Rec. En la clase del 15/11/23 enunciamos el Teorema principal de teoría de Galois:

$K \overset{Gal}{\supset} k :\Leftrightarrow \exists\, G \overset{fin}{<} Aut(K) : k = Fix(K, G)$

En este caso

(1) $\{\text{cuerpos interm de } K \supset k\} \underset{Fix(K,-)}{\overset{Aut(K,-)}{\rightleftarrows}} \{\text{subgr. de } Aut(K,k)\}$ son biyecciones inversas

(2) $K \supset k$ es finita $\Rightarrow$ para $\forall\, K \supset L \supset k$ tenemos
- (a) $[K:L] = |Aut(K,L)|$
- (b) $[L:k] = |Aut(K,k) : Aut(K,L)|$

(3) $\forall\, K \supset L \supset k$:
- (a) $K \overset{Gal}{\supset} L$
- (b) $L \supset k$ Gal $\Leftrightarrow Aut(K,L) \lhd Aut(K,k)$
- (c) $L \overset{Gal}{\supset} k \Rightarrow$
  - $\varphi(L) = L \quad \forall\, \varphi \in Aut(K,k)$
  - $?|_L : Aut(K,k) \twoheadrightarrow Aut(L,k)$ supra
  - $\ker(?|_L) = Aut(K,L)$

En la última clase demostramos (1), (2) y (3a)
Continuamos con (3b) y (3c)

3.2.16 Obs Sea L un campo intermedio de $K \supset \mathbb{k}$ extensión de campos y $\varphi \in Aut(K, \mathbb{k})$, ent.

$$Aut(K, \varphi(L)) = \varphi\, Aut(K, L)\, \varphi^{-1} < Aut(K, \mathbb{k})$$

$\forall\, \varphi \in Aut(K, \mathbb{k})$,
como se verifica fácilmente.

3.2.17 Lema Sea L un campo intermedio de $K \overset{Gal}{\supset} \mathbb{k}$ t.q. $\varphi(L) = L$ $\forall\, \varphi \in Aut(K, \mathbb{k})$

$\Rightarrow ?|_L : Aut(K, \mathbb{k}) \longrightarrow Aut(L, \mathbb{k})$, $\varphi \mapsto \varphi|_L$

es un homomorfismo suprayectivo de grupos

Dem. Solamente la suprayectividad no es evidente.

Sea $G := \mathrm{Im}(?|_L) \leq \mathrm{Aut}(K, k)$.

$K \overset{\text{Gal}}{\supset} k \Longrightarrow k = \mathrm{Fix}(K, \mathrm{Aut}(K, k))$

$= \mathrm{Fix}(L, G)$

$\uparrow$ constr.

y G es finito, ya que es imagen de un grupo finito

$\overset{3.2.12}{\Longrightarrow} \mathrm{Aut}(L, k) = G$

$= \mathrm{Fix}(L, G)$ □

3.2.18 Lema Sea L un campo intermedio de una ext. de Galois $K \supset k$.

Entonces son equiv:

(1) $L \overset{\text{Gal}}{\supset} k$

(2) $\forall \varphi \in \mathrm{Aut}(K, k) : \varphi(L) = L$

(3) $\mathrm{Aut}(K, L) \trianglelefteq \mathrm{Aut}(K, k)$

Dem. (1) $\Rightarrow$ (2) Sea $r = |\mathrm{Aut}(L:k)|$,
$\{\varphi_1 = id_L, \varphi_2, \dots, \varphi_r\} = \mathrm{Aut}(L:k)$. Interpretamos
a los φ_i como $\varphi_i : L \hookrightarrow K$ (inyectivos)

Es suficiente ver que no hay otro hom.
$\varphi_{r+1} : L \to K$ con $\varphi_{r+1}|_k = id_k$,
pues en este caso todo tenemos para todo
$\varphi \in \mathrm{Aut}(K:k)$ que $\varphi|_L \in \{\varphi_1, \dots, \varphi_r\}$
$\overset{\text{finito}}{\Rightarrow}$ $\varphi(L) = L$.

Sea pues $\varphi_{r+1} : L \hookrightarrow K$ con estas propiedades.
Entonces
$$k = \{a \in L \mid a = \varphi_2(a) = \dots = \varphi_r(a)\}$$
$\uparrow$ Gal
$$= \{a \in L \mid \varphi_1(a) = \varphi_2(a) = \dots = \varphi_r(a) = \varphi_{r+1}(a)\}$$

Pero esto último contradice a 3.2.8.:

$[L:k] \geq n+1 \Rightarrow |Aut(L,k)| = [L:k]$ (3.2.17.)

