

CUERPOS Y ALGEBRAS

Notas del curso

Semestre primavera 2013

Profesor : Luis Arenas

Cuerpos

Algunos ejemplos de cuerpos son \mathbb{R} , \mathbb{Q} , \mathbb{C} , \mathbb{F}_p , \mathbb{F}_{p^n} , $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\text{Quot}(D)$ (cuerpo de cocientes del dominio D).

Tenemos que $\text{Quot}(\mathbb{Z}) = \mathbb{Q}$, $K(t) = \text{Quot}(K[t])$ (K cuerpo o dominio).

Tenemos la contención $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{Q}(x)$, luego $\text{Quot}(\mathbb{Z}[x]) \subseteq \mathbb{Q}(x)$.

Es evidente ver que $\mathbb{Q}(x) = \text{Quot}(\mathbb{Z}[x])$ (Para ello basta ver que

$f, g \in \mathbb{Q}[x]$; $f = \lambda f_0$, $g = \mu g_0$, donde f_0, g_0 son primativos en $\mathbb{Z}[x]$)

Ejemplo. Para $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ tenemos $\mathbb{F}_q = \{0, 1, \alpha, \alpha+1\}$. Se

cumple que $\alpha^2 = \alpha + 1$. Se recomienda hacer la tabla de suma y producto. Una manera de construir \mathbb{F}_q es considerar el cociente

$$\mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_2 \oplus \bar{x} \mathbb{F}_2$$

Observación. Para un anillo A , $A[x]/(f) \cong A \oplus \bar{x}A \oplus \dots \oplus \bar{x}^{n-1}A$, donde $f = \sum a_i x^i$, $a_n = 1$.

Para el caso anterior, \mathbb{F}_q es cuerpo ya que $\mathbb{F}_2[x]$ es DIP y x^2+x+1 es primo.

Resultado. $f \in \mathbb{F}_p[x]$ primo, $n = \deg f$. Entonces $\mathbb{F}_p[x]/(f)$ es un cuerpo con p^n elementos (Resultado de Estructuras Algebraicas)

Afirmación. Todo cuerpo K está contenido en un cuerpo algebraicamente cerrado Ω (Lema de Zorn).

Para el caso de $\mathbb{F}_p \subseteq \Omega$, donde Ω contiene las raíces de $x^{p^n} - x = 0$.

En ese caso

$$x^{p^n} - x = \prod_{i=1}^{p^n} (x - \lambda_i)$$

Ahora considerando $f(x) = (x-a)^2 g(x)$, a es raíz doble de $f \Leftrightarrow f'(a) = 0$. Para el caso $f(x) = x^{p^n} - x \rightarrow f'(x) = -1$. Luego $f(x) = x^{p^n} - x$ no tiene raíces dobles.

Ahora, $\mathbb{F}_{p^n} = \{a \in \mathbb{Z} / a^{p^n} = a\}$, $|\mathbb{F}_{p^n}| = p^n$. Es fácil demostrar que es un cuerpo (con p^n elementos). Sea L un cuerpo con p^n elementos, $L^* = L \setminus \{0\}$ es un grupo que cumple $\ell^{p^n-1} = 1 \forall \ell \in L^*$. (Recordar que $|L^*| = p^n - 1$).

Por lo tanto $L = \mathbb{F}_{p^n}$ (ya que $L \subseteq \mathbb{F}_{p^n}$ y $|L| = |\mathbb{F}_{p^n}|$). \mathbb{F}_{p^n} es el único cuerpo con p^n elementos contenido en \mathbb{Z} .

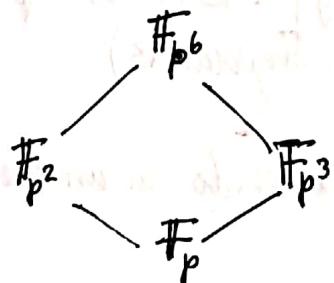
* ¿Cuándo $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$?

Como $[\mathbb{F}_{p^n} : \mathbb{F}] = n$, $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = t$, entonces $p^m = |\mathbb{F}_{p^m}| = |(\mathbb{F}_{p^n})^t| = p^{nt}$. Luego $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Rightarrow n|m$.

Ahora supongamos que $n|m$, $m=nt$ y sea $x \in \mathbb{F}_{p^n}$ que cumple $x^{p^n} = x$. Se tiene que $x^{p^m} = x$ (verificar). Ergo $x \in \mathbb{F}_{p^m}$.

Conclusion: $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m$.

Ejemplo:



Queremos calcular $\#\{\alpha \in \mathbb{F}_p^6 \mid \mathbb{F}_p(\alpha) = \mathbb{F}_p\}$.

Como $\mathbb{F}_p(\alpha) = \mathbb{F}_p \Leftrightarrow \alpha \in \mathbb{F}_p$.

$$\#\{\alpha \mid \mathbb{F}_p(\alpha) = \mathbb{F}_p\} = p$$

$$\#\{\alpha \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^2}\} = p^2 - p$$

$$\#\{\alpha \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^3}\} = p^3 - p$$

entonces $\{\alpha \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}\} = p^6 - (p^2 - p) - (p^3 - p) - p > 0$. En general, existe un $\alpha \in \mathbb{F}_{p^n}$ con $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. (*)

Consideremos ahora la función $S(n) = |\{\alpha \mid \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)\}|$ ($\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \Leftrightarrow \alpha \in \mathbb{F}_{p^n}$). Tenemos $S(n) \leq p^n$. Luego

$$\begin{aligned} S(n) &= p^n - \sum_{\substack{d|n \\ d < n}} \varphi(d) \\ &\geq p^n - \sum_{\substack{d|n \\ d < n}} p^d \geq p^n - \sum_{d < n} p^d = p^n - \frac{p^{n-1}}{p-1} > 0 \end{aligned}$$

(Esto es la demostración de que se cumple (*)

Sea $\alpha \in \mathbb{F}_{p^n}$ con $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Considerando evaluación

$$\varphi: \mathbb{F}_p[x] \rightarrow \mathbb{F}_{p^n}$$

$$\varphi(f(x)) = f(\alpha)$$

Tenemos que $\text{Im } \varphi = \mathbb{F}_p[\alpha]$, $\ker \varphi = (m_\alpha(x))$ (polinomio mínimo).

Como $\mathbb{F}_p[x] \subseteq \mathbb{F}_{p^n}$ es dominio, y $\mathbb{F}_p[x] \cong \mathbb{F}_p[x]/(m_\alpha(x))$, ergo m_α es primo. Luego $\mathbb{F}_p[\alpha]$ es un cuerpo, donde $\mathbb{F}_p[\alpha] = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(m_\alpha(x))$$

m_α es un primo de grado n .

Sea $m(x) \in \mathbb{F}_p[x]$ es un primo de grado n y $\alpha \in \mathbb{Q}$ una raíz. Si $\varphi: \mathbb{F}_p[x] \rightarrow \mathbb{Q}$ es la evaluación en α , $\varphi(\mathbb{F}_p[x]) = \mathbb{F}_p[\alpha]$ es dominio. Entonces $\ker \varphi$ es primo.

$m(\alpha) = 0$, $m \in \ker \varphi$, implica $\ker \varphi = (m(x))$. Se sigue que

$\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/(m(x))$ es un cuerpo de p^n elementos en \mathbb{Q} . Por lo tanto

$$\mathbb{F}_p[\alpha] = \mathbb{F}_{p^n},$$

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(m(x))$$

para cualquier $m \in \mathbb{F}_p[x]$ primo de grado n . Luego no depende de \mathbb{F}_2 .

Ejemplo. ¿Cuántos polinomios de grado 6 hay en $\mathbb{F}_2[x]$? (irreducibles)

$\forall \alpha | \mathbb{F}_2[\alpha] = \mathbb{F}_{2^6}$. Se cumple que

$$\begin{aligned}\beta(6) &= 2^6 - P(2) - P(3) - S(1) \\ &= 2^6 - (2^3 - 2) - (2^2 - 2) - 2 = 54\end{aligned}$$

Hay 9 polinomios.

$m(x)$ irreducible de grado 6 tiene raíces en \mathbb{F}_{2^6} , con $m(x) | x^{2^6} - x$.

Repaso de Teoría de Anillos

Deberemos considerar la cadena de contenidos siguiente:

$$\begin{array}{ccccccccc} (\text{Anillo}) & \supset & (\text{Dominio de Integridad}) & \supset & (\text{Dominio de factorización}) & \supset & (\text{Dominio de ideales}) \\ R & & DI & & DFU & & \text{principales} \\ & & & & \text{única} & & & \\ & & & & & & & \\ & \supset & (\text{Dominio Euclídeo}) & \supset & (\text{Cuerpo}) & & & \end{array}$$

con los siguientes resultados:

- (i) R/P DI $\Leftrightarrow P$ ideal primo
- (ii) R/M cuerpo $\Leftrightarrow M$ maximal
- (iii) R DIP $\Rightarrow (M \text{ maximal} \Leftrightarrow M \text{ primo})$

* Resumen * Hasta el momento deberemos recordar como resultados principales a los siguientes:

- (1) $f \in \mathbb{F}_p[x]$ primo, $n = \deg f$. Entonces $\mathbb{F}_p[x]/(f)$ cuerpo con p^n elementos.
- (2) Todo cuerpo K tiene clausura algebraica Ω (y además, $K \subset \Omega$).
- (3) \mathbb{F}_{p^n} es el cuerpo de descomposición de $p(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
- (4) $L \subseteq K \subseteq F$ (cuerpos), entonces $[F:L] = [F:K][K:L]$.

$$(5) \quad \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m.$$

$$(6) \quad \text{Siempre existe } \alpha \in \mathbb{F}_{p^n}, \quad \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha).$$

(7) Para $\alpha \in \mathbb{F}_p^n$, la función evaluación en α , φ_α

$$\begin{aligned} \varphi_\alpha : \mathbb{F}_p[x] &\longrightarrow \mathbb{F}_{p^n} \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

satisface $\text{Im } \varphi = \mathbb{F}[\alpha]$, $\ker \varphi = (m_\alpha(x))$ (m_α minimal). En particular,

