El teorema fundamental de la teoria de Galois

Facultad de Ciencias UNAM

Introducción

En esta sección concluimos nuestro estudio de la teoría de Galois. Notaras que ya habíamos visto algunos de los resultados de esta sección pero los escribimos por referencia. Por la importancia de todos los resultados que veremos, algunos libros dicen que todos estos resultados son el *teorema fundamental de la teoría de Galois*.

Propiedades básicas de $\mathrm{Gal}(L/K)$ con $F \subset K \subset L$ y L/F de Galois

Teorema 1

Supongamos que L/F es una extensión de Galois. Si K es un campo tal que $F \subset K \subset L$, entonces

a) $L_{\mathrm{Gal}(L/K)} = K$

b) $\left|\mathrm{Gal}(L/K)\right| = [L : K]$

c) $[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] = [K : F]$

Demostración. Antes que nada, notemos que (a) y (b) son equivalentes a que L/K sea una extensión de Galois. Sin embargo, esto es consecuencia inmediata de que $F \subset K \subset L$ y que L/F es de Galois (c.f. corolario 2.21.10).

Para ver $[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] = [K : F]$ considera las siguientes igualdades

$$\begin{aligned}
[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] &= \frac{\left|\mathrm{Gal}(L/F)\right|}{\left|\mathrm{Gal}(L/K)\right|} && \text{(por el teorema de Lagrange)} \\
&= \frac{[L : F]}{[L : K]} && \text{(porque } L/F \text{ y } L/K \text{ son de Galois)} \\
&= [K : F] && \text{(porque } [L : F] = [L : K][K : F]\text{)}
\end{aligned}$$

□

Propiedades básicas de L_H con $H \leq \mathrm{Gal}(L/F)$ y L/F de Galois

Teorema 2

Supongamos que L/F es una extensión de Galois. Si H es un subgrupo de $\mathrm{Gal}(L/F)$, entonces

a) $\mathrm{Gal}(L/L_H) = H$

b) $[L : L_H] = |H|$

c) $[L_H : F] = [\mathrm{Gal}(L/F) : H]$

Demostración. Antes que nada, veamos que

$$H \subset \mathrm{Gal}(L/L_H).$$

Supongamos que $\sigma \in H \leq \mathrm{Gal}(L/F)$. Para ver que $\sigma \in \mathrm{Gal}(L/L_H)$ necesitamos ver que σ fija a L_H. Sin embargo, esto es consecuencia inmediata de que $\sigma \in H$ y de la definición de L_H. Por lo tanto, $H \subset \mathrm{Gal}(L/L_H)$.

En lo que sigue, veremos una desigualdad y una igualdad que nos ayudaran a demostrar (a) y (b).

- $[L : L_H] \leq |H| \leq \left|\mathrm{Gal}(L/L_H)\right|$:

  La segunda desigualdad es consecuencia inmediata de $H \subset \mathrm{Gal}(L/L_H)$. Para la primera desigualdad, notemos que L/L_H es una extensión finita separable[1] y por lo tanto (por el teorema del elemento primitivo) existe $\alpha \in L$ separable tal que $L = L_H(\alpha)$.

  Ahora bien, considera $g_\alpha(x) \coloneqq \prod_{\sigma \in H}(x - \sigma(\alpha))$. De manera análoga a la demostración del lema 2.21.3, el lector puede verificar que los coeficientes de $g_\alpha(x)$ son fijados por cualquier elemento de H, es decir, que $g_\alpha(x) \in L_H[x]$. Como α es raíz de $g_\alpha(x)$, lo anterior implica que $m_{\alpha, L_H}(x)$ divide a $g_\alpha(x)$ y por lo tanto

  $$|H| = \deg g_\alpha(x) \geq \deg m_{\alpha, L_H}(x) = [L_H(\alpha) : L_H] = [L : L_H].$$

- $\left|\mathrm{Gal}(L/L_H)\right| = [L : L_H]$:

  Antes que nada, notemos que esta igualdad es equivalente a que L/L_H sea de Galois. Sin embargo, esto es consecuencia inmediata de que $F \subset L_H \subset L$ y de que L/F es de Galois.

