equivalencia entre los puntos 1) y 3) de la Proposición 10.7. □

Corolario 10.11. *Sea E/K una extensión algebraica y sea F el conjunto de los elementos de E que son puramente inseparables. Se satisfacen:*

1) F/K es una subextensión normal de E/K.

2) Todo elemento de E puramente inseparable sobre F pertenece a F.

3) F es el cuerpo dejado fijo por todos los morfismos de E/K en C/K, donde C es una clausura algebraica de E.

4) Si E/K es normal, entonces F es el cuerpo dejado fijo por los elementos de $\mathrm{G}(E/K)$.

5) Si F' la clausura separable de K en E, entonces $F \cap F' = K$. Además E/F es separable si y sólo si $E = F.F'$.

Demostración. 1) Por la Proposición 10.7, F es un cuerpo. Ahora, por las equivalencias entre los puntos 1) y 2) de la Proposición 10.4 y los puntos 1) y 3) del Teorema 7.4, F/K es normal. Veamos el item 2). Tomemos $x \in E$ puramente inseparable sobre F. Por la equivalencia entre los puntos 1) y 3) de la Proposición 10.7 y por el punto 1) de la Proposición 10.10, $F[x]/K$ es puramente inseparable. Así, por definición, $x \in F$. Es claro que 3) implica 4). Veamos que vale 3). Como $\gamma(F/K) = 1$, todo elemento de $\mathrm{Hom}(E/K, C/K)$ deja fijo a los elementos de F. Resta ver que si $x \in E$ no es puramente inseparable, entonces existe un morfismo f de E/K en C/K tal que $f(x) \neq x$, lo que se deduce de que, por la Proposición 10.2, existe $f\colon K(x)/K \to C/K$ tal que $f(x) \neq x$ y de que, por la Proposición 4.2, este morfismo se extiende a E. Para terminar la demostración, debemos probar el item 5). Por el item 1) de la Proposición 8.16 y el item 1) de la Proposición 10.10, la extensión $(F \cap F')/K$ es separable y puramente inseparable y así, $F \cap F' = K$. Ahora, por el item 1) de la Proposición 10.9 y el item 1) de la Proposición 10.10, $E/F.F'$ es puramente inseparable y si E/F es separable, entonces por el item 1) de la Proposición 8.16, $E/F.F'$ también lo es. Así, en este caso, $E/F.F'$ es separable y puramente inseparable y, por lo tanto, $E = F.F'$. Recíprocamente, si $E = F.F'$, entonces $E/F = F.F'/F$ es separable por ser el levantado de F'/K y por el item 2) de la Proposición 8.16. □

Definición 10.12. Sea E/K una extensión algebraica. La clausura perfecta F de K en E es el conjunto de los elementos de E que son puramente inseparables sobre K.

A continuación construímos una extensión algebraica que está generada por un elemento que no es ni separable ni puramente inseparable.

Ejemplo 10.13. Sea K un cuerpo de característica $p > 0$ y sea t una indeterminada. Por el Criterio de Eisenstein el polinomio $P(X) = X^{p^2} + tX^p + t \in K(t)[X]$ es irreducible. Escribamos $E = K(t)[X]/\langle P(X)\rangle$ y consideremos la extensión $E/K(t)$. El polinomio minimal de la clase $\overline{X}$ de X en E es P. Así, como $P(X) = Q(X^p)$, donde $Q = X^p + tX + t$, el elemento $\overline{X}$ no es separable. Por otra parte, si $\overline{X}$ fuera puramente inseparable sobre $K(t)$, entonces tendríamos

$$X^{p^2} + tX^p + t = (X - \overline{X})^{p^2} = X^{p^2} - \overline{X}^{p^2},$$

lo que se contradeciría con que $t \neq 0$.

11. Existencia de clausura perfecta

Definición 11.1. Un cuerpo K es perfecto si toda extensión algebraica de K es separable.

Observación 11.2. Por el item 2) de la Proposición 8.6 todo cuerpo de característica cero es perfecto.

Proposición 11.3. *Sea K un cuerpo de característica positiva p. Son equivalentes:*

1) *K es perfecto.*
2) *K no tiene extensiones puramente inseparables propias.*
3) *Todo polinomio de la forma $X^{p^h} - c$ con $c \in K$ se factoriza en $K[X]$ como $X^{p^h} - c = (X - x)^{p^h}$.*
4) *Todo polinomio de la forma $X^p - c$ con $c \in K$ tiene una raíz en K.*
5) *El morfismo de Frobenius $\sigma\colon K \to K$, definido por $\sigma(x) = x^p$, es un isomorfismo.*
6) *Todo polinomio irreducible de $K[X]$ es separable.*

Demostración. 1) $\Rightarrow$ 2) Es trivial.

2) $\Rightarrow$ 3) Sea C una clausura algebraica de K y sea $x \in C$ una raíz de $X^{p^h} - c$. Por la equivalencia entre los items 1) y 3) de la Proposición 10.4, x es puramente inseparable. Así, por la Proposición 10.7, $K(x)/K$ es puramente inseparable, de donde $x \in K$. En consecuencia, $X^{p^h} - c = X^{p^h} - x^{p^h} = (X - x)^{p^h}$.

3) $\Rightarrow$ 4) Es trivial.

4) $\Rightarrow$ 5) Es trivial.

5) $\Rightarrow$ 6) Sea P un polinomio irreducible de $K[X]$. Por el item 3) de la Proposición 8.6, existe un polinomio irreducible y separable $Q = a_0 + \cdots + a_n X^n \in K[X]$ y un entero no negativo h tal que $P = Q(X^{p^h})$. Por hipótesis existen $b_0, \ldots, b_n \in K$ tales que $a_i = b_i^{p^h}$. Así, $P = Q(X^{p^h}) = (b_0 + \cdots + b_n X^n)^{p^h}$ y, como P es irreducible, esto implica que $h = 0$.

6) $\Rightarrow$ 1) Sea E/K una extensión algebraica de K. Entonces E/K es separable, ya que por hipótesis $\mathrm{irr}(x, K)$ es separable cualquiera sea $x \in E$. $\square$

Ejemplo. Sea K un cuerpo de característica $p > 0$. Por el Corolario 4.3, si $K/\mathbb{F}_p$ es algebraico, entonces el morfismo de Frobenius $\sigma\colon K \to K$ es sobreyectivo y así, en este caso, K es perfecto.

Proposición 11.4. *Se satisfacen:*

1) Si E/K es algebraica y K es perfecto, entonces E es perfecto.

2) Si E/K es finita y E es perfecto, entonces K es perfecto.

Demostración. 1) Sea E'/E una extensión algebraica. Por el item 1) de la Proposición 3.12 y la hipótesis, E'/K es separable. Ahora, por el item 1) de la Proposición 8.16, E'/E también lo es.

2) Es claro que podemos suponer que la característica de K es $p > 0$. Además un proceso inductivo reduce el problema al caso en que existe $x \in E$ tal que $E = K(x)$. Sea $\mathrm{irr}(x, K) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ el polinomio minimal de x. Entonces la igualdad

$$0 = (x^n + a_{n-1}x^{n-1} + \cdots + a_0)^p = (x^p)^n + a_{n-1}^p(x^p)^{n-1} + \cdots + a_0^p$$

muestra que $(K^p(x^p) : K^p) \leq n = (K(x) : K)$. Por otro lado, como $K(x)$ es perfecto, $K^p(x^p) = K(x)^p = K(x)$. Combinando estos dos hechos obtenemos que $(K(x) : K^p) \leq (K(x) : K)$, lo que implica que $K = K^p$. De aquí se deduce inmediatamente que el automorfismo de Frobenius $\sigma\colon K \to K$, dado por $\sigma(y) = y^p$, es sobreyectivo, de donde, por la Proposición 11.3, K es perfecto. □

Definición 11.5. Sea E/K una extensión puramente inseparable. Si E es perfecto decimos que E es una clausura perfecta de K.

Proposición 11.6. *Sea K un cuerpo de característica positiva p y sea E/K una extensión puramente inseparable. Son equivalentes:*

1) E es una clausura perfecta de K.

2) Todo polinomio de la forma $X^{p^h} - c$ con $c \in K$ se factoriza en $E[X]$ como $X^{p^h} - c = (X - x)^{p^h}$.

3) Todo polinomio irreducible de la forma $X^{p^h} - c$ con $c \in K$ tiene una raíz en E.

Demostración. 1) $\Rightarrow$ 2) Se lo deduce inmediatamente de la Proposición 11.3.

2) $\Rightarrow$ 3) Es trivial.

3) $\Rightarrow$ 1) Sea E'/E una extensión puramente inseparable y sea $x \in E'$. Entonces $\mathrm{irr}(x, K) = X^{p^h} - c$ con $c \in K$. Por hipótesis este polinomio tiene una raíz $y \in E$. Pero entonces $x^{p^h} = y^{p^h}$, de donde $x = y \in E$. Como esto vale para cada $x \in E'$, tenemos que E' es igual a E. □

Teorema 11.7. *Se satisfacen:*

1) Todo cuerpo K tiene una clausura perfecta.

2) Si E/K y E'/K son dos clausuras perfectas de K, entonces existe un isomorfismo de extensiones $f\colon E/K \to E'/K$.

Demostración. 1) Si la característica de K es cero, entonces por la Observación 11.2, K es la clausura perfecta de K. Podemos suponer así que la característica de K es $p > 0$. Sea C una clausura algebraica de K y sea E la clausura perfecta de K en C. Es claro que cada polinomio de la forma $X^{p^h} - c$ con $c \in K$, tiene una raíz en E. Así, por la Proposición 11.6, E/K es una clausura perfecta de K.

2) Por la Proposición 4.2 existe un morfismo f de E/K en E'/K. Si la característica de K es cero, entonces $K = E = E'$ y es inmediato que f es sobreyectiva.

Supongamos ahora que la característica de K es $p > 0$. Por la Proposición 11.3, para cada $x \in E'$, el polinomio $\mathrm{irr}(x, K)$ tiene tanto en E como en E' sólo una raíz. Así, por la Proposición 4.3, f es sobreyectiva. $\square$

12. Extensiones simples

Proposición 12.1. *Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico.*

Demostración. Sea G un subgrupo finito del grupo multiplicativo K^* de un cuerpo K y sea $x \in G$ un elemento de orden máximo N. Se afirma que si y es un elemento de G, entonces el orden n de y divide a N. En efecto, de lo contrario existiría un primo p y un número natural h tal que $p^{h-1} \mid N$, $p^h \nmid N$ y $p^h \mid n$, de donde $x^{p^{h-1}} y^{n/p^h}$ tendría orden pN, contradiciendo la maximalidad de N. En consecuencia G está incluído en el conjunto de las raíces de $X^N - 1$, lo que implica que $|G| \leq N = |\langle x \rangle|$ y, por lo tanto, que $G = \langle x \rangle$. $\square$

Definición 12.2. Una extensión E/K es simple o monogena si existe $x \in E$ tal que $E = K(x)$.

Teorema 12.3. *Sea E/K una extensión. Son equivalentes:*

1) E/K es finita y simple.

2) E/K es algebraica y simple.

3) Sólo hay un número finito de subextensiones de E/K.

Demostración. 1) $\Rightarrow$ 2) Es consecuencia inmediata de la Proposición 3.8.

2) $\Rightarrow$ 3) Sea $x \in E$ tal que $E = K(x)$. Consideremos la función θ, del conjunto de subextensiones F/K de E/K en el de los polinomios mónicos que dividen a $\mathrm{irr}(x, K)$, dada por $\theta(F) = \mathrm{irr}(x, F)$. Como este último es un conjunto finito, para ver que el primero también lo es basta mostrar que θ es inyectiva. Sea F' el subcuerpo de F generado por K y los coeficientes de $\mathrm{irr}(x, F)$. Como $\mathrm{irr}(x, F)$ es irreducible sobre F', tenemos que $\mathrm{irr}(x, F) = \mathrm{irr}(x, F')$. Así, de

$$(E : F) = (F(x) : F) = \mathrm{gr}(\mathrm{irr}(x, F)) = \mathrm{gr}(\mathrm{irr}(x, F') = (F'(x) : F') = (E : F'),$$

deducimos que $F = F'$, lo que muestra que θ es inyectiva.

3) $\Rightarrow$ 1) Dado $x \in E$ existe $m \in \mathbb{N}$ tal que $K(x^{m+1}) = K(x^m)$. Así, cada $x \in E$ y, por lo tanto E, es algebraico. Sea $E_1, \ldots, E_n$ la familia de subextensiones propias de E/K. Para cada $1 \leq i \leq n$ tomemos $x_i \in E \setminus E_i$. Entonces $E = K(x_1, \ldots, x_n)$, lo que por la Proposición 3.7 muestra que E/K es finita. Veamos que E/K es simple. Por la Proposición 12.1 esto es evidente si K y, por lo tanto E, es finito. Supongamos ahora que K es infinito. Es claro que basta ver que dados $x, y \in E$, existe $\lambda \in K$ tal que $K(x, y) = K(x + \lambda y)$. Como entre K y E hay sólo una cantidad finita de cuerpos intermedios, existen $\lambda_1, \lambda_2 \in K$, distintos tales que $K(x + \lambda_1 y) = K(x + \lambda_2 y)$. Así,

$$y = \frac{1}{\lambda_2 - \lambda_1}\big((x + \lambda_2 y) - (x + \lambda_1 y)\big) \quad \text{y} \quad x = (x + \lambda_1 y) - \lambda_1 y,$$

están en $K(x + \lambda_1 y)$, lo que prueba que $K(x, y) = K(x + \lambda_1 y)$. $\square$

Teorema 12.4. *Sea $K(x_1, \dots, x_n, y)/K$ una extensión algebraica. Si los x_i's son separables, entonces $K(x_1, \dots, x_n, y)/K$ es simple.*

Demostración. Por la Proposición 12.1 podemos suponer que K es infinito. Por un argumento inductivo, podemos suponer también que $n = 1$. Sea C una clausura algebraica de $K(x_1, y)$. Denotemos con $\{x_1' = x_1, x_2', \dots, x_r'\}$ y $\{y_1 = y, y_2, \dots, y_s\}$ a las raíces en C de $P(X) = \mathrm{irr}(x_1, K)$ y $Q(X) = \mathrm{irr}(y, K)$, respectivamente. Como K es infinito, existe $\lambda \in K$ tal que los $\lambda x_i' + y_j$ son todos distintos. Escribamos $z = \lambda x_1 + y$. Es claro que $Q(z - \lambda x_1) = Q(y) = 0$ y que $Q(z - \lambda x_i') \neq 0$ para todo $i \neq 1$. Dado que x_1 es una raíz simple de $P(X)$, esto implica que el máximo de los divisores comunes de $P(X)$ y de $Q(z - \lambda X)$ en $K(z)[X]$ es $X - x_1$, de donde $x_1 \in K(z)$. Ahora es claro que $y = z - \lambda x_1$ también está en $K(z)$ y, por lo tanto, que $K(x_1, y) = K(z)$. $\square$

Corolario 12.5. *Toda extensión finita y separable es simple.*

Corolario 12.6. *Si E/K es separable, entonces*

$$(E : K) = \sup\{\mathrm{gr}(\mathrm{irr}(x, K) : x \in E\} = \sup\{\gamma(K(x)/K) : x \in E\} = \gamma(E/K).$$

Demostración. Si E/K es finito, entonces el resultado se deduce inmediatamente de la Proposiciones 3.4 y 8.11 y 12.5. Si $(E : K) = \infty$, entonces para cada $n \in \mathbb{N}$, existe una subextensión finita F/K de E/K tal que $n \leq (F : K)$. En consecuencia, por las Proposiciones 3.4 y 12.5, $(E : K) = \sup\{\mathrm{gr}(\mathrm{irr}(x, K) : x \in E\}$. La segunda igualdad se deduce inmediatamente de la Proposición 8.11. Finalmente, la última se deduce facilmente de que, por la Proposición 6.3, $\gamma(K(x)/K) \leq \gamma(E/K)$ para todo $x \in E$. $\square$

13. Teoría de Galois

Definición 13.1. Sea E/K una extensión y $H \subseteq \mathrm{G}(E/K)$ un subgrupo. Se define $E^H = \{x \in E : \sigma(x) = x \text{ para todo } \sigma \in H\}$. Es claro que E^H es un subcuerpo de E que contiene a K.

Observación 13.2. Sea E/K una extensión, $G = \mathrm{G}(E/K)$ e $\mathrm{I}(E/K)$ y $\mathrm{S}(G)$ los reticulados de subextensiones de E/K y de subgrupos de G respectivamente. Las asignaciones de $\mathrm{I}(E/K)$ en $\mathrm{S}(G)$ y de $\mathrm{S}(G)$ en $\mathrm{I}(E/K)$, dadas por $F/K \mapsto \mathrm{G}(E/F)$ y $H \mapsto E^H$ respectivamente, satisfacen:

1) Si $K \subseteq F \subseteq F' \subseteq E$, entonces $\mathrm{G}(E/F) \supseteq \mathrm{G}(E/F')$.
2) Si $H \subseteq H'$ son subgrupos de G, entonces $E^H \supseteq E^{H'}$.
3) Para cada subextensión F/K de E/K, tenemos $F \subseteq E^{\mathrm{G}(E/F)}$.
4) Para cada subgrupo H de $G(E/K)$ tenemos $H \subseteq \mathrm{G}(E/E^H)$.
5) Para cada $F/K \in I(E/K)$ y cada $f \in G$, tenemos $\mathrm{G}(E/f(F)) = f.\,\mathrm{G}(E/F).f^{-1}$.
6) Para cada $H \in \mathrm{S}(G)$ y cada $f \in G$, tenemos $E^{fHf^{-1}} = f(E^H)$.

El siguiente resultado es una consecuencia formal de los primeros cuatro items de la observación anterior

Corolario 13.3. *Se satisfacen:*

1) $\mathrm{G}(E/F) = \mathrm{G}(E/E^{\mathrm{G}(E/F)})$.

2) $E^H = E^{\mathrm{G}(E/E^H)}$.

3) $\mathrm{G}(E/K(\bigcup_i F_i)) = \bigcap_i \mathrm{G}(E/F_i)$.

4) $E^{\langle \bigcup_i H_i \rangle} = \bigcap_i E^{H_i}$.

5) $\mathrm{G}(E/\bigcap_i F_i) \supseteq \langle \bigcup_i \mathrm{G}(E/F_i) \rangle$.

6) $E^{\bigcap_i H_i} \supseteq K(\bigcup_i E^{H_i})$.

Demostración. 1) La inclusión $\mathrm{G}(E/F) \subseteq \mathrm{G}(E/E^{\mathrm{G}(E/F)})$ es consecuencia del item 4) y la inclusión $\mathrm{G}(E/F) \supseteq \mathrm{G}(E/E^{\mathrm{G}(E/F)})$ del item 1) aplicado al item 3).

2) Es similar a la demostración de 1).

3) Dado que $F_i \subseteq K(\bigcup_i F_i)$, tenemos $\mathrm{G}(E/K(\bigcup_i F_i)) \subseteq \bigcap_i \mathrm{G}(E/F_i)$. Por otro lado $F_i \subseteq E^{\mathrm{G}(E/F_i)} \subseteq E^{\bigcap_i \mathrm{G}(E/F_i)}$ para todo i, de donde $K(\bigcup_i F_i) \subseteq E^{\bigcap_i \mathrm{G}(E/F_i)}$, lo que a su vez implica que $\bigcap_i \mathrm{G}(E/F_i) \subseteq \mathrm{G}(E/E^{\bigcap_i \mathrm{G}(E/F_i)}) \subseteq \mathrm{G}(E/K(\bigcup_i F_i))$.

4) Es similar a la demostración de 3).

5) Dado que $\bigcap_i F_i \subseteq F_j$, tenemos $\mathrm{G}(E/F_j) \subseteq \mathrm{G}(E/\bigcap_i F_i)$ para todo j, de donde $\langle \bigcup_i \mathrm{G}(E/F_i) \rangle \subseteq \mathrm{G}(E/\bigcap_i F_i)$.

6) Es similar a la demostración de 5). □

Decimos que una subextensión F/K de E/K es cerrada si existe un subgrupo $H \in \mathrm{S}(G)$ tal que $F = E^H$. Por el item 2) del corolario anterior, esto equivale a que $F = E^{\mathrm{G}(E/F)}$. De la misma manera decimos que un subgrupo H de G es cerrado si existe una subextensión F/K de E/K tal que $H = \mathrm{G}(E/F)$. Por el item 1) del corolario anterior, esto equivale a que $H = \mathrm{G}(E/E^H)$. Por ejemplo la subextensión trivial E/K de E/K y los subgrupos triviales $\{1\}$ y G de G son cerrados. Denotemos con $\overline{\mathrm{I}}(E/K)$ al subconjunto ordenado de $\mathrm{I}(E/K)$ formado por las subextenciones cerradas de E/K y con $\overline{\mathrm{S}}(G)$ al subconjunto ordenado de $\mathrm{S}(G)$ formado por los subgrupos cerrados de G. Por los items 3) y 4) del corolario anterior $\overline{\mathrm{I}}(E/K)$ y $\overline{\mathrm{S}}(G)$ son reticulados completos y tienen las mismas operaciones de ínfimo que $\mathrm{I}(E/K)$ y $\mathrm{S}(G)$ respectivamente. Además por los items 1) y 2) del mismo corolario, la asignación dada por $F/K \mapsto \mathrm{G}(E/F)$ define un isomorfismo entre el reticulado $\overline{\mathrm{I}}(E/K)$ y el reticulado dual de $\overline{\mathrm{S}}(G)$, cuya inversa es la aplicación dada por $H \mapsto E^H/K$. Por último, del item 5) de la Observación 13.2 se deduce que $\overline{\mathrm{S}}(G)$ es cerrado por conjugación y, del item 6) de la Observación 13.2, que si F/K es una subextensión cerrada de E/K, entonces cualquiera sea $f \in G$, la extensión $f(F)/K$ también lo es.

Sean E/K una extensión y $H_1 \subseteq H_2$ subgrupos de $\mathrm{G}(E/K)$. Es claro que si F/K es una subextensión cerrada de E/K, entonces $E^{\mathrm{G}(E/K)} \subseteq F$. Uno de los teoremas más importantes de esta sección dice que vale la recíproca y el otro que si $(H_2 : H_1) < \infty$ y H_1 es cerrado, entonces H_2 también lo es.

En la demostración del Teorema 13.5 usaremos un lema interesante en si mismo. Sean E/K una extensión y H un subgrupo de $\mathrm{G}(E/K)$. Para cada $x \in E$ definimos $\widehat{x}\colon H \to E$ por $\widehat{x}(g) = g(x)$.

Proposición 13.4. *Sea $x_1, \dots, x_n$ una familia de elementos de E. Entonces $x_1, \dots, x_n$ es linealmente independiente sobre E^H si y sólo si $\widehat{x_1}, \dots, \widehat{x_n}$ es linealmente independiente sobre E.*

Demostración. Supongamos que $\widehat{x_1}, \dots, \widehat{x_n}$ es linealmente independiente sobre E. Sea $a_1x_1 + \cdots + a_nx_n = 0$ una ecuación con coeficientes en E^H. Como, para cada $g \in H$,

$$0 = g(a_1x_1 + \cdots + a_nx_n) = a_1g(x_1) + \cdots + a_ng(x_n) = a_1\widehat{x_1}(g) + \cdots + a_n\widehat{x_n}(g),$$

tenemos que $a_1 = \cdots = a_n = 0$. Supongamos ahora que $x_1, \dots, x_n$ es linealmente independiente sobre E^H pero que $\widehat{x_1}, \dots, \widehat{x_n}$ no es linealmente independiente sobre E. Sea

$$(*) \qquad a_1\widehat{x_1} + \cdots + a_s\widehat{x_s} = 0$$

una ecuación no trivial de dependencia lineal. Cambiando los índices si es necesario, podemos suponer que s es la menor cantidad de sumandos que puede aparecer en una ecuación de este tipo y dividiendo ahora por a_s, podemos suponer también que $a_s = 1$. Observemos que $(*)$ es equivalente a

$$(**) \qquad a_1g(x_1) + \cdots + a_{s-1}g(x_{s-1}) + g(x_s) = 0 \quad \text{para todo } g \in H.$$

Considerando $(**)$ para $g = \mathrm{id} \in H$ obtenemos $a_1x_1 + \cdots + a_{s-1}x_{s-1} + x_s = 0$. Así, de la independencia lineal de los x_i's se sigue que no todos los a_i's están en E^H. Podemos suponer claramente que $a_1 \notin E^H$. Tomemos $g' \in H$ tal que $g'(x_1) \neq x_1$. A partir de $(**)$ obtenemos

$$g'(a_1)g'(g(x_1)) + \cdots + g'(a_{s-1})g'(g(x_{s-1})) + g'(g(x_s)) = 0 \quad \text{para todo } g \in H,$$

o equivalentemente

$$(***) \qquad g'(a_1)g(x_1) + \cdots + g'(a_{s-1})g(x_{s-1}) + g(x_s) = 0 \quad \text{para todo } g \in H.$$

Restando $(***)$ de $(**)$, obtenemos

$$(a_1 - g'(a_1))g(x_1) + \cdots + (a_{s-1} - g'(a_{s-1}))g(x_{s-1}) = 0 \quad \text{para todo } g \in H,$$

lo que es una contradicción, ya que esta es una ecuación no trivial y más corta que $(**)$. $\square$

Teorema 13.5. *Sea E/K una extensión algebraica. Se satisfacen:*

1) *Si $K \subseteq F_1 \subseteq F_2 \subseteq E$, entonces $(\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2)) \leq \gamma(F_2/F_1) \leq (F_2 : F_1)$. Además si E/F_1 es normal, entonces $(\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2)) = \gamma(F_2/F_1)$ y si F_2/F_1 es separable, entonces $\gamma(F_2/F_1) = (F_2 : F_1)$.*
2) *Si $H_1 \subseteq H_2 \subseteq \mathrm{G}(E/K)$, entonces $(E^{H_1} : E^{H_2}) \leq (H_2 : H_1)$.*

Demostración. 1) Sea $\mathrm{G}(E/F_1)/\mathrm{G}(E/F_2) = \{\sigma\,\mathrm{G}(E/F_2) : \sigma \in \mathrm{G}(E/F_1)\}$ el conjunto de las clases a izquierda de $\mathrm{G}(E/F_2)$ en $\mathrm{G}(E/F_1)$. Consideremos la aplicación $\theta\colon \mathrm{G}(E/F_1)/\mathrm{G}(E/F_2) \to \mathrm{Hom}(F_2/F_1, E/F_1)$, dada por $\theta(\sigma\,\mathrm{G}(E/F_2)) = \sigma_{|F_2}$. Como θ es inyectiva, tenemos la primera desigualdad del enunciado. La segunda ya

fue probada en la Proposición 6.4. Supongamos ahora que E/F_1 es normal. Sea C una clausura algebraica de E. Cada $\sigma\colon F_2/F_1 \to E/F_1$ se puede extender a un morfismo $\widetilde{\sigma}\colon E/F_1 \to C/F_1$ y como E/F_1 es normal, tenemos que $\widetilde{\sigma}(E) = E$. Es claro que $\theta(\widetilde{\sigma}) = \sigma$. Por último, que si F_2/F_1 es separable, entonces $\gamma(F_2/F_1) = (F_2 : F_1)$, fue probado en el Corolario 12.6.

2) Sean $x_1, \ldots, x_n \in E^{H_1}$. Debemos ver que si $n > (H_2 : H_1)$, entonces los x_i's no son linealmente independientes sobre E^{H_2}. Por la Proposición 13.4 es suficiente ver que las funciones $\widehat{x_i}\colon H_2 \to E$, definidas por $\widehat{x_i}(g) = g(x_i)$ no son linealmente independientes sobre E. Sea $g_1, \ldots, g_{(H_2:H_1)}$ una familia de representantes de las clases a izquierda de H_1 en H_2. Si $n > (H_2 : H_1)$, entonces existe una combinación lineal no trivial

$$y_1\widehat{x_1} + \cdots + y_n\widehat{x_n} \qquad \text{con } y_1, \ldots, y_n \in E,$$

tal que

$$y_1\widehat{x_1}(g_i) + \cdots + y_n\widehat{x_n}(g_i) = 0 \qquad \text{para todo } 1 \leq i \leq (H_2 : H_1),$$

Sea $g \in H_2$ arbitrario. Escribamos $g = g_i h$ con $h \in H_1$. Como los x_i's pertenecen a E^{H_1}, tenemos

$$\begin{aligned} y_1\widehat{x_1}(g) + \cdots + y_n\widehat{x_n}(g) &= y_1 g_i(h(x_1)) + \cdots + y_n g_i(h(x_n)) \\ &= y_1 g_i(x_1) + \cdots + y_n g_i(x_n) \\ &= y_1\widehat{x_1}(g_i) + \cdots + y_n\widehat{x_n}(g_i) = 0, \end{aligned}$$

lo que prueba que las funciones $\widehat{x_1}, \ldots, \widehat{x_n}$ no son linealmente independientes sobre E. $\square$

El siguiente resultado es una consecuencia formal del Teorema 13.5.