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(m_\alpha(x)) ; \text{ donde } m_\alpha(x) \text{ primo de grado } n, \quad \mathbb{F}_p[\alpha] = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}.$$

$$(8) \quad \mathbb{F}_p[\alpha] = \mathbb{F}_p \text{ si } \alpha \in \mathbb{F}_p.$$

Recordemos que para cualquier \mathbb{F}_p , existe la extensión $\mathbb{F}_{p^r} \cong \mathbb{F}_p[x]/(m(x))$, donde $m(x)$ irreducible. Luego podemos considerar la clausura algebraica

$$\overline{\mathbb{F}_p} = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}.$$

Sea $\mathbb{F}_{p^r} \subset \Omega$. $\mathbb{F}_p(\Omega) = \{w \in \Omega / w \text{ algebraico sobre } \mathbb{F}_p\}$. w es algebraico si existe $m(x) \in \mathbb{F}_p[x]$ irreducible, $m \neq 0$ con $m(w)=0$, $\deg m = n$.

$$\mathbb{F}_p[x]/(m(x)) \cong \mathbb{F}_p[w]$$

$$\mathbb{F}_p \oplus \mathbb{F}_p \oplus \dots \oplus \mathbb{F}_p^{n-1} \quad (\text{como grupos abelianos})$$

Lema. w algebraico sobre \mathbb{F}_p si $\mathbb{F}_p[w]$ es finito. w no algebraico si $\mathbb{F}_p[w] \cong \mathbb{F}_p[x]$.

$$\text{Teneamos que } \overline{\mathbb{F}_p}(\Omega) = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}. \quad \text{Si}$$



Tenemos que $\overline{F_p}(\Omega) \cong \overline{F_p}(\Omega')$, donde

$F_{pr}(\Omega)$: 'Copia de F_{pr} en Ω '

$F_{pr}(\Omega')$: 'Copia de F_{pr} en Ω' '

Nos preguntamos la comutatividad del diagrama siguiente

$$\begin{array}{ccc} \varphi_r : F_{pr}(\Omega) & \longrightarrow & \overline{F_p}(\Omega') \\ \cap & & \cap \\ \varphi_s : F_{ps}(\Omega) & \longrightarrow & \overline{F_p}(\Omega') \end{array}$$

donde r/s . El problema es que el isomorfismo no es único.

Hecho. Los isomorfismos pueden escogerse de manera consistente. En tal caso se define $\Psi : \overline{F_p}(\Omega) \rightarrow \overline{F_p}(\Omega')$ por $\Psi(w) = \varphi_r(w)$ si $w \in F_{pr}(\Omega)$ y esto da un isomorfismo bien definido.

Podemos, para nuestro propósito, estudiar $\text{Aut}(F_{pr})$. Sea $F_{pr} = F_p[\alpha]$, donde $m(x) = (x - \alpha_1) \dots (x - \alpha_r)$, donde $\alpha = \alpha_i$ son raíces distintas (ya que $m(x) | x^{p^r} - x$).

Sea $\Psi \in \text{Aut}(F_{pr})$, entonces Ψ es la identidad sobre F_p (demostrar).

Queremos estudiar $\Psi(\alpha)$. Se tiene que $m(\alpha) = 0$, $\Psi(m(x)) = 0$.

Además

$$m(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0, \quad a_i \in F_p$$

También $\Psi(m(\alpha)) = m(\Psi(\alpha))$ (cuando los coeficientes son invariantes).

$m(\Psi(\alpha)) = 0$. Por lo tanto, $\Psi(\alpha) \in \{\alpha_1, \dots, \alpha_r\}$.

Todo $\beta \in F_{pr}$ es un polinomio en α con coeficientes en F_p .

$$\begin{aligned} \beta &= g(\alpha) \\ \Psi(\beta) &= g(\Psi(\alpha)) \end{aligned}$$

Se tiene que $|\text{Aut}(\mathbb{F}_{p^r})| \leq r$. Un elemento es $\sigma(\beta) = \beta^p$. Es fácil chequear que es un automorfismo (automorfismo de Frobenius). Además

$$\sigma(x) = x \iff x \in \mathbb{F}_p$$

$$\sigma^r(x) = x \iff x \in \mathbb{F}_{p^r}$$

Danotando $G = \text{Aut}(\mathbb{F}_{p^r})$, $\sigma \in G$ tiene orden r . En particular $\text{Aut}(\mathbb{F}_{p^r}) = \langle \sigma \rangle$.

Conclusión. Para cada $i=1, \dots, r$, existe $\varphi \in \text{Aut}(\mathbb{F}_{p^r})$ con $\varphi(\alpha) = \alpha_i$.

Recordemos el diagrama

$$\begin{array}{ccc} \psi_r : \mathbb{F}_{p^r}(\Omega) & \longrightarrow & \mathbb{F}_{p^r}(\Omega') \\ \downarrow & & \downarrow \\ \psi_s : \mathbb{F}_p(\Omega) & \longrightarrow & \mathbb{F}_p(\Omega') \end{array} \quad (*)$$

Sea $\beta \in \mathbb{F}_{p^r}(\Omega)$. Tomando $\psi_s(\beta)^{p^t} = \psi_r(\beta)$ (Los isomorfismos difieren por un automorfismo!). Si reemplazamos ψ_s por $\psi'_s : \mathbb{F}_p(\Omega) \rightarrow \mathbb{F}_p(\Omega')$ definida por $\psi'_s(\beta) = \psi_s(\beta)^{p^t}$, entonces el diagrama (*) comuta.

Como consecuencia de lo anterior, $\mathbb{F}_p(\Omega) = \bigcup_{i=1}^{\infty} \mathbb{F}_{p^{i!}}(\Omega)$ (factoriales están bien ordenados por divisibilidad). Además

$$\begin{array}{ccc} \psi_{i!} = \psi_i : \mathbb{F}_{p^{i!}}(\Omega) & \longrightarrow & \mathbb{F}_{p^{i!}}(\Omega') \\ \downarrow & & \downarrow \\ \psi_{(i+1)!} = \psi_{i+1} : \mathbb{F}_{p^{(i+1)!}}(\Omega) & \longrightarrow & \mathbb{F}_{p^{(i+1)!}}(\Omega') \end{array}$$

Existe un isomorfismo bien definido $\psi : \mathbb{F}_p(\Omega) \rightarrow \mathbb{F}_p(\Omega')$. Además $\mathbb{F}_p(\Omega) \subseteq \mathbb{F}_{p^{i!}}(\Omega)$.

Definiendo $\text{Gal}(\mathbb{F}_p/\mathbb{F}_{p^r}) = \{\varphi \in \text{Aut}(\mathbb{F}_p) \mid \varphi|_{\mathbb{F}_{p^r}} = \text{id}\}$ (Grupo de Galois) ($r|s$).

Evidente que $x^{p^k} = \sigma^k(x) = x$, todo $x \in F_{p^r} \Rightarrow r | k$.

Como resultado, $\text{Gal}(F_{p^s}/F_{p^r}) = \langle \sigma^r \rangle$, donde $\sigma^r(x) = x^{p^r}$.

También

$$(\sigma^r)^k = \text{id}|_{F_{p^s}} \iff s | rk \quad (\frac{s}{r} | k)$$

$$\text{Además } |\text{Gal}(F_{p^s}/F_{p^r})| = \frac{s}{r}$$

Observación. $[F_{p^s} : F_{p^r}] = \frac{s}{r}$ (número de automorfismos).

Para $F_{p^s} = F_{p^r}[\alpha] \quad (\cong F_{p^r}[x]/(m))$, $\varphi: F_{p^s} \rightarrow F_{p^s}$, $\varphi|_{F_{p^r}} = \text{id}$; donde m es el polinomio irreducible de α en $F_{p^r}[x]$, entonces m tiene $\alpha = \alpha_1, \dots, \alpha_t$, $t = \frac{s}{r}$.

Para $\varphi \in G = \text{Gal}(F_{p^s}/F_{p^r})$, $\varphi(\alpha) = \alpha_i$, algún i . α_i determina φ . Luego para cada i , existe $\varphi_i \in G$ con $\varphi_i(\alpha) = \alpha_i$. Además

$$F_{p^r}[x]/(m) \cong F_{p^r} \oplus \dots \oplus \bar{x}^{t-1} F_{p^r}.$$

Ejemplo. Encuentran los polinomios irreducibles de grado 4 en $F_2[x]$.

El número de generadores en F_4 es $|F_2| - 1 | F_2 | = 12$. Hay $\frac{12}{4} = 3$ polinomios irreducibles. Tales polinomios son

$$x^4 + x^3 + x^2 + x + 1$$

$$x^4 + x^3 + 1$$

$$x^4 + x + 1$$

Miscelánea

[1] Si E, F, K son cuerpos, y $E \subseteq F \subseteq K$, entonces F es una extensión sobre E , (denotado por F/E) y K/F . Tenemos además, $[F:E] = \dim_E F$. Por otro lado, se cumple la igualdad

$$[K:E] = [K:F][F:E]$$

Para la demostración sólo basta el caso finito. Para ello sea $\{a_1, \dots, a_n\}$ base de K/F y $\{b_1, \dots, b_m\}$ una base de F/E . Queremos demostrar que $\{a_i b_j\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ es base de K/E . Dado $y \in K$, podemos escribirlo de la forma

$$y = \sum_{i=1}^n e_i a_i ; \quad \{e_1, \dots, e_n\} \subset F$$

pero, para cada i , existe $\{f_{1i}, \dots, f_{ni}\} \subset E$ tal que

$$e_i = \sum_{j=1}^m f_{ji} b_j$$

Por lo tanto, $y = \sum_{i=1}^n \sum_{j=1}^m f_{ji} b_j a_i$. Demostren que es ligeramente independiente fácil.

[2] $F(\alpha)$ es el cuerpo más pequeño que contiene a F y α .

[3] Si \bar{F} es la clausura algebraica de F , entonces \bar{F}/F es una extensión algebraica.