[1] Pues $F \subset L_H \subset L$ y L/F es finita separable

Juntando $[L : L_H] \leq |H| \leq \left|\mathrm{Gal}(L/L_H)\right|$ y $\left|\mathrm{Gal}(L/L_H)\right| = [L : L_H]$ obtenemos $|H| = \left|\mathrm{Gal}(L/L_H)\right|$. Como $H \subset \mathrm{Gal}(L/L_H)$ y $\mathrm{Gal}(L/L_H)$ es finito, lo anterior implica que

$$H = \mathrm{Gal}(L/L_H). \qquad \text{(esto es (a))}$$

Por otro lado, notemos que $[L : L_H] \leq |H| \leq \left|\mathrm{Gal}(L/L_H)\right|$ y $\left|\mathrm{Gal}(L/L_H)\right| = [L : L_H]$ también implican que

$$[L : L_H] = |H|. \qquad \text{(esto es (b))}$$

Finalmente, para ver (c), recuerda que en el teorema anterior demostramos que si K es un campo tal que $F \subset K \subset L$, entonces

$$[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] = [K : F].$$

Poniendo $K = L_H$ y usando la igualdad $H = \mathrm{Gal}(L/L_H)$, obtenemos

$$[\mathrm{Gal}(L/F) : H] = [\mathrm{Gal}(L/F) : \mathrm{Gal}(L/L_H)] = [L_H : F]. \qquad \text{(esto es (c))}$$

□

Teorema 3

Supongamos que L/F es una extensión de Galois. Si H es un subgrupo de $\mathrm{Gal}(L/F)$, entonces

$$L_H/F \text{ es de Galois} \iff H \text{ es un subgrupo normal de } \mathrm{Gal}(L/F)$$

y en este caso,

$$\mathrm{Gal}(L_H/F) \cong \mathrm{Gal}(L/F)/H.$$

Demostración. Es consecuencia inmediata de que $H = \mathrm{Gal}(L/L_H)$ y de que si K es un campo tal que $F \subset K \subset L$, entonces

- K/F es de Galois $\iff$ $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$ (c.f. teorema 2.23.5) y
- $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F)$ (c.f. teorema 2.23.6).

□

Las funciones $K \mapsto \mathrm{Gal}(L/K)$ y $H \mapsto L_H$

Teorema 4

Supongamos que L/F es una extensión de Galois y denotemos

$$\mathcal{K} = \{K \mid K \text{ es un campo y } F \subset K \subset L\}$$
$$\mathcal{H} = \{H \mid H \text{ es un subgrupo de } \mathrm{Gal}(L/F)\}$$

Entonces las funciones

$$\begin{array}{l} \mathcal{K} \to \mathcal{H} \\ K \mapsto \mathrm{Gal}(L/K) \end{array} \quad \text{y} \quad \begin{array}{l} \mathcal{H} \to \mathcal{K} \\ H \mapsto L_H \end{array}$$

son mutuamente inversas y cada una de ellas revierte inclusiones, es decir,

$$K_1 \subset K_2 \implies \mathrm{Gal}(L/K_1) \supset \mathrm{Gal}(L/K_2) \text{ para todo } K_1, K_2 \in \mathcal{K}$$
$$H_1 \subset H_2 \implies L_{H_1} \supset L_{H_2} \text{ para todo } H_1, H_2 \in \mathcal{H}$$

La demostración de que son mutuamente inversas es consecuencia inmediata de las proposiciones anteriores y la de que revierten inclusiones es muy sencilla y por eso se la dejamos al lector.

Diagramas de subgrupos y subcampos

En los siguientes ejemplos, usaremos el teorema anterior para determinar todos los campos intermedios de una extensión dada. Para esto, es útil recordar la notación de diagramas de subgrupos y diagramas de subcampos.