Corolario 13.6. *Sea E/K una extensión algebraica, $F_1 \subseteq F_2$ subcuerpos de E que contienen a K y $H_1 \subseteq H_2$ subgrupos de $\mathrm{G}(E/K)$. Se satisfacen:*

1) Si F_1/K es cerrada, entonces $(\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2)) = (F_2 : F_1)$.

2) Si F_1/K es cerrada y $(F_2 : F_1) < \infty$, entonces F_2/K es cerrada.

3) Si H_1 es cerrado, entonces $(E^{H_1} : E^{H_2}) = (H_2 : H_1)$.

4) Si H_1 es cerrado y $(H_2 : H_1) < \infty$, entonces H_2 es cerrado.

Demostración. Veamos 1) y 2). Si F_1/K es una subextensión cerrada de E/K, entonces $F_1 = E^{\mathrm{G}(E/F_1)}$ y por el Teorema 13.5,

$$\begin{aligned} (F_2 : F_1) &\geq (\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2)) \geq (E^{\mathrm{G}(E/F_2)} : E^{\mathrm{G}(E/F_1)}) \\ &= (E^{\mathrm{G}(E/F_2)} : F_1) = (E^{\mathrm{G}(E/F_2)} : F_2)(F_2 : F_1) \geq (F_2 : F_1). \end{aligned}$$

Así, $(\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2)) = (F_2 : F_1)$ y si además $(F_2 : F_1) < \infty$, entonces $(E^{\mathrm{G}(E/F_2)} : F_2) = 1$, lo que implica que $F_2 = E^{\mathrm{G}(E/F_2)}$. La demostración de 3) y 4) es similar. $\square$

El item 2) del Corolario anterior será mejorado por el item 1) de la Proposición 13.11. La demostración que daremos es independiente de lo que ya obtuvimos. Hemos puesto aquí este resultado parcial más que nada porque se sigue formalmente

del Teorema 13.5 y así tiene validez en otros contextos en los que hay un teorema similar a este.

Una subextensión F/K de E/K tiene codimensión finita si $(E : F) < \infty$. Por el Corolario 13.6, $|\,\mathrm{G}(E/K)| = (E : E^{\mathrm{G}(E/K)})$, los subgrupos finitos de $\mathrm{G}(E/K)$ son cerrados y la asignación dada por $H \mapsto E^H/K$ define un biyección entre el conjunto de los subgrupos finitos de $\mathrm{G}(E/K)$ y el conjunto de las subextensiones de codimensión finita de E/K que son cerradas. Similarmente las subextensiones F/K de E/K, tales que $E^{\mathrm{G}(E/K)} \subseteq F$ y $(F : E^{\mathrm{G}(E/K)}) < \infty$, son cerradas y la asignación dada por $F/K \mapsto \mathrm{G}(E/F)$ define una biyección entre el conjunto de estas subextensiones de E/K y el conjunto los subgrupos de índice finito de $\mathrm{G}(E/K)$ que son cerrados.

Definición 13.7. Una extensión algebraica E/K es galoisiana o de Galois si $E^{\mathrm{G}(E/K)} = K$, es decir si K es cerrada.

Si E/K es de Galois y finita, entonces $|\,\mathrm{G}(E/K)| = (E : K)$ y todas las subextensiones de E/K y todos subgrupos de $\mathrm{G}(E/K)$ son cerrados. Así, en este caso la asignación dada por $F/K \mapsto \mathrm{G}(E/F)$ define un isomorfismo entre el reticulado $\mathrm{I}(E/K)$ de subextensiones de E/K y el reticulado dual del formado por los subgrupos de $\mathrm{G}(E/K)$, cuya inversa es la aplicación dada por $H \mapsto E^H/K$. Este es el teorema fundamental de la teoría de Galois. A continuación caracterizamos a las extensiones de Galois y estudiamos algunas de sus propiedades.

Proposición 13.8. *Sea E/K una extensión algebraica. Son equivalentes:*

1) E/K es de Galois.

2) E/K es el cuerpo de descomposición de una familia de polinomios separables.

3) E/K es normal y separable.

Demostración. 1) $\Rightarrow$ 2) Dado $x \in E$ existen $\sigma_1, \ldots, \sigma_r \in \mathrm{G}(E/K)$ tales que para cada $\sigma \in G(E/K)$ existe un único $1 \leq i \leq r$ tal que $\sigma(x) = \sigma_i(x)$. Consideremos el polinomio $f_x = \prod_{i=1}^{r}(X - \sigma_i(x))$. Observemos los siguientes hechos:

- Como existe $1 \leq i \leq r$ tal que $\sigma_i(x) = \mathrm{id}(x) = x$, el elemento x es raíz de f_x,
- f_x es separable,
- Dado $\gamma \in \mathrm{G}(E/K)$ existe una permutación π de $\{1, \ldots, r\}$ tal que $\gamma \circ \sigma_i(x) = \sigma_{\pi(i)}(x)$. Así, $f_x = \prod_{i=1}^{r}(X - \gamma(\sigma_i(x)))$ y, por lo tanto, es un polinomio con coeficientes en $E^{\mathrm{G}(E/K)} = K$.

2) $\Rightarrow$ 3) Por el Teorema 7.4, E/K es normal y por la Proposición 8.12, E/K es separable.

3) $\Rightarrow$ 1) Esto es consecuencia inmediata del item 4) del Corolario 10.11. $\square$

Observación 13.9. Sea E/K una extensión normal y sean F y F' las clausuras puramente inseparables y separables de K en E, respectivamente. Por el item 1) del Corolario 10.11, F/K es normal y puramente inseparable y por la Proposición 13.8 y el item 4) del Corolario 10.11, E/F es normal y separable. En particular, por el item 5) del Corolario 10.11, $E = F.F'$. Además, por el item 2) del Corolario 8.14, F'/K es normal y separable y, por el item 1) de la Proposición 7.6 y el item 1) de la Proposición 10.9, E/F' es normal y puramente inseparable.

Para el caso de extensiones finitas la Proposición 13.8 puede ser complementada con el siguiente resultado.

Proposición 13.10. *Sea E/K una extensión finita. Son equivalentes:*

1) E/K es de Galois.

2) E/K es normal y separable.

3) E/K es el cuerpo de descomposición de un polinomio irreducible y separable.

4) $|\,\mathrm{G}(E/K)| = (E : K)$.

Demostración. 1) $\Leftrightarrow$ 2) Por la Proposición 13.8.

2) $\Rightarrow$ 3) Por el Corolario 12.5 existe $x \in E$ tal que $E = K(x)$. Como es normal E/K es el cuerpo de descomposición de $\mathrm{irr}(x, K)$, que es irreducible y separable.

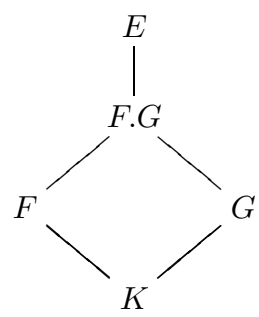
3) $\Rightarrow$ 2) Por la Proposición 13.8.

2) $\Leftrightarrow$ 4) Por la Proposición 6.4, $|\,\mathrm{G}(E/K)| = (E : K)$ equivale a $|\,\mathrm{G}(E/K)| = \gamma(E/K)$ y $\gamma(E/K) = (E : K)$. El resultado se deduce ahora del Teorema 7.5 y de la Proposición 8.11. $\square$

Proposición 13.11. *Se satisfacen:*

1) Sean F/K y E/F dos extensiones. Si E/K es galoisiana, entonces E/F también lo es.

2) Sea



un diagrama de extensiones. Si F/K es galoisiana, entonces también lo es $F.G/G$.

3) Si $(E_i/K)_{i\in I}$ es una familia de subextensiones galoisianas de E/K, entonces $K(\bigcup_{i\in I} E_i)/K$ y $(\bigcap_{i\in I} E_i)/K$ también lo son.

Demostración. Es consecuencia inmediata de la equivalencia entre los items 1) y 3) de la Proposición 13.8 y de las Proposiciones 7.6 y 8.16. $\square$

El teorema de Galois mencionado después de la Definición 13.7, puede ser probado sin usar ni la Proposición 13.4, ni el Teorema 13.5, ni el Corolario 13.6. Observemos en primer lugar que estos resultados no fueron usados ni en las demostraciones de las Proposiciones 13.8, 13.10 y 13.11, ni en la Observación 13.9. Ya sabemos, por la Proposición 13.11, que si E/K es galoisiana, entonces todos los subcuerpos de E que contienen a K son cerrados. Es suficiente probar entonces que si G es un grupo finito de automorfismos de E, entonces $\mathrm{G}(E/E^G) = G$. En efecto, esto muestra que todos los subgrupos finitos de de $\mathrm{G}(E/K)$ son cerrados. Además, para el caso en que E/K es de Galois y finita, las igualdades que aparecen en los items 1) y 3) del Corolario 13.6 se deducen facilmente de la Proposición 13.10. En efecto,

supongamos que $F_1 \subseteq F_2$ son subcuerpos de E que contienen a K. Entonces,

$$\begin{aligned}(\mathrm{G}(E/F_1) : \mathrm{G}(E/F_2))|\,\mathrm{G}(E/F_2)| &= |\,\mathrm{G}(E/F_1)| \\ &= (E : F_1) \\ &= (F_2 : F_1)(E : F_2) \\ &= (F_2 : F_1)|\,\mathrm{G}(E/F_2)|,\end{aligned}$$

lo que implica que $(F_2 : F_1) = (G(E/F_1) : G(E/F_2))$. Si ahora $H_1 \subseteq H_2$ son subgrupos de $\mathrm{G}(E/K)$, entonces

$$(E^{H_1} : E^{H_2}) = (\mathrm{G}(E/E^{H_2}) : \mathrm{G}(E/E^{H_1})) = (H_2 : H_1),$$

donde la última igualdad se sigue de que $H_1 = \mathrm{G}(E/E^{H_1})$ y $H_2 = \mathrm{G}(E/E^{H_2})$. Veamos una demostración directa del resultado enunciado más arriba. Es claro que $G \subseteq \mathrm{G}(E/E^G)$ y que E/E^G es de Galois y, en particular, separable. Dado $x \in E$, consideremos el polinomio $f_x = \prod_{\sigma\in G}(X-\sigma(x))$. Observemos los siguientes hechos:

- Como $\mathrm{id} \in G$, el elemento x es raíz de f_x,
- Dado que para cada $\gamma \in G$, el conjunto $\{\gamma \circ \sigma : \sigma \in G\}$ es igual a G, tenemos que $f_x = \prod_{\gamma\in G}(X - \gamma(\sigma(x)))$ y así, f_x tiene sus coeficientes en E^G.

Esto muestra que $\mathrm{gr}(\mathrm{irr}(x, E^G)) \leq |G|$. Dado que esto vale para cada $x \in E$, por el Corolario 12.6, $(E : E^G) \leq |G|$. Como $|\,\mathrm{G}(E/E^G)| \leq (E : E^G)$, tenemos entonces que $\mathrm{G}(E/E^G) = G$. Esta demostración se debe a Emil Artín.

A continuación estudiamos la relación existente entre las subextensiones normales de una extensión E/K y los subgrupos normales de $\mathrm{G}(E/K)$.

Teorema 13.12. *Sea E/K una extensión algebraica. Se satisfacen:*

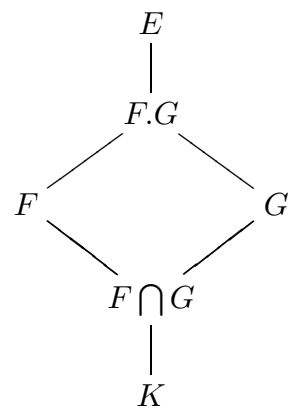
1) *Si F/K es una subextensión normal de E/K, entonces $\mathrm{G}(E/F)$ es un subgrupo normal de $\mathrm{G}(E/K)$.*
2) *Si E/K es normal y H es un subgrupo normal de $\mathrm{G}(E/K)$, entonces E^H/K es normal. Además, el morfismo de $\mathrm{G}(E/K)$ en $\mathrm{G}(E^H/K)$, definido por la restricción, tiene núcleo igual a $\mathrm{G}(E/E^H)$ y es sobreyectivo.*
3) *Si E/K es de Galois, entonces una subextensión F/K de E/K es de Galois si y sólo si $\mathrm{G}(E/F)$ es un subgrupo normal de $\mathrm{G}(E/K)$. Además, en este caso, $\mathrm{G}(F/K) \simeq \mathrm{G}(E/K)/\,\mathrm{G}(E/F)$.*

Demostración. 1) Se lo deduce inmediatamente del item 5) de la Observación 13.2.

2) Sea $f \in \mathrm{Hom}(E^H/K, C/K)$, donde C es una clausura algebraica de E. Por la Proposición 4.2, f se extiende a un morfismo $\widehat{f}\colon E/K \to C/K$. Como E/K es normal, $\widehat{f}(E) = E$, de modo que podemos considerar que $\widehat{f} \in \mathrm{G}(E/K)$. Por el item 6) de Observación 13.2, $f(E^H) = E^{\widehat{f}H\widehat{f}^{-1}} = E^H$. Así, E^H/K es normal. Es claro que el morfismo de $\mathrm{G}(E/K)$ en $\mathrm{G}(E^H/K)$, definido por restricción, tiene núcleo igual a $\mathrm{G}(E/E^H)$. Para ver que es sobreyectivo se puede razonar como en la primera parte de la demostración de este item.

3) Se lo deduce facilmente de los items 1) y 2), teniendo en cuenta que en este caso toda subextensión de E/K es cerrada y que además es de Galois si y sólo si es normal. □

Sea



un diagrama de extensiones con $F/F\bigcap G$ normal. Tomemos una clausura algebraica C de F en $F.G$. Cada morfismo $\sigma \in \mathrm{G}(F.G/G)$, define por restricción, un morfismo $\sigma_{|F} \in \mathrm{Hom}(F/F\bigcap G, C/F\bigcap G)$. Ahora, como $F/F\bigcap G$ es normal, tenemos que $\sigma(F) \subseteq F$. Queda definido de esta manera un morfismo

$$\theta\colon\ \mathrm{G}(F.G/G) \to \mathrm{G}(F/F\bigcap G).$$

Afirmamos que este morfismo es inyectivo. En efecto, tomemos $\sigma \in \mathrm{G}(F.G/G)$ tal que $\sigma_{|F} = \theta(\sigma) = \mathrm{id}_F$. Como $\sigma_{|G} = \mathrm{id}_G$, deducimos de aquí que $\sigma = \mathrm{id}_{F.G}$. Se satisface el siguiente resultado:

Proposición 13.13. *Si $F/F\bigcap G$ es de Galois, entonces $F.G/G$ también lo es y $F^{\mathrm{Im}(\theta)} = F\bigcap G$. Si además $F/F\bigcap G$ es finita, entonces θ es un isomorfismo y $(F : F\cap G) = (F.G : G)$. En particular, $(F.G : G)$ divide a $(F : K)$.*

Demostración. Por el item 2) de la Proposición 13.11, si $F/F\bigcap G$ es de Galois, entonces $F.G/G$ también lo es. Veamos que $F^{\mathrm{Im}(\theta)} = F\bigcap G$. Es claro que si $x \in F$ es dejado fijo por todos los elementos de $\mathrm{Im}(\theta)$, entonces es dejado fijo también por todos los elementos de $\mathrm{G}(F.G/G)$ y pertenece por lo tanto a $F\bigcap G$. Así, por el teorema fundamental de la teoría de Galois, si $F/F\bigcap G$ es finita, entonces $\mathrm{Im}(\theta) = \mathrm{G}(F/F\bigcap G)$ y $(F : F\bigcap G) = |\,\mathrm{G}(F/F\bigcap G)| = |\,\mathrm{G}(F.G/G)| = (F.G : G)$. En particular $(F.G : G)$ divide a $(F : K)$. □

Proposición 13.14. *Sea $E_1/K, \ldots, E_n/K$ una familia de subextensiones finitas de una extensión E/K. Si las extensiones $E_1/K, \ldots, E_{n-1}/K$ son de Galois, entonces $(E_1 \ldots E_n : K) = (E_n : K)\prod_{i=1}^{n-1}(E_i : E_i\bigcap(E_{i+1} \ldots E_{n+1}))$. En particular $(E_1 \ldots E_n : K)$ divide a $\prod_{i=1}^{n}(E_i : K)$ y son equivalentes:*

1) $E_i\bigcap(E_{i+1} \ldots E_n) = K$ para todo $1 \leq i < n$.

2) $(E_1 \ldots E_n : K) = \prod_{i=1}^{n}(E_i : K)$.

Demostración. Por la Proposición 13.13,

$$\begin{aligned}(E_1 \ldots E_n : K) &= (E_1 \ldots E_n : E_2 \ldots E_n)(E_2 \ldots E_n : K)\\ &= (E_1 : E_1\bigcap(E_2 \ldots E_n))(E_2 \ldots E_n : K).\end{aligned}$$

La igualdad del enunciado se sigue inmediatamente de esto por inducción en n. Ahora la equivalencia entre los items 1) y 2) es inmediata. □

Sea $(E_i/K)_{i\in I}$ una familia de subextensiones normales de una extensión E/K. El morfismo $\theta\colon\ \mathrm{G}(K(\bigcup E_i)/K) \to \prod_{i\in I}\mathrm{G}(E_i/K)$, definido por $\theta(f) = (f_{|E_i})_{i\in I}$, es claramente inyectivo. A continuación estudiamos un caso en el que vale la sobreyectividad.

Proposición 13.15. *Si $E_1/K, \dots, E_n/K$ es una familia de subextensiones de Galois finitas de una extensión E/K, entonces $E_1 \dots E_n/K$ también lo es y son equivalentes:*

1) El morfismo θ: $\mathrm{G}(E_1 \dots E_n/K) \to \mathrm{G}(E_1/K) \times \cdots \times \mathrm{G}(E_n/K)$ es biyectivo.

2) $(E_1 \dots E_n : K) = \prod_{i=1}^{n} (E_i : K)$.

2) $E_i \bigcap (E_{i+1} \dots E_n) = K$ para todo $1 \leq i < n$.

Demostración. Por el item 3) de la Proposición 13.11, la extensión $E_1 \dots E_n/K$ es de Galois. Ahora, dado que

$$|\,\mathrm{G}(E_1 \dots E_n/K)| = (E_1 \dots E_n : K) \quad \text{y} \quad \left|\prod_{i=1}^{n} \mathrm{G}(E_i/K)\right| = (E_1 : K) \dots (E_n : K),$$

los items 1) y 2) son equivalentes. La demostración se termina aplicando la Proposición 13.14. □

Los corolarios que siguen dan un ejemplo de como del conocimiento de propiedades del grupo de Galois de una extensión se pueden obtener datos sobre el reticulado de sus subextensiones. Recordemos que un grupo G es el producto semidirecto de un subgrupo normal suyo H_1 con otro subgrupo suyo H_2 si $H_1.H_2 = G$ y $H_1 \bigcap H_2 = \{1\}$.

Corolario 13.16. *Sean E/K una extensión de Galois finita y H_1 y H_2 subgrupos de $\mathrm{G}(E/K)$ con H_1 normal. Si $\mathrm{G}(E/K)$ es el producto semidirecto de H_1 y H_2 de G, entonces se satisfacen:*

1) E^{H_1}/K es de Galois y $\mathrm{G}(E^{H_1}/K) \simeq H_2$.

2) $E = E^{H_1}.E^{H_2}$.

3) $E^{H_1} \bigcap E^{H_1} = K$.

Demostración. 1) Es consecuencia del Teorema 13.12 y de que $\mathrm{G}(E/K)/H_1 \simeq H_2$.

2) Es consecuencia del teorema fundamental de la Teoría de Galois y de que $\mathrm{G}(E/E^{H_1}.E^{H_2}) = \mathrm{G}(E/E^{H_1}) \bigcap \mathrm{G}(E/E^{H_2}) = H_1 \bigcap H_2 = \{1\}$.

3) Se sigue de que, por la Proposición 13.13 y los items 1) y 2),

$$\begin{aligned}(E^{H_1} : E^{H_1} \bigcap E^{H_2}) &= (E^{H_1}.E^{H_2} : E^{H_2}) = (E : E^{H_2}) \\ &= |H_2| = |\,\mathrm{G}(E^{H_1}/K)| = (E^{H_1} : K). \quad \square\end{aligned}$$

Corolario 13.17. *Sea E/K una extensión de Galois finita. Supongamos que $\mathrm{G}(E/K) = G_1 \times \cdots \times G_n$ y escribamos $H_i = G_1 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_n$. Se satisfacen:*

1) E^{H_i}/K es de Galois y $\mathrm{G}(E^{H_i}/K) \simeq G_i$.

2) $E = E^{H_1} \dots E^{H_n}$.

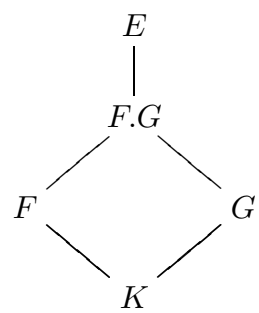
3) $E^{H_i} \bigcap (E^{H_{i+1}} \dots E^{H_n}) = K$, para todo $1 \leq i < n$.

Demostración. Por el Corolario 13.16 aplicado a H_1 y a G_1 obtenemos que E^{H_1}/K es de Galois y $\mathrm{G}(E^{H_1}/K) \simeq G_1$, $E^{H_1}.E^{G_1} = E$ y $E^{H_1} \bigcap E^{G_1} = K$. La proposición se sigue ahora facilmente por inducción en n. □

Definición 13.18. Una extensión E/K es abeliana (cíclica) si es de Galois y $\mathrm{G}(E/K)$ es abeliano (cíclico).

Proposición 13.19. *Se satisfacen:*

1) *Sean F/K y E/F dos extensiones. Si E/K es abeliana o cícica, entonces F/K y E/F también lo son.*
2) *Sea*



un diagrama de extensiones. Si F/K es finita y abeliana o finita y cíclica, entonces $F.G/G$ también lo es.

3) *Si $(E_i/K)_{i\in I}$ es una familia de subextensiones abelianas de E/K, entonces $K(\bigcup_{i\in I} E_i)/K$ también es abeliana.*

Demostración. 1) Se lo deduce facilmente de la Proposición 13.11 y del Teorema 13.12.

2) Se lo deduce facilmente de la Proposición 13.13.

3) Sean $f, g \in \mathrm{G}(K(\bigcup_{i\in I} E_i)/K)$. Como cada E_i/K es normal, $f(E_i) \subseteq E_i$ y $g_i(E_i) \subseteq E_i$ para todo $i \in I$ y como cada $\mathrm{G}(E_i/K)$ es abeliano, $f(g(x)) = g(f(x))$, para todo $x \in \bigcup_{i\in I} E_i$. Ahora es inmediato que $f \circ g = g \circ f$. $\square$

Ejemplo 13.20. Sea K un cuerpo y $K(t_1, \ldots, t_n)$ el cuerpo de fracciones del anillo de polinomios $K[t_1, \ldots, t_n]$ en n variables. El grupo simétrico $\mathfrak{S}_n$ opera sobre $K(t_1, \ldots, t_n)$ via $\sigma(t_i) = t_{\sigma(i)}$. A $K(t_1, \ldots, t_n)^{\mathfrak{S}_n}$ se lo llama el cuerpo de las funciones simétricas. Por el Corolario 13.6 $K(t_1, \ldots, t_n)/K(t_1, \ldots, t_n)^{\mathfrak{S}_n}$ es una extensión de Galois con grupo $\mathfrak{S}_n$. Sean $s_1, \ldots, s_n$ los polinomios simétricos elementales definidos por

$$s_i = \sum_{1\leq j_1<\cdots<j_i\leq n} t_{j_1} \ldots t_{j_i}.$$

Es claro que $K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)^{\mathfrak{S}_n}$. Como

$$P(X) = \prod_{i=1}^{n}(X - t_i) = X^n + \sum_{i=1}^{n}(-1)^i s_i X^{n-i},$$

$K(t_1, \ldots, t_n)$ es el cuerpo de descomposición de $P(X)$ sobre $K(s_1, \ldots, s_n)$. En consecuencia, si $P = P_1^{n_1} \ldots P_r^{n_r}$ con los P_i's irreducibles distintos de $K(s_1, \ldots, s_n)[X]$, entonces

$$\begin{aligned} n! &\geq \mathrm{gr}(P_1)! \ldots \mathrm{gr}(P_r)! \geq (K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)) \\ &\geq (K(t_1, \ldots, t_n) : K(t_1, \ldots, t_n)^{\mathfrak{S}_n})(K(t_1, \ldots, t_n)^{\mathfrak{S}_n} : K(s_1, \ldots, s_n)) \\ &= n!(K(t_1, \ldots, t_n)^{\mathfrak{S}_n} : K(s_1, \ldots, s_n)), \end{aligned}$$

de donde $K(t_1, \ldots, t_n)^{\mathfrak{S}_n} = K(s_1, \ldots, s_n)$ y P es irreducible en $K(s_1, \ldots, s_n)[X]$.

Teorema 13.21. *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

Demostración. Sea $F/\mathbb{C}$ una extensión finita de $\mathbb{C}$ y sea $E/\mathbb{R}$ la clausura normal de $F/\mathbb{R}$, donde $\mathbb{R}$ es el cuerpo de los números reales. Escribamos $(E:\mathbb{R}) = 2^h n$ con n impar. Por el teorema de Sylow existe un subgrupo H de $\mathrm{G}(E/\mathbb{R})$ de orden 2^h. Así, $E^H/\mathbb{R}$ es una extensión de $\mathbb{R}$ de grado n. Por el Corolario 12.5, existe $\alpha \in E^H$ tal que $E^H = \mathbb{R}(\alpha)$. En particular $\mathrm{irr}(\alpha, \mathbb{R})$ tiene grado n y, como en $\mathbb{R}[X]$ todo polinomio de grado impar tiene una raíz, $n = 1$. Así, $G(E/\mathbb{R})$ y, por lo tanto también $\mathrm{G}(E/\mathbb{C})$ es un 2-grupo. Afirmamos que $\mathrm{G}(E/\mathbb{C}) = \{\mathrm{id}\}$. En efecto, de lo contrario $\mathrm{G}(E/\mathbb{C})$ tendría un subgrupo normal H de índice 2 y, por el Teorema 13.12, $E^H/\mathbb{C}$ sería una extensión de grado 2, lo que contradice el hecho de que en $\mathbb{C}[X]$ cada polinomio de grado 2 tiene una raíz. Esto muestra que F es igual a $\mathbb{C}$, de donde $\mathbb{C}$ es algebraicamente cerrado. □

Definición 13.22. Un grupo G de biyecciones de un conjunto A es transitivo si para cada par $x, y \in A$ existe $\sigma \in G$ tal que $\sigma(x) = y$.

Proposición 13.23. *Sea $P \in K[X]$ un polinomio y sea E el cuerpo de descomposición de P. Son equivalentes:*

1) P es una potencia de un polinomio irreducible.

2) El grupo de Galois $\mathrm{G}(E/K)$ de E/K es un subgrupo transitivo del grupo de permutaciones de las raíces de P.

Demostración. 1) ⇒ 2) Sean $x_1, x_2 \in E$ dos raíces de P. Como P es una potencia de un polinomio irreducible existe $\sigma \in \mathrm{Hom}(K(x_1)/K, K(x_2)/K)$, que envía x_1 en x_2. Ahora, como E/K es normal, σ se extiende a un automorfismo de E/K.

2) ⇒ 1) Sea Q un factor irreducible de P, x una raíz de Q e y una raíz cualquiera de P. Por hipótesis existe $\sigma \in \mathrm{G}(E/K)$ tal que $\sigma(x) = y$. Así, $Q(y) = Q(\sigma(x)) = \sigma(Q(x)) = \sigma(0) = 0$, lo que muestra que toda raíz de P es raíz de Q y, por lo tanto, P es una potencia de Q. □

14. Extensiones ciclotómicas

Sea K un cuerpo y n un número natural. Las raíces de $X^n - 1$ en K se llaman raíces n-ésimas de la unidad en K. Es claro que $X^n - 1$ es separable si y sólo si la característica de K es cero o coprima con n. Así, en ese caso, hay n raíces n-ésimas de la unidad en cualquier cuerpo de descomposición de $X^n - 1$ sobre K. Supongamos que la característica de K es $p > 0$. Escribamos $n = p^r m$ con $r \geq 0$ y $p \nmid m$. En $K[X]$ vale la igualdad $X^n - 1 = (X^m - 1)^{p^r}$. Así, las raíces n-ésimas de la unidad en K coinciden con las m-ésimas.

