Tema 4.- Extensiones normales. Separabilidad.

4.1 Extensiones normales.

DEFINICIÓN 4.1.1.– Una extensión algebraica se dice *normal* si el polinomio mínimo de todo elemento de E factoriza en E o, equivalentemente, si todo polinomio irreducible de $k[x]$ con una raíz en E factoriza en E.

TEOREMA 4.1.2.– Una extensión $k \subset L$ es normal y finita si y sólo si L es el cuerpo de descomposición de algún $f \in k[x]$.

PROPOSICIÓN 4.1.3.– Dadas las extensiones $K \subset N \subset L$, si $K \subset L$ es normal, $K \subset N$ también.

En la situación de la proposición anterior, no se tiene en general que $K \subset M$ sea normal.

4.2 Separabilidad.

PROPOSICIÓN 4.2.1.– Sean fy g polinomios en $k[x]$ y $k \subset \Omega$. El máximo común divisor de f y g coincide en $k[x]$ y en $\Omega[x]$. En particular, si f y g son mónicos, irreducibles y $f \neq g$ entonces no tienen ningún factor en ninguna extensión de k.

DEFINICIÓN 4.2.2.– Un polinomio $f \in k[x]$ se dice *separable* si sus factores irreducibles tienen todas sus raíces simples. Un cuerpo k se dice *perfecto* si todos sus polinomios son separables.

PROPOSICIÓN 4.2.3.– Un polinomio $f \in k[x]$ tiene raíces multiples (en un cuerpo de descomposición) sí y sólo si f y su derivada formal $D(f)$ tienen un factor de grado ≥ 1.

PROPOSICIÓN 4.2.4.– Si la característica de un cuerpo k es cero todos los polinomios son separables. Si es $p > 0$ entonces un polinomio $f(x)$ es separable si y sólo si $f(x) = g(x^p)$ para algún $g \in k[x]$.

DEFINICIÓN 4.2.5.– Dado un cuerpo K de característica 0, el *homomorfismo de Frobenius* es la aplicación $\phi : K \longrightarrow K$ que lleva x en x^p.

COROLARIO 4.2.6.– Un cuerpo es perfecto si y sólo si es de característica 0 o es de característica $p > 0$ y el homomorfismo de Frobenius es un isomorfismo.

DEFINICIÓN 4.2.7.– Un elemento algebraico de una extensión se dice separable si su polinomio mínimo es separable. Una extensión algebraica $k \subset E$ se dice separable si el polinomio mínimo de todo elemento de E es separable.

PROPOSICIÓN 4.2.8.– Una extensión $k \subset E$ es separable y normal si y sólo si para cada $\alpha \in E$ el polinomio mínimo de α tiene $[k[\alpha] : k]$ raíces distintas en E.

PROPOSICIÓN 4.2.9.– Dadas las extensiones $K \subset N \subset L$, si $K \subset L$ es separable, $K \subset N$ y $N \subset K$ también.

El recíproco es cierto para extensiones finitas.

4.3 Grupos de automorfismos de cuerpos.

Consideremos extensiones $k \subset E$. Notaremos $\mathrm{Aut}(E/k)$ el grupo de k-automorfismos. Nos interesará especialmente el caso finito.

PROPOSICIÓN 4.3.1.– Si E es el cuerpo de descomposición de un polinomio mónico separable $f \in k[x]$, entonces $\mathrm{Aut}(E/k)$ tiene orden $[E : k]$.

EJEMPLO 4.3.2.– Sea $E = k[\alpha]$ con $f(\alpha) = 0$. Si f no tiene más raíces en E entonces $\mathrm{Aut}(E/k) = 1$. Es el caso de $\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}$ si $\sqrt[3]{2}$ denota la raíz cúbica real de 2. Es esencial que E sea el cuerpo de descomposición.

EJEMPLO 4.3.3.– Volvemos al ejemplo $k = \mathbb{F}_p(t)$. El cuerpo de descomposición de $f = X^p - t \in k[X]$ es $k[\alpha]$ donde α es la única raíz de f. Es esencial que el polinomio sea separable.

Notación.- Si G es un subgrupo del grupo de automorfismos de un cuerpo E, escribiremos

$$E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}.$$

E^G es un subcuerpo de E, el *subcuerpo de E fijo por G*.

LEMA 4.3.4.– (E. Artin) Sea G un grupo finito de automorfismos de E y sea $k = E^G$. Entonces $[E : k] \leq |G|$.

TEOREMA 4.3.5.– Sea $k \subset E$ una extensión. Son equivalentes:

1. E es el cuerpo de descomposición de un polinomio separable.
2. $k = E^G$ para algún G finito de automorfismos de E.
3. E es normal, separable y de grado finito sobre k.

DEFINICIÓN 4.3.6.– Llamaremos extensión de Galois a una extensión como las del teorema anterior. Denotaremos $\mathrm{Gal}(E/k)$ al grupo de los k-automorfismos de E.

COROLARIO 4.3.7.– Toda extensión finita y separable está contenida en una extensión de Galois.

COROLARIO 4.3.8.– Sean $k \subset M \subset E$. Si E es de Galois sobre k lo es sobre M.