ALGEBRA 3 2017
CLASE 10
15/9/17 (1)

Estudio de subextensiones de

$\mathbb{Q}[\sqrt[3]{2}, \zeta_3] = \mathbb{Q}(f) \,/\, \mathbb{Q}$

con $f = X^3 - 2$

$\mathbb{Q}(f) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$ extensión Galois

$Gal(f/\mathbb{Q}) \simeq S_3$.

$\forall\, F/\mathbb{Q}$ subextensión, se tiene $Gal(F/\mathbb{Q}) \leqslant S_3$.

$Gal(f/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ donde
$S_3 = \{1, (12), (13), (23), (123), (132)\}$

Notemos $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$

donde $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\zeta_3$, $\alpha_3 = \sqrt[3]{2}\zeta_3^2$

Entonces:

$\sigma_1 = id$

$\sigma_2 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta \\ \zeta \mapsto \zeta \end{array}$ satisface $\begin{array}{l} \sigma_2(\alpha_1) = \alpha_2 \\ \sigma_2(\alpha_2) = \alpha_3 \\ \sigma_2(\alpha_3) = \alpha_1 \end{array}$ $\quad \sigma_2 \longleftrightarrow (1\,2\,3)$

$\sigma_3 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta^2 \\ \zeta \mapsto \zeta \end{array}$: $\quad \alpha_1 \mapsto \alpha_3 \mapsto \alpha_2$ $\quad \sigma_3 \longleftrightarrow (1\,3\,2)$

$\sigma_4 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta \mapsto \zeta^2 \end{array}$ $\quad \begin{array}{l} \alpha_1 \mapsto \alpha_1 \\ \alpha_2 \mapsto \alpha_3 \mapsto \alpha_2 \end{array}$ $\quad \sigma_4 \longleftrightarrow (2\,3)$

$\sigma_5 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta \\ \zeta \mapsto \zeta^2 \end{array}$ $\quad \begin{array}{l} \alpha_1 \mapsto \alpha_2 \mapsto \alpha_1 \\ \alpha_3 \mapsto \alpha_3 \end{array}$ $\quad \sigma_5 \longleftrightarrow (1\,2)$

$\sigma_6 : \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta^2 \\ \zeta \mapsto \zeta^2 \end{array}$ $\quad \begin{array}{l} \alpha_1 \mapsto \alpha_3 \mapsto \alpha_1 \\ \alpha_2 \mapsto \alpha_2 \end{array}$ $\quad \sigma_6 \longleftrightarrow (1\,3)$

Subgrupos de S_3

$\langle 1 \rangle \longleftrightarrow \langle \sigma_1 \rangle = \langle id \rangle$

$\langle (1\,2) \rangle \longleftrightarrow \langle \sigma_5 \rangle$

$\langle (1\,3) \rangle \longleftrightarrow \langle \sigma_6 \rangle$

$\langle (2\,3) \rangle \longleftrightarrow \langle \sigma_4 \rangle$

$\langle (1\,2\,3) \rangle \longleftrightarrow \langle \sigma_2 \rangle = \langle \sigma_3 \rangle$

$S_3 \longleftrightarrow Gal(\mathbb{Q}(R)/\mathbb{Q})$

$Gal(\mathbb{Q}(R)/\mathbb{Q}(R)) = \{id\}$

$Gal(\mathbb{Q}(R)/\mathbb{Q}(\sqrt[3]{2})) = \langle \sigma_4 \rangle$

$Gal(\mathbb{Q}(R)/\mathbb{Q}(\sqrt[3]{2}\xi)) = \langle \sigma_6 \rangle$

$Gal(\mathbb{Q}(R)/\mathbb{Q}(\sqrt[3]{2}\xi^2)) = \langle \sigma_5 \rangle$

$Gal(\mathbb{Q}(R)/\mathbb{Q}(\xi_3)) = \langle \sigma_2 \rangle = \langle \sigma_3 \rangle$

$Gal(\mathbb{Q}(R)/\mathbb{Q}) = S_3$

Sabemos que $\begin{cases} Gal(E/F) = Gal(E/L) \Rightarrow F = L \\ Gal(E/F) < S_3 \end{cases}$