Observación 14.1. Sea K un cuerpo, n un número natural que no es múltiplo de la característica de K y E un cuerpo de descomposición de $X^n - 1$ sobre K. Por la Proposición 12.1, el grupo U_n^K, formado por las raíces n-ésimas de la unidad en E, es cíclico de orden n. Así tiene $\varphi(n) := \#(\{m : 0 \leq m < n \text{ y } (\mathrm{m{:}n})=1\})$ generadores o raíces n-ésimas primitivas de la unidad. Denotemos con Ω_n^K al conjunto de estas raíces. Se satisfacen:

1) Si $n = ab$ con a y b coprimos, entonces la aplicación $\Theta\colon U_a^K \times U_b^K \to U_n^K$, definida por $\Theta(w_a, w_b) = w_a w_b$, es un isomorfismo con inversa dada por $\Theta^{-1}(w) =$

(w^{sb}, w^{ra}), donde $r, s \in \mathbb{Z}$ son tales que $1 = ra + sb$. En particular, Θ induce una biyección entre $\Omega_a^K \times \Omega_b^K$ y Ω_n^K (ya que $\Omega_a^K \times \Omega_b^K$ es el conjunto de los generadores de $U_a^K \times U_b^K$).

2) Supongamos que d divide a n. El morfismo $\pi\colon U_n^K \to U_{n/d}^K$, definido por $\pi(w) = w^d$ es sobreyectivo y tiene núcleo igual a U_d^K. En efecto, es claro que el núcleo de π es U_d^K. Dado que $\#(U_{n/d}^K) = \#(U_n^K)/\#(U_d^K)$, el morfismo π es sobreyectivo.

El polinomio $\phi_n(X) = \prod_{i=1}^{\varphi(n)}(X - w_i)$, cuyas raíces $w_1, \ldots, w_{\varphi(n)}$ son las raíces n-ésimas primitivas de la unidad, es llamado el n-ésimo polinomio ciclotómico. Es claro que U_n^K y $\phi_n(X)$ no dependen de K sino sólo del del cuerpo primo de K. Se satisfacen:

1) $\mathrm{gr}(\phi_n(X)) = \varphi(n)$.
2) Si $n = ab$ con a y b coprimos, entonces $\varphi(n) = \varphi(a)\varphi(b)$.
3) Si $n = p_1^{r_1} \ldots p_m^{r_m}$ es la fatorización de n como producto de primos, entonces $\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \ldots (p_m^{r_m} - p_m^{r_m-1}) = p_1^{r_1-1}(p_1 - 1) \ldots p_m^{r_m-1}(p_m - 1)$.
4) $X^n - 1 = \prod_{d|n} \phi_d(X)$.
5) $n = \sum_{d|n} \varphi(d)$.
6) Si m y n se factorizan como un producto de primos como $m = p_1^{h_1} \ldots p_s^{h_s}$ y $n = p_1^{l_1} \ldots p_s^{l_s}$ con $0 < h_i \leq l_i$, entonces $\phi_n(X) = \phi_m(X^{p_1^{l_1-h_1} \ldots p_s^{l_s-h_s}})$.
7) Si $n = p_1^{r_1} \ldots p_s^{r_s}$ es la fatorización de n como producto de primos, entonces $\phi_n(X) = \phi_{p_1 \ldots p_s}(X^{p_1^{r_1-1} \ldots p_s^{r_s-1}})$.
8) Si $n = pm$ con p primo y m coprimo con p, entonces $\phi_n(X) = \phi_m(X^p)/\phi_m(X)$.
9) Si $n = 2m$ con m impar, entonces $\phi_n(X) = \phi_m(-X)$.

En efecto, los items 1) y 4) son triviales. Al item 2) se lo deduce inmediatamente de que $\Omega_n^K \simeq \Omega_a^K \times \Omega_b^K$. El item 3) es consecuencia inmediata del 2) y de que si p es primo, entonces $\#(\{m : 0 \leq m < p^r \text{ y } p \mid m\}) = p^{r-1}$, lo que implica que $\varphi(p^r) = p^r - p^{r-1}$. El item 5) se sigue inmediatamente del 4). El item 6) es consecuencia de que cada raíz n-ésima primitiva de la unidad es raíz de $\phi_m(X^{p_1^{l_1-h_1} \ldots p_s^{l_s-h_s}})$ y de que $\mathrm{gr}(\phi_m(X^{p_1^{l_1-h_1} \ldots p_s^{l_s-h_s}})) = p_1^{l_1-h_1} \ldots p_s^{l_s-h_s}\varphi(m)$, que por 3) es igual a $\varphi(n)$. El item 7) es un caso particular del 6). El item 8) se sigue de que ξ es una raíz de $\phi_m(X^p)$ si y sólo si es una raíz primitiva de orden m o n y $\mathrm{gr}(\phi_m(X^p)/\phi_m(X)) = p\varphi(m) - \varphi(m) = \varphi(p)\varphi(m) = \varphi(n)$ y el item 9) se sigue de que ξ es una raíz de $\phi_m(-X)$ si y sólo si ξ es una raíz primitiva de orden n y $\mathrm{gr}(\phi_m(-X)) = \varphi(m) = \varphi(2)\varphi(m) = \varphi(n)$.

Observese que la fórmula del item 4) permite calcular recursivamente los polinomios ciclotómicos y muestra que son mónicos y pertenecen a $\mathbb{F}_p[X]$ si la característica de K es $p > 0$ y a $\mathbb{Z}[X]$ si la característica de K es cero. El siguiente resultado da la relación entre los polinomios ciclotómicos sobre $\mathbb{Q}$ y sobre $\mathbb{F}_p$.

Proposición 14.2. *Sea p un primo positivo y sea $n \in \mathbb{N}$ coprimo con p. Denotemos con $\phi_n^{\mathbb{Q}}(X)$ al n-ésimo polinomio ciclotómico sobre $\mathbb{Q}$ y con $\phi_n^{\mathbb{F}_p}(X)$ al n-ésimo polinomio ciclotómico sobre $\mathbb{F}_p$. Entonces $\phi_n^{\mathbb{F}_p}(X) = \overline{\phi_n^{\mathbb{Q}}(X)}$, donde $\overline{\phi_n^{\mathbb{Q}}(X)}$ denota al polinomio obtenido a partir de $\phi_n^{\mathbb{Q}}(X)$ tomando la clase en $\mathbb{F}_p$ de cada uno de sus coeficientes.*

Demostración. Para $n = 1$ el resultado es inmediato. Supongamos que $n > 1$ y que el resultado vale para todos los divisores propios de n. Como $X^n - 1 = \prod_{d|n} \phi_d^{\mathbb{Q}}(X)$, tenemos que $X^n - 1 = \prod_{d|n} \overline{\phi_d^{\mathbb{Q}}(X)}$. Así, dado que también $X^n - 1 = \prod_{d|n} \phi_d^{\mathbb{F}_p}(X)$ y que $\overline{\phi_d^{\mathbb{Q}}(X)} = \phi_d^{\mathbb{F}_p}(X)$ para todo divisor propio d de n, resulta que $\overline{\phi_n^{\mathbb{Q}}(X)} = \phi_n^{\mathbb{F}_p}(X)$. $\square$

Sean K un cuerpo, C una clausura algebraica de K y $w \in C$ una raíz n-ésima primitiva de la unidad. Entonces la característica de K no divide a n, $E = K(w)$ es el cuerpo de descomposición de $X^n - 1$ sobre K y la asignación,

$$\theta\colon\ \mathrm{G}(E/K) \to \mathbb{Z}_n^*,$$

dada por $\theta(\sigma) = i$ si $\sigma(w) = w^i$ está bien definida y es un morfismo inyectivo de $\mathrm{G}(E/K)$ en el grupo de unidades $\mathbb{Z}_n^*$ de $\mathbb{Z}_n$. Así el orden de $\mathrm{G}(E/K)$ divide a $\varphi(n)$. Además, como $|\,\mathrm{G}(E/K)| = \mathrm{gr}(\mathrm{irr}(w, K)$, son equivalentes:

- $(E : K) = \varphi(n)$,
- θ es sobreyectivo,
- $\phi_n(X)$ es irreducible en $K[X]$.

Ejemplo 14.3. Sean $n > 1$ un número natural, E un cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ y sea $w \in \mathbb{Q}$ una raíz n-ésima primitiva de la unidad, entonces $E = \mathbb{Q}(w)$ y $E/\mathbb{Q}$ es una extensión de Galois de grado $\varphi(n)$ con grupo isomorfo a $\mathbb{Z}_n^*$. En efecto tenemos el siguiente teorema.

Teorema 14.4. *Los polinomios ciclotómicos $\phi_n(X) \in \mathbb{Q}[X]$ son irreducibles.*

Demostración. Sea $P \in \mathbb{Z}[X]$ un divisor irreducible y mónico de $\phi_n(X)$. Queremos ver que $P = \phi_n(X)$. Para ello, como todas las raíces n-ésimas primitivas de la unidad se obtienen a partir de una dada por elevaciones a potencias primas y coprimas con n, es suficiente mostrar que si w es una raíz de P y p es un número primo que no divide a n, entonces w^p es también una raíz de P. Sea $Q \in \mathbb{Z}[X]$ tal que $PQ = X^n - 1$. Si w^p no fuera una raíz de P, entonces sería una raíz de Q y como $P = \mathrm{irr}(w, \mathbb{Q})$, tendríamos así que P dividiría a $Q(X^p)$. Entonces la clase $\overline{P}(X)$ de $P(X)$ en $\mathbb{F}_p[X]$ dividiría a la clase $\overline{Q}(X)^p = \overline{Q}(X^p)$ de $Q(X^p)$ en $\mathbb{F}_p[X]$ y, para todo divisor primo de T de P, tendríamos que T^2 divide a $X^n - 1$, lo que es una contradicción ya que, como p no divide a n, el polinomio $X^n - 1$ es separable en $\mathbb{F}_p[X]$. $\square$

Observación 14.5. Sean K un cuerpo, C una clausura algebraica de K y $w \in C$ una raíz n-ésima primitiva de la unidad. Entonces la característica de K no divide a n y $K(w)$ es el cuerpo de descomposición de $X^n - 1$ sobre K. Supongamos que $n = ab$ con a y b coprimos. Como $ra + sb = 1$ implica que $w^{ra}w^{sb} = w$, tenemos que $K(w^a).K(w^b) = K(w)$. Así, por la Proposición 13.14,

$$(*) \qquad (K(w) : K) \mid (K(w^b) : K)(K(w^a) : K).$$

Como w^b y w^a son raíces a-ésima y b-ésima primitivas de la unidad, respectivamente, tenemos también que

$$(**) \qquad (K(w^b) : K) \mid \varphi(a) \quad \text{y} \quad (K(w^a) : K) \mid \varphi(b).$$

Si $\phi_n(X)$ es primo, entonces $(K(w) : K) = \varphi(n)$, lo que junto a $(*)$, $(**)$ y a la igualdad $\varphi(n) = \varphi(a)\varphi(b)$, da

$$(K(w) : K) = (K(w^b) : K)(K(w^a) : K),$$
$$(K(w^b) : K) = \varphi(a) \quad \text{y} \quad (K(w^a) : K) = \varphi(b).$$

Así, $\phi_a(X)$ y $\phi_b(X)$ son primos y, por la Proposición 13.14, $K(w^b) \bigcap K(w^a) = K$.

Proposición 14.6. *Sean K un cuerpo y m y n dos enteros positivos. Si m divide a n y $\phi_n(X)$ es irreducible, entonces $\phi_m(X)$ también lo es.*

Demostración. Basta ver que si $n = pm$ con p primo y $\phi_n(X)$ es irreducible, entonces $\phi_m(X)$ también lo es. Si $p \nmid m$ esto se deduce de la Observación 14.5 y si $p \mid m$, esto se deduce de que, por el item 6) del comienzo de esta sección, $\phi_n(X) = \phi_m(X^p)$. $\square$

En la Proposición 14.9 probaremos que toda extensión cuadrática de $\mathbb{Q}$ está incluída en una extensión ciclotómica de una manera muy precisa. Nosotros usaremos que si p es un número primo impar, entonces $-1 \in \mathbb{F}_p$ es un cuadrado si y sólo si $p \equiv 1 \pmod 4$.

Observación 14.7. Sea p un número primo impar. Dado $x \in \mathbb{F}_p^*$ escribamos $\left(\frac{x}{p}\right) = x^{(p-1)/2}$. La asignación $x \mapsto \left(\frac{x}{p}\right)$ define un morfismo de grupos de $\mathbb{F}_p^*$ en el grupo multiplicativo $\{-1, 1\}$ de dos elementos. Sea α un generador de $\mathbb{F}_p^*$. Es claro que $\left(\frac{x}{p}\right) = 1$ si y sólo si $x = \alpha^i$ con $0 \leq i < p$ par y que esto ocurre si y sólo si x es un cuadrado en $\mathbb{F}_p^*$. En particular, $-1 \in \mathbb{F}_p$ es un cuadrado si y sólo si $p \equiv 1 \pmod 4$. Extendemos la definición de $\left(\frac{x}{p}\right)$ a $\mathbb{F}_p$ poniendo $\left(\frac{0}{p}\right) = 0$. Es claro que con esta definición sigue siendo válida la igualdad $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$. A $\left(\frac{x}{p}\right)$ se lo denomina el símbolo de Legendre.

Lema 14.8. *Sea p un número primo impar, K un cuerpo, C una clausura algebraica de K y $w \in C$ una raíz p-ésima primitiva de la unidad. Denotemos con α a $\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)w^x$. Entonces $\alpha^2 = \left(\frac{-1}{p}\right)p$.*

Demostración. En efecto, tenemos

$$\begin{aligned}
\alpha^2 &= \sum_{y,z=0}^{p-1}\left(\frac{yz}{p}\right)w^{y+z} \\
&= \sum_{u=0}^{p-1}\left(w^u\sum_{t=1}^{p-1}\left(\frac{t(u-t)}{p}\right)\right) \\
&= \sum_{u=0}^{p-1}\left(w^u\sum_{t=1}^{p-1}\left(\frac{-t^2}{p}\right)\left(\frac{1-ut^{-1}}{p}\right)\right) \\
&= \left(\frac{-1}{p}\right)\sum_{u=0}^{p-1}\left(w^u\sum_{t=1}^{p-1}\left(\frac{1-ut^{-1}}{p}\right)\right)
\end{aligned}$$

$$= \left(\frac{-1}{p}\right)\left(p-1+\sum_{u=1}^{p-1}\left(w^u\sum_{v=2}^{p-1}\left(\frac{v}{p}\right)\right)\right)$$
$$= \left(\frac{-1}{p}\right)\left(p-1-\sum_{u=1}^{p-1}w^u\right)$$
$$= \left(\frac{-1}{p}\right)p. \quad \square$$

Proposición 14.9. *Sea $\mathbb{Q}(\delta)/\mathbb{Q}$ con $\delta \in \mathbb{C}$ tal que δ^2 es un producto $\pm p_1 \dots p_r$ de primos distintos. Se satisfacen:*

1) Si todos los primos p_i son impares y congruentes a 1 módulo 4, entonces $\mathbb{Q}(\delta)/\mathbb{Q}$ está incluído en $\mathbb{Q}(w_\delta)/\mathbb{Q}$, donde w_δ es una raíz δ-ésima primitiva de la unidad.

2) Si alguno de los primos p_i es 2 o congruente a 3 módulo 4, entonces $\mathbb{Q}(\delta)/\mathbb{Q}$ está incluído en $\mathbb{Q}(w_{4\delta})/\mathbb{Q}$, donde $w_{4\delta}$ es una raíz 4δ-ésima primitiva de la unidad.

Demostración. Es suficiente probar que se satisfacen

a) $\sqrt{2} \in \mathbb{Q}(w_8)$, donde w_8 es una raíz de orden 4 primitiva de la unidad.

b) Si p es un primo congruente a 1 módulo 4, entonces $\sqrt{p} \in \mathbb{Q}(w_p)$, donde w_p es una raíz p-ésima primitiva de la unidad.

c) Si p es un primo congruente a 3 módulo 4, entonces $\sqrt{p} \in \mathbb{Q}(w_{4p})$, donde w_{4p} es una raíz $4p$-ésima primitiva de la unidad.

Como $w_8^4 = -1$, tenemos que $(w_8 + w_8^{-1})^2 = w_8^2 + 2 + w_8^{-2} = 2$, lo que prueba el item a). Supongamos ahora que p es un primo impar. Por el Lema 14.8, existe $\alpha \in \mathbb{Q}(w_p)$ tal que $\alpha^2 = \left(\frac{-1}{p}\right)p$. Si $p \equiv 1 \pmod 4$, entonces $\left(\frac{-1}{p}\right) = 1$ y tenemos que $\alpha^2 = p$, de donde $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(w_p)$. Esto prueba el item b). Supongamos ahora que $p \equiv 3 \pmod 4$. En este caso $\left(\frac{-1}{p}\right) = -1$, de modo que $\alpha^2 = -p$. Ahora, dado que $i \in \mathbb{Q}(w_{4p})$ tenemos que $i\alpha \in \mathbb{Q}(w_{4p})$ y la demostración del item c) se termina observando que $(i\alpha)^2 = -\alpha^2 = p$. $\square$

Uno de los teoremas más importantes de la teoría de congruencias es el teorema de reciprocidad cuadrática de Gauss. Una de sus tantas demostraciones se basa en el Lema 14.8. A continuación damos esta demostración. Pero primero probaremos un resultado complementario.

Proposición 14.10. *Sea p un primo impar. Entonces*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8, \\ -1 & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostración. Sea w una raíz primitiva 8-ésima de la unidad en una clausura algebraica de $\mathbb{F}_p$. Escribamos $y = w + w^{-1}$. Entonces

$$y^p = w^p + w^{-p} = \begin{cases} w + w^{-1} = y & \text{si } p \equiv \pm 1 \pmod 8, \\ w^3 + w^{-3} = -y & \text{si } p \equiv \pm 3 \pmod 8, \end{cases}$$

ya que $w^3 + w^{-3} = w^3 + w^5 = w^4(w^{-1} + w) = -y$. Así, como $w^4 = -1$ implica $y^2 = w^2 + 2 + w^{-2} = 2$,

$$\left(\frac{2}{p}\right) = y^{p-1} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8, \\ -1 & \text{si } p \equiv \pm 3 \pmod 8, \end{cases}$$

como queriamos. □

En la demostración de teorema de reciprocidad cuadrática usaremos el siguiente lema.

Lema 14.11. *Sea p un número primo impar, K un cuerpo, C una clausura algebraica de K y $w \in C$ una raíz p-ésima primitiva de la unidad. Denotemos con α a $\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) w^x$. Si $q = \text{char}(K) > 0$, entonces $q \neq p$ y $\alpha^{q-1} = \left(\frac{q}{p}\right)$.*

Demostración. Dado que por hipótesis hay una raíz p-ésima de la unidad en C, necesariamente $\text{char}(K) \neq p$. Ahora

$$\alpha^q = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) w^{xq} = \sum_{y=0}^{p-1} \left(\frac{yq^{-1}}{p}\right) w^y = \left(\frac{q^{-1}}{p}\right) \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) w^y = \left(\frac{q}{p}\right) \alpha,$$

de donde $\alpha^{q-1} = \left(\frac{q}{p}\right)$. □

Teorema 14.12 (de reciprocidad cuadrática). *Sean $p, q > 0$ dos primos impares. Entonces $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$.*

Demostración. Sea C una clausura algebraica de $\mathbb{F}_q$ y $w \in C$ una raíz p-ésima primitiva de la unidad. Denotemos con α a $\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) w^x$. Por los Lemas 14.8 y 14.11,

$$\begin{aligned} \left(\frac{q}{p}\right) &= \alpha^{q-1} \\ &= \left(\frac{\left(\frac{-1}{p}\right) p}{q}\right) \\ &= \left(\frac{\left(\frac{-1}{p}\right)}{q}\right) \left(\frac{p}{q}\right) \\ &= \left(\frac{(-1)^{(p-1)/2}}{q}\right) \left(\frac{p}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) \\ &= (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right). \quad \square \end{aligned}$$

El teorema anterior se puede utilizar para el calculo del símbolo de Legendre. Por ejemplo

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Una de las mayores dificultades que se presenta en este cálculo es en la necesidad de factorizar los números que van apareciendo. Este problema se soluciona mediante la introducción de un símbolo que extiende al de Legendre.

Definición 14.13 (Símbolo de Jacobi). Dados un número entero m y un número natural e impar n definimos el sḿbolo de Jacobi $\left(\frac{m}{n}\right)$ por

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right),$$

donde $n = \prod_{i=1}^{r} p_i$ es la factorización de n como producto de primos.

Lema 14.14. *Si m y n son impares, entonces $2 \mid m-1$, $2 \mid n-1$, $2 \mid mn-1$, $8 \mid m^2-1$, $8 \mid n^2-1$, $8 \mid m^2n^2-1$,*

$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$$

y

$$\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod 2,$$

Demostración. Es inmediato que $2 \mid m-1$, $2 \mid n-1$, $2 \mid mn-1$, $8 \mid m^2-1$, $8 \mid n^2-1$ y $8 \mid m^2n^2-1$. Dado que $(m-1)(n-1) \equiv 0 \pmod 4$, tenemos

$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2.$$

Finalmente, dado que $(m^2-1)(n^2-1) \equiv 0 \pmod{16}$, tenemos

$$\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod 2. \quad \square$$

Teorema 14.15. *Se satisfacen:*

1) $\left(\frac{m}{n_1n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)$.

2) $\left(\frac{m_1m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$.

3) Si $m_1 \equiv m_2 \pmod n$, *entonces* $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$.

4) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

5) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

6) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$.

Demostración. 1) se sigue directamente de la definición. 2) y 3) se siguen de la definición y de la propiedad correspondiente del símbolo de Legendre. Veamos 4). Supongamos que $n = \prod_{i=1}^{r} p_i$ es la factorización de n como producto de primos. Entonces, por el Lemma 14.14

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{r} (-1)^{(p_i-1)/2} = (-1)^{\sum_{i=1}^{r}(p_i-1)/2} = (-1)^{(n-1)/2}.$$

La demostración de 5) es similar. Veamos 6). Si $m = \prod_{i=1}^{r} p_i$ y $n = \prod_{j=1}^{s} q_j$ son las factorizaciones de m y n como productos de primos, entonces, por el Teorema 14.12, los items 1) y 2) de este teorema y el Lema 14.14,

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(p_i-1)(q_j-1)/4}\\ &= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}(p_i-1)(q_j-1)/4}\\ &= (-1)^{\sum_{i=1}^{r}(p_i-1)/2\sum_{j=1}^{s}(q_j-1)/2}\\ &= (-1)^{(m-1)(n-1)/4}.\end{aligned}$$

Por ejemplo

$$\left(\frac{403}{803}\right) = -\left(\frac{803}{403}\right) = -\left(\frac{-1}{403}\right)\left(\frac{3}{403}\right) = \left(\frac{3}{403}\right) = -\left(\frac{403}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Terminamos esta sección con una demostración del teorema de Wedderburn que dice que todo anillo de división finito es un cuerpo. En esta demostración se utilizan tanto la ecuación de las clases de la teoría de grupos finitos, como propiedades de los polinomios ciclotómicos.

Teorema 14.16 (Wedderburn). *Todo anillo de división finito D es un cuerpo.*

Demostración. Denotemos con Z el centro de D y con Z_x al centralizador en D de cada elemento $x \in D$. Es fácil ver que Z es un cuerpo y que cada Z_x es un anillo de división. Así, si $q = \#(Z)$, $n_x = (Z_x : Z)$, $m_x = (D : Z_x)$ y $n = (D : Z)$, tenemos que $n = m_x n_x$, $\#(Z_x) = q^{n_x}$ y $\#(D) = q^n = (q^{n_x})^{m_x}$. Es claro también que Z^* es el centro de D^* y que Z_x^* es el centralizador en D^* de cada elemento $x \in D^*$. Sea R un conjunto de representantes de cada una de las clases de conjugación de D^* que tienen más de un elemento. La ecuación de las clases de D^* queda

$$(*) \qquad q^n - 1 = \#(D^*) = \#(Z^*) + \sum_{x\in R}\frac{\#(D^*)}{\#(Z_x^*)} = q - 1 + \sum_{x\in R}\frac{q^n-1}{q^{n_x}-1}.$$

Dado que $x \notin Z$ para ningún $x \in R$, tenemos que n_x divide propiamente a n para todo $x \in R$. Así, tanto $X^n - 1$ como cada uno de los cocientes $\frac{X^n-1}{X^{n_x}-1}$ son polinomios divisibles por $\phi_n(X)$ en $\mathbb{Z}[X]$. De aquí se deduce inmediatamente que $\phi_n(q)$ divide en $\mathbb{Z}$ tanto a $q^n - 1$ como a cada uno de los enteros $\frac{q^n-1}{q^{n_x}-1}$. Por $(*)$ tenemos entonces que $\phi_n(q) \mid q - 1$, lo que implica que

$$\prod_{w\in\Omega_n}|q - w| = |\phi_n(q)| \mid q - 1,$$

donde Ω_n es el conjunto de las raíces n-ésimas primitivas de la unidad. Dado que si $n > 1$, entonces $|q - w| > q - 1$ para cada $w \in \Omega_n$, deducimos de aquí que $n = 1$ y, por lo tanto, $D = Z$. $\square$

15. Cuerpos finitos

Sea K un cuerpo finito con q elementos. Es claro que K tiene característica positiva p y que $q = p^n$, donde $n = (K : \mathbb{F}_p)$. En efecto, en este caso $K \simeq \mathbb{F}_p^{(n)}$ como $\mathbb{F}_p$-espacio vectorial, lo que implica que $q = p^n$. La siguiente proposición implica en particular que vale la recíproca.

Proposición 15.1. *Para cada primo $p > 0$ y cada número natural n, existe un cuerpo de p^n elementos. Además si un cuerpo tiene p^n elementos, entonces es el cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{F}_p$. En particular, toda extensión finita de un cuerpo finito es normal y separable y dos cuerpos que tienen la misma cantidad de elementos son isomorfos.*

Demostración. Sea C una clausura algebraica de $\mathbb{F}_p$ y sea K el conjunto de las raíces de $X^{p^n} - X$ en C. Como este polinomio es separable K tiene p^n elementos. Además es claro que $0, 1 \in K$ y que K es cerrado para la suma y el producto. Así, K es un anillo. Como K es un dominio finito, es un cuerpo. Supongamos ahora que K es un cuerpo que tiene p^n elementos. Por la Proposición 12.1 K^* es un grupo cíclico de orden $p^n - 1$ y, en consecuencia, todo elemento de K es una raíz de $X^{p^n} - X$. Como este polinomio tiene a lo sumo p^n raíces, K coincide con el conjunto de las raíces de $X^{p^n} - X$. En particular $K/\mathbb{F}_p$ es un cuerpo de descomposición de $X^{p^n} - X$, lo que por el Teorema 7.3, muestra que dos cuerpos finitos con la misma cantidad de elementos son isomorfos. □

A un cuerpo con q elementos lo denotaremos con $\mathbb{F}_q$. Por lo que acabamos de ver, salvo isomorfismos este cuerpo es único y además, $q = p^n$ donde p es la característica de K y $n = (K : \mathbb{F}_p)$.

Sea k un entero positivo. Analicemos la existencia de raíces k-ésimas en $\mathbb{F}_q$. Como el grupo multiplicativo de $\mathbb{F}_q$ es cíclico esto se puede hacer facilmente.

Proposición 15.2. *Sea α un generador de $\mathbb{F}_q$ y sea i un entero positivo. La ecuación $X^k = \alpha^i$ tiene solución si y sólo si $(k : q-1) \mid i$, donde $(k : q-1)$ denota al máximo de los divisores comunes de k y $q-1$. Además, en este caso, $X^k = \alpha^i$ tiene $(k : q-1)$ soluciones distintas. En particular $X^k = \beta$ tiene solución para todo $\beta \in \mathbb{F}_q$ si y sólo si $(k : q-1) = 1$ y, en este caso, la solución es única.*

Demostración. Es claro que $X^k = \alpha^i$ tiene solución si y sólo si existe $j \in \mathbb{N}$ tal que $\alpha^{jk} = \alpha^i$, lo que equivale a que $jk \equiv i \pmod{q-1}$. Así, $X^k = \alpha^i$ tiene solución si y sólo si $(k : q-1) \mid i$. Sean j y j' dos enteros positivos tales que $1 \leq j < j' \leq q-1$. Como $\alpha^{jk} = \alpha^{j'k}$ si y sólo si $q-1$ divide a $k(j'-j)$ o, lo que es lo mismo, si y sólo si $(q-1)/(k : q-1)$ divide a $j'-j$, la ecuación $X^k = \alpha^i$ tiene $(k : q-1)$ soluciones distintas. □

Es fácil determinar los subcuerpos de un cuerpo finito. Hacemos esto el la siguiente Proposición.

