

Extensiones de cuerpos

F

$$K \subseteq F$$

|

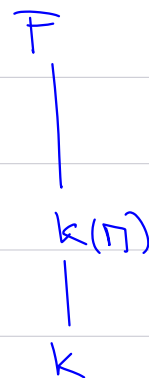
K

- Subcuerpo propio: $K \subsetneq F$
- Cuerpo primo: si no tiene subcuerpos propios
 $\hookrightarrow \mathbb{F}_p$ p primo, $\mathbb{Q}$

$\bigcap F_i \subset F_i \subset F \quad \forall F_i \text{ es subcuerpo de } F$
subcuerpo primo de F

Teo: el subcuerpo primo de F es isomorfo a $\mathbb{F}_p$
si $\text{char}(F) = p$ primo o a $\mathbb{Q}$ si $\text{char}(F) = 0$.

Def: Sea K un subcuerpo de un cuerpo F y sea Π cualquier subconjunto de F . Entonces el cuerpo $K(\Pi)$ se define como la intersección de todos los subcuerpos de F que contienen a K y a Π . Se llama la extensión del cuerpo K obtenida adjuntando los elementos de Π .



Si $\Pi = \{\theta_1, \dots, \theta_n\}$ escribiremos $K(\theta_1, \dots, \theta_n)$.

Si Π tiene un único elemento $\Pi = \{\sigma\}$ se dice que $L = k(\sigma)$ es una extensión simple de k y σ se llama elemento de definición de L sobre k .

Por la forma que se definió, $k(\Pi)$ es el menor subcuerpo de F que contiene a k y a Π .

Def: Sea k un subcuerpo de F y $\sigma \in F$. Si σ es raíz de un polinomio con coeficientes en k entonces decimos que σ es algebraico sobre k es decir, σ es algebraico si

$$a_n \sigma^n + a_{n-1} \sigma^{n-1} + \dots + a_1 \sigma + a_0 = 0$$

$a_n, a_{n-1}, \dots, a_1, a_0 \in k$, no todos nulos.

$\neq$
|
 k

Una extensión L de k (de cuerpos) se llama algebraica si todos sus elementos son algebraicos sobre k .

Def: Si $\sigma \in F$ es un elemento algebraico sobre k , entonces el polinomio mónico en $k[x]$ de menor grado que se anula en σ se lo llama polinomio mínimo de σ sobre k .

Notar que la definición anterior tiene sentido, pues
ni contradicciones

$$I = \{ f(x) \in K[x] : f(\theta) = 0 \}$$

es un ideal y como $K[x]$ es un dominio de
ideales principales existe un único $g(x) \in K[x]$
mónico tal que $I = (g(x))$. Este g es el polinomio
mínimo de θ .

Si $h \in I$ es un polinomio de menor grado
posible y definimos $g(x) = b^{-1} \cdot h(x)$ donde
 b es el coeficiente ppal de h , entonces para
cualquier $f \in I$ por el alg. de la división

$$f(x) = q(x) \cdot g(x) + r(x) \quad \deg r < \deg g$$

Pero entonces $r(x) = f(x) - q(x) \cdot g(x)$ y
como r se anula también en θ
debe ser $r(x) = 0$.

$$\therefore I = (g(x)).$$

Teorema: Si $\alpha \in F$ es algebraico sobre k , entonces su polinomio mínimo g satisface

1) g es irreducible sobre $k[x]$

2) $f \in k[x]$ y $f(\alpha) = 0 \Rightarrow g$ divide a f .

Cuando hablamos del grado de un elemento α algebraico sobre k , nos referiremos al grado de su polinomio mínimo sobre k .

Si L es una extensión de cuerpos de k , L puede verse como un espacio vectorial sobre k , puesto que los elementos de L forman un grupo abeliano bajo la suma y la multiplicación escalar de un elemento $\alpha \in L$ por un $r \in k$ da como resultado $r \cdot \alpha \in L$ el cual cumple:

L
|
 k .

$$r(\alpha + \beta) = r\alpha + r\beta \in L$$

$$(r+s) \cdot \alpha = r\alpha + s\alpha$$

$$(r \cdot s) \cdot \alpha = r(s\alpha)$$

$$1 \cdot \alpha = \alpha.$$

Def: Sea L una extensión de cuerpos de un cuerpo k . Si L considerado como espacio vectorial sobre k tiene dimensión finita, entonces decimos que L es una extensión finita de k . A la dimensión del espacio vectorial L sobre k se le llama grado de L sobre k y se denota $[L:k]$.

