2ª PARTE: TEORIA DE GALOIS

TEMA 9: ANILLOS ABELIANOS UNITARIOS. POLINOMIOS.

I. ANILLOS

1. DEFINICIONES: ANILLOS, UNIDADES, IDEALES

DEF: Dado un conjunto $A \neq \emptyset$ dotado con dos leyes de composición interna que denotamos por $+$ y $\cdot$, decimos que $(A;+,\cdot)$ tiene estructura de anillo si $(A,+)$ es un grupo abeliano, $(A,\cdot)$ un semigrupo y el producto es distributivo respecto de la suma.

Consideraremos, en adelante, anillos abelianos con elemento unidad. En las definiciones sifuientes $(A;+,\cdot)$ es un anillo abeliano con elemento unidad 1.

DEFINICION: Se dice que un elemento $u \in A$ es una unidad si es inversible, es decir, si existe $u' \in A$ tal que $u \cdot u' = 1$.

DEFINICION: Un subconjunto $\mathfrak{a}$ de A diremos que es un ideal de A si $\mathfrak{a}$ es subanillo y se verifica la siguiente propiedad:

$$\forall a \in \mathfrak{a}, \forall x \in A, \; ax \in \mathfrak{a}.$$

DEFINICION: Un ideal $\mathfrak{p} \neq (1)$ (*) es primo si se verifica la condición

$$a \cdot b \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ ó } b \in \mathfrak{p}$$

DEFINICION: Un ideal $\mathfrak{m} \neq (1)$ se dice maximal si es un elemento maximal en el conjunto ordenado por inclusión de los ideales de A distintos de (1).

Se prueba fácilmente, utilizando el LEMA DE ZORN, que todo anillo (unitario) admite un ideal maximal. Sacamos de aquí una consecuencia importante: "Dado un ideal $\mathfrak{a} \neq (1)$ de un anillo A, existe un ideal maximal $\mathfrak{m}$ que contiene a $\mathfrak{a}$". La demostración es trivial si consideramos el anillo cociente $A/\mathfrak{a}$; entonces existe un ideal maximal $\overline{\mathfrak{m}}$ en $A/\mathfrak{a}$ cuya contraimagen por el homomorfismo canonónico $p: A \to A/\mathfrak{a}$ es un ideal de A que contiene a $\mathfrak{a}$.

Damos a continuación unas proposiciones que no demostraremos.

1.1. PROPOSICION: Un anillo A conmutativo y unitario es un cuerpo si y solo si sus únicos ideales son (0) y A.

1.2. PROPOSICION: a) Un ideal $\mathfrak{p}$ es primo si y solo si $A/\mathfrak{p}$ es un dominio de integridad.
b) Un ideal $\mathfrak{m}$ es maximal si y solo si $A/\mathfrak{m}$ es cuerpo.

Como consecuencia inmediata de esta proposición tenemos
1.3. COROLARIO: Todo ideal maximal es primo.

El reciproco no es cierto; sirve de contraejemplo fue (0) es un ideal primo en $\mathbb{Z}$, pues $ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0$ ó $b = 0$, y sin embargo, (0) no es maximal en $\mathbb{Z}$, pues $(0) \subset (p)$ siendo p primo.
1.4. PROPOSICION: Dado $u \in A$, u es unidad si y solo si $A = (u)$.
Demostr.: $(u) = A \Leftrightarrow A \cdot u = A$
Si u es unidad, $\exists v \in A / uv = 1 \Rightarrow 1 \in (u) \Rightarrow A = (u)$.
Si $(u) = A \Rightarrow 1 \in (u) \Rightarrow \exists v \in A / uv = 1 \Rightarrow u$ es inversible. c.q.d.

* Sea A un dominio de integridad (anillo abeliano, íntegro y unitario). Dados dos elementos a y b de A, decimos que a divide a b si y solo si existe $c \in A$ tal que $b = c \cdot a$.

$$a|b \Leftrightarrow \exists c \in A / b = c \cdot a.$$

La relación de divisibilidad definida en A es un preorden (es reflexiva y transitiva). La propiedad antisimétrica, en general, no se verifica, pues pueden existir elementos distintos a y b tales que $a|b$ y $b|a$. Dos elementos a y b que satisfagan lo dicho anteriormente se llaman asociados. Es inmediato comprobar que a y b son asociados sii $b = u \cdot a$ donde u es una unidad de A.

DEFINICIONES: a) Diremos que a es un divisor propio de b si $a|b$ y a y b no son asociados.
b) Diremos que a es irreducible si no es unidad y no admite divisores propios.
c) Diremos que a es primo si a no es unidad y verifica la implicación: $a|b \cdot c \Rightarrow a|b$ ó $a|c$.

1.5. PROPOSICION: Un elemento $a \in A$ es primo si y solo si (a) es un ideal primo.

Demostr.: $\Rightarrow$] Si $b \cdot c \in (a) \Rightarrow a|b \cdot c$ (a primo) $\Rightarrow a|b$ ó $a|c$ es decir $b \in (a)$ o $c \in (a)$.
$\Leftarrow$] Si $a|b \cdot c \Rightarrow bc \in (a)$ ((a) primo) $\Rightarrow b \in (a)$ ó $c \in (a) \Rightarrow a|b$ ó $a|c$. c.q.d.

DEFINICION: Un dominio de integridad unitario A se dice principal si todos sus ideales son principales, es decir, si todo ideal $\mathcal{J}$ de A es de la forma $\mathcal{J}=(a)$ donde $a\in A$.

Recordemos que $(a)=\{c\cdot a / c\in A\}=A\cdot a$.

1.6. PROPOSICION: Sea A un dominio principal. Entonces:

a) Un elemento a de A es irreducible si y solo si (a) es un ideal maximal.
b) Un elemento a de A es irreducible si y solo si a es primo.
c) $\mathcal{M}$ es un ideal maximal de A si y solo si $\mathcal{M}$ es primo.

Demostr.: a) $\Rightarrow$| Sea a un elemento irreducible y $\mathcal{J}$ un ideal de A tal que $\mathcal{J}\supset(a)$. Siendo A un dominio principal, existe $d\in A$ tal que $\mathcal{J}=(d)$.
Entonces $(a)\subset(d)\Rightarrow a\in(d)\Rightarrow \exists c\in A / a=d\cdot c\Rightarrow d|a$.
Siendo a irreducible no admite divisores propios. Entonces, d es una unidad o es un asociado de a.
Si d es unidad, $(d)=A$.
Si d y a son asociados, existe una unidad $u\in A$ tal que $d=u\cdot a$.
Entonces, $(d)=(u\cdot a)=(a)$; que prueba que los únicos ideales que contienen a (a) son A y él mismo. Luego (a) es maximal.
$\Leftarrow$| Supongamos que (a) es maximal. Sea b un divisor de a y probemos que b es una unidad o un asociado de a.
Si $b|a$, $\exists c\in A / a=b\cdot c$.
Siendo (a) maximal, es primo (COROLARIO 1.3) y, por tanto, a es primo (PROPOSICION 1.5). Luego:
$a|b\cdot c\Rightarrow a|b$ ó $a|c$. Supongamos que $a|b$. Como además $b|a$, se tiene que a y b son asociados. Si $a|c$ serían asociados a y c y, por tanto, b sería una unidad. Luego a es irreducible.

b) $\Rightarrow$| Si a es irreducible, (a) es ideal maximal. Luego (a) es un ideal primo y, por tanto, a será primo.
$\Leftarrow$| Sea a primo. Entonces:
$a=b\cdot c\Rightarrow a|b\cdot c\Rightarrow a|b$ ó $a|c$. Como además $b|a$ y $c|a$ se tiene que b ó c es una unidad y, por tanto, a es irreducible.

c) Si $\mathcal{M}$ es un ideal del dominio principal A, existe $u\in A / \mathcal{M}=(u)$.
Entonces, [$\mathcal{M}=(u)$ es maximal] $\overset{a)}{\Leftrightarrow}$ [u es irreducible] $\overset{b)}{\Leftrightarrow}$ [u es primo] $\overset{\text{Prop. 1.5.}}{\Leftrightarrow}$ [$\mathcal{M}$ es un ideal primo]. c.s.q.d.

2. Dominio de factorización única.

Definición: Un dominio de integridad A se dice un dominio de factorización única si se verifican las proposiciones sifuientes:

a) Cada elemento $a \in A$ admite una descomposición como producto de elementos irreducibles: $a = p_1 \cdots p_n$, si a no es una unidad.

b) Esta descomposición es única, salvo unidades (*)

Si $p_1 \cdots p_n$ es "la" descomposición de un elemento $a \in A$ como producto de elementos irreducibles, agrupando en potencias los elementos irreducibles que sean iguales, salvo unidades, podemos escribir $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

* Máximo común divisor y mínimo común multiplo en un dominio de factorización única:

Sea D un dominio de factorización única (D.F.U.) y a y b dos elementos de D que no sean unidades. Sean $a = t_1^{\alpha_1} \cdots t_k^{\alpha_k}$ y $b = q_1^{\beta_1} \cdots q_s^{\beta_s}$ las descomposiciones de a y b como producto de elementos irreducibles. Con el convenio $p^0 = 1$, podemos suponer que en estas descomposiciones aparecen los mismos elementos irreducibles y escribir

$$a = p_1^{\mu_1} \cdots p_r^{\mu_r} \quad \text{y} \quad b = p_1^{\nu_1} \cdots p_r^{\nu_r}, \quad \mu_i, \nu_i \geq 0, \ 1 \leq i \leq r.$$

Definimos entonces el máximo comun divisor de a y b como

$$mcd(a,b) = p_1^{\lambda_1} \cdots p_r^{\lambda_r}, \text{ donde } \lambda_i = \min(\mu_i, \nu_i), \ 1 \leq i \leq r.$$

Definimos el mínimo común múltiplo de a y b como

$$mcm(a,b) = p_1^{\sigma_1} \cdots p_r^{\sigma_r}, \text{ donde } \sigma_i = \max(\mu_i, \nu_i), \ 1 \leq i \leq r.$$

El máximo común divisor y el mínimo común múltiplo de dos elementos son únicos salvo unidades

Propiedades: ① Si $d = mcd(a,b)$, y c es un divisor común de a y b entonces $c \mid d$

② Si $m = mcm(a,b)$ y c es un múltiplo común de a y b, entonces $m \mid c$.

2.1 Teorema: Todo dominio de ideales principales es un dominio de factorización única (D.F.U.)

Demostr.: Sea D un dominio de ideales principales y a un elemento de D que no sea unidad. Si a es irreducible, trivialmente a admite una única descomposición como producto de factores irreducibles. Si a no es irreducible, $a = a_1 \cdot b_1$ donde a_1 y b_1 son divisores propios de a. Si a_1 y b_1 son irreducibles queda proba-

(*) Es decir, en las descomposiciones de un mismo elemento a los elementos irreducibles que intervienen son asociados.

do que a admite una descomposición. Si a_1 no es irreducible, $a_1 = a_2 \cdot b_2$; si a_2 y b_2 son irreducibles y, b_1 también, queda vista la "existencia" de la descomposición. Si no, procedemos de esta manera sucesivamente. Probemos que este proceso no puede ser infinito.
Según lo dicho, $(a) \subset (a_1) \subset (a_2) \subset \dots$ Entonces, trivialmente, $(a) \cup (\bigcup_{i \geq 1} (a_i))$ es un ideal de D. Siendo D un dominio principal, existe $d \in D$ tal que $(a) \cup (\bigcup_{i \geq 1} (a_i)) = (d)$.
Entonces, para un cierto $n \geq 0$ $(a = a_0)$, $d \in (a_n)$. Por otra parte, $a_n \in (d)$. Luego $(d) = (a_n)$. Por tanto, a partir de n todos los ideales de esta cadena son iguales a (d). Entonces, a_n debe ser irreducible, pues de lo contrario $a_n = a_{n+1} \cdot b_{n+1}$ donde a_{n+1} ni es una unidad ni un asociado de a_n y se tendría $(a_n) \subset (a_{n+1})$ y $(a_n) \neq (a_{n+1})$ contra lo probado. Entonces

$$a = a_1 \cdot b_1 = a_2 \cdot b_2 b_1 = a_3 b_3 b_2 b_1 = \dots = a_n \cdot b'_1 = p_1 b'_1$$

donde b' es el producto $b_n \cdots b_1$ y $p_1 = a_n$ es irreducible.
Haciendo lo mismo con b'_1 probamos que $b'_1 = p_2 \cdot b'_2$ donde p_2 es irreducible. Así sucesivamente, probamos que:

$$a = p_1 p_2 \cdots p_s \cdot b'_s$$

Del mismo modo que antes se prueba que este proceso es finito, y por tanto, que existe un r tal que b'_r es irreducible. (*)
Luego, a admite una descomposición como producto de factores irreducibles.
Probemos que la descomposición es única salvo unidades.
Sean $p_1 p_2 \cdots p_s$ y $q_1 q_2 \cdots q_t$ dos descomposiciones de un mismo elemento $a \in D$ como producto de factores irreducibles y supongamos $t \leq s$.
Si $q_1 | a$ y $a = p_1 p_2 \cdots p_s \Rightarrow q_1 | p_1 p_2 \cdots p_s$. Siendo q_1 irreducible y D un dominio principal, se tiene que $q_1 | p_1$ ó $q_1 | p_2$ ó $\dots$ ó $q_1 | p_s$ (**).
Siendo D conmutativo podemos suponer, sin perder generalidad, que $q_1 | p_1$.
Como q_1 y p_1 son irreducibles deben ser asociados, es decir, $p_1 = u_1 q_1$, siendo u_1 una unidad. Del mismo modo, $p_2 = u_2 q_2, \dots, p_t = u_t q_t$, siendo u_i unidades.
Si hacemos $u = u_1 \cdots u_t$, tenemos que:
$a = q_1 \cdots q_t p_{t+1} \cdots p_s u$. Siendo $a = q_1 \cdots q_t$, se deduce que $p_{t+1} \cdots p_s \cdot u = 1$. Debe ser entonces $t = s$, pues si $t < s$ sería $p_{t+1} \cdots p_s$ una unidad, lo cual es absurdo pues un producto de factores irreducibles no puede ser una unidad (pues entonces cada uno

de los factores serían unidades y suponemos que un elemento irreducible no es una unidad). Por tanto, la descomposición de a como producto de factores irreducibles es única salvo unidades. c.s.q.d.

3. Anillo primo. Característica de un anillo.

Definición (Subanillo primo de un anillo).

Sea A un anillo conmutativo y unitario. Definimos el subanillo primo de A como el menor subanillo de A que contiene a 1.

El menor subanillo de un anillo unitario existe siempre y es la intersección de los subanillos de A que contienen a 1.

* Consideremos la aplicación

$$\phi : \mathbb{Z} \longrightarrow A$$
$$n \longmapsto \phi(n) = n \cdot 1_A = 1_A + \overset{n}{\dots} + 1_A$$

donde 1_A es el elemento neutro del producto en A.

ϕ es un homomorfismo de anillos, pues, trivialmente, $(n+m)\cdot 1_A = n1_A + m1_A$ y $(n\cdot m)\cdot 1_A = (n\cdot 1_A)(m\cdot 1_A)$

Sea $\mathbb{Z}\cdot 1_A = \{n\cdot 1_A / n\in\mathbb{Z}\} = \operatorname{Im}\phi$. Entonces $\mathbb{Z}\cdot 1_A$ es el subanillo primo de A, pues $\mathbb{Z}\cdot 1_A = \operatorname{Im}\phi$ es subanillo de A, contiene a 1_A, pues $\phi(1) = 1_A$, y si S es un subanillo de A que contiene a 1_A, entonces $n\cdot 1_A \in S$, $\forall n\in\mathbb{Z}$; luego $S \supset \mathbb{Z}\cdot 1_A$.

Siendo $\mathbb{Z}\cdot 1_A = \operatorname{Im}\phi$, se tiene que:

$$\mathbb{Z}\cdot 1_A \simeq \mathbb{Z}/\ker\phi$$

$\ker\phi$ es un ideal de $\mathbb{Z}$, que es un anillo principal; luego existe $K\in\mathbb{Z}$ tal que $\ker\phi = (K)$. Entonces

$$\mathbb{Z}\cdot 1_A \simeq \mathbb{Z}/(K)$$

K puede ser 0, si ϕ es inyectiva. En este caso decimos que la característica de A es cero. Si $K\neq 0$, decimos que A es de característica K.

Si A es de característica $K\neq 0$ se tiene que $K\cdot 1_A = 1_A + \overset{K}{\dots} + 1_A = 0$, pues $\bar{K} = \bar{0}$ y $\mathbb{Z}\cdot 1_A$ es isomorfo a $\mathbb{Z}/(K) = \mathbb{Z}_K$

Si A es de característica 0, $\mathbb{Z}\cdot 1_A$ es isomorfo $\mathbb{Z}$ y se tiene que $n\cdot 1_A \neq 0$ si $n\neq 0$.

- Sea A un anillo íntegro. Entonces la característica de A es cero o un número primo, pues $\mathbb{Z}\cdot 1_A \simeq \mathbb{Z}/(k)$ y si K no es primo, $\mathbb{Z}/(K)$ no es íntegro ($K = p\cdot q \Rightarrow \bar{p}\cdot\bar{q} = \bar{K} = \bar{0}$) y, por tanto

en $\mathbb{Z}\cdot 1_A \subset A$ hay divisores de cero, en contra de que A es íntegro.

4. Cuerpo de fracciones sobre un dominio de integridad

Sea D un dominio de integridad y $D^* = D - \{0\}$. Consideremos el conjunto producto $D \times D^*$. Definimos en él una relación de equivalencia, que denotamos por $\sim$, del siguiente modo:

$$(a,b) \sim (a',b') \Leftrightarrow ab' = ba'.$$

La clase de representante (a,b) la denotaremos por $\frac{a}{b}$, y diremos de ella que es una fracción. En el conjunto cociente $D \times D^*/\sim$ definimos dos leyes de composición interna del siguiente modo:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \qquad \text{y} \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

Se comprueba fácilmente que están bien definidas (no dependen de los representantes elegidos) y que $(D \times D^*/\sim ; +, \cdot)$ es un cuerpo. El elemento unidad es $\frac{1}{1}$ y el neutro de la suma es $\frac{0}{a}$, $a \in D^*$.

Se dice que $K = D \times D^*/\sim$ es el cuerpo de fracciones del dominio de integridad D.

Se puede considerar D "contenido" en K mediante el homomorfismo inyectivo

$$\begin{aligned} \varphi : D &\longrightarrow K \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

4.1. Proposición: Sea F un cuerpo y A un subanillo de F (*). Sea K el cuerpo de fracciones de A. Si llamamos $F_0 = \{ab^{-1} / b \neq 0, a,b \in A\}$ entonces F_0 es un subcuerpo de F isomorfo a K.

Demostr.: - F_0 es subcuerpo de F, pues

$$ab^{-1}, a'b'^{-1} \in F_0 \Rightarrow \begin{cases} ab^{-1} - a'b'^{-1} = ab b'^{-1} b^{-1} - a' b b^{-1} b'^{-1} = (ab' - a'b)(bb')^{-1} \in F_0 \\ ab^{-1} \cdot (a'b')^{-1} = ab^{-1} b'^{-1} a'^{-1} = ab' \cdot (a'b)^{-1} \in F_0, \text{ pues si} \\ a'b'^{-1} \neq 0 \Rightarrow a' \neq 0 \Rightarrow a'b \neq 0, \text{ ya que } b \neq 0. \end{cases}$$

Es más, F_0 es el menor subcuerpo de F que contiene a A, pues si F_1 es un subcuerpo de F que contiene a A, entonces

$$\forall a, b \in A,\ b \neq 0,\ ab^{-1} \in F_1 \Rightarrow F_0 \subset F_1.$$

- Se prueba fácilmente que la aplicación

$$\begin{aligned} \varphi : K &\longrightarrow F_0 \\ \frac{a}{b} &\longmapsto ab^{-1} \end{aligned}$$

es un isomorfismo de cuerpos. c.s.q.d.

5. CARACTERISTICA DE UN CUERPO. SUBCUERPO PRIMO DE UN CUERPO.

DEFINICION: La característica de un cuerpo F es la característica de F considerado como anillo.

Siendo todo cuerpo un dominio de integridad se deduce que la característica de F o es cero, o es un número primo p.

Si F es de característica p, $\mathbb{Z}\cdot 1_F \simeq \mathbb{Z}/(p) = \mathbb{Z}_p$.

Siendo p primo, $\mathbb{Z}_p$ es un cuerpo. Luego $\mathbb{Z}\cdot 1_F$, que es el subanillo primo de F, es un subcuerpo de F.

DEFINICION: Se llama subcuerpo primo de un cuerpo F al menor subcuerpo de F.

Luego si la característica de F es p, $\mathbb{Z}\cdot 1_F$ es el subcuerpo primo de F.

Si F es de característica nula, $\mathbb{Z}\cdot 1_F \simeq \mathbb{Z}$. Entonces, el menor subcuerpo que contiene a $\mathbb{Z}\cdot 1_F$ es isomorfo al cuerpo de fracciones de $\mathbb{Z}$, que es $\mathbb{Q}$.

II. POLINOMIOS

6. DEFINICION

Sea A un anillo conmutativo y unitario y $P(A)$ el conjunto de las sucesiones en A en las que solo un número finito de términos son distintos de cero. Definimos en $P(A)$ las operaciones internas:

$(a_n) + (b_n) = (c_n)$ siendo $c_n = a_n + b_n$.

$(a_n)\cdot(b_n) = (d_n)$ siendo $d_n = \sum_{i+j=n} a_i b_j$.

6.1. PROPOSICION: a) $(P(A); +, \cdot)$ es un anillo con elemento unidad (e_n), siendo $e_0 = 1$ y $e_n = 0$ si $n \neq 0$.

b) La aplicación $\alpha : a \in A \longmapsto \alpha(a) = \bar{a} = (a, 0, \dots, 0, \dots)$ es un monomorfismo de anillos.

c) Si representamos $x = (0, 1, 0, \dots, 0, \dots)$, entonces

$$\forall k \in \mathbb{N},\quad x^k = (0, \dots, 0, \underset{k+1}{1}, 0, \dots)$$

d) Para cada $f \in P(A) - \{0\}$, existe una única sucesión finita $\langle a_0, a_1, \dots, a_n \rangle$, $a_i \in A$, tal que

$$f = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n$$

siendo, por lo menos, $a_n \neq 0$.

La demostración es trivial.

Denotaremos $P(A) \equiv A[x]$ y diremos que $A[x]$ es el anillo de los polinomios en la indeterminada x. Escribiremos, si $f(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$, por la identificación $\bar{a}_0 = a_0$.

DEFINICION: (Grado de un polinomio)
Si $f(x) \in A[x]$ se puede escribir en la forma $f(x) = a_0 + a_1 x + \dots + a_n x^n$ con $a_n \neq 0$, se dice que $f(x)$ es un polinomio de grado n. Si $f \neq 0$ y $f(x) = a_0$, es decir, si f es un polinomio constante, diremos que f es de grado cero, por el convenio $x^0 = 1$.

6.2. PROPOSICION: a) Si f y g son polinomios no nulos, el grado de $f+g$ es menor o igual que $\max\{\text{grado } f, \text{grado } g\} = \max\{\partial^\circ(f), \partial^\circ(g)\}$ (*)
b) Si A es integro y $f, g \in A[x] - \{0\}$, entonces $\partial^\circ(f \cdot g) = \partial^\circ(f) + \partial^\circ(g)$.

(Ver demostración en ALGEBRA I).
Si queremos que estas fórmulas sigan siendo ciertas cuando se trate del polinomio 0 haremos el convenio $\partial^\circ(0) = -\infty$ (pues si $f = a$, $g = -a$, $\partial^\circ 0 = \partial^\circ(f+g) \leq \partial^\circ(f) + \partial^\circ(g) = 0$ y $\partial^\circ(0) = \partial^\circ(0 \cdot g) = \partial^\circ(0) + \partial^\circ(g)$, y si $\partial^\circ(0)$ fuese un número debería ser $\partial^\circ g = 0$ cualquiera que fuese g, lo cual no es cierto; por eso hacemos, por ¡convenio!, $\partial^\circ(0) = -\infty$).

6.3. PROPOSICION: Si A es íntegro, entonces $A[x]$ es íntegro y las unidades de $A[x]$ son las mismas que las de A.

Demostr.: - Sean $f(x), g(x) \in A[x]$ tales que $f(x) \cdot g(x) = 0$.
Sean $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + b_1 x + \dots + b_m x^m$, $a_n, b_m \neq 0$.
Si $f(x) \cdot g(x) = 0$, entonces $a_n b_m = 0$, con $a_n \neq 0$ y $b_m \neq 0$, en contra de que A es íntegro. Luego $f(x) = 0$ ó $g(x) = 0$.
- Si u es unidad de A, entonces u es unidad de $A[x]$ pues $A \subset A[x]$.
Sea $f(x)$ una unidad de $A[x]$. Entonces existe $g(x) \in A[x]$ tal que $f(x) g(x) = 1$. Siendo $\partial^\circ(f \cdot g) = \partial^\circ f + \partial^\circ g$ se tiene que $\partial^\circ f + \partial^\circ g = 0$ y, por tanto, $\partial^\circ(f) = 0$ y $\partial^\circ(g) = 0$.
Luego f y g son constantes: $f = a_0$, $g = b_0$.
Entonces, $a_0 b_0 = 1$. Luego, a_0 es unidad de A y, por tanto, f es unidad de A. c.q.d.

DEFINICION: Se dice que un polinomio no nulo $f(x)$ es mónico si el coeficiente del término de mayor grado es 1 (o una unidad).

6.4. TEOREMA: (Algoritmo de Euclides)

Sean $f(x)$ y $g(x)$ dos polinomios no nulos con coeficientes en un anillo A íntegro, conmutativo y unitario. Supongamos que $g(x)$ es mónico. Entonces existen dos polinomios $q(x)$ y $r(x)$ en $A[x]$ tales que

$$f(x) = q(x)\cdot g(x) + r(x) \quad \text{y} \quad \partial^\circ(r) < \partial^\circ g.$$

Además $q(x)$ y $r(x)$ son únicos.

(Ver demostración en ALGEBRA I, TEMA 15).

6.5. PROPOSICION: Dado $a \in A$ la aplicación:

$$\phi_a : f(x) = a_0 + a_1x + \dots + a_nx^n \in A[x] \longmapsto \phi_a(f(x)) = a_0 + a_1a + \dots + a_na^n \in A.$$

es un homomorfismo de anillos. Denotaremos $f(a) \equiv \phi_a(f(x))$. (*)

6.6. PROPOSICION: Sea a un elemento del anillo A y $f(x) \in A[x] - \{0\}$. Entonces existe un único $q(x) \in A[x]$ tal que $f(x) = (x-a)q(x) + f(a)$.

Demostr.: Sea $g(x) = x - a$. Entonces, por TEOREMA 6.4, existen $q(x), r(x) \in A[x]$ tal que $f(x) = (x-a)q(x) + r(x)$, $\partial^\circ(r) < \partial^\circ(g)$.
Entonces, $f(a) = (a-a)q(a) + r(a) = r(a)$.
Además, siendo $\partial^\circ(g) = 1$ y $\partial^\circ(r) < \partial^\circ(g)$ se deduce que r es constante, es decir, $r(x) = f(a)$.

6.7. TEOREMA: (DEL RESTO)

Dados $f(x) \in A[x]$ y $a \in A$ se tiene que $(x-a)$ divide a $f(x)$ si y solo si $f(a) = 0$.

Demostr.: $\Rightarrow$| Si $(x-a) \mid f(x)$, $\exists q(x) \in A[x]$ / $f(x) = (x-a)q(x)$.
Dada la unicidad del cociente y el resto y, segun la proposición anterior, se deduce que $f(a) = 0$.
$\Leftarrow$| Dados: $f(x), x-a \in A[x]$, $\exists q(x) \in A[x]$ / $f(x) = q(x)(x-a) + f(a)$
Si $f(a) = 0$, entonces $(x-a) \mid f(x)$. c.s.q.d.

DEFINICION: (raiz de un polinomio)

Se dice que a es una raiz de un polinomio $f(x) \in A[x]$ sobre A si $a \in A$ y $f(a) = 0$.

El concepto de raiz de un polinomio se puede ampliar tambien para elementos de cualquier extensión de A (anillo que contenga a A como subanillo). Sea A un anillo y A' una extensión de A; decimos que $a \in A'$ es una

raiz de $f(x) \in A[x]$ si $f(a)=0$.

6.8. TEOREMA: Sea F es un cuerpo y $f(x)$ un polinomio no nulo con coeficientes en F y de grado n. Entonces f tiene, a lo sumo, n raíces distintas sobre F.

Demostr.: Probemos fue si $a_1, \dots, a_r$ son r raices distintas de $f(x)$, entonces $\prod_{i=1}^{r}(x-a_i) \mid f(x)$. Procederemos por inducción sobre r:

- Si $r=1$, $(x-a_1) \mid f(x)$, por el teorema del resto.
- Supuesto que $\prod_{i=1}^{r-1}(x-a_i) \mid f(x)$, se tiene fue existe $h(x) \in F[x]$ tal que $f(x) = h(x) \cdot \prod_{i=1}^{r-1}(x-a_i)$.

Si a_r es raiz de $f(x)$, entonces $f(a_r)=0$.
Luego $h(a_r) \cdot \prod_{i=1}^{r-1}(a_r-a_i)=0$.
Siendo $a_r - a_i \neq 0$, $1 \leq i \leq r-1$, $\prod_{i=1}^{r-1}(a_r-a_i) \neq 0$, pues F es íntegro.
Entonces debe ser $h(a_r)=0$.
Por el teorema del resto, $(x-a_r) \mid h(x)$.
Luego, $\prod_{i=1}^{r}(x-a_i) \mid f(x)$. Entonces $\exists K(x) \in F[x] / f(x) = \prod_{i=1}^{r}(x-a_i) \cdot K(x)$.
Portanto, $n = \partial^\circ(f) = \partial^\circ(\prod_{i=1}^{r}(x-a_i)) + \partial^\circ(K(x)) = r + \partial^\circ(K(x))$.
Siendo $\partial^\circ(K(x)) \geq 0$ se deduce que $r \leq n$. c.s.g.d.

6.9. COROLARIO: Sea F un cuerpo y $f(x) \in F[x]$. Si T es un subconjunto infinito de F de modo que $\forall a \in T, f(a)=0$, entonces $f(x)$ es el polinomio cero.

Demostr.: Si $f(x) \neq 0$, el grado de f es finito. Segun el teorema anterior, el número de raíces distintas de f será finito, en contra de que se anula para los elementos de un conjunto infinito. Debe ser entonces $f(x)=0$. c.s.g.d.

6.10. COROLARIO: Sean $f(x)$ y $g(x)$ dos polinomios de grado n con coeficientes en un cuerpo F. Si f y g coinciden en $n+1$ puntos distintos de F entonces $f=g$.

Demostr.: Consideremos el polinomio $f-g$. Si $f-g \neq 0$, tenemos que $f-g$ tiene $n+1$ raices distintas sobre F y $\partial^\circ(f-g) \leq \max\{\partial^\circ(f), \partial^\circ(g)\} = n$, lo cual contradice lo probado en TEOREMA 6.8. Por tanto, debe ser $f-g=0$. c.s.g.d.