Supongamos que G es un grupo y que H es un subgrupo de G. Usualmente, esto se denota como

$$\begin{array}{c} G \\ | \\ H \end{array}$$

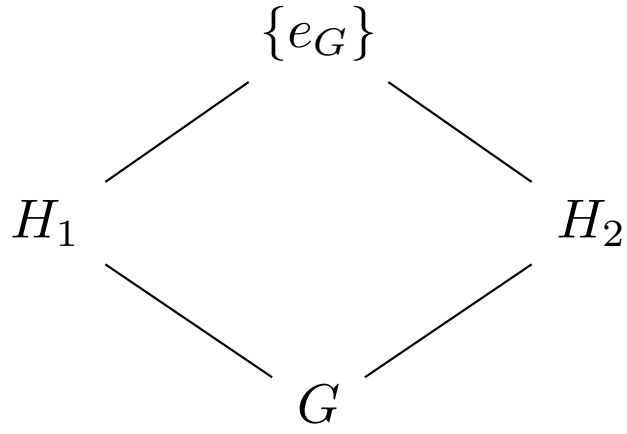
pero para nuestros propósitos, nosotros lo denotaremos como

$$\begin{array}{c} H \\ | \\ G \end{array}$$

Es decir, el grupo chico lo ponemos arriba.

Cabe recalcar que podemos juntar varias veces esta notación para formar diagramas y lo importante es que el grupo chico esta arriba del grupo grande.

Por ejemplo, si G es un grupo, e_G es su unidad y H_1, H_2 son todos los subgrupos no triviales de G, entonces el diagrama



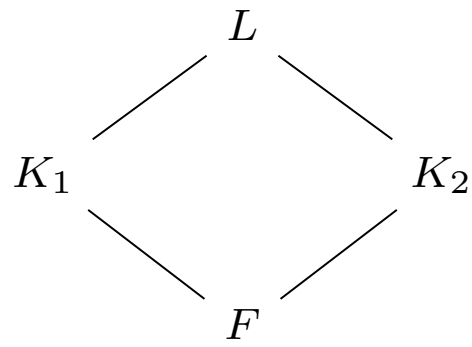
resume toda esta información de forma visual y sencilla.

De manera análoga, (pero "al revés") escribimos

si L/F es una extensión de campos.

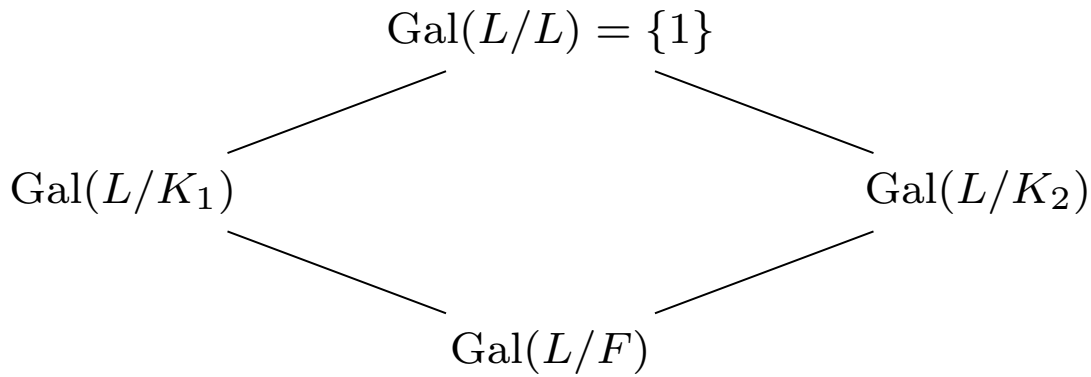
Para entender porque en el caso de subgrupos escribimos al grupo chico arriba y en el caso de subcampos escribimos al campo chico abajo, considera el siguiente ejemplo.

Supongamos que L/F es una extensión de Galois y que K_1, K_2 son todos los campos intermedios no triviales de L/F. Entonces el diagrama de todos los campos intermedios de L/F es



(1)

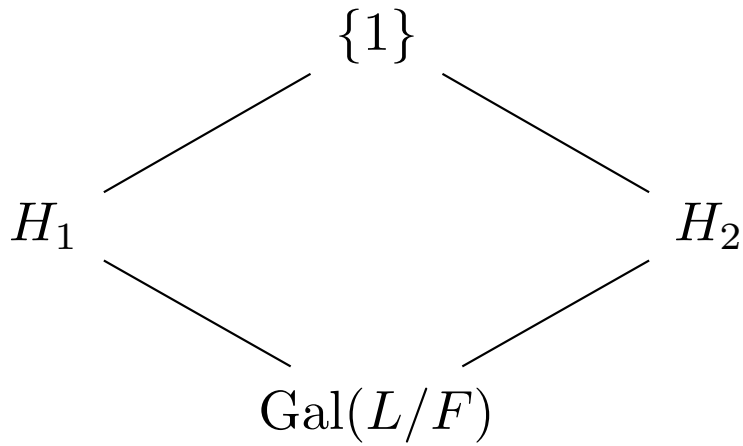
Por el teorema anterior, el diagrama de todos los subgrupos de $\mathrm{Gal}(L/F)$ es