Proposición 15.3. *Sea $p > 0$ un número primo. Entonces $\mathbb{F}_{p^n}$ contiene a $\mathbb{F}_{p^m}$ si y sólo si m divide a n.*

Demostración. Sea F un subcuerpo de $\mathbb{F}_{p^n}$. Denotemos con p^m a la cantidad de elementos de F. Como $\mathbb{F}_{p^n}$ es un F-espacio vectorial, existe r tal que $p^n = \#(\mathbb{F}_{p^n}) = \#(F)^r = p^{mr}$, lo que muestra que m divide a n. Recíprocamente, supongamos que $m \mid n$. Entonces, $p^m - 1 \mid p^n - 1$, de donde $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$ y, por lo tanto,

$X^{p^m} - X \mid X^{p^n} - X$. Así, el cuerpo de descomposición $\mathbb{F}_{p^n}$ de $X^{p^n} - X$ sobre $\mathbb{F}_p$ contiene un cuerpo de descomposición $\mathbb{F}_{p^m}$ de $X^{p^m} - X$ sobre $\mathbb{F}_p$. $\square$

A continuación damos una demostración alternativa de que toda extensión finita de un cuerpo finito es de Galois y calculamos su grupo de Galois.

Proposición 15.4. *El grupo de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$ es cíclico de orden n y está generado por el elemento σ de $\mathrm{G}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, definido por $\sigma(x) = x^q$.*

Demostración. Es claro que $(\mathbb{F}_{q^n} : \mathbb{F}_q) = n$. Por la Proposición 12.1, los grupos $\mathbb{F}_q^*$ y $\mathbb{F}_{q^n}^*$ son cíclicos de orden $q-1$ y q^n-1, respectivamente. Como $x^{q^r} = \sigma^r(x) = x$ para todo $x \in \mathbb{F}_{q^n}$ equivale a que n/r, el orden de $\langle\sigma\rangle$ es n. Así, por las Proposiciones 6.4 y 13.10, la extensión $\mathbb{F}_{q^n}/\mathbb{F}_q$ es de Galois y $\mathrm{G}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\sigma\rangle$. $\square$

A continuación estudiamos los polinomios irreducibles sobre cuerpos finitos.

Proposición 15.5. *Para cada cuerpo finito $\mathbb{F}_q$ y cada entero positivo n, existe un polinomio irreducible $P \in \mathbb{F}_q[X]$ de grado n. Además si $P \in \mathbb{F}_q[X]$ es un polinomio irreducible de grado n y α es una raíz de P en una clausura algebraica C de $\mathbb{F}_q$, entonces se satisfacen:*

1) *P es separable y el cuerpo de descomposición de P sobre $\mathbb{F}_q$ es $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$.*
2) *Las raíces de P en C son $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$.*
3) *$\alpha^{q^m} = \alpha$ si y sólo si $n \mid m$. En particular n es el menor entero positivo tal que $\alpha^{q^n} = \alpha$.*
4) *$P \mid X^{q^m} - X$ si y sólo si $n \mid m$. En particular n es el menor entero positivo tal que $P \mid X^{q^n} - X$.*
5) *Supongamos que $P \neq X$.Entonces $P \mid X^{q^m-1} - 1$ si y sólo si $n \mid m$. En particular n es el menor entero positivo tal que $P \mid X^{q^n-1} - 1$. Además todas las raíces de P están en $\mathbb{F}_{q^n}^*$ y tienen el mismo orden en $\mathbb{F}_{q^n}^*$.*

Demostración. Como $\mathbb{F}_{q^n}/\mathbb{F}_q$ es simple, existe $\beta \in \mathbb{F}_{q^n}$ tal que $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$. Así, $\mathrm{irr}(\beta, \mathbb{F}_q)$ es un polinomio irreducible de grado n sobre $\mathbb{F}_q$. Supongamos ahora que $P \in \mathbb{F}_q[X]$ es un polinomio irreducible de grado n y que α es una raíz de P en una clausura algebraica C de $\mathbb{F}_q$. Como $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ es de Galois, P se factoriza en $\mathbb{F}_q(\alpha)$ como un producto de polinomios distintos de grado 1. En consecuencia, P es separable y $\mathbb{F}_q(\alpha)$ es el cuerpo de descomposición de P sobre $\mathbb{F}_q$. Como además $(\mathbb{F}_q(\alpha) : \mathbb{F}_q) = \mathrm{gr}(P) = n$, este cuerpo $\mathbb{F}_q(\alpha)$ es isomorfo a $\mathbb{F}_{q^n}$. Esto prueba el item 1). Los items 2) y 3) se siguen inmediatamente de que el grupo de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$ es cíclico de orden n y está generado por el elemento σ de $\mathrm{G}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, definido por $\sigma(x) = x^q$. Veamos el item 4). Como $P = \mathrm{irr}(\alpha, \mathbb{F}_q)$, tenemos que $P \mid X^{q^m} - X$ si y sólo si α es raíz de $X^{q^m} - X$, lo que por el item 3) equivale a que $n \mid m$. Por último, la primera parte del item 5) se sigue inmediatamente del item 4) y la segunda de que, por ser un automorfismo, $\sigma\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, preserva el orden de α en $\mathbb{F}_{q^n}^*$. $\square$

Sea $P \in \mathbb{F}_q[X]$ un polinomio irreducible distinto de X. Por los item 2) y 3) de la proposición anterior todas las raíces de P generan el mismo subgrupo cíclico de $\mathbb{F}_{q^n}^*$, donde n es el grado de P. Al orden de este subgrupo lo llamamos el orden de P y lo denotamos $o(P)$. Cuando $o(P) = q^n - 1$, decimos que P es primitivo sobre $\mathbb{F}_q$. El siguiente resultado da una manera de calcular el orden ν de P.

Proposición 15.6. *Sea $P \in \mathbb{F}_q[X]$ un polinomio irreducible distinto de X. Si P tiene orden ν, entonces $P \mid X^k - 1$ si y sólo si $\nu \mid k$. En particular ν es el menor entero positivo tal que $P \mid X^\nu - 1$.*

Demostración. Supongamos primero que $\nu \mid k$. Cada raíz α de P satisface $\alpha^\nu - 1 = 0$ y, por lo tanto, $\alpha^k - 1 = 0$. Como P es separable, esto implica que $P \mid X^k - 1$. Recíprocamente, si $P \mid X^k - 1$, entonces cada raíz de P es una raíz de $X^k - 1$ y así su orden divide a k. □

El siguiente corolario muestra en particular que el grado de un polinomio orreducible de $P \in F_q[X]$, distinto de X, está determinado por su orden.

Corolario 15.7. *Sea $P \in \mathbb{F}_q[X]$ un polinomio irreducible distinto de X. Denotemos con n a su grado y con ν a su orden. Son equivalentes:*

1) $P \mid X^{q^m-1} - 1$.

2) $n \mid m$.

3) $\nu \mid q^m - 1$.

En particular ν es coprimo con q y n es el orden de la clase de q en $\mathbb{Z}_\nu^*$.

Demostración. 1) $\Leftrightarrow$ 2) Por el item 5) de la Proposición 15.5.

1) $\Leftrightarrow$ 3) Por la Proposición 15.6. □

El siguiente corolario da un método que permite verificar si un polinomio es primo.

Corolario 15.8. *Sea $P \in \mathbb{F}_q[X]$ un polinomio de grado n y sea $\alpha \neq 0$ una raíz de P de orden ν. Son equivalentes:*

1) P es irreducible y distinto de X.

2) ν es coprimo con q y n es el orden de la clase de q en $\mathbb{Z}_\nu^*$.

Demostración. 1) $\Rightarrow$ 2) Por el Corolario 15.7.

2) $\Rightarrow$ 1) Por el Corolario 15.7 n es el grado de $\mathrm{irr}(\alpha, \mathbb{F}_q)$. Como $\mathrm{irr}(\alpha, \mathbb{F}_q)$ divide a P y los dos polinomios tienen el mismo grado, difieren en un múltiplo por un escalar no nulo. Es claro así que P es irreducible. □

Corolario 15.9. *Sean $P \in \mathbb{F}_q[X]$ un polinomio irreducible distinto de X, n y ν el grado y orden de P respectivamente y p un primo que divide a $q^n - 1$. Si $q^n - 1 = p^r u$ y $\nu = p^s v$ con $p \nmid u$ y $p \nmid v$, entonces $t = r - s$ es el mayor entero tal que $P \mid X^{(q^n-1)/p^t} - 1$.*

Demostración. Por el Corolario 15.7 $p^s v = \nu$ divide a $q^n - 1 = p^r u$. Es claro ahora que, por la Proposición 15.6, $t = r - s$ es el mayor entero tal que $P \mid X^{(q^n-1)/p^t} - 1$. □

Ejemplo. Consideremos el polinomio irreducible $X^6 + X + 1 \in \mathbb{F}_2[X]$. Como $P \nmid X^{21} - 1$ y $P \mid X^{63} - 1$ y como $P \nmid X^9 - 1$ y $P \mid X^{63} - 1$, por el Corolario 15.9, $3^2 \mid \nu$ y $7 \mid \nu$. Así, $\nu = 3^2.7 = 63$.

Ejemplo. Consideremos el polinomio irreducible $X^6 + X^4 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Como $q = 2$, tenemos que $q^6 - 1 = 63 = 3^2.7$. Como $P \nmid X^7 - 1$ y $P \mid X^{21} - 1$ y como $P \nmid X^9 - 1$ y $P \mid X^{63} - 1$, por el Corolario 15.9, $3 \mid \nu$ pero $3^2 \nmid \nu$ y $7 \mid \nu$. Así, $\nu = 3.7 = 21$.

Los ejemplos anteriores muestran que el orden de un polinomio irreducible no está determinado por su grado.

Proposición 15.10. *Sea $P \in \mathbb{F}_q[X]$ un polinomio irreducible distinto de X y sean n el grado de P y m un entero positivo. Entonces P se factoriza en $\mathbb{F}_{q^m}[X]$ como un producto de $(n : m)$ factores, cada uno de los cuales tiene grado igual a $n/(n : m)$.*

Demostración. Sean ν el orden de P y Q un factor primo de P en $\mathbb{F}_{q^m}[X]$. Por el Corolario 15.7 el grado de Q es igual al menor entero positivo r tal que $\nu \mid q^{mr} - 1$. La proposición se sigue inmediatamente de que, nuevamente por el Corolario 15.7, $r = n/(n : m)$. $\square$

Sea $\mathbb{F}_q$ un cuerpo finito de q elementos, n un número natural, E un cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{F}_q$ y $w \in E$ una raíz n-ésima primitiva de la unidad. La existencia de w muestra en particular que n es coprimo con q. Por el Corolario 15.7, $\mathrm{irr}(w, F_q)$ tiene grado igual al orden $o_n(\overline{q})$ de la clase $\overline{q}$ de q en $\mathbb{Z}_n^*$, de modo que $E = \mathbb{F}_q(w) = \mathbb{F}_{q^{o_n(\overline{q})}}$. Además, por la Proposición 15.4, $\mathrm{G}(E/\mathbb{F}_q)$ es cíclico de orden $o_n(\overline{q})$ y está generado por el elemento $\sigma \in \mathrm{G}(E/\mathbb{F}_q)$, definido por $\sigma(w) = w^q$. En particular, la aplicación $\theta\colon \mathrm{G}(E/\mathbb{F}_q) \to \mathbb{Z}_n^*$, definida después de la Proposición 14.2, satisface $\theta(\sigma) = \overline{q}$ y así es sobreyectiva si y sólo si $o_n(\overline{q}) = \varphi(n)$. Sea x un generador del grupo multiplicativo $\mathbb{F}^*_{q^{o_n(\overline{q})}}$ de $\mathbb{F}_{q^{o_n(\overline{q})}}$. A continuación determinamos que potencias de x son las raíces n-ésimas primitivas de la unidad en $\mathbb{F}^*_{q^{o_n(\overline{q})}}$.

Proposición 15.11. *Sea x un generador del grupo multiplicativo $\mathbb{F}^*_{q^{o_n(\overline{q})}}$ de $\mathbb{F}_{q^{o_n(\overline{q})}}$. El elemento x^k de $\mathbb{F}^*_{q^{o_n(\overline{q})}}$ es una raíz n-ésima primitiva de la unidad en $\mathbb{F}^*_{q^{o_n(\overline{q})}}$ si y sólo si $k = u\frac{q^{o_n(\overline{q})}-1}{n}$, donde $1 \leq u < n$ y $(u : n) = 1$.*

Demostración. Observemos en primer lugar que n divide a $q^{o_n(\overline{q})} - 1$. Para todo $k \geq 1$, el orden $o(x^k)$ de x^k es $o(x^k) = \frac{q^{o_n(\overline{q})}-1}{(q^{o_n(\overline{q})}-1:k)}$. En consecuencia, $o(x^k) = n$ si y sólo si $(q^{o_n(\overline{q})} - 1 : k) = \frac{q^{o_n(\overline{q})}-1}{n}$, es decir si $k = u\frac{q^{o_n(\overline{q})}-1}{n}$, donde $1 \leq u < n$ y $(u : n) = 1$. $\square$

Proposición 15.12. *Sea $n > 1$ un entero positivo y coprimo con q. Se satisfacen:*

1) *El polinomio ciclotómico $\phi_n(X) \in \mathbb{F}_q[X]$ se factoriza como el producto de todos los polinomios mónicos e irreducibles de orden n de $\mathbb{F}_q[X]$.*
2) *Denotemos con $o_n(\overline{q})$ al orden de la clase de q en $\mathbb{Z}_n^*$. Todos los polinomios mónicos e irreducibles de orden n de $\mathbb{F}_q[X]$ tienen grado $o_n(\overline{q})$ y su cantidad es $\varphi(n)/o_n(\overline{q})$.*

Demostración. 1) Sea P un polinomio mónico e irreducible de orden n de $\mathbb{F}_q[X]$. Por definición todas las raíces de P tienen orden n y son por lo tanto raíces de $\phi_n(X)$. Como P es separable, esto implica que $P \mid \phi_n(X)$. Dado que por otra parte, todo polinomio mónico e irreducible que divide a $\phi_n(X)$ tiene orden n, concluímos que $\phi_n(X) \in \mathbb{F}_q[X]$ se factoriza como el producto de todos los polinomios mónicos e irreducibles de orden n de $\mathbb{F}_q[X]$.

2) Por el Corolario 15.7 los polinomios irreducibles de orden n de $\mathbb{F}_q[X]$ tienen grado $o_n(\overline{q})$. Así, item 1) la cantidad de los que además son mónicos es $\varphi(n)/o_n(\overline{q})$. $\square$

Corolario 15.13. *Sea $n > 1$ un entero positivo y coprimo con q. El producto de todos los polinomios $P \in \mathbb{F}_q[X]$ distintos de X, que son mónicos e irreducibles y cuyo orden divide a n es igual a $X^n - 1$.*

Demostración. Esto se deduce inmediatamente de que $X^n - 1 = \prod_{d|n} \phi_d$ y de la Proposición 15.12. □

Proposición 15.14. *Sea $\mathbb{F}_q$ un cuerpo finito y n un número natural. El producto de todos los polinomios mónicos e irreducibles de $\mathbb{F}_q[X]$, cuyos grados dividen a n es igual a $X^{q^n} - 1$.*

Demostración. Por el item 4) de la Proposición 15.5, un polinomio mónico e irreducible de $\mathbb{F}_q[X]$ divide a $X^{q^n} - X$ si y sólo si su grado divide a n. La demostración se termina facilmente usando que $X^{q^n} - 1$ es separable. □

Dado un cuerpo finito $\mathbb{F}_q$ y un número natural n denotemos con $(\Upsilon_n)_{n\geq 1}$ al producto de todos los polinomios mónicos e irreducibles de $\mathbb{F}_q[X]$ de grado n. Por la Proposición 15.14, $X^{q^n} - X = \prod_{d|n} \Upsilon_d$. Esto da una manera recursiva de calcular los polinomios Υ_n, que muestra además que estos polinomios tienen coeficientes en el cuerpo primo de $\mathbb{F}_q$.

Sea $P \in \mathbb{F}_q[X]$ un polinomio de grado n. El método para ver si P es irreducible, enunciado en el Corolario 15.8, tiene la desventaja de que se requiere conocer el orden de alguna raíz de P. Los siguientes resultados puede ser utiles a la hora de comprobar si P es irreducible.

Proposición 15.15. *Sea $\mathbb{F}_q$ un cuerpo primo y $P \in \mathbb{F}_q[X]$ un polinomio mónico. Escribamos a P como un producto de polinomios mónicos e irreducibles $P = \prod_{i\in I} P_i$ y denotemos con n al mínimo de los múltiplos comunes de los grados de los P_i's. Son equivalentes:*

1) P es separable.

2) $P \mid X^{q^n} - X$.

3) Existe $m \in \mathbb{N}$ tal que $P \mid X^{q^m} - X$.

Además, en este caso, $P \mid X^{q^m} - X$ si y sólo si $n \mid m$.

Demostración. Denotemos con n_i al grado de P_i. Por la Proposición 15.5, $P_i \mid X^{q^m} - X$ si y sólo si $n_i \mid m$. Así, si P es separable, entonces $P \mid X^{q^m} - X$ si y sólo si $n \mid m$. Esto muestra en particular que 1) implica 2). Es trivial que 2) implica 3). Finalmente 3) implica 1) ya que $X^{q^m} - X$ es separable. □

Proposición 15.16. *Sea $\mathbb{F}_q$ un cuerpo primo y $P \in \mathbb{F}_q[X]$ un polinomio mónico que no es divisible por X. Escribamos a P como un producto de polinomios mónicos e irreducibles $P = \prod_{i\in I} P_i$ y denotemos con ν y n al mínimo de los múltiplos comunes de los ordenes y de los grados de los P_i's, respectivamente. Son equivalentes:*

1) P es separable.

2) $P \mid X^\nu - 1$.

Además, en este caso, $\nu \mid q^n - 1$ y $P \mid X^t - 1$ si y sólo si $\nu \mid t$.

Demostración. Denotemos con ν_i al orden de P_i. Por la Proposición 15.6, $P_i \mid X^t - 1$ si y sólo si $\nu_i \mid t$. Así, si P es separable, entonces $P \mid X^t - 1$ si y sólo si $\nu \mid t$. Esto muestra en particular que 1) implica 2). Veamos que 2) implica 1). En efecto, por el Corolario 15.7, ν es coprimo con q y por lo tanto $X^\nu - 1$ es separable. Así, si $P \mid X^\nu - 1$, entonces P es separable. Por último, por la Proposición 15.15, si P es separable, $\nu \mid q^n - 1$. □

16. Independencia lineal y algebraica de morfismos. Teorema de la base normal

Definición 16.1. Sea G un monoide y F un cuerpo. Un carácter de G en F es un morfismo $\xi\colon G \to F^*$, de G en el grupo multiplicativo de F. Al carácter que toma el valor constante 1 se lo llama carácter trivial.

Teorema 16.2 (Artín). *Cada familia $\xi_1, \dots, \xi_n$ de carácteres distintos de G en F es linealmente independiente sobre F.*

Demostración. Supongamos que existe una ecuación no trivial

$$a_1\xi_1 + \cdots + a_s\xi_s = 0 \tag{*}$$

de dependencia lineal con coeficientes en F. Cambiando los índices si es necesario, podemos suponer que s es la menor cantidad de sumandos que pueden aparecer en una ecuación de este tipo. Es claro que $s \geq 2$. Como $\xi_1 \neq \xi_2$ existe $z \in G$ tal que $\xi_1(z) \neq \xi_2(z)$. Para todo $x \in G$ tenemos $a_1\xi_1(zx) + \cdots + a_s\xi_s(zx) = 0$, de donde, como $\xi_1, \dots, \xi_n$ son carácteres,

$$a_1\xi_1(z)\xi_1 + \cdots + a_s\xi_s(z)\xi_s = 0.$$

Dividiendo esta relación por $\xi_1(z)$ y restandosela a $(*)$ obtenemos la ecuación

$$a_2(1 - \xi_2(z)/\xi_1(z))\xi_2 + \cdots + a_s(1 - \xi_s(z)/\xi_1(z))\xi_s = 0,$$

que es no trivial y tiene menos sumandos que $(*)$, lo que es absurdo. □

Corolario 16.3 (Dedekind). *Sean E/K y F/K dos extensiones. Cada familia de morfismos distintos de E/K en F/K es linealmente independiente sobre F.*

El resultado que acabamos de ver asegura que una familia $\sigma_1, \dots, \sigma_n$ de K-inclusiones distintas de E en F, es linealmente independiente sobre F. En otras palabras, dice que si $P(X_1, \dots, X_n) = \lambda_1X_1 + \cdots + \lambda_nX_n \in F[X_1, \dots, X_n]$ es un polinomio lineal no nulo, entonces $P(\sigma_1, \dots, \sigma_n) \neq 0$. Bajo circunstancias especiales, este resultado puede refinarse considerablemente. Dado un polinomio no necesariamente lineal $P(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$ denotamos con $P(\sigma_1, \dots, \sigma_n)$ a la función de E en F, definida por $P(\sigma_1, \dots, \sigma_n)(x) = P(\sigma_1(x), \dots, \sigma_n(x))$. Por ejemplo si $n = 2$ y $P(X_1, X_2) = X_1^2 + X_1X_2$, entonces $P(\sigma_1, \sigma_2)(x) = \sigma_1(x)^2 + \sigma_1(x)\sigma_2(x)$. Decimos que una famila $\sigma_1, \dots, \sigma_n$ de elementos de $\mathrm{Hom}(E/K, F/K)$ es algebraicamente independiente sobre F si para cada polinomio $P \in F[X_1, \dots, X_n]$, tenemos que $P(\sigma_1, \dots, \sigma_n) = 0$ si y sólo si $P = 0$. Probaremos a continuación que, bajo ciertas condiciones muy generales, vale la independencia algebraica de morfismos. En la demostración usaremos el siguiente resultado, importante en si mismo.

Teorema 16.4. *Sean E/K una extensión separable de grado n y $\sigma_1, \dots, \sigma_n$ las K-inclusiones de E en una clausura algebraica C de E. Una familia $B = \{\lambda_1, \dots, \lambda_n\}$ de elementos de E es una base de E sobre K si y sólo si* $\det(\sigma_i(\lambda_j)) \neq 0$.

Demostración. Tomemos $\alpha_1, \dots \alpha_n \in C$ y supongamos que B es una base de E sobre K. Entonces $\sum_{i=1}^n \alpha_i\sigma_i(\lambda_j) = 0$ para todo j implica que $\sum_{i=1}^n \alpha_i\sigma_i = 0$, lo que por el Corolario 16.3, implica a su vez que $\alpha_1 = \cdots = \alpha_n = 0$. Así, $\det(\sigma_i(\lambda_j)) \neq 0$. Recíprocamente supongamos que vale esta condición y que $\sum_{j=1}^n \alpha_j\lambda_j = 0$ con los α_j en K. Entonces $0 = \sigma_i(0) = \sum_{j=1}^n \alpha_j\sigma_i(\lambda_j)$, de donde $\alpha_j = 0$ para todo j. □

Teorema 16.5. *Sean E/K y F/K dos extensiones y $\sigma_1, \ldots, \sigma_n$ una familia de elementos distintos de* $\mathrm{Hom}(E/K, F/K)$. *Si E/K es finita y K es infinito, entonces $\sigma_1, \ldots, \sigma_n$ es algebraicamente independiente sobre F.*

Demostración. Como las restricciones de $\sigma_1, \ldots, \sigma_n$ a la clausura separable de K en E son todas distintas, podemos suponer que E/K es separable y reemplazando F, primero por su clausura algebraica y luego por la clausura algebraica de K en F, podemos suponer que F es la clausura algebraica de K. Considerando por último todos los morfismos de extensiones cuerpo de E/K en F/K podemos suponer que n es el grado de E/K. Supongamos que $P(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ es un polinomio tal que $P(\sigma_1, \ldots, \sigma_n)(x) = 0$, para todo $x \in E$. Sea $\{\lambda_1, \ldots, \lambda_n\}$ una base de E sobre K. Consideremos el polinomio $Q(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$, definido por

$$Q(X_1, \ldots, X_n) = P\left(\sum_{j=1}^{n} X_j \sigma_1(\lambda_j), \ldots, \sum_{j=1}^{n} X_j \sigma_n(\lambda_j)\right).$$

Para toda familia $\alpha_1, \ldots, \alpha_n$ de elementos de K,

$$\begin{aligned} Q(\alpha_1, \ldots, \alpha_n) &= P\left(\sum_{j=1}^{n} \alpha_j \sigma_1(\lambda_j), \ldots, \sum_{j=1}^{n} \alpha_j \sigma_n(\lambda_j)\right) \\ &= P\left(\sigma_1\left(\sum_{j=1}^{n} \alpha_j \lambda_j\right), \ldots, \sigma_n\left(\sum_{j=1}^{n} \alpha_j \lambda_j\right)\right) = 0, \end{aligned}$$

y así como K es infinito, $Q(X_1, \ldots, X_n) = 0$. Sean $\beta_1, \ldots, \beta_n \in F$. Dado que por el Teorema 16.4 $\det(\sigma_i(\lambda_j)) \neq 0$, existen $\alpha_1, \ldots, \alpha_n \in F$ tales que $\beta_i = \sum_{j=1}^{n} \alpha_j \sigma_i(\lambda_j)$ para todo i. Así,

$$P(\beta_1, \ldots, \beta_n) = P\left(\sum_{j=1}^{n} \alpha_j \sigma_1(\lambda_j), \ldots, \sum_{j=1}^{n} \alpha_j \sigma_n(\lambda_j)\right) = Q(\alpha_1, \ldots, \alpha_n) = 0,$$

para todo $\beta_1, \ldots, \beta_n \in F$, de donde $P = 0$. □

Teorema 16.6 (de la base normal). *Sean E/K una extensión de Galois de grado n y $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{G}(E/K)$. Existe $\lambda \in E$ tal que $\{\sigma_1(\lambda), \ldots, \sigma_n(\lambda)\}$ es una base de E sobre K.*

Demostración. Supongamos primero que K es un cuerpo finito $\mathbb{F}_q$. Entonces $E = \mathbb{F}_{q^n}$ y $\mathrm{G}(E/K) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{q^{n-1}}\}$, donde σ está definida por $\sigma(x) = x^q$. Por el Corolario 16.3, estas aplicaciones son linealmente independientes sobre $\mathbb{F}_{q^n}$. Así, el polinomio minimal de σ es $X^n - 1$ y, por lo tanto, coincide con el característico. Por el teorema de la descomposición cíclica de endomorfismos de espacios vectoriales de dimensión finita aplicado a este caso, existe $\lambda \in \mathbb{F}_{q^n}$ tal que

$$\{\lambda = \mathrm{id}(\lambda), \lambda^q = \sigma(\lambda), \lambda^{q^2} = \sigma^2(\lambda), \ldots, \lambda^{q^{n-1}} = \sigma^{q^{n-1}}(\lambda)\}$$

es una base de E sobre K. Supongamos ahora que K es infinito. Por el Teorema 16.4, para ver que existe $\lambda \in E$ tal que $\{\sigma_1(\lambda), \ldots, \sigma_n(\lambda)\}$ es una base de

E sobre K, es suficiente comprobar que existe $\lambda \in E$ tal que $\det(\sigma_i(\sigma_j(\lambda))) \neq 0$. Veamos esto. Consideremos la matriz

$$M = \begin{pmatrix} \sigma_1 \circ \sigma_1 & \sigma_1 \circ \sigma_2 & \dots & \sigma_1 \circ \sigma_n \\ \sigma_2 \circ \sigma_1 & \sigma_2 \circ \sigma_2 & \dots & \sigma_2 \circ \sigma_n \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n \circ \sigma_1 & \sigma_n \circ \sigma_2 & \dots & \sigma_n \circ \sigma_n \end{pmatrix}.$$

Observese que cada una de las filas y cada una de las columnas de M es una permutación $\sigma_1, \dots, \sigma_n$. Así,

$$M = \begin{pmatrix} \sigma_{1_1} & \sigma_{1_2} & \dots & \sigma_{1_n} \\ \sigma_{2_1} & \sigma_{2_2} & \dots & \sigma_{2_n} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n_1} & \sigma_{n_2} & \dots & \sigma_{n_n} \end{pmatrix},$$

donde $(i_1, \dots, i_n)$ es una permutación de $\{1, \dots, n\}$ para cada i y $(1_j, \dots, n_j)$ es una permutación de $\{1, \dots, n\}$ para cada j. Consideremos la matriz

$$N(X_1, \dots, X_n) = \begin{pmatrix} X_{1_1} & X_{1_2} & \dots & X_{1_n} \\ X_{2_1} & X_{2_2} & \dots & X_{2_n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n_1} & X_{n_2} & \dots & X_{n_n} \end{pmatrix}.$$

obtenida reemplazando cada σ_i por X_i en M. Afirmamos que el polinomio

$$P(X_1, \dots, X_n) = \det(N(X_1, \dots, X_n))$$

es no nulo. En efecto, como la matriz $N(1, 0, \dots, 0)$ tiene un 1 en cada fila y cada columna y cero en todos los demás lugares, $P(1, 0, \dots, 0) = \pm 1$, de donde $P \neq 0$. Así, por el Teorema 16.5, existe $\lambda \in E$ tal que $\det(\sigma_i(\sigma_j(\lambda))) = P(\sigma_1, \dots, \sigma_n)(\lambda) \neq 0$. $\square$

Sean E/K una extensión de Galois de grado n y $\{\sigma_1, \dots, \sigma_n\} = \mathrm{G}(E/K)$. Una base de E sobre K de la forma $\{\sigma_1(\lambda), \dots, \sigma_n(\lambda)\}$ se llama normal. A continuación damos un ejemplo de base normal.