6.11. COROLARIO: Sea F un cuerpo. Entonces, todo subgrupo finito del grupo multiplicativo de F es cíclico. En particular, si F es finito, $F^* = F - \{0\}$ es un grupo cíclico multiplicativo. (*)

Demostr.: Sea G un subgrupo finito multiplicativo de F. Entonces G es suma directa de sus p-subgrupos de Sylow (Tema 6º, TEOREMA 2.2.):

$$G = S(p_1) \oplus \dots \oplus S(p_k)$$

Si probamos que cada $S(p_i)$ es cíclico quedará visto que G es cíclico por Teorema 1.7., Tema 5º. Sea p un número primo que divide a $o(G)$. Veamos que $S(p)$ es cíclico. Siempre podemos encontrar en $S(p)$ un elemento a de orden maximal, pues los elementos de $S(p)$ tienen de orden una potencia de p entre las cuales podemos tomar siempre la mayor y un elemento de $S(p)$ cuyo orden sea dicha potencia. Sea $o(a) = p^r$. Consideremos el polinomio $x^{p^r} - 1$ sobre F.

Como $\forall b \in S(p)$, $b^{p^r} = 1$, pues p^r es el mayor de los órdenes de los elementos de $S(p)$ y dado $b \in S(p)$, $o(b) \mid p^r$, se tiene que los elementos de $S(p)$ son raíces de dicho polinomio. Como el polinomio $x^{p^r} - 1$ es de grado p^r, tiene u raíces sobre F con $u \leq p^r$. Entonces, debe ser $u = p^r$ ya que, por otra parte $u \geq p^r$ pues $o(S(p)) \geq o(\langle a \rangle) = p^r$ y los elementos de $S(p)$ son raíces de dicho polinomio. En consecuencia, $p^r = o(\langle a \rangle) \leq o(S(p)) \leq u = p^r \Rightarrow$

$\Rightarrow o(S(p)) = p^r$ y, por tanto, $S(p) = \langle a \rangle$.

En definitiva, según se indicó anteriormente, G es cíclico. c.s.q.d.

6.12. TEOREMA: Si F es un cuerpo, $F[x]$ es dominio de ideales principales.

Demostr.: Siendo F íntegro, $F[x]$ es íntegro. Veamos que todo ideal de $F[x]$ es principal. Sea I un ideal de $F[x]$.

Si $I = \{0\}$, entonces $I = (0)$. Supongamos entonces que $I \neq \{0\}$. Sea $f(x)$ un polinomio de $I - \{0\}$ de grado mínimal y mónico, que siempre existe, pues si $a_0 + a_1 x + \dots + a_n x^n$ es un polinomio de grado mínimal multiplicando por a_n^{-1} obtenemos un polinomio mónico de grado mínimal. Probemos que $I = (f(x))$.

Sea $g(x) \in I - \{0\}$. Entonces existen $q(x), r(x) \in F[x]$ tal que

$$g(x) = f(x) \cdot q(x) + r(x) \quad \text{con } \partial^\circ(r) < \partial^\circ(f).$$

Como $f(x) \in I$ e I es ideal se tiene que $q(x) \cdot f(x) \in I$. Además $g(x) \in I$. Luego $r(x) = g(x) - f(x) \cdot q(x) \in I$. Siendo $\partial^\circ(r) < \partial^\circ(f)$

f un polinomio de grado mínimal en $I-\{0\}$ debe ser $r(x)=0$.
Luego, $g(x)=f(x)\cdot q(x) \Rightarrow g(x)\in(f(x))$.
Por tanto, $I=(f(x))$.
En definitiva, todo ideal de $F[x]$ es principal. cqd.

6.13. TEOREMA: Si F es un cuerpo, $F[x]$ es un dominio de factorización única, es decir, todo polinomio con coeficientes en F se escribe de manera única (salvo unidades) como producto de polinomios irreducibles

Es consecuencia inmediata del teorema anterior y del teorema 2.1.
La unicidad de la descomposición es salvo unidades de $F[x]$, que son las mismas que las de F, que son los elementos de $F-\{0\}$, pues F es cuerpo.

6.14. COROLARIO: a) Un polinomio $f(x)\in F[x]$ es irreducible si y solo si es primo, si F es cuerpo
b) Si F es cuerpo son equivalentes las proposiciones siguientes
① $f(x)\in F[x]$ es irreducible
② $(f(x))$ es un ideal maximal
③ $(f(x))$ es un ideal primo.
④ $F[x]/(f(x))$ es un cuerpo.

Es consecuencia inmediata del teorema 6.12 y las proposiciones 1.2 y 1.6.

7. Si D es D.F.U entonces $D[x]$ es D.F.U.

7.1. Lema: Sea D un D.F.U. Entonces todo elemento irreducible es primo.
Demostr.: Sea π un elemento irreducible de D.
Supongamos que $\pi \mid a\cdot b$, $a,b\in D$. Entonces $\exists K\in D / a\cdot b = K\cdot\pi$.
Si descomponemos a y b en producto de factores irreducibles obtenemos una descomposición de $K\cdot\pi$ en producto de factores irreducibles.
Siendo π irreducible y la descomposición única, se deduce que π aparece en la descomposición de a o en la de b, es decir, $\pi \mid a$ ó $\pi \mid b$. cqd.

DEFINICION: (Polinomio primitivo).
Sea D un D.F.U y $f(x)\in D[x]$. Si $f(x)=a_0+a_1x+\dots+a_nx^n$ decimos que $f(x)$ es un polinomio primitivo si $mcd(a_0,a_1,\dots,a_n)=1$ (salvo unidades).

DEFINICION: (Contenido de un polinomio).
Sea D un D.F.U y $f(x)\in D[x]$. Definimos el contenido de f como
$$cont(f)=mcd(a_0,a_1,\dots,a_n).$$

7.2. Lema: Si D es D.F.U, todo polinomio $f(x) \in D[x] - \{0\}$ se puede escribir en la forma $f = c \cdot f^*$ siendo $c = cont(f)$ y f^* un polinomio primitivo.

Demostr.: Supongamos que $f(x) = a_0 + a_1 x + \dots + a_n x^n$ y sea $c = cont(f)$.
Entonces dado $i \in \{0,1,\dots,n\}$, existe $a_i^* \in D$ tal que $a_i = c \cdot a_i^*$
Entonces, si $f^*(x) = a_0^* + a_1^* x + \dots + a_n^* x^n$ tenemos que $f = c \cdot f^*$.
Veamos que f^* es primitivo.
Sea $c^* = cont(f^*)$. Entonces dado $i \in \{0,1,\dots,n\}$, $\exists b_i \in D / a_i^* = c^* b_i$.
Entonces $a_i = cc^* \cdot b_i$. Luego $cc^* | a_i$, $0 \le i \le n$
Por tanto, $cc^* | c = cont(f)$. Como además $c | cc^*$ se tiene que c y cc^* son asociados y, por tanto, c^* es una unidad, que prueba que f^* es primitivo.

7.3. Lema: Si $f = d \cdot f_1$, siendo f_1 primitivo y $d \in D$ (D.F.U), entonces $d = cont(f)$ y f_1 es asociado a f^* (con la notación del lema anterior).

Demostr.: Siendo $mcd(da, db) = d \cdot mcd(a,b)$ tenemos que
$cont(f) = cont(d f_1) = d \cdot cont(f_1) = d \cdot u$, pues f_1 es primitivo, siendo u una unidad.
Además $f = cont(f) \cdot f^* = ud \cdot f_1$
Luego $f^* = u \cdot f_1$. c.s.q.d.

7.4. Lema: Sea D un D.F.U y F el cuerpo de fracciones de D. Sea $f \in F[x]$. Entonces existe $\gamma \in F$, y es único salvo unidades de D, tal que $f = \gamma \cdot f^*$ donde f^* es un polinomio primitivo de $D[x]$.

Demostr.: Sea $f(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n$, con $\alpha_i = \frac{a_i}{b_i}$, siendo $(a_i, b_i) \in D \times D^*$.
Sea $b = \prod_{i=1}^{n} b_i$. Entonces $b \cdot f \in D[x]$
Luego $b \cdot f$ se puede escribir $b \cdot f = c \cdot f^*$, $c = cont(b \cdot f)$ y f^* es un polinomio primitivo de $D[x]$.
Entonces $f = \frac{c}{b} \cdot f^*$, pues $b \neq 0$. Haciendo $\gamma = \frac{c}{b}$ queda probada la existencia.
Supongamos que $f = \delta \cdot f_1$ siendo f_1 primitivo en $D[x]$ y $\delta \in F$.
Entonces existe $(d,e) \in D \times D^*$ tal que $\delta = \frac{d}{e}$.
Luego $\frac{d}{e} f_1 = \frac{c}{b} f^* \Rightarrow db \cdot f_1 = ce \cdot f^*$.
Siendo $db, ce \in D$ y f_1 y f^* primitivos en $D[x]$ son asociados. Luego $db = uce$, donde u es una unidad de D.
En definitiva $\frac{d}{e} = u \cdot \frac{c}{b} = u\gamma$, que prueba que γ es único salvo unidades de D. c.s.q.d.

DEFINICION: Sea D un D.F.U. y F el cuerpo de fracciones de D. Dado $f \in F[x]$ definimos el contenido de f a $\gamma \in F$ tal que $f = \gamma \cdot f^*$, siendo f^* un polinomio primitivo de $D[x]$.

Sabemos por el teorema anterior que γ es único salvo unidades de D.

7.5. Lema: (de Gauss)

> Sea D un D.F.U. y f y g polinomios de $D[x]$ primitivos. Entonces, $f \cdot g$ es primitivo.

Demostr.: Sea $\pi \in D$ un elemento irreducible. Siendo f primitivo, $\text{cont}(f) = 1$; luego existe un coeficiente de f que no es divisible por π. Análogamente, existe un coeficiente de g que no es divisible por π. Sea a_i el primer coeficiente de f que no es divisible por π y sea b_j el primer coeficiente de g que no es divisible por π. Veamos que π no divide al coeficiente c_{i+j} del término en x^{i+j} de $f \cdot g$.

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + \dots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \dots + a_{i+j} b_0)$$

Como $a_0, a_1, \dots, a_{i-1}$ son divisibles por π, pues así hemos tomado a_i, el primer paréntesis es divisible por π. Además, $b_{j-1}, \dots, b_0$ son divisibles por π; luego el segundo paréntesis también es divisible por π. Entonces, c_{i+j} no es divisible por π, pues si lo fuese se tendría que $\pi \mid a_i b_j$. Siendo D un D.F.U, π es primo. Entonces, $\pi \mid a_i$ ó $\pi \mid b_j$ en contra de que $\pi \nmid a_i$ y $\pi \nmid b_j$. Luego $\pi \nmid c_{i+j}$.

Por tanto, ningún elemento irreducible divide a todos los coeficientes de $f \cdot g$. Luego si $f \cdot g = c_0 + c_1 x + \dots + c_{m+n} x^{m+n}$, $\text{mcd}(c_0, \dots, c_{m+n}) = 1$ pues si $\text{cont}(f \cdot g)$ no es una unidad, existiría al menos un elemento irreducible que lo dividiría, ya que D es D.F.U. Por tanto, $f \cdot g$ es primitivo. c.s.q.d.

7.6. TEOREMA: Sea D un D.F.U y F el cuerpo de fracciones de D

> a) Si $f \in D[x]$ es irreducible y no constante, entonces f es irreducible en $F[x]$.
>
> b) Si $f \in D[x]$ es primitivo e irreducible en $F[x]$, entonces f es irreducible en $D[x]$.

Demostr: a) Sea f un polinomio irreducible y no constante en $D[x]$. Supongamos que $f = f_1 \cdot f_2$ siendo $f_1, f_2 \in F[x]$. Según lema 7.4, $f_1 = \gamma_1 f_1^*$ y $f_2 = \gamma_2 \cdot f_2^*$ siendo f_1^* y f_2^* primitivos en $D[x]$ y $\gamma_1, \gamma_2 \in F$. Por el lema de Gauss, $f_1^* \cdot f_2^*$ es primitivo en $D[x]$,

Como $f = \gamma_1 \gamma_2 f_1^* f_2^*$ y f y $f_1^* f_2^*$ son primitivos en $D[x]$, $u = \gamma_1 \cdot \gamma_2$ es una unidad de D. Como f es irreducible en $D[x]$ y $f_1^*, f_2^* \in D[x]$, se tiene que f_1^* ó f_2^* es una unidad de D. Por tanto, ó f_1 ó f_2 es constante en $F[x]$. Siendo las constantes en $F[x]$ unidades de $F[x]$, tenemos que f es irreducible en $F[x]$.

b) Sea f un polinomio primitivo en $D[x]$ e irreducible en $F[x]$; por tanto, f no es constante (un polinomio constante en $F[x]$ es una unidad en $F[x]$ y, por tanto, no irreducible).

Supongamos que $f = f_1 \cdot f_2$, con $f_1, f_2 \in D[x]$.

Como $F \supset D$, $f_1 \cdot f_2$ es una descomposición de f en $F[x]$.

Entonces, por hipótesis, ó f_1 ó f_2 es una unidad en $F[x]$. Supongamos que f_1 es unidad en $F[x]$. Entonces, $f_1 \in F$.

Como los coeficientes de f_1 pertenecen a D, pues $f_1 \in D[x]$, se tiene que $f_1 \in D$.

Sea $f_2 = c_2 \cdot f_2^*$, siendo $c_2 = \text{cont}(f_2)$ y f_2^* un polinomio primitivo. Siendo $f = c_2 f_1 f_2^*$ y f_2^* primitivos, se deduce que, salvo unidades, $c_2 f_1 = \text{cont}(f)$ y, por tanto, $c_2 f_1$ es una unidad de D, pues f es primitivo. Luego, f_1 es una unidad de D (*)

Por tanto, f es irreducible en $D[x]$. c.s.q.d.

7.7. TEOREMA: Si D es un dominio de factorización única, entonces $D[x]$ es dominio de factorización única.

Demostr.: *Sea f un polinomio no unidad de $D[x]$. Veamos que f admite una descomposición como producto de factores irreducibles.

Si f es constante, es decir, si $f \in D$, admite una descomposición como producto de factores irreducibles de D, $f = \pi_1 \pi_2 \cdots \pi_n$, siendo π_i irreducible en D. Veamos que si π es irreducible en D es irreducible en $D[x]$ y quedará visto que si f es constante admite una descomposición como producto de factores irreducibles de $D[x]$. Sea π irreducible en D y supongamos que $\pi = g \cdot h$, $g, h \in D[x]$. Entonces $0 = \partial^\circ(\pi) = \partial^\circ(h) + \partial^\circ(g) \Rightarrow \partial^\circ(h) = \partial^\circ(g) = 0$. Luego $h, g \in D$ y, por tanto, ó h ó g es una unidad, que prueba que π es irreducible en $D[x]$.

Supongamos que f no es constante; entonces $\partial^\circ f \geq 1$. Si F es el cuerpo de fracciones de D se tiene que $f \in F[x]$, pues $D[x] \subset F[x]$. Siendo F cuerpo, $F[x]$ es D.F.U. Luego

$f = f_1 f_2 \cdots f_n$, donde f_i es irreducible en $F[x]$

Sea, para cada $i \in \{1, \dots, n\}$, $f_i = a_i f_i^*$ donde $a_i = \text{cont}(f) \in F$ y f_i^* es primitivo en $D[x]$.

Si f_i es irreducible en $F[x]$, f_i^* es irreducible en $F[x]$, pues a_i es una unidad de $F[x]$. Siendo f_i^* primitivo e irreducible en $F[x]$, es irreducible en $D[x]$.

Siendo $f = (a_1 \cdots a_n) f_1^* \cdots f_n^*$ y $f_1^* \cdots f_n^*$ primitivo (Lema de Gauss), $a_1 \cdots a_n = \text{cont}(f)$, salvo unidades

Como f es un polinomio con coeficientes en D, $\text{cont}(f) \in D$.

Luego $a = a_1 \cdots a_n \in D$. Siendo D un D.F.U, $a = \pi_1 \cdots \pi_s$, donde π_i es irreducible en D. Como $f = \pi_1 \cdots \pi_s f_1^* \cdots f_n^*$ queda visto que f admite una descomposición como producto de factores irreducibles en $D[x]$.

** Probemos ahora que la descomposición es única, salvo unidades.

Supongamos que $f \in D[x]$, no unidad, admite dos descomposiciones como producto de factores irreducibles en $D[x]$:

$f = f_1 f_2 \cdots f_n$, $f = g_1 g_2 \cdots g_m$, f_i, g_j irreducibles en $D[x]$.

Queremos ver que $m = n$ y $g_i = u_i f_i$, $1 \le i \le n$, siendo u_i unidad de D.

Si f es constante, cada f_i y cada g_j pertenecen a D. Siendo D un D.F.U, la descomposición es única. Supongamos que f no es constante. Algunos de los factores pueden ser constantes. Reordenando convenientemente los factores y agrupando las constantes en una sola c podemos escribir $f = c f_1 f_2 \cdots f_r$, supuesto $f_k \in D$ si $k \ge r+1$. De la misma manera, $f = d g_1 g_2 \cdots g_s$, con $g_p \in D$ si $p \ge s+1$.

Dado $i \le r$, $f_i \in D[x]$ es irreducible y no constante, y, por tanto irreducible en $F[x]$, siendo F el cuerpo de fracciones de D.

Análogamente, si $j \le s$, g_j es irreducible en $F[x]$.

Además, los f_i y g_j son primitivos, por ser irreducibles en $D[x]$.

Luego $f_1 f_2 \cdots f_r$ y $g_1 g_2 \cdots g_s$ son primitivos. Por tanto, d y c son el contenido de f, salvo unidades; es decir, $d = u \cdot c$, siendo u una unidad de D.

Luego $f = c f_1 f_2 \cdots f_r = c u g_1 g_2 \cdots g_s \Rightarrow$

$\Rightarrow f_1 f_2 \cdots f_r = u g_1 \cdots g_s$

y, siendo $F[x]$ D.F.U, podemos suponer sin perder generalidad que $r = s$ y $f_1 = v_1 u g_1$, $f_2 = v_2 g_2$, $\dots$, $f_r = v_r g_r$, siendo v_i unidad de D, ya que f_i y g_i son primitivos.

Por otra parte, $d = u \cdot c$ $\Rightarrow$

$q_{r+1} = v_{r+1} u f_{r+1}, \dots, q_n = v_n f_n$, pues D es D.F.U.
Por tanto la descomposición es única salvo unidades. c.s.q.d.

8. CRITERIOS DE IRREDUCIBILIDAD DE POLINOMIOS.

1er CRITERIO: (de Eisenstein)

> Sea D un D.F.U y F el cuerpo de fracciones de D. Sea $f(x) \in D[x]$ de grado mayor o igual que 1 (no constante). Supongamos que existe p elemento primo de D tal que si $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_n \neq 0$, entonces $p \nmid a_n$, $p \mid a_i$ si $0 \leq i < n$, pero $p^2 \nmid a_0$. Entonces, en estas hipótesis, f es irreducible en $F[x]$.

Demostr: Siempre podemos escribir $f = c \cdot f^*$ siendo $c = \text{cont}(f) \in D$ y f^* primitivo. Entonces, f es irreducible en $F[x]$ si y solo si f^* es irreducible en $D[x]$ (Teorema 7.6). Podemos suponer, sin perder generalidad, que f es primitivo y probar que f es irreducible en $D[x]$.
Supongamos que f no es irreducible en $D[x]$; entonces, $f = g \cdot h$ con $g, h \in D[x]$ y $\partial^\circ(g) \geq 1$ y $\partial^\circ(h) \geq 1$, pues f es primitivo.
Sea $g = b_0 + b_1 x + \dots + b_r x^r$ y $h = c_0 + c_1 x + \dots + c_s x^s$.
Si $p \nmid a_n$, siendo $b_r c_s = a_n$ y p primo, se tiene que $p \nmid b_r$ y $p \nmid c_s$. Siendo $a_0 = b_0 c_0$ y $p \mid a_0$, se deduce que $p \mid b_0$ ó $p \mid c_0$, pero no a ambos, pues $p^2 \nmid a_0$. Supongamos que $p \mid c_0$ y $p \nmid b_0$. Sea c_k el primer coeficiente de h no divisible por p (que existe pues $p \nmid c_s$). Probaremos que $p \nmid a_k$, lo cual contradice la hipótesis ya que $k \leq s < n$ pues $n = \partial^\circ(f) = \partial^\circ(g) + \partial^\circ(h) = r + s$ y $r \geq 1$, y, por tanto, debería ser f irreducible.

$$a_k = b_0 c_k + b_1 c_{k-1} + \dots + b_k c_0$$

Tal como se ha tomado c_k se tiene que $p \mid c_i$ si $i < k$. Como $p \nmid c_k$ se tiene que $p \nmid a_k$, pues si $p \mid a_k$ se tendría que $p \mid (a_k - b_1 c_{k-1} - \dots - b_k c_0) \Rightarrow p \mid b_0 c_k \overset{p \text{ primo}}{\Longrightarrow} p \mid b_0$ ó $p \mid c_k$ en contra de que $p \nmid b_0$ y $p \nmid c_k$.
Luego, según se indicó anteriormente, f debe ser irreducible. c.s.q.d.
Ejemplo: El polinomio $3x^3 + 2x^2 - 4x + 6 \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Q}[x]$, pues $2 \nmid 3$, $2^2 \nmid 6$, $2 \mid 2$, $2 \mid (-4)$ y $2 \mid 6$.

2º CRITERIO: Sean D_1 y D_2 dominios de factorización única y $\sigma: D_1 \to D_2$ un homomorfismo, el cual se puede extender a un homomorfismo de $D_1[x]$ en $D_2[x]$ del siguiente modo:

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in D_1[x] \longmapsto f^\sigma(x) = \sigma(a_0) + \sigma(a_1) x + \dots + \sigma(a_n) x^n \in D_2[x].$$

Sea $f \in D_1[x]$ de modo que $f^\sigma \neq 0$ y $\partial^\circ(f) = \partial^\circ(f^\sigma)$. Entonces, si $f = gh$

irreducible sobre $F_2[x]$, se tiene que f_1 es irreducible sobre $F_1[x]$, siendo F_1 y F_2 los cuerpos de fracciones respectivos de D_1 y D_2.

Demostr: Supongamos que f no es irreducible en $F_1[x]$. Entonces podemos escribir $f = c \cdot g \cdot h$ donde $c \in D_1$ y g, h son polinomios primitivos de $D_1[x]$. (*)

Además, si f no es irreducible en $F_1[x]$ podemos suponer $\text{fue } \partial^\circ(g) \geq 1$ y $\partial^\circ(h) \geq 1$, pues de lo contrario f sería irreducible (si $\partial^\circ(g) = 0$, g es constante y, por tanto, una unidad de $F_1[x]$).

Tal como está construido σ tenemos $\text{fue } \partial^\circ(g^\sigma) \leq \partial^\circ(g)$ y $\partial^\circ(h^\sigma) \leq \partial^\circ(h)$. Siendo $\partial^\circ(c) = 0$, $\partial^\circ(f^\sigma) = \partial^\circ(h^\sigma) + \partial^\circ(g^\sigma)$ por ser σ homomorfismo y $\partial^\circ(f^\sigma) = \partial^\circ(f)$ por hipótesis tenemos fue

$$\partial^\circ(f) = \partial^\circ(f^\sigma) = \partial^\circ(g^\sigma) + \partial^\circ(h^\sigma) \leq \partial^\circ(g) + \partial^\circ(h) = \partial^\circ(f).$$

Luego $\partial^\circ(g) + \partial^\circ(h) = \partial^\circ(g^\sigma) + \partial^\circ(h^\sigma) \Rightarrow \partial^\circ(g) = \partial^\circ(g^\sigma)$ y $\partial^\circ(h) = \partial^\circ(h^\sigma)$, pues $\partial^\circ(g^\sigma) \leq \partial^\circ(g)$ y $\partial^\circ(h^\sigma) \leq \partial^\circ(h)$.

Luego $f^\sigma = c^\sigma \cdot g^\sigma \cdot h^\sigma$ en $F_2[x]$ y $\partial^\circ(g^\sigma) \geq 1$, $\partial^\circ(h^\sigma) \geq 1$.

Luego f^σ no sería irreducible en $F_2[x]$, contra la hipótesis.

Por tanto, f debe ser irreducible en $F_1[x]$. cqqd.

Ejemplo: Sea $f(x) = x^2 + x - 1 \in \mathbb{Z}[x]$.

Consideremos el homomorfismo canónico $\sigma: \mathbb{Z} \longrightarrow \mathbb{Z}/(3) = \mathbb{Z}_3$

Entonces $f^\sigma(x) = \bar{1}x^2 + \bar{1}x - \bar{1} = x^2 + x + \bar{2}$

$f^\sigma(x)$ es irreducible en $\mathbb{Z}_3$ pues no tiene raíces en el cuerpo $\mathbb{Z}_3$ ya que $f^\sigma(\bar{0}) = \bar{2}$, $f^\sigma(\bar{1}) = \bar{1}$ y $f^\sigma(\bar{2}) = \bar{2}$. Luego f es irreducible sobre $\mathbb{Q}[x]$.

TEMA 10º: TEORIA DE CUERPOS

1. DEFINICION. PRIMERAS PROPIEDADES.

DEFINICION: Un cuerpo es un anillo conmutativo en el que todos sus elementos no nulos son unidades. (*)

Sabemos que la característica de un cuerpo K es la característica de K considerado como anillo, y que la característica de un cuerpo ó es 0 ó un número primo. Si K es de característica 0, el menor subcuerpo de K es isomorfo a $\mathbb{Q}$. Si K es de característica p(primo), el menor subcuerpo de K es isomorfo a $\mathbb{Z}_p$. Decir que K es de característica p significa que $p\cdot 1 = 1+\overset{p}{\cdots}+1 = 0$. Entonces, si K es de característica $p\neq 0$, $\forall a\in K$, $pa=0$, pues $pa = a+\overset{p}{\cdots}+a = a\cdot 1+\overset{p}{\cdots}+a\cdot 1 = a(1+\overset{p}{\cdots}+1) = 0$.

1.1. PROPOSICION: Todo homomorfismo entre cuerpos es inyectivo.

Demostr.: Sean K_1 y K_2 dos cuerpos y $\phi: K_1 \to K_2$ un homomorfismo. Entonces $\operatorname{Ker}\phi$ es un ideal de K_1. Siendo K_1 cuerpo, los únicos ideales de K_1 son $\{0\}$ y K_1. Entonces, $\operatorname{Ker}\phi = \{0\}$ ó $\operatorname{Ker}\phi = K_1$. Pero $\operatorname{Ker}\phi \neq K_1$, pues $\phi(1_{K_1}) = 1_{K_2} \neq 0$. Por tanto, $\operatorname{Ker}\phi = \{0\}$ y, en consecuencia, ϕ es inyectivo. c.s.q.d.

* Los cuerpos de característica $p\neq 0$ no tienen que ser finitos, necesariamente. Si denotamos por $\mathbb{F}_p$ el cuerpo $\mathbb{Z}/(p)$, el cuerpo de fracciones $\mathbb{F}_p(x)$ del anillo de polinomios $\mathbb{F}_p[x]$ es infinito y de característica p, pues $\forall f(x)\in \mathbb{F}_p[x]$, $p\cdot f(x) = 0$.

* HOMOMORFISMO DE FROBËNIUS: Sea K un cuerpo de característica p. Entonces la aplicación

$$\pi: K \longrightarrow K$$
$$x \longmapsto \pi(x) = x^p$$

es un homomorfismo, llamado de Frobënius, pues $\pi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k$, ya que la fórmula de Newton es válida en anillos conmutativos. Si $k\neq 0$ y $k\neq p$, entonces $\binom{p}{n}$ es múltiplo de p (para p primo) y, por tanto, $\binom{p}{n} x^{p-n} y^n = 0$, pues K es de característica p. Por tanto, $\pi(x+y) = (x+y)^p = x^p + y^p = \pi(x) + \pi(y)$. Además $\pi(xy) = (xy)^p = x^p \cdot y^p$, pues K es conmutativo. Según la proposición 1.1, π es inyectivo. Luego si K es finito, π es un isomorfismo. Si K es infinito, π no será, en general, un isomorfismo.

fismo. Por ejemplo, el homomorfismo de Frobënius del cuerpo $\mathbb{F}_p(x)$ no es un isomorfismo, pues $x \in \mathbb{F}_p(x)$ no tiene contraimagen por π: si $\pi\left(\frac{f(x)}{g(x)}\right) = x$, $(f(x), g(x)) \in \mathbb{F}_p[x] \times \mathbb{F}_p^*[x]$, entonces $\left(\frac{f(x)}{g(x)}\right)^p = x$. Siendo $\partial^\circ(f(x)^p) = pn$ si $\partial^\circ(f) = n$ y $\partial^\circ(g(x)^p) = pm$ si $\partial^\circ(g) = m$ debería ser $pn = pm + \partial^\circ(x) = pm+1 \Rightarrow p(n-m) = 1$ lo cual no puede ser pues $p \neq 1$ y $n, m \in \mathbb{Z}^+$

1.2. PROPOSICION: Sea S un anillo y A un subanillo de S. Dado $s \in S$ la aplicación

$$\varphi: A[x] \longrightarrow S$$
$$f(x) \longmapsto f(s)$$

es un homomorfismo. Además $A[s] = \operatorname{Im}\varphi$, es un subanillo de S y es el menor subanillo de S que contiene a A y a s.

Demostr.: Que φ es homomorfismo es trivial y $A[s] = \operatorname{Im}\varphi$ es subanillo de S, por ser φ homomorfismo.
Sea S' subanillo de S que contiene a $A \cup \{s\}$.
Un "polinomio en s" es de la forma $a_0 + a_1 s + \dots + a_n s^n$ que es un elemento de S' ya que S' es subanillo que contiene a $A \cup \{s\}$ y $a_0, a_1, \dots, a_n \in A$. Luego $S' \supset A[s]$. c.q.d.

2. EXTENSION DE UN CUERPO: Extensiones simples. Elementos algebraicos y transcendentes.

DEFINICION: Sea K un cuerpo. Una extensión de K es un cuerpo $\mathbb{K}$ tal que K es subcuerpo de $\mathbb{K}$.
Denotaremos que $\mathbb{K}$ es una extensión de K con la notación $\mathbb{K}|K$.
Se prueba fácilmente que $\mathbb{K}|K$ es un espacio vectorial sobre K. La dimensión de este espacio vectorial se llama grado de la extensión y denotamos $\dim \mathbb{K}|K$ por $[\mathbb{K} : K]$.
Ejemplo: $\mathbb{R}$ es una extensión de $\mathbb{Q}$. $[\mathbb{R} : \mathbb{Q}]$ es infinito, pues si $[\mathbb{R} : \mathbb{Q}] = n$, $\mathbb{R}|\mathbb{Q}$ admitiría una base $\{\alpha_1, \dots, \alpha_n\}$; entonces $\mathbb{R} = \{\sum_{i=1}^{n} \lambda_i \alpha_i \,/\, \lambda_i \in \mathbb{Q}\}$, lo cual no puede ser pues el conjunto de las combinaciones lineales de un número finito de vectores con escalares en un conjunto numerable es numerable y $\mathbb{R}$ no lo es.