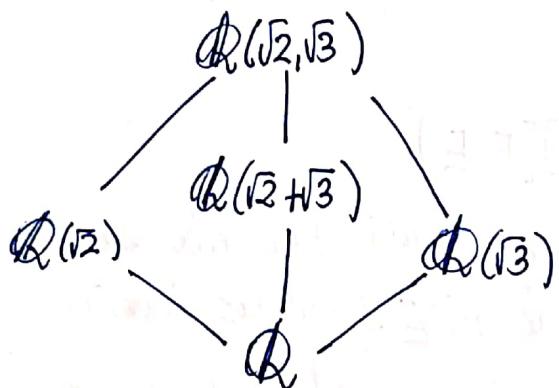
[4] El cuerpo más pequeño que contiene a F, α, β se denota por $F(\alpha, \beta)$, y es evidente que $F(\alpha)(\beta) = F(\alpha, \beta)$.

[5] Sean $L, M \subseteq K$ cuerpos, entonces LM denota al cuerpo más pequeño que contiene a L y M (composición de L y M). Si $L/F, M/F$ son extensiones finitas, entonces

$$[LM:F] \leq [L:F][M:F]$$

En efecto, si $L = F(\alpha_1, \dots, \alpha_n)$, $M = F(\beta_1, \dots, \beta_m)$, entonces,
 $LM = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$; donde $[L:F]=n$, $[M:F]=m$. Por lo
tanto $[LM:F] \leq nm$.

Como aplicación, observemos



Afirmación. $Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$.

Extensión de homomorfismos.

Proposición. Sea E/F una extensión de cuerpos algebraica y Ω cuerpo algebraicamente cerrado. Sea $\varphi: F \rightarrow \Omega$ un homomorfismo. Entonces existe un homomorfismo

$$\bar{\varphi}: E \rightarrow \Omega$$

que extiende a φ ($\bar{\varphi}|_F = \varphi$).

Observación. E/F es extensión algebraica si cada $\alpha \in E$ es algebraico sobre F . También, si $F' \supseteq F$ y α es algebraico sobre F , entonces es algebraico sobre F' . α es algebraico sobre F ssi $F[\alpha]$ es cuerpo.

- Demarcación - Sea

$$\Sigma = \left\{ (F, \varphi) \mid \begin{array}{l} F \subseteq F' \subseteq E \\ \varphi: F' \rightarrow \Omega \\ \text{extiende a } \varphi \end{array} \right\}$$

Definimos un orden \leq por

$$(F', \varphi') \leq (F'', \varphi'') \text{ ssi } (F' \subseteq F'', \varphi''|_{F'} = \varphi')$$

Tenemos que $\Sigma \neq \emptyset$, $(F, \varphi) \in \Sigma$. $\{(F_i, \varphi_i)\}_{i \in I}$ es cadena si $i, j \in I \Rightarrow ((F_i, \varphi_i) \leq (F_j, \varphi_j) \vee (F_j, \varphi_j) \leq (F_i, \varphi_i))$. Tenemos

$$F' = \bigcup_{i \in I} F_i$$

$$\varphi: F' \rightarrow \Omega$$

$$\alpha \in F_i \Rightarrow \varphi(\alpha) = \varphi_i(\alpha)$$

Además $\alpha \in F_i$, $\varphi(\alpha) = \varphi_i(\alpha)$. $\alpha \in F_j$, $\varphi(\alpha) = \varphi_j(\alpha)$.

$(F_i, \varphi_i) \leq (F_j, \varphi_j)$ implica $F_i \subseteq F_j$, $\varphi_j|_{F_i} = \varphi_i$.

$$\alpha \in F_i, \quad \varphi_j(\alpha) = \varphi_j|_{F_i}(\alpha) = \varphi_i(\alpha)$$

Ejercicio. φ' es homomorfismo.

Además $(F', \varphi') \in \Sigma'$ y $(F_i, \varphi_i) \leq (F', \varphi')$. Por lo tanto Σ' tiene elemento maximal $(\bar{F}, \bar{\varphi})$.

Por demostrar que $\bar{F} = E$.

Supongamos que existe $\alpha \in E$, con $\alpha \notin \bar{F}$. α es algebraico sobre \bar{F} . Se sigue que $\bar{F}[\alpha]$ es merojo, $\bar{F}[\alpha] \neq \bar{F}$.

Debemos demostrar que existe extensión $\hat{\varphi}: \bar{F}[\alpha] \rightarrow \Omega_2$ de $\bar{\varphi}: \bar{F} \rightarrow \Omega_2$.

Para esto definimos

$$\hat{\varphi}: \bar{F}[x] \rightarrow \Omega_2[x]$$

$$\hat{\varphi}(a_n x^n + \dots + a_0) = \bar{\varphi}(a_n) x^n + \dots + \bar{\varphi}(a_0)$$

y consideramos $m_{\bar{F}, \alpha}(x) = m_\alpha(x)$ (polinomio irreducible de α en \bar{F}).

$m_\alpha(x) \in \bar{F}[x]$. Si $n(x) = \hat{\varphi}(m_\alpha(x)) \in \Omega_2[x]$, entonces existe $\beta \in \Omega_2$ con $n(\beta) = 0$.

Ahora definimos la evaluación en β :

$$\psi_\beta: \Omega_2[x] \rightarrow \Omega_2$$

$$f(x) \mapsto f(\beta)$$

donde $\bar{F}[x] \xrightarrow{\hat{\varphi}} \Omega_2[x] \xrightarrow{\psi_\beta} \Omega_2$. Resulta de lo anterior

$\lambda = \psi_\beta \circ \hat{\varphi}: \bar{F}[x] \rightarrow \Omega_2$, donde $\lambda(m_\alpha(x)) = \psi_\beta(n(x)) = 0$. Ahora existe

$$\bar{\lambda}: \frac{\bar{F}[x]}{(m_\alpha(x))} \longrightarrow \Omega_2$$

$$\bar{\lambda}(\bar{f}(x)) = \lambda(f(x))$$

Por teorema de isomorfía,

$$\frac{\bar{F}[x]}{(m_\alpha(x))} \cong \bar{F}[\alpha]$$

Por lo tanto existe $\bar{\varphi}: \bar{F}[x] \rightarrow \bar{\Omega}_2$ que extiende a $\bar{\varphi}$. Se concluye que $\bar{F} = E$.

Corolario. F campo, Ω_1, Ω_2 clausuras algebraicas. Entonces $\Omega_2 \cong \Omega_1$.

Observación. Ω_2 clausura algebraica de F : (i) Ω_2 algebraicamente cerrado
(ii) Ω_2/F algebraica.

Sean

$$\varphi_1: F \hookrightarrow \Omega_1, \quad \bar{\varphi}_1: \bar{\Omega}_2 \rightarrow \Omega_1.$$

$$\varphi_2: F \hookrightarrow \Omega_2, \quad \bar{\varphi}_2: \bar{\Omega}_2 \rightarrow \Omega_2$$

$\bar{\varphi}_2$ injectivo por ser homomorfismo de cuerpos. Sea $\Omega'_1 = \bar{\varphi}_2(\Omega_2)$, $\Omega'_1 \cong \Omega_2$.

Observación. Ω'_1 algebraicamente cerrado. Ω'_1/F algebraica. $\Omega'_1 \subseteq \Omega_2$, $\alpha \in \Omega_2$.

Debemos demostrar que $\alpha \in \Omega'_1$. $\alpha \in \Omega_2$ entonces α/F algebraico, lo que implica α/Ω'_1 algebraico. Luego $\alpha \in \Omega'_1$.

Así $\Omega'_1 = \Omega_2$. ■

Nota. $\bar{\mathbb{F}}_p = \bigcup_{t=1}^{\infty} \mathbb{F}_{p^t}$. $\mathbb{F}_q \cong \mathbb{Z}^{[i]} / 3\mathbb{Z}^{[i]}$.

Ejemplo. (1) $\overline{\mathbb{R}} = \mathbb{C}$

(2) $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Es más, $\overline{\mathbb{Q}}$ es numerable

(3) $\overline{\mathbb{C}((t))} \cong \bigcup_{n=1}^{\infty} \mathbb{C}(t^n)$

Extensiones separables.

Sea F campo, $F \subseteq E$, α/E algebraico. Además $m_\alpha(x)$ polinomio irreducible de α .

Definición. α se dice separable sobre F si $m_\alpha(x)$ tiene raíces distintas en \bar{F} .

$$m_\alpha(x) = \prod_{i=1}^n (x - \alpha_i)$$

Observación. L/K algebraica, entonces $\bar{L} = \bar{K}$.

Ejemplo. (1) $x^2 - t^2$ es irreducible en $\mathbb{F}_2(t^2)$ ($x^2 - u$ irreducible en $\mathbb{F}_2(u)$).
En $\overline{\mathbb{F}_2(t^2)} = \overline{\mathbb{F}_2(t)}$, $x^2 - t^2 = (x-t)^2$ (tiene raíces iguales).

Lema. Si $\alpha_1, \dots, \alpha_n$ son algebraicos sobre F , entonces $F(\alpha_1, \dots, \alpha_n)$ es algebraico sobre F .

Idea:

$$\begin{array}{c} F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \\ | \quad \swarrow \\ F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) \\ | \quad \swarrow \\ F(\alpha_1) \\ | \quad \swarrow \\ F \end{array}$$

Corolario. Si $F \subset E$ son cuerpos, los elementos de E que son algebraicos sobre F forman un cuerpo.

Proposición. Sea $F(\alpha_1, \dots, \alpha_n)/F$ una extensión algebraica. Las siguientes afirmaciones son equivalentes:

- (1) Cada $\beta \in F(\alpha_1, \dots, \alpha_n)$ es separable sobre F .
- (2) $\alpha_1, \dots, \alpha_n$ son separables sobre F .
- (3) Existen $N = [F(\alpha_1, \dots, \alpha_n) : F]$ homomorfismos $\varphi: F(\alpha_1, \dots, \alpha_n) \rightarrow \bar{F}$ con $\varphi|_F = \text{id}_F$.