Proposición 16.7. *Sea K un cuerpo, $n \in \mathbb{N}$ un número que no es múltiplo de la característica de K y E el cuerpo de descomposición de $X^n - 1$ sobre K. Supongamos que $\phi_n(X) \in K[X]$ es irreducible. Entonces, el conjunto Ω_n de las raíces n-ésimas primitivas de la unidad de E es una base normal de E sobre K si y sólo si n es un producto de primos distintos.*

Demostración. Sea $w \in E$ una raíz n-ésima primitiva de la unidad. Por el comentario que sigue a la Proposición 14.1, $E = K(w)$ y la aplicación $\theta\colon\ \mathrm{G}(E/K) \to \mathbb{Z}_n^*$, definida por $\theta(\sigma) = i$ si $\sigma(w) = w^i$, es un isomorfismo. Así,

$$\Omega_n = \{w^i : 1 \leq i \leq n \text{ y } (i : n) = 1\} = \{\sigma(w) : \sigma \in \mathrm{G}(E/K)\},$$

de modo de que si Ω_n es una base de E sobre K, entonces es una base normal. Veamos primero que si n es un producto de primos distintos, entonces Ω_n es una

base de E sobre K. Si n es un primo p, entonces $\Omega_p = \{w, \dots, w^{p-1}\}$, donde w es una raíz p-ésima primitiva de la unidad. Como $(E : K) = p - 1$ y $E = K(w)$, el conjunto $\{1, w, \dots, w^{p-2}\}$ es una base E sobre K. Así, dado que $1 + w + \cdots + w^{p-1} = \phi_p(w) = 0$, el conjunto $\Omega_p = \{w, \dots, w^{p-1}\}$ también es una base E sobre K. Supongamos ahora que el resultado es cierto para divisores propios de n y escribamos $n = pm$ con p primo. Sean w_1 raíz p-ésima primitiva de la unidad y w_2 una raíz m-ésima primitiva de la unidad. De la Proposición 14.6 se sigue que $(K(w_1) : K) = \varphi(p)$ y $(K(w_2) : K) = \varphi(m)$. Así, por hipótesis inductiva, Ω_p es una base de $K(w_1)$ sobre K y Ω_m es una base de $K(w_2)$ sobre K. En consecuencia, dado que $E = K(w_1).K(w_2)$, el conjunto $\Omega_n = \Omega_p\Omega_m := \{w_1w_2 : w_1 \in \Omega_p \text{ y } w_2 \in \Omega_m\}$ genera a E sobre K. Como $(E : K) = \varphi(n) = \#(\Omega_n)$ tenemos finalmente que Ω_n es una base de E sobre K. Para la inversa, supongamos que $n = p^k m$ con $k > 1$. Dado que, por el item 6) de la Observación 14.1, $\phi_n(X) = \phi_{pm}(X^{p^{k-1}})$, el coeficiente de $X^{\varphi(n)-1}$ en $\phi_n(X)$ es cero. Como este coeficiente es la suma de las raíces n-ésimas primitivas de la unidad, en este caso, estas raíces no forman una base de E sobre K. □

17. Polinomios simétricos

En lo que sigue probamos que todo polinomio simétrico se escribe de manera única como un polinomio en los polinomios simétricos elementales. Nosotros trabajamos en un contexto más general que el dado en el Ejemplo 13.20, permitiendo que los polinomios tengan coeficientes en un anillo conmutativo arbitrario.

Sea A un anillo conmutativo y $A[t_1, \dots, t_n]$ el anillo de polinomios en n variables. El grupo simétrico $\mathfrak{S}_n$ opera sobre $A[t_1, \dots, t_n]$ via $\sigma(t_i) = t_{\sigma(i)}$. A los polinomios $P \in A[t_1, \dots, t_n]$ que satisfacen la ecuación $\sigma(P) = P$ se los denomina polinomios simétricos. Denotamos con $A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ al subanillo de $A[t_1, \dots, t_n]$ formado por los polinomios simétricos. Sean $s_1, \dots, s_n$ los polinomios simétricos elementales definidos por

$$s_i = \sum_{1 \le j_1 < \cdots < j_i \le n} t_{j_1} \dots t_{j_i}.$$

Es claro que $A[s_1, \dots, s_n] \subseteq A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. En el Teorema 17.2 mostramos que todo polinomio simétrico se escribe de manera única como un polinomio en los polinomios simétricos elementales.

Teorema 17.1. *Los polinomios simétricos elementales $s_1, \dots, s_n$ son algebraicamente independientes sobre A.*

Demostración. Supongamos que el resultado es falso. Sea n el menor entero positivo para el que falla y sea

$$P(X_1, \dots, X_n) \neq 0 \quad \text{de grado mínimo con} \quad P(s_1, \dots, s_n) = 0.$$

Escribamos

$$P(X_1, \dots, X_n) = P_0(X_1, \dots, X_{n-1}) + \cdots + P_d(X_1, \dots, X_{n-1})X_n^d.$$

Debe ser $P_0(X_1, \dots, X_{n-1}) \neq 0$, ya que si no

$$P(X_1, \dots, X_n) = X_nQ(X_1, \dots, X_n) \Rightarrow Q(s_1, \dots, s_n) = 0,$$

lo que es absurdo porque $\mathrm{gr}(Q) < \mathrm{gr}(P)$. Evaluando ahora en $t_n = 0$, la igualdad

$$0 = P_0(s_1, \ldots, s_{n-1}) + \cdots + P_d(s_1, \ldots, s_{n-1}) s_n^d,$$

obtenemos que $0 = P_0(s'_1, \ldots, s'_{n-1})$, donde los s'_i's son los polinomios simétricos elementales en $t_1, \ldots, t_{n-1}$, lo que contradice la minimalidad de n. $\square$

Teorema 17.2. *Sea $P \in A[t_1, \ldots, t_n]$ un polinomio simétrico. Entonces existe un único polinomio $Q(X_1, \ldots, X_n)$, tal que*

$$P(t_1, \ldots, t_n) = Q(s_1, \ldots, s_n).$$

Demostración. La unicidad se deduce de la independencia algebraica de los s_i's. Veamos la existencia. Ordenemos los monomios $t_1^{\alpha_1} \ldots t_n^{\alpha_n}$, poniendo

$$t_1^{\alpha_1} \ldots t_n^{\alpha_n} > t_1^{\beta_1} \ldots t_n^{\beta_n}$$

si $\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$ o si ambas sumas coinciden, pero existe $0 \leq s < n$ tal que $\alpha_1 = \beta_1, \ldots, \alpha_s = \beta_s$ y $\alpha_{s+1} > \beta_{s+1}$. Es fácil ver que existen sólo una cantidad finita de monomios que son menores que un monomio dado. Sea P un polinomio simétrico. Sea $t_1^{\alpha_1} \ldots t_n^{\alpha_n}$ el monomio más grande que aparece en P con coeficiente c no nulo. Como P es simétrico, los momomios obtenidos a partir de $t_1^{\alpha_1} \ldots t_n^{\alpha_n}$, permutando las variables, aparecen en P con el mismo coeficiente Así $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. Dado que el monomio más grande que aparece en s_i con coeficiente no nulo es $t_1 \ldots t_i$, el mayor monomio que aparece en $s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \ldots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n}$ es $t_1^{\alpha_1} \ldots t_n^{\alpha_n}$. Así, el monomio más grande que aparece en

$$P(t_1, \ldots, t_n) - c s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \ldots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n}$$

con coeficiente no nulo es menor que $t_1^{\alpha_1} \ldots t_n^{\alpha_n}$. La demostración se termina ahora fácilmente, usando un argumento inductivo. $\square$

A continuación consideramos una familia importante de polinomios simétricos, conocidos como polinomios de Newton, y encontramos fórmulas recursivas que permiten calcularlos. Para cada $k \geq 0$ definimos el polinomio de Newton $p_k \in A[t_1, \ldots, t_n]$ por

$$p_k(t_1, \ldots, t_n) = t_1^k + \cdots + t_n^k.$$

Antes de enunciar las fórmulas recursivas mencionadas arriba probamos un lema que usaremos en la demostración de estas fórmulas.

Lema 17.3. *Sea A un anillo conmutativo y $P \in A[t_1, \ldots, t_n]$ un polinomio de grado $d < n$. Si P se anula cada vez que $n - d$ de sus indeterminadas son evaluadas en cero, entonces $P = 0$.*

Demostración. Si $P \neq 0$, entonces P es suma de términos no nulos de la forma

$$\alpha t_{i_1}^{v_1} \ldots t_{i_m}^{v_m},$$

con $v_i \geq 1$ y $v_1 + \cdots + v_m \leq d$. Como esto implica que $m \leq d$, evaluando en cero $n - d$ variables distintas de $t_{i_1}, \ldots, t_{i_m}$, se obtiene un polinomio no nulo. $\square$

Teorema 17.4 (relaciones de Newton). *Escribamos $s_i = 0$ para todo $i > n$. Entonces,*

$$p_k - p_{k-1}s_1 + \cdots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k = 0,$$

para todo $k \geq 0$.

Demostración. Un cálculo directo muestra que

$$t_i^n - s_1 t_i^{n-1} + \cdots + (-1)^{n-1} s_{n-1} t_i + (-1)^n s_n = 0 \quad \text{para todo } 1 \leq i \leq n.$$

Así, para todo $1 \leq i \leq n$ y todo $k \geq n$,

$$t_i^k - s_1 t_i^{k-1} + \cdots + (-1)^{n-1} s_{n-1} t_i^{k-n+1} + (-1)^n s_n t_i^{k-n} = 0.$$

Sumando estas igualdades, para i entre 1 y n deducimos que el resultado vale para todo $k \geq n$. Consideremos ahora el polinomio simétrico

$$P(t_1, \ldots, t_n) = p_k - p_{k-1}s_1 + \cdots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k,$$

para $k < n$. Por la parte del teorema que ya hemos probado aplicada al caso $n = k$,

$$P(t_1, \ldots, t_k, 0, \ldots, 0) = 0.$$

Dado que P es simétrico, esto muestra que P se anula cada vez que evaluamos $n-k$ cualesquiera de sus variables en cero. Así, por el Lema 17.3, P es nulo. □

El resultado anterior no sólo da una manera recursiva para expresar los polinomios de Newton en función de los polinomios simétricos elementales, sino que también permite expresar los polinomios simétricos elementales $s_1, \ldots, s_n$ en función de $p_1, \ldots, p_n$, bajo la hipótesis de que A contenga a los racionales. De aquí se deduce la parte de la existencia del siguiente resultado:

Corolario 17.5. *Sea A un anillo conmutativo que contiene a $\mathbb{Q}$ y $P \in A[t_1, \ldots, t_n]$ un polinomio simétrico. Entonces existe un único polinomio $Q(X_1, \ldots, X_n)$, tal que*

$$P(t_1, \ldots, t_n) = Q(p_1, \ldots, p_n).$$

Demostración. Acabamos de probar que existe Q. Para ver que es único se puede proceder exactamente como en el Teorema 17.1. □

Veamos una demostración de que el cuerpo de los números complejos es algebraicamente cerrado, que utiliza que cada polinomio simétrico es un polinomio en los polinomios simétricos elementales. Usaremos los siguientes hechos:

1) Todo polinomio de grado impar con coeficientes reales tiene una raíz real.
2) Todo polinomio de segundo grado con coeficientes complejos tiene sus raíces en el cuerpo de los números complejos.
3) Dado un polinomio no constante P de $\mathbb{R}[X]$, existe una extensión K de $\mathbb{C}$ en donde P se descompone como producto de polinomios de grado 1.
4) Todo polinomio simétrico es un polinomio en los polinomios simétricos elementales.

Teorema 17.6. *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

Demostración. Tenemos que ver que todo polinomio no constante $P(X) \in \mathbb{C}[X]$ tiene una raíz en $\mathbb{C}$. Considerando el polinomio $F(X) = \frac{1}{|\lambda|^2} P(X)\overline{P(X)}$, donde $\overline{P(X)}$ es el conjugado de $P(X)$ y λ el coeficiente principal de P, reducimos el problema al caso de polinomios mónicos y con coeficientes reales. Escribamos

$$\mathrm{gr}(F) = d = 2^n q \quad \text{con } q \text{ impar}$$

Hacemos la demostración por inducción en n. Si $n = 0$ el resultado se sigue de 1). Supongamos entonces que $n \geq 1$. Por 3) existe una extensión K de $\mathbb{C}$ y $x_1, \ldots, x_d \in K$ tal que

$$F(X) = \prod_{i=1}^{d} (X - x_i).$$

Sea c un elemento arbitrario de $\mathbb{R}$ y consideremos los elementos $y_{ij} = x_i + x_j + c x_i x_j$ con $i \leq j$ de K. Su cantidad es $\frac{1}{2} d(d+1) = 2^{n-1} q(d+1)$ y $q(d+1)$ es impar. Los coeficientes de

$$G(X) = \prod_{i \leq j} (X - y_{ij})$$

son polinomios reales y simétricos en los x_i's. Así, por 4) los coeficientes de G son polinomios reales evaluados en los coeficientes de F y, por lo tanto, son números reales. Por la hipótesis inductiva $G(X)$ tiene una raíz z_c en $\mathbb{C}$. Esta raíz es uno de los y_{ij}. Escribamos

$$z_c = y_{i_c j_c} = x_{i_c} + x_{j_c} + c x_{i_c} x_{j_c}.$$

Como $\mathbb{R}$ es infinito y el conjunto de los pares (i, j) con $i \leq j$ es finito, existen dos números reales distintos c y c' tales que $i_c = i_{c'}$ y $j_c = j_{c'}$. Denotemos con r y s a estos índices. Entonces,

$$x_r + x_s + c x_r x_s \in \mathbb{C} \qquad \text{y} \qquad x_r + x_s + c' x_r x_s \in \mathbb{C},$$

de donde se deduce inmediatamente que $x_r + x_s$ y $x_r x_s$ pertenecen a $\mathbb{C}$. Así el polinomio $(X - x_r)(X - x_s)$ tiene sus coeficientes en $\mathbb{C}$ y por 2) $x_r, x_s \in \mathbb{C}$. $\square$

18. Norma y traza

Definición 18.1. Sean E/K una extensión finita, C una clausura algebraica de K y $\sigma_1, \ldots, \sigma_n$ la familia de morfismos de extensiones de E/K en C/K. Definimos la traza $\mathrm{T}_K^E(\alpha)$ y la norma $\mathrm{N}_K^E(\alpha)$ de un elemento α de E, como

$$\mathrm{T}_K^E(\alpha) = (E : K)_i \sum_{j=1}^{n} \sigma_j(\alpha) \quad \text{y} \quad \mathrm{N}_K^E(\alpha) = \left(\prod_{j=1}^{n} \sigma_j(\alpha) \right)^{(E:K)_i},$$

respectivamente.

Teorema 18.2. *Se satisfacen:*

1) *La traza es una función K-lineal de E en K, no depende de la clausura algebraica de C de K elegida y es no nula si y sólo si E/K es separable.*
2) *La norma es una función multiplicativa que manda E^* en K^* y no depende de la clausura algebraica C de K elegida.*

Demostración. Tomemos en primer lugar una clausura algebraica C de E y denotemos con $\mathrm{T}_K^{E,C}$ y $\mathrm{N}_K^{E,C}$ a la traza y la norma definidas usando esta clausura algebraica. Denotemos con E' a la clausura normal de E en C. Para cada $\sigma \in \mathrm{Hom}(E'/K, C/K)$ existe una permutación π de $\{1, \ldots, n\}$ tal que $\sigma \circ \sigma_i = \sigma_{\pi(i)}$ para $1 \leq i \leq n$. Así,

$$\sigma\left(\sum_{i=1}^{n} \sigma_i(\alpha)\right) = \sum_{i=1}^{n} \sigma_{\pi(i)}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

y

$$\sigma\left(\prod_{i=1}^{n} \sigma_i(\alpha)\right) = \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

de modo que, por el item 3) del Corolario 10.11, $\sum_{i=1}^{n} \sigma_i(\alpha)$ y $\prod_{i=1}^{n} \sigma_i(\alpha)$ pertenecen a la clausura puramente inseparable F de K en E'. Ahora, si E/K no es separable, entonces $(E : K)_i \neq 1$, lo que implica que $\mathrm{T}_K^{E,C} = 0$. Por otro lado, si E/K es separable, entonces por el Corolario 16.3, $\mathrm{T}_K^{E,C} \neq 0$. Además, por la Proposición 8.17, E'/K también es separable, de modo que $F = K$ y así la imagen de $\mathrm{T}_K^{E,C}$ está siempre incluída en K. Afirmamos que la imagen de E por $\mathrm{N}_K^{E,C}$ está incluída en K. En efecto, si $\alpha \in E$, entonces por los items 2) y 3) de la Proposición 10.7, $\alpha^{(E:K)_i}$ es separable, de modo de que

$$\mathrm{N}_K^E(\alpha) = \left(\prod_{j=1}^{n} \sigma_j(\alpha)\right)^{(E:K)_i} = \prod_{j=1}^{n} \sigma_j\left(\alpha^{(E:K)_i}\right)$$

también lo es. Así, por el item 5) del Corolario 10.11, $\mathrm{N}_K^E(\alpha) \in K$. Veamos ahora que la traza y la norma no dependen de la clusura algebraica de K elegida. En efecto, supongamos que C' es otra clausura algebraica de K y denotemos con $\mathrm{T}_K^{E,C'}$ y $\mathrm{N}_K^{E,C'}$ a la traza y la norma definidas usando esta clausura algebraica. Consideremos un isomorfismo σ de extensiones de C/K en C'/K y sea $\alpha \in E$. Como $\mathrm{T}_K^{E,C}(\alpha)$ y $\mathrm{N}_K^{E,C}(\alpha)$ están en K y $(\sigma \circ \sigma_i)_{1 \leq i \leq n}$ es la familia de morfismos de extensiones de E/K en C'/K,

$$\mathrm{T}_K^{E,C}(\alpha) = \sigma(\mathrm{T}_K^{E,C}(\alpha)) = (E : K)_i \sum_{j=1}^{n} \sigma(\sigma_j(\alpha)) = \mathrm{T}_K^{E,C'}(\alpha),$$

y

$$\mathrm{N}_K^{E,C}(\alpha) = \sigma(\mathrm{N}_K^{E,C}(\alpha)) = \left(\prod_{j=1}^{n} \sigma(\sigma_j(\alpha))\right)^{(E:K)_i} = \mathrm{N}_K^{E,C'}(\alpha).$$

Por último es inmediato que T_K^E es K-lineal, que N_K^E es multiplicativa y que $\mathrm{N}_K^E(E^*) \subseteq K^*$. $\square$

Teorema 18.3. *Sean F/K y E/F dos extensiones finitas. Se satisfacen:*

$$\mathrm{T}_K^E = \mathrm{T}_K^F \circ \mathrm{T}_F^E \qquad y \qquad \mathrm{N}_K^E = \mathrm{N}_K^F \circ \mathrm{N}_F^E .$$

Demostración. Sea C una clausura algebraica de F y sean $(\tau_i)_{1\leq i\leq r}$ la familia de morfismos de extensiones de F/K en C/K y $(\sigma_j)_{1\leq j\leq s}$ la familia de morfismos de extensiones de E/F en C/F. Para cada $1 \leq i \leq r$ tomemos una extensión $\widetilde{\tau}_i \in \mathrm{Hom}(C/K, C/K)$ de τ_i. Claramente, $(\widetilde{\tau}_i \circ \sigma_j)_{\substack{1\leq i\leq r,\\ 1\leq j\leq s}}$ es una familia de morfismos distintos de E/K en C/K. Como $\gamma(E/K) = \gamma(E/F)\gamma(F/K) = rs$, estos son todos los morfismos de extensiones de E/K en C/K. Así, para cada $\alpha \in E$,

$$\mathrm{N}_K^F(\mathrm{N}_F^E(\alpha)) = \left(\prod_{i=1}^{r} \tau_i(\mathrm{N}_F^E(\alpha))\right)^{(F:K)_i} = \left(\prod_{i=1,j=1}^{r,s} \widetilde{\tau}_i(\sigma_j(\alpha))\right)^{(E:K)_i} = \mathrm{N}_K^E(\alpha).$$

De la misma manera se ve que $\mathrm{T}_K^E = \mathrm{T}_K^F \circ \mathrm{T}_F^E$. $\square$

Teorema 18.4. *Sea E/K una extensión finita y sea $\alpha \in E$. Si*

$$\mathrm{irr}(\alpha, K) = X^m + a_{m-1}X^{m-1} + \cdots + a_0,$$

entonces $\mathrm{T}_K^E(\alpha) = -(E : K(\alpha))a_{m-1}$ y $\mathrm{N}_K^E(\alpha) = ((-1)^m a_0)^{(E:K(\alpha))}$.

Demostración. Sea C una clausura algebraica de $K(\alpha)$ y sean $\sigma_1, \ldots, \sigma_n$ la familia de morfismos de extensiones de $K(\alpha)/K$ en C/K. El polinomio minimal de α sobre K se factoriza como

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 = \left(\prod_{i=1}^{n}(X - \sigma_i(\alpha))\right)^{(K(\alpha):K)_i} .$$

Así,

$$\mathrm{T}_K^{K(\alpha)}(\alpha) = (K(\alpha) : K)_i \sum_{i=1}^{n} \sigma_i(\alpha) = -a_{m-1}$$

y

$$\mathrm{N}_K^{K(\alpha)}(\alpha) = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^{(K(\alpha):K)_i} = (-1)^m a_0,$$

lo que por los Teoremas 18.2 y 18.3, implica que

$$\mathrm{T}_K^E(\alpha) = \mathrm{T}_K^{K(\alpha)}(\mathrm{T}_{K(\alpha)}^E(\alpha)) = (E : K(\alpha))\,\mathrm{T}_K^{K(\alpha)}(\alpha) = -(E : K(\alpha))a_{m-1}$$

y

$$\mathrm{N}_K^E(\alpha) = \mathrm{N}_K^{K(\alpha)}(\mathrm{N}_{K(\alpha)}^E(\alpha)) = \mathrm{N}_K^{K(\alpha)}(\alpha)^{(E:K(\alpha))} = ((-1)^m a_0)^{(E:K(\alpha))}. \quad \square$$

Proposición 18.5. *Sea E/K una extensión finita y sea $\alpha \in E$. La traza y la norma de α son iguales respectivamente a la traza y el determinante del endomorfismo K-lineal $\overline{\alpha}$ de E, definido por $\overline{\alpha}(x) = \alpha x$.*

Demostración. Sea $\operatorname{irr}(\alpha, K) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ y sea $\{v_1, \ldots, v_{(E:K(\alpha))}\}$ una base de E sobre $K(\alpha)$. entonces

$$\{v_1, \alpha v_1, \ldots, \alpha^{m-1}v_1, \ldots, v_{(E:K(\alpha))}, \alpha v_{(E:K(\alpha))}, \ldots, \alpha^{m-1}v_{(E:K(\alpha))}\}$$

es una base de E sobre K. La matriz de $\overline{\alpha}$ en esta base tiene la forma

$$\begin{pmatrix} A & 0 & \ldots & 0 \\ 0 & A & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A \end{pmatrix} \quad \text{donde} \quad A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{m-2} \\ 0 & 0 & \ldots & 1 & -a_{m-1} \end{pmatrix}.$$

En consecuencia, por el Teorema 18.4, $\mathrm{T}(\overline{\alpha}) = -(E : K(\alpha))a_{m-1} = \mathrm{T}_K^E(\alpha)$ y $\det(\overline{\alpha}) = ((-1)^m a_0)^{(E:K(\alpha))} = \mathrm{N}_K^E(\alpha)$. □

Definición 18.6. Sea E/K una extensión finita. Denotamos con $\langle\ ,\ \rangle \colon E \times E \to K$ a la forma bilineal definida por $\langle \alpha, \beta \rangle = \mathrm{T}_K^E(\alpha\beta)$.

Definición 18.7. Sea E/K una extensión separable de grado n. Definimos el discriminante $\Delta_{E/K} \colon E^n \to K$, por

$$\Delta_{E/K}(\alpha_1, \ldots, \alpha_n) = \det((\langle \alpha_i, \alpha_j \rangle)_{1 \le i,j \le n}).$$

Notación 18.8. *Sea E/K una extensión separable de grado n y $\sigma_1, \ldots, \sigma_n$ los morfismos de extensiones de E/K en C/K, donde C una clausura algebraica de E. Dados $\alpha_1, \ldots, \alpha_n \in E$, denotamos con $\mathrm{M}(\alpha_1, \ldots, \alpha_n)$ a la matriz*

$$\mathrm{M}(\alpha_1, \ldots, \alpha_n) = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Teorema 18.9. *Sea E/K una extensión separable de grado n. Entonces*

$$\Delta_{E/F}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{M}(\alpha_1, \ldots, \alpha_n))^2.$$

Demostración. Un cálculo directo muestra que

$$(\langle \alpha_i, \alpha_j \rangle)_{1 \le i,j \le n} = \mathrm{M}(\alpha_1, \ldots, \alpha_n)^{\mathrm{T}}\, \mathrm{M}(\alpha_1, \ldots, \alpha_n),$$

donde $\mathrm{M}(\alpha_1, \ldots, \alpha_n)^{\mathrm{T}}$ denota a la matriz transpuesta de $\mathrm{M}(\alpha_1, \ldots, \alpha_n)$. El resultado se deduce inmediatamente de este hecho. □

El siguiente corolario da un criterio para determinar cuando, en una extensión separable E/K de grado n, una familia de elementos $\alpha_1, \ldots, \alpha_n$ de E es una base de E sobre K. Una parte de este criterio ya había sido dada en el Teorema 16.4.

Corolario 18.10. *Sea E/K una extensión separable de grado n y $\alpha_1, \ldots, \alpha_n$ una familia de elementos de E. Son equivalentes:*

1) $\alpha_1, \ldots, \alpha_n$ *es una base de E sobre K,*

2) $\det(\mathrm{M}(\alpha_1, \ldots, \alpha_n)) \neq 0$,

3) $\Delta_{E/K}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Demostración. Es consecuencia inmediata de las Teoremas 16.4 y Teorema 18.9. □

Corolario 18.11. *Sea E/K una extensión finita. Son equivalentes:*

1) E/K es separable,

2) La forma bilineal $\langle\ ,\ \rangle\colon E \times E \to K$ es no degenerada,

3) La forma bilineal $\langle\ ,\ \rangle\colon E \times E \to K$ es no nula,

Demostración. 1) $\Rightarrow$ 2) Si E/K es separable, entonces por el Corolario 18.10, $\Delta_{E/K}(\alpha_1, \ldots, \alpha_n) \neq 0$, para toda base $\alpha_1, \ldots, \alpha_n$ de E sobre K, lo que claramente implica que $\langle\ ,\ \rangle$ es no degenerada.

2) $\Rightarrow$ 3) Es trivial.