DEFINICION: Sea K un cuerpo y K_1 y K_2 dos extensiones de K. Entonces un K-homomorfismo de K_1 en K_2 es un homomorfismo de K_1 en K_2 que es K-lineal, es decir, $f: K_1 \to K_2$ es un K-homomorfismo si f es homomorfismo y se verifica que
$\forall \lambda \in K, \forall u \in K_1, f(\lambda u) = \lambda \cdot f(u)$.
$f: K_1 \to K_2$ es K-lineal si y solo si f:

pues si f es K-lineal, $f(\lambda \cdot 1) = \lambda \cdot f(1) = \lambda \cdot 1 = \lambda$, $\forall \lambda \in K$ y si f deja fijos los elementos de K, dados $\lambda \in K$ y $u \in K_1$, $f(\lambda u) = f(\lambda) \cdot f(u) = \lambda \cdot f(u)$

2.1. PROPOSICION: Sean $L, \bar{K}$ y K cuerpos tales que $L \supset \bar{K} \supset K$

Entonces $[L : K] = [L : \bar{K}] \cdot [\bar{K} : K]$

Demostr.: Sea $\mathcal{B}_1 = \{u_i / i \in I\}$ una base de $L|\bar{K}$ y $\mathcal{B}_2 = \{v_j / j \in J\}$ una base de $\bar{K}|K$. Si probamos que $\mathcal{B} = \{u_i v_j / (i,j) \in I \times J\}$ es base de $L|K$ quedará visto que $[L : K] = \text{card}(I \times J) = \text{card}(I) \times \text{card}(J) = [L : \bar{K}] \cdot [\bar{K} : K]$.

- $\mathcal{B}$ es sistema de generadores de $L|K$: Dado $u \in L$, $\exists \{c_i\}_{i \in I} \subset \bar{K}$ tal que $u = \sum_{i \in I} c_i u_i$, donde los c_i son nulos salvo, quizás, un número finito de ellos, pues los elementos de L son combinaciones lineales finitas de elementos de $\mathcal{B}_1$ con escalares en $\bar{K}$.

Dado $c_i \in \bar{K}$, $\exists \{c_{ij}\}_{j \in J} / c_i = \sum_{j \in J} c_{ij} v_j$ siendo esta suma finita, pues $\mathcal{B}_2$ es base de $\bar{K}|K$, donde $c_{ij} \in K$.

Luego $u = \sum_{i \in I} \left(\sum_{j \in J} c_{ij} v_j \right) u_i = \sum_{i,j} c_{ij} (u_i v_j)$

donde esta suma es finita y $c_{ij} \in K$.

- $\mathcal{B}$ es un sistema libre:

Dada una suma finita $\sum_{i,j} \lambda_{ij} u_i v_j = 0 \Rightarrow \sum_i \left(\sum_j \lambda_{ij} v_j \right) u_i = 0 \Rightarrow$

$\overset{(1)}{\Rightarrow} \sum_j \lambda_{ij} v_j = 0, \forall i \overset{(2)}{\Rightarrow} \lambda_{ij} = 0, \forall i,j$

(1) pues $\mathcal{B}_1$ es base de $L|\bar{K}$ y $\sum_j \lambda_{ij} v_j \in \bar{K}$

(2) pues $\mathcal{B}_2$ es base de $\bar{K}|K$ y $\lambda_{ij} \in K$. c.s.q.d.

DEFINICIONES: Sea $\bar{K}$ una extensión del cuerpo K y S un subconjunto de $\bar{K}$. Designaremos por $K\langle S \rangle$ el subespacio vectorial de $\bar{K}|K$ generado por S, es decir, el menor de los subespacios vectoriales de $\bar{K}|K$ que contiene (≡ ⊆ ≠) a S. Designamos por $K[S]$ el menor subanillo de $\bar{K}$ que contiene a K y a S. Designamos por $K(S)$ el menor subcuerpo de $\bar{K}$ que contiene a K y a S. Con las notaciones de esta definición tenemos:

2.2. PROPOSICION: $K\langle S \rangle \subset K[S] \subset K(S)$.

Demostr.: $K[S] \subset K(S)$, pues $K(S)$ es un subanillo de $\bar{K}$ que contiene a K y a S, y $K[S]$ es el menor de los subanillos de $\bar{K}$ que contienen a K y a S.

Si probamos que $K[S]$ es subespacio vectorial de $K_{|K}$ que contiene a K y a S quedará visto que $K\langle S\rangle \subset K[S]$.
Que $K[S] \supset K \cup S$ se tiene por definición.
Además, dados $\lambda, \mu \in K$ y $s_1, s_2 \in K[S]$, $\lambda s_1 - \mu s_2 \in K[S]$, pues $K \subset K[S]$ y $K[S]$ es subanillo. Luego $K\langle S\rangle \subset K[S]$. c.s.q.d.
Con las mismas notaciones anteriores y representando por $\mathcal{P}_f(S)$ el conjunto de las partes finitas de S tenemos

2.3. PROPOSICION a) $K\langle S\rangle = \bigcup_{F \in \mathcal{P}_f(S)} K\langle F\rangle$

b) $K[S] = \bigcup_{F \in \mathcal{P}_f(S)} K[F]$ c) $K(S) = \bigcup_{F \in \mathcal{P}_f(S)} K(F)$

Demostr: a) Que $\bigcup_{F \in \mathcal{P}_f(S)} K\langle F\rangle \subset K\langle S\rangle$ es trivial si tenemos en cuenta que $\forall F \in \mathcal{P}_f(S)$, $F \subset S \Rightarrow K\langle F\rangle \subset K\langle S\rangle$.
Si probamos que $\bigcup_{F \in \mathcal{P}_f(S)} K\langle F\rangle$ es subespacio vectorial de $K_{|K}$ quedará visto, por la definición de $K\langle S\rangle$, que $K\langle S\rangle = \bigcup_{F \in \mathcal{P}_f(S)} K\langle F\rangle$
Dados $u, v \in \bigcup_{F \in \mathcal{P}_f(F)} K\langle F\rangle$, $\exists F_1, F_2 \in \mathcal{P}_f(S) / u \in K\langle F_1\rangle$ y $v \in K\langle F_2\rangle$.
Entonces $u, v \in K\langle F_1 \cup F_2\rangle$ y, por tanto, dados $\lambda, \mu \in K$, $\lambda u - \mu v \in K\langle F_1 \cup F_2\rangle \subset \bigcup_{F \in \mathcal{P}_f(S)} K\langle F\rangle$, como queríamos ver.
b) y c) se demuestran de modo análogo, con solo ver que $\bigcup_{F \in \mathcal{P}_f(S)} K[F]$ y $\bigcup_{F \in \mathcal{P}_f(S)} K(F)$ son, respectivamente, subanillo y subcuerpo de K que contienen a K y a S. c.s.q.d.

Si S es finito, $S = \{s_1, s_2, \dots, s_n\}$, denotamos $K\langle S\rangle = K\langle s_1, s_2, \dots, s_n\rangle$, $K[S] = K[s_1, s_2, \dots, s_n]$ y $K(S) = K(s_1, s_2, \dots, s_n)$. Con estas notaciones:

2.4. PROPOSICION: a) $K\langle s_1, s_2, \dots, s_n\rangle = \{\sum_{i=1}^{n} \lambda_i s_i / \lambda_i \in K\}$

b) $K[s_1, s_2, \dots, s_n]$ es el conjunto de los "polinomios en $s_1, s_2, \dots, s_n$".
Un polinomio en $s_1, s_2, \dots, s_n$ es de la forma
$$f(s_1, s_2, \dots, s_n) = \sum \lambda_{i_1 i_2 \dots i_n} s_1^{i_1} \cdots s_n^{i_n}$$

c) $K(s_1, s_2, \dots, s_n)$ es el cuerpo de fracciones de $K[s_1, s_2, \dots, s_n]$, es decir, el conjunto de los elementos $\frac{f(s_1, s_2, \dots, s_n)}{g(s_1, s_2, \dots, s_n)}$ tales que $(f(s_1, s_2, \dots, s_n), g(s_1, s_2, \dots, s_n)) \in K[s_1, s_2, \dots, s_n] \times (K[s_1, s_2, \dots, s_n] - \{0\})$

a) $K\langle s_1, s_2, \dots, s_n\rangle$, subespacio vectorial de $K_{|K}$ engendrado por

por $\{s_1, s_2, \dots, s_n\}$, es el conjunto de las combinaciones lineales de dichos elementos con escalares en K.

b) Evidentemente todo polinomio en $s_1, \dots, s_n$, $f(s_1, \dots, s_n) = \sum \lambda_{i_1 \dots i_n} \cdot s_1^{i_1} \cdots s_n^{i_n}$ es un elemento de $K[s_1, s_2, \dots, s_n]$, por ser una suma de productos de elementos de $K \cup \{s_1, \dots, s_n\}$ y ser $K[s_1, \dots, s_n]$ un subanillo de K que contiene a $K \cup \{s_1, \dots, s_n\}$.

Si probamos que el conjunto de los polinomios en $s_1, \dots, s_n$ es un subanillo de K que contiene a $K \cup \{s_1, \dots, s_n\}$, al estar contenido en $K[s_1, \dots, s_n]$, será igual a dicho conjunto pues $K[s_1, \dots, s_n]$ es el menor subanillo de K que contiene a $K \cup \{s_1, \dots, s_n\}$.

Dados dos polinomios en $s_1, \dots, s_n$, $f(s_1, \dots, s_n)$ y $g(s_1, \dots, s_n)$ es trivial que $f(s_1, \dots, s_n) + g(s_1, \dots, s_n)$ y $f(s_1, \dots, s_n) \cdot g(s_1, \dots, s_n)$ son polinomios en $s_1, \dots, s_n$. Luego, y como queríamos probar,

$$K[s_1, \dots, s_n] = \{ f(s_1, \dots, s_n) \text{ polinomio en } s_1, \dots, s_n \}.$$

c) Sea $H = \left\{ \dfrac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)} \;/\; f(s_1, \dots, s_n), g(s_1, \dots, s_n) \in K[s_1, \dots, s_n],\ g(s_1, \dots, s_n) \neq 0 \right\}$

Se trata de ver que $K(s_1, \dots, s_n) = H$.

- $H \subset K(s_1, \dots, s_n)$: Dado $\dfrac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)} \in H$, $f(s_1, \dots, s_n), g(s_1, \dots, s_n) \in K[s_1, \dots, s_n] \subset K(s_1, \dots, s_n)$. Siendo $K(s_1, \dots, s_n)$ cuerpo, se deduce que $\dfrac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)} \in K(s_1, \dots, s_n)$ y, por tanto, $H \subset K(s_1, \dots, s_n)$.

Si probamos que H es subcuerpo de K que contiene a $K \cup \{s_1, \dots, s_n\}$ quedará visto que $H = K(s_1, \dots, s_n)$, por definición de $K(s_1, \dots, s_n)$.

Dados $\dfrac{f_1}{g_1}, \dfrac{f_2}{g_2} \in H$, $\dfrac{f_1}{g_1} - \dfrac{f_2}{g_2} = \dfrac{f_1 g_2 - f_2 g_1}{g_1 g_2} \in H$, pues

$f_1, g_2, f_2, g_1 \in K[s_1, \dots, s_n] \Rightarrow f_1 g_2 - f_2 g_1 \in K[s_1, \dots, s_n] \wedge g_1 g_2 \in K[s_1, \dots, s_n] - \{0\}$

Además, dados $\dfrac{f_1}{g_1}, \dfrac{f_2}{g_2} \in H$, $\dfrac{f_2}{g_2} \neq 0 \Rightarrow \dfrac{f_1}{g_1} \cdot \left(\dfrac{f_2}{g_2}\right)^{-1} = \dfrac{f_1 g_2}{g_1 f_2} \in H$

Luego $H = K(s_1, \dots, s_n)$. c.s.q.d.

* DEFINICION: (Extensión simple)

Se dice que la extensión $\mathbb{K}|K$ es simple si existe $s \in \mathbb{K}$ tal que $\mathbb{K} = K(s) = \left\{ \dfrac{f(s)}{g(s)} \;/\; g(s) \neq 0 \text{ y } f(s), g(s) \in K[s] \right\}$.

Supongamos tener una extensión simple $\mathbb{K}|K$. Consideremos el homomorfismo $\varphi : f(x) \in K[x] \longmapsto f(s) \in K[s]$. Trivialmente, φ es sobre. $\ker \varphi$ es un ideal de $K[x]$. Si $\ker \varphi = \{0\}$, entonces $K[x] \simeq K[s]$

Siendo K cuerpo, $K[x]$ es ~~una~~ dominio principal. Luego si $\operatorname{Ker}\varphi \neq \{0\}$, $\operatorname{Ker}\varphi = (f_s(x))$, $f_s(x) \in K[x]$.
Como $K[s] \subset \mathbb{K}$ y $\mathbb{K}$ es íntegro se tiene que $K[s]$ es íntegro
Como $\operatorname{Im}\varphi \simeq \frac{K[x]}{\operatorname{Ker}\varphi}$, φ es sobre y $\operatorname{Ker}\varphi = (f_s(x))$ se tiene que
$K[s] \simeq \frac{K[x]}{(f_s(x))}$. Luego $\frac{K[x]}{(f_s(x))}$ es íntegro y, por tanto, $(f_s(x))$ es un ideal primo de $K[x]$ (Tema 9°, PROPOSICION 1.2.)
Siendo $K[x]$ un dominio principal, se deduce que $(f_s(x))$ es un ideal maximal de $K[x]$ (Tema 9°, PROPOSICION 1.6) y, por tanto, $f_s(x)$ es irreducible. Además, como $f_s(x)$ tiene coeficientes en el cuerpo K, podemos tomarlo mónico. Entonces

DEFINICIONES: Sea $K|K$ una extensión simple, $K = K(s)$. Sea φ el homomorfismo definido anteriormente. Diremos que s es transcendente sobre K si $\operatorname{Ker}\varphi = \{0\}$, es decir, si $K[x] \simeq K[s]$. Diremos que s es algebraico sobre K si $\operatorname{Ker}\varphi \neq \{0\}$.

Si s es transcendente, $\operatorname{Ker}\varphi = \{0\}$. Luego $\forall f(x) \in K[x] - \{0\}$, $f(s) \neq 0$, es decir, s no es raiz de ninfun polinomio con coeficientes en K.

Si s es algebraico, $\operatorname{Ker}\varphi \neq \{0\}$. Luego $\exists f(x) \in K[x] - \{0\} / f(s) = 0$, es decir, s es raiz de un polinomio con coeficientes en K

Con las notaciones anteriores, si $\operatorname{Ker}\varphi = (f_s(x)) \neq \{0\}$

DEFINICION: Decimos que $f_s(x)$ es el polinomio mínimo de s. (*)

$f_s(x)$ es el polinomio mónico de menor grado que se anula sobre s. Segun hemos visto, $f_s(x)$ es irreducible sobre K.

2.5. PROPOSICION: Sea K una extensión de K y $s \in K$. Entonces:

a) Si s es transcendente, $K(s)$ es isomorfo a $K(x)$
b) Si s es algebraico, entonces $K(s) = K[s]$, y por tanto, $K(s) \simeq \frac{K[x]}{(f_s(x))}$

Además, en este caso, $K(s)|K$ es de dimensión finita verificándose que si $n = \partial^o(f_s(x))$, $[K(s):K] = n$ y $K(s) = K\langle 1, s, \dots, s^{n-1}\rangle$.

Demostr: a) Si s es transcendente, $K[x] \simeq K[s]$ y, en consecuencia, $K(x)$ es isomorfo a $K(s)$, pues $K(x)$ es el cuerpo de fracciones de $K[x]$ y $K(s)$ es el cuerpo de fracciones de $K[s]$.

b) Si s es algebraico, $K[s] \simeq \frac{K[x]}{(f_s(x))}$

Siendo $(f_s(x))$ un ideal maximal de $K[x]$, $\frac{K[x]}{(f_s(x))}$ es un cuerpo.

Como $K[s] \subset K(s)$ y $K(s)$ es el menor subcuerpo de $\bar{K}$ que contiene a K y a $\{s\}$ debe ser $K[s] = K(s)$.
Siendo $n = \partial^\circ(f_s(x))$, si probamos que $\mathcal{B} = \{1, s, \dots, s^{n-1}\}$ es base de $K(s)|K$ quedará terminada la demostración.
- $\mathcal{B}$ es sistema de generadores: Los elementos de $K(s)$ son polinomios en s, pues hemos visto que $K(s) = K[s]$.
Sea $g(s) \in K[s]$. Consideremos la división euclídea de $g(x) \in K[x]$ por $f_s(x)$, donde $g(x)$ es un polinomio en x cuyos coeficientes son iguales a los de $g(s)$. Existen, entonces, $q(x)$ y $r(x)$ en $K[x]$ tales que

$$g(x) = q(x) \cdot f_s(x) + r(x), \quad \partial^\circ(r(x)) < \partial^\circ(f_s(x)).$$

Siendo $f_s(s) = 0$, se tiene que $g(s) = r(s)$
Como $\partial^\circ(r) < \partial^\circ(f_s) = n$, $r(s) = a_0 + a_1 s + \dots + a_k s^k$, $k \leq n-1$, $a_i \in K$
Por tanto, $g(s) = r(s)$, está generado por $\{1, s, \dots, s^{n-1}\}$.
- $\mathcal{B}$ es un sistema libre: Supongamos que $\sum_{i=0}^{n-1} a_i s^i = 0$, $a_i \in K$.
Sea $g(x) = \sum_{i=0}^{n-1} a_i x^i \in K[x]$. Luego $\partial(g) \leq n-1$.

Además $g(s) = 0$. Debe ser entonces $g = 0$, pues si $g \neq 0$ tenemos $g(s) = 0$ y $\partial^\circ(g) < \partial^\circ(f_s)$, en contra de que f_s es el polinomio mínimo de s. Luego $g = 0 \Rightarrow a_i = 0$, $0 \leq i \leq n-1$. c.q.d.

EJEMPLOS: ① $\mathbb{R}|\mathbb{Q}$ no es una extensión simple
② $\mathbb{Q}(\sqrt{2})$ es una extensión simple sobre $\mathbb{Q}$. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$, pues $\sqrt{2}$ es raiz de $x^2 - 2$, que es irreducible y mónico sobre $\mathbb{Q}$. Luego $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Entonces
$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$ pues una base de $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es $\{1, \sqrt{2}\}$.

Hemos visto que existen cuerpos "entre" $\mathbb{Q}$ y $\mathbb{R}$.
* Dado un cuerpo K y $f(x) \in K[x]$, cabe preguntarse si existe una extensión $\mathbb{K}$ de K en la que f tiene al menos una raiz.
La respuesta está en el siguiente

2.6. TEOREMA: (de Krönecker).

> Si $f(x) \in K[x]$ existe una extensión $E|K$ en la que f tiene al menos una raiz, siendo $\partial^\circ(f) \geq 1$.

Demostr.: $K[x]$ es un dominio de factorización única. Podemos suponer que f es irreducible, pues si $f = f_1 \cdots f_n$, f_i irreducibles.

y probamos que existe una extensión $\bar{K}_{|K}$ en la que un f_i tiene una raiz, f tendrá esta misma raiz en esta misma extensión.

- Supongamos, entonces, que f es irreducible. Entonces, $(f(x))$ es ideal maximal de $K[x]$ y, por tanto, $\frac{K[x]}{(f(x))}$ es cuerpo. Consideremos el homomorfismo canónico

$$\sigma : K[x] \longrightarrow \frac{K[x]}{(f(x))}$$

Denotaremos por K^σ al conjunto imagen. Sabemos que $K[x] \supset K$. Entonces la restricción $\sigma_{|K}$ es inyectiva, puesto que se trata de un homomorfismo de cuerpos.

Dado el polinomio $f(x) \in K[x]$ consideremos el polinomio $f^\sigma(y)$ con coeficientes en K^σ de manera que si $f(x) = a_0 + a_1 x + \dots + a_n x^n$, sea $f^\sigma(y) = \sigma(a_0) + \sigma(a_1)\, y + \dots + \sigma(a_n) \cdot y^n$.

Veamos que $f^\sigma(y)$ tiene una raiz en K^σ

Dado $x \in K[x]$, $\xi = \sigma(x) \in K^\sigma$. Además

$f^\sigma(\xi) = \sigma(a_0) + \sigma(a_1) \cdot \xi + \dots + \sigma(a_n)\, \xi^n = \sigma(a_0) + \sigma(a_1)\sigma(x) + \dots + \sigma(a_n)\sigma(x^n) =$

$= \sigma(a_0 + a_1 x + \dots + a_n x^n) = \sigma(f(x)) = 0$

ya que el ideal $(f(x))$ es el cero en $\frac{K[x]}{(f(x))}$ y $f(x) \in (f(x))$.

Luego ξ es raiz de f^σ en K^σ.

Según dijimos antes $\sigma_{|K} : K \longrightarrow K^\sigma$ es inyectivo.

Consideramos el conjunto $K^\sigma - \sigma(K)$. Sea S un conjunto del mismo cardinal que $K^\sigma - \sigma(K)$ y disjunto con K.

Sea $E = K \cup S$. Entonces $\text{card}(E) = \text{card}(K^\sigma)$ pues $\text{card}(E) = \text{card}(K) + \text{card}(S)$ y $\text{card}(K^\sigma) = \text{card}(\sigma(K)) + \text{card}(K^\sigma - \sigma(K))$ y $\text{card}(K) = \text{card}(\sigma(K))$ pues σ es inyectiva.

Podemos definir una biyección del siguiente modo:

$$\tilde{\sigma} : E \longrightarrow K^\sigma$$

$$u \longmapsto \tilde{\sigma}(u) = \begin{cases} = \sigma(u) \text{ si } u \in K \\ = u' \in K^\sigma - \sigma(K) \text{ si } u \in S \end{cases} \quad (*)$$

Mediante esta biyección podemos transportar la estructura de cuerpo de K^σ a E del siguiente modo:

Dados $x, y \in E$, $x + y = \tilde{\sigma}^{-1}(\tilde{\sigma}(x) + \tilde{\sigma}(y))$ y $x \cdot y = \tilde{\sigma}^{-1}(\tilde{\sigma}(x) \cdot \tilde{\sigma}(y))$.

Además, cuando dos elementos $x, y \in K \subset E$, los componemos mediante estas nuevas operaciones obtenemos el mismo elemento de K que si los componemos mediante las leyes de composición existentes en K desde un principio, ya que si $x, y \in K$, $\tilde{\sigma}^{-1}(\tilde{\sigma}(x) + \tilde{\sigma}(y)) = \sigma^{-1}(\sigma(x) + \sigma(y)) = x + y$, y de modo

logo se hace para el producto.

Veamos, por último, que f tiene una raiz en $\mathcal{E}$. Probaremos que $\tilde{\sigma}^{-1}(\xi)$ es raiz de f:

$$f(\tilde{\sigma}^{-1}(\xi)) = a_0 + a_1\tilde{\sigma}^{-1}(\xi) + \dots + a_n\cdot\tilde{\sigma}^{-1}(\xi^n) =$$
$$= \tilde{\sigma}^{-1}(\tilde{\sigma}(a_0)) + \tilde{\sigma}^{-1}(\tilde{\sigma}(a_1))\cdot\tilde{\sigma}^{-1}(\xi) + \dots + \tilde{\sigma}^{-1}(\tilde{\sigma}(a_n))\cdot\tilde{\sigma}^{-1}(\xi^n) =$$
$$= \tilde{\sigma}^{-1}(\tilde{\sigma}(a_0)) + \tilde{\sigma}^{-1}(\tilde{\sigma}(a_1)\cdot\xi) + \dots + \tilde{\sigma}^{-1}(\tilde{\sigma}(a_n)\cdot\xi^n) =$$
$$= \tilde{\sigma}^{-1}(\tilde{\sigma}(a_0) + \tilde{\sigma}(a_1)\xi + \dots + \tilde{\sigma}(a_n)\xi^n) =$$
$$\overset{(*)}{=} \tilde{\sigma}^{-1}(\sigma(a_0) + \sigma(a_1)\cdot\xi + \dots + \sigma(a_n)\xi^n) =$$
$$= \tilde{\sigma}^{-1}(0) = 0, \text{ pues } \tilde{\sigma} \text{ es isomorfismo.}$$

Siendo $\mathcal{E}$ una extensión de K y $\tilde{\sigma}^{-1}(\xi) \in \mathcal{E}$ queda probado el teorema. c.s.q.d.

3. Cuerpo de ruptura de un polinomio.

DEFINICION: Dado un cuerpo K y un polinomio $f \in K[x]$, un cuerpo de ruptura de este polinomio es una extensión simple $\bar{K}$ de K tal que $\bar{K} = K(s)$ y $f(s) = 0$. (***)

3.1. TEOREMA: Sea $\sigma: K \to K'$ un isomorfismo de cuerpos y f un polinomio irreducible sobre K. Supongamos que $\bar{K}$ y $\bar{K}'$ son cuerpos de ruptura de f y f^σ respectivamente, es decir, $\exists (s, s') \in \bar{K}\times\bar{K}' / \bar{K} = K(s), \bar{K}' = K'(s')$ y $f(s) = 0, f^\sigma(s') = 0$. Entonces, existe una única prolongación $\bar{\sigma}: \bar{K} \to \bar{K}'$ de σ tal que $\bar{\sigma}(s) = s'$. (**)

Demostr: Toda prolongación homomórfica $\bar{\sigma}: \bar{K} \longrightarrow \bar{K}'$ de σ tal que $\bar{\sigma}(s) = s'$ es de la forma $g(s) \in \bar{K} = K(s) \longmapsto g^\sigma(s') \in \bar{K}' = K'(s')$. Luego, de existir $\bar{\sigma}$ es único, trivialmente. Probemos entonces la existencia.

Si $K \simeq K'$, entonces $K[x] \overset{\varphi}{\simeq} K'[x]$. La "restricción" de φ a $(f(x))$ es un isomorfismo entre $(f(x))$ y $(f^\sigma(x))$. Luego $\dfrac{K[x]}{(f(x))} \simeq \dfrac{K'[x]}{(f^\sigma(x))}$.

Además, trivialmente, $f^\sigma(x)$ es irreducible, pues $f(x)$ lo es.

Siendo s algebraico sobre K y s' algebraico sobre K', pues $f(s) = 0$ y $f^\sigma(s') = 0$, y siendo y f y f^σ los polinomios mínimos de s y s', por ser irreducibles, tenemos, segun proposición 2.5, que $K(s) \simeq \dfrac{K[x]}{(f(x))}$ y $K'(s') \simeq \dfrac{K'[x]}{(f^\sigma(x))}$.

Luego $K(s) \overset{\phi_1}{\simeq} \dfrac{K[x]}{(f(x))} \overset{\phi_2}{\simeq} \dfrac{K'[x]}{(f^\sigma(x))} \overset{\phi_3}{\simeq} K'(s')$, y por tanto, existe un isomorfismo $\bar{\sigma}: K(s) \longrightarrow K'(s')$. Probemos que $\bar{\sigma}$ es una prolongación de σ de manera que $\bar{\sigma}(s) = s'$.

$\forall a \in K$, $\bar{\sigma}(a) = (\phi_3\circ\phi_2\circ\phi_1)(a) = (\phi_3\circ\phi_2)(a + (f(x))) = \phi_3(\sigma(a) + (f^\sigma(x))) = \sigma(a)$

Además, $\bar{\sigma}(s) = (\phi_3\circ\phi_2\circ\phi_1)(s) = (\phi_3\circ\phi_2)(x + (f(x))) = \phi_3(x + (f^\sigma(x))) = s'$. c.s.q.d.

3.2. COROLARIO: Dos cuerpos de ruptura de un polinomio irreducible sobre un cuerpo K son K-isomorfos.

Demostr: Sea $f(x) \in K[x]$ y $K(s)$ y $K(s')$ cuerpos de ruptura de f.

$$\begin{array}{ccc} K & \xrightarrow{i} & K \\ \downarrow & & \downarrow \\ K(s) & \xrightarrow{\bar{i}} & K(s') \end{array}$$

Consideremos el diagrama del margen, donde i es el isomorfismo identidad. Según el teorema anterior existe una única prolongación $\bar{i}: K(s) \to K(s')$ de i tal que $\bar{i}(s) = s'$. Entonces si $g(s) = a_0 + a_1 s + \dots + a_n s^n \in K(s)$ se tiene que $\bar{i}(g(s)) = a_0 + a_1 s' + \dots + a_n s'^n$. Trivialmente $\bar{i}$ es isomorfismo. Además, siendo $\bar{i}|K = i$ se deduce que $\bar{i}$ deja fijos los elementos de K. Luego, $K(s)$ y $K(s')$ son K-isomorfos, c.s.q.d.

4. EXTENSIONES ALGEBRAICAS

DEFINICION: Dado un cuerpo K, una extensión $K|k$ diremos que es algebraica si todo elemento de K es algebraico sobre k.

DEFINICION: Una extensión K sobre un cuerpo k se dice de generación finita si existe $S = \{s_1, \dots, s_n\} \subset K$ tal que $K = k(s_1, \dots, s_n)$.

4.1. PROPOSICION: Una extensión K de un cuerpo k es finita si, y solo si, es algebraica y de generación finita. (*)

Demostr: $\Rightarrow$| Supongamos que $[K:k] = n$. Probemos que $K|k$ es una extensión algebraica y de generación finita.

- $K|k$ es algebraica: Dado $u \in K$, el conjunto $\{1, u, \dots, u^n\}$ es un sistema ligado pues tenemos $n+1$ vectores en un espacio vectorial de dimensión n. Entonces $\exists \{\lambda_i\}_{i=0}^n \subset k / \sum_{i=0}^n \lambda_i u^i = 0$, donde al menos uno de los λ_i no es nulo. Consideremos el polinomio no nulo $f(x) = \sum_{i=0}^n \lambda_i x^i \in k[x]$. Entonces $f(u) = 0$, que prueba que u es algebraico sobre k. Luego, $K|k$ es una extensión algebraica.
- $K|k$ es de generación finita: Sea $\{u_1, \dots, u_n\}$ una base de $K|k$. Entonces $K = k\langle u_1, \dots, u_n \rangle \subset k(u_1, \dots, u_n) \subset K$, trivialmente. Luego $K = k(u_1, \dots, u_n)$.

$\Leftarrow$| Sea $K|k$ una extensión algebraica de generación finita. Supongamos que $K = k(u_1, \dots, u_n)$. Evidentemente se tienen las contenciones: $k \subset k(u_1) \subset k(u_1)(u_2) \subset k(u_1, u_2)(u_3) \subset \dots \subset k(u_1, \dots, u_{n-1})(u_n)$.

Veamos que las extensiones simples $k(u_1)|k$ y $k(u_1, \dots, u_{i-1})(u_i)|k(u_1, \dots, u_{i-1})$, $i = 2, \dots, n$, son finitas

Por hipótesis, para cada $i \in \{1, \dots, n\}$, u_i es algebraico sobre k

Luego para cada $i\in\{1,\dots,n\}$, $\exists f_i\in K[x]$ / $f_i(u_i)=0$.
Entonces $f=f_1\cdots f_n\in K[x]$ y se verifica que $f(u_i)=0$, $\forall i\in\{1,\dots,n\}$.
Como $K\subset K(u_1,\dots,u_{i-1})$ se deduce que $f\in K(u_1,\dots,u_{i-1})[x]$ y $f(u_i)=0$ y, en consecuencia, u_i es algebraico sobre $K(u_1,\dots,u_{i-1})$. Por tanto, en virtud de PROPOSICION 2.5, la extensión $K(u_1,\dots,u_{i-1})(u_i)|K(u_1,\dots,u_{i-1})$ es finita. Sea $[K(u_1,\dots,u_{i-1})(u_i):K(u_1,\dots,u_{i-1})]=r_i$, $i=2,\dots,n$ y $[K(u_1):K]=r_1$. Entonces

$[K(u_1,\dots,u_n):K]=[K(u_1,\dots,u_{n-1})(u_n):K(u_1,\dots,u_{n-2})(u_{n-1})]\cdot\dots\cdot[K(u_1):K]=$
$=r_n\cdots r_1$, lo cual prueba que $\bar{K}=K(u_1,\dots,u_n)$ es una extensión finita de K. c.s.q.d. (*)

4.2. LEMA: Sea Δ un dominio de integridad que contiene a un cuerpo K. Entonces, considerando Δ como espacio vectorial sobre K, se verifica que si $[\Delta:K]$ es finita, Δ es cuerpo.

