Tema 2.- Extensiones de cuerpos. Extensiones algebraicas y finitas

2.1 Generalidades

Una primera definición de *extensión de cuerpos* es sencillamente un par de cuerpos k, K de manera que k es un subcuerpo de K. No obstante, a veces nos encontramos situaciones donde lo que tenemos es un homomorfismo de anillos $i : k \to K$ entre dos cuerpos, que necesariamente ha de ser inyectivo (pues $\ker i$ es un ideal propio de k y por tanto es 0). En este caso no podemos decir que k sea un subcuerpo de K, pues ni siquiera tiene por qué ser un subconjunto. Sin embargo i establece un isomorfimso entre k y su imagen $i(k)$ que sí es un subcuerpo de K. Esto nos lleva a dar la siguiente definición formal:

Definición 2.1.1.– Una *extensión de cuerpos* es una terna k, K, i donde k y K son cuerpos e $i : k \to K$ es un homomorfismo de anillos, que necesariamente es inyectivo.

Diremos que dos extensiones de cuerpos $i : k \to K$ y $j : k \to L$ son *isomorfas* si existe un isomorfismo de cuerpos $\psi : K \to L$ tal que $\psi \circ i = j$.

Cuando k sea un subcuerpo de K e i sea la inclusión omitiremos toda referencia a i y hablaremos sencillamente de la extensión de cuerpos $k \subset K$.

Notemos que una extensión de cuerpos k, K, i siempre da lugar a otra extensión de cuerpos en el sentido obvio $i(k) \subset K$.

Ejemplo 2.1.2.– Son extensiones de cuerpos: $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$.
Si k es un cuerpo arbitrario y $f(x) \in k[x]$ es un polinomio irreducible, entonces el ideal $(f(x))$ es maximal y por tanto el anillo cociente $k[x]/(f(x))$ es un cuerpo. Tenemos un homomorfismo de anillos $\varphi : k \to k[x]/(f(x))$ composición de la inclusión $k \subset k[x]$ y del paso al cociente $k[x] \to k[x]/(f(x))$, que es pues una extensión de cuerpos.
Dado un cuerpo arbitrario k consideremos el cuerpo de fracciones del dominio de integridad $k[x]$, que notamos $k(x)$. La inclusión natural $k \hookrightarrow k(x)$ es una extensión de cuerpos.
Podemos considerar extensiones distintas con los mismos cuerpos. Por ejemplo, tomemos la identidad $\mathrm{Id} : k(x) \to k(x)$. Pero también podemos definir otro homomorfismo $\varphi : k(x) \to k(x)$ de la siguiente forma. Sea $\varphi_0 : k[x] \to k(x)$ el único homomorfismo de anillos tal que $\varphi_0(a) = a$ para todo $a \in k$ y $\varphi_0(x) = x^2$ (propiedad universal de los anillos de polinomios, tema 3 de Algebra). Viendo que φ_0 es inyectivo, podemos aplicar la propiedad universal del cuerpo de fracciones de un dominio para deducir un único homomorfismo de cuerpos $\varphi : k(x) \to k(x)$ que extiende a φ_0. Obviamente $\varphi \neq \mathrm{Id}$.

Definición 2.1.3.– Si $\varphi : k \to K$ es una extensión de cuerpos, podemos considerar a K como un espacio vectorial sobre k tomando el grupo abeliano $(K, +)$ y el producto por escalares dado por

$$(a, b) \in k \times K \mapsto a \cdot b := \varphi(a)b \in K.$$

A la dimensión de K como k espacio vectorial la llamaremos *grado de la extensión* y lo notaremos $[K : k]$[1]. Si dicha dimensión es finita, diremos que se trata de una *extensión finita*.

Ejemplo 2.1.4.– La extensión $\mathbb{Q} \subset \mathbb{R}$ no es finita. Las extensiones $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}[i]$ son finitas de grado 2.
Si k es un cuerpo arbitrario y $f(x) \in k[x]$ es un polinomio irreducible, la extensión $k \hookrightarrow k[x]/(f(x))$ es finita y su grado coincide con el grado del polinomio $f(x)$.
Dado un cuerpo arbitrario k, la extensión $k \hookrightarrow k(x)$ no es finita.

Proposición 2.1.5.– *(Fórmula del grado)* Consideremos las extensiones de cuerpos $k \subset K \subset L$. Las siguientes propiedades son equivalentes:

[1] En esta notación no se hace referencia al homomorfismo φ con objeto de aligerarla, pero ha de tenerse en cuenta que de hecho depende de φ, como pone de manifiesto el último apartado del ejemplo anterior.

1. La extensión $k \subset L$ es finita.

2. Las extensiones $k \subset K$, $K \subset L$ son finitas.

Además, en el caso anterior se tiene la fórmula $[L : k] = [L : K][K : k]$.