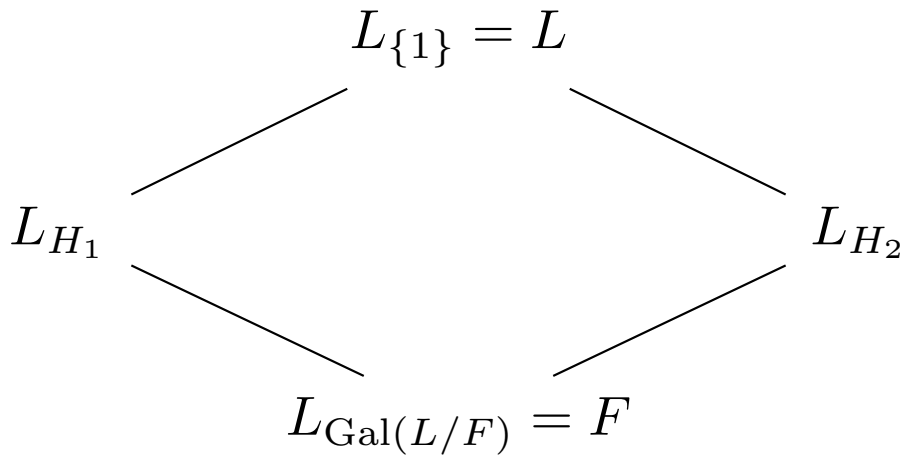
(2)

Notemos que obtenemos (2) simplemente aplicando $K \mapsto \mathrm{Gal}(L/K)$ a cada uno de los campos que aparecen en (1). Si no hubiéramos hecho la convención de escribir al grupo chico arriba, tendríamos que voltear el diagrama. Este ejemplo, también ilustra la importancia de observar que las funciones $K \mapsto \mathrm{Gal}(L/K)$ y $H \mapsto L_H$ revierten inclusiones.

Conversamente, supongamos que L/F es una extensión de Galois y que H_1, H_2 son todos los subgrupos no triviales de $\mathrm{Gal}(L/F)$. Entonces



es el diagrama de todos los subgrupos de $\mathrm{Gal}(L/F)$ y por lo tanto (por el teorema anterior), el diagrama de todos los campos intermedios de L/F es



En los siguientes ejemplos usaremos esta idea para determinar todos los campos intermedios de una extensión dada.

Los campos intermedios de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

En lo que sigue, determinaremos explícitamente a todos los campos intermedios de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Antes que nada, notemos que podemos usar el teorema 4 porque $\mathbb{Q}(\sqrt{2},\sqrt{3})$ es el campo de descomposición de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$. Mas aun, recordemos que en la sección 2.18 vimos que si

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

entonces el homomorfismo de grupos de $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$ en $\mathbb{Z}_2 \times \mathbb{Z}_2$ que satisface

$$\sigma \mapsto (1,0) \quad \text{y} \quad \tau \mapsto (0,1)$$

es un isomorfismo.

Es fácil verificar (por contradicción) que los subgrupos no triviales de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son precisamente

$$\{(0,0),(1,0)\}, \quad \{(0,0),(0,1)\}, \quad \{(0,0),(1,1)\}.$$

Usando el isomorfismo[2], vemos que los subgrupos no triviales de $\text{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$ son precisamente

$$\{1,\sigma\},\ \{1,\tau\},\ \{1,\sigma\tau\}.$$

Por lo tanto, los campos intermedios de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ son precisamente

$$L_{\{1,\tau\}},\ L_{\{1,\sigma\}},\ L_{\{1,\sigma\tau\}}$$

En lo que sigue, determinaremos estos subcampos explícitamente.

[2]Recuerda que este isomorfismo satisface $(1,0) \mapsto \sigma$ y $(0,1) \mapsto \tau$.