Demostr.: Probaremos que todo elemento no nulo de Δ es una unidad.
Sea $a\in\Delta-\{0\}$. Consideremos la aplicación

$$\varphi_a:\ b\in\Delta\longmapsto a\cdot b\in\Delta$$

Esta aplicación es un homomorfismo entre espacios vectoriales, pues $\forall b,b'\in\Delta$, $a\cdot(b+b')=ab+ab'$ y $\forall\lambda\in K,\forall b\in\Delta$, $a(\lambda\cdot b)=\lambda(a\cdot b)$ pues $K\subset A$ y Δ es conmutativo.
Además es inyectivo, pues si $b\in\ker\varphi_a$, $a\cdot b=0\Rightarrow b=0$, pues Δ es íntegro y $a\neq 0$.
Siendo Δ espacio vectorial sobre K de dimensión finita se deduce que φ_a es sobre. Luego, dado $1\in\Delta$, $\exists b\in\Delta$ / $ab=1$, que prueba que a es una unidad. c.s.q.d.

4.3. TEOREMA: Sea $\bar{K}$ una extensión de un cuerpo K y S una parte de $\bar{K}$ tal que todo elemento u de S es algebraico sobre K. Entonces $K(S)=K[S]$ y la extensión $K(S)|K$ es algebraica.

Demostr.: Según PROPOSICION 2.3, $K(S)=\bigcup_{F\in\mathcal{P}_f(S)}K(F)$, donde $\mathcal{P}_f(S)$ es el conjunto de las partes finitas de S. Sea $F=\{u_1,\dots,u_n\}$ una parte finita de S. Siendo cada u_i algebraico sobre K se deduce que $K(F)$ es una extensión algebraica y de generación finita. Luego, segun PROPOSICION 4.1, $K(F)$ es una extensión finita de K.
Considerando $K[F]$ como subespacio vectorial de $K(F)$ pues $K[F]\subset K(F)$ tenemos que $K[F]$ es de dimensión finita, pues lo es $K(F)$. Como $K[F]$ es íntegro, en virtud del

una anterior tenemos que $K[F]$ es un cuerpo, que contiene a K y a F. Entonces, por definición de $K(F)$, tenemos que $K[F] = K(F)$, y esto para cada parte finita F de S.
Luego $K(S) = \bigcup_{F \in P_f(S)} K(F) = \bigcup_{F \in P_f(S)} K[F] = K[S]$

Veamos que $K(S)|K$ es una extensión algebraica.
Dado $u \in K(S)$, $\exists F \in P_f(S) / u \in K(F)$.
Siendo $K(F)|K$ una extensión algebraica, se deduce que u es algebraico sobre K. c.s.q.d.

4.4. COROLARIO: Sea K una extensión de un cuerpo K. Entonces el conjunto $E = \{u \in K / u \text{ es algebraico sobre } K\}$ es un cuerpo que contiene a K y la extensión $E|K$ es algebraica.

Demostr.: Probemos que $K(E) = E$ y quedará probado el corolario, pues $K(E)$ es un cuerpo.
Por el teorema anterior la extensión $K(E)|K$ es algebraica.
Luego, si $u \in K(E)$, u es algebraico sobre K y, como además $u \in K$, se tiene que $u \in E$. Por tanto, $K(E) \subset E$.
Pero, por definición, $E \subset K(E)$. Luego $K(E) = E$. c.s.q.d.

4.5. PROPOSICION: Sean L, K y K tres cuerpos tales que $L \supset K \supset K$. Entonces, $L|K$ es una extensión algebraica si, y solo si, lo son $L|K$ y $K|K$.

Demostr.: $\Rightarrow$| Supongamos que $L|K$ es una extensión algebraica.
Dado $u \in L$, $\exists f(x) \in K[x]$ tal que $f(u) = 0$. Como $K \subset K$, $K[x] \subset K[x]$.
Luego $f(x) \in K[x]$ y, por tanto, u es algebraico sobre K; en consecuencia, $L|K$ es algebraica.
Además, como todo elemento de L es algebraico sobre K, por hipótesis, y siendo $K \subset L$ se deduce que $K|K$ es algebraica.
$\Leftarrow$| Supongamos que $L|K$ y $K|K$ son extensiones algebraicas
Dado $u \in L$, $\exists f(x) \in K[x]$ tal que $f(u) = 0$.
Sea $f(x) = v_0 + v_1 x + \dots + v_n x^n$, $v_i \in K$, $i = 0, 1, \dots, n$.
Consideremos el subcuerpo de K, $K(v_0, \dots, v_n)$. Entonces, u es algebraico sobre este subcuerpo de K. Por tanto, según PROPOSICION 2.5, $K(v_0, \dots, v_n)(u)$ es una extensión finita de $K(v_0, \dots, v_n)$. Además, siendo $K|K$ algebraica, $v_0, v_1, \dots, v_n$ son algebraicos sobre K y, por tanto, $K(v_0, v_1, \dots, v_n)|K$ es algebraica (Teorema 4.3) y siendo $K(v_0, \dots, v_n)|$

extensión de generación finita, se deduce que $K(v_0,\dots,v_n)|K$ es una extensión finita; En consecuencia $K(v_0,\dots,v_n)(u)|K$ es una extensión finita, pues $[K(v_0,\dots,v_n)(u):K] =$

$= [K(v_0,\dots,v_n)(u):K(v_0,\dots,v_n)]\cdot[K(v_0,\dots,v_n):K]$.

Por tanto, $K(v_0,\dots,v_n)|K$ es una extensión algebraica (PROPOSICION 4.1) y, en definitiva, u es algebraico sobre K. Luego $L|K$ es algebraica, esq

TEMA 11º: CLAUSURA ALGEBRAICA. CUERPO DE DESCOMPOSICION.

1. CUERPO ALGEBRAICAMENTE CERRADO. CLAUSURA ALGEBRAICA.

DEFINICION: Un cuerpo K es algebraicamente cerrado si no admite una extensión algebraica propia, es decir, si $lK|K$ es una extensión algebraica, entonces $lK = K$.

11. TEOREMA: Las proposiciones siguientes son equivalentes:

a) K es algebraicamente cerrado.

b) Cada polinomio con coeficientes en K tiene una raiz en K.

c) Cada polinomio con coeficientes en K se descompone en $K[x]$.

Demostr.: **a) ⇒ b)** Sea f un polinomio con coeficientes en K. Consideremos $\mathbf{K} = K(u)$ un cuerpo de ruptura de f; $f(u) = 0$.
Entonces u es algebraico sobre K y, por tanto, la extensión $K(u)|K$ es algebraica (Teorema 4.3., Tema 10). Por hipótesis K es algebraicamente cerrado. Luego $K(u) = K$ y, en consecuencia, $u \in K$. Luego f tiene una raiz en K.

b ⇒ c) Sea $f \in K[x]$. Por hipótesis, existe $u_0 \in K$ tal que $f(u_0) = 0$.
Entonces $f(x) = (x - u_0) f_1(x)$, donde $f_1(x) \in K[x]$.
Analogamente, existe $u_1 \in K$ tal que $f_1(u_1) = 0$. Luego $f(x) = (x-u_0)(x-u_1) f_2(x)$. Pero este proceso es finito, pues f tiene un número finito de raices. Por tanto podremos escribir

$$f(x) = c \cdot \prod_{i=0}^{n} (x - u_i), \quad c \in K, \{u_i\}_{i=0}^{n} \subset K.$$

c ⇒ a) Sea $lK|K$ una extensión algebraica.
Dado $u \in lK$, sea f el polinomio mínimo de u en $K[x]$ (*)
Por hipótesis, $f = c \prod_{i=0}^{n} (x - v_i)$, $c \in K$, $\{v_i\}_{i=0}^{n} \subset K$.
Entonces, siendo $f(u) = 0$, $\exists i \in \{0, \dots, n\} / u = v_i$. Luego $u \in K$.
En definitiva, $lK = K$. c.s.q.d.

EJEMPLO: $\mathbb{C}$ es un cuerpo algebraicamente cerrado.

DEFINICION: Sea K un cuerpo y $lK|K$ una extensión. Diremos que lK es una clausura algebraica de K si $lK|K$ es una extensión algebraica maximal de K, es decir, si verifica:

a) $lK|K$ es algebraica.

b) Si lK' es una extensión algebraica sobre K y lK' es una extensión

de $\mathbb{K}$, entonces $\mathbb{K}'=\mathbb{K}$.
Es equivalente a decir que $\mathbb{K}$ sea una clausura algebraica de K, que $\mathbb{K}|K$ sea algebraica y $\mathbb{K}$ sea algebraicamente cerrado

1.2. TEOREMA: Sea K un cuerpo. Entonces, existe un cuerpo L algebraicamente cerrado que contiene a K como subcuerpo.

Demostr: Veamos que existe un cuerpo E_1 en el que todo polinomio con coeficientes en K tiene una raiz.
Asociamos a cada $f\in K[x]$ una indeterminada x_f y consideremos el conjunto $S=\{x_f / f\in K[x]\}$, que se corresponde biyectivamente con $K[x]$. Denotamos por $K[S]$ el conjunto de polinomios con un número finito de indeterminadas de S, es decir, si $g\in K[S]$ es de la forma $g=\sum \lambda_{i_1\dots i_n} x_{f_{i_1}}^{\gamma_{i_1}}\cdot\dots\cdot x_{f_{i_r}}^{\gamma_{i_r}}$, $f_{i_k}\in K[x]$.
Trivialmente, $K[S]$ tiene estructura de anillo.
Consideremos el conjunto $H=\{f(x_f)\in K[S] / f\in K[x]\}$, es decir, un elemento de H es un polinomio que tiene los mismos coeficientes en K que un cierto polinomio $f\in K[x]$ y con la indeterminada x_f correspondiente. Sea $\mathfrak{a}$ el ideal de $K[S]$ generado por H. Este ideal es distinto de $K[S]$, pues si fuese igual se tendría que 1, elemento unidad de $K[S]$, pertenecería a $\mathfrak{a}$ y, por tanto, existirían $g_1,\dots,g_n\in K[S]$ tal que $g_1 f_1(x_{f_1})+\dots+g_n f_n(x_{f_n})=1$, pues de esta forma son los elementos del ideal generado por H. Escribiremos, para simplificar la notación, $x_{f_i}=x_i$. Los polinomios g_i tienen un número finito de indeterminadas x_i (elementos de S) y podemos suponer que son $x_1,\dots,x_N$ las indeterminadas de dichos polinomios, es decir, de manera que $g_i=g_i(x_1,\dots,x_N)$, y también podemos considerar $N\geq n$.
Tendríamos, entonces, que $\sum_{i=1}^{n} g_i(x_1,\dots,x_N) f_i(x_i)=1$. Sea F un cuerpo en el que cada polinomio f_i tenga una raiz α_i. (*)
Sustituyendo entonces x_i por α_i obtendríamos que, haciendo $\alpha_i=0$ si $i>n$, $\sum_{i=1}^{n} g_i(\alpha_1,\dots,\alpha_n,0,\dots,0) f_i(\alpha_i)=0$, lo cual es absurdo, pues $\sum_{i=1}^{n} g_i(x_1,\dots,x_N) f_i(x_i)=1$
Por tanto debe ser $\mathfrak{a}\neq K[S]$. Sea, entonces, $\mathfrak{M}$ un ideal maxi-

(*) Este cuerpo F existe, en virtud del siguiente corolario del teorema de Kronecker:
Corolario: Dado un cuerpo K y $\{f_1,\dots,f_n\}$ una familia de polinomios sobre K de grado mayor o igual que 1. Existe entonces una extensión F de K en la que cada f_i tiene una raiz.
Demostr: Sea F_1 una extensión de K en la que f_1 tiene una raiz. Como $K\subset F_1$ podemos suponer que $f_2\in F_1[x]$. Por Th. de Kronecker, existe una extensión F_2 de F_1 y, por tanto de K, en la que f_2 tiene una raiz. Además f_1 tiene una raiz en F_1 y, por tanto en F_2. Así sucesivamente llegamos a una extensión $F=F_n$ de K en la que cada f_i tiene una raiz.

mal de $K[S]$ que contiene a ∂.

$K[S]/M$ es un cuerpo, pues M es maximal, y el homomorfismo canónico $\sigma: K[S] \longrightarrow K[S]/M$ restringido a K es inyectivo, pues σ/K es un homomorfismo de cuerpos.

Dado un polinomio $f \in K[x]$ cualquiera, por el mismo razonamiento hecho en la demostración del teorema de Krönecker se tiene que $f^{\sigma}(x_f) \in K[S]/M$ tiene una raiz en $K[S]/M$, y que existe una extensión E_1 de K en la que todo polinomio $f \in K[x]$ tiene una raiz (si $\partial^{\circ}(f) \geq 1$).

De la misma manera se prueba que existe una extensión E_2 de E_1 en la que todo polinomio de $E_1[x]$ tiene una raiz y, en general, que dado $n \in \mathbb{N}$ existe una extensión E_{n+1} de E_n en la que todo polinomio de $E_n[x]$ tiene una raiz.

Tenemos, entonces, una sucesión de cuerpos $E_1 \subset \dots \subset E_n \subset \dots$ (I)

Sea $L = \bigcup_{n \in \mathbb{N}} E_n$. Evidentemente, L es un cuerpo que contiene a K. Además, dado un polinomio de $L[x]$, $f(x) = a_0 + a_1 x + \dots + a_m x^m$, $a_i \in L$, existe $n \in \mathbb{N}$ tal que $a_i \in E_n$, $i = 0, \dots, m$, en virtud de las contenciones (I). Luego $f(x) \in E_n[x]$ y, por tanto, f tiene una raiz en E_{n+1} y, en consecuencia, en L. Lo cual, de acuerdo con TEOREMA 1.1, significa que L es algebraicamente cerrado. c.s.q.d.

1.3. COROLARIO: Todo cuerpo K admite una clausura algebraica, es decir, dado un cuerpo K existe un cuerpo $\bar{K}$ tal que $\bar{K} \supset K$, $\bar{K}|K$ es una extensión algebraica y $\bar{K}$ es algebraicamente cerrado.

Demostr.: Por el teorema anterior existe una extensión L de K de modo que L es algebraicamente cerrado.

Sea $\bar{K} = \{u \in L \,/\, u \text{ es algebraico sobre } K\}$. Según COROLARIO 4.4 (Tema 10), $\bar{K}$ es una extensión algebraica de K. Veamos que $\bar{K}$ es algebraicamente cerrado.

Sea $f \in \bar{K}[x]$. Como $\bar{K} \subset L$ y L es algebraicamente cerrado, f tiene una raiz u en L. Luego u es algebraico sobre $\bar{K}$ y, por tanto, $\bar{K}(u)|\bar{K}$ es algebraica. Como $\bar{K}|K$ es algebraica, según PROPOSICION 4.5, $\bar{K}(u)|K$ es algebraica. Luego u es algebraico sobre K. Entonces, por definición de $\bar{K}$, $u \in \bar{K}$, que prueba que f tiene una raiz en $\bar{K}$ y, en consecuencia, que $\bar{K}$ es algebraicamente cerrado. c.s.q.d.

1.4 LEMA: a) Si K es un cuerpo infinito y $|K|K$ es algebraica entonces $\text{card}(|K) = \text{card}(K)$.
b) Si K es finito y $|K|K$ es algebraica, $\text{card}(|K) \leq \aleph_0$. (*)

Demostr.: a) Supongamos que K es un cuerpo infinito y $|K|K$ una extensión algebraica.
Sea $P = \{f \in K[x] / f \text{ es mónico}\}$ y sea $P_n = \{f \in P / \partial^\circ(f) = n\}$.
Evidentemente la aplicación $\varphi: (a_0, a_1, \dots, a_{n-1}) \in K^n \longmapsto a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + x^n \in P_n$ es biyectiva. Luego $\text{card}(P_n) = \text{card}(K^n)$.
Según un teorema de teoría de cardinales si K es infinito, $\text{card}(K^n) = \text{card}(K)$. Luego $\text{card}(P_n) = \text{card}(K)$
Siendo $P = \bigcup_{n=0}^{\infty} P_n$ se verifica que

$$\text{card}(P) \leq \aleph_0 \cdot \text{card}(K) = \text{card}(K) \quad (I)$$

Por otro lado, la extensión $|K|K$ es algebraica; luego a cada elemento $u \in |K$ podemos hacerle corresponder el polinomio mínimo de u sobre K, f_u, que podemos notar por $f_u = \text{Irr}(u, K)$. Sea $R_u = \{v \in |K / f_u(v) = 0\}$.
Trivialmente, $|K = \bigcup_{u \in |K} R_u$.
Sea P' el conjunto de polinomios de P que son mínimos para algún $u \in |K$, $P' = \{f \in P / \exists u \in |K / f = \text{Irr}(u, K)\}$.
Entonces, si denotamos por $R_f = \{v \in |K / f(v) = 0\}$, tenemos que

$$|K = \bigcup_{u \in |K} R_u = \bigcup_{f \in P'} R_f$$

Como $\text{card}(R_f) \leq \aleph_0$ tenemos que

$$\text{card}(|K) \leq \aleph_0 \cdot \text{card}(P') \leq \aleph_0 \cdot \text{card}(P) \overset{(I)}{\leq} \aleph_0 \cdot \text{card}(K) = \text{card}(K)$$

Además $K \subset |K \Rightarrow \text{card}(K) \leq \text{card}(|K)$
Luego $\text{card}(K) = \text{card}(|K)$.

b) Supongamos que K es un cuerpo finito y $|K|K$ una extensión algebraica. Utilizando las mismas notaciones que en el caso anterior, si $\text{card}(K) = q$, $\text{card}(P_n) = q^n \leq \aleph_0$
Luego $\text{card}(P) \leq \aleph_0 \cdot \aleph_0 = \aleph_0$.
De la misma manera que en a), $|K = \bigcup_{f \in P'} R_f$.
Luego $\text{card}(|K) \leq \aleph_0 \cdot \text{card}(P') \leq \aleph_0 \cdot \text{card}(P) \leq \aleph_0 \cdot \aleph_0 = \aleph_0$. c.s.q.d.

Utilizando este lema vamos a probar de otro modo el COROLARIO 13.

1.5. TEOREMA: Todo cuerpo K admite una clausura algebraica.

Demostr.: Sea Ω un conjunto que contiene a K y tal que $\text{card}(\Omega) > \max(\aleph_0, \text{card}\, K)$. Siempre podemos encontrar un conjunto Ω que satisfaga lo anterior. (*)

Sea $\mathcal{J} = \{K \subset \Omega \,/\, K \text{ cuerpo} \supset K \text{ y } K|_K \text{ es algebraica}\}$.

Evidentemente $\mathcal{J} \neq \emptyset$, pues $K \in \mathcal{J}$. Definimos en $\mathcal{J}$ un orden $\leq$ por: $K_1 \leq K_2$ si $K_1 \subset K_2$.

Probemos que este orden es inductivo, es decir, que toda cadena admite cota superior. Sea $\Sigma = (|K_i)_{i\in I}$ una cadena en $\mathcal{J}$.

Trivialmente, $|K = \bigcup_{i\in I} |K_i$ es un cuerpo y está contenido en Ω.

Probemos que $|K|_K$ es una extensión algebraica.

Dado $u \in |K$, existe $i \in I$ tal que $u \in |K_i$. Como $|K_i|_K$ es algebraica, u es algebraico sobre K. Por tanto, $|K$ es una cota superior de Σ.

El lema de Zorn nos garantiza la existencia en $\mathcal{J}$ de un elemento maximal $\overline{K}$. Probemos que $\overline{K}$ es una clausura algebraica de K. Dado que $\overline{K} \in \mathcal{J}$, nos resta probar que $\overline{K}$ es un cuerpo algebraicamente cerrado.

Supongamos que E es una extensión algebraica de $\overline{K}$. Queremos ver que $E = \overline{K}$. Si $E|_{\overline{K}}$ es algebraica, como $\overline{K}|_K$ también es algebraica, tenemos que la extensión $E|_K$ es algebraica. Según el lema anterior, $\text{card}(E) \leq \max(\aleph_0, \text{card}(K)) < \text{card}(\Omega)$. Entonces $\text{card}(E - \overline{K}) < \text{card}(\Omega - \overline{K})$.

Existe entonces una inyección $\varphi: E - \overline{K} \to \Omega - \overline{K}$ que podemos prolongar mediante la identidad en $\overline{K}$ a la aplicación inyectiva:

$$\sigma: E \longrightarrow \Omega$$
$$x \longmapsto \sigma(x) = \begin{cases} = x \text{ si } x \in \overline{K} \\ = \varphi(x) \text{ si } x \in E - \overline{K} \end{cases}$$

Si $E' = \sigma(E)$, $\sigma: E \to E'$ es una biyección.

Mediante σ podemos transportar la estructura de cuerpo de E a E' del siguiente modo:

$\forall x', y' \in E'$, $x' + y' = \sigma(\sigma^{-1}(x') + \sigma^{-1}(y'))$, $x' \cdot y' = \sigma(\sigma^{-1}(x') \cdot \sigma^{-1}(y'))$.

Trivialmente, las restricciones de estas leyes de composición a $\overline{K}$ coinciden con las operaciones que ya teníamos en $\overline{K}$.

Probemos que $E'|\bar{K}$ es una extensión algebraica. (*)
Sea $u' \in E'$; existe entonces $u \in E$ tal que $u' = \sigma(u)$.
Como $E|\bar{K}$ es algebraica, existe $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \bar{K}[x]$ tal que $f(u) = 0$. Veamos que $f(\sigma(u)) = 0$; observar que $f = f^\sigma$.
$f(\sigma(u)) = a_0 + a_1 \sigma(u) + \dots + a_n \sigma(u)^n = \sigma(a_0 + a_1 u + \dots + a_n u^n) = \sigma(0) = 0$
Luego u' es algebraico sobre $\bar{K}$.
Entonces $E' \subset \Omega$, $E'|K$ es algebraica (pues lo son $E'|\bar{K}$ y $\bar{K}|K$) y $\bar{K}$ maximal de f. Luego $E' = \bar{K}$ y, por tanto,
$$E = \sigma^{-1}(E') = \sigma^{-1}(\bar{K}) = \bar{K}. \quad \text{c.s.q.d.}$$

2. CUERPO DE DESCOMPOSICION DE UNA FAMILIA DE POLINOMIOS.

DEFINICION: Sea P una familia de polinomios sobre un cuerpo K. Diremos que $\mathbb{K}$ es un cuerpo de descomposición de P si:
a) Cada $f \in P$ se descompone en la forma $f(x) = c \prod_{i=1}^{n} (x - u_i)$, $c, u_i \in \mathbb{K}$.
b) $\mathbb{K} = K(S)$ donde S es el conjunto de las raices de los polinomios de P en $\mathbb{K}$. (Lo denotamos así: $S = \text{Raices}_{\mathbb{K}} P$).

2.1. TEOREMA: Dado un cuerpo K y una familia P de polinomios de $K[x]$, existe $\mathbb{K}$ cuerpo de descomposición de P.

Demostr.: Sea $\bar{K}$ una clausura algebraica. Entonces, por ser $\bar{K}$ algebraicamente cerrado, cada polinomio $f \in P$ se descompone en $\bar{K}$.
Sea S el conjunto de las raices de los polinomios de P en $\bar{K}$; esto lo denotamos así: $S = \text{Raices}_{\bar{K}} P$
Sea $\mathbb{K} = K(S)$. Entonces $\mathbb{K}$ es un cuerpo de descomposición de P, pues cada $f \in P$ se descompone en la forma $f(x) = c \prod_{i=1}^{n} (x - u_i)$ donde $c \in K$ y $u_i \in S$ y, por tanto, $c \in \mathbb{K}$ y $u_i \in \mathbb{K}$, $i = 1, \dots, n$, y además S es el conjunto de raices de P en $\mathbb{K}$, pues $S \subset \mathbb{K}$ y en S están todas las raices de P. c.s.q.d.

OBSERVACION: Indirectamente, en la demostración de la existencia del cuerpo de descomposición se ha utilizado el lema de Zorn, pues se ha utilizado el teorema 1.5. Vamos a probar la existencia del cuerpo de descomposición si la familia P es numerable, sin utilizar dicho lema.
(1) Si P es unitario, $P = \{f\}$ con $f \in K[x]$, consideremos $\mathbb{K}_1$ un cuerpo de ruptura de f: $\mathbb{K}_1 = K(u_1)$. Entonces, $f = (x - u_1) f_1(x)$, con $f_1(x) \in \mathbb{K}_1[x]$.
Sea $\mathbb{K}_2 = \mathbb{K}_1(u_2)$ un cuerpo de ruptura de f_1. Entonces $f = (x - u_1)(x - u_2) f_2(x)$.
Así sucesivamente, en un número finito de pasos, pues f tiene un número finito de raices, obtendremos que $K \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \dots \subset \mathbb{K}_n$ y $f = c \prod_{i=1}^{n} (x - u_i)$

Por tanto f se descompone en $\mathbb{K}_n$. Además
$\mathbb{K}_n = \mathbb{K}_{n-1}(u_n) = \mathbb{K}_{n-2}(u_{n-1})(u_n) = \dots = K(u_1, \dots, u_n)$
donde $\{u_1, \dots, u_n\} = \text{Raices}_{\mathbb{K}_n} f$.
Luego $\mathbb{K}_n$ es un cuerpo de descomposición de $P = \{f\}$.

(2) Supongamos ahora que $P = \{f_n\}_{n \in \mathbb{N}} \subset K[x]$
Sea E_1 el cuerpo de descomposición de f_1 sobre K.
Como $K \subset E_1$ podemos suponer que $f_2 \in E_1[x]$. Sea entonces, E_2 el cuerpo de descomposición de f_2 sobre E_1. Así sucesivamente, llamamos E_n al cuerpo de descomposición de f_n sobre E_{n-1}, para cada $n \in \mathbb{N}$.
Dado que $E_1 \subset \dots \subset E_n \subset \dots$ se verifica trivialmente que $E = \bigcup_{n \in \mathbb{N}} E_n$ es un cuerpo. Dado $f_n \in P$, f_n se descompone en E_n y, por tanto, en E.
Sea, para cada $n \in \mathbb{N}$, $S_n = \text{Raices}_{E_n} f_n$. Entonces
$E_n = E_{n-1}(S_n) = E_{n-2}(S_{n-1} \cup S_n) = \dots = K(S_1 \cup S_2 \cup \dots \cup S_n)$
Luego $E = K(\bigcup_{n \in \mathbb{N}} S_n)$, que prueba que E es un cuerpo de descomposición de P.

Para probar la "unicidad" del cuerpo de descomposición de una familia de polinomios probaremos antes un teorema más general.

2.2. TEOREMA: Sean K y K' dos cuerpos y $\sigma: K \to K'$ un isomorfismo. Sea P una familia de polinomios de $K[x]$ y $\mathbb{K}$ un cuerpo de descomposición de P sobre K. Sea $\mathbb{K}'$ un cuerpo de descomposición de $\sigma(P) = \{f^\sigma / f \in P\}$ sobre K'. Entonces existe un isomorfismo $\bar{\sigma}: \mathbb{K} \to \mathbb{K}'$ que prolonga a σ, es decir, tal que $\bar{\sigma}|_K = \sigma$.

Demostr.: (a) Supongamos, en un primer caso, que P es unitaria: $P = \{f\}$.
Probaremos el teorema por inducción sobre $\partial^\circ(f)$.
Si $\partial^\circ(f) = 1$, $f(x)$ será de la forma $x - u$ (no es ninguna restricción considerarlo mónico). Como $f \in K[x]$ se tiene $u \in K$ y, por tanto, $\mathbb{K} = K(u) = K$. De la misma manera, siendo $\partial^\circ(f^\sigma) = 1$, $\mathbb{K}' = K'$.
Supongamos cierto el teorema para polinomios de grado $n-1$.
Sea f un polinomio de grado n. Sea u una raiz de f en $\mathbb{K}$.
Consideremos el polinomio mínimo de u en K: $g = \text{Irr}(u, K)$.
Siendo g irreducible en K y σ isomorfismo se verifica que g^σ es irreducible en K'. Sea u' una raiz de g^σ en $\mathbb{K}'$
Entonces, $K(u)$ es un cuerpo de ruptura de g y $K'(u')$, un cuerpo de ruptura de g^σ. Luego, según teorema 3.1 (Tema 10), σ se puede extender

der a un isomorfismo σ_1 de $K(u)$ en $K'(u')$ de modo que $\sigma_1(u) = u'$. Entonces en $K(u)$ f admite la siguiente expresión: $f(x) = (x-u) f_1(x)$ y en $K'(u')$ podemos escribir $f^{\sigma_1}(x) = (x-u') f_1^{\sigma_1}(x)$; además, si $\mathbb{K}$ es cuerpo de descomposición de f en K y $\{u, u_1, \dots, u_{n-1}\} = \text{Raices}_{\mathbb{K}} f$ entonces $\mathbb{K} = K(u, u_1, \dots, u_{n-1}) = K(u)(u_1, \dots, u_{n-1})$ y, por tanto, $\mathbb{K}$ es cuerpo de descomposición de f_1 en $K(u)$, ya que $f_1(x) = \prod_{i=1}^{n-1}(x-u_i)$. Del mismo modo $\mathbb{K}'$ es cuerpo de descomposición de $f_1^{\sigma_1}$ en $K'(u')$.

Siendo $\partial^\circ(f_1) = \partial^\circ(f_1^{\sigma_1}) = n-1$, por hipótesis de inducción, el isomorfismo $\sigma_1 : K(u) \to K'(u')$ se puede extender a un isomorfismo $\overline{\sigma} : \mathbb{K} \to \mathbb{K}'$, que también es una prolongación de σ.

(b) Supongamos que $\mathcal{P}$ es una familia cualquiera de polinomios de $K[x]$. Para una subfamilia S de $\mathcal{P}$ denotaremos por $\mathbb{K}_S$ el conjunto $K(\text{Raices}_{\mathbb{K}} S)$, es decir $\mathbb{K}_S$ es el cuerpo de descomposición de S. Análogamente denotaremos $\mathbb{K}'_S = K'(\text{Raices}_{\mathbb{K}'} \sigma(S))$

Consideremos $\mathcal{J} = \{(S, \alpha) / S \subset \mathcal{P}$ y α es isomorfismo de $\mathbb{K}_S$ en $\mathbb{K}'_S$ tal que σ prolongue a $\alpha\}$

Veamos que $\mathcal{J}$ es un conjunto: Los K-isomorfismos de $\mathbb{K}_S$ en $\mathbb{K}'_S$ forman un conjunto (subconjunto del conjunto producto $\mathbb{K}'^{\mathbb{K}_S}_S$). Si denotamos por $\mathcal{I}_S$ dicho conjunto tenemos que dado $S \in \mathcal{P}(\mathcal{P})$ $(S, \alpha) \in \{S\} \times \mathcal{I}_S$. Luego $\mathcal{J} = \bigcup_{S \in \mathcal{P}(\mathcal{P})} \{S\} \times \mathcal{I}_S$ que es un conjunto como unión de conjuntos.