3) $\Rightarrow$ 1) Por el item 1) del Teorema 18.2, si E/K no es separable, entonces la forma bilineal $\langle\ ,\ \rangle\colon E \times E \to K$ es nula. □

Supongamos que E/K es una extensión separable de grado n y sean $B = \{\alpha_1, \ldots, \alpha_n\}$ y $B' = \{\alpha'_1, \ldots, \alpha'_n\}$ dos bases de E sobre K. Denotemos con (c_{ij}) a la matriz de cambio de base de B' en B. Así, (c_{ij}) está definida por las ecuaciones $\alpha'_u = \sum_i c_{iu}\alpha_i$. La igualdades $\langle \alpha'_u, \alpha'_v\rangle = \sum_{i,j} c_{iu}c_{jv}\langle \alpha_i, \alpha_j\rangle$ muestran que $(c_{iu})^{\mathrm{T}}(\langle \alpha_i, \alpha_j\rangle)(c_{jv}) = (\langle \alpha'_u, \alpha'_v\rangle)$. Así,

$$\Delta_{E/K}(\alpha'_1, \ldots, \alpha'_n) = \Delta_{E/K}(\alpha_1, \ldots, \alpha_n)\det(c_{ij})^2,$$

de modo de que el hecho de que $\Delta_{E/K}(\alpha_1, \ldots, \alpha_n)$ sea un cuadrado en K^* no depende de la base $\{\alpha_1, \ldots, \alpha_n\}$ elegida. Es claro, por el Teorema 18.9, que esto ocurre si y sólo si $\mathrm{M}(\alpha_1, \ldots, \alpha_n) \in K$. Ahora, por el Corolario 12.5, existe $\alpha \in E$ tal que $E = K(\alpha)$. Sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ las raíces de $\mathrm{irr}(\alpha, K)$ en una clausura algebraica de E. Consideremos la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de E sobre K. Es claro que

$$\det(\mathrm{M}(1, \alpha, \ldots, \alpha^{n-1})) = \det\begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i<j}(\alpha_i - \alpha_j).$$

Llamemos δ a $\prod_{i<j}(\alpha_i - \alpha_j)$ y Δ a $\Delta_{E/K}(1, \alpha, \ldots, \alpha^{n-1})$. Entonces $\Delta = \delta^2$ y tenemos el siguiente teorema.

Teorema 18.12. *Supongamos que E/K es galoisiana. Se satisfacen:*

1) Si $\mathrm{char}(K) \neq 2$, *entonces*

  a) Si Δ es un cuadrado en K, entonces $\mathrm{G}(E/K)$ es un subgrupo del grupo $\mathfrak{A}_n$ de permutaciones pares de $\{\alpha_1, \ldots, \alpha_n\}$.

b) Si Δ no es un cuadrado en K, entonces $\mathrm{G}(E/K)$ es un subgrupo del grupo $\mathfrak{S}_n$ de permutaciones de $\{\alpha_1, \ldots, \alpha_n\}$, que contiene la misma cantidad de permutaciones pares que impares. Además $E^{\mathrm{G}(E/K)\cap\mathfrak{A}_n} = K(\delta)$.

2) Si $\mathrm{char}(K) = 2$, entonces Δ es un cuadrado en K, pero $\mathrm{G}(E/K)$ no es necesariamente un subgrupo del grupo $\mathfrak{A}_n$ de permutaciones pares de $\{\alpha_1, \ldots, \alpha_n\}$.

Demostración. Es claro que $\sigma(\delta) = \mathrm{sg}(\sigma)\delta$, para todo $\sigma \in \mathrm{G}(E/K)$. Así, $\delta \in K = E^{\mathrm{G}(E/K)}$ si y sólo si $\mathrm{char}(K) = 2$ o $\mathrm{char}(K) \neq 2$ pero $\mathrm{G}(E/K) \subseteq \mathfrak{A}_n$. Supongamos que $\mathrm{G}(E/K)$ contiene alguna permutación impar τ. Entonces la aplicación $\sigma \mapsto \tau\circ\sigma$ define una biyección del subconjunto de las permutaciones pares de $\mathrm{G}(E/K)$ en el de las impares. Además, es claro que $K(\delta) \subseteq E^{\mathrm{G}(E/K)\cap\mathfrak{A}_n}$ y, como

$$(E^{\mathrm{G}(E/K)\cap\mathfrak{A}_n} : K) = (\mathrm{G}(E/K) : \mathrm{G}(E/K) \cap \mathfrak{A}_n) = 2,$$

si $\mathrm{char}(K) \neq 2$, entonces $K(\delta) = E^{\mathrm{G}(E/K)\cap\mathfrak{A}_n}$. Por último, considerando el Ejemplo 13.20, vemos que $\mathrm{G}(E/K)$ no siempre está incluído en $\mathfrak{A}_n$, ni siquiera cuando la característica de K es 2. □

Lo que acabamos de ver puede ser generalizado de la siguiente manera: Sea $P \in K[X]$ un polinomio mónico y separable. Denotemos con $\alpha_1, \ldots, \alpha_n$ a las raíces de P en alguna clausura algebraica de K y sea $E = K(\alpha_1, \ldots, \alpha_n)$ el cuerpo de descomposición de P. Entonces $\mathrm{G}(E/K)$ es un subgrupo del grupo $\mathfrak{S}_n$ de permutaciones de las raíces de P. El discriminante de P es por definición $\Delta_P = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Es claro que Δ_P es dejado fijo por todos los elementos de $\mathfrak{S}_n$ y así pertenece a K. Es fácil ver que el Teorema 18.12 se extiende a este contexto, con la misma demostración. Además

$$\Delta_P = \det(\mathrm{M}(1, \alpha_1, \ldots, \alpha_1^{n-1})^T)\,\mathrm{M}(1, \alpha_1, \ldots, \alpha_1^{n-1}) = \det\begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{pmatrix},$$

donde los p_i's son los polinomios de Newton evaluados en $\alpha_1, \ldots, \alpha_n$. Dado que estos polinomios se pueden calcular recursivamente en función de los polinomios simétricos elementales, obtenemos así una manera de calcular el discriminante de P en función de sus coeficientes. En la siguiente sección damos otra manera de calcular el discriminante.

19. La resultante y el discriminante

Sean n y m enteros positivos, $v_0, \ldots, v_n, w_0, \ldots, w_m, X$ indeterminadas sobre $\mathbb{Z}$ y $F(X)$ y $G(X)$ los polinomios

$$F(X) = v_0X^n + \cdots + v_n \qquad \text{y} \qquad G(X) = w_0X^m + \cdots + w_m.$$

La resultante $\mathrm{R}(F, G)$ de F y G es el determinante de la matriz de $n + m$ filas por $n + m$ columnas

$$(*) \qquad \begin{pmatrix} v_0 & v_1 & \ldots & v_n & 0 & \ldots\ldots & 0 \\ 0 & v_0 & v_1 & \ldots & v_n & 0 & \ldots & 0 \\ \ldots\ldots & & & & & & & \\ 0 & \ldots\ldots & 0 & v_0 & v_1 & \ldots & v_n \\ w_0 & w_1 & \ldots & w_m & 0 & \ldots\ldots & 0 \\ 0 & w_0 & w_1 & \ldots & w_m & 0 & \ldots & 0 \\ \ldots\ldots & & & & & & & \\ 0 & \ldots\ldots & 0 & w_0 & w_1 & \ldots & w_m \end{pmatrix}$$

Observese que $\mathrm{R}(F,G) \in \mathbb{Z}[v,w]$ es homogeneo de grado m en las v's y de grado n en las w's. Además $\mathrm{R}(F,G)$ contiene al monomio $v_0^m w_m^n$ con coeficiente 1. Llamemos $C_0,\dots,C_{n+m}$ a las columnas de $(*)$ y escribamos $C = X^{n+m-1}C_0 + \cdots + 1\cdot C_{n+m}$. Entonces se tiene

$$\mathrm{R}(F,G) = \det(C_0,\dots,C_{n+m}) = \det(C_0,\dots,C_{n+m-1},C).$$

Desarrollando por la última columna se ve que existen $\varphi,\psi \in \mathbb{Z}[v,w,X]$, de grados $m-1$ y $n-1$ en X respectivamente, tales que

$$\mathrm{R}(F,G) = \varphi F + \psi G.$$

Sea A un anillo conmutativo. La resultante $R(f,g)$ de dos polinomios

$$f(X) = a_0X^n + \cdots + a_n \qquad \text{y} \qquad g(X) = b_0X^m + \cdots + b_m$$

de grados n y m respectivamente, con coeficientes en A, es el elemento

$$\mathrm{R}(f,g) = \mathrm{R}(F,G)(a_0,\dots,a_n,b_0,\dots,b_m)$$

de A. Por lo dicho antes existen $\varphi,\psi \in A[X]$, de grados $m-1$ y $n-1$ respectivamente, tales que

$$\mathrm{R}(f,g) = \varphi f + \psi g.$$

En consecuencia si f y g tienen alguna raíz común en algún anillo que contiene a A, entonces $\mathrm{R}(f,g) = 0$. Para ver bajo que condiciones vale la recíproca de este resultado, conviene dar primero algunas expresiones importantes para la resultante.

Nota. Supongamos que $a_0 \neq 0$ y que $b_0 = \cdots = b_{i-1} = 0$ pero $b_i \neq 0$ para algún $0 \leq i \leq m$. Entonces se deduce facilmente de la definición de la resultante que

$$\mathrm{R}(F,G)(a_0,\dots,a_n,b_0,\dots,b_m) = a_0^i\,\mathrm{R}(f,g).$$

Análogamente, si $b_0 \neq 0$ y $a_0 = \cdots = a_{i-1} = 0$ pero $a_i \neq 0$ para algún $0 \leq i \leq n$, entonces

$$\mathrm{R}(F,G)(a_0,\dots,a_n,b_0,\dots,b_m) = (-1)^{mi}b_0^i\,\mathrm{R}(f,g).$$

Finalmente si $a_0 = b_0 = 0$, entonces

$$\mathrm{R}(F,G)(a_0,\dots,a_n,b_0,\dots,b_m) = 0.$$

Teorema 19.1. *Sean $v_0,t_1,\dots,t_n,w_0,u_1,\dots,u_m,X$ indeterminadas. Consideremos los polinomios*

$$\begin{aligned} F(X) &= v_0(X-t_1)\dots(X-t_n) = v_0X^n + \cdots + v_n,\\ G(X) &= w_0(X-u_1)\dots(X-u_m) = w_0X^m + \cdots + w_m, \end{aligned}$$

donde $v_i = (-1)^i v_0 s_i(t_1,\dots,t_n)$ y $w_j = (-1)^j w_0 s_j(u_1,\dots,u_m)$. Entonces

$$\mathrm{R}(F,G) = v_0^m w_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(t_i-u_j) = v_0^m \prod_{i=1}^{n} G(t_i) = (-1)^{nm} w_0^n \prod_{j=1}^{m} F(u_j).$$

Demostración. Escribamos

$$S = v_0^m w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j).$$

Dado que $\mathrm{R}(F, G)$ es un polinomio en las v's y en las w's,

$$\mathrm{R}(F, G) = T(v_0, w_0, t_1, \ldots, t_n, u_1, \ldots, u_m),$$

donde T es un polinomio con coeficientes enteros. Veamos que S divide a $\mathrm{R}(F, G)$. Como $\mathbb{Z}[v_0, w_0, t_1, \ldots, t_n, u_1, \ldots, u_m]$ es factorial y los polinomios $v_0^m w_0^n$ y $t_i - u_j$'s son coprimos dos a dos es suficiente ver que $v_0^m w_0^n \mid \mathrm{R}(F, G)$ y que cada $t_i - u_j \mid \mathrm{R}(F, G)$. Lo primero se deduce inmediatamente de que $\mathrm{R}(F, G)$ es un polinomio homogeneo de grado m en los v's y de grado n en los w's y de que $v_0 \mid v_i$ para todo i y $w_0 \mid w_j$ para todo j. Para lo segundo consideremos a $\mathrm{R}(F, G)$ como un polinomio en t_i con coeficientes en $\mathbb{Z}[v_0, w_0, t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n, u_1, \ldots, u_m]$ y lo dividimos por $t_i - u_j$, lo que nos da una expresión de la forma

$$\mathrm{R}(F, G) = (t_i - u_j)Q(F, G) + R'(F, G),$$

con $R'(F, G) \in \mathbb{Z}[v_0, w_0, t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n, u_1, \ldots, u_m]$. Dado que la resultante de dos polinomios que tienen una raíz en común es nula, evaluando en la expresión de arriba t_i en u_j, obtenemos que $R'(F, G) = 0$ y así $t_i - u_j \mid \mathrm{R}(F, G)$. Escribamos $\mathrm{R}(F, G) = cS$. Un cálculo directo muestra ahora que

$$S = v_0^m \prod_{i=1}^{n} G(t_i) = (-1)^{nm} w_0^n \prod_{j=1}^{m} F(u_j),$$

de donde

$$S \in \mathbb{Z}[v_0, \ldots, v_n, w_0, u_1, \ldots, u_m] \cap \mathbb{Z}[v_0, t_1, \ldots, t_n, w_0, \ldots, w_m]$$

y es homogeneo de grado n en las w's y de grado m en las v's. En consecuencia

$$c \in \mathbb{Z}[v_0, \ldots, v_n, w_0, u_1, \ldots, u_m] \cap \mathbb{Z}[v_0, t_1, \ldots, t_n, w_0, \ldots, w_m]$$

y es homogeneo de grado 0 en las v's y en las w's, de donde

$$c \in \mathbb{Z}[w_0, u_1, \ldots, u_m] \cap \mathbb{Z}[v_0, t_1, \ldots, t_n] = \mathbb{Z}.$$

Para terminar la demostración debemos ver que $c = 1$. Puesto que en $\mathrm{R}(F, G)$ el monomio $v_0^m w_m^n$ aparece con coeficiente 1, debemos ver que lo mismo ocurre con S, lo que se sigue de que $S = v_0^m \prod_{i=1}^{n} G(t_i)$. □

Corolario 19.2. *Sean $f(X) = a_0 X^n + \cdots + a_n$ y $g(X) = b_0 X^m + \cdots + b_m$ dos polinomios de grados n y m respectivamente, con coeficientes en un cuerpo K. Entonces $\mathrm{R}(f, g) = 0$ si y sólo si f y g tienen una raíz común en alguna clausura algebraica de K.*

Demostración. Por el teorema anterior

$$\mathrm{R}(f, g) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j),$$

donde los α_i's son las raíces de f y los β_j's las de g. Así, si $\mathrm{R}(f,g)=0$ debe ser $\alpha_i=\beta_j$ para algún par (i,j). La otra implicación ya la hemos probado. $\square$

Veamos ahora la relación con el discriminante. Sean $v_0,t_1,\dots,t_n,X$ indeterminadas sobre $\mathbb{Z}$ y sea $F(X)$ el polinomio

$$F(X)=v_0(X-t_1)\dots(X-t_n)=v_0X^n+\cdots+v_n,$$

donde $v_i=(-1)^i v_0 s_i(t_1,\dots,t_n)$. El discriminante D_F de F es por definición

$$D_F=v_0^{2n-2}\prod_{i<j}(t_i-t_j)^2.$$

Teorema 19.3. *Sea $F(X)$ como arriba y denotemos con $F'(X)$ a la derivada*

$$F'(X)=nv_0X^{n-1}+(n-1)v_1X^{n-2}+\cdots+v_{n-1}$$

de $F(X)$. Consideremos a $\mathrm{R}(F,F')$ como un polinomio en $v_0,\dots,v_n$. Entonces

$$\mathrm{R}(F,F')=v_0^{n-1}\prod_{i=1}^{n}F'(t_i)=(-1)^{\frac{n(n-1)}{2}}v_0D_F.$$

Demostración. Por la regla de derivación de un producto

$$F'(X)=\sum_{i=1}^{n}v_0(X-t_1)\dots(X-t_{i-1})(X-t_{i+1})\dots(X-t_n),$$

de donde $F'(t_i)=v_0(t_i-t_1)\dots(t_i-t_{i-1})(t_i-t_{i+1})\dots(t_i-t_n)$ para cada $1\le i\le n$. En consecuencia, por la fórmula $\mathrm{R}(F,G)=v_0^m\prod_{i=1}^n G(t_i)$ aplicada a $G=F'$ se obtiene que

$$\mathrm{R}(F,F')=v_0^{n-1}\prod_{i=1}^{n}F'(t_i)=v_0^{2n-1}\prod_{i\neq j}(t_i-t_j)=(-1)^{\frac{n(n-1)}{2}}v_0D_F.\quad\square$$

Sea ahora $f(X)$ un polinomio de grado n con coeficientes en un cuerpo K. Escribamos

$$f(X)=a_0(X-\alpha_1)\dots(X-\alpha_n)=a_0X^n+\cdots+a_n,$$

donde $\alpha_1,\dots,\alpha_n$ son las raíces de f en una clausura algebraica C de K y $a_i=(-1)^i a_0 s_i(\alpha_1,\dots,\alpha_n)$. El discriminante Δ_f de f es por definición

$$\Delta_f=a_0^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

Teorema 19.4. *Sea $f(X)$ como arriba. Entonces,*

$$\Delta_f=(-1)^{\frac{n(n-1)}{2}}a_0^{n-2}\prod_{i=1}^{n}f'(\alpha_i)=(-1)^{\frac{n(n-1)}{2}}a_0^{n-2-\mathrm{gr}(f')}\,\mathrm{R}(f,f').$$

Demostración. Las primera fórmula se sigue inmediatamente del Teorema 19.3 y la segunda del Teorema 19.3 y de la nota que precede al Teorema 19.1. $\square$

Teorema 19.5. *Sea $f(X)$ como arriba. Si $f(X)$ es irreducible y separable, entonces*

$$\Delta_f=(-1)^{\frac{n(n-1)}{2}}a_0^{n-2}\,\mathrm{N}_K^{K(\alpha_1)}(f'(\alpha_1)).$$

Demostración. Se sigue inmediatamente de la primera fórmula del Teorema 19.4, de la definición de la norma, de para cada i entre 1 y n hay un único morfismo de $K(\alpha_1)/K$ en C/K que envía α_1 en α_i y de que estos son todos los morfismos de $K(\alpha_1)/K$ en C/K. $\square$

20. Extensiones cíclicas

En esta sección estudiamos las extensiones cíclicas E/K de orden n bajo la hipótesis de que en K hay una raíz n-ésima primitiva de la unidad. Observese que esto implica en particular que la característica de K no divide a n. También consideramos las extensiones cíclicas E/K de orden $p = \mathrm{char}(K)$. En este estudio usaremos el siguiente resultado:

Teorema 20.1 (90 de Hilbert). *Sea E/K una extensión cíclica, σ un generador de $\mathrm{G}(E/K)$ y β un elemento de E. Se satisfacen:*

1) $\mathrm{N}_K^E(\beta) = 1$ *si y sólo si existe* $\alpha \neq 0$ *en* E *tal que* $\beta = \alpha/\sigma(\alpha)$.

2) $\mathrm{T}_K^E(\beta) = 0$ *si y sólo si existe* $\alpha \in E$ *tal que* $\beta = \alpha - \sigma(\alpha)$.

Demostración. 1) Es claro que si existe $\alpha \neq 0$ en E tal que $\beta = \alpha/\sigma(\alpha)$, entonces $\mathrm{N}_K^E(\beta) = 1$. Denotemos con n al grado de $(E : K)$ y supongamos que $\prod_{h=0}^{n-1} \sigma^h(\beta) = \mathrm{N}_K^E(\beta) = 1$. Esto implica que la función

$$\tau = \mathrm{id} + \sum_{j=1}^{n-1} \left(\prod_{h=0}^{j-1} \sigma^h(\beta) \right) \sigma^j$$

satisface la igualdad $\beta(\sigma \circ \tau) = \tau$. Por el Corolario 16.3 existe $\theta \in E$ tal que $\alpha = \tau(\theta) \neq 0$. El resultado se sigue ahora inmediatamente de que $\beta\sigma(\alpha) = \beta\sigma(\tau(\theta)) = \tau(\theta) = \alpha$.

2) Es claro que si existe $\alpha \neq 0$ en E tal que $\beta = \alpha - \sigma(\alpha)$, entonces $\mathrm{T}_K^E(\beta) = 0$. Supongamos ahora que $\mathrm{T}_K^E(\beta) = 0$. Por el item 1) del Teorema 18.2 existe $\theta \in E$ tal que $\mathrm{T}_K^E(\theta) \neq 0$. Dividiendo θ por $\mathrm{T}_K^E(\theta)$, podemos suponer que $\mathrm{T}_K^E(\theta) = 1$. Sea

$$\alpha = \sum_{j=1}^{n-1} \left(\sum_{h=0}^{j-1} \sigma^h(\beta) \right) \sigma^j(\theta),$$

donde $n = (E : K)$. Entonces

$$\begin{aligned} \beta + \sigma(\alpha) &= \beta \sum_{j=0}^{n-1} \sigma^j(\theta) + \sum_{j=2}^{n} \left(\sum_{h=1}^{j-1} \sigma^h(\beta) \right) \sigma^j(\theta) \\ &= \beta\sigma^0(\theta) + \beta\sigma^1(\theta) + \sum_{j=2}^{n-1} \left(\sum_{h=0}^{j-1} \sigma^h(\beta) \right) \sigma^j(\theta) + \left(\sum_{h=1}^{n-1} \sigma^h(\beta) \right) \sigma^n(\theta) \\ &= \sum_{j=1}^{n-1} \left(\sum_{h=0}^{j-1} \sigma^h(\beta) \right) \sigma^j(\theta) + \left(\sum_{h=0}^{n-1} \sigma^h(\beta) \right) \theta = \alpha, \end{aligned}$$

de donde $\beta = \alpha - \sigma(\alpha)$. □

Corolario 20.2. *Sea E/K una extensión cíclica y σ un generador de $\mathrm{G}(E/K)$. Las sucesiones de grupos abelianos*

$$1 \longrightarrow K^* \xrightarrow{\ i\ } E^* \xrightarrow{\ \varphi\ } E^* \xrightarrow{\ \mathrm{N}_K^E\ } K^*$$

y

$$0 \longrightarrow K \xrightarrow{j} E \xrightarrow{\phi} E \xrightarrow{\mathrm{T}_K^E} K \longrightarrow 0,$$

donde i y j son las inclusiones canónicas y φ y ϕ están definidas por $\varphi(x) = x/\sigma(x)$ y $\phi(x) = x - \sigma(x)$, son exactas.

Proposición 20.3. *Sea E/K una extensión finita. Si K es un cuerpo finito, entonces la norma $N_K^E \colon E^* \to K^*$ es sobreyectiva.*

Demostración. Por la Proposición 15.4, la extensión E/K es cíclica y así, por el corolario anterior, hay una la sucesión exacta

$$1 \longrightarrow K^* \xrightarrow{i} E^* \xrightarrow{\varphi} E^* \xrightarrow{\mathrm{N}_K^E} K^*.$$

En consecuencia, $\#(\mathrm{Im}(\mathrm{N}_K^E)) = \#(E^*)/\#(\mathrm{Im}(\varphi))$ y $\#(\mathrm{Im}(\varphi)) = \#(E^*)/\#(K^*)$, lo que implica que $\#(\mathrm{Im}(\mathrm{N}_K^E)) = \#(K^*)$. $\square$

Proposición 20.4. *Sea K un cuerpo y $n \in \mathbb{N}$. Supongamos que en K hay una raíz n-ésima primitiva de la unidad w. Se satisfacen:*

1) *Si E/K es una extensión cíclica de grado n, entonces existe $\alpha \in E$ tal que $E = K(\alpha)$ y α es raíz de un polinomio irreducible de $K[X]$ de la forma $X^n - a$.*
2) *Si α es una raíz de un polinomio de $K[X]$ de la forma $X^n - a$, entonces $K(\alpha)/K$ es una extensión cíclica de grado d con d un divisor de n e $\mathrm{irr}(\alpha : K) = X^d - b$, donde $b = \alpha^d$.*

Demostración. 1) Sea σ un generador de $\mathrm{G}(E/K)$. Como $w \in K$ la norma de w^{-1} satisface $\mathrm{N}_K^E(w^{-1}) = (w^{-1})^n = 1$, de donde, por el item 1) del Teorema 20.1, existe $\alpha \in E$ tal que $\sigma(\alpha) = \alpha w$. En consecuencia, $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n w^n = \alpha^n$, lo que implica que $a = \alpha^n \in K$ y así, $\mathrm{irr}(\alpha, K) \mid X^n - a$. Como además todos los conjugados $\sigma^i(\alpha) = \alpha w^i$ de α son distintos, $\mathrm{gr}(\mathrm{irr}(\alpha, K)) = (K(\alpha) : K) \geq \gamma(K(\alpha)/K) = n$, de donde $K(\alpha) = E$ e $\mathrm{irr}(\alpha, K) = X^n - a$.

2) El caso $a = 0$ es trivial. Supongamos entonces que $a \neq 0$. Como w tiene orden n, la característica de K no divide a n. Así $X^n - a$ y, por lo tanto también $K(\alpha)/K$, es separable. Como además todas la raíces αw^i de $X^n - a$ están en $K(\alpha)$, la extensión $K(\alpha)/K$, es de Galois. Sea σ un automorfismo de $K(\alpha)/K$. Dado que $\sigma(\alpha)$ es una raíz de $X^n - a$, existe $0 \leq i(\sigma) < n$ tal que $\sigma(\alpha) = \alpha w^{i(\sigma)}$. Queda definido así un morfismo inyectivo $\theta \colon \mathrm{G}(K(\alpha)/K) \to \mathbb{Z}_n$ por $\theta(\sigma) = i(\sigma)$. En consecuencia $\mathrm{G}(K(\alpha)/K)$ es cíclico de orden d con d un divisor de n. Sea σ un generador de $\mathrm{G}(K(\alpha)/K)$. Como $\alpha = \mathrm{id}(\alpha) = \sigma^d(\alpha) = \alpha w^{i(\sigma)d}$, tenemos que $w^{i(\sigma)d} = 1$, lo que implica que $\sigma(\alpha^d) = \sigma(\alpha)^d = (\alpha w^{i(\sigma)})^d = \alpha^d$. Esto muestra que $b = \alpha^d \in K$, de donde $\mathrm{irr}(\alpha, K) \mid X^d - b$. Así, como $\mathrm{gr}(\mathrm{irr}(\alpha, K)) = (K(\alpha) : K) = d$, el polinomio minimal $\mathrm{irr}(\alpha, K)$ de α sobre K es $X^d - b$. $\square$

Proposición 20.5 (Artín-Schreier). *Sea K un cuerpo de característica $p > 0$. Se satisfacen:*

1) *Si E/K es una extensión cíclica de grado p, entonces existe $\alpha \in E$ tal que $E = K(\alpha)$ y α es raíz de un polinomio irreducible de $K[X]$ de la forma $X^p - X - a$.*

2) Sea $P = X^p - X - a \in K[X]$. Si P tiene una raíz en K, entonces todas sus raíces están en K y si P no tiene ninguna raíz en K, entonces P es irreducible en $K[X]$. Además, en este caso, si α es una raíz de P, entonces $K(\alpha)/K$ es cíclica de grado p.

Demostración. 1) Sea σ un generador de $\mathrm{G}(E/K)$. Como $\mathrm{T}_K^E(-1) = p.(-1) = 0$, por el item 2) del Teorema 20.1, existe $\alpha \in E$ tal que $\sigma(\alpha) = \alpha+1$. En consecuencia todos los conjugados $\sigma^i(\alpha) = \alpha + i$ de α son distintos y así, $(K(\alpha) : K) \geq p$, lo que muestra que $E = K(\alpha)$. Como $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, el elemento $a = \alpha^p - \alpha$ pertenece a K. Así, $\mathrm{irr}(\alpha, K) \mid X^p - X - a$ y, como $\mathrm{gr}(\mathrm{irr}(\alpha, K)) = (K(\alpha) : K) = p$, el polinomio minimal de α sobre K es $X^p - X - a$.