Antes que nada, recordemos que todo elemento de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ es de la forma

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}, \quad a,b,c,d\in\mathbb{Q}. \tag{3}$$

Empecemos por determinar $L_{\{1,\tau\}}$. Por definición, $\alpha\in L_{\{1,\tau\}}$ si y solo si $\{1,\tau\}$ fija a α si y solo si $\tau\alpha=\alpha$. Como $\tau(\sqrt{2})=\sqrt{2}$ y $\tau(\sqrt{3})=-\sqrt{3}$, entonces (3) implica que los $\alpha\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ tales que $\tau\alpha=\alpha$ son precisamente los elementos de la forma $a+b\sqrt{2}$ con $a,b\in\mathbb{Q}$. Es decir,

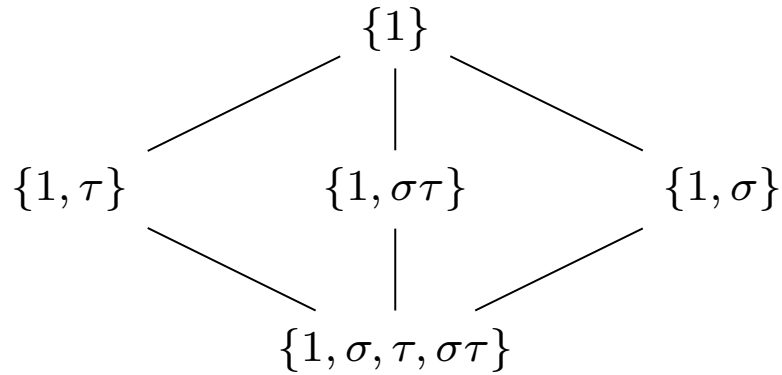
$$L_{\{1,\tau\}}=\mathbb{Q}(\sqrt{2})$$

De manera análoga es fácil ver que

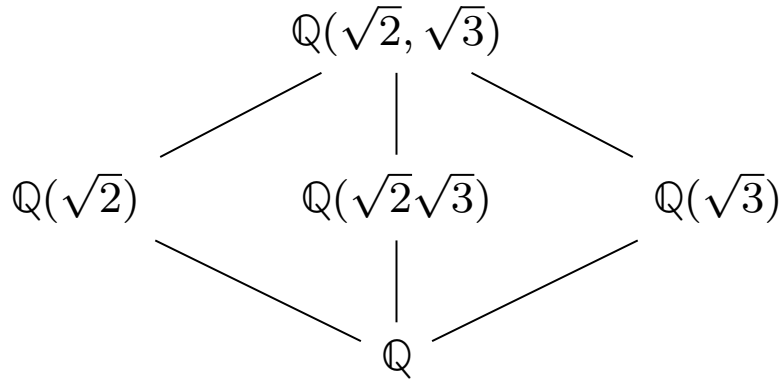
$$L_{\{1,\sigma\}}=\mathbb{Q}(\sqrt{3}) \quad \text{y} \quad L_{\{1,\sigma\tau\}}=\mathbb{Q}(\sqrt{2}\sqrt{3})$$

Usando diagramas de subgrupos y subcampos podemos reescribir lo anterior de la siguiente manera.

Considera los siguientes diagramas.



(4)



(5)

Entonces

- (4) es el diagrama de todos los subgrupos de $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)$,
- (5) es el diagrama de todos los campos intermedios de $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,
- la imagen de (4) bajo $H \mapsto L_H$ es (5), y
- la imagen de (5) bajo $K \mapsto \mathrm{Gal}(L/K)$ es (4).

Los campos intermedios de la extensión $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}$

En lo que sigue, determinaremos explícitamente a todos los campos intermedios de la extensión $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}$ donde $\zeta = \frac{-1+i\sqrt{3}}{2}$ (es una 3-esima raíz primitiva de la unidad).