Además $\mathcal{J}$ es no vacío, pues si S es unitario está probado en el apartado (a) la existencia de un isomorfismo $\overline{\sigma} : \mathbb{K}_S \to \mathbb{K}'_S$ y, por tanto, $(S, \overline{\sigma}) \in \mathcal{J}$.

Definimos en $\mathcal{J}$ una relación $\lesssim$ del siguiente modo:

$(S_1, \alpha_1) \lesssim (S_2, \alpha_2) \overset{\text{def}}{\Longleftrightarrow} (S_1 \subset S_2)$ y $(\alpha_2 | \mathbb{K}_{S_1} = \alpha_1)$

Fácilmente se comprueba que $\lesssim$ es un orden en $\mathcal{J}$.

Probemos ahora que este orden es inductivo, es decir, que toda cadena en $\mathcal{J}$ admite una cota superior.

Sea $\Sigma = ((S_i, \alpha_i))_{i \in I}$ una cadena en $\mathcal{J}$

Sea $S = \bigcup_{i \in I} S_i$. Evidentemente, $\mathbb{K}_S = K(\text{Raices}_{\mathbb{K}} \bigcup_{i \in I} S_i) \supset \bigcup_{i \in I} K(\text{Raices}_{\mathbb{K}} S_i)$ pues $\forall i \in I$, $S_i \subset \bigcup_{i \in I} S_i \Rightarrow \text{Raices}_{\mathbb{K}} S_i \subset \text{Raices}_{\mathbb{K}} S \Rightarrow K(\text{Raices}_{\mathbb{K}} S_i) \subset \mathbb{K}_S$, $\forall i \in I$.

Si probamos que $\bigcup_{i \in I} K(\text{Raices}_{\mathbb{K}} S_i)$ es un cuerpo, por contener a K y a las raíces de S en K y siendo $\mathbb{K}_S$ el menor cuerpo que verifica esto, quedará visto que $\mathbb{K}_S = \bigcup_{i \in I} K(\text{Raices}_{\mathbb{K}} S_i)$.

Pero que $\bigcup_{i \in I} K(\text{Raices}_{\mathbb{K}} S_i)$ es un cuerpo es trivial, pues siendo Σ cadena dados $i, j \in I$, $S_i \subset S_j$ ó $S_j \subset S_i \Rightarrow K(\text{Raices}_{\mathbb{K}} S_i) \subset K(\text{Raices}_{\mathbb{K}} S_j)$ ó

Definimos entonces

$$\alpha : |K_S \longrightarrow |K'_S$$

$$x \longmapsto \alpha(x) = \alpha_i(x) \text{ si } x \in K(\text{Raices}_{|K} S_i) = |K_{S_i}$$

α está bien definida, pues si $x \in |K_{S_i} \cap |K_{S_j}$ se tendría que $\alpha(x) = \alpha_i(x)$ y $\alpha(x) = \alpha_j(x)$; pero esto no significa que x tenga dos imágenes, pues, siendo Σ una cadena, podemos suponer que $(S_i, \alpha_i) \lesssim (S_j, \alpha_j)$ y, por tanto, $\alpha_j|_{|K_{S_i}} = \alpha_i$; luego $\alpha_j(x) = \alpha_i(x)$.
Es trivial que α es isomorfismo. Luego $(S, \alpha) \in \mathcal{J}$ y además es una cota superior de Σ, pues $\forall i \in I$, $S_i \subset S$ y $\alpha|_{|K_{S_i}} = \alpha_i$ por definición.
Por tanto, el lema de Zorn garantiza la existencia de un elemento maximal en $\mathcal{J}$. Sea (T, δ) dicho elemento maximal.
Veamos que $T = P$. Si fuese $T \neq P$, existiría $f \in P - T$.
Sea $R = T \cup \{f\}$. $\delta : |K_T \to |K'_T$ es un isomorfismo. Además

$$|K_R = K(\text{Raices}_{|K} T \cup \{f\}) = K[(\text{Raices}_{|K} T) \cup (\text{Raices}_{|K} \{f\})] =$$
$$= K(\text{Raices}_{|K} T)(\text{Raices}_{|K} f) = |K_T(\text{Raices}_{|K} f)$$

Es decir, $|K_R$, cuerpo de descomposición de R sobre K, es un cuerpo de descomposición de f sobre $|K_T$. Análogamente, $|K'_R = |K'_T(\text{Raices}_{|K'} f^\sigma)$
Entonces, por el caso (a), el isomorfismo $\delta : |K_T \to |K'_T$ se puede extender a un isomorfismo $\bar{\delta} : |K_R \to |K'_R$. Tendríamos entonces que $(R, \bar{\delta}) \in \mathcal{J}$, $(T, \delta) \lesssim (R, \bar{\delta})$ y $(T, \delta) \neq (R, \bar{\delta})$ en contra del carácter maximal de (T, δ).
Debe ser entonces $T = P$ y δ un isomorfismo de $|K_P = |K$ en $|K'_P = |K'$ que prolonga a σ. c.s.q.d.

2.3. Corolario Dos cuerpos de descomposición de una familia de polinomios P sobre un cuerpo K son K-isomorfos.

Demostr.: Sean $|K$ y $|K'$ cuerpos de descomposición de P. El isomorfismo identidad $i : K \to K$ se puede prolongar a un isomorfismo $\bar{i} : |K \to |K'$ que prueba que $|K$ y $|K'$ son K-isomorfos. c.s.q.d.

2.4. Teorema: Sea K un cuerpo. Entonces $\bar{K}$ es una clausura algebraica de K si, y solo si, $\bar{K}$ es un cuerpo de descomposición de $K[x]$.

Demostr.: $\Rightarrow$| Supongamos que $\bar{K}$ es una clausura algebraica de K. Entonces, siendo $\bar{K}$ algebraicamente cerrado, todo polinomio $f \in K[x]$ se descompone en $\bar{K}$.
Sea $S = \text{Raices}_{\bar{K}} K[x]$. Veamos que $\bar{K} = K(S)$ en [illegible]

terminada esta demostración. Como $K, S \subset \bar{K}$ se tiene que $K(S) \subset \bar{K}$, pues $K(S)$ es el menor cuerpo que contiene a K y a S. Dado $u \in \bar{K}$, como la extensión $\bar{K}|K$ es algebraica, u es raiz de un cierto polinomio $f \in K[x]$. Por tanto $u \in S \subset K(S)$. Luego $\bar{K} = K(S)$, que prueba que $\bar{K}$ es cuerpo de descomposición de $K[x]$.

$\Leftarrow$| Si $\bar{K}$ es cuerpo de descomposición de $K[x]$ se tiene que $\bar{K} = K(S)$ donde $S = \text{Raices}_{\bar{K}} K[x]$. Todo elemento u de K es algebraico sobre K (trivial pues es raiz de $x-u \in K[x]$) y todo elemento de S es algebraico sobre K, por definición de S, luego la extensión $K(S)|K$ es algebraica, es decir, $\bar{K}|K$ es algebraica.

Veamos que $\bar{K}$ es algebraicamente cerrado.

Sea $\mathbb{K}|\bar{K}$ una extensión algebraica; siendo $\bar{K}|K$ algebraica se tiene que $\mathbb{K}|K$ es algebraica, es decir, dado $u \in \mathbb{K}$, u es raiz de un cierto polinomio de $K[x]$. Luego u pertenece al cuerpo de descomposición de $K[x]$, es decir, $u \in \bar{K}$. Luego $\mathbb{K} \subset \bar{K}$

Además siendo $\mathbb{K}$ una extensión de $\bar{K}$ debe ser $\mathbb{K} = \bar{K}$. Luego $\bar{K}$ es algebraicamente cerrado. En definitiva, $\bar{K}$ es clausura algebraica. cqd

2.5. COROLARIO: Si K y K' son dos cuerpos, $\sigma: K \to K'$ un isomorfismo y $\bar{K}$ y $\bar{K}'$ clausuras algebraicas respectivas de K y K', entonces σ se puede extender (o prolongar) a un isomorfismo $\bar{\sigma}: \bar{K} \to \bar{K}'$.

Demostr.: Segun el teorema anterior, $\bar{K}$ y $\bar{K}'$ son cuerpos de descomposición de $K[x]$ y $K'[x]$, respectivamente.

Siendo σ isomorfismo tenemos trivialmente que $K'[x] = \sigma(K[x])$.

Entonces, segun Teorema 2.2, existe un isomorfismo $\bar{\sigma}: \bar{K} \to \bar{K}'$ que prolonga a σ. cqd.

2.6. COROLARIO: Dos clausuras algebraicas de un mismo cuerpo K son K-isomorfas.

Demostr.: La identidad $i: K \to K$ es un isomorfismo que se puede prolongar a un isomorfismo $\bar{i}: \bar{K}_1 \to \bar{K}_2$, donde $\bar{K}_1$ y $\bar{K}_2$ son clausuras algebraicas de K. Por tanto, $\bar{i}$ es un K-isomorfismo entre ambas clausuras. cqd.

2.7. PROPOSICION: a) Supuesto que $\mathbb{K}|K$ es algebraica, si $\overline{\mathbb{K}}$ es clausura algebraica de $\mathbb{K}$, entonces $\overline{\mathbb{K}}$ es clausura algebraica de K.

b) Si $K \subset \mathbb{K} \subset \bar{K}$, donde $\bar{K}$ es una clausura algebraica de K, entonces $\bar{K}$ es clausura algebraica de $\mathbb{K}$.

Demostr.: a) $\overline{\mathbb{K}}$ es algebraicamente cerrado por ser clausura algebraica de $\mathbb{K}$. Además la extensión $\overline{\mathbb{K}}|\mathbb{K}$ es algebraica pues lo son las extensiones $\overline{\mathbb{K}}|\mathbb{K}$ y $\mathbb{K}|\mathbb{K}$. Luego $\overline{\mathbb{K}}$ es clausura algebraica de $\mathbb{K}$.

b) $\overline{K}$ es algebraicamente cerrado. Además, como $\overline{K} \supset \mathbb{K}$, $\overline{K}$ es una extensión de $\mathbb{K}$. Veamos fue es algebraica.

Siendo $\overline{K}|\mathbb{K}$ algebraica, según Proposición 4.5 (Tema 10), $\overline{K}|\mathbb{K}$ es algebraica y, por tanto, $\overline{K}$ es clausura algebraica de $\mathbb{K}$. c.s.q.d.

Apuntes de la asignatura
ÁLGEBRA II
de Agustín García Nogales
Licenciatura en Matemáticas UEx
Curso 1980/1981
Profesor: Francisco Montalvo
TEORÍA DE GALOIS

TEMA 12°: CUERPOS FINITOS

Antes de entrar en el estudio de los cuerpos finitos veamos algunos conceptos de polinomios sobre cuerpos.

DEFINICION: (Derivada de un polinomio)

Dado un cuerpo K se define la aplicación derivada como una aplicación $D: K[x] \longrightarrow K[x]$ que a cada polinomio $f(x) = a_0 + a_1x + \dots + a_nx^n$ asocia el polinomio $D(f(x)) = a_1 + 2a_2x + \dots + na_nx^{n-1}$

Se comprueba que D es un endomorfismo del espacio vectorial de los polinomios con coeficientes en K.

Se demuestra, además, que $D(f\cdot g) = f\cdot D(g) + g\cdot D(f)$.

* Dado un cuerpo K y $f(x) \in K[x]$, si $\mathbb{K}$ es un cuerpo de descomposición de f, f se descompone en $\mathbb{K}[x]$ en la forma

$$f(x) = c(x-u_1)^{r_1}\cdots(x-u_n)^{r_n}, \text{ con } u_i \neq u_j \text{ si } i \neq j.$$

Diremos que la raiz u_K es simple si $r_K = 1$ y diremos que es múltiple si $r_K > 1$. A r_K se le llama orden de multiplicidad de u_K.

Vamos a demostrar una proposición que despues utilizaremos para probar un teorema fundamental sobre cuerpos finitos.

PROPOSICION: Sea K un cuerpo y f un polinomio mónico (*) sobre K. Entonces condición necesaria y suficiente para que f no tenga raices múltiples en un cuerpo de descomposición $\mathbb{K}$ de f que el maximo común divisor de f y su polinomio derivado $D(f) = f'$ en $K[x]$ sea 1, o una unidad de $K[x]$, es decir que sea constante.

Demostr.: $\Rightarrow$] Supongamos que todas las raices de f en $\mathbb{K}$ son simples. Siendo $\mathbb{K}$ cuerpo de descomposición de f tenemos que

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

y, segun lo dicho, se tiene que $u_i \neq u_j$ si $i \neq j$.

El polinomio derivado de f es

$$f'(x) = \sum_{j=1}^{n}(x-u_1)\cdots(x-u_{j-1})\overset{\vee}{(x-u_j)}(x-u_{j+1})\cdots(x-u_n)$$

donde $\overset{\vee}{(x-u_j)}$ significa que se suprime el término $x-u_j$, es decir, $f'(x)$ es la suma de n términos formados por $n-1$ de los factores de $f(x)$ (suprimiendo un factor en cada término).

Entonces $\forall i \in \{1,\dots,n\}$, $(x-u_i) \nmid f'(x)$, pues $x-u_i$ divide a todos los sumandos de $f'(x)$ excepto a $\overset{\vee}{(x-u_1)}\cdots(x-u_i)\cdots(x-u_n)$ y se tiene $(x-u_i) \nmid (x-u_j)$ si $i \neq j$. Entonces si $d = mcd(f,f')$ en $K[x]$ se

ser $\partial^\circ(d)=0$, pues si $\partial^\circ(d)\geq 1$, como $d \mid f$, para un cierto $i\in\{1,\dots,n\}$ se tendría que $(x-u_i)\mid d$ y, como $d\mid f'$ se verificaría que $(x-u_i)\mid f'$ contra lo probado. Luego $\partial^\circ(d)=0$ y, por tanto, d es constante, es decir, d es una unidad. Se puede escribir, entonces, $(f,f')=1$.

$\Leftarrow$| Supongamos que u es una raiz múltiple de f en $\mathbb{K}$. Entonces $f(x)=(x-u)^r g(x)$ con $r>1$.

Luego $f'(x)=(x-u)^r g'(x)+(x-u)^{r-1}g(x)$

Siendo $r>1$ se tiene que $(x-u)\mid f'$ y, por tanto, si $d(x)=mcd(f,f')$, $(x-u)\mid d(x)$ en $\mathbb{K}[x]$ que prueba que $\partial^\circ(d)>0$ en contra de que $d=1$. Por tanto, f no tiene raíces múltiples en $\mathbb{K}$. c.s.q.d.

1 Estudio de los cuerpos finitos

1.1 Teorema: a) Si K es un cuerpo finito de característica p (*) existe un natural $n\geq 1$ tal que $o(K)=p^n$.
b) Para cada primo p y para cada $n\geq 1$ existe un único cuerpo, salvo isomorfismos, K de orden p^n. Concretamente, K es un cuerpo de descomposición del polinomio $X^{p^n}-X\in \mathbb{F}_p[x]$ donde $\mathbb{F}_p=\mathbb{Z}/(p)$. (**)

Demostr.: a) Sea Π el cuerpo primo de K. Entonces, siendo K de característica p, Π es isomorfo a $\mathbb{F}_p$.
Siendo K un cuerpo finito, el grado de la extensión $K|\Pi$ es finito; sea $[K:\Pi]=n$. Sea $\{u_1,\dots,u_n\}$ una base de $K|\Pi$. Entonces $K=\{\sum_{i=1}^{n}\lambda_i u_i \;/\; \lambda_i\in\Pi\}$.
Como $o(\Pi)=p$, el orden de K, que coincide con el número de combinaciones lineales de los elementos $u_1,\dots,u_n$ con escalares en Π, será:

$$o(K)=V'_{p,n}=p^n.$$

b) * **Existencia:** Consideremos el polinomio $X^{p^n}-X$ con coeficientes en el cuerpo $\mathbb{F}_p$. Sea K el cuerpo de descomposición de $X^{p^n}-X$ sobre $\mathbb{F}_p$.
Queremos probar que $o(K)=p^n$.
Consideremos el homomorfismo de Fröbenius (Tema 10, aptdo 3):

$$\sigma: K\longrightarrow K,\quad u\longmapsto u^p$$

Podemos considerar dicho homomorfismo sobre K tanto como $\mathbb{F}_p$

Entonces, dado $n \geq 1$, la aplicación

$$\sigma^n : u \in K \longmapsto \sigma^n(u) = u^{(p^n)} \in K$$

es un homomorfismo, (la demostración es analoga a la hecha para probar que σ es homomorfismo). (*)

Veamos que el conjunto $Raices_K(x^{p^n} - x)$ es subcuerpo de K.

Si α, β son raices en K de $x^{p^n} - x$ entonces $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$.

Luego, siendo σ^n homomorfismo, tenemos que

$(\alpha + \beta)^{(p^n)} = \alpha^{(p^n)} + \beta^{(p^n)} = \alpha + \beta$ que prueba que $\alpha + \beta \in Raices_K(x^{p^n} - x)$.

y tambien $(\alpha \cdot \beta)^{(p^n)} = \alpha^{(p^n)} \cdot \beta^{(p^n)} = \alpha \cdot \beta \Rightarrow \alpha \cdot \beta \in Raices_K(x^{p^n} - x)$.

Además, si $\alpha \in Raices_K(x^{p^n} - x)$, $(-\alpha)^{(p^n)} = -\alpha^{(p^n)} = -\alpha$, pues σ^n es homomorfismo y $(\alpha^{-1})^{(p^n)} = (\alpha^{(p^n)})^{-1} = \alpha^{-1}$.

Luego $Raices_K(x^{p^n} - x)$ es subcuerpo de K.

Veamos ahora que $\mathbb{F}_p \subset Raices_K(x^{p^n} - x)$:

dado $u \in \mathbb{F}_p$, $u^p = u$, pues $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ es un grupo cíclico multiplicativo de orden $p-1$ (corolario 6.11, Tema 9) y, por tanto, $u^{p-1} = 1 \Rightarrow u^p = u$.

Entonces $u^{(p^n)} = (u^p)^{(p^{n-1})} = u^{(p^{n-1})} = (u^p)^{(p^{n-2})} = u^{(p^{n-2})} = \dots = u^p = u$.

Es decir, $u \in Raices_K(x^{p^n} - x)$ y, por tanto, $\mathbb{F}_p \subset Raices_K(x^{p^n} - x)$.

Siendo $Raices_K(x^{p^n} - x)$ un cuerpo que contiene a $\mathbb{F}_p$ se verifica que $\mathbb{F}_p(Raices_K(x^{p^n} - x)) = Raices_K(x^{p^n} - x)$

Pero, por definición, $K = \mathbb{F}_p(Raices_K(x^{p^n} - x))$.

Entonces $K = Raices_K(x^{p^n} - x)$.

Veamos cuantas raices distintas tiene $x^{p^n} - x$ en K con lo cual conoceremos $o(K)$. Si probamos que todas las raices de $x^{p^n} - x$ son simples, quedará visto que $card(Raices_K(x^{p^n} - x)) = p^n$ y, por tanto, que $o(K) = p^n$, ya que $\partial^\circ(x^{p^n} - x) = p^n$.

$f(x) = x^{p^n} - x \Rightarrow f'(x) = p^n x^{p^n - 1} - 1$.

Siendo p^n el neutro de la suma en $\mathbb{F}_p$ ($p^n = \bar{0}$) se tiene que $f'(x) = -1$. Luego $mcd(f, f') = 1$, que prueba, en virtud de la proposicion anterior, que $x^{p^n} - x$ no tiene raices múltiples y, en consecuencia, $o(K) = p^n$.

Luego existe al menos un cuerpo K de orden p^n.

** UNICIDAD: Sea K un cuerpo de orden p^n. Sabemos que el grupo multiplicativo $K^* = K - \{0\}$ es cíclico de orden $p^n - 1$ entonces, como el orden de todo elemento de K^* es divisor de $p^n - 1$, se tiene que $\forall u \in K^*$, $u^{p^n - 1} = 1$ y, por tanto,

$\forall u \in K^*$, $u^{(p^n)} = u$. Esta igualdad es también cierta para $u = 0$.
Luego $\forall u \in K$, $u^{(p^n)} = u$.
Por tanto, $K \subset Raices_K (x^{p^n} - x)$. (I)
Por otra parte, $o(K) = p^n \geq card\,(Raices_K (x^{p^n} - x))$
y según (I), $p^n \leq card\,(Raices_K (x^{p^n} - x))$.
Luego $o(K) = card\,(Raices_K (x^{p^n} - x))$ y, en virtud de (I)

$$K = Raices_K (x^{p^n} - x). \quad (II)$$

Si Π es el subcuerpo primo de K, trivialmente tenemos que

$$K = \Pi\,(Raices_K (x^{p^n} - x))$$

pues $\Pi \subset K$, $Raices_K (x^{p^n} - x) = K$, K cuerpo $\Rightarrow \Pi\,(Raices_K (x^{p^n} - x)) \subset K$, por ser $\Pi(Raices_K (x^{p^n} - x))$ el menor cuerpo que contiene a Π y a $Raices_K (x^{p^n} - x)$ y además $K = Raices_K (x^{p^n} - x) \subset \Pi\,(Raices_K (x^{p^n} - x))$.
Además de (II) se deduce que $x^{p^n} - x$ se descompone totalmente en K.
Por tanto, K es un cuerpo de descomposición de $x^{p^n} - x$ sobre Π.
La unicidad del cuerpo de orden p^n es consecuencia inmediata de esto: Sean K_1 y K_2 dos cuerpos de orden p^n. Si Π_1 y Π_2 son los subcuerpos primos respectivos, existe un isomorfismo σ de Π_1 en Π_2 pues $\Pi_1 \simeq \mathbb{F}_p$ y $\Pi_2 \simeq \mathbb{F}_p$.
Según lo visto anteriormente K_1 es cuerpo de descomposición de $x^{p^n} - x$ sobre Π_1 y K_2 es cuerpo de descomposición de $x^{p^n} - x$ sobre Π_2. Del teorema 2.2 (Tema 11) deducimos que, siendo $\sigma(x^{p^n} - x) = x^{p^n} - x$, el isomorfismo $\sigma: \Pi_1 \to \Pi_2$ se extiende a un isomorfismo $\bar{\sigma}: K_1 \to K_2$. c.s.q.d.

1.2. Corolario: Sea K un cuerpo finito, $\bar{K}$ una clausura algebraica de K y u un elemento de $\bar{K}$. Entonces, el polinomio mínimo de u en K, $f = irr(u, K)$, no tiene raíces múltiples en $\bar{K}$.

Demostr.: Siendo $u \in \bar{K}$ y $\bar{K}$ clausura algebraica de K se deduce que u es algebraico sobre K y, por tanto, $K(u)|K$ es una extensión simple y algebraica. Entonces, según proposición 4.1 (Tema 10), $[K(u) : K]$ es finito. Supuesto que $[K(u) : K] = n$ y $o(K) = p$ se tiene que $o(K(u)) = p^n$ (se prueba de la misma forma que se hizo en teorema 1.1 (a)).
Luego $K(u)$ es un cuerpo de orden p^n contenido en $\bar{K}$.
Ahora bien, dos cuerpos del mismo orden contenidos en una clausura algebraica son, no solamente isomorfos, sino exactamente iguales, pues si K_1 y K_2 son cuerpos de orden p^n y $\bar{K}$ es una clausura

y $K_2 = \text{Raices}_{\bar{K}}(x^{p^n} - x)$ donde $x^{p^n} - x \in \mathbb{F}_p[x]$. Luego $K_1 = K_2$.
Entonces, siendo $K(u)$ y $\mathbb{F}_{p^n}$ cuerpos de orden p^n contenidos en $\bar{K}$, debe ser $K(u) = \mathbb{F}_{p^n}$.
Luego $K(u) = \text{Raices}_{\bar{K}}(x^{p^n} - x)$ y, en consecuencia, u es raiz de $x^{p^n} - x$, y, por definición del polinomio mínimo de u en K, $f_u(x) = \text{irr}(u, K)$, se tiene que $f_u(x) \mid (x^{p^n} - x)$.
Como el polinomio $x^{p^n} - x$ tiene todas sus raices simples, $f_u(x)$, como divisor de él, debe tener todas sus raices simples. csqd.

1.3. PROPOSICION: Si $\overline{\mathbb{F}_p}$ es una clausura algebraica de $\mathbb{F}_p$, entonces

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

donde $\mathbb{F}_{p^n}$ es "el" cuerpo de orden p^n contenido en $\overline{\mathbb{F}_p}$ (*)

Demostr.: Trivialmente, $\bigcup_{n\geq 1} \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$, tal como hemos considerado $\mathbb{F}_{p^n}$.
Además, dado $u \in \overline{\mathbb{F}_p}$, u es algebraico sobre $\mathbb{F}_p$.
Entonces, siendo $\mathbb{F}_p(u)$ una extensión simple y algebraica sobre el cuerpo finito $\mathbb{F}_p$, se deduce que $\mathbb{F}_p(u)$ es finito y contenido en $\overline{\mathbb{F}_p}$.
Siendo $\mathbb{F}_p(u)$ un cuerpo finito su orden es una potencia de p, y, por tanto, debe existir n tal que $o(\mathbb{F}_p(u)) = p^n$ y, en consecuencia, $\mathbb{F}_p(u) = \mathbb{F}_{p^n}$ que prueba que $u \in \bigcup_{n\geq 1} \mathbb{F}_{p^n}$. csqd.

1.4. PROPOSICION: Si $\mathbb{F}_{p^n}$ y $\mathbb{F}_{p^m}$ son cuerpos contenidos en la clausura algebraica $\overline{\mathbb{F}_p}$ entonces $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si, y solosi, n divide a m.

Demostr: $\Rightarrow$| Si $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, de la igualdad

$$[\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] \cdot [\mathbb{F}_{p^n} : \mathbb{F}_p]$$

y teniendo en cuenta que $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$ y $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ se deduce que $n \mid m$.

$\Leftarrow$| Supongamos que existe $d \in \mathbb{Z}$ tal que $m = n \cdot d$ (es decir, $n \mid m$).
Siendo $\mathbb{F}_{p^n} = \text{Raices}_{\overline{\mathbb{F}_p}}(x^{p^n} - x)$ se tiene que

dado $u \in \mathbb{F}_{p^n}$, $u^{(p^n)} - u = 0$, o tambien, $u^{p^n} = u$.
Entonces $u^{(p^m)} = u^{(p^{n\cdot d})} = (u^{p^n})^{(p^{(d-1)n})} = u^{(p^{(d-1)n})} = (u^{p^n})^{(p^{(d-2)n})} = u^{(p^{(d-2)n})} = \ldots =$
$= u^{(p^n)} = u$. Es decir, $u \in \text{Raices}_{\overline{\mathbb{F}_p}}(x^{p^m} - x) = \mathbb{F}_{p^m}$.
Por tanto, $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$. csqd.

TEMA 13º: EXTENSIONES SEPARABLES Y RADICALES

1. Polinomios separables y radicales

DEFINICIONES: (A) Sea $f(x)$ un polinomio con coeficientes en un cuerpo K. Se dice que f es separable si no tiene raices múltiples en una clausura algebraica de K.

(B) Se dice que $f(x) \in K[x]$ es radical o puramente inseparable cuando en $\overline{K}$, clausura algebraica de K, todas sus raices son iguales.

* En el caso de que el grado de f sea 1 las definiciones anteriores coinciden.

1.1. PROPOSICION: Un polinomio irreducible $f \in K[x]$ es separable si, y solo si, el polinomio derivado $f'(x)$ es no nulo.

Demostr.: $\Rightarrow$] Si f es separable (no tiene raices multiples), entonces (Tema 12) el maximo comun divisor de $f(x)$ y $f'(x)$ en $K[x]$ es 1. Debe ser entonces $f' \neq 0$.

$\Leftarrow$] Supongamos fue f no fuese separable, es decir, que admitiese una raiz múltiple. Entonces, $mcd(f, f') \neq 1$ (en $K[x]$).
Siendo f irreducible, no admite más divisores que él mismo y cualquier unidad. Como $(f, f') \mid f$ y (f, f') no es una unidad, debe ser $(f, f') = f$ (o un asociado suyo).
Además $(f, f') \mid f'$. Luego $f \mid f'$, de donde se deduciría fue, si $f' \neq 0$, $\partial^\circ(f') \geq \partial^\circ(f)$. Pero, por la definición de f', $\partial^\circ(f) > \partial^\circ(f')$.
Debería ser entonces $f' = 0$, en contra de la hipótesis.
Por tanto, f no puede tener raices múltiples. c.s.q.d.

1.2. COROLARIO: Todo polinomio irreducible sobre un cuerpo K de caracteristica cero es separable.

Demostr.: Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ e irreducible. Entonces $n \geq 1$ ya que f no puede ser constante (=unidad) por ser irreducible.
Entonces $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.
Si f no fuese separable sería $f' = 0$ y, por tanto, $i \cdot a_i = 0$, $1 \leq i \leq n$.
Siendo K de caracteristica cero, si $a_i \neq 0$ debe ser $i a_i \neq 0$, $1 \leq i \leq n$.
Entonces, si $f' = 0$, debe ser f constante (*), en contra de que f es irreducible. Luego $f' \neq 0$ y, por tanto, f es separable. c.s.q.d.

(*) Si $f' = 0$ ...

OBSERVACION: Como consecuencia del corolario 1.2 (Tema 12) podemos decir que todo polinomio irreducible sobre un cuerpo finito K es separable y, segun el corolario anterior, todo polinomio irreducible sobre un cuerpo K de caracteristica cero es separable. Cabe preguntarse si existen polinomios irreducibles con coeficientes en un determinado cuerpo que no sea separable. La respuesta es afirmativa; concretamente, existen polinomios irreducibles y no separables sobre el cuerpo $\mathbb{F}_p(x)$, que es infinito y de característica p.

1.3 COROLARIO: Sea f un polinomio irreducible sobre un cuerpo K de característica p. Siempre es posible escribir f(x) en la forma $f(x) = g(x^{p^e})$ donde $e \in \mathbb{N} \cup \{0\}$ y es el mayor de los naturales que verifica esto. Además, el polinomio $g(y) \in K[y]$ es irreducible y separable.

Demostr.: El conjunto $E = \{r \in \mathbb{N} \cup \{0\} / \exists g(y) \in K[y] \text{ tal que } f(x) = g(x^{p^r})\}$ es no vacío, puesto que $0 \in E$ ya que dado $f(x) \in K[x]$ existe $f(y) \in K[y]$ tal que $f(x) = f(x^{p^0}) = f(x)$. Además, dicho conjunto está acotado superiormente trivialmente ya que $\partial^\circ(f) \in \mathbb{N}$. Por tanto, existe $e = \max E$. Dado que $e \in E$, existe un polinomio $g(y) \in K[y]$ tal que $f(x) = g(x^{p^e})$ (*).

- Veamos que g es irreducible. Si g no fuese irreducible se tendría que $g(y) = h_1(y) \cdot h_2(y)$. Entonces será

$$f(x) = h_1(x^{p^e}) \cdot h_2(x^{p^e})$$

lo cual contradice que f es irreducible.