Teorema: Si L es una extensión finita de k y Π es una extensión finita de L entonces Π es una extensión finita de k y se cumple

$$\begin{array}{c} L \\ | < \infty \\ k \end{array}$$

$$[\Pi:k] = [\Pi:L] \cdot [L:k].$$

Dem: Supongamos que $[\Pi:L] = m$ $[L:k] = n$ y

$\{\alpha_1, \dots, \alpha_m\}$ una base de Π/L

$\{\beta_1, \dots, \beta_n\}$ una base de L/k .

Si $\alpha \in \Pi$, entonces existen $\delta_1, \dots, \delta_m \in L$ tales que

$$\alpha = \delta_1 \alpha_1 + \dots + \delta_m \alpha_m$$

Pero a su vez L/k tiene base $\beta_1, \dots, \beta_n$

$$\alpha = \sum_{i=1}^m \alpha_i \alpha_i = \sum_{i=1}^m \overbrace{\left(\sum_{j=1}^n r_{ij} \beta_j \right)}^{\alpha_i} \cdot \alpha_i$$

$$= \sum_{i=1}^m \sum_{j=1}^n \underbrace{r_{ij}}_{\in k} \beta_j \cdot \alpha_i$$

Para ver que $\{ \beta_j \alpha_i \}_{\substack{i=1, \dots, m \\ j=1, \dots, n}}$ son L.I.

Supongamos que $\sum_{i=1}^m \underbrace{\left(\sum_{j=1}^n s_{ij} \beta_j \right)}_{\in L} \alpha_i = 0$

Como $\{ \alpha_1, \dots, \alpha_m \} \rightarrow$ base $\Rightarrow$ son L.I. $\Rightarrow$

$$\forall i = 1, \dots, m \quad \sum_{j=1}^n \underbrace{s_{ij}}_{\in k} \beta_j = 0$$

Como $\{ \beta_1, \dots, \beta_n \}$ son base $\Rightarrow$ son L.I. $\Rightarrow$

$$\forall j = 1, \dots, n \quad s_{ij} = 0.$$

$$\{ \alpha_i \beta_j \}_{\substack{i=1, \dots, m \\ j=1, \dots, n}}$$

$$[n:k] = [n:L][L:k]$$



Teorema: Todo extensión finita de k es algebraica sobre k .

Dem.

Sea L una extensión finita de k . $[L:k] = m$

Si $\theta \in L \setminus k$, entonces $1, \theta, \theta^2, \dots, \theta^m$ son $m+1$ elementos de L que deben ser L.D. sobre k y por lo tanto existen $a_0, a_1, \dots, a_m \in k$ no todos nulos tales que

$$a_0 + a_1 \theta + \dots + a_m \theta^m = 0$$

$\Rightarrow \theta$ es algebraico sobre k . / 

Si adjuntamos a un cuerpo k un elemento θ que es algebraico sobre k , obtenemos una extensión simple $k(\theta)$ que es finita y por lo tanto algebraica

$$\begin{array}{c} \mathbb{F} \\ | \\ k(\theta) \\ | < \infty \\ k \end{array}$$

Teorema: Sea $\theta \in \mathbb{F}$ un elemento algebraico sobre k de grado n , y sea g el polinomio mínimo de θ sobre k . Entonces

1) $k(\theta)$ es isomorfo a $k[x]/(g(x))$

2) $[k(\theta):k] = n$ y $\{1, \theta, \dots, \theta^{n-1}\}$ es una base de $k(\theta)$ sobre k .

3) Todo $\alpha \in k(\theta)$ es algebraico sobre k y su grado sobre k es un divisor de n .

Los elementos que pertenecen a la extensión simple $k(\sigma)$ sobre k se pueden ver como expresiones polinómicas en σ .

$$\begin{array}{c} \sigma \in F \\ | \\ k(\sigma) \\ | \\ k \end{array}$$

Teorema: Sea $f \in k[x]$ un polinomio irreducible sobre k . Entonces existe una extensión algebraica simple de k con una raíz de f como elemento de definición.

Dem

$$k \quad f$$

Como f es irreducible sobre k sabemos que $L = k[x]/(f)$ es un cuerpo, y sus elementos son las clases $[h] = h + (f)$ $h \in k[x]$.