(4) Para cada homomorfismo $\psi: F \rightarrow \bar{\Delta}_2$ con $\bar{\Delta}_2$ algebraicamente cerrado, existen N homomorfismos $\psi_1, \dots, \psi_N: F(\alpha_1, \dots, \alpha_n) \rightarrow \bar{\Delta}_2$ que extienden ψ .

En cualquiera de estos casos se dice que $F(\alpha_1, \dots, \alpha_n)$ es separable sobre F .
Más generalmente, se dice que E/F es separable si cada $\beta \in E$ es separable sobre F .

- Demarcación - (2) \Rightarrow (1), (4) \Rightarrow (3) evidentes.

(1) \Rightarrow (4)

$$F(\alpha_1, \dots, \alpha_r)$$

$$\begin{array}{c} | \\ \vdots \\ n_3 | \\ F(\alpha_1, \alpha_2) \quad ; \quad n = n_1 n_2 \dots n_r \\ | \\ n_2 | \\ F(\alpha_1) \\ | \\ n_1 \\ F \end{array}$$

Basta ver que ψ se puede extender de n , maneras a $F(\alpha_1)$, pues α_2 es separable sobre $K(\alpha_1)$, etc.

Lema. Si α es separable sobre K y $L \supseteq K$, entonces α es separable sobre L .

- Demarcación - $ir_{K,\alpha}(x)$ tiene raíces distintas, $ir_{K,\alpha}(x) \in L[x]$. Luego $ir_{L,\alpha}(x) \mid ir_{K,\alpha}(x)$, donde $\ker \varphi_\alpha = (ir_{K,\alpha}(x))$. Si $ir_{K,\alpha}$ tiene raíces distintas, también las tiene $ir_{L,\alpha}$.

Ahora procedemos a demostrar la proposición anterior.

Sea $\Psi: K \rightarrow \Omega$ homomorfismo, $m(x) = ir_{K,\alpha}(x)$, $d = \deg m$.

$$\bar{\Psi}(m)(x) \in \bigcap_{i=1}^d [x]$$

$$\bar{\Psi}(m)(x) = \prod_{i=1}^d (x - \beta_i)$$

Si $m(x)$ tiene raíces distintas en \overline{K} , $\bar{\Psi}(m)(x)$ tiene raíces distintas en Ω . (Pues $\overline{K} \hookrightarrow \Omega$).

Sea $\tilde{\Psi}_i: K[x] \rightarrow \Omega$ el homomorfismo definido por $\tilde{\Psi}_i(f(x)) = \bar{\Psi}(f)(\beta_i)$, donde $\tilde{\Psi}_i(m(x)) = \bar{\Psi}(m)(\beta_i) = 0$. Luego existe $\Psi_i: K[\alpha] \rightarrow \Omega$ con

$$\Psi_i|_K = \Psi, \quad \Psi_i(\alpha_i) = \beta_i.$$

luego ψ_1, \dots, ψ_d son extensiones distintas de K a $K[\alpha_1]$.

$$d = [K[\alpha_1] : K] = n_1. \quad (K=F), \text{ arreglar después} \\ (n=r)$$

Observación. El número de extensiones es siempre menor o igual al grado de la extensión.

Sea $\beta \in L$, $K \subseteq K[\beta] \subseteq L$

$$\begin{array}{c} L \\ | \\ s \\ | \\ K[\beta] \\ | \\ m \\ | \\ K \end{array} \quad n = sm$$

Hay $s \leq s$ extensiones de cualquier homomorfismo $\lambda: K[\beta] \rightarrow \bar{K}$ a L .

Hay $m' \leq m$ extensiones de la identidad a $K[\beta]$, $\psi_1, \dots, \psi_{m'}$.

El número total de extensiones es $ms = n = \sum_{i=1}^m s_{\psi_i} \leq m'$'s. Por lo tanto $m' = m$.

$g(x) = \text{irr}_{K[\beta]}(x)$, $\deg g = m$, $g(x) = \prod_{i=1}^m (x - \beta_i)$; β_1, \dots, β_m tiene que ser distintas para que tengamos m extensiones distintas.

Por lo tanto f es separable sobre K .

Observación. Si $f(x)$ tiene raíz doble, esta es raíz de su derivada.

$$(f \text{ con raíz doble} \Rightarrow f(x) = (x-\alpha)^2 g(x))$$

Proposición. Sea $f(x) \in K[x]$ un polinomio irreducible. Entonces f tiene raíces distintas en \bar{K} ssi $f'(x) = 0$.

- Demarcación - Si f tiene una raíz repetida, entonces a es raíz de f'

luego, como f es irreducible, $f = \text{irr}_{K[x]}$

Luego $f \mid f'$. Por lo tanto $f' = 0$.

Ahora supongamos que $f'(x) = 0$,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$f'(x) = a_n n x^{n-1} + \dots + a_1$$

se sigue que $i a_i = 0$, para todo i .

Es decir, $a_i = 0$, si la característica no divide a i .

Si la característica es 0, f es constante.

Si $\text{char } k = p$,

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$$

En \bar{K} , $a_{rp} = b_r^p$, $b_r \in \bar{K}$.

$$f(x) = b_0^p + b_1^p x^p + b_2^p x^{2p} + \dots$$

$$= (b_0 + b_1 x + b_2 x^2 + \dots)^p$$

Por lo tanto, la multiplicidad de cada raíz es divisible por p .

Definición. Un cuerpo K se dice perfecto si todo polinomio irreducible en $K[X]$ tiene raíces distintas.

Proposición. Todo cuerpo de característica 0 es perfecto.

Proposición. Si $\text{char } k = p$, entonces K es perfecto si $K = K^p$
($K^p = \{a^p / a \in K\}$).

- Democión - Si $K = K^p$ y $f(x) \in K[X]$ irreducible con raíces repetidas,

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$$

$$a_{ip} = b_i^p, b_i \in K,$$

$$f(x) = (b_0 + b_1 x + b_2 x^2 + \dots)^p$$

no es irreducible ($\Rightarrow \Leftarrow$).

Si $K \neq K^p$, existe $a \in K$ con $a \notin K^p$, y sea $b \in \bar{K}$ una raíz de $x^p - a = 0$, $m(x) = m_{k,b}(x)$ implica $m(x) | x^p - a$. En \bar{K} , $x^p - a = x^p - b^p - (x - b)^p$. Luego $m(x)$ tiene una sola raíz en \bar{K} . Como $b \notin K$, $\deg m > 1$, luego m tiene raíces repetidas. Se concluye que K no es perfecto.

Observación. Como m tiene raíces repetidas y es irreducible, $p \nmid \deg m$. Implica que $m(x) = x^p - a$.

Corolario. Todo cuerpo finito es perfecto.

-Demostración- $\varphi: K \rightarrow K$ frobenius. $\ker \varphi = \langle 0 \rangle$. Por lo tanto φ es epiyectivo (K es finito). Por lo tanto $K^p = K$.

Ejemplo. $\mathbb{F}_p(t)^p = \mathbb{F}_p(t^p)$. Luego $\mathbb{F}_p(t)$ no es perfecto.

$m_{\mathbb{F}_p(t^p), t}(x) = x^p - t^p$ es irreducible en $\mathbb{F}_p(t^p)[x]$.

$$[\mathbb{F}_p(t) : \mathbb{F}_p(t^p)] = p.$$

Miscelánea

[1] Dado un cuerpo F de característica $p > 0$, $F(x)$ no es perfecto.

Basta demostrar que $\varphi: F(x) \rightarrow F(x)$, $\varphi\left(\frac{f(x)}{g(x)}\right) = \left(\frac{f(x)}{g(x)}\right)^p$ no es epiyectiva.

Una forma es suponer que existen $f(x), g(x)$ tales que $x = \left(\frac{f(x)}{g(x)}\right)^p$ con $\text{mcd}(f(x), g(x)) = 1$, donde $g(x)$ puede ser unidad. Luego $g(x)^p x = f(x)^p$, entonces $g(x) | f(x)$ ($\Rightarrow \Leftarrow$)

Otra forma es suponer que existen $f(x), g(x)$ tales que $x g(x)^p = f(x)^p$. Derivando ambos lados nos queda que $g(x)^p = 0$. Luego $g(x) = 0$ ($\Leftarrow \Rightarrow$).

[2] $d \mid m \Leftrightarrow x^d \mid x^n - 1$.

-Demostración- (\Rightarrow) Evidente

(\Leftarrow) Desarrollando algoritmo de la división tenemos $n = dq + r$. Debemos demostrar que $r=0$.

[3] K es algebraico sobre F si para todo subanillo $E \subseteq K$ tal que $F \subseteq E$, E es cuerpo.

-Demostración- Sea $F \subseteq R \subseteq K$. R es comunitativo y no tiene divisores de cero. (además tiene unidad). Tomemos $\alpha \in R \setminus F$, $\alpha \in K$. Como K/F algebraica, existe $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Sea $p(x) = m_{\alpha, F}(x)$. Además

$$p(\alpha) = \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_1 \alpha + b_0 = 0$$

donde $b_i \in F \setminus \{0\}$. Al sacar lo anterior, existe $a \in F$ tal que $a_0 b_0 = 1$. A continuación:

$$a_0 p(\alpha) = a_0 \alpha^n + a_0 b_{n-1} \alpha^{n-1} + \dots + a_0 b_1 \alpha + a_0 b_0 = 0$$

$$\Rightarrow 1 = \alpha \underbrace{\left(-a_0 \alpha^{n-1} - \dots - a_0 b_1 \right)}_{\in R}$$

Observación. Notar que $\mathbb{Q}(\sqrt[3]{2}) \cong \frac{\mathbb{Q}[x]}{(x^3 - 2)} = \langle 1, \bar{x}, \bar{x}^2 \rangle$. La demostración anterior es útil para encontrar un inverso de $1 + \sqrt[3]{2}$ como combinación lineal de $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$.

(\Leftarrow) Sea $\alpha \in K \setminus F$. Podemos construir $F[\alpha] = \{f(\alpha) / f(x) \in F[x]\}$.