Luego:

$Gal(E/F) = \{id\} \Rightarrow F = \mathbb{Q}(R)$

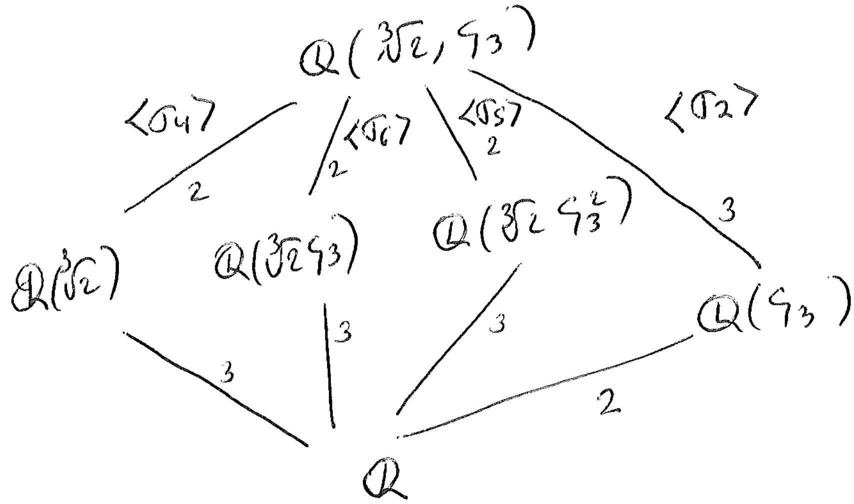
$Gal(E/F) = \langle \sigma_4 \rangle \Rightarrow F = \mathbb{Q}(\sqrt[3]{2})$

$Gal(E/F) = \langle \sigma_6 \rangle \Rightarrow F = \mathbb{Q}(\sqrt[3]{2}\xi)$

$Gal(E/F) = \langle \sigma_5 \rangle \Rightarrow F = \mathbb{Q}(\sqrt[3]{2}\xi^2)$

$Gal(E/F) = \langle \sigma_2 \rangle \Rightarrow F = \mathbb{Q}(\xi)$

$Gal(E/F) = S_3 \Rightarrow F = \mathbb{Q}$.



¿Quiénes son las subextensiones normales de $E/\mathbb{Q}$?

La única es $\mathbb{Q}(\zeta_3)$

¿Quiénes son los subgrupos normales de $Gal(E/\mathbb{Q})$?

El único es $A_3 = \langle (1\,2\,3) \rangle$ que tiene índice 2 ⊗

(Rdo: $H < G$. $H \trianglelefteq G \iff ghg^{-1} \in H, \ \forall h \in H, \forall g \in G$

$\iff gHg^{-1} = H, \ \forall g \in G$

Los subgrupos normales son los que permiten cocientar y considerar G/H que tiene estructura de grupo)

⊗ Por ejemplo $\langle (1\,2) \rangle \ntriangleleft S_3$ pues

$(1\,3\,2)(1\,2)(1\,2\,3) = (1\,3)$.

Observemos que en este ejemplo: ~~[illegible]~~

$$Gal(E/F) \trianglelefteq Gal(E/\mathbb{Q}) \iff$$

~~∀~~ F subextensión normal de E/K ⟺ $Gal(E/F) \trianglelefteq Gal(E/\mathbb{Q})$

Teorema de correspondencia de Galois

① Sea E/K Galois

$$\begin{array}{ccl}
E & \longmapsto & Gal(E/E) = \{id\} \\
| & & \quad\cap| \\
F & \longmapsto & Gal(E/F) = \{\sigma \in Gal(E/K) : \sigma|_F = id\} \\
 & & \qquad\qquad < Gal(E/K) \\
| & & \quad\cap| \\
K & \longmapsto & Gal(E/K)
\end{array}$$

$$\text{Subextensiones de } E/K \xrightarrow{\Phi} \text{Subgrupos de } Gal(E/K)$$

$$E/K \supseteq F/K \longmapsto Gal(E/F) < Gal(E/K)$$

Vamos a probar que Φ es inyectiva en todos los casos (por ahora lo sabemos para E/K finita) y que Φ es sobreyectiva cuando E/K finita.