En particular, para cualquier $a \in k$ podemos considerar $[a]$ como polinomio constante y si $a \neq b$ entonces $[a] \neq [b]$, pues f es de grado positivo.

Entonces $a \mapsto [a]$ es un isomorfismo de cuerpos de k sobre k' que es un subcuerpo de L .

Por lo tanto podemos identificar a k con k' y pensar en L como una extensión de k .

$$k(x) = L = k[x]/(f)$$

$$k \cong k'$$

$$a \mapsto [a]$$

Además $h \in k[x]$ $h(x) = a_0 + a_1x + \dots + a_nx^n$
 $a_0, a_1, \dots, a_n \in k$

$$[h] = [a_0 + a_1x + \dots + a_nx^n] = [a_0] + [a_1][x] + \dots + [a_n][x]^n$$

$$k' \cong k$$

$$= a_0 + a_1[x] + \dots + a_n[x]^n \quad a_0, \dots, a_n \in k.$$

Entonces se puede describir a cualquier elemento de L como una expresión polinomial en $[x]$ y coeficientes en k , podemos identificar a L con la extensión simple $k(x)$ ya que es la que contiene a k y a $[x]$.

$$b_i \in k.$$

Además si $f = b_0 + b_1x + \dots + b_mx^m$

$$f([x]) = b_0 + b_1[x] + \dots + b_m[x]^m =$$

$$= [b_0 + b_1x + \dots + b_mx^m] = [f] \stackrel{L = k[x]/(f)}{=} 0.$$



Ejemplo: Consideremos $\mathbb{F}_3 = \{0, 1, 2\}$ y el polinomio
 $f(x) = x^2 + x + 2$ que es irreducible pues
 $(f(0)=2, f(1)=1, f(2)=2)$

$$\mathbb{F}_3[x]/(x^2+x+2) = L$$

$$L = \mathbb{F}_3(\theta)$$

$$= \{ [0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2] \}$$

$$\mathbb{F}_3$$

$$f(\theta) = \theta^2 + \theta + 2 = 0$$

$$\mathbb{F}_3(\theta) = \{ 0, 1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2 \}$$

$$\theta+2, 2\theta, 2\theta+1, 2\theta+2 \}$$

$$\theta^2 = -\theta - 2 = 2\theta + 1$$

$$\theta^3 = \theta \cdot \theta^2 = \theta(2\theta + 1) = 2\theta^2 + \theta =$$

$$= 2(2\theta + 1) + \theta =$$

$$= 4\theta + 2 + \theta =$$

$$= 5\theta + 2 = 2\theta + 2$$

Notar que $2\theta+2$ es otra raíz de $f(x)$

$$f(x) = x^2 + x + 2$$

$$f(2\theta+2) = (2\theta+2)^2 + (2\theta+2) + 2 =$$

$$= 4\theta^2 + 8\theta + 4 + 2\theta + 4 = \theta^2 + \theta + 2 = f(\theta) = 0$$

Si en lugar de adjuntar θ a $\mathbb{F}_3$ adjunto $2\theta+2$, obtengo la misma extensión $\mathbb{F}_3(x)/(\neq)$

$$\mathbb{F}_3(\theta) \simeq \mathbb{F}_3(2\theta+2).$$

Teorema: Sean α y β dos raíces del polinomio $f \in k[x]$ que es irreducible sobre k . Entonces $k(\alpha)$ y $k(\beta)$ son isomorfos por el isomorfismo que manda α en β y deja fijos a todos los elementos de k .

Ahora vamos a considerar extensiones que contengan a todas las raíces de un polinomio.

Def: $f \in k[x]$ de grado positivo y F una extensión de k . Entonces decimos que f se descompone en F si existen $\alpha_1, \dots, \alpha_n \in F$

$$f(x) = a \prod_{i=1}^n (x - \alpha_i)$$

El cuerpo F se llama cuerpo de descomposición de f sobre k si f se descompone en F y $F = k(\alpha_1, \dots, \alpha_n)$

Teorema: (Existencia y unicidad de los cuerpos de descomposición)

Si K es un cuerpo y f es cualquier polinomio de grado positivo en $K[x]$ existe un cuerpo de descomposición para f sobre K .
Además, cualesquiera dos cuerpos de descomposición de f sobre K son isomorfos bajo el isomorfismo que deje fijo a los elementos de K y mueva a los raíces de f entre sí.