Como $F[x]$ es anillo, por hipótesis, $F[\alpha] = F(\alpha)$ es círculo.

Como $\alpha^{-1} \in F(\alpha)$, existe $p(x) \in F[x]$ tal que $\alpha^{-1} = p(\alpha)$. Por lo tanto $p(\alpha) \neq 0$. Extendiendo lo anterior nos queda

$$p(\alpha) = b_n \alpha^n + \dots + b_1 \alpha + b_0 = \alpha^{-1}$$

$$\alpha p(\alpha) = b_n \alpha^{n+1} + \dots + b_1 \alpha^2 + b_0 \alpha = 1$$

$$\Rightarrow \alpha p(\alpha) - 1 = b_n \alpha^{n+1} + \dots + b_1 \alpha^2 + b_0 \alpha$$

Luego tenemos el polinomio $x p(x) - 1$. Por lo tanto α es algebraico sobre F .

Extensiones normales

Definición. Una extensión algebraica L/K se dice normal si cada polinomio irreducible en $K[x]$ que tenga una raíz en L , se factoriza completamente en $L[x]$.

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

Ejemplo. $K = \mathbb{F}_2(t)$, $L = \mathbb{F}_2(t)$. $a \in L$ implica $a = \frac{f(t)}{g(t)}$.

$$f \in \mathbb{F}_2[x]: \quad f(x) = x^{r_1} + x^{r_2} + \dots + x^t$$

$$\text{Se cumple } f(x)^2 = f(x^2)$$

Ejercicio. $g(x) \in \mathbb{F}_p[x] \Rightarrow g(x)^p = g(x^p)$

Por otro lado, $a^2 = \left(\frac{f(t)}{g(t)}\right)^2 = \frac{f(t^2)}{g(t^2)} \in K$. Podemos tomar $a \in L$, $\text{irr}_{K,a}(x) = x^2 - a^2$.

En $L[x]$, $x^2 - a^2 = (x - a)^2$. Por lo tanto L/K es normal.

Ejemplo. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$. Tomando $a \in L$, $a = c + d\sqrt{2}$, $c, d \in \mathbb{Q}$.
a satisface el polinomio $x^2 - 2cx + (c^2 - 2d^2) = 0$, donde su otra raíz es $c - d\sqrt{2}$. Por lo tanto es una extensión normal.

Ejemplo. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$. L/K no es una extensión normal.
(Estudiar las raíces de $\text{irr}_{K,a}(x)$, donde $a = \sqrt[3]{2}$).

Proposición. Sea $L = k[\alpha_1, \dots, \alpha_r]/k$ extensión algebraica. Las siguientes afirmaciones son equivalentes:

(1) L/k es normal

(2) Para $i=1, \dots, r$, L contiene todas las raíces de $\text{irr}_{k,\alpha_i}(x)$

(3) Para todo homomorfismo $\varphi: L \rightarrow \bar{k}$ tal que $\varphi|_k = \text{id}$, se tiene $\varphi(L) = L$.

-Demostración- (1) \Rightarrow (2) (trivial)

(2) \Rightarrow (3) : Sea $\varphi: L \rightarrow \bar{K}$ un homomorfismo con $\varphi|_K = id$.

$$\varphi(K[\alpha_1, \dots, \alpha_r]) = K[\varphi(\alpha_1), \dots, \varphi(\alpha_r)]$$

Basta probar que $\varphi(\alpha_i) \in L$. Para ello, tomando $m_i(x) = \text{irr}_{K, \alpha_i}(x)$

$$0 = \varphi(0) = \varphi(m_i(\alpha_i)) = m_i(\varphi(\alpha_i))$$

Luego $\varphi(\alpha_i)$ es raíz de m_i , luego $\varphi(\alpha_i) \in L$.

(3) \Rightarrow (1) : Sea $\beta \in L$, y sea β' otra raíz de $\text{irr}_{K, \beta}(x) = m(x)$. Tenemos

$$K[\beta] \cong \frac{K[x]}{(m(x))} \cong K[\beta']$$

Luego existe homomorfismo $\psi: K[\beta] \rightarrow K[\beta']$, $\psi(\beta) = \beta'$.

$$K[\beta] \subseteq L$$

Existe $\tilde{\psi}: L \rightarrow \bar{K}$ que extiende ψ , $\tilde{\psi}(\beta) = \beta'$.

$$\tilde{\psi}(L) \subseteq L \Rightarrow \beta' \in L$$

Luego como β, β' eran arbitrarias, L es normal.

Ejemplo. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Raíces de $\text{irr}_{\mathbb{Q}, \sqrt[3]{2}}(x)$ son $\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \in L$. Raíces de $\text{irr}_{\mathbb{Q}, \omega}(x)$ son $\omega, \omega^2 \in L$.

$$\text{irr}_{\mathbb{Q}, \omega}(x) = x^2 + x + 1 = \frac{x^3 - 1}{x - 1}$$

Definición (Extensión Galoiana) Una extensión algebraica L/K se dice Galoiana si es normal y separable. Suponiendo que L/K es finita, $n = [L:K]$ (siempre es el caso)

Observación. (i) Separable : Existen n homomorfismos $\varphi: L \rightarrow \bar{K}$, $\varphi|_K = id$.
(ii) Normal : Para todos ellos, $\varphi(L) = L$.

Definición. $\text{Gal}(L/K) = \{\sigma : L \rightarrow L \text{ automorfismo} / \sigma|_K = \text{id}\}$ (Grupo de Galois)

Corolario. $|\text{Gal}(L/K)| = n$ si L/K es Galoiana.

Paréntesis: Grado de una extensión de cuerpos de funciones.

Sea F cuerpo, $L = F(t)$, $K = F(h)$, $h \in L$. L/K extensión algebraica.

Si $h(t) = \frac{f(t)}{g(t)}$, entonces $f(t) - h(t)g(t) = 0$. Luego x es raíz de

$$F(x, h) = f(x) - hg(x)$$

$$\deg_x F(x, h) = \max\{\deg f, \deg g\}$$

Supongamos que f y g son relativamente primos.

Observación. (1) $f(x) - hg(x)$ es irreducible en $K(x)[h]$ (es de grado 1).

(2) $f(x) - hg(x)$ es irreducible en $K[x][h]$ (es irreducible en $K(x)[h]$ y primitivo)

(3) $f(x) - hg(x)$ es irreducible en $K(h)[x]$ (Lema de Gauss)

Por lo tanto, $[L : K] = \max\{\deg f(x), \deg g(x)\}$

Ejemplo. $h(x) = \frac{3x^2 - 1}{2x^3 + 1}$, $F = \mathbb{C}$. $[L : k] = 3$

Sea L un cuerpo y G un grupo que actúa fielmente por automorfismos en L .

$$\alpha \in G, \quad u \mapsto \alpha \cdot u$$

automorfismo

Si $\beta \in G$ satisface $u = \beta \cdot u$ para todo $u \in L$, entonces $\beta = e_G$.

Si $u \in L$, la órbita de u es

$$\Omega(u) = \{\alpha(u) / \alpha \in G\}$$

Polinomio primitivo:

Aquel que sus coeficientes son relativamente primos.

$$K = L^G = \{ u \in L \mid \alpha(u) = u \quad \forall \alpha \in G \}$$

Ejercicio. L^G es un cuerpo. $G \curvearrowright L \Rightarrow L^G \subseteq L$ cuerpo
 G finito $\Rightarrow L/L^G$ algebraica

Sea L/K extensión. Si G es finito, L/K es algebraica, $a \in L$. Sea

$$f(x) = \prod_{b \in \theta(a)} (x-b)$$

Sea $\alpha \in G$.

Observación. G actúa en $L[x]$ (actuando en los coeficientes) y con esta acción

$$L[x]^G = K[x]$$

Por otro lado, $\alpha(f(x)) = f(x)$ (ejercicio). Por lo tanto, $f(x) \in K[x]$.

Proposición. Si $a \in L$, entonces

$$\text{irr}_{L^G, a}(x) = \prod_{b \in \theta(a)} (x-b) \quad (\text{en } L[x])$$

Demonstración. Supongamos $f(x) = g(x)h(x)$, $\theta(a) = T \cup S$.

$$g(x) = \prod_{b \in T} (x-b), \quad h(x) = \prod_{b \in S} (x-b)$$

Supongamos que $T \neq \emptyset, S \neq \emptyset$. Para ello, $d \in T, c \in S$.

Existe $\alpha \in G$ con $\alpha(d) = c$

$$m(x) = \text{irr}_{K,d}(x)$$

$$\alpha(m(x)) = \text{irr}_{K,c}(x)$$

\Downarrow
 $m(x)$

$g(d) = 0$. Luego $m \mid g$. Además $h(c) = 0$. Luego $m \mid h$.

Por lo tanto $m^2 \mid f$, pero f tiene raíces distintas ($\Rightarrow \Leftarrow$)

f es irreducible.

Corolario. L/L_G es Galoiana.

Observación. $G \subseteq \text{Gal}(L/L_G)$.

Ejemplo. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $a \in L$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \downarrow \quad \downarrow \\ \mathbb{Q}(\sqrt{2}) \quad | \quad \mathbb{Q}(\sqrt{3}) \\ \downarrow \quad \downarrow \\ \mathbb{Q} \end{array}$$

$a = b + c\sqrt{3}$, $b, c \in \mathbb{Q}(\sqrt{2})$. Existe $\sigma: L \rightarrow L$ con

$$\sigma(\sqrt{3}) = -\sqrt{3}$$

$$\sigma(\sqrt{2}) = -\sqrt{2}$$

Existe $\tau: L \rightarrow L$, $\tau(\sqrt{3}) = \sqrt{3}$

$$\tau(\sqrt{2}) = -\sqrt{2}$$

$G = \{\sigma, \tau, \sigma\tau, \text{id}\}$, $\sigma\tau = \tau\sigma$ (grupo de Klein)

Tomando $a = \sqrt{2} + \sqrt{3}$, nos queda

$$\theta(a) = \{\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}\}$$

Por lo tanto, $irreducible(x) = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$.