DEFINICIÓN 2.1.6.– Sea $k \subset K$ una extensión de cuerpos y $S \subset K$ un subconjunto. El subanillo de K *generado por* k *y por* S es la intersección de todos los subanillos de K que contienen a k y a S, y se nota $k[S]$.

LEMA 2.1.7.– En las condiciones de la definición anterior, los elementos de $k[S]$ son todas las sumas finitas

$$\sum a_{i_1 \cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}$$

donde $a_{i_1 \cdots i_n} \in k$ y $\alpha_i \in S$.

LEMA 2.1.8.– Consideremos una extensión de cuerpos $k \subset K$. Si R es un subanillo de K tal que $k \subset R \subset K$ y que considerado como k-espacio vectorial es de dimensión finita, entonces R es un cuerpo.

PRUEBA: Tan sólo hemos de probar que si $a \in R$, $a \neq 0$, entonces $a^{-1} \in R$.

Consideremos la aplicación $f : R \to R$ dada por $f(x) = ax$ para cada $x \in R$. Evidentemente es una aplicación lineal de k-espacios vectoriales. Como $a \neq 0$ y R es un dominio de integridad, la aplicación f es inyectiva. Ahora bien, una aplicación lineal inyectiva entre dos espacios vectoriales de la misma dimensión finita ha de ser un isomorfismo. En particular ha de ser sobreyectiva, por lo que existe un $b \in R$ tal que $ab = f(b) = 1$, de donde $a^{-1} = b \in R$. □

El lema anterior se aplica por ejemplo a $k = \mathbb{Q} \subset R = \mathbb{Q}[i] \subset K = \mathbb{C}$.

DEFINICIÓN 2.1.9.– Sea $k \subset K$ una extensión de cuerpos y $S \subset K$ un subconjunto. El subcuerpo de K *generado por* k *y* S es la intersección de todos los subcuerpos de K que contienen a k y a S, y se nota $k(S)$. Dicho subcuerpo coincide con el cuerpo de fracciones de $k[S]$.

DEFINICIÓN 2.1.10.– Diremos que una extensión de cuerpos $k \subset K$ es finitamente generada si existe un subconjunto finito $S \subset K$ tal que $K = k(S)$.

EJEMPLO 2.1.11.– Toda extensión finita es finitamente generada.
La extensión $k \subset k(x)$ es finitamente generada pero no es finita.

2.2 Extensiones algebraicas y extensiones trascendentes

En lo que sigue $k \subset K$ denotará una extensión de cuerpos.

DEFINICIÓN 2.2.1.– Diremos que un elemento $\alpha \in K$ es *algebraico* sobre k si existe un polinomio $f(X)$ no nulo de grado mayor o igual que 1 tal que $f(\alpha) = 0$. En caso contrario diremos que α es trascendente sobre k.

Dado $\alpha \in K$ consideremos el homomorfismo de anillos $\sigma : k[x] \to K$ dado por la "sustitución de X por α". Obviamente α es algebraico sobre k si y sólo si $\ker \sigma \neq 0$. En este caso, por el primer teorema de isomorfía, $k[x]/\ker \sigma$ es isomorfo a $\mathrm{Im}\sigma \subset K$, que es un dominio de integridad. Por tanto $\ker \sigma$ es un ideal primo (y maximal) de $k[x]$ y estará generado por un único polinomio mónico irreducible de grado mayor o igual que 1, que llamaremos *polinomio mínimo de* α. El grado de dicho polinomio se llamará *grado de* α.

PROPOSICIÓN 2.2.2.– Si $\alpha \in K$ es algebraico sobre k, entonces $k[\alpha] = \mathrm{Im}\sigma = k(\alpha)$ y el grado de α coincide con $[k[\alpha] : k]$.

Definición 2.2.3.– Diremos que la extensión $k \subset K$ es *algebraica* si todos los elementos de K son algebraicos sobre k. En caso contrario diremos que es una extensión *trascendente*.

Ejemplo 2.2.4.– Todo elemento de k es algebraico sobre k y de grado 1.
El número $e \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$.
La extensión $k \subset k(x)$ es trascendente.

Proposición 2.2.5.– Las propiedades siguientes son equivalentes:

1. La extensión $k \subset K$ es finitamente generada y algebraica.
2. La extensión $k \subset K$ es finita.
3. Existen $\alpha_1, \ldots, \alpha_n \in K$ elementos algebraicos sobre k tales que $K = k(\alpha_1, \ldots, \alpha_n)$.

Corolario 2.2.6.– Supongamos que la extensión $k \subset K$ es algebraica. Entonces todo subanillo R de K que contiene a k es un cuerpo y la extensión $k \subset R$ es de nuevo algebraica.

Proposición 2.2.7.– Consideremos dos extensiones de cuerpos $k \subset K$ y $K \subset L$. Las propiedades siguientes son equivalentes:

1. Las extensiones $k \subset K$ y $K \subset L$ son algebraicas.
2. La extensión $k \subset L$ es algebraica.