2) Es claro que si α es raíz de P también $\alpha + i$ con $1 \leq i < p$ es raíz de P. Así P tiene p raíces distintas y si una de ellas está en K todas las demás también lo están. Supongamos que ninguna raíz de P está en K. Veamos que P es irreducible. Sea Q un factor irreducible mónico de P. Las raíces de Q tienen la forma $\alpha+i_1, \ldots, \alpha+i_d$, donde $d = \mathrm{gr}(Q)$ y $0 \leq i_1 < \cdots < i_d < p$. Como la suma $d\alpha + \sum_j i_j$ pertenece a K y $\alpha \notin K$ tenemos que $d = p$, lo que muestra que $Q = P$. Dado que todas las raíces de $\mathrm{irr}(X, \alpha) = P$ están en $K(\alpha)$ tenemos que $K(\alpha)$ es el cuerpo de descomposición de P. Así, como este polinomio es separable, $K(\alpha)/K$ es una extensión de Galois de grado p. Es claro que $\mathrm{G}(K(\alpha)/K)$ es cíclico, ya que su orden es primo. Un generador de $\mathrm{G}(K(\alpha)/K)$ es por ejemplo el automorfismo $\sigma \in \mathrm{G}(K(\alpha)/K)$ que envía α en $\alpha + 1$. □

21. Teorema de Jordan-Hölder y grupos resolubles

Lema 21.1 (de la mariposa). *Sean G un grupo y $H_1 \subseteq H_2$ y $L_1 \subseteq L_2$ subgrupos de G. Si H_1 es un subgrupo normal de H_2 y L_1 es un subgrupo normal de L_2, entonces $H_1(L_1 \cap H_2)$ es un subgrupo normal de $H_1(L_2 \cap H_2)$, $H_2(L_2 \cap H_1)$ es un subgrupo normal de $H_2(L_2 \cap H_2)$ y existe un isomorfismo*

$$\frac{H_1(L_2 \cap H_2)}{H_1(L_1 \cap H_2)} \simeq \frac{L_1(L_2 \cap H_2)}{L_1(L_2 \cap H_1)}.$$

Demostración. Sean $K = H_1(L_1 \cap H_2)$ y $L = L_2 \cap H_2$. Como $L_1 \cap H_2$ está incluído en el normalizador de H_1 el conjunto K es un subgrupo de G. Como ahora L está incluído en el normalizador de K, el conjunto KL es un subgrupo de G y K es un subgrupo normal de KL. Así, por el teorema de Noether, $L \cap K$ es un subgrupo normal de L y $L/(L \cap K) \simeq KL/K$. Reemplazando K y L por sus definiciones obtenemos

$$\frac{H_1(L_2 \cap H_2)}{H_1(L_1 \cap H_2)} \simeq \frac{L_2 \cap H_2}{(L_2 \cap H_1)(L_1 \cap H_2)}.$$

La demostración sale ahora por simetría. □

Definición 21.2. Sea G un grupo. Dos cadenas $H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_m$ y $L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n$ de subgrupos de G tales que H_{i-1} es un subgrupo normal de H_i para todo $1 \leq i \leq m$ y L_{j-1} es un subgrupo normal de L_j para todo $1 \leq j \leq n$ son equivalentes si $m = n$ y existe una permutación σ de $\{1, \ldots, m\}$ tal que $\frac{H_i}{H_{i-1}} \simeq \frac{L_{\sigma(i)}}{L_{\sigma(i)-1}}$, para todo i entre 1 y m.

Teorema 21.3 (de Schreier). *Sea G un grupo. Dos cadenas finitas $H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_m = G$ y $L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n = G$ de subgrupos de G tales que H_{i-1} es un subgrupo normal de H_i para todo $1 \leq i \leq m$ y L_{j-1} es un subgrupo normal de L_j para todo $1 \leq j \leq n$, se pueden extender a cadenas equivalentes.*

Demostración. Sin pérdida de generalidad podemos suponer que $H_0 = L_0 = \{1\}$. Dados $0 \leq i \leq n$ y $1 \leq j \leq m$ escribamos $H_{ij} = H_{j-1}(L_i \cap H_j)$ y dados $1 \leq i \leq n$ y $0 \leq j \leq m$ escribamos y $L_{ij} = L_{i-1}(L_i \cap H_j)$. Quedan formadas cadenas

$$H_0 = H_{01} \subseteq H_{11} \subseteq \ldots \subseteq H_{n1} = H_1 = H_{02} \subseteq \ldots \subseteq H_{nm} = H_m$$

y

$$L_0 = L_{10} \subseteq L_{11} \subseteq \ldots \subseteq L_{1m} = L_1 = L_{20} \subseteq \ldots \subseteq L_{nm} = L_n,$$

donde no necesariamente las inclusiones son propias. Por el Lema 21.1, $H_{i-1,j}$ es un subgrupo normal de H_{ij} para todo $1 \leq i \leq n$ y todo $1 \leq j \leq m$, $L_{i,j-1}$ es un subgrupo normal de L_{ij} para todo $1 \leq i \leq n$ y todo $1 \leq j \leq m$ y hay isomorfismos $\frac{H_{ij}}{H_{i-1,j}} \simeq \frac{L_{ij}}{L_{i,j-1}}$ para todo $1 \leq i \leq n$ y $1 \leq j \leq m$. La demostración se termina fácilmente usando este hecho. $\square$

Definición 21.4. Sea G un grupo. Una serie de descomposición de longitud n de G es una cadena $\{1\} = G_0 \subsetneq \cdots \subsetneq G_n = G$ de subgrupos de G, tal que G_{i-1} es un subgrupo normal de G_i y $\frac{G_i}{G_{i-1}}$ es simple, para todo $1 \leq i \leq n$.

Teorema 21.5 (de Jordan-Hölder). *Si un grupo G tiene una serie de descomposición, entonces cada cadena $\{1\} = G_0 \subsetneq \cdots \subsetneq G_n = G$ de subgrupos de G tal que G_{i-1} es un subgrupo normal de G_i para todo $1 \leq i \leq n$, se puede refinar a una serie de descomposición. Además todas las series de descomposición de G son equivalentes y por lo tanto tienen la misma longitud.*

Demostración. Se sigue inmediatamente del Teorema 21.3. $\square$

Definición 21.6. Sea G un grupo. La longitud $l(G)$ de G es

$$l(G) = \begin{cases} n & \text{si } G \text{ tiene una serie de descomposición de longitud } n, \\ \infty & \text{en otro caso.} \end{cases}$$

Notese que $l(\{1\}) = 0$.

Teorema 21.7. *Sean G un grupo y H un subgrupo normal de G. Entonces G tiene una serie de descomposición si y sólo si H y G/H la tienen. Además $l(G) = l(H) + l(G/H)$.*

Demostración. Se sigue facilmente del Teorema 21.5. $\square$

Teorema 21.8 (de la dimensión). *Sean G un grupo y H y L subgrupos normales de G. Entonces $l(H)$ y $l(L)$ son finitos, si y sólo si $l(HL)$ y $l(H \cap L)$ lo son. Además $l(HL) + l(H \cap L) = l(H) + l(L)$.*

Demostración. Se lo deduce facilmente aplicando el Teorema 21.7 a las sucesiones exactas

$$1 \longrightarrow H \cap L \longrightarrow H \longrightarrow \frac{H}{H \cap L} \longrightarrow 1$$

y

$$1 \longrightarrow L \longrightarrow HL \longrightarrow \frac{HL}{L} \longrightarrow 1,$$

y usando el hecho de que $\frac{H}{H\cap L} \simeq \frac{HL}{L}$. $\square$

Definición 21.9. Un grupo G es resoluble si tiene una serie de descomposición

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = G$$

con los cocientes G_{i+1}/G_i abelianos.

Proposición 21.10. *Todo subgrupo de un grupo resoluble es resoluble.*

Demostración. Sea $\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = G$ una serie de descomposición de G y H un subgrupo de G. Tomemos $1 \leq i \leq n$. Como G_{i-1} es un subgrupo invariante de G_i, el subgrupo $H \cap G_{i-1}$ de $H \cap G_i$ es invariante y $\frac{H\cap G_i}{H\cap G_{i-1}} \subseteq \frac{G_i}{G_{i-1}}$. Así, $\frac{H\cap G_i}{H\cap G_{i-1}}$ es abeliano. La proposición se deduce immediatamente de esto. $\square$

Proposición 21.11. *Sea G un grupo y H un subgrupo normal de G. Son equivalentes:*

1) G es resoluble.

2) H y G/H son resolubles.

Demostración. Se sigue facilmente del Teorema 21.5. $\square$

Lema 21.12. *Si $n \geq 5$ y G y H son subgrupos de $\mathfrak{S}_n$ tales que H es un subgrupo normal de G, G/H es abeliano y G contiene a todos los tresciclos, entonces H contiene a todos los tresciclos.*

Demostración. Sean $\alpha = (ijk)$ y $\beta = (krs)$ dos tresciclos. Dado que G/H es abeliano $\alpha^{-1}\beta^{-1}\alpha\beta \in H$. Así, como $\alpha^{-1}\beta^{-1}\alpha\beta = (kji)(srk)(ijk)(krs) = (kjs)$, el grupo H contiene a todos los tresciclos. $\square$

Proposición 21.13. *Si $n \geq 5$, entonces ni $\mathfrak{S}_n$ ni $\mathfrak{A}_n$ son resolubles.*

Demostración. Es consecuencia inmediata del Lema 21.12. $\square$

22. Extensiones resolubles por radicales

Observación 22.1. *Sea E/K una extensión finita y separable y E' la clausura normal de E/K. Son equivalentes:*

1) $\mathrm{G}(E'/K)$ es resoluble.

2) Existe una extensión de Galois E''/K con $E \subseteq E''$ tal que $\mathrm{G}(E''/K)$ es resoluble.

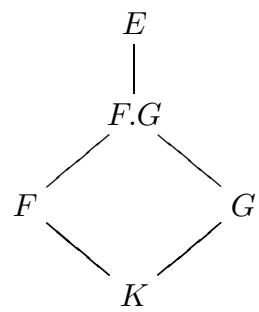
Demostración. Que 1) implica 2) es trivial. Veamos que 2) implica 1). Es claro que $E' \subseteq E''$. Así, por el punto 3) del Teorema 13.12 y la Proposición 21.11, $\mathrm{G}(E'/K)$ es resoluble. $\square$

Definición 22.2. Una extensión es resoluble si verifica las condiciones equivalentes de la Observación 21.1.

Proposición 22.3. *Se satisfacen:*

1) Sean F/K y E/F dos extensiones. Entonces E/K es resoluble si y sólo si F/K y E/F lo son.

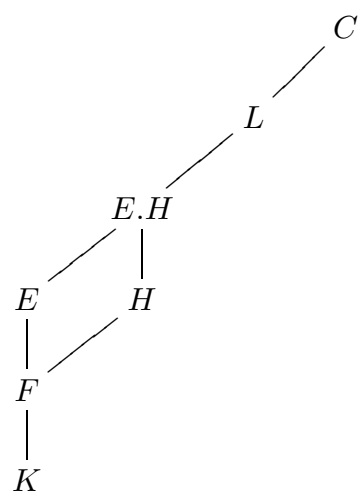
2) Sea



un diagrama de extensiones. Si F/K es resoluble, entonces $F.G/G$ también lo es.

Demostración. 2) Sea F'/K una extensión de Galois con $F \subseteq F'$ y $\mathrm{G}(F'/K)$ resoluble. Por la Proposición 13.13 $F'.G/G$ es de Galois y $\mathrm{G}(F'.G/G)$ es un subgrupo de $\mathrm{G}(F'/K)$. Así, por la Proposición 21.10, $F.G/G$ es resoluble.

1) Supongamos que E/K es resoluble. Es claro entonces que F/K también lo es. Por el punto 2) aplicado al caso $G = F$ y $F = E$, también E/F es resoluble. Supongamos ahora que F/K y E/F son resolubles. Consideremos el diagrama,



donde, H/K y L/H son extensiones de Galois resolubles y finitas y C es una clausura algebraica de L. Sea $M = K(\bigcup_\sigma \sigma(L))$, donde σ recorre los elementos de $\mathrm{Hom}(L/K, C/K)$. Por las Proposiciones 8.17, 13.8 y 13.11, M/K y M/H son de Galois. Como $\sigma(H) = H$ para todo $\sigma \in \mathrm{Hom}(L/K, C/K)$ y la aplicación $\theta\colon \mathrm{G}(L/H) \to \mathrm{G}(\sigma(L)/\sigma(H))$, definida por $\theta(\tau) = \sigma \circ \tau \circ \sigma^{-1}$ es un isomorfismo, los grupos $\mathrm{G}(\sigma(L)/H)$ son todos resolubles. En consecuencia, por la Proposición 21.11, también $\prod_\sigma \mathrm{G}(\sigma(L)/H)$ es resoluble. Como para todo $\sigma \in \mathrm{Hom}(L/K, C/K)$, la extensión $\sigma(L)/H$ es normal, tenemos que $\tau(\sigma(L)) = \sigma(L)$ para todo $\tau \in \mathrm{G}(M/H)$ y todo $\sigma \in \mathrm{Hom}(L/K, C/K)$. Así, podemos definir un morfismo $\vartheta\colon \mathrm{G}(M/H) \to \prod_\sigma \mathrm{G}(\sigma(L)/H)$, poniendo $\vartheta(\tau) = (\tau_{|\sigma(L)})_\sigma$. Dado que ϑ es claramente inyectivo, por la Proposición 21.10, $\mathrm{G}(M/H)$ es resoluble. Ahora, por el item 3) del Teorema 13.12, $\mathrm{G}(M/H)$ es un subgrupo normal de $G(M/K)$

y $\mathrm{G}(M/K)/\mathrm{G}(M/H) \simeq \mathrm{G}(H/K)$. Dado que $\mathrm{G}(M/H)$ y $\mathrm{G}(H/K)$ son resolubles, deducimos de la Proposición 21.11, que también $\mathrm{G}(M/K)$ lo es. $\square$

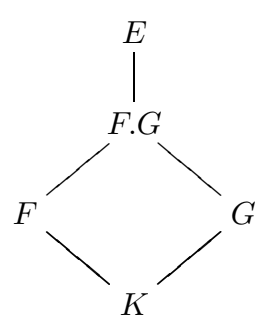
Definición 22.4. Una resolución por radicales es una cadena $E_0 \subseteq E_1 \subseteq \ldots \subseteq E_{n-1} \subseteq E_n$ de cuerpos tal que $E_{i+1} = E_i(\xi_i)$ para cada $i \in \{0, \ldots, n-1\}$, donde ξ_i es una raíz de un polinomio de la forma $X^m - a \in E_i[X]$ con m un número natural no divisible por la característica de K o de un polinomio de la forma $X^p - X - a \in E_i[X]$ con $p = \mathrm{char}(K) > 0$. Una extensión E/K es radical si existe una resolución por radicales con $E_0 = K$ y $E_n = E$.

Observese que toda extensión radical es separable.

Proposición 22.5. *Se satisfacen:*

1) Sean F/K y E/F dos extensiones. Si E/K es radical, entonces E/F también lo es y si F/K y E/F son radicales, entonces E/K también lo es.

2) Sea



un diagrama de extensiones. Si F/K es radical, entonces $F.G/G$ también lo es.

Demostración. 2) Es inmediato que si $K = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{n-1} \subseteq F_n = F$ es una resolución por radicales de F/K, entonces $G = F_0.G \subseteq F_1.G \subseteq \ldots \subseteq F_{n-1}.G \subseteq F_n.G = F.G$ es una resolución por radicales de $F.G/G$.

1) Es claro que si $K = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{m-1} \subseteq F_m = F$ y $F = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_{n-1} \subseteq E_n = E$ son resoluciones por radicales de F/K y E/F respectivamente, entonces, $K = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{m-1} \subseteq F_m \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_n = E$ es una resolución por radicales de E/K. Supongamos ahora que E/K es radical. Por el punto 2) aplicado al caso $G = F$ y $F = E$ se deduce que E/F también lo es. $\square$

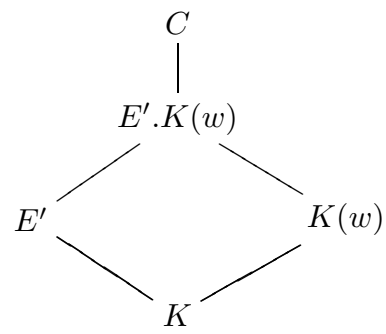
Definición 22.6. Una extensión finita E/K es resoluble por radicales si existe una extensión radical E'/K con $E \subseteq E'$.

Por la Proposición 8.16 toda extensión resoluble por radicales es separable.

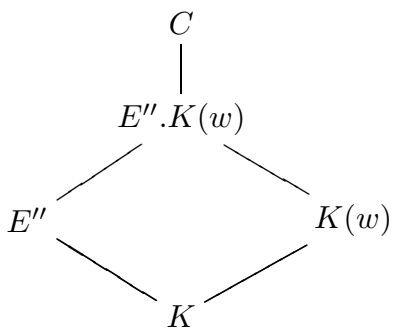
Teorema 22.7. *Una extensión es resoluble por radicales si y sólo si es resoluble.*

Demostración. Veamos primero que si E/K es resoluble, entonces E/K es resoluble por radicales. Sea C una clausura algebraica de E y E'/K la clausura normal de E/K en C. Por definición E'/K es una extensión resoluble de Galois. Sea m el producto de todos los primos que son distintos de la característica de K y que dividen a $(E' : K)$ y sea $w \in C$ una raíz m-ésima primitiva de la unidad.

Consideremos el diagrama de extensiones



Por el item 2) de las Proposiciones 13.11 y 22.3, la extensión $E'.K(w)/K(w)$ es de Galois y resoluble. Sea $\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = \mathrm{G}(E'.K(w)/K(w))$ una serie de descomposición de $\mathrm{G}(E'.K(w)/K(w))$. Por el teorema de Jordan-Hölder todos los cocientes G_{i+1}/G_i tienen orden primo. Consideremos la cadena $K(w) = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_n = E'.K(w)$ de subcuerpos de $E'.K(w)$, obtenida poniendo $F_i = (E'.K(w))^{G_{n-i}}$. Para cada $0 \leq i < n$ sea $p_i = (F_{i+1} : F_i)$. Si $p_i \neq \mathrm{char}(K)$, entonces por el item 1) de la Proposición 20.4, existe $\alpha_i \in F_{i+1}$ tal que $F_{i+1} = F_i(\alpha_i)$ y α_i es una raíz de un polinomio irreducible de la forma $X^{p_i} - a \in F_i[X]$ y si $p_i = \mathrm{char}(K)$, entonces por el item 1) de la Proposición 20.5, existe $\alpha_i \in F_{i+1}$ tal que $F_{i+1} = F_i(\alpha_i)$ y α_i es una raíz de un polinomio irreducible de la forma $X^{p_i} - X - a \in F_i[X]$. Así, la extensión $E'.K(w)/K(w)$ es radical y como $K(w)/K$ también es radical, se deduce del item 1) de la Proposición 22.5, que también $E'.K(w)/K$ lo es. Esto prueba que E/K es resoluble por radicales. Supongamos ahora que E/K es resoluble por radicales y veamos que es resoluble. Sea E'/K una extensión radical con $E \subseteq E'$ y sea E''/K la clausura normal de E'/K en alguna clausura algebraica C de E'. Por las Proposiciones 8.17, 13.8 y 22.5, E''/K es radical y de Galois. Sea $K = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_n = E''$ una cadena de subcuerpos de E'', tal que para cada $0 \leq i < n$ existe $\alpha_i \in F_{i+1}$ tal que $F_{i+1} = F_i(\alpha_i)$ y α_i es una raíz de un polinomio de la forma $X^{n_i} - a \in F_i[X]$ donde n_i es un número natural no divisible por la característica de K o de un polinomio de la forma $X^p - X - a \in F_i[X]$ donde $p = \mathrm{char}(K) > 0$. Sea m el producto de todos los n_i's que aparecen mencionados arriba y sea $w \in C$ una raíz m-ésima primitiva de la unidad. Consideremos el diagrama de extensiones



Por el item 2) de la Proposición 13.11 la extensión $E''.K(w)/K(w)$ es de Galois. Sea $\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n = \mathrm{G}(E''.K(w)/K(w))$ la cadena de subgrupos de $\mathrm{G}(E''.K(w)/K(w))$, obtenida poniendo $G_i = \mathrm{G}(E''.K(w)/F_{n-i}.K(w))$. Como para cada $0 \leq i < n$, la extensión $F_{i+1}.K(w)/F_i.K(w)$ es normal, cada G_i es un

subgrupo normal de G_{i+1}. Además, por el item 2) de las Proposiciones 20.4 y 20.5, los cocientes G_{i+1}/G_i son cíclicos. En consecuencia, la extensión $E''.K(w)/K(w)$ es resoluble y como $K(w)/K$ también es resoluble, deducimos del item 1) de la Proposición 22.3, que $E'.K(w)/K$ también lo es. □

Teorema 22.8 (Abel). *Si $n \geq 5$, entonces la ecuación general de grado n no es resoluble.*

Demostración. Se sigue inmediatamente del Ejemplo 13.20, de la Proposición 21.13 y del Teorema 22.7. □

23. Bases de trascendencia

Definición 23.1. Sea A una K-álgebra conmutativa. Un conjunto S de A es algebraicamente independiente sobre K si el morfismo de K-álgebras $\gamma\colon K[X_t\ (t \in S)] \to A$, definido por $\gamma(X_t) = t$ para todo $t \in S$, es inyectivo. Un conjunto que no es algebraicamente independiente sobre K se denomina algebraicamente dependiente sobre K.

Observación 23.2. Si S es algebraicamente dependiente sobre K existe un subconjunto finito S' de S que también es algebraicamente dependiente sobre K.

Proposición 23.3. *Sea E/K una extensión de cuerpos, S un subconjunto de E y S' un subconjunto de S. Son equivalentes:*

1) S es algebraicamente independiente sobre K.

2) S' es algebraicamente independiente sobre K y s es trascendente sobre $K(S\setminus\{s\})$ para cada $s \in S \setminus S'$.

Demostración. 1) $\Rightarrow$ 2) Es claro que S' es algebraicamente independiente sobre K. Supongamos que existe $s \in S \setminus S'$ tal que s es algebraico sobre $K(S \setminus \{s\})$. Sea $P(X) \in K(S \setminus \{s\})[X]$ un polinómio mónico tal que $P(s) = 0$. Escribamos

$$P(X) = X^d + \sum_{i=1}^{d-1} \frac{P_i(s_1, \ldots, s_m)}{Q_i(s_1, \ldots, s_m)} X^i,$$

donde los s_i son elementos distintos de $S \setminus \{s\}$. Sacando denominador común y evaluando X en s obtenemos una igualdad de la forma

$$\sum_{i=1}^{d} R_i(s_1, \ldots, s_m) s^i = 0,$$

con $R_d(s_1, \ldots, s_m) \neq 0$. Esto muestra que S es algebraicamente dependiente sobre K, lo que contradice la hipótesis. Así, s es trascendente sobre $K(S \setminus \{s\})$ para cada $s \in S \setminus S'$.

2) $\Rightarrow$ 1) Supongamos que existe una familia no vacía $s_1, \ldots, s_n$ de elementos distintos de S tal que $P(s_1, \ldots, s_n) = 0$ para algún polinomio no nulo $P \in K[X_1, \ldots, X_n]$. Tomemos una familia minimal con esta propiedad. Por hipótesis algún s_i no pertenece a S'. Es evidente que podemos suponer que $i = n$. Escribamos

$$P(X_1, \ldots, X_n) = \sum_{i=0}^{d} P_i(X_1, \ldots, X_{n-1}) X_n^i.$$

con $P_d(X_1, \ldots, X_{n-1}) \neq 0$. Es claro por la minimalidad de n que $P_d(s_1, \ldots, s_{n-1}) \neq 0$ y así s_n es algebraico sobre $K(s_1, \ldots, s_{n-1})$. □

Corolario 23.4. *Sea E/K una extensión de cuerpos y $S = \{s_1, \dots, s_n\}$ un subconjunto de E. Entonces S es algebraicamente independiente sobre K si y sólo si s_i es trascendente sobre $K(s_1, \dots, s_{i-1})$ para todo $1 \leq i \leq n$.*

Teorema 23.5. *Sea E/K una extensión de cuerpos y S un subconjunto de E. Son equivalentes:*

1) S es maximal entre los subconjuntos de E que son algebraicamente independientes sobre K.

2) S es minimal entre los subconjuntos de E tales que $E/K(S)$ es algebraico.

Demostración. 1) $\Rightarrow$ 2) Por la Proposición 23.3, aplicada al caso $S' = S$, tenemos que $E/K(S)$ es algebraico. La minimalidad se deduce de que por la misma proposición, s es trascendente sobre $K(S \setminus s)$ para cada $s \in S$.

2) $\Rightarrow$ 1) Por la Proposición 23.3, aplicada a $S' = S$, ningún subconjunto de E más grande que S puede ser algebraicamente independiente. Así, es suficiente ver que S lo es. Supongamos que esto es falso. Entonces, nuevamente por la Proposición 23.3, existe $s \in S$ tal que s es algebraico sobre $K(S \setminus \{s\})$. Así, por las Proposiciones 3.8 y 3.9, $E/K(S \setminus \{s\})$ es algebraico, lo que contradice la minimalidad de S. $\square$

Definición 23.6. Sea E/K una extensión de cuerpos. Una base de trascendencia de E/K es un subconjunto S de E que es algebraicamente independiente sobre K y que satisface la propiedad de que la extensión $E/K(S)$ es algebraica.

Teorema 23.7. *Sea E/K una extensión de cuerpos, $T \subseteq E$ tal que $E/K(T)$ es algebraico y $S \subseteq T$ un subconjunto algebraicamente independiente sobre K. Existe una base de trascendencia de E/K que contiene a S y que está contenida en T*

Demostración. Sea $\mathcal{S}$ una cadena maximal de subconjuntos de T que contienen a S y son algebraicamente independientes sobre K. Tomemos $S' = \bigcup_{S'' \in \mathcal{S}} S''$. Por la Observación 23.2 el conjunto S' es algebraicamente independiente sobre K. Es claro que S' es maximal entre los subconjuntos de T que tienen esta propiedad y en consecuencia, por la Proposición 23.3, los elementos de T son algebraicos sobre $K(S')$. Así, por las Proposiciones 3.8 y 3.9, E es algebraico sobre $K(S')$ y, por lo tanto, S' es una base de trascendencia de E/K. $\square$

Proposición 23.8 (lema de intercambio). *Sea E/K una extensión de cuerpos y $S \subseteq E$ un subconjunto finito y algebraicamente independiente de E sobre K. Si $T \subseteq E$ es tal que $E/K(T)$ es algebraica, entonces existe un subconjunto T' de T con la misma cantidad de elementos que S y tal que $E/K((T \setminus T') \cup S)$ también es algebraica.*

Demostración. Sea $S' \subseteq S$ maximal con la propiedad de que $S \cap T \subseteq S'$ y existe un subconjunto T' de T que tiene la misma cantidad de elementos que S' y tal que $E/K((T \setminus T') \cup S')$ es algebraica. Hay que ver que $S' = S$. Supongamos que existe $s \in S \setminus S'$. Como $s \notin (T \setminus T') \cup S'$, por la Proposición 23.3, el conjunto $(T \setminus T') \cup S' \cup \{s\}$ es algebraicamente dependiente sobre K. Así, dado que $S' \cup \{s\}$ es algebraicamente independiente sobre K, por la misma proposición, existe $t' \in T \setminus T'$ tal que t' es algebraico sobre $K((T \setminus (T' \cup \{t'\})) \cup S' \cup \{s\})$. En consecuencia, por las Proposiciones 3.8 y 3.9, la extensión $E/K(T \setminus (T' \cup \{t'\})) \cup S' \cup \{s\})$ es algebraica. $\square$

Teorema 23.9. *Sea E/K una extensión de cuerpos. Todas las bases de trascendencia de E/K tienen el mismo cardinal.*

Demostración. Sean S y T dos bases de trascendencia. Si S o T tiene una cantidad finita de elementos el resultado se deduce inmediatamente de la Proposición 23.8. Así podemos suponer que tanto S como T tienen infinitos elementos. Por simetría basta ver que $\#(S) \geq \#(T)$. Dado $s \in S$ existe un subconjunto finito T_s de T tal que s es algebraico sobre $K(T_s)$. Como $\#(S)$ es infinito, $\#(S) \geq \#\left(\bigcup_{s\in S} T_s\right)$. Así basta ver que $T = \bigcup_{s\in S} T_s$, lo que se deduce del Teorema 23.5 y de que, por las Proposiciones 3.8 y 3.9, E es algebraico sobre $K\left(\bigcup_{s\in S} T_s\right)$. $\square$

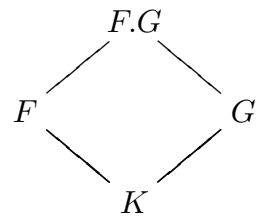
Ejemplo 23.10. Sea K un cuerpo, $K(t_1, \ldots, t_n)$ el cuerpo de fracciones del anillo de polinomios $K[t_1, \ldots, t_n]$ en n variables y $s_1, \ldots, s_n$ los polinomios simétricos elementales. Como $K(t_1, \ldots, t_n)$ es algebraico sobre $K(s_1, \ldots, s_n)$ y $\{t_1, \ldots, t_n\}$ es una base de trascendencia de $K(t_1, \ldots, t_n)/K$, de los Teoremas 23.7 y 23.9 se deduce que los polinomios $s_1, \ldots, s_n$ son algebraicamente independientes sobre K.

Definición 23.11. Sea E/K una extensión de cuerpos. El grado de trascendencia $\mathrm{grtr}(E/K)$ de E/K es el cardinal de cualquier base de trascendencia de E/K.

Proposición 23.12. *Se satisfacen:*

1) *Sean F/K y E/F dos extensiones. Si S es una base de trascendencia de F/K y T es es una base de trascendencia de E/F, entonces S y T son disjuntos y $S \cup T$ es una base de trascendencia de E/K. En particular* $\mathrm{grtr}(E/K) = \mathrm{grtr}(F/K) + \mathrm{grtr}(E/F)$.

2) *Sea*



un diagrama de extensiones. Si S es una base de trascendencia de F/K, entonces hay una base de trascendencia de $F.G/G$ que está incluída en S. En particular $\mathrm{grtr}(F.G/G) \leq \mathrm{grtr}(F/K)$.