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4.$$

Proposición. Si K es un cuerpo infinito y $f \in K[x_1, \dots, x_n]$ es un polinomio no nulo, entonces existe $(a_1, \dots, a_n) \in K^n$ con $f(a_1, \dots, a_n) \neq 0$.

-Demostración- Si $n=1$, f tiene un número finito de raíces. Supongamos que es cierto para $n=k$. $m=k+1$ tenemos

$$f(x_1, \dots, x_k, x_{k+1}) = \sum_{i=0}^N g_i(x_1, \dots, x_k) x_{k+1}^i ; \quad g_N \neq 0$$

$g_N \in K[x_1, \dots, x_k]$. Por hipótesis de inducción, existe $(a_1, \dots, a_k) \in K^k$ con $g_N(a_1, \dots, a_k) \neq 0$.

$$\tilde{f}(x_{k+1}) = f(a_1, \dots, a_k, x_{k+1}) = \sum_{i=0}^N g_i(a_1, \dots, a_k) x_{k+1}^i$$

Luego existe $a_{k+1} \in K$ tal que $\tilde{f}(a_{k+1}) \neq 0$. Por lo tanto $f(a_1, \dots, a_{k+1}) \neq 0$.

Corolario. Si K es un cuerpo infinito, V espacio vectorial dimensión finita sobre K y $V = V_1 \cup V_2 \cup \dots \cup V_N$ con V_i subespacio, entonces $V = V_j$ para algún j . (Suponemos $V = K^n$)

- Demonstración - Sea $n = \dim_K V$ y supongamos que no se cumple. Sin pérdida de generalidad, suponemos $\dim V_i = n-1$

$$V_i = \{(a_1, \dots, a_n) \in K^n / l_i(a_1, \dots, a_n) = 0\}$$

$$\text{Sea } f(x_1, \dots, x_n) = \prod_{i=1}^n l_i(x_1, \dots, x_n)$$

$$(a_1, \dots, a_n) \in V_1 \cup \dots \cup V_N \Leftrightarrow f(a_1, \dots, a_n) = 0$$

Por lo tanto existe $(a_1, \dots, a_n) \notin V_1 \cup \dots \cup V_N$.

Observación. $l_i : V \rightarrow K$ lineal (polinomio en n variables).

$$l_i = b_1 x_1 + \dots + b_n x_n.$$

Teorema (Primer teorema fundamental de la Teoría de Galois).

Sea L un cuerpo, G un grupo finito que actúa por automorfismos de L .

Sea $K = L^G$. Entonces:

(1) L/K es una extensión Galoiana finita.

(2) $\text{Gal}(L/K) \cong G$.

-Demostración- L/K es Galoiana.

Sean $\varphi: L \rightarrow L$ un automorfismo, $a \in L$ ($\varphi|_K = id$).

$$m(x) = \inf_{k,a}(x) \implies m(\varphi(a)) = 0$$

Se tiene que $m(x) = \inf_{b \in \vartheta(a)} (x-b)$. $\varphi(a) \in \vartheta(a)$. Por lo tanto $\varphi(a) = \sigma(a)$, $\sigma \in G$.

Sea $W \subseteq L$ un K -espacio vectorial de dimensión finita. Para $\sigma \in G$,

$$W_\sigma = \{w \in W / \varphi(w) = \sigma(w)\}$$

Tenemos $W_\sigma \leq W$ y $W = \bigcup_{\sigma \in G} W_\sigma$. Luego $W = W_\sigma$ para algún $\sigma \in G$.

Sea $L_\sigma = \{\lambda \in L / \varphi(\lambda) = \sigma(\lambda)\}$. Si $L_\sigma \neq L$, escogemos $x \in L$, $x \notin L_\sigma$. Si $L_\sigma \neq L$ para todo σ , tengo x_σ definido para cada $\sigma \in G$ y podemos tomar

$$W = \langle x_\sigma / \sigma \in G \rangle \text{ (dimensión finita)}$$

$x_\sigma \notin W_\sigma$ para todo $\sigma \in G$. Por lo tanto, existe $\sigma \in G$ con $L = L_\sigma$ ($\varphi = \sigma$).

Falta demostrar que $G = \text{Gal}(L/K)$. En particular tiene r elementos.

Sea F/K una extensión Galoiana finita, con $F \subseteq L$. Definiendo

$$M = |\text{Gal}(F/K)| = [F : K]$$

Cada automorfismo $\varphi \in \text{Gal}(F/K)$ se extiende a un homomorfismo $\tilde{\varphi}: L \rightarrow \overline{K}$, de hecho $\tilde{\varphi} \in \text{Gal}(L/K)$.

$$[F : K] \leq |\text{Gal}(L/K)| = |G|$$

Observación: Si $E = K[a_1, \dots, a_n]$ es extensión finita separable, entonces $\tilde{E} = K[b_1, \dots, b_r]$, donde b_1, \dots, b_r son todas las raíces de $\inf_{K, a_i}(x)$ ($i \in \{1, \dots, n\}$) es Galoiana sobre K .

Ejemplo: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es Galoiana. $\mathbb{Q}(\sqrt[3]{2}, \omega^3\sqrt[3]{2}, \omega^2\sqrt[3]{2})/\mathbb{Q}$ es Galoiana.

Observación. Una extensión Galoiana infinita tiene subextensión Galoiana de grado arbitrariamente grande. Luego L/K es finita y $[L:K] = |G|$. Se concluye $\text{Gal}(L/K) = G$.

Ejemplo. $L = F(x_1, \dots, x_n)$. S_n actúa sobre L permutando las variables:

$$(1234) \left(\frac{x_1+x_3}{x_2+x_5} \right) = \frac{x_2+x_4}{x_3+x_5}$$

$$\text{Sea } K = L^{S_n}. \varphi(t) = \prod_{i=1}^n (t-x_i) \in K[t]. \varphi(t) = \text{irr}_{K, x_1}(t)$$

$= \text{irr}_{K, x_2}(t) = \dots$ (misma órbita, mismo polinomio irreducible ...)

$$\varphi(t) = t^n - \sigma_1(x_1, \dots, x_n)t^{n-1} + \sigma_2(x_1, \dots, x_n)t^{n-2} + \dots \pm \sigma_n(x_1, \dots, x_n)$$

$$\begin{aligned} \sigma_1(x_1, \dots, x_n) &= x_1 + \dots + x_n && \text{(funciones simétricas)} \\ \sigma_2(x_1, \dots, x_n) &= x_1 x_2 + \dots + x_{n-1} x_n && \text{(elementales)} \end{aligned}$$

$$\sigma_m(x_1, \dots, x_n) = x_1 x_2 \dots x_n$$

Sea $K' = F(\sigma_1, \dots, \sigma_n)$; $K' \subseteq K$

$$[L:K] = |S_n| = n!$$

$$\text{irr}_{K', x_1} = \varphi(t)$$

Como $L = K'[x_1, \dots, x_n]$ (x_i raíces de φ y $\deg \varphi = n$)

$$[L:K'] \leq n! \quad (*)$$

Por lo tanto $K' = K$. Luego toda función racional simétrica en x_1, \dots, x_n , es una función racional de $\sigma_1, \dots, \sigma_n$.

Ejemplo. ($n=3$)

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{\sigma_2}{\sigma_3}$$

$$x_1^2 + x_2^2 + x_3^2 = \sigma_1^2 - 2\sigma_2$$

Proposición. Si $\alpha_1, \dots, \alpha_n$ son las raíces en \bar{K} de $f(x) = 0$, con $\deg f = m$, entonces $[K(\alpha_1, \dots, \alpha_n) : K] \leq m!$.

- Demonstración - Tenemos que $[K(\alpha_1) : K] \leq m$, $f(x) = (x - \alpha_1)^t g(x)$ en $K(\alpha_1)$, $\deg g \leq m-1$. $\alpha_2, \dots, \alpha_n$ son las raíces de g , luego

$$[K(\alpha_1, \dots, \alpha_n) : K(\alpha_1)] \leq (m-1)!$$

$$\begin{array}{c} K(\alpha_1, \dots, \alpha_n) \\ | \quad \leq (m-1)! \\ K(\alpha_1) \quad | \quad \leq m! \\ | \quad \leq m \\ K \end{array}$$

Ejemplo. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$; $\sigma, \tau : L \rightarrow L$ tales que

$$\begin{array}{ll} \sigma(\sqrt{2}) = \sqrt{2} & \tau(\sqrt{2}) = -\sqrt{2} \\ \sigma(\sqrt{3}) = -\sqrt{3} & \tau(\sqrt{3}) = \sqrt{3} \end{array}$$

Tenemos $G = \langle \sigma, \tau \rangle \cong C_2 \times C_2$; $\text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$. $[L : L^G] = 4$ y con ello $L^G = \mathbb{Q}$. $\lambda \in L$ es racional si $\sigma(\lambda) = \lambda$, $\tau(\lambda) = \lambda$.

$$\sigma \left(\underbrace{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}}_{=\lambda} \right) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$\tau \left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \right) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\sigma(\lambda) = \lambda \iff c = d = 0$$

$$\tau(\lambda) = \lambda \iff b = d = 0$$

Ejemplo. $\beta = e^{2\pi i/7}$, in $\mathbb{Q}, \beta(x) = \frac{x^7 - 1}{x + 1} = x^6 + x^5 + \dots + 1$. Tomando

$\sigma : L \rightarrow \bar{\mathbb{Q}}$, $\sigma_i(\beta) = \beta^i$ $i = 1, \dots, 6$ (se cumple, comprobar). Además $\sigma_i(L) = L$. Por lo tanto, L/\mathbb{Q} es Galoisiana. Por otro lado

$$\sigma_i(\sigma_j(\beta)) = \sigma_i(\beta^j) = \sigma_i(\beta)^j = (\beta^i)^j = \beta^{ij} = \sigma_{ij}(\beta)$$

$$\text{Entonces } \sigma_i \circ \sigma_j = \sigma_{ij}.$$

$\text{Gal}(\mathbb{L}/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^* = C_6$. Tomando $\tau: L \rightarrow L$, $\tau(p) = p^2$, $|\langle \tau \rangle| = 3$. ¿ $L^{<\tau>}$?