Para ello, construcción inversa de (1)

Dado un subgrupo $H < Gal(E/K)$, construimos en forma natural una subextensión de E/K:

$$\begin{array}{l} \{1\} \\ \cap \\ H \longmapsto \underline{E^H := \{x \in E \,/\, \sigma(x) = x, \ \forall \sigma \in H\}} \\ \cap \\ Gal(E/K) \end{array}$$

(cuerpo fijo de H)

ⓐ E^H subextensión de E/K?

- $K \subseteq E^H \subseteq E$ como conjuntos
- E^H subcuerpo de E: $x, y \in E^H \Rightarrow x \pm y, xy, 1/x \in E^H$

pues
$$\begin{cases} \sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y, \ \forall x, y \in E^H \\ \sigma(xy) = \sigma(x)\sigma(y) = xy \\ \sigma(1/x) = 1/\sigma(x) = \frac{1}{x} \\ 0, 1 \in E^H \end{cases}$$

<u>Definición</u>: Sea E/K Galois, y sea $H < E/K$.

El subcuerpo fijo de E por H es

$$E^H := \{x \in E \,/\, \sigma(x) = x, \ \forall \sigma \in H\}$$

$$\text{Subgrupos de } Gal(E/K) \xrightarrow{\Psi} \text{Subextensiones de } E/K$$
$$H \longmapsto E^H$$

Observación

Si $H=\{id\}$, $E^H=E$

Proposición: Sea E/K Galois, entonces $E^{Gal(E/K)}=K$
(En particular Φ es inyectiva)

Demostración: $K\subseteq E^{Gal(E/K)}$

pues $\forall a\in K$, $\sigma(a)=a$, $\forall\sigma\in Gal(E/K)$

Sea $\alpha\notin K$, entonces $gr(f(\alpha,K))\geq 2$ y como $f(\alpha,K)$ separable,
$\exists\beta\neq\alpha$ raíz de $f(\alpha,K)$: $\exists\sigma\in Gal(E/K)$ / $\sigma(\alpha)=\beta$
o sea $\sigma(\alpha)\neq\alpha\Rightarrow\alpha\notin E^{Gal(E/K)}$ $\boxtimes$

Notar que habíamos visto antes (lo que usaban Lagrange y Vandermonde) que $E^{S_n}=K$
Lo que hizo Galois es darse cuenta de tomar en cuenta las relaciones entre las raíces, alcanza $E^{Gal(E/K)}=K$:
no hace falta todo el grupo simétrico, solo los que respetan las relaciones entre las raíces

RESUMEN: Sea E/K Galois

$$\text{Subextensiones de } E/K \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \text{Subgrupos de } Gal(E/K)$$

$$F/K \overset{\Phi}{\longmapsto} Gal(E/F)$$

$$E^H \overset{\Psi}{\longmapsfrom} H$$

Φ es inyectiva: $Gal(E/F)=Gal(E/L)\Rightarrow F=L$
pues $Gal(E/F)=Gal(E/L)\Rightarrow$
$E^{Gal(E/F)}=E^{Gal(E/L)}\Rightarrow F=L$

Equivalentemente:

$$\Psi \circ \Phi(F) = F, \quad \forall\ F/K \text{ subextensión de } F/K$$

pues $\Psi \circ \Phi(F) = \Psi(Gal(E/F)) = E^{Gal(E/F)}$.

Sobreyectividad ?

¿ Dado $H < Gal(E/K)$, $\exists\ F/K$ subext de E/K tq
~~[illegible]~~ $Gal(E/F) = H$?

Notar que Φ sobreyectiva $\Leftrightarrow$ $\Phi \circ \Psi(H) = H$, $\forall H < Gal(E/K)$
i.e. $Gal(E/E^H) = H$, $\forall H$

pues:
Φ sobre $\Rightarrow \exists\ F\ /\ Gal(E/F) = H$ y $F = E^{Gal(E/F)}$

o sea $\exists F/\ F = E^H \Rightarrow Gal(E/E^H) = H$

$Gal(E/E^H) = H \Rightarrow H = \Phi(E^H)$ luego Φ sobre.