Antes que nada, notemos que podemos usar el teorema 4 porque $\mathbb{Q}(\zeta, \sqrt[3]{2})$ el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$. Mas aun, recordemos que en la sección 2.18 demostramos que si

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \\ \zeta \mapsto \zeta \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta \mapsto \zeta^2 \end{cases}$$

entonces

$$\sigma^3 = 1, \quad \tau^2 = 1, \quad \sigma\tau = \tau\sigma^2, \quad \text{y}$$
$$\operatorname{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right) = \left\{1, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\right\}.$$

Usando esto, es fácil (pero tedioso) verificar que los subgrupos de $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right)$ son precisamente

$$\langle\sigma\rangle\,,\ \langle\tau\rangle\,,\ \langle\tau\sigma\rangle\,,\ \langle\sigma\tau\rangle$$

donde $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$.
Por lo tanto, los campos intermedios de la extension $\mathbb{Q}(\zeta, \sqrt[3]{2})$ son precisamente

$$L_{\langle\sigma\rangle},\ L_{\langle\tau\rangle},\ L_{\langle\tau\sigma\rangle},\ L_{\langle\sigma\tau\rangle}$$

En lo que sigue, determinaremos estos subcampos explícitamente.
Antes de esto, cabe recalcar que para determinar los subgrupos de $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}\right)$, pudimos haber procedido como en el ejemplo anterior dando un isomorfismo explicito $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})\mathbb{Q}\right) \cong S_3$ y determinando los subgrupos de S_3.

Antes que nada, recordemos que el conjunto

$$\left\{1,\ \sqrt[3]{2},\ (\sqrt[3]{2})^2,\ \zeta,\ \zeta\sqrt[3]{2},\ \zeta(\sqrt[3]{2})^2\right\} \tag{6}$$

es una $\mathbb{Q}$-base de $\mathbb{Q}(\zeta, \sqrt[3]{2})$.

Empecemos por determinar $L_{\langle\sigma\rangle}$. Como $\sigma^3 = 1$, entonces $\langle\sigma\rangle = \{1, \sigma, \sigma^3\}$ y por lo tanto, $\alpha \in L_{\langle\sigma\rangle}$ si y solo si $\sigma\alpha = \alpha$ y $\sigma^2\alpha = \alpha$. Mas aun, como

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \\ \zeta \mapsto \zeta \end{cases} \qquad \sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \zeta^2\sqrt[3]{2} \\ \zeta \mapsto \zeta \end{cases}$$

Es fácil verificar directamente que los únicos elementos de (6) que satisfacen $\sigma\alpha = \alpha$ y $\sigma^2\alpha = \alpha$ son 1 y ζ. Usando esto, es fácil ver que

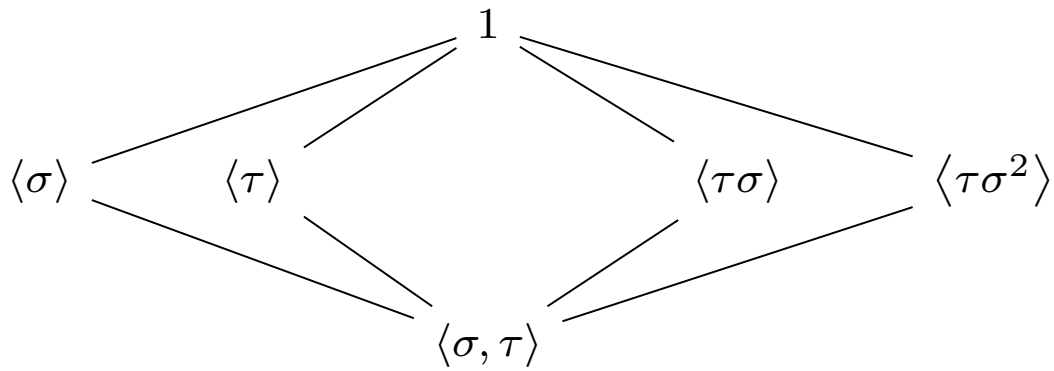
$$L_{\langle\sigma\rangle} = \{a + b\zeta \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\zeta).$$