- Probemos que g es separable, es decir, que no tiene raices múltiples. Sea $g(y) = \sum_{i=0}^{n} b_i y^i$. Entonces $g'(y) = \sum_{i=1}^{n} i b_i y^{i-1}$.

Si fuese $g'(y) = 0$, entonces $i \cdot b_i = 0$, $i = 1, \dots, n$.

Siendo K de característica p debe ser $b_i = 0$ o $p \mid i$

Si $p \mid i$, tenemos $i = k_i \cdot p$ y por tanto $b_i y^i = b_i y^{k_i p}$

Si algún b_j fuese cero tambien podemos escribir $b_j y^j = b_j y^{k_j p}$ para un k_j cualquiera, pues este término no aparece. En definitiva podremos escribir, haciendo $k_0 = 0$,

$$g(y) = \sum_{i=0}^{n} b_i y^{k_i p}$$

y, haciendo, $h(y) = \sum_{i=0}^{n} b_i y^{k_i}$ tenemos fin $g(y) = h(y^p)$

(*) Ejemplo: Dado el polinomio $f(x) = x^{18} + 2x^9 + 1 \in \mathbb{F}_3[x]$, lo podemos escribir como

Por tanto, $f(x) = g(x^{p^e}) = h(x^{(p^e)^p}) = h(x^{p^{e+1}})$
en contra de que $e = \max T$.
Debe ser, entonces, $g' \neq 0$ y, por tanto, $g(y)$ será separable. c.s.g.d.

DEFINICION: Dado un polinomio $f(x)$, no constante, sobre un cuerpo K de característica p, definimos el exponente radical de f como el máximo del conjunto $\{r \in \mathbb{N} \cup \{0\} / \exists g(y) \in K[y] / f(x) = g(x^{p^r})\}$.

1.4. COROLARIO: Sea f un polinomio irreducible con coeficientes en un cuerpo K de característica p. Sea e el exponente radical de f y $f(x) = g(x^{p^e})$. Si $\partial^\circ(g) = m$ entonces f tiene m raices distintas, y todas ellas son de multiplicidad p^e.

Demostr: Siendo g separable podemos escribir
$$g(y) = c\prod_{j=1}^{m}(y - v_j) \quad \text{con } v_i \neq v_j \text{ si } i \neq j$$
donde $\{v_j\}_{j=1}^m$ son las raices de g en un clausura algebraica $\bar{K}$ de K.
Entonces
$$f(x) = g(x^{p^e}) = c\prod_{j=1}^{m}(x^{p^e} - v_j)$$
Segun proposicion 2.7 (Tema 11), $\bar{K}$ es clausura algebraica de $\bar{K}$ ($pues\ K \subset \bar{K} \subset \bar{K}$).
Entonces, dado $x^{p^e} - v_j \in \bar{K}[x]$, existe $u_j \in \bar{K}$ tal que $u_j^{p^e} - v_j = 0$.
Entonces, $f(x) = c\prod_{j=1}^{m}(x^{p^e} - u_j^{p^e})$.
Siendo K de característica p, $\sigma: a \in K \mapsto a^p \in K$ es homomorfismo (de Frobenius) y, trivialmente, $\sigma^e: a \in K \mapsto a^{p^e} \in K$ tambien es homomorfismo. Este homomorfismo se extiende trivialmente a un homomorfismo de $K[x]$ en $K[x]$ y podemos escribir $(x^{p^e} - u_j^{p^e}) = (x - u_j)^{p^e}$
Por tanto, $f(x) = c\prod_{j=1}^{m}(x - u_j)^{p^e}$.
Además $u_i \neq u_j$ si $i \neq j$, pues $u_i = u_j \Rightarrow u_i^{p^e} = u_j^{p^e} \Rightarrow v_i = v_j \Rightarrow i = j$.
Luego $f(x)$ tiene m raices distintas y de orden de multiplicidad p^e. c.s.g.d.

1.5 COROLARIO: Un polinomio irreducible sobre un cuerpo K de característica p es separable si, y solo si, su exponente radical es cero

Demostr: $\Rightarrow$| Si $f(x) \in K[x]$ es separable tiene todas sus raices distintas. Segun el corolario anterior debe ser $p^e = 1$ y, por tanto, $e = 0$.
$\Leftarrow$| Si $e = 0$, segun el corolario anterior f tiene

tintas de orden de multiplicidad $p^e=1$, es decir, no tiene raíces múltiples. cs q d.

1.6. COROLARIO: Todo polinomio irreducible y radical sobre un cuerpo de característica p es de la forma $c(x-u)^{p^e}$.

2. EXTENSIONES SEPARABLES Y RADICALES

DEFINICION: Sea K un cuerpo y $\overline{K}$ una clausura algebraica de K. Un elemento $u \in \overline{K}$ diremos que es separable (resp. radical) sobre K si el polinomio mínimo de u en K, $f_u(x) = Irr(u,K)$, es separable (resp. radical).

2.1 PROPOSICION: Si K es un cuerpo de característica p, un elemento $u \in \overline{K}$ es separable y radical si, y solo si, $u \in K$.

Demostr.: $\Rightarrow$| Si u es separable sobre K, su polinomio mínimo tiene de exponente radical $e=0$. Además, siendo u radical $f_u(x) = c(x-u)^{p^e} = c(x-u)$.

Como $f_u \in K[x]$, se tiene que $c \in K$ y $u \in K$.

$\Leftarrow$| Si $u \in K$, su polinomio mínimo es $Irr(u,K) = x-u$, que prueba que u es separable y radical. cs q d.

DEFINICION: Diremos que una extensión algebraica $|K$ de un cuerpo K es separable (resp. radical) si cada elemento u de $|K$ es separable (resp. radical) sobre K.

Necesariamente, para que $|K|K$ sea separable debe ser algebraica, para poder hablar del polinomio mínimo de cada elemento de $|K$ sobre K.

2.2 PROPOSICION: Sean K, $|K'$ y $|K$ cuerpos tales que $K \subset |K' \subset |K$. Si la extensión $|K|K$ es separable (resp. radical) entonces $|K|K'$ es separable (resp. radical).

Demostr.: Dado $u \in |K$ sea $f_u(x) = Irr(u,K)$ y $g_u(x) = Irr(u,|K')$. Ya que $K[x] \subset |K'[x]$, de la definición de $g_u(x)$ se tiene que $g_u(x) \mid f_u(x)$.

Siendo u separable sobre K, $f_u(x)$ no tiene raíces múltiples, y, en consecuencia, $g_u(x)$, como divisor de $f_u(x)$, tampoco las tendrá, lo que prueba que $g_u(x)$ es separable y, por tanto, u es separable sobre $|K'$, como queríamos ver.

Si $|K|K$ es radical, $f_u(x)$ solo tiene una raíz. Por tanto, $g_u(x)$ solo tendrá una raíz, que prueba que $g_u(x)$ es radical y, en consecuencia, u es radical sobre $|K'$. Por tanto, la extensión $|K|K'$ es radical. cs q d.

2.3. PROPOSICION: Sea $\bar{K}$ una clausura algebraica de un cuerpo K [característica p. de caracte-]

Sea $u \in \bar{K}$, $f_u(x) = Irr(u, K)$ y $f_u(x) = g(x^{p^e})$ donde e es el exponente radical de f_u. Entonces u^{p^e} es separable sobre K y u es radical sobre $K(u^{p^e})$.

Demostr.: Segun Corolario 1.3, el polinomio $g(y) \in K[y]$ es separable e irreducible, pues $f_u(x)$ lo es.

Siendo u raiz de $f_u(x)$, u^{p^e} es raiz de $g(y)$. Luego, por ser g irreducible debe ser $g(y) = Irr(u^{p^e}, K)$

Como g es separable, u^{p^e} es separable sobre K.

Veamos ahora fue u es radical sobre $K(u^{p^e})$.

u es raiz del polinomio $x^{p^e} - u^{p^e} \in K(u^{p^e})[x]$.

Siendo K de característica p, se tiene $x^{p^e} - u^{p^e} = (x-u)^{p^e}$.

Como u es raiz de $(x-u)^{p^e}$, se tiene que $Irr(u, K(u^{p^e})) \mid (x-u)^{p^e}$ (*) y, siendo $(x-u)^{p^e}$ radical (solo tiene la raiz u), $Irr(u, K(u^{p^e}))$ solo tiene la raiz u, que prueba fue u es radical sobre $K(u^{p^e})$. cqd

2.4. PROPOSICION: Sea K un cuerpo de característica p, y $\bar{K}$ una clausura algebraica.

a) $u \in \bar{K}$ es separable sobre K si, y solosi, $K(u) = K(u^p)$.

b) $u \in \bar{K}$ es radical sobre K si, y solosi, $\exists e \geq 0 / u^{p^e} \in K$.

Demostr. a) $\Rightarrow$| Evidentemente $K(u) \supset K(u^p) \supset K$. Segun proposición 2.2, si u es separable sobre K, es separable sobre $K(u^p)$.

Veamos fue u es radical sobre $K(u^p)$.

u es raiz de $x^p - u^p \in K(u^p)[x]$. Siendo K de característica p se tiene que $x^p - u^p = (x-u)^p$. Como $Irr(u, K(u^p)) \mid x^p - u^p$ y $x^p - u^p = (x-u)^p$ es radical se tiene fue $Irr(u, K(u^p))$ es radical y, por tanto, u es radical sobre $K(u^p)$. Como $\bar{K}$ es clausura algebraica de $K(u^p)$ (proposición 2.7, Tema 11) se verifica en virtud de la proposición 2.1 que $u \in K(u^p)$. Siendo $K(u)$ el menor cuerpo fue contiene a u y a K debe ser $K(u) \subset K(u^p)$ y, en definitiva, $K(u) = K(u^p)$.

$\Leftarrow$| Suponganos que u no es separable sobre K y probemos fue $K(u) \neq K(u^p)$.

Si u no es separable sobre K, $f_u(x) = Irr(u, K)$ tiene raices múltiples y, segun corolario 1.5, debe ser $e \geq 1$, donde e es el exponente radical de $f_u(x)$. Entonces podremos escribir $f_u(x) = g(x^{p^e})$. Siendo $f_u(x)$ irreducible, g debe serlo tambien. Ademas u

g, pues u es raiz de f_u. Por tanto $g = Irr(u^p, K)$.
Entonces $[K(u^p):K] = \partial^\circ(g)$
Como $[K(u):K] = \partial^\circ(f_u)$ y $\partial^\circ(f_u) > \partial^\circ(g)$, pues $\partial^\circ(f_u) = p^e \cdot \partial^\circ(g)$ y $p > 1$, se tiene que $[K(u^p):K] < [K(u):K]$ y, por tanto, $K(u^p) \neq K(u)$, contra la hipótesis.
Debe ser entonces u separable.

b) (u es radical sobre K) $\Leftrightarrow$ ($f_u(x)$ es radical) $\Leftrightarrow$
$\Leftrightarrow$ ($f_u(x) = (x-u)^{p^e}$) $\overset{C.1.6}{\Leftrightarrow}$ ($f_u(x) = x^{p^e} - u^{p^e}$)
Luego, si u es radical sobre K, $f_u(x) = x^{p^e} - u^{p^e} \in K[x]$ y por tanto, $u^{p^e} \in K$.
Reciprocamente, si existe $e \geq 0$ tal que $u^{p^e} \in K$, tomamos el menor de los naturales r tales que $u^{p^r} \in K$ y se verifica que $f_u(x) = x^{p^r} - u^{p^r} = (x-u)^{p^r}$, que prueba que u es radical sobre K. c.q.d.

2.5. TEOREMA: Sea K un cuerpo de caracteristica p, $\overline{K}$ una clausura algebraica de K y u un elemento de $\overline{K}$. Entonces, u es separable (resp. radical) si, y solo si, la extensión $K(u)|K$ es separable (resp. radical).

Demostr.: La condición suficiente es trivial, dado que $u \in K(u)$.
CONDICION NECESARIA: * Veamos primero que si u es radical, $K(u)|K$ es radical.
Probaremos que dado $v \in K(u)$ existe $e \geq 0$ tal que $v^{p^e} \in K$.
Si $v \in K(u)$ es de la forma $v = \sum_{i=0}^{n} a_i u^i$,
Siendo u radical, existe $e \geq 0$ tal que $u^{p^e} \in K$.
Entonces $v^{p^e} = (\sum_{i=0}^{n} a_i u^i)^{p^e} \overset{(1)}{=\!=} \sum_{i=0}^{n} a_i^{p^e} (u^i)^{p^e} = \sum_{i=0}^{n} a_i^{p^e} (u^{p^e})^i$
La igualdad (1) es cierta por ser K de característica p.
Puesto que $a_i \in K$ y $u^{p^e} \in K$ se tiene que $a_i^{p^e} \in K$ y $(u^{p^e})^i \in K$ y, en consecuencia, $v^{p^e} \in K$, como queriamos probar.
** Supongamos que u es separable sobre K. Entonces $K(u) = K(u^p)$.
Sea $[K(u):K] = [K(u^p):K] = n$.
Entonces $\{1, u, u^2, \ldots, u^{n-1}\}$ y $\{1, u^p, u^{2p}, \ldots, u^{(n-1)p}\}$ son bases del espacio vectorial $K(u)|K$. Veamos que si $\{r_0, r_1, \ldots, r_{n-1}\}$ es base de $K(u)|K$ entonces $\{r_0^p, r_1^p, \ldots, r_{n-1}^p\}$ tambien es base.
Si $\{r_j\}_{j=0}^{n-1}$ es base, dado $u^i \in K(u)$, $\exists \{a_{ji}\}_{j=0}^{n-1} \subset K$ / $u^i = \sum_{j=0}^{n-1} a_{ji} r_j$
Entonces $(u^i)^p = \sum_{j=0}^{n-1} a_{ji}^p r_j^p$. Por tanto, todo elemento de la base $\{1, u^p, u^{2p}, \ldots, u^{(n-1)p}\}$ se puede expresar como combinación lineal

Veamos entonces que $K(u)|K$ es separable.
Dado $v \in K(u)$ se tiene que $[K(v):K] = m \leq n$, pues $K(v) \subset K(u)$.
Entonces $\{1, v, \dots, v^{m-1}\}$ es base de $K(v)$. Haciendo $r_i = v^i$, $i = 0, \dots, m-1$ siempre podemos prolongar la base $\{r_0, r_1, \dots, r_{m-1}\}$ de $K(v)$ a una base $\{r_0, r_1, \dots, r_{m-1}, r_m, \dots, r_n\}$ de $K(u)$
Según lo probado antes, $\{r_0^p, r_1^p, \dots, r_{m-1}^p, \dots, r_n^p\}$ es base de $K(u)|K$. En consecuencia $\{r_0^p, r_1^p, \dots, r_{m-1}^p\}$ constituye un sistema libre. Es decir: $\{1, v^p, v^{2p}, \dots, v^{(m-1)p}\}$ es un sistema libre de $K(v^p)|K$. Entonces $[K(v^p):K] \geq m$.
Como $K(v^p) \subset K(v)$, se tiene que $[K(v^p):K] \leq [K(v):K] = m$.
En definitiva, $m \leq [K(v^p):K] \leq [K(v):K] \leq m \Rightarrow K(v^p) = K(v)$.
Por tanto, según PROPOSICION 2.4, v es separable sobre K. c.s.q.d.

3. K-automorfismos. Cuerpo fijo.

DEFINICION: Sea K un cuerpo y $\bar{K}$ una clausura algebraica de K. Sea $G = \mathrm{Aut}_K \bar{K}$ el conjunto de los automorfismos de $\bar{K}$ que dejan fijos los elementos de K, es decir, G es el conjunto de los K-automorfismos de $\bar{K}$. Definimos el cuerpo fijo de G como el conjunto

$$\bar{K}^G = \{u \in \bar{K} / \sigma(u) = u, \forall \sigma \in G\}$$

Evidentemente, $K \subset \bar{K}^G$, pues los elementos de G dejan fijos los elementos de K.
Es trivial que $\bar{K}^G$ es un subcuerpo de $\bar{K}$:
si $u, v \in \bar{K}^G$, $\sigma(u-v) = \sigma(u) - \sigma(v) = u - v$ y $\sigma(uv^{-1}) = \sigma(u) \cdot \sigma(v)^{-1} = uv^{-1}$, $\forall \sigma \in G$.

3.1. PROPOSICION: Dado $f(x) \in K[x]$, el grupo G opera sobre el conjunto $\mathrm{Raices}_{\bar{K}} f$, y esta operación es transitiva si f es irreducible.

Demostr.: Definimos la operación del siguiente modo

$$\begin{array}{ccc} G \times \mathrm{Raices}_{\bar{K}} f & \longrightarrow & \mathrm{Raices}_{\bar{K}} f \\ (\sigma, u) & \longmapsto & \sigma(u) \end{array}$$

Veamos que esta aplicación está bien definida (es decir, que $\mathrm{Raices}_{\bar{K}} f$ es G-estable, o también, que $\forall \sigma \in G$, $\forall u \in \mathrm{Raices}_{\bar{K}} f$, $\sigma(u) \in \mathrm{Raices}_{\bar{K}} f$).
f admite la descomposición $f(x) = c \prod_{i=1}^{n} (x - u_i)$ en $\bar{K}$, donde $\{u_i\}_{i=1}^{n} = \mathrm{Raices}_{\bar{K}} f$.
Dado $\sigma \in G$, $\sigma(f(x)) = c \prod_{i=1}^{n} (x - \sigma(u_i))$, pues $c \in K$ y $\sigma|_K = i_K$

K debe ser $\sigma(f(x)) = f(x)$. Por tanto, $\sigma(u_i) \in \text{Raices}_{\bar{K}} f$, $\forall u_i \in \text{Raices}_{\bar{K}} f$. Fácilmente se comprueba que G opera sobre $\text{Raices}_{\bar{K}} f$.

Veamos ahora que, si f es irreducible, la operación es transitiva, es decir que, si $u \in \text{Raices}_{\bar{K}} f$ entonces la órbita de u es el total, es decir $G \cdot u = \text{Raices}_{\bar{K}} f$.

Hemos de probar que dado $u' \in \text{Raices}_{\bar{K}} f$, $\exists \sigma \in G / \sigma(u) = u'$.

Según Teorema 3.1 (Tema 10), siendo f irreducible y $K(u)$ y $K(u')$ cuerpos de ruptura de f existe un isomorfismo $\sigma_1 : K(u) \to K(u')$ que deja fijos los elementos de K y lleva u en u'.

Si $\bar{K}$ es una clausura algebraica de K, dado que $K \subset K(u) \subset \bar{K}$ y $K \subset K(u') \subset \bar{K}$ tenemos que $\bar{K}$ es clausura algebraica de $K(u)$ y $K(u')$. Entonces, según corolario 25. (Tema 11), existe un isomorfismo $\sigma : \bar{K} \to \bar{K}$ y por tanto automorfismo, que prolonga a σ_1. Entonces σ es un K-automorfismo de $\bar{K}$ tal que $\sigma(u) = u'$ pues $\sigma|_{K(u)} = \sigma_1$. Luego existe $\sigma \in G / \sigma(u) = u'$. c.s.q.d.

3.2. COROLARIO: Sea K un cuerpo, $\bar{K}$ una clausura algebraica de K y $G = \text{Aut}_K \bar{K}$. Entonces las órbitas de los elementos de $\bar{K}$ son finitas, es decir, $\forall u \in \bar{K}$, $G \cdot u = \{\sigma(u) / \sigma \in G\}$ es finito.

Demostr.: Dado $u \in \bar{K}$ sea $f_u(x) = \text{Irr}(u, K)$. Por la proposición anterior G opera transitivamente en $\text{Raices}_{\bar{K}} f_u(x)$. Entonces $G \cdot u = \text{Raices}_{\bar{K}} f_u(x)$, que es un conjunto finito. c.s.q.d.

3.3. PROPOSICION: Si $|K|K$ es una extensión finita, el conjunto de los K-homomorfismos de $|K$ en $\bar{K}$, clausura algebraica de K, es finito, es decir $\text{Hom}_K(|K, \bar{K}) = \{\sigma : |K \to \bar{K} \text{ homomorfismo} / \sigma(a) = a, \forall a \in K\}$ es finito.

Demostr.: Sea $[|K : K] = n$ y $\{u_1, \dots, u_n\}$ una base de $|K|K$.
Consideremos para cada u_i su polinomio mínimo $f_{u_i}(x) = \text{Irr}(u_i, K)$. (*)
Veamos que $\forall \sigma \in \text{Hom}_K(|K, \bar{K})$, $\sigma(u_i) \in \text{Raices}_{\bar{K}} f_{u_i}(x)$.

En $|K[x]$ podemos poner $f_{u_i}(x) = (x - u_i) g(x)$.
Siendo σ K-homomorfismo y $f_{u_i}(x) \in K[x]$ se tiene que $\sigma(f_{u_i}(x)) = f_{u_i}(x)$.
Por otra parte $\sigma(f_{u_i}(x)) = (x - \sigma(u_i)) \cdot \sigma(g(x))$
Luego $f_{u_i}(x) = (x - \sigma(u_i)) g^{\sigma}(x)$ que prueba que $\sigma(u_i) \in \text{Raices}_{\bar{K}} f_{u_i}(x)$.
Entonces $\forall \{1, \dots, n\}$, $\forall \sigma \in \text{Hom}_K(|K, \bar{K})$, $\sigma(u_i) \in \bigcup_{j=1}^{n} \text{Raices}_{\bar{K}} f_{u_j}(x)$, que es un conjunto finito. Puesto que σ queda determinado al conocer las imágenes de los elementos de la base queda visto que solo existe un nº finito de K-homo

morfismos de K en $\bar{K}$. c.s.q.d.

3.4. PROPOSICION: Sea K un cuerpo, $\bar{K}$ una clausura algebraica y $\bar{K}^G$ el cuerpo fijo de $G = Aut_K \bar{K}$. Entonces

a) La extensión $\bar{K}|\bar{K}^G$ es separable. Además, $\forall u \in \bar{K}$, $G\cdot u = Raices_{\bar{K}} f_u(x)$, con $f_u(x) = Irr(u, \bar{K}^G)$

b) La extensión $\bar{K}^G|K$ es radical. Además $\bar{K}^G = \{u \in \bar{K} / u$ es radical sobre $K\}$.

Demostr.: a) Dado $u \in \bar{K}$, la órbita $G\cdot u$ es finita. Sea $G\cdot u = \{u_1, \dots, u_n\}$, con $u \in \{u_1, \dots, u_n\}$. Consideremos el polinomio $g(x) = \prod_{i=1}^{n} (x - u_i)$.

Sea $\sigma \in Aut_K \bar{K}$. Entonces $\sigma(g(x)) = \prod_{i=1}^{n} (x - \sigma(u_i))$.

Pero $\sigma(u_i) \in \{u_1, \dots, u_n\}$, ya que $u_i \in G\cdot u \Rightarrow G\cdot u_i = G\cdot u \Rightarrow$
$\Rightarrow \sigma(u_i) \in G\cdot u$, ya que $\sigma(u_i) \in G\cdot u_i$. Además, siendo σ biyectiva debe ser, necesariamente, $\sigma(\{u_1, \dots, u_n\}) = \{u_1, \dots, u_n\}$.

Reordenando convenientemente los factores en $g(x)$ podemos poner $\sigma(g(x)) = \prod_{i=1}^{n} (x - \sigma(u_i)) = \prod_{j=1}^{n} (x - u_j) = g(x)$, y esto cualquiera que sea $\sigma \in G$. En consecuencia, los coeficientes de g están en $\bar{K}^G$, es decir, $g(x) \in \bar{K}^G[x]$.

Además $g(x)$ es separable sobre $\bar{K}^G$, por construcción

Sea $f_u(x) = Irr(u, \bar{K}^G)$. Veamos que $f_u(x)$ es separable.

Puesto que u es raiz de $g(x)$, por definición de $f_u(x)$, se tiene que $f_u(x) \mid g(x)$. (De aquí ya se deduce que f_u es separable, pues g lo es).

Sea $G' = Aut_{\bar{K}^G} \bar{K}$. Como $f_u \in \bar{K}^G[x]$ y es irreducible, G' opera transitivamente sobre $Raices_{\bar{K}^G} f_u(x)$ y, por tanto

$$G'\cdot u = Raices_{\bar{K}^G} f_u(x) = Raices_{\bar{K}} f_u(x) \quad (*)$$

Se verifica que $G' \supset G$, pues si $\sigma \in G = Aut_K \bar{K}$, es un K-automorfismo de $\bar{K}$ que deja fijos los elementos de $\bar{K}^G$, por definición de $\bar{K}^G$. Luego σ es un $\bar{K}^G$-automorfismo de $\bar{K}$, es decir, $\sigma \in G'$.

Entonces, $G' \supset G \Rightarrow G'\cdot u \supset G\cdot u$.

Siendo $G\cdot u = Raices_{\bar{K}} g(x)$ y $G'\cdot u = Raices_{\bar{K}} f_u(x)$ se tiene que $f_u(x)$ tiene todas las raices de $g(x)$. Como, además, $f_u(x) \mid g$ debe ser $f_u(x) = g(x)$, es decir, $g(x) = Irr(u, \bar{K}^G)$. Como g es separable sobre $\bar{K}^G$ se tiene que u es separable sobre $\bar{K}^G$.

Por tanto, la extensión $\bar{K}|\bar{K}^G$ es separable.

Además $f_u(x) = g(x) \Rightarrow Raices_{\bar{K}} f_u(x) = Raices_{\bar{K}} g(x) = G\cdot u$.

b) Se trata de ver que la extensión $\bar{K}^G|K$ es radical. Probemos que $u \in \bar{K}^G$ si, y solo si, u es radical sobre K y, en particular, la extensión $\bar{K}^G|K$ será radical, y, aun más, $\bar{K}^G = \{u \in \bar{K} / u$ es radical sobre $K\}$.

Por definición, $(u \in \bar{K}^G) \Leftrightarrow (\sigma(u)=u, \forall \sigma \in G)$ (I)
Sea $f_u(x) = Irr(u,K)$. Entonces $G\cdot u = Raices_{\bar{K}} f_u(x)$. (II)
Además $(\sigma(u)=u, \forall \sigma \in G) \Leftrightarrow G\cdot u = \{u\}$ (III)
De las equivalencias (I) y (III) y de la igualdad (II) deducimos que $(u \in \bar{K}^G) \Leftrightarrow (Raices_{\bar{K}} f_u(x) = \{u\})$, es decir, $u \in \bar{K}^G$ si, y sólo si, f_u tiene una única raiz, que equivale a que u sea radical sobre K. c.s.q.d.

3.5. COROLARIO: Una extensión $|K|K$ es radical si, y solosi, $|K \subset \bar{K}^G$.

Demostr.: $\Rightarrow$| Si $|K|K$ es radical, todo elemento u de $|K$ es radical, es decir $u \in \bar{K}^G$, ya que $\bar{K}^G = \{u \in \bar{K} / u$ es radical sobre $K\}$. Luego $|K \subset \bar{K}^G$.
$\Leftarrow$| Si $|K \subset \bar{K}^G = \{u \in \bar{K} / u$ es radical sobre $K\}$ trivialmente $|K|K$ es radical. c.s.q.d.

4. Teorema del elemento primitivo.

* Sea u un elemento algebraico sobre un cuerpo K. Entonces la extensión $K(u)|K$ es finita, por ser simple y algebraica. Estudiemos el conjunto $Hom_K(K(u), \bar{K})$ de los K-homomorfismos de $K(u)$ en $\bar{K}$, clausura algebraica de K, donde K es un cuerpo de característica p.
Si $\sigma \in Hom_K(K(u), \bar{K})$, $\sigma(u) \in Raices_{\bar{K}} f_u(x)$, donde $f_u(x) = Irr(u,K)$, pues $f_u(u)=0 \Rightarrow \sigma(f_u(u))=0$. Siendo σ K-homomorfismo, $\sigma(f_u(u)) = f_u(\sigma(u))$
Luego $\sigma(u)$ es raiz de f_u en $\bar{K}$.
Por tanto, $o(Hom_K(K(u), \bar{K})) \leq card(Raices_{\bar{K}} f_u(x))$ (*)
Sea e el exponente radical de f_u. Entonces, existe $g(x) \in K[x]$ tal que $f_u(x) = g(x^{p^e})$. Se verifica, según corolario 1.4, que $card(Raices_{\bar{K}} f_u(x)) = \partial^\circ(g)$.
Entonces $o(Hom_K(K(u), \bar{K})) \leq \partial^\circ(g)$. Veamos que se da la igualdad.
Si $u' \in Raices_{\bar{K}} f_u(x)$ se tiene que $K(u) \simeq K(u')$, por ser cuerpos de ruptura del polinomio irreducible $f_u(x)$. Además existe un único K-isomorfismo $\varphi: K(u) \to K(u')$ tal que $\varphi(u)=u'$. Como $K(u') \subset \bar{K}$ se tiene que $\varphi \in Hom_K(K(u), \bar{K})$.
Puesto que $(\forall \sigma \in Hom_K(K(u), \bar{K}), \sigma(u) \in Raices_{\bar{K}} f_u(x)) \,y\, (\forall u' \in Raices_{\bar{K}} f_u(x), \exists \sigma \in Hom_K(K(u), \bar{K})$ tal que $\sigma(u)=u')$ se verifica que $o(Hom_K(K(u), \bar{K})) = card(Raices_{\bar{K}} f_u(x)) = \partial^\circ(g)$.
El número de K-homomorfismos de $K(u)$ en $\bar{K}$ esta ligado a que u sea separable o no.
Consideremos las extensiones $K \subset K(u^{p^e}) \subset K(u)$. Según PROPOSICION 2.3, u^{p^e} es separable sobre K y u es radical sobre $K(u^{p^e})$. Además siendo $f_u(x) = Irr(u,K)$ y $f_u(x) = g(x^{p^e})$ se tiene que $g = Irr(u^{p^e}, K)$.
Entonces $[K(u^{p^e}) : K] = \partial^\circ(g)$.

siendo u^{p^e} separable, $K(u^{p^e})|K$ es separable y, por tanto, $K(u^{p^e}) \subset K(u)_{sep}$ y, además, dado $v \in K(u)_{sep}$, v es separable sobre cualquier cuerpo intermedio entre K y $K(u)$; en particular, v es separable sobre $K(u^{p^e})$, como además v es radical sobre $K(u^{p^e})$, pues $K(u)|K(u^{p^e})$ es radical debe ser $v \in K(u^{p^e})$, según Proposición 2.1

Entonces $[K(u)_{sep} : K] = \partial^\circ(g)$. Por tanto, $o(\mathrm{Hom}_K(K(u), \bar{K})) = [K(u)_{sep} : K]$.

Hemos probado fue $K(u)_{sep}$ es un cuerpo ($K(u)_{sep} = K(u^{p^e})$) y que $o(\mathrm{Hom}_K(K(u^{p^e}), \bar{K}) = o(\mathrm{Hom}_K(K(u), \bar{K}))$ pues

$o(\mathrm{Hom}_K(K(u^{p^e}), \bar{K})) = \mathrm{card}(\mathrm{Raices}_{\bar{K}} \mathrm{Irr}(u^{p^e}, K)) = \mathrm{card}(\mathrm{Raices}_{\bar{K}} g) = \partial^\circ(g)$

y $o(\mathrm{Hom}_K(K(u), \bar{K})) = \partial^\circ(g)$.

Vamos a generalizar estos resultados obtenidos para extensiones simples finitas de cuerpos de característica p a extensiones finitas de cuerpos cualesquiera. Veamos antes una definición y un lema preliminares.