Observación. p, p^2, \dots, p^6 es base de L/\mathbb{Q} . Además

$$\tau(a + bp^2 + cp^3 + dp^4 + ep^5 + fp^6) = ap^2 + bp^4 + cp^6 + dp + ep^3 + fp^5$$

$$\lambda = \tau(1), \text{ entonces } a=d=b, c=e=f.$$

$$\lambda = a(p + p^2 + p^4) + c(p^3 + p^5 + p^6) \quad \left(\begin{array}{l} u = p + p^2 + p^4 \\ v = p^3 + p^5 + p^6 \end{array} \right)$$

Si $a=-1, c=-1$, entonces $\lambda=1$. Nos dará que $1=-u-v, v=-u-1$.

Obtenemos $[L : L^{<\tau>}]=3$, $[L : \mathbb{Q}]=6$, y con ello, $[L^{<\tau>} : \mathbb{Q}]=2$.

Por lo tanto $L^{<\tau>} = \mathbb{Q}(\sqrt{D})$

Objetivo: Encontrar D .

$$\text{Para ello, } L^{<\tau>} = \mathbb{Q}(p + p^2 + p^4) \cong \mathbb{Q}(p + p^2 + p^4, p^3 + p^5 + p^6) \\ (p + p^2 + p^4)^2 = p^2 + p^4 + p + 2(p^3 + p^5 + p^6)$$

Tomando $u = p + p^2 + p^4$; $u^2 = u + 2(-u-1)$. $u^2 + u + 2 = 0$. Las raíces son

$$u = \frac{-1 \pm \sqrt{-7}}{2}$$

$$D = -7.$$

Segundo teorema fundamental de la Teoría de Galois

Sea L/K una extensión galoisiana finita, entonces existe una correspondencia

$$\left\{ \begin{array}{l} \text{extensiones intermedias} \\ F \text{ con } K \subseteq F \subseteq L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgrupos de} \\ \text{Gal}(L/K) \end{array} \right\}$$

dada por $F \mapsto \text{Gal}(L/F)$, $H \mapsto L^H$. Es decir:

$$F = L^{\text{Gal}(L/F)}, H = \text{Gal}(L/L^H)$$

-Demostración-

$H = \text{Gal}(L/L^H)$ sigue del 1º teorema fundamental. Sea F campo con $K \subseteq F \subseteq L$.
Observación: L/F es galoisiana



$L = K(a_1, \dots, a_n)$, a_i tiene polinomio irreducible f_i sobre K . En particular $L = F(a_1, \dots, a_n)$. a_i tiene polinomio irreducible g_i sobre F . Por lo tanto $g_i | f_i$ en $F[x]$.

(i) f_i tiene raíces distintas $\Rightarrow g_i$ tiene raíces distintas

(ii) f_i tiene todas sus raíces en $L \Rightarrow g_i$ tiene todas sus raíces en L

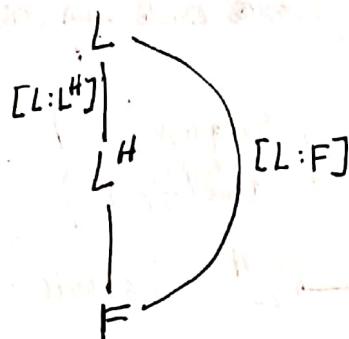
Por lo tanto L/F es galoisiana.

$$[L:F] = \text{Gal}(L/F), H := \text{Gal}(L/F).$$

Por otro lado, $H = \text{Gal}(L/L^H)$, en particular $[L:L^H] = |H|$.

Y no olvidar que $F \subseteq L^H$.

Ahora



Como $[L:L^H] = [L:F]$, $[L^H:F] = 1$ ($F = L^H$).

Proposición. Sea L/K Galoisiana. $K \subseteq F \subseteq L$, entonces F/k es Galoisiana (Normal) si y sólo si

$$\text{Gal}(L/F) \trianglelefteq \text{Gal}(L/k)$$

Lema. Si $K \subseteq F \subseteq L$, como arriba, entonces para todo $\sigma \in \text{Gal}(L/k)$

$$\sigma(F) = L^{\sigma \text{Gal}(L/F)\sigma^{-1}}$$

- Demonstración - Sea $H = \text{Gal}(L/F)$, $F = L^H$, $\sigma \in \text{Gal}(L/k)$.

$$l \in \sigma(F) \Rightarrow l = \sigma(m), m \in F,$$

Para $\tau \in \text{Gal}(L/F)$

$$(\tau \tau^{-1})(l) = (\tau \tau^{-1})(\sigma(m)) = \tau(\tau(m)) = \tau(m) = l$$

$$\therefore \sigma(F) \subseteq L^{\sigma H \sigma^{-1}} \quad \begin{matrix} F = K(\alpha_1, \dots, \alpha_n) \\ \sigma(F) = \sigma(K)(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \end{matrix}$$

$$[\sigma(F):k] = [\sigma(F):\sigma(K)] = [F:k]. \quad \text{Por lo tanto } = k(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

$$[L:\sigma(F)] = [L:F] = |H| = |\sigma H \sigma^{-1}|$$

$$[L:L^{\sigma H \sigma^{-1}}] = |\sigma H \sigma^{-1}|$$

$$\therefore \sigma(F) = L^{\sigma H \sigma^{-1}}$$

Observación. El lema es equivalente a $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.

- Demostración de la proposición -

F/K es normal si y sólo si para todo homomorfismo $\sigma: F \rightarrow \overline{K}$, se tiene $\sigma(F) = F$.

Para todo $\sigma: F \rightarrow \overline{K}$, y toda extensión $\tilde{\sigma}: L \rightarrow \overline{K}$, se tiene $\tilde{\sigma}(L) = L$.
Luego podemos suponer $\sigma \in \text{Gal}(L/K)$.

$$\begin{aligned} F/K \text{ normal} &\Leftrightarrow \sigma(F) = F \text{ para todo } \sigma \in \text{Gal}(L/K) \\ &\Leftrightarrow \text{Gal}(L/\sigma(F)) = \text{Gal}(L/F), \text{ para todo } \sigma \in \text{Gal}(L/K) \\ &\Leftrightarrow \sigma \text{Gal}(L/F)\sigma^{-1} = \text{Gal}(L/F), \forall \sigma \in \text{Gal}(L/K) \\ &\Leftrightarrow \text{Gal}(L/F) \triangleleft \text{Gal}(L/K). \end{aligned}$$

Observación $\text{Gal}(L/\sigma(F)) = \sigma \text{Gal}(L/F)\sigma^{-1}$

Proposición. En las notaciones anteriores, si F/K es normal

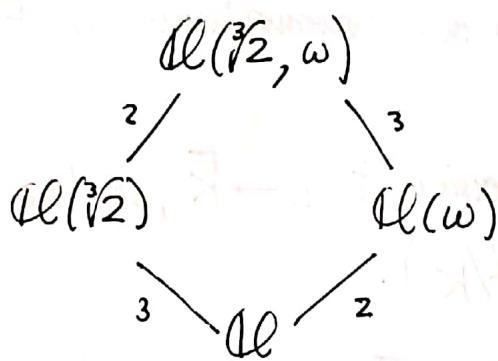
$$\text{Gal}(F/K) \cong \frac{\text{Gal}(L/K)}{\text{Gal}(L/F)}$$

- Demostración - Definimos $\varphi: \text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$, $\varphi(\sigma) = \sigma|_F$.
 $\sigma(F) = F$, $\sigma|_F \in \text{Gal}(F/K)$.

$$\begin{aligned} \sigma \in \ker \varphi &\Leftrightarrow \sigma|_F = \text{id}_F \Leftrightarrow \sigma \in \text{Gal}(L/F) \quad \text{Luego por teorema de isomorfía} \\ \text{Im } \varphi &\cong \frac{\text{Gal}(L/K)}{\text{Gal}(L/F)} \end{aligned}$$

φ es epiyectiva por el teorema de extensión de homomorfismos. \blacksquare

Ejemplo. $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $K = \mathbb{Q}$



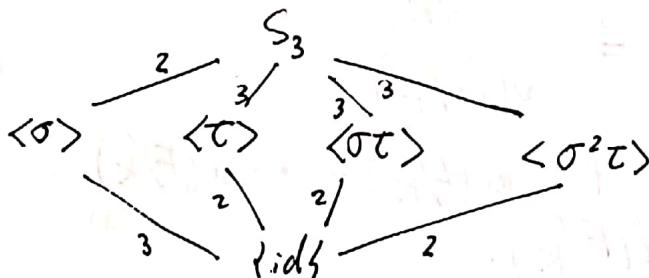
$$\omega^3 = 1, \omega \neq 1 \quad (\omega = e^{2\pi i/3})$$

$$H = \text{Gal}(L/\mathbb{Q}(\sqrt[3]{2})), N = \text{Gal}(L/\mathbb{Q}(\omega)), G = \text{Gal}(L/\mathbb{Q})$$

$N \trianglelefteq G$, $H \not\trianglelefteq G$. Tenemos que $|G| = 6$, luego tenemos dos opciones, $G \cong \mathbb{Z}_6$, $G \cong S_3$. Como $H \not\trianglelefteq G$, $G \cong S_3$.