Análogamente,

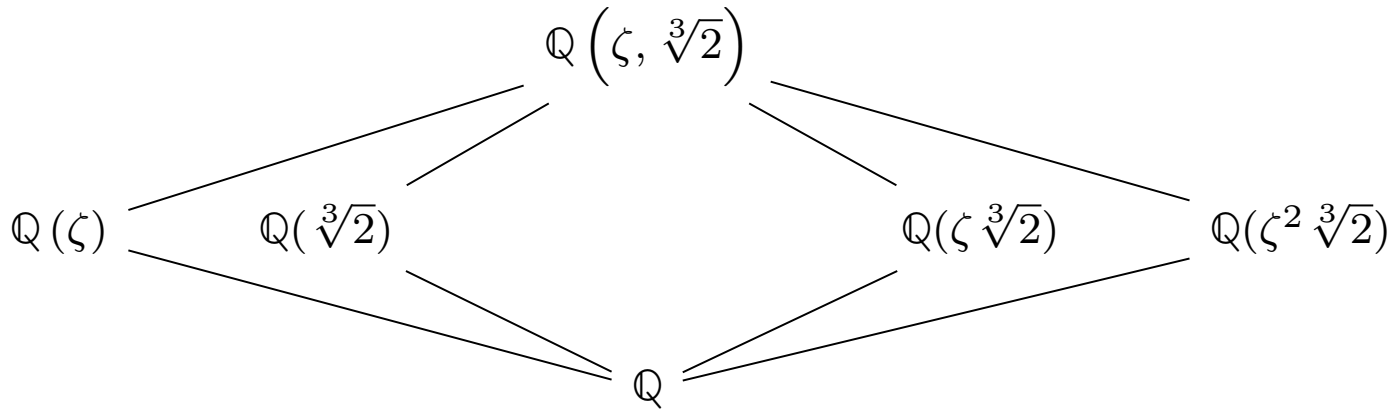
$$L_{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2}), \quad L_{\langle\tau\sigma\rangle} = \mathbb{Q}(\zeta\sqrt[3]{2}), \quad L_{\langle\tau\sigma^2\rangle} = \mathbb{Q}(\zeta^2\sqrt[3]{2})$$

Usando diagramas de subgrupos y subcampos podemos reescribir lo anterior de la siguiente manera.

Considera los siguientes diagramas.



(7)



(8)

Entonces

- (7) es el diagrama de todos los subgrupos de $\mathrm{Gal}\left(\mathbb{Q}(\zeta, \sqrt[3]{2})\right)$,
- (8) es el diagrama de todos los subcampos intermedios de $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}$,
- la imagen de (7) bajo $H \mapsto L_H$ es (8), y
- la imagen de (8) bajo $K \mapsto \mathrm{Gal}(L/K)$ es (7).

Solo hay una cantidad finita de campos intermedios de una extensión finita separable

Corolario 5

Si L/F es finita separable, entonces

$$\mathcal{K} = \{K \mid K \text{ es un campo y } F \subset K \subset L\}$$

es un conjunto finito.

Demostración. Como L/F es finita separable, entonces existe una extensión M/L tal que M/F es de Galois (por supuesto, nos referimos a la cerradura de Galois de L/F). Ahora bien, si

$$\mathcal{K}' = \left\{K \mid K \text{ es un campo y } F \subset K \subset M\right\} \text{ y}$$
$$\mathcal{H}' = \left\{H \mid H \text{ es un subgrupo de } \mathrm{Gal}(M/F)\right\},$$

entonces

- $|\mathcal{K}| \leq \left|\mathcal{K}'\right|$ pues $\mathcal{K} \subset \mathcal{K}'$,
- $\left|\mathcal{K}'\right| = \left|\mathcal{H}'\right|$ por el teorema 4, y
- $\left|\mathcal{H}'\right| < \infty$ porque $\mathrm{Gal}(M/F)$ es un grupo finito.

Juntando todo esto, obtenemos

$$|\mathcal{K}| \leq \left|\mathcal{K}'\right| = \left|\mathcal{H}'\right| < \infty$$

y por lo tanto $\mathcal{K}$ es un conjunto finito. □

Los campos intermedios de la extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$

En lo que sigue, determinaremos explícitamente a todos los campos intermedios de la extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$.

Antes que nada, recordemos que vimos que $\mathbb{F}_{p^n}/\mathbb{F}_p$ es de Galois[3] y por lo tanto, podemos usar el teorema 4. Mas aun, en la sección 2.21 también vimos que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle \cong \mathbb{Z}_n$ donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es tal que $\sigma(\alpha) = \alpha^p$ y el isomorfismo $\langle\sigma\rangle \cong \mathbb{Z}_n$ esta dado por $k \overset{\phi}{\mapsto} \sigma^k$.