PROPOSICIÓN: Sea E/K Galois finita

Entonces $Gal(E/E^H) = H$, $\forall H < Gal(E/K)$
(En particular Φ es sobreyectiva)

Demostración:

① $H \subseteq Gal(E/E^H)$:

Sea $\tau \in H$. qpq $\tau \in Gal(E/E^H)$. i.e τ es autom de E
que satisface $\tau(\alpha) = \alpha$, $\forall \alpha \in E^H$

Pero $E^H = \{\alpha \in E\ /\ \psi(\alpha) = \alpha, \forall \psi \in H\}$
esto en particular $\tau \in H$ y por lo tanto $\tau(\alpha) = \alpha$, $\forall \alpha \in E^H$

(Notar que aquí no usamos que E/K es finita)

② $\mathrm{Gal}(E/E^H) = H$

Como ambos grupos son finitos por ser subgrupos del grupo finito $\mathrm{Gal}(E/K)$ (Aquí usamos E/K finita)

Y como ya sabemos q $H \subseteq \mathrm{Gal}(E/E^H)$,

alcanza con probar que $|H| = |\mathrm{Gal}(E/E^H)|$, o que

$|H| \geq |\mathrm{Gal}(E/E^H)|$ (pues $H \subseteq \mathrm{Gal}(E/E^H)$)

Probemos entonces $|H| \geq |\mathrm{Gal}(E/E^H)|$:

Como E es Galois sobre E^H, $\exists\, \theta \in E \,/\, E = E^H[\theta]$

(por el teo del elto primitivo para ext. separables)

y $|\mathrm{Gal}(E/E^H)| = gr(f(\theta, E^H))$

Por otro lado si definimos

$$f := \prod_{\tau \in H} (x - \tau(\theta)) \in E[X]$$

sabemos que $gr(f) = |H|$.

Si probamos $f \in E^H[X]$, entonces $f(\theta, E^H) \mid f \Rightarrow$

$$|\mathrm{Gal}(E/E^H)| = gr(f(\theta, E^H)) \leq gr(f) = |H|.$$

Pero $f \in E^H[X]$ pues $\forall\, \psi \in H$, tenemos

$$\psi(f) = \prod_{\tau \in H} (x - \psi \circ \tau(\theta)) = \prod_{\tau \in H} (x - \tau(\theta)) = f$$

ya que $\{\psi \circ \tau, \tau \in H\} = \{\tau, \tau \in H\}$

por ser H grupo y $\psi \in H$:

$\subseteq$ ✓

$\supseteq$ $\tau = \psi \circ (\psi^{-1} \circ \tau)$.

⊠

Teorema de Galois

Sea E/K Galois

$$\begin{tikzcd}
E \arrow[r, mapsto] \arrow[d, dash] & \{id\} \arrow[d, phantom, "\cap"] \\
E^{Gal(E/F)} = F \arrow[r, shift left, "\Phi"] \arrow[d, phantom, "\supseteq"] & Gal(E/F) \arrow[l, shift left, dashed] \arrow[d, phantom, "\supseteq"] \\
E^H \arrow[r, shift right, dashed] \arrow[d, dash] & H = Gal(E/E^H) \text{ si } E/H \text{ finita} \arrow[l, shift right, "\Psi"'] \arrow[d, phantom, "\cap"] \\
K \arrow[r, mapsto] & Gal(E/K)
\end{tikzcd}$$

Se tiene: $E^{Gal(E/F)} = F \quad (\Psi \circ \Phi = id)$

Y si E/K es <u>finita</u>, $\quad Gal(E/E^H) = H$.