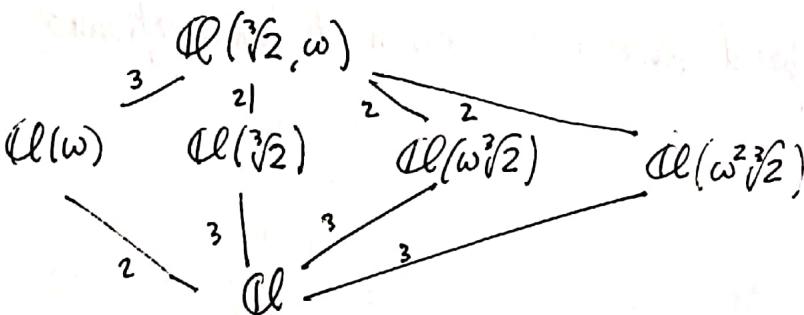
Recordar

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \sigma\tau = \tau\sigma^{-1} \rangle$$



$$(\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma\sigma^{-1}\tau\tau = \tau^2 = \text{id}, \quad \sigma(\tau)\sigma^{-1} = \sigma\tau\sigma^{-1} = \sigma^2\tau, \quad \sigma^2(\tau)\sigma^{-2} = \sigma\tau.$$

$$S_3 = \{ \text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$$



Ejemplo. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

$$|\downarrow$$
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = F$$

$$|\downarrow$$

$$\mathbb{Q}(\sqrt{2})$$

$$|\downarrow$$

$$\mathbb{Q} = K$$

Supongamos que $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$$\bar{\sigma}: \mathbb{Q}(\sqrt{5}) \rightarrow \mathbb{Q}(\sqrt{5})$$

$$\bar{\sigma}(\sqrt{5}) = -\sqrt{5}$$

Luego por el teorema de extensión de homomorfismos, existe $\sigma \in \text{Gal}(F/K)$ con $\sigma(\sqrt{5}) = -\sqrt{5}$. $\lambda, \tau \in \text{Gal}(F/K)$

$$\lambda(\sqrt{2}) = -\sqrt{2}, \quad \lambda(\sqrt{3}) = \sqrt{3}$$

$$\tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

$$\lambda(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\text{Si } \lambda(\sqrt{5}) = -\sqrt{5}$$

$$\sqrt{5} = b\sqrt{2} + d\sqrt{6}$$

$$5 = 2b^2 + 6d^2 + 2bd\sqrt{3}$$

$$\Rightarrow bd = 0 \Rightarrow b \neq 0 \text{ o } d = 0 \quad (\Leftrightarrow)$$

Lo mismo si $\tau(\sqrt{5}) = \sqrt{5}$, o si $\lambda \tau(\sqrt{5}) = -\sqrt{5}$. Por lo tanto $\sqrt{5} \notin F$.

$$\text{Luego } [L:K] = 8.$$

$$|\text{Gal}(\mathbb{Q}_K)| = 8$$



$$G \in \left\{ D_4^{\textcolor{red}{5}}, \mathbb{Q}_8^{\textcolor{red}{3}}, C_8, C_4 \times C_2^{\textcolor{red}{3}}, C_2 \times C_2 \times C_2 \right\}$$

Por lo tanto $\text{Gal}(\mathbb{Q}_K) \cong C_2 \times C_2 \times C_2 \cong \mathbb{F}_2^3$.

$$\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$$

$$\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$$

$$\sigma(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$$

$$\begin{aligned} \sigma: \quad & \sqrt{2} \mapsto -\sqrt{2} \\ & \sqrt{3} \mapsto \sqrt{3} \\ & \sqrt{5} \mapsto \sqrt{5} \end{aligned} \quad (\sqrt{2}, \sqrt{3}, \sqrt{5}) \mapsto (-\sqrt{2}, \sqrt{3}, \sqrt{5})$$

$$(-\sqrt{2}, -\sqrt{3}, \sqrt{5})$$

$$\begin{aligned} \tau: \quad & \sqrt{2} \mapsto \sqrt{2} \\ & \sqrt{3} \mapsto -\sqrt{3} \\ & \sqrt{5} \mapsto \sqrt{5} \end{aligned}$$

$$\begin{aligned} \rho: \quad & \sqrt{2} \mapsto \sqrt{2} \\ & \sqrt{3} \mapsto \sqrt{3} \\ & \sqrt{5} \mapsto -\sqrt{5} \end{aligned}$$

Misurámen

[1] $\overline{\mathbb{Q}}$ es numerable. Existe aplicación biyectiva $\bigcup_{n \in \mathbb{N}} \mathbb{Q}^n \rightarrow \overline{\mathbb{Q}}$.

$\overline{\mathbb{Q}}/\mathbb{Q}$ es extensión infinita, $x^n - p$ irreducible para todo p primo y todo $n \in \mathbb{N}$.

$[\mathbb{Q}(\alpha_n) : \mathbb{Q}] = n$, donde α_n raíz de $x^n - p$. $\mathbb{Q}(\alpha_n) \subseteq \overline{\mathbb{Q}}$ $\forall n$.

$\overline{\mathbb{Q}}$ tiene infinitos automorfismos, para todo p primo, existe $\varphi_p \in \text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ tal que $\varphi_p(\sqrt[p]{p}) = -\sqrt[p]{p}$. En $\overline{\mathbb{Q}}$ están todas las extensiones $\mathbb{Q}(\sqrt[p]{p})$.
 $\#\text{Aut}(\overline{\mathbb{Q}})$ es no numerable.

[2] $\text{Aut}(\mathbb{R}) = \{ \text{id} \}$

[3] Para encontrar el cuerpo de descomposición de $x^6 + x^3 + 1$, veamos que

$$x^3 - 1 = (x^3)^2 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$$

Las raíces de $x^6 + x^3 + 1$ están en $\{1, e^{\frac{2\pi i}{3}}, \dots, e^{\frac{2\pi i(3k)}{3}}\}$. Las raíces de $x^3 - 1$ son $\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$. Sea $\omega = e^{\frac{2\pi i}{3}}$

$$K = \mathbb{Q}(\omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^9)$$

Es claro que $K = \mathbb{Q}(\omega)$. Además $x^6 + x^3 + 1$ ssi $(x+1)^6 + (x+1)^3 + 1$ irreducibles ($\mathbb{Q}[x] \cong \mathbb{Q}[x+1]$). Por criterio de Eisenstein, $x^6 + x^3 + 1$ es irreducible.

$$\therefore [\mathbb{Q}(\omega) : \mathbb{Q}] = 6$$

Afirmación: $|\text{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})| = 6$

Busquemos automorfismos:

$$\text{Id}, \quad \varphi(\omega) = \omega^2 \dots \text{(Avanquean)}$$

$$\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_6$$

[4] Encuentra un solo de descomposición de $x^8 - 2$ (ver Dummit).

Dados $\lambda = \sqrt[8]{2}$, $\rho = e^{2\pi i/8}$, las raíces del polinomio son $\lambda\rho^j$, $0 \leq j \leq 7$.

Ejercicio. $[K:\mathbb{Q}] \geq 8$.

Tomando $\rho = e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$. $\mathbb{Q}(\rho) \subseteq \mathbb{Q}(\sqrt{2}, i)$, $\rho^2 = i$

$\rho + \rho^7 = \sqrt{2}$, $i, \sqrt{2} \in \mathbb{Q}(\rho)$. Se tiene que $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{2}, i)$

$K = \mathbb{Q}(\lambda, \rho) = \mathbb{Q}(\sqrt[8]{2}, \sqrt{2}, i) = \mathbb{Q}(\sqrt[8]{2}, i)$. $[K : \mathbb{Q}(\lambda)] = 2$, entonces $[K : \mathbb{Q}] = 16$. Por lo tanto $|\text{Gal}(K/\mathbb{Q})| = 16$.

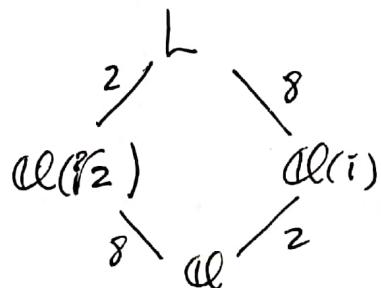
$\mathbb{Q}(\lambda)$ no es extensión Galoiana, implica que $\text{Gal}(K/\mathbb{Q})$ no es abeliano.

Afirmación. $\text{Gal}(K/\mathbb{Q}) = D_8$.

Miscelánea

[1] $L = \text{Cl}(\sqrt[8]{2}, \rho)$, $\rho = \frac{1+i}{\sqrt{2}}$

Tomemos $\text{Cl}(\sqrt[8]{2}, \rho) = \text{Cl}(\sqrt[8]{2}, i)$



Luego existen

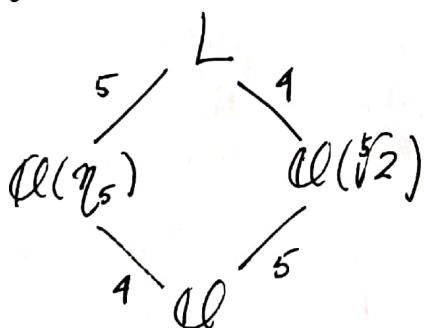
$$\sqrt[8]{2} \xrightarrow{\sigma} \sqrt[8]{2} \quad ; \quad \sqrt[8]{2} \xrightarrow{\tau} \rho \sqrt[8]{2} \quad ; \quad \sigma^2 = \tau^8 = \text{id}$$

Vemos que se cumplen

$$\begin{aligned} \sigma^r(i) &= -i \\ \sigma^r(\sqrt[8]{2}) &= \rho^r \sqrt[8]{2} \end{aligned} \quad ; \quad \begin{aligned} \sigma \tau^r(i) &= -i \\ \sigma \tau^r(\sqrt[8]{2}) &= \sigma(\rho^r \sqrt[8]{2}) = \rho^{-r} \sqrt[8]{2} \end{aligned}$$

En particular, $\tau \sigma = \sigma \tau^{-1}$

[2] $x^5 - 2$, $\gamma_5 = e^{\frac{2\pi i}{5}}$



$$\begin{aligned} \gamma_5 &\xrightarrow{\sigma} \gamma_5^2 \\ \sqrt[5]{2} &\xrightarrow{\sigma} \sqrt[5]{2} \end{aligned} \quad ; \quad \begin{aligned} \gamma_5 &\xrightarrow{\tau} \gamma_5^5 \\ \sqrt[5]{2} &\xrightarrow{\tau} \gamma_5 \sqrt[5]{2} \end{aligned} \quad ; \quad \sigma^4 = \tau^5 = \text{id}$$