(2) $\Rightarrow$ (3)

Por (2) el mapeo $?|_L : Aut(K,k) \to Aut(L,k)$ está bien definido y $Aut(K,L) = \ker(?|_L) \trianglelefteq Aut(K,k)$

(3) $\Rightarrow$ (2)

Por Obs. 3.2.16 $Aut(K,\varphi(L)) = Aut(K,L)$ $\forall \varphi \in Aut(K,k)$.

(2) $\Rightarrow$ (1)

Por 3.2.17 $?|_L : Aut(K,k) \to Aut(L,k)$ es suprayectivo $\Rightarrow H = Aut(L,k)$ finito y $k = Fix(L,H)$ sigue de $?|_L$ suprayectivo y $k = Fix(K, Aut(K,k))$ (Gal.)

Claramente 3.2.17 y 3.2.18 implican Thm 3.2.4 (3b)

3.3. Extensiones Normales

Roc $G \overset{\text{fin}}{<} Aut(K)$ y $L := Fix(K, G) \overset{\text{Def.}}{\Longrightarrow} K \overset{\text{Gal}}{\supset} L$

$\overset{3.2.12}{\Longrightarrow}$ $Aut(K, L) = G$

3.3.1. Def. Una extn. $K \supset k$ de cuerpos es **normal** si

(a) $K \supset k$ es algebraica

(b) Si $f \in k[X]$ es irred y $\exists\, a \in K$ con $f(a) = 0$ entonces f factoriza en factores lin. / K

Obviamente (b) es equiv. a

(b') $\forall\, a \in K$ el polinomio mínimo de a / k factoriza en factores lineales / K.

3.3.2 Prop. Para una extensión finita de campos $K \supset k$ son equivalentes

(1) $K \supset k$ es normal

(*) (2) K es el campo de descomposición de algún $f \in k[x]$

(3) Si $K' \supset K$ es una extn. de campos y $\varphi : K \longrightarrow K'$ hom. de campos con $\varphi|_k = id_k$, entonces $\varphi(K) = K$.

Dem (1) $\Rightarrow$ (2) fácil

(2) $\Rightarrow$ (3)

Por hipótesis $\exists\, f \in k[x]$ y $a_1, a_2, \dots, a_n \in K$, $b \in k$ con $f = b(x-a_1)(x-a_2)\cdots(x-a_n)$ t.q. $K = k(a_1, a_2, \dots, a_n)$

Si $\varphi : K \longrightarrow K'$ hom. de campos con $\varphi|_k = id_k$
como en (3), entonces

$$f(\varphi(a_i)) \overset{\uparrow}{=} \varphi(f(a_i)) = 0 \Rightarrow \varphi(a_i) \in \{a_1, \dots, a_n\}$$
$$f \in k[x]$$

$\Rightarrow \varphi(K) \subseteq K$.

(3) $\Rightarrow$ (1)

$[K : k] < \infty \Rightarrow K \supset k$ alg (1.32)

Sea $f \in k[x]$ irred y $a \in K$ con $f(a) = 0$

Entonces cojamos $a_1, a_2, \dots, a_n \in K$ t.q.

$K = k(a, a_1, \dots, a_n)$

y sea $f_i \in k[x]$ pol. min. de a_i / k

$\Rightarrow K$ es campo intermedio de $K' \supset k$

con K' campo de desc. de $g := f \cdot f_1 \cdots f_n$

Si $b \in K'$ es un cero de f, entonces por 2.2.7 $\exists\, \psi \in Aut(K', k)$ con $\psi(a) = b$

$\Rightarrow b = \psi(a) = \psi_K(a) \overset{(3)}{\in} K$

$\Rightarrow f$ se descompone sobre K en fac. lin. $\square$

Ejemplos
- $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ es normal
- $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}(\sqrt{2})$ es normal
- $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}$ NO es normal:
  $x^4 - 2 \in \mathbb{Q}[x]$ es irred y tiene un cero ($\sqrt[4]{2}$) en $\mathbb{Q}[\sqrt[4]{2}]$, pero
  $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + 2)$
  ↑ irred en $\mathbb{Q}(\sqrt[4]{2})[x]$ ya que los ceros no son reales

3.4. Extensiones Separables

3.4.1 Def Sea k un campo, $K \supset k$ campo de desc. de $f \in k[x]$ ($\deg(f) \geq 1$), $a \in K$, entonces

$$\mu(f,a) := \max\{n \in \mathbb{Z}_{\geq 0} \mid (x-a)^n \mid f \text{ en } K[x]\}$$

la <u>multiplicidad</u> de f en a

$\mu(f,a) = 1 :\Leftrightarrow a$ es un <u>cero simple</u> de f

$\mu(f,a) \geq 2 :\Leftrightarrow \ldots$ un <u>cero multiple</u> de f

3.4.2. Def.

a) Sea k un campo. Un polinomio $f \in k[x]$ se llama separable si sólo tiene ceros simples en su campo de desc. En otro caso f es inseparable.