** Sea $|K|K$ una extensión finita de un cuerpo K. Entonces:

DEFINICION: Definimos $|K_{sep} = \{u \in |K / u$ es separable sobre $K\}$ y $|K_{rad} = \{u \in |K / u$ es radical sobre $K\}$.

4.1 LEMA: Sean $|K_1$ y $|K_2$ extensiones de un cuerpo infinito K y sea $\{\sigma_1, \dots, \sigma_n\}$ un conjunto finito de K-homomorfismos de $|K_1$ en $|K_2$. Entonces $\exists v \in |K_1$ tal que $\sigma_i(v) \neq \sigma_j(v)$ si $i \neq j$.

Además, si $|K_1|K$ es algebraica, podemos elegir v separable.

Demostr: Puesto fue $\sigma_i \neq \sigma_j$ si $i \neq j$ existe $u_{ij} \in |K_1$ talque $\sigma_i(u_{ij}) \neq \sigma_j(u_{ij})$ y esto para cada par (i,j), $i \neq j$. Sea $\{u_{ij}\}_{i \neq j} = \{u_0, u_1, \dots, u_m\}$.

Se verifica entonces que $[\forall r \in \{0,1,\dots,m\}, \sigma_i(u_r) = \sigma_j(u_r)] \Leftrightarrow (i = j)$.

Consideremos el polinomio $h(x) = \sum_{r=0}^{m} u_r x^r$.

Entonces $\sigma_i(h(x)) \neq \sigma_j(h(x))$ si $i \neq j$. Es decir $\sigma_i(h(x)) - \sigma_j(h(x)) \neq 0$ si $i \neq j$.

Consideremos el polinomio $\prod_{i \neq j} [\sigma_i(h(x)) - \sigma_j(h(x))]$ que es no nulo pues todos los factores son distintos de cero y $|K_2[x]$ es dominio de integridad.

Entonces existe $u \in K$, tal que

$$\prod_{i \neq j} [\sigma_i(h(u)) - \sigma_j(h(u))] \neq 0$$

ya que el número de raices de este polinomio es finito y K es infinito.

Sea $v = h(u) \in |K_1$ (ya que $\{u, u_0, \dots, u_m\} \subset |K_1$). Como $\sigma_i(v) \neq \sigma_j(v)$ si $i \neq j$ queda probado el lema.

- Supongamos ahora fue $|K_1|K$ es algebraica. Hemos probado fue $\exists v \in |K_1 / \sigma_1(v), \dots, \sigma_n(v)$ son distintos dos a dos.

Si caract$(K) = 0$, como consecuencia inmediata del COROLARIO 1.2, TEOREMA

Supongamos entonces que caract $(K_1) = p$. Como v es algebraico podemos hablar de $f_v(x) = Irr(v, K)$. Sea e el exponente radical de $f_v(x)$. Sabemos que v^{p^e} es separable sobre K. Veamos que $\sigma_i(v^{p^e}) \neq \sigma_j(v^{p^e})$ si $i \neq j$
Supongamos que $\sigma_i(v^{p^e}) = \sigma_j(v^{p^e})$. Entonces, siendo σ_i y σ_j homomorfismos se tiene que $[\sigma_i(v)]^{p^e} = [\sigma_j(v)]^{p^e}$
Consideremos el homomorfismo de Frobënius sobre $|K_2$ (pues $|K_2$ es de característica p)$^{(*)}$ $\xi : u \in |K_2 \longmapsto u^p \in |K_2$. Entonces $\xi^e = \xi \circ \overset{e}{\ldots} \circ \xi$ es homomorfismos de cuerpos y, por tanto, inyectivo. Entonces $[\sigma_i(v)]^{p^e} = [\sigma_j(v)]^{p^e} \Rightarrow \sigma_i(v) = \sigma_j(v) \Rightarrow i = j$. como queríamos probar.

4.2. TEOREMA: a) (Teorema del elemento primitivo). Sea $|K|K$ una extensión finita. Entonces $\exists u \in |K$ / $|K_{sep} = K(u)$. En particular $|K_{sep}$ será un cuerpo.
b) La extensión $|K|_{|K_{sep}}$ es radical.
c) La aplicación $\sigma \in Hom_K(|K, \bar{K}) \longmapsto \sigma_{|_{|K_{sep}}} \in Hom_K(|K_{sep}, \bar{K})$ es biyectiva. Ambos conjuntos tendrán entonces el mismo número de elementos.
En el apartado c) se supondrá que K es de característica p.

Demostr.: a) * Supongamos que K es finito. Entonces siendo $|K$ una extensión finita de K debe ser $|K$ finito. Como consecuencia del COROLARIO 12. (Tema 12) la extensión $|K|K$ es separable, es decir, $|K_{sep} = |K$. Veamos que la extensión es simple. Siendo $|K$ finito, $|K^*$ es, para un cierto n, el conjunto de raíces n-simas de la unidad unión con $\{0\}$. Sabemos que las raíces n-simas de la unidad constituyen un grupo cíclico a cuyos generadores se les llama raíces primitivas (ver problemas). Entonces $|K = K(\xi)$ donde ξ es una raíz primitiva.
** Supongamos entonces que K es infinito. Consideremos el conjunto $Hom_K(|K, \bar{K})$ que es finito, ya que la extensión $|K|K$ es finita (proposición 33).
Sea $Hom_K(|K, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$. En virtud del lema anterior sabemos que existe $u \in |K$ tal que $\sigma_i(u) \neq \sigma_j(u)$ si $i \neq j$; además podemos considerar u separable, pues siendo $|K|K$ una extensión finita, es algebraica.
Sea $\bar{K}$ una clausura algebraica de K que contenga a $|K$.
Uno de los K-homomorfismos $\{\sigma_i\}_{i=1}^n$ es la inclusión de $|K$ en $\bar{K}$. Supongamos que es σ_1, es decir, que $\forall x \in |K$, $\sigma_1(x) = x$.
Queremos probar que $|K_{sep} = K(u)$.
Puesto que u es separable, $K(u)_{|K}$ es separable y, por tanto, $K(u) \subset |K_{sep}$.
Veamos que para probar que $|K_{sep} \subset K(u)$ es suficiente que $|K|_{K(u)}$ sea una extensión radical, pues, supuesto que $|K|K(u)$ es radical sabemos que dado $v \in |K_{sep}$, v es separable sobre K y, por tanto, sobre $K(u)$

Queda probar entonces que la extensión $|K|K(u)$ es radical.
Según corolario 3.5, es suficiente que veamos que $|K \subset \overline{K(u)}^G$, donde $G = Aut_{K(u)} \overline{K(u)}$. Según PROPOSICION 2.7. (Tema 11) podemos tomar $\overline{K(u)} = \overline{K}$. Entonces $G = Aut_{K(u)} \overline{K}$. Veamos que $|K \subset \overline{K(u)}^G$, es decir, que dado $v \in |K$ y $\sigma \in Aut_{K(u)} \overline{K}$ entonces $\sigma(v) = v$.

Como σ deja fijo a $K(u)$ se tiene que $\sigma(u) = u = \sigma_1(u)$. Como la restricción $\sigma_{|K}$ de σ a $|K$ es un K-homomorfismo de $|K$ en $\overline{K}$ se tiene que $\sigma_{|K} \in \{\sigma_i\}_{i=1}^n$. Pero de los homomorfismos σ_i solo uno deja fijo a u que es σ_1, pues $\sigma_i(u) \neq \sigma_j(u)$ si $i \neq j$; entonces, $\sigma_{|K} = \sigma_1$. Es decir, $\forall v \in |K, \sigma(v) = v$, y esto cualquiera que sea $\sigma \in G$. Por tanto, $|K \subset \overline{K(u)}^G$. Luego, $|K_{sep} = K(u)$, como queríamos probar.

b) Hemos probado en el apartado a) que $|K|K(u)$ es radical y, siendo $|K_{sep} = K(u)$, se tiene que $|K|_{|K_{sep}}$ es radical.

c) - La aplicación es inyectiva: Sean $\sigma, \varepsilon \in Hom_K(|K, \overline{K})$ tales que $\sigma_{|K_{sep}} = \varepsilon_{|K_{sep}}$. Veamos que $\sigma = \varepsilon$, es decir, que $\forall v \in |K, \sigma(v) = \varepsilon(v)$.
Dado $v \in |K$, existe $e \geq 0$ tal que $v^{p^e} \in |K_{sep}$ ya que $|K|_{|K_{sep}}$ es radical (proposición 2.4). Entonces $\sigma(v^{p^e}) = \varepsilon(v^{p^e})$ y, por tanto, $\sigma(v)^{p^e} = \varepsilon(v)^{p^e}$

Consideremos el homomorfismo de Frobenius sobre $\overline{K}$ (*)

$$x \in \overline{K} \longmapsto x^p \in \overline{K}$$

Entonces $x \in \overline{K} \longmapsto x^{p^e} \in \overline{K}$ es también homomorfismo que, por tanto, será inyectivo. Luego $\sigma(v)^{p^e} = \varepsilon(v)^{p^e} \Rightarrow \sigma(v) = \varepsilon(v)$. Luego la aplicación $\sigma \longmapsto \sigma_{|K_{sep}}$ es inyectiva. Veamos que es sobre: Sea $\varphi: |K_{sep} \to \varphi(|K_{sep}) \subset \overline{K}$ que es un isomorfismo de $|K_{sep}$ en $\varphi(|K_{sep})$ (pues es isomorfismo de $|K_{sep}$ en $\overline{K}$). Siendo $\overline{K}$ clausura algebraica de $|K_{sep}$ y $\varphi(|K_{sep})$, podemos extender el K-isomorfismo φ a un K-isomorfismo $\sigma: \overline{K} \to \overline{K}$. Entonces $\sigma_{|K} \in Hom_K(|K, \overline{K})$ y extiende a φ. c.s.q.d.

4.3. COROLARIO: Toda extensión finita y separable es simple.

Demostr.: Si $|K|K$ es finita, $\exists u \in |K / |K_{sep} = K(u)$. Si $|K|K$ es separable entonces $|K_{sep} = |K$. Luego $|K = K(u)$. c.s.q.d.

4.4. COROLARIO: Sea $|K$ una extensión cualquiera de K. Entonces $|K_{sep}$ es un cuerpo

Demostr: Dados $u, v \in |K_{sep}$, consideremos la extensión $K(u,v)|K$ que es finita. Entonces, por el teorema anterior, $K(u,v)_{sep}$ es cuerpo. Luego $u+v, u \cdot v, -u, u^{-1} \in K(u,v)_{sep} \subset |K_{sep}$. Luego $|K_{sep}$ es cuerpo. c.s.q.d.

(*) Observar que podemos considerar el homomorfismo de Frobenius

4.5 COROLARIO: Sea $\mathbb{K}$ una extensión de un cuerpo K y S un subconjunto de $\mathbb{K}$. Entonces $K(S)$ es separable si, y solo si, todo elemento de S es separable.

Demostr.: $\Rightarrow$| Si $K(S)$ es separable sobre K, puesto que $S \subset K(S)$ se verifica que todo elemento de S es separable.

$\Leftarrow$| Si $S \subset \mathbb{K}_{sep}$, como $K \subset \mathbb{K}_{sep}$ debe ser $K(S) \subset \mathbb{K}_{sep}$ ya que $\mathbb{K}_{sep}$ es cuerpo y $K(S)$ es el menor subcuerpo que contiene a K y a S. Luego $K(S)|K$ es separable. c.s.q.d.

4.6 PROPOSICION: Sea $\mathbb{K}$ una extensión de un cuerpo K de característica p. Entonces $\mathbb{K}_{rad} = \{u \in \mathbb{K} / u \text{ es radical sobre } K\}$ es un cuerpo.

Demostr.: Dados $u, v \in \mathbb{K}_{rad}$, $\exists\, e_1, e_2 \geq 0 / u^{p^{e_1}} \in K$ y $v^{p^{e_2}} \in K$.
Sea $e = \max\{e_1, e_2\}$. Entonces $(u+v)^{p^e} \in K$, pues
$(u+v)^{p^e} = u^{p^e} + v^{p^e} = u^{p^{e_1} \cdot p^{e-e_1}} + v^{p^{e_2} \cdot p^{e-e_2}} = (u^{p^{e_1}})^{p^{e-e_1}} + (v^{p^{e_2}})^{p^{e-e_2}}$ que es un elemento de K ya que $u^{p^{e_1}}, v^{p^{e_2}} \in K$. Luego $u+v \in \mathbb{K}_{rad}$.
Análogamente se prueba que $u \cdot v \in \mathbb{K}_{rad}$, y que $u^{-1}, -u \in \mathbb{K}_{rad}$ cualesquiera que sean $u, v \in \mathbb{K}_{rad}$. c.s.q.d.

4.7 PROPOSICION: Sea $\mathbb{K}$ una extensión de un cuerpo K de característica p y S un subconjunto de $\mathbb{K}$. Entonces $K(S)|K$ es radical si, y solo si, todo elemento de S es radical sobre K.

Demostr.: Es consecuencia inmediata de la proposición anterior, (análoga a la del corolario 4.5).

4.8 PROPOSICION: Sea K un cuerpo de característica p y L y $\mathbb{K}$ cuerpos tales que $L \supset \mathbb{K} \supset K$. Entonces la extensión $L|K$ es separable si, y solo si, son separables las extensiones $L|\mathbb{K}$ y $\mathbb{K}|K$.

Demostr.: $\Rightarrow$| Sabemos que si $L|K$ es separable, también lo es $L|\mathbb{K}$.
Que $\mathbb{K}|K$ es separable es trivial pues $\mathbb{K} \subset L$ y $L|K$ es separable.

$\Leftarrow$| Supongamos que $L|\mathbb{K}$ y $\mathbb{K}|K$ son separables y probemos que $L|K$ es separable, es decir, que, si $L_{sep} = \{u \in L / u \text{ separable sobre } K\}$ entonces $L_{sep} = L$.
L_{sep} es un cuerpo que contiene a $\mathbb{K}$, pues todos los elementos de $\mathbb{K}$ son separables sobre K. Tenemos entonces $L \supset L_{sep} \supset \mathbb{K}$.
Supongamos probado que $L|L_{sep}$ es radical.

ble sobre $\mathbb{K}$, pues $L|\mathbb{K}$ es separable, y, por tanto, u es separable sobre cualquier cuerpo intermedio entre L y $\mathbb{K}$; en particular, u es separable sobre L_{sep}. En definitiva queda:

$[(\forall u \in L),\ (u \text{ radical sobre } L_{sep}) \text{ y } (u \text{ separable sobre } L_{sep})] \Rightarrow [u \in L_{sep}]$

y por tanto $L = L_{sep}$, como pretendíamos probar.

Queda, para terminar la demostración, ver que $L|L_{sep}$ es radical:

Dado $u \in L$, existe $e \geq 0$ tal que u^{p^e} es separable sobre K, es decir $u^{p^e} \in L_{sep}$ y, por tanto, u es radical sobre L_{sep}. c.s.q.d.

4.9 PROPOSICION: La extensión $L|K$ es radical si, y solo si, son radicales las extensiones $L|\mathbb{K}$ y $\mathbb{K}|K$, donde K es de característica p y $L \supset \mathbb{K} \supset K$.

Demostr.: $\Rightarrow$] Si $L|K$ es radical, sabemos que $L|\mathbb{K}$ es radical.
Además, $\mathbb{K}|K$ es radical, pues $\mathbb{K} \subset L$ y $L|K$ es radical.
$\Leftarrow$] Dado $u \in L$, $\exists e_1 \geq 0 / u^{p^{e_1}} \in \mathbb{K}$, pues $L|\mathbb{K}$ es radical.
Dado $u^{p^{e_1}} \in \mathbb{K}$, $\exists e_2 \geq 0 / (u^{p^{e_1}})^{p^{e_2}} \in K$, pues $\mathbb{K}|K$ es radical.
Luego $\exists e = e_1 + e_2 \geq 0 / u^{p^e} \in K$, que prueba que $L|K$ es radical. c.s.q.d.

5. Grado de separabilidad y grado radical de una extensión.

DEFINICION: Sea $\mathbb{K}|K$ una extensión algebraica. Definimos el grado de separabilidad de la extensión como el grado de la extensión $[\mathbb{K}_{sep} : K]$.
Escribiremos $[\mathbb{K} : K]_S = [\mathbb{K}_{sep} : K]$.
Definimos el grado radical de la extensión como

$$[\mathbb{K} : K]_r = [\mathbb{K} : \mathbb{K}_{sep}]$$

Es trivial que $[\mathbb{K} : K] = [\mathbb{K} : K]_S \cdot [\mathbb{K} : K]_r$.

5.1. PROPOSICION: Sea $\mathbb{K}|K$ una extensión finita. Entonces

$$o(\mathrm{Hom}_K(\mathbb{K}, \bar{K})) = [\mathbb{K} : K]_S$$

es decir, el grado de separabilidad de la extensión coincide con el número de K-homomorfismos de $\mathbb{K}$ en un clausura algebraica $\bar{K}$ de K.

Demostr.: Sabemos que $o(\mathrm{Hom}_K(\mathbb{K}, \bar{K})) = o(\mathrm{Hom}_K(\mathbb{K}_{sep}, \bar{K}))$
Siendo $\mathbb{K}|K$ una extensión finita, en virtud del teorema del elemento primitivo $\exists u \in \mathbb{K} / \mathbb{K}_{sep} = K(u)$
Sabemos que, para extensiones simples, $o(\mathrm{Hom}_K(K(u), \bar{K})) = \mathrm{card}(\mathrm{Raices}_{\bar{K}} f_u(x))$
donde $f_u(x) = \mathrm{Irr}(u, K)$.
Puesto que u es separable ($u \in \mathbb{K}_{sep}$), $f_u(x)$ es separable. Por tanto, todos

$\text{card}(\text{Raices}_{\overline{K}} f_u(x)) = \partial^\circ(f_u)$.
Siendo f_u irreducible, $\partial^\circ(f_u) = [K(u):K] = [K_{sep}:K] = [K:K]_s$.
En definitiva, $o(\text{Hom}_K(K,\overline{K})) = [K:K]_s$. c.s.q.d.

5.2. PROPOSICION: Sea K una extensión finita de un cuerpo K de característica p. Entonces $\exists e \geq 0 / [K:K]_r = p^e$. Además, $\forall u \in K, u^{p^e} \in K_{sep}$ (*)

Demostr.: Dado que la extensión $K|K_{sep}$ es radical y finita, es suficiente que probemos el resultado para una extensión $K|K$ radical y finita, pues entonces se tendría, en nuestro caso, que $[K_s:K]_r = [K:K_{sep}] = p^e$.
Supongamos que $K|K$ es una extensión radical y finita
Si $K - K = \emptyset$, es decir, si $K = K$ no hay nada que probar (basta tomar $e=0$).
Si $K - K \neq \emptyset$, $\exists u_1 \in K - K$. Siendo u_1 radical sobre K, existe $e_1 \geq 0$ tal que $u_1^{p^{e_1}} \in K$.
Siempre podemos considerar que e_1 es el menor natural que verifica esto.
Haciendo $v_1 = u_1^{p^{e_1-1}}$ se tiene, entonces, que $v_1 \in K - K$ y $v_1^p = u_1^{p^{e_1}} \in K$.
Entonces $[K(v_1):K] = p$, pues siendo v_1 radical sobre K su polinomio mínimo sobre K es de la forma $(x - v_1)^{p^r}$ y, ya que $v_1^p \in K$, el polinomio mínimo es $(x-v_1)^p$ y, por tanto, $\partial^\circ(\text{Irr}(v_1,K)) = p$.
Si $K = K(v_1)$ el teorema queda probado.
Si $K - K(v_1) \neq \emptyset$, sea $u_2 \in K - K(v_1)$. Entonces u_2 es radical sobre K y por tanto, sobre $K(v_1)$. Luego $\exists e_2 \geq 0 / u_2^{p^{e_2}} \in K(v_1)$ y consideramos e_2 el menor natural que verifica lo anterior.
Entonces $v_2 = u_2^{p^{e_2-1}} \in K - K(v_1)$ y $v_2^p \in K(v_1)$. Luego $[K(v_1)(v_2):K(v_1)] = p$
Puesto que la extensión $K|K$ es finita, en un número finito e de pasos obtenemos $K = K(v_1, v_2, \dots, v_e)$, siendo $[K(v_1,\dots,v_{k-1})(v_k):K(v_1,\dots,v_{k-1})] = p$, $k \in \{2,\dots,e\}$. Luego $[K:K] = [K(v_1):K] \cdot \prod_{i=2}^{e} [K(v_1,\dots,v_{i-1})(v_i):K(v_1,\dots,v_{i-1})] = p^e$.
Entonces, según se indicó al principio de la demostración, $\exists e \geq 0 / [K:K]_r = p^e$.
Veamos que $\forall u \in K, u^{p^e} \in K_{sep}$
Dado $u \in K$, $u^p \in K_{sep}(v_1,\dots,v_{e-1})$ ya que si $u \in K = K_{sep}(v_1,\dots,v_{e-1})(v_e)$, $u = \sum_{i=1}^{n} a_i v_e^i \Rightarrow u^p = \sum_{i=1}^{n} a_i^p (v_e^p)^i \in K_{sep}(v_1,\dots,v_{e-1})$
De la misma manera $u^{p^2} \in K_{sep}(v_1,\dots,v_{e-2})$. Así sucesivamente, $u^{p^e} \in K_{sep}$ c.s.q.d.

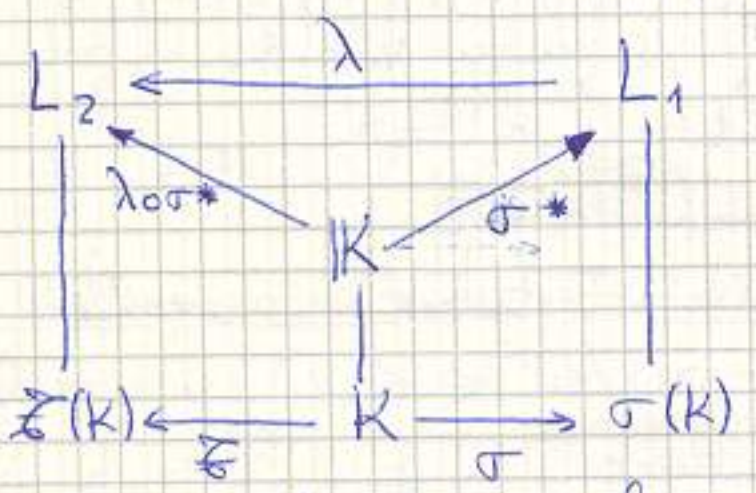
* Sabemos que si $K|K$ es una extensión finita el número de K-homomorfismos de K en una clausura algebraica $\overline{K}$ de K es finito, es decir, el número de homomorfismos de K en $\overline{K}$ que prolongan la identidad en K (es decir, que dejan fijos los elementos de K) es finito. Podemos preguntarnos si, dada una inmersión $\sigma: K \to \overline{K}$ (un homomorfismo de K en K que será, necesariamente, inyectivo), el número de prolongaciones de σ a K coincide

con $o(\mathrm{Hom}_K(\mathbb{K},\bar{K}))$. La respuesta es afirmativa como prueba el siguiente:

5.3. LEMA: Sean L_1 y L_2 clausuras algebraicas de un cuerpo K y $\sigma: K \to L_1$ y $\xi: K \to L_2$ homomorfismos. Sea $\mathbb{K}|K$ una extensión algebraica. Llamamos S_σ (resp. S_ξ) al conjunto de prolongaciones de σ a $\mathbb{K}$ (resp. de ξ a $\mathbb{K}$). Entonces $\mathrm{card}(S_\sigma) = \mathrm{card}(S_\xi)$.

Demostr.: Siendo σ y ξ inyectivas, las aplicaciones $\sigma: K \to \sigma(K) \subset L_1$ y $\xi: K \to \xi(K)$ son biyectivas. Entonces $\xi \circ \sigma^{-1}: \sigma(K) \longrightarrow \xi(K) \subset L_2$ es un isomorfismo. Considerando L_1 y L_2 como clausuras algebraicas de $\sigma(K)$ y $\xi(K)$, respectivamente, según corolario 2.5, Tema 11, $\xi \circ \sigma^{-1}$ se puede prolongar a un isomorfismo λ de L_1 en L_2. Vamos a establecer una biyección φ de S_σ en S_ξ, de manera que a cada prolongación σ^* de σ a $\mathbb{K}$ asocia la aplicación $\lambda \circ \sigma^*$, es decir

$$\varphi: S_\sigma \longrightarrow S_\xi$$
$$\sigma^* \longmapsto \varphi(\sigma^*) = \lambda \circ \sigma^*$$



Veamos que φ está bien definida, es decir, que $\lambda \circ \sigma^* \in S_\xi$. $\lambda \circ \sigma^*$ es un homomorfismo de $\mathbb{K}$ en L_2. Veamos que $\lambda \circ \sigma^*|_K = \xi$.

Como $\sigma^*|_K = \sigma$, pues $\sigma^* \in S_\sigma$, se tiene que

$$(\lambda \circ \sigma^*)|_K = \lambda \circ (\sigma^*|_K) = \lambda \circ \sigma = (\lambda|_{\sigma(K)}) \circ \sigma$$

Siendo $\lambda|_{\sigma(K)} = \xi \circ \sigma^{-1}$, por definición de λ, se tiene que

$$(\lambda \circ \sigma^*)|_K = (\xi \circ \sigma^{-1}) \circ \sigma = \xi \circ (\sigma^{-1} \circ \sigma) = \xi.$$

Luego φ está bien definida.

- φ es inyectiva: Si dados $\sigma_1, \sigma_2 \in S_\sigma$, $\lambda \circ \sigma_1 = \lambda \circ \sigma_2 \Rightarrow$
$\Rightarrow \lambda^{-1} \circ (\lambda \circ \sigma_1) = \lambda^{-1} \circ (\lambda \circ \sigma_2) \Rightarrow \sigma_1 = \sigma_2$.

Entonces $\mathrm{card}(S_\sigma) \leq \mathrm{card}(S_\xi)$.

Puesto que los "papeles" de σ y ξ son totalmente simétricos, se tiene del mismo modo que $\mathrm{card}(S_\xi) \leq \mathrm{card}(S_\sigma)$.

En definitiva, $\mathrm{card}(S_\sigma) = \mathrm{card}(S_\xi)$. c.s.q.d.

5.4. COROLARIO: Si $\mathbb{K}|K$ es una extensión finita, $[\mathbb{K}:K]_s$ es el número de prolongaciones de cualquier inmersión $\sigma: K \to \bar{K}$ a $\mathbb{K}$.

Demostr: El número de homomorfismos de $\mathbb{K}$ en $\bar{K}$ que prolongan

a un homomorfismo σ (inmersión) de K en $\overline{K}$ no depende de σ según el lema anterior. Siendo $[\mathbb{K}:K]_s = o(\mathrm{Hom}_K(\mathbb{K},\overline{K}))$ y $\mathrm{Hom}_K(\mathbb{K},\overline{K})$ el conjunto de prolongaciones a $\mathbb{K}$ de la inyección $i: K \to \overline{K}$, queda probado el enunciado ■

5.5. TEOREMA: Sea $L|K$ una extensión finita y $\mathbb{K}$ un cuerpo intermedio entre L y K, es decir, tal que $L \supset \mathbb{K} \supset K$. Entonces

$$[L:K]_s = [L:\mathbb{K}]_s \cdot [\mathbb{K}:K]_s \quad \text{y}$$
$$[L:K]_r = [L:\mathbb{K}]_r \cdot [\mathbb{K}:K]_r.$$

Demostr.: Sea $\overline{K}$ una clausura algebraica de K que contiene a L y $\mathbb{K}$. Dada una inmersión $\sigma: K \to \overline{K}$ denotamos por S_σ^L el conjunto de las prolongaciones de σ a L y por $S_\sigma^{\mathbb{K}}$ el conjunto de las extensiones de σ a $\mathbb{K}$. Entonces

$$\mathrm{card}(S_\sigma^L) = [L:K]_s \quad \text{y} \quad \mathrm{card}(S_\sigma^{\mathbb{K}}) = [\mathbb{K}:K]_s.$$

Sea, entonces, $S_\sigma^{\mathbb{K}} = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$

Si $S_{\sigma_i}^L$ es el conjunto de prolongaciones de $\sigma_i: \mathbb{K} \to \overline{K}$ a L, se verifica que $[L:\mathbb{K}]_s = \mathrm{card}(S_{\sigma_i}^L)$, y esto cualquiera que sea $i \in \{1,\dots,n\}$

Veamos que $S_\sigma^L = \bigcup_{i=1}^n S_{\sigma_i}^L$.

Dado $\overline{\sigma} \in S_\sigma^L$, $\overline{\sigma}$ es un homomorfismo de L en $\overline{K}$ que prolonga a σ. Entonces, la restricción $\overline{\sigma}_{|\mathbb{K}}: \mathbb{K} \to \overline{K}$ es un homomorfismo que prolonga a σ, es decir, $\overline{\sigma}_{|\mathbb{K}} \in \{\sigma_i\}_{i=1}^n = S_\sigma^{\mathbb{K}}$; luego $\overline{\sigma}$ es una extensión de un cierto σ_i y, por tanto, $\overline{\sigma} \in \bigcup_{i=1}^n S_{\sigma_i}^L$.

Para un i arbitrario, sea $\overline{\sigma} \in S_{\sigma_i}^L$. Entonces

$$\begin{array}{ccc} L & \xrightarrow{\overline{\sigma}} & \overline{K} \\ | & & | \\ \mathbb{K} & \xrightarrow{\sigma_i} & \overline{K} \\ | & & | \\ K & \xrightarrow{\sigma} & \overline{K} \end{array}$$

$\overline{\sigma}_{|\mathbb{K}} = \sigma_i$ y, puesto que $\sigma_i|_K = \sigma$, se tiene que $\overline{\sigma}|_K = \sigma$, es decir, $\overline{\sigma} \in S_\sigma^L$.

Luego $S_\sigma^L = \bigcup_{i=1}^n S_{\sigma_i}^L$.

Además, $S_{\sigma_i}^L \cap S_{\sigma_j}^L = \emptyset$ si $i \neq j$, pues si $\overline{\sigma} \in S_{\sigma_i}^L$, $\overline{\sigma}$ es un prolongación de σ_i, que es distinta de σ_j y, por tanto, $\overline{\sigma} \notin S_{\sigma_j}^L$.

Luego $\mathrm{card}(S_\sigma^L) = n \cdot \mathrm{card}(S_{\sigma_i}^L) = \mathrm{card}(S_\sigma^{\mathbb{K}}) \cdot \mathrm{card}(S_{\sigma_i}^L)$

En definitiva, $[L:K]_s = [\mathbb{K}:K]_s \cdot [L:\mathbb{K}]_s$.

- Siendo $[L:K] = [L:K]_r \cdot [L:K]_s$ se tiene que:

$$[L:K]_r = \frac{[L:K]}{[L:K]_s} = \frac{[L:\mathbb{K}]\cdot[\mathbb{K}:K]}{[L:\mathbb{K}]_s \cdot [\mathbb{K}:K]_s} = [L:\mathbb{K}]_r \cdot [\mathbb{K}:K]_r. \quad \text{c.q.d.}$$

2ª PARTE: TEORIA DE GALOIS (CONTINUACION)

TEMA 14: EXTENSIONES NORMALES. EXTENSIONES DE GALOIS.