$(\Phi \circ \Psi = id)$

~~Además, ~~[illegible]~~, si $F \subseteq L \Leftrightarrow Gal(E/F) \supseteq Gal(E/L)$:~~

~~$(\Rightarrow)$ $\{\sigma \in Gal(E/K) / \sigma|_L = id\} \subseteq \{\psi \in Gal(E/K) / \sigma|_F = id\}$~~

~~$(\Leftarrow)$ $Gal(E/L) \subseteq Gal(E/F) \Rightarrow E^{Gal(E/L)} \supseteq E^{Gal(E/F)} \Rightarrow L \supseteq F$~~

~~$\{x \in E / \sigma(x) = x, \forall x \in Gal$~~

<u>Observación</u>

① $F \subseteq L \Rightarrow Gal(E/F) \supseteq Gal(E/L)$

pues $\{\sigma \in Gal(E/K) / \sigma|_L = id\} \subseteq \{\sigma \in Gal(E/K) / \sigma|_F = id\}$

② $H \subseteq H' \Rightarrow E^H \supseteq E^{H'}$

pues $\{x \in E / \sigma(x) = x, \forall \sigma \in H'\} \subseteq \{x \in E / \sigma(x) = x, \forall \sigma \in H\}$

Y por lo tanto ③ $F \subseteq L \Leftrightarrow Gal(E/F) \supseteq Gal(E/L)$

Y si E/K finita ④ $H \subseteq H' \Leftrightarrow E^H \supseteq E^{H'}$

Teorema: Sea E/K algebraica.

Entonces E/K Galois (normal y separable)

$\iff E^{Aut(E/K)} = K$

(donde $Aut(E/K)$ son los K-automorfismos de E)

Demostración

($\Rightarrow$) Visto en la correspondencia de Galois

($\Leftarrow$) Qpq $\forall \alpha \in E$, α es separable, luego E/K sep.

y que $\forall \sigma : E \xrightarrow[K]{} \overline{K}$, y $\forall \alpha \in E$, $\sigma(\alpha) \in E$ (para que las inmersiones sean endomorfismos, luego automorfismos, que es otra caracterización de normalidad)

Sea $\alpha \in E$. Como $K(\alpha)/K$ es finita por ser α alg$/K$, $\exists\ \sigma_1, .., \sigma_n$ (finitos) automorfismos de E

tq $\{\sigma(\alpha) ; \sigma \in Aut(E/K)\} = \{\underbrace{\sigma_1(\alpha), \dots, \sigma_n(\alpha)}_{\text{todos} \neq \text{entre sí}}\}$

(O sea con $\sigma_1(\alpha), .., \sigma_n(\alpha)$ obtengo todos los automorfismos de E evaluados en α).

Considero $f := \prod_{1 \leq i \leq n} (X - \sigma_i(\alpha)) \in E[X]$.

Se tiene

1. $f(\alpha) = 0$ pues $\sigma_i(\alpha) = \alpha$ es uno de ellos ($\sigma = id$)
2. $f \in E^{Aut(E/K)}[X]$ pues

$\forall\, \sigma \in \mathrm{Aut}(E/K)$ se tiene

$$\sigma(f) = \prod_{1\le i\le n} (X - \sigma\circ\sigma_i(\alpha)) = \prod_{1\le i\le n} (X - \sigma_i(\alpha)) = f$$

dado que para $\sigma, \sigma_1, .., \sigma_n \in \mathrm{Aut}(E/K)$, se tiene

$\{\sigma_1(\alpha), .., \sigma_n(\alpha)\} = \{\sigma\circ\sigma_1(\alpha), .., \sigma\circ\sigma_n(\alpha)\}$ dado que

$\{\sigma_1(\alpha), .., \sigma_n(\alpha)\}$ son todos los posibles valores de automorfismos que E.

Por lo tanto $f \in E^{\mathrm{Aut}(E/K)}[X] = K[X]$ por hipotesis.

Así $f \in K[X]$

(3) Como f tiene todas raíces $\neq$, α es raíz de un polinomio separable. Luego α es separable

Probemos ahora que $\forall\, \sigma : E \xrightarrow[K]{} \overline{K}$, $\sigma(\alpha) \in E$.

Pero $\forall\, \sigma : E \xrightarrow[K]{} \overline{K}$, $\sigma(\alpha) = \beta$ donde β es raíz de $f(\alpha, K)$

y se tiene $f(\alpha, K) \mid f$ construido arriba. Luego $\beta \in E$

porque todas las raíces de f pertenecen a E. $\boxtimes$