b) Sea $K \supset k$ una extn. de campos. Un elemento $a \in K$ que es alg. / k se llama separable / k si su polinomio mínimo / k es separable.

c) Una extensión de campos $K \supset k$ es separable, si todos los elementos de K son separables / k.

d) Un campo k es perfecto si cada polinomio irred. $f \in k[x]$ es separable.

Veremos pronto que $\mathrm{char}(k) = 0 \Rightarrow k$ perfecto y más adelante que k finito $\Rightarrow k$ perfecto.

En cálculo, ceros multiples se caracterizan por ser también ceros de la derivada. Vamo a imitar esta idea algebraicamente,

3.4.3 Def. Sea R un anillo conmutativo con 1. El mapeo

$$D : R[X] \longrightarrow R[X],$$

$$\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=1}^{n} i \cdot a_i X^{i-1}$$

se llama diferenciación formal.

D NO es un homomorfismo de anillos, pero sí es una derivación formal

$$D(r_1 f_1 + r_2 f_2) = r_1 D(f_1) + r_2 D(f_2) \;\text{y}$$
$$D(f_1 \cdot f_2) = D(f_1)\cdot f_2 + f_1 \cdot D(f_2)$$

$\forall\, r_1, r_2 \in R$ y $f_1, f_2 \in R[X]$.

3.4.4. Lema Sea k un campo, y $K \supset k$ el campo de desc. de $f \in k[X]$ con $\deg(f) \geq 1$. Entonces para $a \in K$ tenemos

(1) $\mu(f, a) = 1 \iff f(a) = 0$ y $(Df)(a) \neq 0$

(2) $\mu(f, a) \geq 2 \iff f(a) = 0$ y $(Df)(a) = 0$.

Dem estándar.

3.4.5. Cor. Sea k un campo, $f \in k[x]$ no const. y $K \supset k$ campo de desc. de f. Entonces son equiv.:

(1) f tiene ceros múlt. en K

(2) $\mathrm{mcd}_{k[x]}(f, Df)$ no es trivial

Dem. (1) $\Rightarrow$ (2) $a \in K$ con $\mu(f, a) \geq 1 \Rightarrow$ $(x-a) \mid f$ y $(x-a) \mid Df$ en $K[x] \Rightarrow$ $\mathrm{mcd}_{K[x]}(f, Df)$ no es triv. pero por el alg. de Euclides podemos calcular $\mathrm{mcd}(f, Df)$ de forma igual en $k[x]$ y $K[x]$.

(2) $\Rightarrow$ (1) Sea $g \in \mathrm{mcd}_{k[x]}(f, Df)$ no triv. K campo de desc. $\Rightarrow \exists\, a \in K$ con $x-a \mid g$.

3.4.6 Prp. Sea k un campo y $f \in k[x]$ irred.
Entonces f es separable $\iff Df \neq 0$

Dem. Sea K campo de descomp. de f.

$Df = 0 \overset{3.4.4}{\Longrightarrow}$ todos los ceros de f en K tienen multiplicidad ≥ 2.
$\Rightarrow f$ no es sep.

$Df \neq 0 \overset{!}{\Longrightarrow} f$ sep.

De hecho, de lo contrario existe un $g \in k[x]$ con $\deg g \geq 1$ y $g \in mcd(f, Df)$,
pero f es irred $\Rightarrow \deg(g) \geq \deg(f)$,
pero y $g \mid Df$ pero $\deg(Df) < \deg(f)$ ¡¡.

3.4.7 Prop. Sea k un campo, $f \in k(x)$,

a) $\operatorname{char}(k) = 0$ implica $Df = 0 \iff \deg(f) \leq 0$

b) $\operatorname{char}(k) = n > 0$ implica

$Df = 0 \iff f(x) = g(x^n)$ para algún $g \in k[x]$

Dem. Ejercicio.

3.4.8 Cor Si $\operatorname{char}(k) = 0$ entonces k es perfecto.

3.4.9 Ejemplo Sea $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ para algún primo $p \in \mathbb{Z}_{\geq 1}$. Entonces, por Eisenstein $X^p - Y \in \mathbb{F}_p(Y)[X]$ irred, pero $D(X^p - Y) \equiv 0 \Rightarrow \mathbb{F}_p(Y)$ NO es perfecto.