1. EXTENSIONES NORMALES

DEFINICION: Diremos que una extensión algebraica $|K|k$ es normal si $|K$ es estable por $G = Aut_k \bar{K}$, es decir, si

$\forall u \in |K, \forall \sigma \in G, \sigma(u) \in |K$, o tambien que

$\forall \sigma \in G, \sigma(|K) \subset |K$.

1.1. PROPOSICION: Si la extensión $|K|k$ es normal, entonces cualquiera que sea $\sigma \in Aut_k \bar{K}$ se verifica que $\sigma(|K) = |K$.

Demostr.: Puesto que $\sigma(|K) \subset |K$, la aplicación $\sigma_{|K} : |K \longrightarrow |K$, $u \longmapsto \sigma(u)$ está bien definida. Si probamos que es sobre quedará visto que $\sigma(|K) = |K$.

Puesto que $\sigma^{-1} \in Aut_k \bar{K}$, $\sigma^{-1}(|K) \subset |K$.

Por tanto, dado $v \in |K$, $u = \sigma^{-1}(v) \in |K$.

Luego $\forall v \in |K, \exists u = \sigma^{-1}(v) \in |K$ / $v = \sigma(u)$. c.s.g.d.

1.2. PROPOSICION: Una extensión algebraica $|K|k$ es normal si, y solosi, $|K$ es el cuerpo de descomposición de una familia de polinomios irreducibles en $K[x]$.

Demostr.: $\Rightarrow$ Consideremos la familia de polinomios irreducibles en $K[x]$ siguiente: $P = \{f_u(x) / u \in |K\}$ donde $f_u(x) = Irr(u, K)$.

Si $G = Aut_k \bar{K}$, sabemos que $G \cdot u = Raices_{\bar{K}} f_u(x)$ (PROPOSICION 3.1, Tema 13).

Siendo $|K|k$ normal, $\forall \sigma \in G, \sigma(|K) \subset |K$, luego

$\forall u \in |K$, $Raices_{\bar{K}} f_u(x) \subset |K$.

Por tanto todos los polinomios de P se descomponen en $|K$.

Falta ver que $|K = K(Raices_{\bar{K}} P)$.

Dado $u \in |K$; $u \in Raices_{\bar{K}} f_u(x) \subset Raices_{\bar{K}} P \Rightarrow |K \subset Raices_{\bar{K}} P \subset K(Raices_{\bar{K}} P)$

Además puesto que $\forall u \in |K$, $Raices_{\bar{K}} f_u(x) \subset |K$ se tiene que $Raices_K P \subset |K$ y, dado que $K \subset |K$, se tiene que $|K \supset K(Raices_K P)$.

$\Leftarrow$ Sea P una familia de polinomios irreducibles en $K[x]$ y supongamos que $|K = K(Raices_{\bar{K}} P)$. Veamos que $|K|k$ es normal.

Sea $G = Aut_k \bar{K}$. Sabemos que G opera transitivamente sobre $Raices_{\bar{K}} f(x)$ si f es irreducible, es decir, las raices de

elementos de 6 K-automorfismos se deduce que los elementos de K son estables por 6. En consecuencia $K(\text{Raices}_K P)$ es estable por 6, pues los polinomios de P son irreducibles. Siendo $\mathbb{K} = K(\text{Raices}_K P)$, $\mathbb{K}$ es estable por 6, es decir, $\forall \sigma \in 6$, $\sigma(\mathbb{K}) \subset \mathbb{K}$. c.q.d.

1.3. PROPOSICION: Si la extensión $\mathbb{K}|K$ es normal y $6 = \text{Aut}_K \mathbb{K}$ entonces el cuerpo fijo de 6 y el conjunto de elementos radicales de $\mathbb{K}$ coinciden, es decir, $\mathbb{K}^6 = \mathbb{K}_{rad}$. Además la extensión $\mathbb{K}|\mathbb{K}_{rad}$ es separable.

Demostr.: Sea $\overline{K}$ una clausura algebraica de K que contenga a $\mathbb{K}$ y $6' = \text{Aut}_K \overline{K}$. Siendo $\mathbb{K}|K$ normal se tiene que $\mathbb{K}^{6'} = \mathbb{K}^6$. (*) Trivialmente, $\mathbb{K}^{6'} = \overline{K}^{6'} \cap \mathbb{K}$. Según PROPOSICION 3.4. (Tema 13), $\overline{K}^{6'} = \overline{K}_{rad}$. Luego $\mathbb{K}^{6'} = \overline{K}_{rad} \cap \mathbb{K} = \mathbb{K}_{rad}$. En definitiva $\mathbb{K}^6 = \mathbb{K}_{rad}$.

Veamos que la extensión $\mathbb{K}|\mathbb{K}_{rad}$ es separable. Dado $u \in \mathbb{K}$, sabemos que $6' \cdot u$ es finito. Sea $6' \cdot u = \{u_1, \dots, u_n\}$. Pero, siendo $\mathbb{K}|K$ normal, $6' \cdot u = 6 \cdot u$, ya que dado $\sigma' \in 6'$ su restricción a $\mathbb{K}$ pertenece a 6 y dado $\sigma \in 6$, existe un $\sigma' \in 6'$ que prolonga a σ y, por tanto, como $u \in \mathbb{K}$, $6' \cdot u = 6 \cdot u \subset \mathbb{K}$, pues $\mathbb{K}|K$ es normal.

Consideremos el polinomio $g(x) = \prod_{i=1}^{n} (x - u_i)$

Dado $\sigma \in 6$, $\sigma(g(x)) = \prod_{i=1}^{n} (x - \sigma(u_i)) \overset{(1)}{=} \prod_{i=1}^{n} (x - u_i) = g(x)$

(1) es cierta pues dado $\sigma \in 6$ y $u_i \in 6 \cdot u$, $\sigma(u_i) \in 6 \cdot u$ y, siendo σ automorfismo, se tiene $\sigma(\{u_1, \dots, u_n\}) = \{u_1, \dots, u_n\}$. Por tanto, σ deja fijos los coeficientes de $g(x)$, es decir, los coeficientes de $g(x)$ están en $\mathbb{K}^6$, o también, $g(x) \in \mathbb{K}^6[x]$. Por construcción g tiene todas sus raices simples. Además u es raiz de $g(x)$ pues $u \in 6 \cdot u = \text{Raices}_{\mathbb{K}} g(x)$. Luego $f_u(x) \mid g(x)$, si $f_u(x) = \text{Irr}(u, \mathbb{K}^6)$. Por tanto, $f_u(x)$ es separable sobre $\mathbb{K}^6$. En consecuencia, la extensión $\mathbb{K}|\mathbb{K}^6$ es separable. Siendo $\mathbb{K}^6 = \mathbb{K}_{rad}$, queda terminada la demostración. ■

OBSERVACION: En la proposición anterior se puede probar que $f_u(x) = g(x)$ de manera análoga a PROPOSICION 3.4. (Tema 13).

(*) $\mathbb{K}^6 = \mathbb{K}^{6'}$: $\mathbb{K}^6 = \{u \in \mathbb{K} / \sigma(u) = u, \forall \sigma \in 6\}$, $\mathbb{K}^{6'} = \{u \in \mathbb{K} / \sigma'(u) = u, \forall \sigma' \in 6'\}$.
Dado $u \in \mathbb{K}^6$ y dado $\sigma' \in 6'$, $\sigma'|_{\mathbb{K}} \in 6$ pues $\mathbb{K}|K$ es normal. Luego $\sigma'|_{\mathbb{K}}(u) = u \Rightarrow \sigma'(u) = u \Rightarrow$

2. EXTENSIONES DE GALOIS

DEFINICION: Se dice que una extensión algebraica $|K|k$ es de Galois si k es el cuerpo fijo de algún subgrupo G del grupo $Aut(|K)$, es decir, si $\exists\, G$ subgrupo de $Aut(|K)$ tal que

$$|K^G = k.$$

Consecuencia inmediata de la definición es que si $|K|k$ es de Galois y $|K^G = k$, entonces $G \subset Aut_k(|K)$, pues $k = \{u \in |K / \sigma(u) = u, \forall \sigma \in G\}$

2.1. PROPOSICION: Si la extensión $|K|k$ es de Galois y $G' = Aut_k |K$ entonces $|K^{G'} = k$

Demostr.: Por hipótesis, existe un subgrupo G de $Aut_k |K$ tal que $|K^G = k$. Veamos que $|K^{G'} = k$. Trivialmente $|K^{G'} \supset k$, pues los elementos de $|K^{G'}$ son aquellos elementos de $|K$ que permanecen fijos por los k-automorfismos de $|K$. Veamos que $|K^{G'} \subset k$.

Si $u \in |K^{G'}$, $\sigma(u) = u$, $\forall \sigma \in G'$. En particular, puesto que $G \subset G'$, $\forall \sigma \in G$, $\sigma(u) = u$. Luego $u \in |K^G = k$. c.q.d.

2.2. TEOREMA: Sea $|K|k$ una extensión algebraica. Las proposiciones siguientes son equivalentes:

a) $|K|k$ es de Galois.

b) $|K$ es cuerpo de descomposición de una familia P de polinomios en $k[x]$ irreducibles y separables.

c) La extensión $|K|k$ es normal y separable.

Demostr.: a) $\Rightarrow$ b)] Sea $P = \{f_u(x) / u \in |K\}$ donde $f_u(x) = Irr(u, k)$. Dado $u \in |K$, el conjunto $Raices_{|K} f_u(x)$ es no vacío (u es raiz de $f_u(x)$ y $u \in |K$) y finito. Sea $Raices_{|K} f_u(x) = \{u_1, \dots, u_n\}$.

Consideremos el polinomio $g(x) = \prod_{i=1}^{n} (x - u_i)$.

Si $G = Aut_k |K$, entonces $|K^G = k$, pues $|K|k$ es de Galois.

Dado $\sigma \in G$, $\sigma(g(x)) = \prod_{i=1}^{n} (x - \sigma(u_i))$

Puesto que G opera transitivamente sobre $Raices_{|K} f_u(x)$, y σ es automorfismo de $|K$ se tiene que $\sigma(\{u_1, \dots, u_n\}) = \{u_1, \dots, u_n\}$

Por tanto, $\sigma(g(x)) = g(x)$ y, como en otras ocasiones, $g(x) \in |K^G[x]$

Pero $|K^G = k$. Luego $g(x) \in k[x]$. Siendo u raiz de $g(x)$, ya que $u \in \{u_1, \dots, u_n\}$ se tiene que $f_u(x) \mid g(x)$. Dado que f_u tiene todas las raices de g, por definición de g, debe ser $g(x) \mid f_u(x)$

Luego $f_u(x) = g(x)$. Siendo g separable, por cons[illegible]

$\mathbb{K}$ es cuerpo de descomposición de P, pues $\mathbb{K} = K(\text{Raices}_{\mathbb{K}} P)$, pues cada $u \in \mathbb{K}$ es raiz de $f_u(x) \in P$ y además $\text{Raices}_{\mathbb{K}} P \subset \mathbb{K}$. c.s.g.d.

b) ⇒ c) La extensión $\mathbb{K}|K$ es normal en virtud de PROPOSICION 1.2.

Veamos que es separable. Por hipótesis, $\mathbb{K} = K(\text{Raices}_{\mathbb{K}} P)$. Si probamos que todo elemento de $\text{Raices}_{\mathbb{K}} P$ es separable sobre K quedará visto que $\mathbb{K}|K$ es separable (ver corolario 4.5, Tema 13).

Si $u \in \text{Raices}_{\mathbb{K}} P$, u es raiz de un polinomio $f(x) \in P$ que es irreducible y separable. Luego $f(x) = \text{Irr}(u, K)$ y f es separable, que prueba que u es separable sobre K. c

c) ⇒ a) Si $\mathbb{K}|K$ es normal y llamamos $G = \text{Aut}_K \mathbb{K}$, entonces $\mathbb{K}^G = \mathbb{K}_{\text{rad}}$ (PROPOSICION 1.3). Luego todo elemento de $\mathbb{K}^G$ es radical sobre K.

Además, ($\mathbb{K}|K$ es separable) y ($\mathbb{K}^G \subset \mathbb{K}$) ⇒ ($\mathbb{K}^G|K$ es separable).

Luego todo elemento u de $\mathbb{K}^G$ es separable sobre K.

Por tanto, todo elemento u de $\mathbb{K}^G$ es separable y radical sobre K, y en consecuencia, $u \in K$. En definitiva, $\mathbb{K}^G = K$, que prueba que $\mathbb{K}|K$ es de Galois. c.s.q.d.

2.3. PROPOSICION: Sean L, $\mathbb{K}$ y K cuerpos tales que $L \supset \mathbb{K} \supset K$. Si $L|K$ es de Galois, entonces $L|\mathbb{K}$ es de Galois.

Demostr.: Si $L|K$ es de Galois, es separable y, por tanto, $L|\mathbb{K}$ es separable. Veamos que $L|\mathbb{K}$ es normal.

Siendo $L|K$ normal, $L = K(\text{Raices}_{\bar{K}} P)$ donde P es una familia de polinomios irreducibles sobre K, de $K[x]$.

Puesto que $K \subset \mathbb{K}$, $K(\text{Raices}_{\bar{K}} P) \subset \mathbb{K}(\text{Raices}_{\bar{K}} P)$.

Además $\mathbb{K} \subset L = K(\text{Raices}_{\bar{K}} P)$. Luego $L = \mathbb{K}(\text{Raices}_{\bar{K}} P)$.

Sea P' el conjunto de factores irreducibles sobre $\mathbb{K}$ de los polinomios de P. Evidentemente, $\text{Raices}_{\bar{K}} P' = \text{Raices}_{\bar{K}} P$.

Luego $L = \mathbb{K}(\text{Raices}_{\bar{K}} P')$, es decir, L es un cuerpo de descomposición sobre $\mathbb{K}$ de una familia de polinomios irreducibles sobre $\mathbb{K}$ y, por tanto, según PROPOSICION 1.2, $L|\mathbb{K}$ normal.

En definitiva, ($L|\mathbb{K}$ normal y separable) ⇒ ($L|\mathbb{K}$ de Galois). c.s.q.d.

DEFINICION: (Grupo de Galois de una extensión de Galois).

Si $\mathbb{K}|K$ es una extensión de Galois se llama grupo de Galois de la extensión a $\text{Aut}_K \mathbb{K}$. Escribiremos

$$\text{Gal}(\mathbb{K}|K) = \text{Aut}_K \mathbb{K}.$$

2.4. TEOREMA: (de Artin)

Sea K un cuerpo y G un subgrupo finito del grupo $Aut(K)$. Entonces la extensión $K|K^G$ es de Galois y el grado de la extensión es $o(G)$, es decir, $[K:K^G]=o(G)$.

Demostr.: Que la extensión $K|K^G$ es de Galois es trivial por la definición de extensión de Galois.

① $[K:K^G]\leq o(G)$: Probaremos esto en varias etapas.

1.a) $\forall u\in K$, $[K^G(u):K^G]\leq o(G)$: Sea $G=\{\sigma_1,\dots,\sigma_n\}$. Dado $u\in K$, consideremos $\sigma_1(u),\dots,\sigma_n(u)$. De estos elementos algunos pueden repetirse. Consideremos en G un subconjunto <u>maximal</u> $\{\sigma_1,\dots,\sigma_r\}$ tal que $\sigma_i(u)\neq\sigma_j(u)$ si $i\neq j$, es decir, tomamos $\{\sigma_1,\dots,\sigma_r\}\subset G$ de modo que $\sigma_i(u)\neq\sigma_j(u)$ si $i\neq j$ y si $k>r$ $\sigma_k(u)=\sigma_i(u)$ para algún $i\leq r$.

Consideremos el polinomio $f(x)=\prod_{i=1}^{r}(x-\sigma_i(u))$. Veamos ahora que $\forall\tau\in G$, $\tau(f(x))=f(x)$.

Dado $\tau\in G$, $\tau(f(x))=\prod_{i=1}^{r}[x-\tau(\sigma_i(u))]$

Siendo τ biyectiva, los elementos $\tau(\sigma_1(u)),\tau(\sigma_2(u)),\dots,\tau(\sigma_r(u))$ son distintos dos a dos. Sea $\Delta=\{\sigma_1(u),\dots,\sigma_r(u)\}$.

Veamos que $\tau(\Delta)=\Delta$. Dado $i\in\{1,\dots,r\}$, si $\tau(\sigma_i(u))\notin\Delta$, los elementos $\sigma_1(u),\dots,\sigma_r(u),\tau(\sigma_i(u))$ son distintos dos a dos y, puesto que $\tau\circ\sigma_i\in G$, hemos llegado a una contradicción con el carácter maximal de $\{\sigma_1,\dots,\sigma_r\}$. Luego $\tau(\sigma_i(u))\in\Delta$, $\forall i\in\{1,\dots,r\}$. En particular, $u\in\Delta$, pues si $u\notin\Delta$ tomando $\tau=id_K\in G$ llegaríamos nuevamente a una contradicción con el carácter maximal de $\{\sigma_i\}_{i=1}^{r}$.

Luego $\tau(f(x))=f(x)$, y por tanto, los coeficientes de $f(x)$ están en K^G, es decir, $f(x)\in K^G[x]$. Además $\partial^\circ(f(x))=r\leq o(G)$.

Siendo u raiz de $f(x)$ se tiene que $Irr(u,K^G)\mid f(x)$ y, en consecuencia, $\partial^\circ(Irr(u,K^G))\leq\partial^\circ(f(x))\leq o(G)$.

Ya que $[K^G(u):K^G]=\partial^\circ(Irr(u,K^G))$, se tiene que $[K^G(u):K^G]\leq o(G)$ y esto cualquiera que sea $u\in K$.

Como $\{[K^G(u):K^G]/u\in K\}$ está acotado superiormente por $o(G)$, siempre podemos tomar $u\in K$ tal que $[K^G(v):K^G]\leq[K^G(u):K^G]$, $\forall v\in K$.

1.b) Probemos que $K=K^G(u)$. Evidentemente, $K^G(u)\subset K$. Si existiese $v\in K$ tal que $v\notin K^G(u)$ podríamos considerar la extensión

braica y de generación finita) y además separable, por serlo $K|K^G$, será simple (por el teorema del elemento primitivo), es decir, existe $\xi \in K$ tal que $K^G(u,v) = K^G(\xi)$.

Se tendría entonces $[K^G(\xi) : K^G] > [K^G(u) : K^G]$, en contra de la elección de u. Por tanto, $K = K^G(u)$.

Como por 1.a) $[K^G(u) : K^G] \leq o(G)$, se tiene que $[K : K^G] \leq o(G)$.

② $[K : K^G] \geq o(G)$: Siendo $K|K^G$ separable, por ser de Galois, $[K : K^G] = [K : K^G]_S$. Dado que $K|K^G$ es finita (por ①) se tiene $[K : K^G]_S = o(\mathrm{Hom}_{K^G}(K, \bar{K}))$

Siendo la extensión $K|K^G$ normal, se tiene que

$$o(\mathrm{Hom}_{K^G}(K, \bar{K})) = o(\mathrm{Aut}_{K^G} K)$$

pues si $\sigma \in \mathrm{Hom}_{K^G}(K, \bar{K})$, $\sigma(K) = K$ y, por tanto, $\sigma : K \to K$ es un automorfismo de K que deja fijos los elementos de K^G y, recíprocamente, todo automorfismo de K que deja fijos los elementos de K^G, puede "ser considerado" como un K^G-homomorfismo de K en $\bar{K}$.

Puesto que $G \subset \mathrm{Aut}_{K^G} K$, por definición de K^G, se verifica que $o(\mathrm{Aut}_{K^G} K) \geq o(G)$. En definitiva, $[K : K^G] \geq o(G)$.

En resumen, $[K : K^G] = o(G)$. c.s.q.d.

2.5. TEOREMA: (fundamental de la Teoría de Galois).

> Si $\mathbb{K}|K$ es una extensión finita de Galois, existe una biyección entre los subcuerpos intermedios de la extensión y los subgrupos de $\mathrm{Aut}_K \mathbb{K}$, es decir, si $\mathcal{J}$ es el conjunto de cuerpos K' tales que $K \subset K' \subset \mathbb{K}$ y $\mathcal{S}(\mathrm{Aut}_K \mathbb{K})$ es el conjunto de subgrupos de $\mathrm{Aut}_K \mathbb{K}$, entonces existe una biyección entre $\mathcal{J}$ y $\mathcal{S}(\mathrm{Aut}_K \mathbb{K})$.

Demostr.: Consideremos las aplicaciones:

$$\Phi : \mathcal{S}(\mathrm{Gal}(\mathbb{K}|K)) = \mathcal{S}(\mathrm{Aut}_K \mathbb{K}) \longrightarrow \mathcal{J}$$
$$H \longmapsto \mathbb{K}^H$$

$$\Psi : \mathcal{J} \longrightarrow \mathcal{S}(\mathrm{Gal}(\mathbb{K}|K))$$
$$K' \longmapsto \mathrm{Gal}(\mathbb{K}|K')$$

Estas aplicaciones están bien definidas, pues si H es un subgrupo de $\mathrm{Gal}(\mathbb{K}|K)$, entonces $\mathbb{K}^H$ es un subcuerpo de $\mathbb{K}$ que contiene a K, y si K' es un subcuerpo de $\mathbb{K}$ que contiene a K, entonces el grupo $\mathrm{Gal}(\mathbb{K}|K') = \mathrm{Aut}_{K'} \mathbb{K}$ es un subgrupo de $\mathrm{Gal}(\mathbb{K}|K) = \mathrm{Aut}_K \mathbb{K}$.

Si probamos que $\Psi \circ \Phi$ es la identidad en $\mathcal{S}(\mathrm{Gal}(\mathbb{K}|K))$ y

$$* \quad S(Gal(\mathbb{K}|k)) \xrightarrow{\varphi} \mathcal{J} \xrightarrow{\psi} S(Gal(\mathbb{K}|k))$$
$$H \longmapsto \mathbb{K}^H \longmapsto Gal(\mathbb{K}|\mathbb{K}^H)$$

Se trata de ver que $(\psi\circ\varphi)(H) = H$, es decir, que $Gal(\mathbb{K}|\mathbb{K}^H) = H$.
Sea $G = Gal(\mathbb{K}|\mathbb{K}^H)$. Segun Proposición 2.1, $\mathbb{K}^H$ es el cuerpo fijo de $Aut_{\mathbb{K}^H}\mathbb{K}$, ya que siendo $\mathbb{K}|k$ de Galois, tambien es de Galois la extensión $\mathbb{K}|\mathbb{K}^H$; es decir, $\mathbb{K}^H = \mathbb{K}^G$.
Por el teorema de Artin, siendo $\mathbb{K}|\mathbb{K}^H$ una extensión finita se tiene que $[\mathbb{K}:\mathbb{K}^H] = o(H)$; de la misma manera, $[\mathbb{K}:\mathbb{K}^G] = o(G)$.
Puesto que $\mathbb{K}^H = \mathbb{K}^G$, debe ser $o(H) = o(G)$.
Como $H \subset G = Aut_{\mathbb{K}^H}\mathbb{K}$, pues los elementos de H son automorfismos de $\mathbb{K}$ y dejan fijos los elementos de $\mathbb{K}^H$, por definicion de $\mathbb{K}^H$, se tiene que $H = G$. Luego $\psi\circ\varphi = id_{S(Gal(\mathbb{K}|k))}$

$$** \quad \mathcal{J} \xrightarrow{\psi} S(Gal(\mathbb{K}|k)) \xrightarrow{\varphi} \mathcal{J}$$
$$K' \longmapsto H = Gal(\mathbb{K}|K') \longmapsto \mathbb{K}^H$$

Se trata de ver que $(\varphi\circ\psi)(K') = K'$, es decir, que $\mathbb{K}^H = K'$, pero esto es trivial pues, por definición de extensión de Galois, K' es el cuerpo fijo de H de la extensión, es decir, $K' = \mathbb{K}^H$. c.s.q.d.

2.6. PROPOSICION: Sea $\mathbb{K}|k$ una extensión finita de Galois y K' un cuerpo intermedio de la extensión $(k \subset K' \subset \mathbb{K})$. Entonces $K'|k$ es de Galois si, y solo si, $H = Aut_{K'}\mathbb{K}$ es un subgrupo normal de $G = Gal(\mathbb{K}|k)$

Demostr: $\Rightarrow$ Supongamos que $K'|k$ es de Galois y veamos que H es subgrupo normal de $G = Aut_k\mathbb{K}$.
Consideremos la aplicación

$$\psi : Gal(\mathbb{K}|k) \longrightarrow Gal(K'|k)$$
$$\sigma \longmapsto \sigma|_{K'}$$

ψ está bien definida, pues si $\sigma \in Aut_k\mathbb{K}$, la restricción de σ a K' es un k-automorfismo de K' (por ser normal la extensión $K'|k$).
Veamos que ψ es homomorfismo, es decir, que
$\forall \sigma, \xi \in Aut_k\mathbb{K}$, $(\sigma\circ\xi)|_{K'} = \sigma|_{K'} \circ \xi|_{K'}$.
Dado $u \in K'$, $\xi(u) \in K'$, pues $K'|k$ es normal y, por tanto, con razon, $(\sigma\circ\xi)(u) \in K'$. Entonces
$\forall u \in K'$, $(\sigma\circ\xi)(u) = \sigma(\xi|_{K'}(u)) = (\sigma|_{K'} \circ \xi|_{K'})(u)$.
$\forall u \in K'$, $(\sigma\circ\xi)|_{K'} = \sigma|_{K'} \circ \xi|_{K'}$

Además Ψ es sobre: Dado $\sigma_1 \in Aut_K K'$, σ_1 se puede prolongar a un automorfismo $\bar{\sigma}$ de $\bar{K}$, cuya restricción a K ($\sigma = \bar{\sigma}|_K$) es un K-automorfismo de K, pero ser $K|_K$ normal. Además $\sigma|_{K'} = \sigma_1$. Luego dado $\sigma_1 \in Gal(K'|_K)$, $\exists\, \sigma \in Gal(K|_K)$ / $\Psi(\sigma) = \sigma_1$.

Si probamos que $Ker\,\Psi = Gal(K|_{K'})$ quedará probado que $H = Aut_{K'} K$ es subgrupo normal de $G = Aut_K K$, pues $Ker\,\Psi$ es siempre un subgrupo normal.

$(\sigma \in Ker\,\Psi) \Leftrightarrow (\sigma|_{K'} = id_{K'}) \Leftrightarrow (\sigma$ deja fijo a $K') \Leftrightarrow (\sigma \in H = Aut_{K'} K)$.

Luego, $Gal(K|_{K'})$ es subgrupo normal de $Gal(K|_K)$.

$\Leftarrow$ Suponemos que $H = Aut_{K'} K$ es subgrupo normal de $G = Gal(K|_K)$

Queremos probar que $K'|_K$ es normal, pues ya es separable. (*)

Se trata de ver entonces que $\forall \sigma \in Aut_K \bar{K}$, $\sigma(K') \subset K'$, donde $\bar{K}$ es una clausura algebraica de K que contiene a K (y por tanto, a K'), o también, que $\forall u \in K'$, $\forall \sigma \in Aut_K \bar{K}$, $\sigma(u) \in K'$.

Si tenemos en cuenta que $H = Aut_{K'} K$, tendremos que $K' = K^H = \{u \in K \,/\, \xi(u) = u, \forall \xi \in H\}$. En definitiva, lo que queremos probar es que $\forall u \in K'$, $\forall \sigma \in Aut_K \bar{K}$, $\forall \xi \in H$, $\xi(\sigma(u)) = \sigma(u)$.

Siendo normal la extensión $K|_K$, dado $\sigma \in Aut_K \bar{K}$, la restricción $\sigma_1 = \sigma|_K : K \to K$ es un automorfismo de K.

Puesto que H es normal en $G = Aut_K K$, se tiene que $\forall \xi \in H$, $\sigma_1^{-1} \xi \sigma_1 \in H$ y, siendo H el conjunto de K'-automorfismos de K se deduce que $\forall u \in K'$, $(\sigma_1^{-1} \xi \sigma_1)(u) = u$, y, por tanto, $\forall u \in K'$, $\xi(\sigma_1(u)) = \sigma_1(u)$.

Pero, dado que $\sigma_1 = \sigma|_K$ se tiene que $\sigma_1(u) = \sigma(u)$.

Luego $\forall u \in K'$, $\forall \xi \in H$, $\forall \sigma \in Aut_K \bar{K}$, $\xi(\sigma(u)) = \sigma(u) \Rightarrow$
$\Rightarrow \forall u \in K'$, $\forall \sigma \in Aut_K \bar{K}$, $\sigma(u) \in K^H = K'$. Por tanto, $K'|_K$ es de Galois, como se indicó anteriormente. c.s.q.d.

2.7. COROLARIO: Si $K|_K$ es una extensión finita y K' es un cuerpo intermedio de la extensión y las extensiones $K|_K$ y $K'|_K$ son de Galois, entonces

$$Gal(K'|_K) \simeq Gal(K|_K) / Gal(K|_{K'})$$

La demostración es consecuencia inmediata de la hecha en el teorema anterior (en la condición necesaria), si tenemos en cuenta que Ψ es sobre y que $Im\,\Psi \simeq \frac{Gal(K|_K)}{Ker\,\Psi}$.

* Recogemos en el siguiente teorema algunos resultados importantes ya probados o que son consecuencia inmediata de resultados anteriores.

2.8. TEOREMA: Sea $\mathbb{K}|K$ una extensión finita de Galois y $G = Gal(\mathbb{K}|K)$.

① Si H es un subgrupo de G entonces $[\mathbb{K} : \mathbb{K}^H] = o(H)$.
② Si H es subgrupo de G, $i(H) = [\mathbb{K}^H : K]$.
③ Sean H_1 y H_2 subgrupos de G, entonces $H_1 \supset H_2 \Leftrightarrow \mathbb{K}^{H_1} \subset \mathbb{K}^{H_2}$.
④ Si K' es un cuerpo tal que $K \subset K' \subset \mathbb{K}$, entonces
$(K'|K$ es de Galois$) \Leftrightarrow (H = Aut_{K'}\mathbb{K} \lhd G)$
y, en este caso, $Gal(K'|K) \simeq Gal(\mathbb{K}|K)/H$

Demostr.: ① Th. de Artin.

② Siendo $K = \mathbb{K}^G$, $o(G) = [\mathbb{K} : K] = [\mathbb{K} : \mathbb{K}^H] \cdot [\mathbb{K}^H : K] = o(H) \cdot [\mathbb{K}^H : K]$.
Siendo $o(G) = o(H) \cdot i(H)$, debe ser $i(H) = [\mathbb{K}^H : K]$.

③ $\Rightarrow$ Si $H_1 \supset H_2$, se tiene que $Aut_{H_1}\mathbb{K} \subset Aut_{H_2}\mathbb{K}$ y, por tanto, $\mathbb{K}^{H_1} \subset \mathbb{K}^{H_2}$.
$\Leftarrow$ Si $\mathbb{K}^{H_1} \subset \mathbb{K}^{H_2} \subset \mathbb{K}$, entonces $Gal(\mathbb{K}|\mathbb{K}^{H_2}) \subset Gal(\mathbb{K}|\mathbb{K}^{H_1})$, es decir $H_2 \subset H_1$, pues $H_1 = Gal(\mathbb{K}|\mathbb{K}^{H_1})$ y $H_2 = Gal(\mathbb{K}|\mathbb{K}^{H_2})$.

④ PROPOSICIÓN 2.6. COROLARIO 2.7.