Ahora bien, como

$$\{\text{subgrupos de } \mathbb{Z}_n\} = \{\mathbb{Z}_d \mid d \in \mathbb{Z}_{\geq 0} \text{ divide a } n\}$$

y $\phi : \mathbb{Z}_n \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$ es un isomorfismo, entonces

$$\{\text{subgrupos de } \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)\} = \{\phi(\mathbb{Z}_d) \mid d \in \mathbb{Z}_{\geq 0} \text{ divide a } n\}$$

y por lo tanto

$$\{\text{campos intermedios de } \mathbb{F}_{p^n}/\mathbb{F}_p\} = \{L_{\phi(\mathbb{Z}_d)} \mid d \in \mathbb{Z}_{\geq 0} \text{ divide a } n\}$$

[3]Es el campo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$ (c.f. proposición 2.13.8).

Por eso, para determinar explícitamente a todos los subcampos intermedios de $\mathbb{F}_{p^n}/\mathbb{F}_p$, necesitamos determinar explícitamente a $L_{\phi(\mathbb{Z}_d)}$ con d divisor de n. Para esto, notemos que

$$\phi(\mathbb{Z}_d) = \left\{\phi(kd) \mid k \in \{1, \ldots, n/d\}\right\} = \left\{\sigma^{kd} \mid k \in \{1, \ldots, n/d\}\right\}$$

y en particular, $\left|\phi(\mathbb{Z}_d)\right| = n/d$. Usando el inciso (b) del teorema 2 obtenemos

$$[\mathbb{F}_{p^n} : L_{\phi(\mathbb{Z}_d)}] = \left|\phi(\mathbb{Z}_d)\right| = n/d. \tag{9}$$

De donde

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \underbrace{[\mathbb{F}_{p^n} : L_{\phi(\mathbb{Z}_d)}]}_{n/d}[L_{\phi(\mathbb{Z}_d)} : \mathbb{F}_p]. \tag{10}$$

lo cual implica que $[L_{\phi(\mathbb{Z}_d)} : \mathbb{F}_p] = d$. Por el lema 2.13.6, esto es equivalente a que $\left|L_{\phi(\mathbb{Z}_d)}\right| = p^d$ y por lo tanto $L_{\phi(\mathbb{Z}_d)} \cong \mathbb{F}_{p^d}$. Si hacemos la convención $L_{\phi(\mathbb{Z}_d)} = \mathbb{F}_{p^d}$, entonces podemos resumir lo anterior de la siguiente manera:

$$\{\text{campos intermedios de } \mathbb{F}_{p^n}/\mathbb{F}_p\} = \{\mathbb{F}_{p^d} \mid d \in \mathbb{Z}_{\geq 0} \text{ divide a } n\}$$

A pesar de que demostramos $L_{\phi(\mathbb{Z}_d)} \cong \mathbb{F}_{p^d}$ demostrando que $[L_{\phi(\mathbb{Z}_d)} : \mathbb{F}_p] = d$, veamos que la convención $L_{\phi(\mathbb{Z}_d)} = \mathbb{F}_{p^d}$ es muy razonable dando una descripción explicita de $L_{\phi(\mathbb{Z}_d)}$:

$$\begin{aligned} L_{\phi(\mathbb{Z}_d)} &= \left\{\alpha \in \mathbb{F}_{p^n} \mid \tau\alpha = \alpha \text{ para toda } \tau \in \phi(\mathbb{Z}_d)\right\} \\ &= \left\{\alpha \in \mathbb{F}_{p^n} \mid \sigma^{kd}\alpha = \alpha \text{ para toda } k \in \{1, \ldots, n/d\}\right\} \\ &= \left\{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^{kd}} = \alpha \text{ para toda } k \in \{1, \ldots, n/d\}\right\} \\ &= \left\{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^d} = \alpha\right\} \end{aligned}$$

donde la inclusión "$\supset$" en la ultima igualdad se cumple porque si $\alpha^{p^d} = \alpha$, entonces

$$\alpha^{p^{2d}} = \alpha^{(p^d)^2} = \alpha^{p^d \cdot p^d} = \left(\alpha^{p^d}\right)^{p^d} = \alpha^{p^d} = \alpha$$

y en general, $\alpha^{p^{kd}} = \alpha$ para toda $k \in \mathbb{Z}_{\geq 0}$ si $\alpha^{p^d} = \alpha$.