Demostración. 1) Es claro que $S \cap T \subseteq F \cap T = \emptyset$. Veamos que $S \cup T$ es algebraicamente independiente. Por la Observación 23.2 es suficiente ver que cada subconjunto finito $s_1, \ldots, s_m, t_1, \ldots, t_n$ con los $s_i \in S$ y los $t_j \in T$ es algebraicamente independiente sobre K. Sea

$$P(X_1, \ldots, X_m, Y_1, \ldots, Y_n) \in K[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$$

un polinomio tal que $P(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Escribamos

$$P(X_1, \ldots, X_m, Y_1, \ldots, Y_n) = \sum_{i_1,\ldots,i_n \geq 0} P_{i_1,\ldots,i_n}(X_1, \ldots, X_m) Y_1^{i_1} \ldots Y_n^{i_n}$$

Como $t_1, \dots, t_n$ es algebraicamente independiente sobre F, cada uno de los coeficientes $P_{i_1,\dots,i_n}(s_1, \dots, s_m)$ es nulo. Así, como $s_1, \dots, s_m$ es algebraicamente independiente sobre K, cada polinomio $P_{i_1,\dots,i_n}(X_1, \dots, X_m)$ y, por lo tanto también P, es nulo. Resta ver que E es algebraico sobre $K(S \cup T)$. Ahora, E es algebraico sobre $F(T)$ y por la Proposición 3.8, $F(T) = K(F \cup T)$ es algebraico sobre $K(S \cup T)$. Así, por la Proposición 3.9, E es algebraico sobre $K(F \cup T)$.

2) Por el item 2) de la Proposición 3.12, la extensión $F.G/G(S)$ es algebraica. Así, el resultado se sigue inmediatamente del Teorema 23.7. □

Definición 23.13. Una extensión es puramente trascendente si tiene una base de trascendencia que es también un conjunto de generadores.

Proposición 23.14. *Sea K un cuerpo y t un elemento trascendente sobre K. Se satisfacen:*

1) *Si $s = f(t)/g(t) \in K(t)$ con $f(t)$ y $g(t)$ primos relativos y al menos uno de ellos no constante, entonces s es trascendente sobre K y $[K(t) : K(s)] = \max(\mathrm{gr}(f(t)), \mathrm{gr}(g(t)))$.*
2) *$K(t)$ es algebraico sobre cualquier cuerpo F que satisface $K \subsetneq F \subseteq K(t)$.*

Demostración. 1) El polinomio

$$P(X) = g(X)s - f(X) \in K(s)[X]$$

se anula en t. Así, t es algebraico sobre $K(s)$, lo que implica que s es trascendente sobre K, ya que de lo contrario, $K(t)/K$ sería algebraica. Además $P(X)$ es irreducible. En efecto, si $P(X) = A(s)P_1(s, X)P_2(s, X)$ con $P_1, P_2 \in K[s][X]$ primitivos, entonces como $P(X)$ tiene grado 1 en s, uno de los polinomios P_1 o P_2 pertenece a $K[X]$. Evaluando la igualdad de arriba en $s = 0$ y $s = 1$ obtenemos que este polinomio divide a $f(X)$ y a $g(X)$ y, por lo tanto, es una constante. Así, $P(X)$ es irreducible. Como $\mathrm{gr}(P(X)) = \max(\mathrm{gr}(f(t)), \mathrm{gr}(g(t))$, esto implica que $[K(t) : K(s)] = \max(\mathrm{gr}(f(t)), \mathrm{gr}(g(t)))$.

2) Se sigue facilmente de 1). □

Corolario 23.15. *Si E/K es puramente trascendente, entonces cada elemento de $E \setminus K$ es trascendente sobre K.*

Demostración. Sea $s \in E \setminus K$. Es claro que existe $\{t_1, \dots, t_n\}$ algebraicamente independiente sobre K tal que $s \in K(t_1, \dots, t_n)$. Ahora, por el item 1) de la Proposición 23.14, todo elemento de $K(t_1) \setminus K$ es trascendente sobre K. De la misma manera todo elemento de $K(t_1, t_2) \setminus K(t_1)$ es trascendente sobre $K(t_1)$ y, por lo tanto, también sobre K, etcetera. □

A continuación construímos una extensión con grado de trascendencia 1 que no es puramente trascendente.

Ejemplo 23.16. Sea $n \geq 3$ y K un cuerpo cuya característica no divide a n. Sea u trascendente sobre K y v una raíz de $P(X) = X^n + u^n - 1$ en alguna clausura algebraica de $K(u)$. Claramente, $K(u, v)/K$ no es algebraico. Veamos que tampoco es puramente trascendente. Como v es algebraico sobre $K(u)$, el grado de trascendencia de $K(u, v)/K$ es 1. Así, si $K(u, v)/K$ fuera puramente trascendente,

existiría un elemento $t \in K(u,v)$ trascendente sobre K tal que $K(t) = K(u,v)$. Veamos que esto no es posible. Si $K(t) = K(u,v)$, entonces

$$u = \frac{a(t)}{b(t)} \qquad \text{y} \qquad v = \frac{c(t)}{d(t)}$$

con $a(t)$ o $b(t)$ no constante y $a(t)$ coprimo con $b(t)$ y $c(t)$ coprimo con $d(t)$. Sea $(b(t); d(t))$ el máximo de los divisores comunes de $b(t)$ y $d(t)$. De la igualdad

$$\left(\frac{a(t)}{b(t)}\right)^n + \left(\frac{c(t)}{d(t)}\right)^n = 1$$

obtenemos que

$$(*) \qquad f(t)^n + g(t)^n = h(t)^n,$$

donde

$$f(t) = a(t)\frac{d(t)}{(b(t); d(t))}, \quad g(t) = c(t)\frac{b(t)}{(b(t); d(t))} \quad \text{y} \quad h(t) = \frac{b(t)d(t)}{(b(t); d(t))}.$$

Es fácil ver que $f(t)$, $g(t)$ y $h(t)$ son coprimos dos a dos. En efecto, supongamos que $q(t)$ es un primo de $K[t]$, que divide a $f(t)$, $g(t)$ y $h(t)$. Entonces divide a $b(t)$ o a $d(t)$. Supongamos que divide a $b(t)$. Como $a(t)$ y $b(t)$ son coprimos y $q(t)$ divide a $f(t)$, esto implica que $q(t)$ divide a $d(t)/(b(t); d(t))$. Así, como $b(t)/(b(t); d(t))$ y $d(t)/(b(t); d(t))$ son coprimos y $q(t) \mid g(t)$, tenemos que $q(t) \mid c(t)$. Pero esto se contradice con que $q(t)$ divide a $d(t)/(b(t); d(t))$, ya que $c(t)$ y $d(t)$ son coprimos. Supongamos que $\operatorname{gr}(f(t)) \leq \operatorname{gr}(g(t))$. Entonces $\operatorname{gr}(h(t)) \leq \operatorname{gr}(g(t))$. Dividiendo $(*)$ por $h(t)^n$ y derivando respecto a t, obtenemos

$$f(t)^{n-1}(f'(t)h(t) - f(t)h'(t)) + g(t)^{n-1}(g'(t)h(t) - g(t)h'(t)) = 0.$$

Como $f(t)$ y $g(t)$ son coprimos, deducimos de aquí que $g(t)^{n-1} \mid f'(t)h(t) - f(t)h'(t)$. Así,

$$(n-1)\operatorname{gr}(g(t)) \leq \operatorname{gr}(f(t)h(t)) - 1 = \operatorname{gr}(f(t)) + \operatorname{gr}(h(t)) - 1 \leq 2\operatorname{gr}(g(t)) - 1,$$

lo que no es posible, ya que $n \geq 3$. El caso en que $\operatorname{gr}(g(t)) \leq \operatorname{gr}(f(t))$ es similar.

Teorema 23.18 (Luroth). *Sea t un elemento trascentente sobre K. Si E es un subcuerpo de $K(t)$, que contiene a K estrictamente, entonces $E = K(s)$ para algún $s \in E \setminus K$.*

Demostración. Sea $s \in E \setminus K$. Escribamos $s = f(t)/g(t)$ con $f(t)$ y $g(t)$ coprimos. Por la Proposición 23.14,

$$[K(t) : E] \leq [K(t) : K(s)] = \max(\operatorname{gr}(f(t)), \operatorname{gr}(g(t))).$$

Escribamos $d_s := \max(\operatorname{gr}(f(t)), \operatorname{gr}(g(t)))$ y $n := [K(t) : E]$. Por lo que acabamos de ver $d_s \geq n$. Debemos encontrar s tal que d_s sea igual a n. Escribamos

$$P(X) = \operatorname{irr}(t, E) = X^n + \frac{a_1(t)}{b_1(t)}X^{n-i_1} + \cdots + \frac{a_m(t)}{b_m(t)}X^{n-i_m},$$

con $1 \leq i_1 < \cdots < i_m \leq n$ y donde cada $a_k(t)/b_k(t)$ es un cociente no nulo de polinomios coprimos. Como t no es algebraico sobre K, no todos los coeficientes de $P(X)$ estan en K. Por lo tanto tenemos que

$$s := \frac{a_k(t)}{b_k(t)} \in E \setminus K$$

para algún k. Consideremos el polinomio

$$H(X) = a_k(X) - \frac{a_k(t)}{b_k(t)} b_k(X) \in E(X).$$

Dado que $H(t) = 0$, tenemos que $P(X) \mid H(X)$ en $E[X]$. Así, existe $Q(X) \in E[X]$, tal que

$$a_k(X)b_k(t) - a_k(t)b_k(X) = b_k(t)Q(X)P(X).$$

Multiplicando esta igualdad por $b_1(t) \dots b_m(t)$, obtenemos que

$$(*) \qquad b_1(t) \dots b_m(t)(a_k(X)b_k(t) - a_k(t)b_k(X)) = b_k(t)Q(X)P'(t, X),$$

donde

$$\begin{aligned} P'(t, X) &= b_1(t) \dots b_m(t)P(X) \\ &= b_1(t) \dots b_m(t)X^n + \sum_{k=1}^{m} b_1(t) \dots b_{k-1}(t)a_k(t)b_{k+1}(t) \dots b_m(t)X^{n-i_k}. \end{aligned}$$

Factoricemos $P'(t, X)$ como $P'(t, X) = h(t)P''(t, X)$, donde $h(t)$ es el máximo de los divisores comunes de los coeficientes de $P'(t, X) \in K[t][X]$ y $P''(t, X)$ es primitivo, en el sentido de que no es divisible por ningún polinomio en t que no sea constante. Como $h(t)$ divide al máximo de los divisores comunes de

$$b_1(t) \dots b_m(t) \quad \text{y} \quad b_1(t) \dots b_{k-1}(t)a_k(t)b_{k+1}(t) \dots b_m(t),$$

que es $b_1(t) \dots b_{k-1}(t)b_{k+1}(t) \dots b_m(t)$, tenemos que $b_k(t)$ y $a_k(t)$ dividen a los coeficientes de X^n y X^{n-i_k} en $P''(t, X)$, respectivamente. Así,

$$\mathrm{gr}_t(P''(t, X)) \geq \max(\mathrm{gr}(a_k(t)), \mathrm{gr}(b_k(t))) = d_s,$$

donde $\mathrm{gr}_t(P''(t, X))$ es el grado en t de $P''(t, X)$. Multiplicando $(*)$ por un $u(t) \in K[t]$ apropiado, obtenemos

$$u(t)b_1(t) \dots b_m(t)(a_k(X)b_k(t) - a_k(t)b_k(X)) = h(t)b_k(t)Q'(t, X)P''(t, X),$$

donde $Q'(t, X) \in K[t, X]$. Ahora, como $P''(t, X)$ no es divisible por ningún polinomio en t que no es constante, tenemos que $u(t)b_1(t) \dots b_m(t) \mid h(t)b_k(t)Q'(t, X)$. Así, existe $Q''(t, X) \in k[t, X]$, tal que

$$a_k(X)b_k(t) - a_k(t)b_k(X) = Q''(t, X)P''(t, X).$$

Como el grado en t del lado izquierdo de esta igualdad es a lo sumo igual a $\max(\mathrm{gr}(a_k(t)), \mathrm{gr}(b_k(t))) = d_s$ y el grado en t de $P''(t, X)$ es al menos d_s, resulta que $Q''(t, X)$ no depende de t y así

$$a_k(X)b_k(t) - a_k(t)b_k(X) = Q''(X)P''(t, X),$$

donde $Q''(X) \in K[X]$. Ahora, dado que el lado derecho de esta igualdad no es divisible por ningún polinomio en t que no es constante y el lado izquierdo es simétrico en X y en t, el lado derecho tampoco es divisible por ningún polinomio en X que no es constante. En consecuencia,

$$a_k(X)b_k(t) - a_k(t)b_k(X) = QP''(t, X),$$

con $Q \in K$. Por último, como los grados en t y en X del lado izquierdo de esta igualdad coinciden, tenemos

$$n = \mathrm{gr}_X(P'(t, X)) = \mathrm{gr}_X(P''(t, X)) = \mathrm{gr}_t(P''(t, X)) \geq d_s \geq n,$$

lo que implica que $d_s = n$. □

Definición 23.19. Una extensión E/K es finitamente generada si existen una cantidad finita $e_1, \ldots, e_n$ de elementos de E tal que $E = K(e_1, \ldots, e_n)$.

Se deduce inmediatamente del Teorema 23.7 que si E/K está generada por n elementos, entonces $\mathrm{grtr}(E/K) \leq n$.

24. Subextensiones linealmente disjuntas y libres

Proposición 24.1. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Son equivalentes:*

1) *Toda familia de elementos de F linealmente independiente sobre K es linealmente independiente sobre G.*
2) *Toda familia de elementos de G linealmente independiente sobre K es linealmente independiente sobre F.*
3) *Sean $(e_i)_{i\in I}$ y $(f_j)_{j\in J}$ familias de elementos de F y G respectivamente. Si $(e_i)_{i\in I}$ y $(f_j)_{j\in J}$ son linealmente independientes sobre K, entonces $(e_i f_j)_{i\in I, j\in J}$ también es linealmente independiente sobre K.*
4) *Existe una base de F sobre K que es linealmente independiente sobre G.*
5) *Existe una base de G sobre K que es linealmente independiente sobre F.*
6) *Existen bases $(e_i)_{i\in I}$ de F sobre K y $(f_j)_{j\in J}$ de G sobre K tales que $(e_i f_j)_{i\in I, j\in J}$ es linealmente independiente sobre K.*

Demostración. 1) $\Rightarrow$ 3) Supongamos que $\sum_{i\in I, j\in J} \lambda_{ij} e_i f_j = 0$ es una ecuación de dependencia lineal de $(e_i f_j)_{i\in I, j\in J}$ sobre K. Entonces

$$\sum_{i\in I} \left(\sum_{j\in J} \lambda_{ij} f_j \right) e_i = \sum_{i\in I, j\in J} \lambda_{ij} e_i f_j = 0$$

y así, dado que $(e_i)_{i\in I}$ es linealmente independiente sobre G,

$$\sum_{j\in J}\lambda_{ij}f_j = 0,$$

para todo $i \in I$. De la independencia lineal de $(f_j)_{j\in J}$, obtenemos ahora que $\lambda_{ij} = 0$ para todo $i \in I$ y $j \in J$, lo que implica 3).

3) $\Rightarrow$ 1) Sea $(e_i)_{i\in I}$ una familia de elementos de F, linealmente independiente sobre K y sea $\sum_{i\in I} g_i e_i = 0$ una ecuación de dependencia lineal sobre G. Tomemos una base $(f_j)_{j\in J}$ de G sobre K y escribamos $g_i = \sum_{j\in J}\lambda_{ij}f_j$ para todo $i \in I$. Así,

$$\sum_{i\in I, j\in J}\lambda_{ij}e_i f_j = \sum_{i\in I} g_i e_i = 0,$$

lo que por hipótesis implica que $\lambda_{ij} = 0$ para todo $i \in I$ y $j \in J$. Pero entonces $g_i = \sum_{j\in J}\lambda_{ij}f_j = 0$ para todo $i \in I$, de donde $(e_i)_{i\in I}$ es linealmente independiente sobre G. La demostración de que 2) $\Leftrightarrow$ 3) es similar a la de que 1) $\Leftrightarrow$ 3).

1) $\Leftrightarrow$ 4). Es claro que 1) implica 4). Supongamos que $(v_i)_{i\in I}$ es una base de F sobre K que es linealmente independiente sobre G. Tomemos una familia finita $(e_j)_{j\in J}$ de elementos de F, linealmente independiente sobre K. Consideremos un subconjunto finito I' de I tal que los e_j's están en el K-subespacio vectorial de F generado por $(v_i)_{i\in I'}$. Existe un subconjunto I'' de I' con la misma cantidad de elementos de J y tal que $(v_i)_{i\in I'\setminus I''}\bigcup(e_j)_{j\in J}$ genera el mismo K-subespacio vectorial de F que $(v_i)_{i\in I'}$. En particular los G-subespacios vectoriales de E generados por $(v_i)_{i\in I'\setminus I''}\bigcup(e_j)_{j\in J}$ y $(v_i)_{i\in I'}$ coinciden. Como este último conjunto es linealmente independiente sobre G y $(I'\setminus I'')\bigcup J$ tiene el mismo cardinal que I' esto implica que $(v_i)_{i\in I'\setminus I''}\bigcup(e_j)_{j\in J}$ también es linealmente independiente sobre G.

2) $\Leftrightarrow$ 5) y 3) $\Leftrightarrow$ 6) son similares a 1) $\Leftrightarrow$ 4). $\square$

Definición 24.2. Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Decimos que F y G son linealmente disjuntos sobre K si satisfacen las condiciones de la Proposición 24.1. También decimos en este caso que F es linealmente disjunta de G sobre K o que G es linealmente disjunta de F sobre K.

Nota 24.3. Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Es fácil ver que F y G son linealmente disjuntos sobre K si y sólo si existen una familia $(F_i/K)_{i\in I}$ de subextensiones finitamente generadas de F/K y una familia $(G_j/K)_{j\in J}$ de subextenciones finitamente generadas de G/K tales que

1) Cada subextensión finitamente generada de F/K es una subextensión de algún F_i/K.
2) Cada subextensión finitamente generada de G/K es una subextensión de algún G_j/K.
3) Para cada par de indices $i \in I$ y $j \in J$, los cuerpos F_i y G_j son linealmente disjuntos sobre K.

Proposición 24.4. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Si existe una familia $(f_i)_{i\in I}$ de elementos de F que satisface*

1) $(f_i)_{i\in I}$ es una base sobre K de un subanillo A de F cuyo cuerpo de fracciones es F,

2) Existe un subanillo B de G cuyo cuerpo de fracciones es G y tal que no hay ninguna ecuación no trivial de dependencia lineal

$$0 = b_1 f_{i_1} + \cdots + b_n f_{i_n}$$

con $i_1, \ldots, i_n \in I$ y $b_1, \ldots, b_n$ en B,

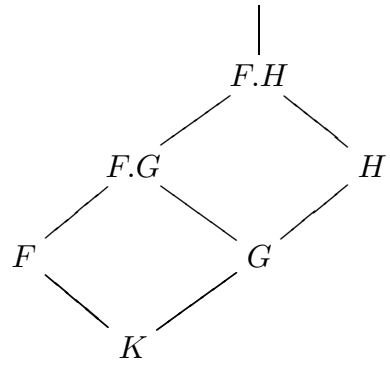
entonces F y G son linealmente disjuntos sobre K.

Demostración. Veamos primero que la familia $(f_i)_{i\in I}$ es linealmente independiente sobre G. Sea

$$0 = g_1 f_{i_1} + \cdots + g_m f_{i_m}$$

una ecuación de dependencia lineal con $i_1, \ldots, i_m \in I$ y coeficientes $g_1, \ldots, g_m$ en G. Tomemos $b \in B$ no nulo tal que $bg_i \in B$ para todo $1 \leq i \leq m$. Multiplicando la ecuación de arriba por b obtenemos una ecuación $0 = bg_1 f_{i_1} + \cdots + bg_m f_{i_m}$ con coeficientes bg_i en B. Por hipótesis estos coeficientes son todos nulos. Es claro entonces que los g_i también lo son. Sea ahora $f'_1, \ldots, f'_r$ una familia de elementos de F que es linealmente independiente sobre K. Sea a un elemento no nulo de A tal que $af'_i \in A$ para todo $1 \leq i \leq r$. Claramente $af'_1, \ldots, af'_r$ también es linealmente independiente sobre K. Consideremos $i_1, \ldots, i_s \in I$ tales que el K-espacio vectorial generado por $af'_1, \ldots, af'_r$ está incluído en el K-espacio vectorial V generado por $f_{i_1}, \ldots, f_{i_s}$. Existe una base de V cuyos primeros elementos son $af'_1, \ldots, af'_r$. Dado que por lo que vimos antes el G-espacio vectorial generado por V tiene dimensión s, los elementos $af'_1, \ldots, af'_r$ deben ser linealmente independientes sobre G. □

Proposición 24.5. *Sea,*



un diagrama de extensiones. Son equivalentes:

1) F y H son linealmente disjuntos sobre K.

2) F y G son linealmente disjuntos sobre K y $F.G$ y H son linealmente disjuntos sobre G.

Demostración. 1) ⇒ 2) Es claro que F y G son linealmente disjuntos sobre K. Veamos que $F.G$ y H son linealmente disjuntos sobre G. El cuerpo $F.G$ es el cuerpo de cocientes de $G[F]$. Como F y G son linealmente disjuntos sobre K, una base de F sobre K es también una base de $G[F]$ sobre G. Ahora, dado que F y H son linealmente disjuntos sobre K, esta base es linealmente independiente sobre H. Por la Proposición 24.4, $F.G$ y H son linealmente disjuntos sobre G.

2) $\Rightarrow$ 1) Sea $(f_j)_{j\in J}$ una familia de elementos de F que es linealmente independiente sobre K. Como F y G son linealmente disjuntos sobre K, la familia $(f_j)_{j\in J}$ es linealmente independiente sobre G y así, como $F.G$ y H son linealmente disjuntos sobre G, la familia $(f_j)_{j\in J}$ es linealmente independiente sobre H. $\square$

Proposición 24.6. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Son equivalentes:*

1) *Toda familia de elementos de F algebraicamente independiente sobre K es algebraicamente independiente sobre G.*
2) *Toda familia de elementos de G algebraicamente independiente sobre K es algebraicamente independiente sobre F.*

Demostración. Veamos que 1) implica 2). Sea $g_1,\dots,g_r$ una familia de elementos de G algebraicamente independiente sobre K y sea F'/K una subextensión finitamente generada de F/K. Por el item 1) de la Proposición 23.12,

$$\begin{aligned}\operatorname{grtr}(F'(g_1,\dots,g_r)/F') + \operatorname{grtr}(F'/K) &= \operatorname{grtr}(F'(g_1,\dots,g_r)/K)\\ &= \operatorname{grtr}(F'(g_1,\dots,g_r)/K(g_1,\dots,g_r)) + \operatorname{grtr}(K(g_1,\dots,g_r)/K).\end{aligned}$$

Dado que toda familia de elementos de F que es algebraicamente independiente sobre K es algebraicamente independiente sobre G,

$$\operatorname{grtr}(F'(g_1,\dots,g_r)/K(g_1,\dots,g_r)) = \operatorname{grtr}(F'/K).$$

Así, $\operatorname{grtr}(F'(g_1,\dots,g_r)/F') = \operatorname{grtr}(K(g_1,\dots,g_r)/K) = r$, de donde $g_1,\dots,g_r$ es algebraicamente independiente sobre F'. Como esto vale para toda subextensión F'/K finitamente generada de F/K, tenemos que $g_1,\dots,g_r$ también es algebraicamente independiente sobre F. La demostración de que 2) implica 1) es identica a la de que 1) implica 2). $\square$

Definición 24.7. Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Decimos que F y G son libres sobre K si satisfacen las condiciones de la Proposición 24.6.

Nota 24.8. Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Es fácil ver que F y G son libres sobre K si y sólo si existen una familia $(F_i/K)_{i\in I}$ de subextensiones finitamente generadas de F/K y una familia $(G_j/K)_{j\in J}$ de subextenciones finitamente generadas de G/K tales que

1) Cada subextensión finitamente generada de F/K es una subextensión de algún F_i/K.
2) Cada subextensión finitamente generada de G/K es una subextensión de algún G_j/K.
3) Para cada par de indices $i\in I$ y $j\in J$, los cuerpos F_i y G_j son libres sobre K.

Proposición 24.9. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Si existe una base de trascendencia de F/K que es algebraicamente independiente sobre G, entonces F y G son libres sobre K.*

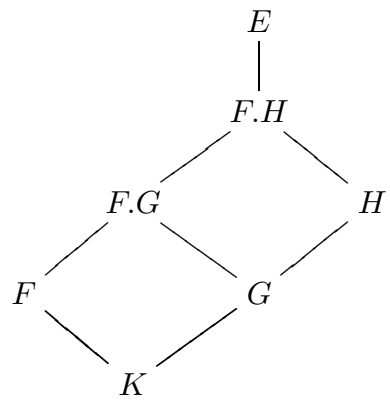
Demostración. Sea $(f_i)_{i\in I}$ una base de trascendencia de F/K que es algebraicamente independiente sobre G. Sea $f'_1,\dots,f'_r$ una familia de elementos de F que es algebraicamente independiente sobre K. Es fácil ver que existen $i_1,\dots,i_s\in I$

tales que los elementos $f'_1, \ldots, f'_r$ son algebraicos sobre $K(f_{i_1}, \ldots, f_{i_s})$. Consideremos una base de trascendencia de $K(f'_1, \ldots, f'_r, f_{i_1}, \ldots, f_{i_s})/K$ cuyos primeros elementos son $f'_1, \ldots, f'_r$. Dado que por hipótesis el grado de trascendencia de $G(f'_1, \ldots, f'_r, f_{i_1}, \ldots, f_{i_s})/G$ es s, los elementos $f'_1, \ldots, f'_r$ deben ser algebraicamente independientes sobre G. □

Corolario 24.10. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Si F/K es algebraico, entonces F y G son libres sobre K.*

Demostración. Es obvio que toda base de trascendencia de F/K es algebraicamente independiente sobre G. □

Proposición 24.11. *Sea,*



un diagrama de extensiones. Son equivalentes:

1) F y H son libres sobre K.

2) F y G son libres sobre K y $F.G$ y H son libres sobre G.

Demostración. 1) ⇒ 2) Sea $(g_i)_{i\in I}$ una familia de elementos de $G \subseteq H$ que es algebraicamente independiente sobre K. Como F y H son libres sobre K, la familia $(g_i)_{i\in I}$ es algebraicamente independiente sobre F. Esto muestra que F y G son libres sobre K. Veamos que $F.G$ y H son libres sobre G. Como F y G son libres sobre K, una base de trascendencia de F sobre K es también una base de trascendencia de $F.G$ sobre G. Ahora, dado que F y H son libres sobre K, esta base de trascendencia es algebraicamente independiente sobre H. Por la Proposición 24.9, $F.G$ y H son libres sobre G.

2) ⇒ 1) Sea $(f_j)_{j\in J}$ una familia de elementos de F que es algebraicamente independiente sobre K. Como F y G son libres sobre K, la familia $(f_j)_{j\in J}$ es algebraicamente independiente sobre G y así, como $F.G$ y H son libres sobre G, la familia $(f_j)_{j\in J}$ es algebraicamente independiente sobre H. □

Proposición 24.12. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Si F y G son linealmente disjuntos sobre K, entonces F y G son libres sobre K.*

Demostración. Sea $(f_i)_{i\in I}$ una familia de elementos de F que es algebraicamente independiente sobre K. Consideremos la familia de monomios en las variables f_i's. Claramente esta familia es linealmente independiente sobre K. Así, por hipótesis, también es linealmente independiente sobre G. De aquí se deduce inmediatamente que $(f_i)_{i\in I}$ es algebraicamente independiente sobre G, lo que prueba que F y G son libres sobre K. □

A continuación damos un recíproca parcial del resultado que acabamos de probar.

Proposición 24.13. *Sean E/K una extensión y F/K y G/K dos subextensiones de E/K. Si F/K es puramente trascendente y F y G son libres sobre K, entonces F y G son linealmente disjuntos sobre K.*

Demostración. Sea $(f_i)_{i\in I}$ una base de trascendencia de F que genera a F. La familia $M(\mathcal{F})$ de los monomios sobre esta base de trascendencia, es una base como K-espacio vectorial, de un subanillo de F cuyo cuerpo de fracciones es F. Dado que por hipótesis $(f_i)_{i\in I}$ es algebraicamente independiente sobre G, la familia $M(\mathcal{F})$ es linealmente independiente sobre G. Así, por la Proposición 24.4, F y G son linealmente disjuntos sobre K. $\square$